Дж. Прескилл

Квантовая информация и квантовые вычисления

Том 1


Ассоциация
Компьютерных
Исследований


R&C
Dynamics

Lecture Notes for Physics 229: Quantum Information and Computation

John Preskill
California Institute of Technology

September, 1998

Дж. Прескилл

Квантовая информация и квантовые вычисления

Том 1

Перевод с английского
Нечаевой Т. С.

Под научной редакцией
Ефимова С. С. и Новокшонова С. Г.

Москва ♦ Ижевск

2008

УДК 22.314.1
ББК 517.958:530.145.6
П73

Издание осуществлено при финансовой поддержке Российского фонда фундаментальных исследований по проекту №01-02-30013.

Прескилл Дж.
Квантовая информация и квантовые вычисления. Том 1. — М.–Ижевск: НИЦ «Регулярная и хаотическая динамика»; Институт компьютерных исследований, 2008. – 464 с.

Книга Дж. Прескилла, известного специалиста в области квантовых вычислений и квантовой информации, написана на базе одноименного курса, читаемого автором в КАЛТЕХе, и представляет собой подробное и всестороннее введение в эту новую, быстро развивающуюся область науки.

На русском языке книга издается в двух томах. В первом из них излагаются основы теории квантовой информации и квантовых вычислений: свойства, отличающие квантовую информацию от классической; использование этих свойств для разработки систем безопасной передачи информации, квантовой телепортации, быстрых квантовых алгоритмов и другие вопросы.

Ясный физический характер изложения делает книгу доступной для новичка в этой области, находящейся на стыке физики, математики, информатики и технологии. Она содержит необходимые для понимания основного материала сведения из квантовой механики, классической теории информации и основные понятия из классических теорий вычислений и сложности. Каждая глава завершается небольшой подборкой задач разного уровня, способствующих более глубокому усвоению материала.

Для студентов, аспирантов, преподавателей и исследователей в области физики, математики и информатики, интересующихся квантовой теорией информации и вычислений.

ISBN 978-5-93972-651-1 **ББК 22.314.1**

© Дж. Прескилл, 1998
© Перевод на русский язык:
НИЦ «Регулярная и хаотическая динамика», 2008

http://shop.rcd.ru
http://ics.org.ru

Оглавление

Предисловие к русскому изданию

Физика квантовой информации и квантовых вычислений — новая, стремительно развивающаяся область науки, возникшая на стыке квантовой механики, современной математической физики и информатики. Огромный интерес к ней во многом стимулируется захватывающими перспективами, которые обещает открыть реализация ее идей практически во всех областях человеческой деятельности, связанных с передачей, хранением и обработкой информации.

За последние десять лет на русском языке было издано довольно много книг, посвященных данной теме (см., например, [1–7]). Несмотря на это, ощущается некоторый дефицит учебной литературы по теории квантовых вычислений и квантовой информации, адресованной в первую очередь читателю не математику в строгом смысле этого слова. Мы надеемся, что этот пробел может восполнить предлагаемый вашему вниманию курс лекций Дж. Прескилла, на протяжении более чем десяти лет читаемый автором в Калифорнийском Технологическом Институте (КАЛТЕХе), одном из крупнейших мировых исследовательских и образовательных центров в области квантовых информационных технологий. На русском языке книга выходит в двух томах; второй том в настоящее время готовится к изданию.

Большая часть этого курса лекций была написана в конце 90-х годов. Для столь бурно развивающейся отрасли науки это очень большой срок. Тем не менее книга Дж. Прескилла не утратила своего значения и по ряду причин до сих пор остается одним из базовых учебников по теории квантовых вычислений и квантовой информации. Во-первых, автор постоянно работал над совершенствованием содержания этого курса лекций. В частности, по сравнению с исходным вариантом была серьезно переработана и дополнена четвертая глава, посвященная квантовому запутыванию. Добавлена новая глава, посвященная квантовым топологическим вычислениям (войдет во второй том этой книги), теме, которой читатель не найдет ни в одной из вышедших до 2007 г. книг. Таким образом, курс Дж. Прескилла до сих пор остается одним из наиболее полных, отражающим практически все актуальные в настоящее время темы. Во-вторых, автор довольно подробно и математически строго рассматривает решение конкретных за-

дач, но при доказательстве математических теорем и утверждений он, как правило, переходит на качественный язык, справедливо полагая, что физику и инженеру гораздо важнее не уметь доказывать тонкие математические теоремы, а правильно пользоваться ими. Это делает книгу привлекательной для читателя, не имеющего специальной математической подготовки. Наконец, каждая глава данной книги сопровождается небольшим, но тщательно подобранным комплектом задач. Многие из них фактически представляют дальнейшее развитие теоретического материала.

С исследованиями в области квантовых вычислений и квантовой информации тесно связано возрождение интереса к старым принципиальным проблемам, таким как интерпретация квантовой механики, квантовая теория измерений, корреляции в запутанных квантовых состояниях и другие. В свое время по этим проблемам в физическом сообществе сформировалась FAPP-пригодная[1] точка зрения и, хотя проблемы остались, научный интерес к ним стал угасать. Как следствие, в современных учебниках по квантовой механике, преследующих более прагматические цели, этим вопросам уделяется незаслуженно мало внимания.

В этом отношении книга Дж. Прескилла представляет приятное исключение. Три ее главы (2-4) посвящены основаниям квантовой механики. После краткого введения в ее математический аппарат, автор детально обсуждает понятия и вопросы, имеющие непосредственное отношение к главной теме книги. При этом в большинстве случаев его подход оригинален и открывает перед читателем новые аспекты казалось бы хорошо знакомых проблем. Например, в стандартных курсах квантовой механики понятие матрицы плотности вводится аксиоматически. Дж. Прескилл выбирает физически более естественный путь. На простом примере он показывает, что к понятию матрицы плотности мы неизбежно приходим, пытаясь описать квантовомеханическое состояние доступной наблюдению части более широкой системы.

Большое внимание в книге уделено теории квантовых измерений, как ортогональных (измерения фон Неймана), так и обобщенных. При этом автор широко пользуется разложением единицы в гильбертовом пространстве физической системы (или ПОЗМ, положительной операторно-значной мерой), описывающим статистику результатов измерения. В настоящее время ПОЗМ является одним из эффективных инструментов теории квантовых измерений, хотя в русскоязычной учебной литературе это еще не нашло достаточного отражения.

Отдельная глава посвящена квантовому запутыванию несепарабельных двух- и многочастичных состояний, анализу возникающих в этих со-

[1] FAPP — *For All Practical Purposes*, то есть для всех практических целей (Дж. Белл).

стояниях квантовых корреляций, нарушающих неравенства Белла, и другим связанным с этим вопросам. Интерес к ним возобновился в последние годы, поскольку выяснилось, что именно использование запутывание как ресурса позволяет хранить и передавать квантовую информацию, а также оперировать ею и обеспечивать защиту от ошибок.

С этой точки зрения книга Дж. Прескилла может послужить прекрасным дополнением к любому стандартному курсу квантовой механики.

Все это позволяет сказать, что книга Дж. Прескилла представляет собой современный, оригинальный и достаточно полный курс лекций и будет полезна любому читателю, стремящемуся получить систематические знания в области квантовых вычислений и квантовой информации.

1) *Физика квантовой информации*, под ред. Д. Боумейстера, А. Экерта и А. Цайлингера. — М.: Постмаркет (2002).
2) К.А. Валиев, А.А. Кокин, *Квантовые компьютеры: надежда и реальность*. — Москва–Ижевск: РХД (2004).
3) А.А. Кокин, *Твердотельные квантовые компьютеры на ядерных спинах*. — Москва–Ижевск: ИКИ–РХД (2004).
4) Г.П. Берман, Г.Д. Дуплен, Р. Майнъери, В.И. Цифринович, *Введение в квантовые компьютеры*. — Москва–Ижевск: ИКИ–РХД (2004).
5) М. Нильсен, И. Чанг, *Квантовые вычисления и квантовая информация*. — М.: Мир (2006).
6) А. Китаев, А. Шень, М. Вялый, *Классические и квантовые вычисления*. — М.: МЦНМО-ЧеРо (1999).
7) А.С. Холево, *Введение в квантовую теорию информации*. — М.: МЦНМО (2002).

С. Г. Новокшонов

Часть I

Лекции

Глава 1

Введение и обзор

Курс имеет свою web-страницу:

`http://www.theory.caltech.edu/people/preskill/ph219/`

Здесь можно найти общую информацию, в том числе краткое содержание курса и важные ссылки.

К нашему предмету можно подойти с разных позиций, однако в этих лекциях будет принята точка зрения физика-теоретика (то есть моя точка зрения как физика-теоретика). Ввиду междисциплинарного характера предмета я осознаю, что студенты могут иметь самый разный уровень предварительной подготовки, и буду стараться учитывать это в лекциях. Пожалуйста, сообщайте мне, если я буду пользоваться неизвестными вам понятиями.

1.1. Физика информации

Почему физик преподает курс информации? Дело в том, что по меньшей мере несколько десятилетий *физика информации и вычислений* является общепризнанной дисциплиной. Это естественно. В конце концов, информация представляет собой нечто закодированное в состоянии физической системы; вычисление — нечто, что может быть выполнено реальным физически осуществимым устройством. Поэтому изучение информации и вычислений стоит связать с изучением лежащих в их основе физических процессов. Конечно, с технической точки зрения, владение принципами физики и материаловедения необходимо для совершенствования существующего вычислительного «железа» (Карвер Мид называет группой «физики вычислений» свою исследовательскую группу в КАЛТЕХе, которая занимается разработкой чипов).

С более абстрактной теоретической точки зрения, имеется несколько важных этапов в развитии нашего понимания того, как физика ограничивает возможность использовать информацию и оперировать ею. Например:

• **Принцип Ландауэра.** В 1961 году Рольф Ландауэр показал, что уничтожение информации — это непременно *диссипативный* процесс[1]. В его представлении уничтожение всегда влечет за собой сокращение фазового объема и, следовательно, необратимо.

Например, я могу хранить один бит информации, поместив единственную молекулу в ящик слева или справа от разделяющей его перегородки. Уничтожение означает, что мы перемещаем молекулу, скажем, в левую часть, независимо от того, где она находилась сначала – слева или справа. Я могу внезапно удалить перегородку, а затем с помощью поршня медленно сжимать состоящий из одной молекулы «газ» до тех пор, пока молекула действительно не окажется на левой стороне. Эта процедура уменьшает энтропию газа на $\Delta S = k \ln 2$ и сопровождается отводом соответствующего количества тепла из ящика в окружающее пространство. Если этот процесс является изотермическим при температуре T, то выполненная над ящиком работа $W = kT \ln 2$ — это работа, которую совершил я. Если я должен уничтожить информацию, то за это придется расплатиться энергией.

• **Обратимые вычисления.** Логические элементы (вентили), используемые для выполнения вычислений, обычно *необратимы*, например, логический элемент NAND (НЕ И)

$$(a, b) \rightarrow \neg(a \wedge b) \tag{1.1}$$

имеет два входящих бита и один выходящий бит, по которому мы не можем однозначно восстановить информацию на входе. Поскольку логическим элементом уничтожается около (в среднем по его возможным входам) одного бита информации, то, в соответствии с принципом Ландауэра, для его функционирования необходимо затратить работу, как минимум равную $W = kT \ln 2$. Если мы имеем ограниченный запас энергии, возникает теоретический предел продолжительности выполнения вычислений.

Однако в 1973 году Чарльз Беннет установил, что любые вычисления могут быть выполнены с помощью одних лишь обратимых операций, и, таким образом, в принципе нет необходимости ни в диссипации, ни в затратах энергии[2]. Фактически, мы можем создать обратимую версию логи-

[1] R. Landauer, Irreversibility and Heat Generation in the Computing Process, IBM J. Res. Develop., **3**, 183, (1961); русский перевод в сборнике статей *Квантовый компьютер и квантовые вычисления* под ред. В.А. Садовничего, Ижевск, РХД (1999). — *Прим. ред.*

[2] C.H. Bennett, Logical Reversibility of Computation, IBM J. Res. Develop., **17**, 525, (1973); русский перевод в сборнике статей *Квантовый компьютер и квантовые вычисления* под ред. В.А. Садовничего, Ижевск, РХД (1999). Популярное обсуждение физических ограничений, накладываемых на процессы вычислений, а также реализации обратимых вычислений см. в статье Шарль Г. Бенне (он же Чарльз Г. Беннет), Рольф Ландауэр, Физические пределы вычислений, В мире науки №9, 24 (1985), перевод журнала Scientific American. — *Прим. ред.*

ческого элемента NAND, который сохраняет всю входящую информацию: например, элемент Тоффоли

$$(a, b, c) \rightarrow (a, b, c \oplus a \wedge b) \tag{1.2}$$

является обратимым трехбитовым элементом, который «инвертирует» третий бит, если первые два принимают значение 1, и ничего не меняет в остальных случаях. Если $c = 1$, то третий выходящий бит принимает логическое значение НЕ a И b. Заменяя логические элементы NAND элементами Тоффоли, мы можем превратить необратимые вычисления в обратимые. В принципе эти вычисления могут быть выполнены с ничтожной диссипацией.

Однако в этом процессе мы производим много лишней информации. Возникает вопрос: может быть, мы всего лишь отложили энергетические затраты и нам придется расплатиться, когда потребуется уничтожить весь этот хлам. Обращаясь к этой проблеме, Беннет указал, что обратимый компьютер может выполнить вычисления до конца, распечатать ответ (логически обратимая операция), а затем совершить все шаги в обратном направлении, чтобы вернуться к начальному состоянию. Эта процедура удаляет избыточную информацию без каких-либо энергетических затрат.

Тогда в принципе нам не нужно тратить энергию для выполнения вычислений. На практике, используемые в настоящее время (необратимые) компьютеры рассеивают энергию, во всяком случае на порядки большую, чем $kT \ln 2$ на один элемент, поэтому с технической точки зрения предел Ландауэра не существенен. Но, поскольку вычислительное «железо» продолжает сокращаться в размерах, преодоление предела Ландауэра может оказаться важным для предотвращения плавления деталей, и тогда обратимые вычисления могут оказаться единственной альтернативой.

• **Демон Максвелла.** Идеи Ландауэра и Беннета привели последнего в 1982 году к примирению демона Максвелла со вторым началом термодинамики. Максвелл рассматривал газ в ящике, разделенном перегородкой на две части: A и B. В перегородке имеется заслонка, которой управляет демон. Наблюдая за молекулами, приближающимися к заслонке, он пропускает быстрые молекулы из A в B, а медленные – из B в A. Следовательно, A охлаждается, а B нагревается с пренебрежимо малыми затратами работы. Тепло без затрат переходит из холодной области в горячую, явно нарушая второе начало термодинамики.

Решение Беннета состоит в том, что демон должен собирать и хранить информацию о молекулах. Если объем памяти демона ограничен, то он не может бесконечно продолжать охлаждение газа; в конце концов эта

информация должна быть удалена. В этот момент мы и рассчитываемся энергией за достигнутое охлаждение. (Если же демон не уничтожает свою запись или мы хотим сделать термодинамический расчет до ее удаления, то с записанной информацией следует связывать некоторую энтропию.)[1]

Во многом эти идеи были предвосхищены еще в 1929 году Лео Сцилардом — настоящим пионером физики информации[2]. В своем анализе демона Максвелла Сцилард предложил понятие *бита* информации (само слово «бит» было введено позднее Тьюки) и связал энтропию $\Delta S = k \ln 2$ с приобретением одного бита (по-видимому, Сцилард не осознавал до конца принцип Ландауэра, согласно которому неизбежных затрат требует именно уничтожение бита информации).

Эти примеры показывают, что работа на стыке физики и информации породила замечательные результаты, представляющие интерес как для физиков, так и для исследователей в области вычислений.

1.2. Квантовая информация

Итак, мы выяснили, что «информация материальна»[3], поэтому поучительно посмотреть, что говорит физика об информации. В своей основе Вселенная является квантово-механической. Как квантовая теория освещает природу информации?

Уже на заре квантовой теории должно было стать ясно, что в свете новой физики классические идеи об информации требуют пересмотра. Например, щелчки, регистрируемые детектором, который следит за радиоактивным источником, описываются *истинно случайным* пуассоновским процессом. Напротив, в детерминистской классической динамике нет места истинной случайности [хотя, конечно, поведение сложной

[1]Популярное изложение идей Беннета можно найти в статье Чарльз Г. Беннет, Демоны, двигатели и второе начало термодинамики, В мире науки №1, 52 (1988), перевод журнала Scientific American. Всестороннее обсуждение этих вопросов см. также в книге Б.Б. Кадомцев, *Динамика и информация*, редакция журнала УФН, М. (1999). — *Прим. ред.*

[2]Классическая работа Сцилларда опубликована на немецком языке: L. Szilard, *Über die Entropieverminderung in Einem Thermodynamischen System bei Eingriffen Intelligenter Wesen*, Zeitschrift für Physik, 53, 840–856 (1929); на английском языке статья: L. Szilard, *On the Decrease of Entropy in a Thermodynamic System by the Intervention of Intelligent Beings* публиковалась по меньшей мере трижды (1964, 1983, 2003гг.) см., например, *Maxwell's Demon 2. Entropy, Classical and Quantum Information, Computing*, Ed. by H.S. Leff and A.F. Rex, IoP Publishing, Bristol, Philadelphia, (2003) pp. 110–119. — *Прим. ред.*

[3]Этот очень емкий тезис фактически представляет собой название статьи Р. Ландауэра: R. Landauer, Information is physical, Phys. Today, May, 23–29 (1991). — *Прим. ред.*

(хаотической) системы может быть практически неотличимо от случайного].

Более того, в квантовой теории некоммутирующие наблюдаемые не могут одновременно иметь точно определенные значения (принцип неопределенности). Фактически измерение одной наблюдаемой A неизбежно влияет на результат последующего измерения наблюдаемой B, если A и B не коммутируют. Следовательно, процесс получения информации о физической системе неизбежно возмущает ее состояние. В классической физике не существует подобного ограничения.

Компромисс между получением информации и возмущением состояния системы тесно связан с квантовой случайностью. Поскольку результат измерения несет в себе элемент случайности, мы не можем извлечь из него информацию о начальном состоянии системы.

То, что получение информации является причиной возмущения, также связано с другим существенным различием между квантовой и классической информацией: квантовую информацию нельзя воспроизвести с абсолютной точностью (принцип невозможности клонирования, анонсированный Вутерсом и Зуреком, а также Диксом в 1982 году). Если бы мы могли сделать точную копию квантового состояния, то мы могли бы измерить наблюдаемую данной копии, не нарушая состояние оригинала и отменяя тем самым принцип возмущения. С другой стороны, ничто не мешает нам точно копировать классическую информацию (приятное свойство, дающее возможность засорять жесткие диски).

Эти свойства квантовой информации существенны, но особенно серьезный аспект, отличающий квантовую информацию от классической, выяснен в работе Джона Белла в 1964 году. Он показал, что никакая локальная теория скрытых параметров не может воспроизвести предсказания квантовой механики. Согласно Беллу, квантовая информация может быть закодирована (и фактически закодирована) в нелокальных корреляциях между различными частями физической системы, в корреляциях, не имеющих классического аналога. Я еще вернусь к теореме Белла в этой лекции, но детально мы обсудим ее позднее.

Изучение квантовой информации как последовательной дисциплины началось в 1980-х и достигло расцвета в 1990-х гг. Многие из основных результатов теории классической информации имеют квантовые аналоги, которые были обнаружены и разработаны в последнее время. Некоторые из них мы обсудим в этом курсе, включая сжатие квантовой информации, пределы классической информации, закодированной в квантовых системах, пределы квантовой информации, надежно пересылаемой по квантовому каналу с помехами (шумом).

1.3. Эффективные квантовые алгоритмы

Учитывая то, что квантовая информация обладает множеством необычных свойств, можно было ожидать, что квантовая теория окажет глубокое влияние на наше понимание вычислений. Но то, что это действительно так, для многих из нас явилось как гром среди ясного неба, произведенный Питером Шором в апреле 1994 года [специалист по вычислительной технике AT&T (Американ Телефон энд Телеграф) и выпускник КАЛТЕХа]. Шор показал, что, по крайней мере в принципе, квантовый компьютер может эффективно факторизовать большое число [1].

Факторизация (поиск простых множителей составного числа) является примером *трудно разрешимой* задачи, обладающей следующими свойствами:

— Найденное решение можно *легко проверить*.

— Но найти это решение *сложно*.

То есть, если p и q — большие простые числа, произведение $n = pq$ может быть вычислено быстро (необходимое число элементарных операций примерно равно $\log_2 p \log_2 q$). Но при заданном n найти p и q очень *сложно*. Время, необходимое для поиска множителей, твердо считается (хотя это никогда не было доказано) суперполиномиальным по $\log n$. То есть с ростом n необходимое время растет, как минимум, быстрее любой степени $\log n$. Наиболее известный алгоритм факторизации («решето числового поля») требует

$$\text{time} \simeq \exp\left[c(\ln n)^{1/3}(\ln \ln n)^{2/3}\right], \tag{1.3}$$

где $c = (64/9)^{1/3} \sim 1{,}9$. Текущее состояние дел таково, что 65-разрядные множители 130-разрядного числа могут быть найдены в течение одного месяца сетью сотен процессоров. Используя это для оценки префактора в уравнении (1.3), мы найдем, что факторизация 400-разрядного числа потребовала бы 10^{10} лет, что равно возрасту Вселенной. Итак, даже с учетом существенного развития технологии, факторизация 400-разрядного числа в ближайшее время останется недоступной.

Проблема факторизации интересна с точки зрения теории сложности, как пример задачи, которая считается трудно разрешимой; то есть задачи,

[1] Полная версия статьи: P. Shor, Polinomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, SIAM J. on Computing, **26**, 1484 (1997); русский перевод в сборнике статей *Квантовый компьютер и квантовые вычисления* под ред. В.А. Садовничего, Ижевск, РХД (1999). — *Прим. ред.*

которая не может быть решена за время, полиномиально зависящее от длины входящего сигнала, в данном случае от $\log n$. Она также имеет и практическое значение, поскольку сложность факторизации лежит в основе систем шифрования с открытым ключом, например, широко используемой схемы RSA[1].

Новый волнующий результат, полученный Шором, состоит в том, что квантовый компьютер может выполнять факторизацию за полиномиальное время, например, за время $O[(\ln n)^3]$. Таким образом, если бы у нас был квантовый компьютер, который мог бы факторизовать 130-разрядное число за один месяц (конечно, у нас его нет, пока по крайней мере!), то, следуя алгоритму Шора, он смог бы факторизовать 400-разрядное число менее, чем за три года. Чем сложнее задача, тем большим преимуществом обладает квантовый компьютер.

Результат Шора пробудил мой собственный интерес к квантовой информации (если бы не Шор, не думаю, что я преподавал бы этот курс). Очень приятно размышлять о проблемах, требующих знания теории сложности, квантовой теории и прикладных наук.

1.4. Квантовая сложность

Конечно, работа Шора имела серьезную предысторию. На то, что квантовая система может выполнять вычисления, было впервые явно указано Полем Бениоффом и независимо Ричардом Фейнманом в 1982 году[2]. В известном смысле интерес к этой проблеме был понятен, принимая во внимание неуклонную тенденцию миниатюризации в микросхемотехнике. Если эта тенденция будет продолжаться, мы неизбежно приблизимся к режиму, в котором квантовая теория исключительно важна для функционирования вычислительных устройств. Возможно, это наблюдение обеспечило некоторую мотивацию после работы Бениоффа. Однако главная мотивация Фейнмана была совершенно иной и весьма интересной. Чтобы понять точку зрения Фейнмана, необходимо более точное математическое описание квантовой информации и квантовых вычислений.

Неделимой единицей классической информации является бит: объект, который может принимать любое из двух значений: 0 или 1. Соответству-

[1]R. Rivest, A. Shamir, L. Adleman. — *Прим. ред.*

[2]P. Benioff, Quantum-Mechanical Hamiltonian Models of Turing Machines, J. Stat. Phys., **29**, 515, (1982); R.P. Feynman, Simulation Physics with Computers Int. J. Theor. Phys., **21**, 467 (1982); русские переводы в сборнике статей *Квантовый компьютер и квантовые вычисления* под ред. В.А. Садовничего, Ижевск, РХД (1999). Впервые идея квантовых вычислений была выдвинута Ю.И. Маниным именно в связи с большей информационной емкостью квантовых систем. См. Ю.И. Манин *Вычислимое и невычислимое*, Сов. Радио, М., 1980. — *Прим. ред.*

ющая единица квантовой информации — квантовый бит или *кубит*. Кубит представляет собой вектор в двумерном комплексном векторном пространстве со скалярным (внутренним) произведением; из уважения к классическому биту будем называть элементы ортонормированного базиса в этом пространстве $|0\rangle$ и $|1\rangle$. Тогда нормированный вектор может быть представлен в виде:

$$|\psi\rangle = a|0\rangle + b|1\rangle, \qquad |a|^2 + |b|^2 = 1, \tag{1.4}$$

где $a, b \in \mathbb{C}$. Мы можем выполнить измерение, которое проецирует $|\psi\rangle$ на базис $|0\rangle$, $|1\rangle$. Результат такого измерения не детерминирован — вероятность того, что в итоге мы получим $|0\rangle$, равна $|a|^2$, а вероятность того, что мы получим $|1\rangle$, равна $|b|^2$.

Квантовое состояние N кубитов можно изобразить вектором в 2^N-мерном пространстве. В качестве ортонормированного базиса в этом пространстве можно выбрать состояния, в которых каждый кубит имеет определенное значение $|0\rangle$ или $|1\rangle$. Их можно обозначить двоичными последовательностями чисел, такими как:

$$|01110010\ldots1001\rangle. \tag{1.5}$$

Произвольный нормированный вектор разлагается в данном базисе как

$$\sum_{x=0}^{2^N-1} a_x|x\rangle, \tag{1.6}$$

где каждой двоичной последовательности сопоставляется номер, равный соответствующему ей числу в двоичной системе счисления и изменяющийся в пределах от 0 до $2^N - 1$. Здесь величины a_x — комплексные числа, удовлетворяющие условию $\sum\limits_x |a_x|^2 = 1$. Если мы измеряем все N кубитов, проецируя каждый из них на базис $\{|0\rangle, |1\rangle\}$, то вероятность получения результата $|x\rangle$ равна $|a_x|^2$.

Итак, квантовое вычисление можно описать следующим образом. Мы собираем N кубитов и готовим их в стандартном начальном состоянии, таком как $|0\rangle|0\rangle|0\rangle\cdots|0\rangle$ или $|x = 0\rangle$. Затем применяем к ним унитарное преобразование U. (Преобразование U сконструировано как произведение стандартных *квантовых логических вентилей*, унитарных преобразований, которые действуют лишь на несколько кубитов одновременно). После применения U мы измеряем все кубиты путем проецирования на базис $\{|0\rangle, |1\rangle\}$. Итогом измерения является результат вычисления. Таким образом, окончательным результатом является классическая информация, которая может быть распечатана на листе бумаги и опубликована в журнале «Физикл Ревью» (Physical Review).

Обратите внимание на то, что реализованный квантовым компьютером алгоритм является *вероятностным*. То есть мы можем выполнить одну и ту же операцию дважды и, вследствие случайности процесса квантового измерения, получить разные результаты. Фактически, квантовый алгоритм порождает распределение вероятностей возможных результатов. (В действительности алгоритм факторизации Шора не гарантирует успеха в получении простых множителей; он достигает цели лишь с определенной вероятностью. Однако этого достаточно, поскольку легко проверить, верны ли найденные множители).

Из данного описания должно быть ясно, что квантовый компьютер, в отличие от классического, должен будет работать в соответствии с другими физическими принципами. Тем не менее он не сможет сделать ничего сверх того, что может делать классический компьютер. Классические компьютеры могут хранить векторы, вращать их и моделировать процесс квантового измерения, проецируя векторы на взаимно ортогональные оси. То есть классический компьютер, несомненно, может сколь угодно точно имитировать (моделировать) квантовый компьютер. Наше представление о том, что является вычислимым, не зависит от того, пользуемся мы классическим или квантовым компьютером.

Но мы должны считаться с тем, как много времени занимает это моделирование. Предположим, у нас есть компьютер, который оперирует с умеренным количеством кубитов, например, $N = 100$. Тогда, чтобы представить типичное квантовое состояние компьютера, нам пришлось бы записать $2^N = 2^{100} \sim 10^{30}$ комплексных чисел! Ни один из существующих или будущих цифровых компьютеров не сможет сделать этого. А выполнение произвольного поворота вектора в пространстве размерности 10^{30} находится далеко за пределами вычислительных способностей любого мыслимого классического компьютера.

(Конечно, N классических битов тоже могут принимать 2^N возможных значений. Но полное описание конфигурации каждого из них очень просто — это двоичная последовательность длиной N. Квантовая информация отличается тем, что полное описание даже одной типичной конфигурации N кубитов очень сложно).

Итак, классический компьютер действительно может имитировать квантовый, но с ростом числа кубитов N имитация становится крайне неэффективной. Квантовая механика *сложна* (с точки зрения вычислений), потому что мы должны работать с огромными матрицами — гильбертово пространство слишком велико. Это наблюдение привело Фейнмана к предположению, что квантовый компьютер может оказаться способным выполнять определенные задания, недосягаемые для любого возможного

классического компьютера (квантовому компьютеру не нужно моделировать *самого себя*!). Похоже, что результат Шора поддерживает эту точку зрения.

Так ли неизбежен этот вывод? В конце концов, моделирование должно предоставить способ определения вероятностей всех возможных результатов окончательного измерения. При классическом моделировании совсем не обязательно следовать полному описанию квантового состояния N кубитов. Нас вполне устроил бы *классический вероятностный алгоритм*, результаты которого не определяются однозначно входом, а возникают в соответствии с тем распределением вероятностей, которое генерируется квантовым вычислением. Мы могли бы рассчитывать на выполнение *локального* моделирования, при котором каждый кубит в каждый момент времени имеет определенное значение, а каждый квантовый вентиль может действовать на кубиты различными возможными способами, которые определяются генератором (псевдо-) случайных чисел. Такое моделирование было бы гораздо проще, чем описание эволюции вектора в экспоненциально огромном пространстве.

Однако вывод теоремы Джона Белла однозначно говорит о том, что такое моделирование осуществить невозможно: не существует *локального вероятностного алгоритма*, способного воспроизводить результаты квантовой механики. Таким образом, хотя доказательство этого отсутствует, кажется весьма правдоподобным, что моделирование квантового компьютера является очень сложной задачей для любого классического компьютера.

Чтобы лучше понять, почему математическое описание квантовой информации с необходимостью такое сложное, представим квантовую систему $3N$ кубитов ($N \gg 1$), состоящую из трех подсистем по N кубитов каждая (называемых подсистемами (1), (2) и (3)). Мы случайным образом выбираем квантовое состояние $3N$ кубитов, а затем разделяем три подсистемы, отправляя (1) в Санта-Барбару, (3) — в Сан-Диего, в то время как (2) остается в Пасадене. Теперь мы бы хотели произвести некоторые измерения, чтобы как можно больше узнать о квантовом состоянии. Чтобы облегчить себе задачу, представим, что мы имеем огромное количество копий состояния системы, поэтому мы можем измерить любую из них, а также какие угодно наблюдаемые[1]. Но при одном условии: нам разрешено выполнять измерения лишь внутри одной из подсистем — коллективные измерения, снимающие границы между подсистемами, запрещены. Тогда для *типичного* состояния системы $3N$ кубитов наши измерения почти ни-

[1]Мы не можем сделать копии неизвестного квантового состояния сами, но можем попросить приятеля приготовить множество идентичных копий состояния (он это может, потому что знает, что делать) и не сообщать нам о том, что он сделал.

чего о нем не скажут. Почти вся информация, отличающая одно состояние от другого, содержится в *нелокальных корреляциях* между результатами измерений в подсистемах (1), (2) и (3). Это и есть те самые нелокальные корреляции, которые Белл считал важнейшей частью физического описания.

Мы увидим, что объем информации можно определить количественно с помощью энтропии (большая энтропия подразумевает незначительную информацию). Если мы выбираем состояние $3N$ кубитов случайно, то почти всегда находим, что энтропия каждой подсистемы очень близка к

$$S \cong N - 2^{-(N+1)}, \tag{1.7}$$

результат, полученный Доном Пейджем. Здесь N — максимально возможное значение энтропии, соответствующее случаю, в котором подсистема вообще не несет доступной информации. Таким образом, рассматривая каждую подсистему независимо, при большом N мы можем иметь доступ лишь к экспоненциально малому количеству информации.

То есть измерения дают очень мало информации, если мы не учитываем корреляции результатов, полученных в Сан-Диего, Пасадене и Санта-Барбаре. В терминологии, которой я пользуюсь, измерение корреляции считается «коллективным» измерением (даже если бы фактически оно было выполнено экспериментаторами, которые наблюдали разные части одной и той же копии состояния, а затем созвонились, чтобы сравнить свои результаты). Измеряя корреляции, мы можем узнать намного больше; в принципе мы можем полностью реконструировать состояние.

Любое удовлетворительное описание состояния $3N$ кубитов должно характеризовать эти исключительно сложные нелокальные корреляции. Вот почему классическое моделирование большой квантовой системы требует огромных ресурсов. (Когда подобные нелокальные корреляции существуют между частями системы, мы говорим, что части «запутаны», имея в виду то, что мы не можем полностью расшифровать состояние системы путем ее деления и изучения отдельных частей).

1.5. Квантовый параллелизм

В 1985 году Дэвид Дойч придал идее Фейнмана более конкретную форму. Дойч подчеркнул, что квантовый компьютер может лучше всего реализовать свой вычислительный потенциал, осуществляя то, что он назвал «квантовым параллелизмом»[1]. Чтобы понять, что это означает, лучше всего рассмотреть пример.

[1] D. Deutsch, Quantum Theory, the Church–Turing Principle and the Universal Quantum Computer, Proc. Roy. Soc., London, **A400**, 97 (1985); русский перевод в сборнике статей *Кван-*

Следуя Дойчу, представим черный ящик, вычисляющий функцию, которая преобразует один бит x в один бит $f(x)$. Мы не знаем, что происходит внутри ящика, но это должно быть нечто сложное, потому что вычисление занимает 24 часа. Существует четыре возможные функции $f(x)$ [поскольку каждая из $f(0)$ и $f(1)$ может принять одно из двух возможных значений], и мы бы хотели знать, что вычисляет ящик. Вычисление обеих функций $f(0)$ и $f(1)$ заняло бы 48 часов.

Но мы не располагаем таким временем; нам нужен ответ через 24 часа, а не через 48. И пусть нас даже устроило бы знание того, является $f(x)$ постоянной [$f(0) = f(1)$] или сбалансированной [$f(0) \neq f(1)$][1]. Но даже в этом случае получение ответа займет 48 часов.

Теперь представим квантовый черный ящик, вычисляющий $f(x)$. Конечно, $f(x)$ может быть необратимой, в то время как действие квантового компьютера унитарно и должно быть обратимым, поэтому нам понадобится преобразование U_f, трансформирующее два кубита в два:

$$U_f : |x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle. \tag{1.8}$$

(Этот механизм инвертирует второй кубит, если действие f на первый кубит дает 1, и ничего не делает, если действие f на первый кубит дает 0.) Мы можем определить, является ли $f(x)$ постоянной или сбалансированной, использовав квантовый черный ящик дважды. Но получение одного результата по-прежнему занимает сутки, поэтому такой способ не годится. Можем ли мы получить ответ (за 24 часа), воспользовавшись квантовым черным ящиком *лишь раз*? (Это так называемая «Задача Дойча»).

Так как черный ящик является квантовым компьютером, мы можем выбрать в качестве входящего состояния *суперпозицию* $|0\rangle$ и $|1\rangle$. Если второй кубит приготовлен в начальном состоянии $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, то

$$U_f : |x\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \rightarrow |x\rangle\frac{1}{\sqrt{2}}(|f(x)\rangle - |1 \oplus f(x)\rangle) =$$

$$= |x\rangle(-1)^{f(x)}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \tag{1.9}$$

то есть функция f оказывается локализованной в зависящей от x фазе.

товый компьютер и квантовые вычисления под ред. В.А. Садовничего, Ижевск, РХД (1999). *Прим. ред.*

[1] Этот несколько необычный термин обозначает, что два различных значения функции $f(x)$ сбалансированы, то есть каждое из них соответствует ровно половине значений аргумента x. – *Прим. ред.*

Теперь предположим, что первый кубит приготовлен в начальном состоянии $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Тогда черный ящик действует следующим образом:

$$U_f: \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \rightarrow$$

$$\rightarrow \frac{1}{\sqrt{2}}\left[(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\right]\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \quad (1.10)$$

Наконец, мы можем выполнить измерение, проецирующее первый кубит на базис

$$|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle). \quad (1.11)$$

Очевидно, что мы всегда будем получать $|-\rangle$, если функция $f(x)$ сбалансированная, и $-|+\rangle$, если она постоянна[1].

Итак, мы решили задачу Дойча, а также нашли разницу между тем, что доступно классическому компьютеру, а что квантовому. Классическому компьютеру придется воспользоваться черным ящиком дважды, чтобы отличить сбалансированную функцию от постоянной, а квантовый компьютер выполняет это задание за один раз!

Это возможно, потому что квантовый компьютер не ограничивается вычислением только $f(0)$ или $f(1)$. Он может действовать на суперпозицию $|0\rangle$ и $|1\rangle$, извлекая таким образом «глобальную» информацию о функции, информацию, которая зависит и от $f(0)$, и от $f(1)$. Это и есть квантовый параллелизм.

Теперь предположим, что нас интересуют глобальные свойства функции, которая действует на N битов, функции, зависящей от 2^N возможных аргументов. Чтобы вычислить полную таблицу значений $f(x)$, нам пришлось бы считать f 2^N раз, что совершенно невозможно при $N >> 1$ (например, 10^{30} раз для $N = 100$). Но с квантовым компьютером, действующим в соответствии с

$$U_f : |x\rangle|0\rangle \rightarrow |x\rangle|f(x)\rangle, \quad (1.12)$$

мы могли бы выбрать следующее состояние входного регистра:

$$\left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right]^N = \frac{1}{2^{N/2}}\sum_{x=0}^{2^N-1}|x\rangle, \quad (1.13)$$

[1] В предыдущем описании квантовых вычислений мы говорили, что окончательное измерение проецирует каждый кубит на базис $\{|0\rangle, |1\rangle\}$, но здесь мы допускаем возможность измерения в другом базисе. Чтобы описать эту процедуру в старом базисе, необходимо перед окончательным измерением применить к каждому кубиту подходящее унитарное преобразование.

и, вычислив $f(x)$ только один раз, генерировать состояние:

$$\frac{1}{2^{N/2}} \sum_{x=0}^{2^N-1} |x\rangle|f(x)\rangle. \tag{1.14}$$

В этом состоянии закодированы глобальные свойства f, и мы могли бы извлечь некоторые из них, если бы только смогли придумать для этого эффективный способ.

Это квантовое вычисление демонстрирует «массовый квантовый параллелизм»; имитация подготовки такого состояния на классическом компьютере потребовала бы от нас вычислять f невообразимо огромное количество раз (для $N >> 1$). Тем не менее с помощью квантового компьютера мы сделали это в один заход. Это именно тот тип массового параллелизма, который был осуществлен Шором в его алгоритме факторизации.

Как было отмечено ранее, характерной чертой квантовой информации является то, что она может быть закодирована в нелокальных корреляциях между разными частями физической системы. Действительно, этот случай отображен в уравнении (1.14); свойства функции f хранятся в корреляциях между «входным регистром» и «выходным регистром» квантового компьютера. Однако не так просто расшифровать эту нелокальную информацию.

Например, если бы я измерил входной регистр, то получил бы результат $|x_0\rangle$, где x_0 совершенно случайным образом выбрано из 2^N возможных значений. Такая процедура приготовила бы состояние

$$|x_0\rangle|f(x_0)\rangle. \tag{1.15}$$

Мы могли бы перейти к измерению выходного регистра, чтобы получить значение $f(x_0)$. Но у нас нет возможности определить $f(y_0)$ для любого $y_0 \neq x_0$ посредством дальнейших измерений, поскольку уравнение (1.14) разрушено предыдущим измерением и сложные корреляции между регистрами утеряны. Следовательно, в этом случае квантовое вычисление не дает преимущества перед классическим.

Урок, полученный при решении задачи Дойча, состоит в том, что использование закодированных в уравнении (1.14) корреляций иногда требует изобретательности. Искусство создания квантовых алгоритмов во многом заключается в поиске способов эффективного использования нелокальных корреляций.

1.6. Новая классификация сложности

Компьютер на вашем рабочем столе не является квантовым, но все же это замечательное устройство: в принципе, он способен выполнить любое мыслимое вычисление. Но в действительности существуют вычисления,

которые вы не можете выполнить: вам не хватает либо времени, либо памяти. Но если объем вашей памяти неограничен и вы согласны ждать столько, сколько потребуется, тогда все, что достойно называться вычислением, может быть выполнено вашим маленьким ПК. Поэтому мы называем его «универсальным компьютером».

Классическая теория сложности изучает, какие задачи являются сложными, а какие простыми. Обычно понятия «сложная» и «простая» определяются количеством необходимых времени и/или памяти. Но как придать смысл различию между простым и сложным, не описав аппаратные средства, которые мы будем использовать? Задача может быть сложной для ПК, но, наверное, я смог бы разработать устройство специального назначения, которое смогло бы решить ее гораздо быстрее. А может быть в будущем появится более совершенный универсальный компьютер, способный решить эту задачу гораздо эффективнее. Действительно имеющие смысл различия между сложным и простым должны быть универсальными — они не должны зависеть от того, какое устройство мы используем.

Теория сложности главным образом обращает внимание на различие между алгоритмами, выполняемыми за «полиномиальное время» и за «экспоненциальное время». С любым алгоритмом A, действующим на вход переменной длины, можно сопоставить функцию сложности $T_A(N)$, где N — длина входа в битах. $T_A(N)$ представляет собой максимальное «время» (то есть количество элементарных операций), необходимое для полного выполнения алгоритма для любого входа из N битов. [Например, если A — алгоритм факторизации, то $T_A(N)$ — время, необходимое для факторизации N-битового числа в худшем случае.] Мы говорим, что A выполняется за полиномиальное время, если

$$T_A(N) \leqslant \mathrm{Poly}(N), \tag{1.16}$$

где $\mathrm{Poly}(N)$ обозначает полином от переменной N. Следовательно, полиномиальное время означает, что необходимое для решения задачи время растет не быстрее степени количества входящих битов.

Если задача выполняется не за полиномиальное время, то мы говорим, что ее решение требует экспоненциального времени (хотя на самом деле терминологически это не совсем верно, поскольку, конечно, существуют суперполиномиальные функции типа $N^{\log N}$, которые на самом деле возрастают гораздо медленнее экспоненциальных). Это рациональный критерий определения грани между простым и сложным. Но действительно решающим доводом в пользу этого различия служит его независимость от того, какой компьютер мы используем. Универсальность различия между полиномиальным и экспоненциальным следует из одного из главных результатов теории вычислительных систем: универсальный (классический)

компьютер может моделировать другой в худшем случае с «полиномиальным превышением» (времени). Это значит, что если на вашем компьютере алгоритм выполняется за полиномиальное время, то я всегда могу выполнить его на своем компьютере за полиномиальное время. Если я не могу придумать лучший способ сделать это, то я всегда могу эмулировать работу вашего компьютера на своем; ценой эмуляции является лишь полиномиальное время. Так же ваш компьютер может эмулировать мой, то есть мы всегда будем единодушны в том, какие алгоритмы выполняются за полиномиальное время[1].

Итак, истина в том, что информация и вычисления в физическом мире в основе своей квантово-механические. Но это мнение, каким бы дорогим оно ни было для физиков, не представляло бы особого интереса (по крайней мере, с точки зрения теории сложности), если бы было возможно моделирование квантового компьютера классическим с полиномиальным превышением времени. Тогда квантовые алгоритмы представляли бы лишь технический (специальный) интерес, возможно, не больший, чем будущие успехи классических алгоритмов, способных ускорить решение некоторых задач.

Но если, как показывает (но не доказывает!) алгоритм Шора, никакое моделирование квантового компьютера за полиномиальное время невозможно, то это меняет все. Результаты тридцатилетних исследований в теории сложности по-прежнему останутся математическими истинами, как, например, теоремы, характеризующие возможности классических компьютеров. Но они не устоят как физические истины, поскольку классическая машина Тьюринга — неподходящая модель вычислений, которые действительно могут быть выполнены в физическом мире.

Если квантовая классификация сложности действительно отличается от классической (как подозревается, но не доказано), тогда этот результат перевернет основы информатики. В долгосрочном плане это также может сильно повлиять на технологию. Однако какое значение это имеет для физики? Я не уверен. Но, наверное, это говорит о том, что ни одно мыслимое классическое вычисление не может точно предсказать поведение даже скромного числа кубитов (порядка 100). Это наводит на мысль, что сравнительно небольшие квантовые системы имеют больший потенциал, чем мы можем себе представить даже в самых смелых мечтах.

1.7. Как насчет ошибок?

Существует другое, недавно обнаруженное, свойство квантовой информации, такое же важное, каким может оказаться алгоритм факториза-

[1] Чтобы сделать это утверждение точным, мы должны соблюдать некоторую осторожность. Например, следует исключить некоторые виды «неуместных» машин, как, например, параллельная сеть компьютеров с неограниченным числом станций.

ции Шора: открытие коррекции квантовых ошибок. Действительно, если бы не этот результат, перспективы квантовых вычислительных технологий не казались бы такими радужными.

Как мы уже отмечали, основным свойством квантовой информации, которую использует квантовый компьютер, является наличие нелокальных корреляций между разными частями физической системы. Если я наблюдаю лишь часть системы за раз, то я могу извлечь только очень малую долю закодированной в ней информации.

К сожалению, эти нелокальные корреляции крайне хрупкие и на практике склонны очень быстро распадаться. Проблема в том, что наша квантовая система неизбежно контактирует с намного большей системой — с окружающей ее средой. Полностью изолировать большую квантовую систему от ее окружения практически невозможно, даже если для этого мы предпримем героические усилия. Взаимодействия между квантовым устройством и окружающей средой устанавливают нелокальные корреляции между ними. В итоге квантовая информация, изначально закодированная нами в устройстве, вместо этого оказывается закодированной в корреляциях между устройством и окружающей средой. На этой стадии мы уже не можем получить доступ к информации, наблюдая только за устройством. На практике информация безвозвратно потеряна. С макроскопическим устройством это происходит очень быстро, даже если его связь с окружением достаточно слабая.

Эрвин Шредингер критиковал сторонников основного направления интерпретации квантовой механики, обращая внимание на то, что теория допускает квантовое состояние кота в форме

$$|\text{cat}\rangle = \frac{1}{\sqrt{2}}\big(|\text{dead}\rangle + |\text{alive}\rangle\big). \tag{1.17}$$

В возможности таких состояний Шредингер видел дефект теории, потому что каждый встречавшийся ему кот был либо живым, либо мертвым, а не полуживым-полумертвым.

Одно из наиболее важных достижений квантовой теории за последние 15 лет состоит в том, что мы узнали, как аргументированно ответить Шредингеру. Состояние $|\text{cat}\rangle$ в принципе возможно, но редко наблюдается вследствие его *крайней нестабильности*. Встречавшиеся Шредингеру коты никогда не были достаточно изолированы от окружающей среды. Если бы кто-нибудь приготовил состояние $|\text{cat}\rangle$, то квантовая информация, закодированная в суперпозиции $|\text{dead}\rangle$ и $|\text{alive}\rangle$, *немедленно* переместилась бы в корреляции между котом и окружающей средой, став тем самым полностью недоступной. В действительности окружающая среда постоянно измеряет кота, проецируя его на состояние $|\text{alive}\rangle$ или $|\text{dead}\rangle$. Этот процесс

называется *декогерентизацией*. Мы еще вернемся к изучению декогерентизации в этом курсе.

Итак, чтобы выполнить сложное квантовое вычисление, мы должны приготовить хрупкую суперпозицию состояний относительно большой квантовой системы (хотя, возможно, и не такой большой, как кот). К сожалению, эту систему нельзя полностью изолировать от окружающей среды, поэтому эта суперпозиция, как состояние $|\text{cat}\rangle$, очень быстро распадается. Закодированная квантовая информация быстро теряется и наш квантовый компьютер терпит банкротство.

Другими словами, контакт компьютера с окружающей средой (декогерентизация) служит причиной *ошибок*, разрушающих квантовую информацию. Для того чтобы обеспечить надежную работу квантового компьютера, необходимо найти какой-нибудь способ предотвращения или исправления этих ошибок.

На самом деле декогерентизация — не единственная проблема. Мы не могли бы ожидать безупречно точной работы квантового компьютера, даже если бы добились его полной изоляции от окружающей среды. Реализованные в машине квантовые вентили представляют собой унитарные преобразования, которые одновременно оперируют несколькими кубитами, скажем, унитарные 4×4-матрицы, действующие на два кубита. Конечно, эти унитарные матрицы образуют континуум. Мы можем иметь протокол применения U_0 к двум кубитам, но его выполнение не будет безупречным, поэтому фактическое преобразование

$$U = U_0(1 + O(\varepsilon)) \tag{1.18}$$

будет отличаться от запланированного U_0 на некоторую величину порядка ε. Накопление этих ошибок после применения около $1/\varepsilon$ вентилей приведет к серьезной неудаче. Подобные трудности испытывают и классические аналоговые приборы, тогда как для устройств, работающих на основе дискретной логики, малые ошибки создают гораздо меньше проблем.

В действительности современные цифровые цепи удивительно надежны. Столь высокой точности они достигают, благодаря диссипации. Мы можем представить классический вентиль, действующий на бит, который изображается мячом, находящимся в одном из минимумов двухъямного потенциала. Вентиль может перебросить мяч через промежуточный барьер на другую сторону потенциала. Конечно, действие вентиля не будет идеальным; он может ударить по мячу чуть сильнее. Со временем эти несовершенства могут накопиться и явиться причиной ошибки.

Чтобы исправить положение, мы охлаждаем бит (в буквальном смысле этого слова) после каждого вентиля. Это диссипативный процесс, при кото-

ром высвобождается тепло в окружающую среду и сокращается доступный мячу фазовый объем, приближая его к локальному минимуму потенциала. Поэтому малые ошибки, которые мы можем совершить, скорее ликвидируются путем выброса тепла в окружающую среду, нежели подвергнут риску работу устройства.

Но мы не можем подобным образом охлаждать квантовый компьютер. Контакт с окружающей средой может повысить достоверность классической информации, но закодированную квантовую информацию он разрушит. В более широком смысле аккумуляция ошибок будет проблемой и для обратимых классических вычислений. Чтобы предотвратить накопление ошибок, нужно избавляться от несущей их информации, а удаление информации — всегда диссипативный процесс.

И все же, не будем сдаваться раньше времени. Для борьбы с ошибками в классической информации был разработан изощренный аппарат — теория кодов, исправляющих ошибки. В какой степени можно воспользоваться этим опытом, чтобы также защитить и квантовую информацию?

Как работает классическая коррекция ошибок? Простейшим примером классического кода, исправляющего ошибки, является код повторения: мы заменяем бит, который хотим защитить, его тремя копиями:

$$\begin{aligned} 0 &\to (000), \\ 1 &\to (111). \end{aligned} \tag{1.19}$$

Теперь пусть может возникнуть ошибка, которая инвертирует один из трех битов; если это, скажем, первый бит, то

$$\begin{aligned} (000) &\to (100), \\ (111) &\to (011). \end{aligned} \tag{1.20}$$

Несмотря на эту ошибку, мы по-прежнему можем правильно декодировать бит путем подсчета простого большинства голосов.

Конечно, если вероятность ошибки в каждом бите равна p, то возможно инвертирование двух битов из трех или даже всех трех битов. Двойное инвертирование может произойти в трех разных случаях, таким образом, его вероятность равна $3p^2(1-p)$, в то время как вероятность тройного инвертирования равна p^3. Тогда в целом вероятность того, что подсчет простого большинства потерпит неудачу, равна $3p^2(1-p)+p^3 = 3p^2 - 2p^3$. Но при

$$3p^2 - 2p^3 < p, \quad \text{или} \quad p < \frac{1}{2}, \tag{1.21}$$

код увеличивает достоверность информации.

Мы можем еще больше увеличить достоверность, используя более длинный код. Один такой код (хотя и далеко не самый эффективный) —

код повторения N-битов. Согласно центральной предельной теореме, при $N \to \infty$ распределение вероятностей для среднего значения бита стремится к гауссовскому с шириной $1/\sqrt{N}$. Если $P = \frac{1}{2} + \varepsilon$ — вероятность того, что каждый бит имеет истинное значение, тогда вероятность того, что подсчет простого большинства потерпит неудачу (для большого N), определяется хвостом распределения Гаусса и равна

$$P_{\text{ошибка}} \sim \mathrm{e}^{-N\varepsilon^2}. \tag{1.22}$$

Таким образом, для любого $\varepsilon > 0$, вводя достаточное количество вспомогательных битов, можно достичь сколь угодно высокой надежности. Все в порядке будет даже при $\varepsilon < 0$, если учитывать, что в этом случае большинство голосов отдается ошибочному результату. Лишь при $P = \frac{1}{2}$ эта схема не обоснована, ибо тогда блок из N битов будет случайным и не будет содержать никакой информации.

В 1950-х гг. Джон Фон Нейман показал, что классический компьютер с шумящими элементами может надежно работать, используя достаточное количество вспомогательных битов. Он обратил внимание на то, что при необходимости каждую логическую операцию можно выполнить многократно и получить мажоритарный результат. (Фон Нейману было особенно интересно, почему его мозг так хорошо функционировал, несмотря на ненадежность нейронов. Думаю, что ему было приятно найти объяснение своей сообразительности).

Но теперь мы хотим использовать коррекцию ошибок для того, чтобы сохранить работоспособность *квантового компьютера*. Нетрудно видеть связанные с этим трудности:

1. Фазовые ошибки. Квантовая информация более подвержена ошибкам. В дополнение к ошибкам инвертирования битов

$$\begin{aligned} |0\rangle &\to |1\rangle, \\ |1\rangle &\to |0\rangle \end{aligned} \tag{1.23}$$

в ней также могут появляться и фазовые ошибки:

$$\begin{aligned} |0\rangle &\to |0\rangle, \\ |1\rangle &\to -|1\rangle. \end{aligned} \tag{1.24}$$

Фазовая ошибка влечет за собой серьезные последствия, потому что она превращает состояние $\frac{1}{\sqrt{2}}\big[|0\rangle + |1\rangle\big]$ в ортогональное ему состояние $\frac{1}{\sqrt{2}}\big[|0\rangle - |1\rangle\big]$. Однако классическое кодирование не обеспечивает защиты от фазовых ошибок.

2. Малые ошибки. Как уже отмечалось, квантовая информация непрерывна. Если кубит находится в состоянии

$$a|0\rangle + b|1\rangle, \tag{1.25}$$

то ошибка может изменить a и b на величину порядка ε. Со временем эти малые ошибки могут накапливаться. Классические же методы предназначены для исправления больших ошибок (ошибок инвертирования битов).

3. Измерение – причина возмущения. Согласно схеме подсчета простого большинства голосов, для обнаружения и исправления ошибок нужно было измерять биты в коде. Однако нельзя измерять кубиты, не возмущая закодированную в них информацию.

4. Невозможность клонирования. При классическом кодировании информация защищалась путем создания ее дополнительных копий. Однако известно, что квантовую информацию нельзя воспроизвести с абсолютной точностью.

1.8. Квантовые коды, корректирующие ошибки

Несмотря на эти трудности, оказывается, что квантовая коррекция ошибок действительно возможна. Первый пример квантового кода, исправляющего ошибки, был построен около двух лет назад (угадайте, кем!) Питером Шором. Это открытие привело к возникновению новой, удивительно быстро развившейся, дисциплины – теории квантовых кодов коррекции ошибок. Мы рассмотрим ее позже в этом курсе.

По-видимому, проще всего понять принцип работы квантовой коррекции ошибок, рассматривая оригинальный код Шора. Это наиболее простое квантовое обобщение классического трехбитового кода повторения.

Давайте еще раз рассмотрим этот трехбитовый код, но на этот раз учитывая требование, что в случае с квантовым кодом мы должны быть в состоянии исправлять ошибки без измерения какой бы то ни было закодированной информации.

Предположим, что мы кодируем один кубит тремя кубитами:

$$\begin{aligned} |0\rangle &\to |\bar{0}\rangle = |000\rangle, \\ |1\rangle &\to |\bar{1}\rangle = |111\rangle, \end{aligned} \tag{1.26}$$

другими словами, мы кодируем суперпозицию

$$a|0\rangle + b|1\rangle \to a|\bar{0}\rangle + b|\bar{1}\rangle = a|000\rangle + b|111\rangle. \tag{1.27}$$

Мы хотели бы суметь исправить ошибку инвертирования бита, не разрушая эту суперпозицию.

Конечно, нельзя измерять значение одного кубита. Если я измерил первый кубит и получил результат $|0\rangle$, то это значит, что я приготовил состояние $|\bar{0}\rangle$ для всех трех кубитов, и мы потеряли квантовую информацию, закодированную в коэффициентах a и b.

Но нет никакой необходимости ограничиваться измерением одного кубита. Я мог бы также выполнить коллективное измерение на двух кубитах сразу, и этого достаточно для диагностики ошибки инвертирования бита. Для трехкубитового состояния $|x, y, z\rangle$ я мог бы измерить, скажем, двухкубитовые наблюдаемые $y \oplus z$ или $x \oplus z$ (где $\oplus$ обозначает сложение по модулю два). Как для $|x, y, z\rangle = |000\rangle$, так и для $|x, y, z\rangle = |111\rangle$ результат был бы равен нулю, но если какой-нибудь бит инвертируется, тогда по крайней мере одна из этих величин будет равна единице. Фактически, если инвертируется один бит, то два бита

$$(y \oplus z, x \oplus z) \tag{1.28}$$

непосредственно определяют в двоичной записи позицию (1, 2 или 3) инвертированного бита. Эти два бита составляют *синдром*, диагностирующий появившуюся ошибку.

Например, если инвертировался первый бит

$$a|000\rangle + b|111\rangle \rightarrow a|100\rangle + b|011\rangle, \tag{1.29}$$

тогда измерение $(y \oplus z, x \oplus z)$ дает результат $(0, 1)$, информирующий нас о необходимости инвертировать первый бит; это действительно исправляет ошибку.

Конечно, вместо (большой ошибки) инвертирования бита, возможна малая ошибка:

$$\begin{aligned} |000\rangle &\rightarrow |000\rangle + \varepsilon|100\rangle, \\ |111\rangle &\rightarrow |111\rangle - \varepsilon|011\rangle. \end{aligned} \tag{1.30}$$

Но даже в этом случае вышеописанная процедура будет прекрасно работать. Измеряя $(y \oplus z, x \oplus z)$, мы восстанавливаем собственное состояние этой наблюдаемой. В большинстве случаев (с вероятностью $1 - |\varepsilon|^2$) мы получаем результат $(0, 0)$ и проецируем поврежденное состояние на исходное, исправляя таким образом ошибку. Иногда (с вероятностью $|\varepsilon|^2$) мы получаем результат $(0, 1)$ и проецируем состояние на уравнение (1.29). Но тогда синдром приказывает нам инвертировать первый бит, что восстанавливает исходное состояние. Аналогично, если амплитуда вероятности инвертирования каждого из трех кубитов имеет порядок ε, тогда измерение синдрома с вероятностью порядка $|\varepsilon|^2$ спроецирует состояние на то,

в котором один из трех битов инвертирован, а синдром укажет — какой из них.

Итак, мы преодолели три из четырех ранее упомянутых трудностей. Мы видим, что без ущерба для информации можно выполнить диагностирующее ошибку измерение [ответ на пункт (3)]. Квантовое измерение может проецировать состояние с малой ошибкой на состояние без ошибки или на состояние с большой дискретной ошибкой, способ исправления которой нам известен [ответ на пункт (2)]. Что касается пункта (4), то эта проблема вообще не возникла, поскольку состояние $a|\bar{0}\rangle + b|\bar{1}\rangle$ получено не клонированием — оно не совпадает с $(a|0\rangle + b|1\rangle)^3$; то есть не образовано тремя копиями незакодированного состояния.

Остается только одна проблема: (1) фазовые ошибки. Наш код пока не обеспечивает никакой защиты от них. Если в любом одном из трех кубитов возникнет фазовая ошибка, тогда наше закодированное состояние $a|\bar{0}\rangle + b|\bar{1}\rangle$ преобразуется в $a|\bar{0}\rangle - b|\bar{1}\rangle$ и закодированная квантовая информация разрушится. В действительности *использование кода троекратного повторения* втрое увеличивает частоту возникновения фазовых ошибок. Но, располагая методами, преодолевшими проблемы (2)–(4), мы можем с уверенностью подойти и к первой проблеме. Введя вспомогательные (дополнительные) биты, мы защитились от ошибок инвертирования битов. Это подсказывает как защититься от фазовых ошибок с помощью кодирования вспомогательных (дополнительных) фаз.

Следуя Шору, закодируем один кубит девятью

$$
\begin{aligned}
|0\rangle \to |\bar{0}\rangle &= \frac{1}{2^{3/2}}\big(|000\rangle + |111\rangle\big)\big(|000\rangle + |111\rangle\big)\big(|000\rangle + |111\rangle\big),\\
|1\rangle \to |\bar{1}\rangle &= \frac{1}{2^{3/2}}\big(|000\rangle - |111\rangle\big)\big(|000\rangle - |111\rangle\big)\big(|000\rangle - |111\rangle\big).
\end{aligned}
\tag{1.31}
$$

$|\bar{0}\rangle$ и $|\bar{1}\rangle$ состоят из трех кластеров, в каждом из которых по три кубита, причем каждый кластер приготовлен в одном и том же квантовом состоянии. Каждый из кластеров имеет три вспомогательных бита, поэтому мы можем исправить инвертирование одного бита в любом кластере описанным выше методом.

Предположим, что в одном из кластеров происходит обращение фазы. Ошибка изменяет относительный знак $|000\rangle$ и $|111\rangle$ в этом кластере так, что

$$
\begin{aligned}
|000\rangle + |111\rangle &\to |000\rangle - |111\rangle,\\
|000\rangle - |111\rangle &\to |000\rangle + |111\rangle.
\end{aligned}
\tag{1.32}
$$

Это значит, что относительная фаза поврежденного кластера отличается от фаз двух других кластеров. Таким образом, как и при исправлении инвертированного бита, мы можем определить поврежденный кластер, не измеряя относительные фазы в каждом из них (что вызвало бы возмущение закодированной информации), а сравнивая фазы пар кластеров. В этом случае для проведения сравнения нам необходимо измерить шестикубитовую наблюдаемую, например, наблюдаемую, которая инвертирует от одного до шести кубитов. Поскольку двукратное инвертирование является тождественным преобразованием, квадрат этой наблюдаемой равен единице, а ее собственные значения ± 1. Пара кластеров с одинаковым знаком представляет собой собственное состояние с собственным значением $+1$, а пара кластеров с противоположными знаками — собственное состояние с собственным значением -1. Измерив шестикубитовую наблюдаемую для второй пары кластеров, мы можем определить, какой из кластеров имеет отличный от других знак. Тогда мы применяем унитарное фазовое преобразование к одному из кубитов в этом кластере, чтобы обратить знак и исправить ошибку.

Предположим, что унитарная ошибка $U = I + O(\varepsilon)$ возникает в каждом из девяти кубитов. Наиболее общее однокубитовое унитарное преобразование (с точностью до физически несущественной общей фазы) может быть разложено в первом порядке по ε:

$$U = 1 + i\varepsilon_x \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + i\varepsilon_y \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} + i\varepsilon_z \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \qquad (1.33)$$

Три слагаемых порядка ε в этом разложении можно интерпретировать как оператор инвертирования бита, оператор обращения фазы и оператор, совершающий обе эти операции. Если мы приготовим закодированное состояние $a|\bar{0}\rangle + b|\bar{1}\rangle$, в котором появление унитарных ошибок возможно в каждом кубите, а затем измерим синдромы инвертирования бита и обращения фазы, тогда в большинстве случаев мы вернем состоянию его первоначальный вид. Но с вероятностью порядка $|\varepsilon|^2$ в одном из кубитов возникнет большая ошибка: инвертирование бита, обращение фазы или и то и другое. Благодаря синдрому, мы узнаем, какой из битов инвертировался и в каком из кластеров появилась фазовая ошибка, тогда для исправления ошибки можно применить соответствующее однокубитовое унитарное преобразование.

Исправление ошибки не удастся, если, согласно измерению синдрома, в каждом из двух кластеров имеется две ошибки инвертирования бита (что влечет за собой фазовую ошибку в закодированной информации) или если фазовые ошибки возникнут в двух разных кластерах (что сводится к ошибке инвертирования бита в закодированной информации). Но вероятность

такой двойной фазовой ошибки имеет порядок $|\varepsilon|^4$. Поэтому при достаточно малой $|\varepsilon|$ кодирование увеличивает надежность квантовой информации.

Код также защищает от декогерентизации. Восстанавливая квантовое состояние, независимо от природы ошибки, наша процедура устраняет любое запутывание между квантовым состоянием и его окружением.

Как обычно, коррекция ошибок представляет диссипативный процесс, поскольку информация о природе ошибок изгоняется из квантовой системы. В этом случае, когда информация является неотъемлемой частью записанных результатов наших измерений, при удалении этой записи будет выделяться тепло.

Позднее в этом курсе мы обсудим дальнейшие результаты в области коррекции квантовых ошибок, включая такие как:

- Как и в случае классического кодирования, оказывается, что существуют «хорошие» квантовые коды, позволяющие добиться сколь угодно высокой надежности, пока доля ошибок на один кубит достаточно мала.

- Мы предположили, что процедура исправления ошибок сама по себе выполняется безупречно. Но измерение синдрома оказалось сложным — для выявления ошибок нам было необходимо измерить двухкубитовую и шестикубитовую коллективные наблюдаемые — так что, пытаясь исправить информацию, фактически мы могли нанести ей еще больший ущерб. Однако мы покажем, что коррекция ошибок может быть выполнена так, что она будет эффективно работать даже при появлении случайных ошибок в самом процессе восстановления.

- Чтобы оперировать с квантовым компьютером, мы хотим не только надежно хранить информацию, но также и обрабатывать ее. Мы покажем, что возможно применение квантовых вентилей к закодированной информации.

Подытожим важнейшие идеи, которые лежат в основе квантовой схемы коррекции ошибок:

1) Мы перевели ошибки в цифровую форму. Даже если ошибки в квантовой информации были малыми, мы выполнили измерение, которое проецировало наше состояние на состояние без ошибок либо на состояние с одной из дискретного множества ошибок, способ исправления которой известен.

2) Мы измеряли ошибки, не измеряя информацию. Наши измерения вскрывали природу ошибки, не вскрывая при этом (и, следовательно, не возмущая) закодированную информацию.

3) Ошибки локальны, а закодированная информация нелокальна. Необходимо подчеркнуть основное предположение, лежащее в основе строения кода — ошибки, повреждающие разные кубиты, в хорошем приближении некоррелированы. Мы неявно предположили, что событие, вызывающее ошибку в двух кубитах, гораздо менее вероятно, чем событие, вызывающее ошибку в одном кубите. Конечно, это вопрос физики, обоснованно это предположение или нет — нетрудно представить себе процесс, который станет причиной возникновения ошибок в двух кубитах сразу. Если подобные коррелированные ошибки окажутся достаточно распространенными, то кодирование потерпит неудачу в повышении надежности.

Код пользуется предполагаемой локальной природой ошибок, кодируя информацию нелокальным способом, то есть информация хранится в корреляциях, охватывающих несколько кубитов. Невозможно отличить $|\bar{0}\rangle$ от $|\bar{1}\rangle$, измеряя один кубит из девяти. Если мы измерим один кубит, то с вероятностью $1/2$ получим $|0\rangle$ или $|1\rangle$, независимо от значения закодированного кубита. Чтобы получить доступ к закодированной информации, нам необходимо измерить трехкубитовую наблюдаемую (оператор, инвертирующий все три кубита в кластере, может отличить $|000\rangle + |111\rangle$ от $|000\rangle - |111\rangle$).

Окружающая среда может случайно повлиять на один из кубитов, на самом деле «измеряя» его. Но закодированная информация не может быть повреждена возмущением одного кубита, потому что сам по себе одиночный кубит фактически вообще не несет информации. Нелокально закодированная информация невосприимчива к локальным воздействиям — это основной принцип, на котором основаны квантовые коды коррекции ошибок.

1.9. Квантовое «железо»

Теоретические разработки в области квантовой сложности и квантовой коррекции ошибок сопровождались первыми экспериментальными попытками обработки когерентной квантовой информации. Здесь я кратко опишу некоторые из этих опытов[1].

Чтобы создать аппаратное обеспечение для квантового компьютера, необходима технология, позволяющая управлять кубитами. «Железу» придется столкнуться с некоторыми жесткими техническими требованиями:

[1]Это единственный раздел, в котором очень кратко говорится об аппаратном обеспечении и физических реализациях квантовых вычислений. Читателям, интересующимся этими вопросами, можно порекомендовать книги [1–5] из списка литературы к предисловию, а также цитированную в них литературу. — *Прим. ред.*

1. **Хранение:** Необходимо хранить кубиты в течение длительного времени, достаточного для выполнения интересующих нас вычислений.

2. **Изоляция:** Необходима надежная изоляция кубитов от окружения, чтобы минимизировать ошибки, возникающие вследствие декогерентизации.

3. **Считывание:** Необходимо эффективно и достоверно измерять кубиты.

4. **Вентили:** Необходимо управлять квантовыми состояниями отдельных кубитов и индуцировать контролируемые взаимодействия между ними так, чтобы можно было выполнять квантовые операции.

5. **Точность:** Для надежности работы устройства необходима высокая точность выполнения квантовых операций.

1.9.1. Ионная ловушка

Один из возможных путей достижения этих целей был предложен Игнасио Цираком и Питером Цоллером; его дальнейшей разработкой занялась группа Дэвида Вайнленда из национального института стандартов и технологий (NIST), а также и другие группы. В этой схеме каждый кубит переносится одним ионом, удерживаемым в линейной ловушке Пауля. Квантовое состояние каждого иона – это линейная комбинация основного состояния $|g\rangle$ (интерпретируемого как $|0\rangle$) и особого долгоживущего метастабильного возбужденного состояния $|e\rangle$ (интерпретируемого как $|1\rangle$). Когерентная линейная комбинация двух уровней,

$$a|g\rangle + be^{i\omega t}|e\rangle, \tag{1.34}$$

может существовать в течение времени, сравнимого со временем жизни возбужденного состояния (хотя, конечно, относительная фаза осциллирует вследствие расщепления энергии $\hbar\omega$ между уровнями). Ионы настолько хорошо изолированы, что доминирующей формой декогерентизации может быть спонтанный распад.

Нетрудно считать информацию о состоянии ионов с помощью измерения, проецирующего на базис $\{|g\rangle, |e\rangle\}$. Пусть лазер настроен на переход из состояния $|g\rangle$ в короткоживущее возбужденное состояние $|e'\rangle$. Когда лазер освещает ионы, каждый кубит со значением $|0\rangle$ многократно поглощает и снова излучает свет лазера и таким образом становится видимым (флуоресценция). Кубиты со значением $|1\rangle$ остаются невидимыми.

Вследствие их взаимного кулоновского отталкивания, ионы достаточно хорошо изолированы и на каждый из них можно индивидуально направить импульсы лазеров. Если лазер настроен на частоту перехода ω и сфокусирован на n-ом ионе, то между состояниями $|0\rangle$ и $|1\rangle$ возбуждаются осцилляции Раби. При подходящем выборе продолжительности и фазы лазерного импульса мы сможем реализовать любое однокубитовое унитарное преобразование. В частности, действуя на $|0\rangle$, лазерный импульс может приготовить любую желаемую линейную комбинацию $|0\rangle$ и $|1\rangle$.

Но наиболее сложной частью разработки и создания аппаратного обеспечения квантовых вычислений является организация взаимодействия двух кубитов между собой. В ионной ловушке взаимодействия обусловлены кулоновским отталкиванием между ионами, вследствие чего возникает спектр связанных нормальных мод колебаний захваченных ионов. Когда ион поглощает или излучает лазерный фотон, его центр масс смещается. Но если лазер настроен подходящим образом, то при поглощении или излучении одним ионом произойдет когерентное смещение множества вовлеченных в нормальную моду ионов (эффект Мёссбауэра).

Наиболее низкочастотной колебательной модой (частота ν) является мода центра масс (cm), в которой ионы синхронно колеблются в гармонических ямах ловушек. Ионы можно охладить лазером до температур гораздо меньших ν, так что каждая колебательная мода с большой вероятностью находится в своем основном квантово-механическом состоянии. Теперь представим, что настроенный на частоту $\omega - \nu$ лазер светит на n-ый ион. При должной длительности импульса состояние $|e\rangle_n$ перейдет в $|g\rangle_n$, в то время как cm-осциллятор совершит переход из его основного состояния $|0\rangle_{cm}$ в первое возбужденное $|1\rangle_{cm}$ (рождение cm-«фонона»). В то же время состояние $|g\rangle_n|0\rangle_{cm}$ не находится в резонансе для любого перехода и поэтому не меняется под влиянием лазерного импульса. Таким образом, лазерный импульс совершает унитарное преобразование, действующее как

$$\begin{aligned} |g\rangle_n|0\rangle_{cm} &\to |g\rangle_n|0\rangle_{cm}, \\ |e\rangle_n|0\rangle_{cm} &\to -i|g\rangle_n|1\rangle_{cm}. \end{aligned} \tag{1.35}$$

Эта операция удаляет бит информации, первоначально хранившийся во внутреннем состоянии n-го иона, и помещает его в коллективное состояние движения всех ионов.

Это означает, что внутреннее состояние n-го иона оказало влияние на состояние движения m-го иона ($m \neq n$). В этом смысле нам удалось индуцировать взаимодействие между ионами. Для завершения квантовой операции мы должны переместить квантовую информацию от cm-фоно-

на обратно во внутреннее состояние одного из ионов. Процедура должна быть построена таким образом, чтобы после выполнения операции cm-мода возвращалась в ее основное состояние $|0\rangle_{cm}$. Например, Цирак и Цоллер показали, что квантовый XOR-вентиль (исключающее ИЛИ, или контролируемое НЕ)

$$|x, y\rangle \rightarrow |x, y \oplus x\rangle \tag{1.36}$$

может быть выполнен в ионной ловушке всего пятью лазерными импульсами. Обусловленное этим возбуждение фонона (1.35) для одного захваченного в ловушку иона было продемонстрировано экспериментально группой из NIST.

Серьезным недостатком компьютера на ионных ловушках является то, что по своей природе это медленно работающее устройство. Очевидно, его быстродействие ограничено соотношением неопределенности энергия–время. Поскольку неопределенность энергии лазерного фотона должна быть мала по сравнению с характерной колебательной энергией ν, продолжительность каждого лазерного импульса должна быть велика по сравнению с ν^{-1}. На практике ν, как правило, имеет порядок 100 кГц.

1.9.2. КЭД-резонатор

Другое направление разработки аппаратного обеспечения (предложенное Пеллицари, Гардинером, Цираком и Цоллером) поддерживает группа Джефа Кимбла здесь, в КАЛТЕХе. Идея состоит в том, чтобы захватить несколько нейтральных атомов в маленький с высокой точностью изготовленный оптический резонатор[1]. Вновь квантовая информация может храниться во внутренних состояниях атомов. Но здесь атомы взаимодействуют, благодаря связи с нормальными модами электромагнитного поля в резонаторе (вместо колебательных мод ионной ловушки). Снова, возбуждая переходы импульсами лазеров, мы можем вызвать в одном атоме переход, обусловленный внутренним состоянием другого атома.

Другая возможность хранения кубита – использование поляризации фотона вместо внутреннего состояния иона. Тогда захваченный атом может использоваться как посредник, обеспечивающий взаимодействие одного фотона с другим (вместо фотона, использовавшегося для связи одного атома с другим). Эти эксперименты с «летающим кубитом» продолжаются уже два года. Группа Кимбла продемонстрировала действие двухфотонного квантового вентиля, в котором циркулярная поляризация одного фотона

[1] Квантово-электродинамический (КЭД) резонатор. — *Прим. ред.*

влияет на фазу другого фотона:

$$\begin{aligned} |L\rangle_1|L\rangle_2 &\to |L\rangle_1|L\rangle_2, \\ |L\rangle_1|R\rangle_2 &\to |L\rangle_1|R\rangle_2, \\ |R\rangle_1|L\rangle_2 &\to |R\rangle_1|L\rangle_2, \\ |R\rangle_1|R\rangle_2 &\to e^{i\Delta}|R\rangle_1|R\rangle_2, \end{aligned} \tag{1.37}$$

где $|L\rangle$, $|R\rangle$ обозначают состояния фотонов с левой и правой циркулярной поляризацией. Чтобы добиться этого взаимодействия, один фотон хранится в резонаторе, где он, находясь в состоянии с поляризацией $|L\rangle$, не взаимодействует с атомом и, напротив, сильно связан с ним, будучи в состоянии с поляризацией $|R\rangle$. Второй фотон пересекает резонатор, и он также преимущественно взаимодействует с атомом, находясь в состоянии с одной определенной поляризацией. Волновой пакет второго фотона приобретает некоторый фазовый сдвиг $e^{i\Delta}$, если только оба фотона имеют $|R\rangle$ поляризацию. Так как фазовый сдвиг обусловлен поляризацией обоих фотонов, это нетривиальный двухкубитовый квантовый вентиль.

1.9.3. ЯМР

Третья схема аппаратного обеспечения (темная лошадка) появилась в прошлом году и обошла ионную ловушку и КЭД-резонатор, захватив лидерство в когерентной квантовой обработке. Новая схема использует технику ядерного магнитного резонанса (ЯМР). Здесь носителями кубитов служат ядерные спины определенного типа молекул. Каждый спин может быть ориентирован по ($|\uparrow\rangle = |0\rangle$) или против ($|\downarrow\rangle = |1\rangle$) направления приложенного постоянного магнитного поля. Спины имеют большое время релаксации или декогерентизации, поэтому кубиты могут сохраняться в течение приемлемого времени.

Мы можем также включить импульсное вращающееся магнитное поле с частотой ω (где ω – расщепление энергии между состояниями спин вверх и спин вниз) и возбудить осцилляции Раби между двумя спиновыми состояниями. При подходящей длительности импульса, мы можем выполнить желаемое унитарное преобразование на отдельном спине (точно так же, как в случае ионной ловушки). Все спины в молекуле испытывают воздействие вращающегося магнитного поля, но отзываются на него лишь те, которые находятся в резонансе.

Более того, между спинами существуют диполь-дипольные взаимодействия, и эта связь может использоваться для выполнения операций. Расщепление между $|\uparrow\rangle$ и $|\downarrow\rangle$ для одного спина фактически зависит от состояния

соседних спинов. Следовательно, находится или нет управляющий импульс в резонансе, чтобы опрокинуть спин, обусловлено состоянием другого спина.

Все это уже давно было известно химикам. Тем не менее лишь в прошлом году Гершенфельд и Чанг и независимо Кори, Фами и Гавел указали, что ЯМР предоставляет полезную реализацию квантовых вычислений. Это не было очевидным по ряду причин. Наиболее важная: ЯМР-системы очень *горячие*. Типичная спиновая температура (скажем, комнатная температура) по порядку может быть в миллионы раз больше энергии расщепления между $|0\rangle$ и $|1\rangle$. Это означает, что квантовое состояние нашего компьютера (спинов в отдельной молекуле) существует на фоне очень интенсивного шума – оно испытывает очень сильные термические флуктуации. Этот шум будет искажать квантовую информацию. Более того, мы фактически выполняем нашу процедуру не на одной молекуле, а на макроскопическом образце, содержащем порядка 10^{23} «компьютеров», а считываемый нами сигнал в действительности усреднен по этому ансамблю. Но *вероятностный* характер квантовых алгоритмов обусловлен случайностью квантовых измерений. Следовательно, усреднение по ансамблю не эквивалентно выполнению вычислений на одном приборе; усреднение может скрыть результат.

Гершенфельд и Чанг, а также Кори, Фами и Гавел объяснили, как преодолеть эти трудности. Они описали, как можно готовить, управлять и контролировать «эффективно чистые состояния», выполняя соответствующие операции на термическом ансамбле. Идея состоит в том, чтобы обеспечить усреднение флуктуирующих свойств молекулы во время детектирования сигнала, так чтобы измерялись только интересующие нас когерентные свойства. Они также отметили, что некоторые квантовые алгоритмы (в том числе алгоритм факторизации Шора) можно разработать в детерминистской форме (так что, по крайней мере большая часть компьютеров будет давать один и тот же результат); тогда усреднение по многим вычислениям не нанесет ущерба результату.

Совсем недавно методы ЯМР были использованы для приготовления максимально запутанного состояния трех кубитов, чего не удавалось добиться раньше.

Очевидно, разработки квантового вычислительного «железа» находятся в младенческом состоянии. Необходимо на много порядков величины (как по количеству хранящихся кубитов, так и по количеству операций, которые могут быть применены) увеличить возможности существующего аппаратного обеспечения, прежде чем можно будет пытаться реализовать вычислительные амбиции. В случае метода ЯМР существует особенно се-

рьезное ограничение, которое возникает как принципиальный вопрос, поскольку отношение когерентного сигнала к фону экспоненциально спадает с ростом количества спинов, приходящихся на одну молекулу. На практике было бы очень заманчиво выполнить квантовое ЯМР-вычисление с более чем десятью кубитами. Возможно, для того чтобы квантовые компьютеры в конце концов стали реальными приборами, потребуются новые идеи в разработке квантового аппаратного обеспечения.

1.10. Резюме

Этим завершается наш вводный обзор квантовых вычислений. Мы увидели, что здесь соединились три фактора, сделавшие захватывающим этот предмет.

1) Квантовые компьютеры могут решать сложные задачи. Представим, что построена новая классификация сложности, лучше опирающаяся на фундаментальные законы физики, чем традиционная теория сложности. (Тогда остается более строго охарактеризовать класс задач, в которых квантовые компьютеры имеют большое преимущество перед классическими компьютерами.)

2) Квантовые ошибки можно корректировать. С помощью подходящих методов кодирования мы можем защитить сложную квантовую систему от разрушительного действия декогерентизации. Мы никогда не сможем увидеть настоящего полуживого-полумертвого кота, но, вероятно, сможем приготовить и сохранить в таком состоянии закодированного кота.

3) Квантовое аппаратное обеспечение можно сконструировать. У нас есть привилегия быть свидетелями начала эпохи когерентных манипуляций с квантовой информацией в лаборатории.

Целью этого курса будет углубление нашего понимания пунктов (1), (2) и (3).

Глава 2

Основы I: Состояния и ансамбли

2.1. Аксиомы квантовой механики

В предыдущих лекциях я говорил то одно, то другое о квантовом, хотя нигде не давал определения, что такое квантовая теория. Пришло время восполнить этот пробел.

Квантовая теория — это математическая модель физического мира. Чтобы охарактеризовать модель, необходимо определить, как она будет представлять состояния, наблюдаемые, измерения и динамику.

1. Состояния. Состояния представляют полное описание физической системы. В квантовой механике состояниями являются *лучи* в *гильбертовом пространстве*.

Что такое гильбертово пространство?

1) Это векторное пространство над полем комплексных чисел $\mathbb{C}$. В дальнейшем векторы будут обозначаться как $|\psi\rangle$ (кет-вектор Дирака).
2) В нем определено внутреннее произведение $\langle\varphi|\psi\rangle$. Оно представляет собой отображение упорядоченной пары векторов на $\mathbb{C}$, определяемое свойствами:
   а) положительность: $\langle\psi|\psi\rangle > 0$ для любого $|\psi\rangle \neq 0$;
   б) линейность: $\langle\varphi|(a|\psi_1\rangle + b|\psi_2\rangle) = a\langle\varphi|\psi_1\rangle + b\langle\varphi|\psi_2\rangle$;
   в) эрмитовская симметрия: $\langle\varphi|\psi\rangle = \langle\psi|\varphi\rangle^*$.
3) Оно полно по норме $\|\psi\| = \sqrt{\langle\psi|\psi\rangle}$.
   (В бесконечномерных функциональных пространствах полнота является важным условием, обеспечивающим сходимость разложений по определенным базисам собственных функций, например, рядов Фурье. Однако, как правило, нас вполне удовлетворит работа с внутренними произведениями в конечномерных пространствах.)

Что такое луч? Это класс эквивалентности векторов, отличающихся друг от друга ненулевым комплексным скалярным множителем. В качестве представителя такого класса (для любого ненулевого вектора) можно выбрать вектор, нормированный на единицу

$$\langle\psi|\psi\rangle = 1. \tag{2.1}$$

Будем также говорить, что $|\psi\rangle$ и $e^{i\alpha}|\psi\rangle$, где $|e^{i\alpha}| = 1$, описывают одно и то же физическое состояние.

[Заметим, что каждый луч соответствует возможному состоянию, то есть из двух данных состояний $|\varphi\rangle$ и $|\psi\rangle$ можно сформировать другое состояние $a|\varphi\rangle + b|\psi\rangle$ («принцип суперпозиции»). Физический смысл в этой суперпозиции имеет *относительная фаза*; мы отождествляем $a|\varphi\rangle + b|\psi\rangle$ с $e^{i\alpha}(a|\varphi\rangle + b|\psi\rangle)$, но отличаем его от $a|\varphi\rangle + e^{i\alpha}b|\psi\rangle$.]

2. Наблюдаемые. Наблюдаемой является свойство физической системы, которое в принципе может быть измерено. В квантовой механике наблюдаемая представляется *самосопряженным оператором*. Оператор определяет линейное отображение одного вектора в другой

$$\mathbf{A} : |\psi\rangle \to \mathbf{A}|\psi\rangle, \qquad \mathbf{A}(a|\psi\rangle + b|\varphi\rangle) = a\mathbf{A}|\psi\rangle + b\mathbf{B}|\varphi\rangle. \tag{2.2}$$

Оператор, сопряженный к $\mathbf{A}$, определяется соотношением

$$\langle\varphi|\mathbf{A}\psi\rangle = \langle\mathbf{A}^\dagger\varphi|\psi\rangle \tag{2.3}$$

для любой пары векторов $|\varphi\rangle$ и $|\psi\rangle$ (здесь я обозначил $\mathbf{A}|\psi\rangle$ символом $|\mathbf{A}\psi\rangle$). Оператор $\mathbf{A}$ самосопряжен, если $\mathbf{A} = \mathbf{A}^\dagger$.

Если $\mathbf{A}$ и $\mathbf{B}$ — самосопряженные операторы, то $\mathbf{A}+\mathbf{B}$ — тоже самосопряжен [поскольку $(\mathbf{A}+\mathbf{B})^\dagger = \mathbf{A}^\dagger+\mathbf{B}^\dagger$], но $(\mathbf{AB})^\dagger = \mathbf{B}^\dagger\mathbf{A}^\dagger$ и поэтому $\mathbf{AB}$ — самосопряженный оператор только в том случае, когда $\mathbf{A}$ и $\mathbf{B}$ коммутируют. Заметим, что $\mathbf{AB}+\mathbf{BA}$ и $i(\mathbf{AB}-\mathbf{BA})$ всегда самосопряженные, если таковыми являются $\mathbf{A}$ и $\mathbf{B}$.

Для самосопряженного оператора в гильбертовом пространстве $\mathcal{H}$ существует спектральное представление — его собственные состояния образуют полный, ортонормированный базис в $\mathcal{H}$. Мы можем представить самосопряженный оператор $\mathbf{A}$ в виде

$$\mathbf{A} = \sum_n a_n \mathbf{P}_n. \tag{2.4}$$

Здесь каждое a_n — собственное значение оператора $\mathbf{A}$, а $\mathbf{P}_n$ — соответствующий ортогональный проектор (проекционный оператор) на пространство собственных векторов, отвечающих собственному значению a_n. (Если a_n не вырождено, то $\mathbf{P}_n = |n\rangle\langle n|$ — проектор на соответствующий собственный вектор.) Проекторы $\mathbf{P}_n$ обладают свойствами

$$\mathbf{P}_n\mathbf{P}_m = \delta_{n,m}\mathbf{P}_n, \qquad \mathbf{P}_n^\dagger = \mathbf{P}_n. \tag{2.5}$$

(Определение самосопряженности и формулировка спектральной теоремы для неограниченных операторов в бесконечномерном пространстве более тонкие, но здесь это не должно нас беспокоить.)

3. Измерение. В квантовой механике численным результатом измерения наблюдаемой $\mathbf{A}$ является одно из ее собственных значений; сразу после измерения квантовым состоянием является собственное состояние $\mathbf{A}$, соответствующее измеренному собственному значению a_n. Если непосредственно перед измерением квантовое состояние описывалось вектором $|\psi\rangle$, то результат a_n получается с *вероятностью*

$$\mathrm{Prob}(a_n) = \|\mathbf{P}_n|\psi\rangle\|^2 = \langle\psi|\mathbf{P}_n|\psi\rangle. \tag{2.6}$$

Если полученным результатом является a_n, то (нормированным) квантовым состоянием становится

$$\frac{\mathbf{P}_n|\psi\rangle}{\sqrt{\langle\psi|\mathbf{P}_n|\psi\rangle}}. \tag{2.7}$$

(Заметим, что если тотчас повторить измерение, тогда согласно этому правилу вновь, с вероятностью единица, будет получен тот же самый результат.)

4. Динамика. Эволюция во времени квантового состояния унитарна; она порождается самосопряженным оператором, называемым *гамильтонианом* системы. В *шредингеровской картине* динамики вектор, описывающий систему, изменяется во времени согласно *уравнению Шредингера*

$$\frac{d}{dt}|\psi(t)\rangle = -i\mathbf{H}|\psi(t)\rangle, \tag{2.8}$$

где $\mathbf{H}$ — гамильтониан. Мы можем переписать это уравнение в первом порядке по бесконечно малой величине dt:

$$|\psi(t+dt)\rangle = (\mathbf{1} - i\mathbf{H}dt)|\psi(t)\rangle. \tag{2.9}$$

Оператор $\mathbf{U}(dt) = \mathbf{1} - i\mathbf{H}dt$ унитарен, поскольку $\mathbf{H}$ самосопряжен; в линейном порядке по dt он удовлетворяет соотношению $\mathbf{U}^\dagger\mathbf{U} = 1$. Поскольку произведение унитарных операторов унитарно, эволюция в конечном интервале времени также унитарна:

$$|\psi(t)\rangle = \mathbf{U}(t)|\psi(0)\rangle. \tag{2.10}$$

Если гамильтониан $\mathbf{H}$ не зависит от времени, то можно записать $\mathbf{U}(t) = e^{-i\mathbf{H}t}$.

Этим завершается математическая формулировка квантовой механики. Мы непосредственно замечаем ее некоторые необычные черты. Одна ее странность состоит в том, что уравнение Шредингера линейно, тогда как мы привыкли к нелинейным динамическим уравнениям классической физики. Очевидно, это свойство требует объяснения. Однако гораздо более странным представляется таинственный дуализм; два совершенно разных способа изменения квантовых состояний. С одной стороны, существует детерминистская унитарная эволюция. Если мы точно определили $|\psi(0)\rangle$, то теория предсказывает состояние $|\psi(t)\rangle$ в любой более поздний момент времени.

С другой стороны, имеется вероятностное измерение. Теория не дает определенных предсказаний относительно результатов измерения; она лишь приписывает вероятности различным альтернативам. Это вызывает беспокойство, поскольку неясно, почему, в отличие от других процессов, измерение должно управляться иными физическими законами.

Начинающие изучать квантовую механику, впервые столкнувшись с этими правилами, редко спрашивают «почему?». В этом есть определенная мудрость. Но я надеюсь, что может быть полезно спросить: почему? В будущих лекциях мы вернемся к этому вызывающему замешательство дуализму между унитарной эволюцией и измерением и найдем его разрешение.

2.2. Кубит

Неделимой единицей классической информации является *бит*, принимающий одно из двух возможных значений $\{0, 1\}$. Соответствующую единицу квантовой информации называют «квантовый бит» или *кубит*. Он описывает состояние простейшей квантовой системы.

Минимальное нетривиальное гильбертово пространство двумерно. Будем обозначить ортогональный базис в двумерном векторном пространстве

как $\{|0\rangle, |1\rangle\}$. Тогда наиболее общее нормированное состояние может быть представлено в виде

$$a|0\rangle + b|1\rangle, \tag{2.11}$$

где a, b — комплексные числа, удовлетворяющие условию $|a|^2 + |b|^2 = 1$, а общая фаза физически несущественна. *Кубитом* является состояние в двумерном гильбертовом пространстве, которое может принимать любое значение, описываемое уравнением(2.11). Мы можем выполнить измерение, проецирующее кубит на базис $\{|0\rangle, |1\rangle\}$. Тогда с вероятностью $|a|^2$ мы получим результат $|0\rangle$, а с вероятностью $|b|^2$ — результат $|1\rangle$. Более того, за исключением случаев $a = 0$ и $b = 0$ измерение неизбежно ведет к возмущению состояния. Если начальное значение кубита неизвестно, тогда нет способа определить a и b с помощью одного такого или любого другого мыслимого измерения. Однако *после* измерения кубит оказывается в *известном* состоянии — $|0\rangle$ или $|1\rangle$ — отличающемся (вообще говоря) от его предыдущего состояния.

В этом отношении кубит отличается от классического бита; мы можем измерить классический бит, не возмущая его, и расшифровать всю закодированную в нем информацию. Допустим, мы имеем классический бит, который в действительности имеет определенное, но неизвестное нам значение (0 или 1). Опираясь на доступную информацию, мы можем только сказать, что с *вероятностью* p_0 бит имеет значение 0, а с вероятностью p_1 — значение 1, причем $p_0 + p_1 = 1$. Измеряя бит, мы получаем дополнительную информацию, позволяющую узнать его значение со 100% уверенностью.

Важный вопрос: в чем суть различия между кубитом и *вероятностным* классическим битом? По разным причинам, которые мы с вами изучим, это действительно не одно и то же.

2.2.1. Спин-1/2

Прежде всего заметим, что коэффициенты a и b в уравнении (2.11) содержат нечто большее, чем просто вероятности результатов измерения в базисе $\{|0\rangle, |1\rangle\}$. В частности, *относительная фаза* a и b также имеет физическое значение.

Для физика естественно интерпретировать уравнение (2.11) как спиновое состояние объекта со спином-1/2 (типа электрона). Тогда состояния $|0\rangle$ и $|1\rangle$ представляют собой состояния спин вверх $|\uparrow\rangle$ и спин вниз $|\downarrow\rangle$ вдоль некоторой оси, например, оси z. Два вещественных числа, характеризующих кубит (комплексные числа a и b, без учета их общей фазы и нормы), описывают ориентацию спина в трехмерном пространстве (полярный угол θ и азимутальный угол φ).

Мы не имеем возможности углубляться здесь в теорию симметрии в квантовой механике, напомним лишь кратко ее некоторые элементы, которые окажутся полезными в дальнейшем. Симметрия представляет собой преобразование, действие которого на состояние системы оставляет неизменными все наблюдаемые свойства системы. В квантовой механике наблюдениями являются измерения самосопряженных операторов. Если $\mathbf{A}$ измеряется в состоянии $|\psi\rangle$, то с вероятностью $|\langle a|\psi\rangle|^2$ будет получен результат $|a\rangle$ (собственный вектор оператора $\mathbf{A}$). Симметрия должна оставлять неизменными эти вероятности (если мы «поворачиваем» систему *вместе* с приборами).

Операция симметрии представляет собой отображение векторов в гильбертовом пространстве

$$|\psi\rangle \rightarrow |\psi'\rangle, \tag{2.12}$$

сохраняющее абсолютные значения внутренних произведений

$$|\langle\varphi|\psi\rangle| = |\langle\varphi'|\psi'\rangle| \tag{2.13}$$

для любых $|\varphi\rangle$ и $|\psi\rangle$. Согласно знаменитой теореме Вигнера, отображение с таким свойством всегда может быть выбрано (принимая соответствующее соглашение относительно фазы) унитарным или антиунитарным. Важная для дискретных симметрий антиунитарная альтернатива может быть исключена в случае непрерывных симметрий. Тогда преобразование симметрии действует как

$$|\psi\rangle \rightarrow |\psi'\rangle = \mathbf{U}|\psi\rangle, \tag{2.14}$$

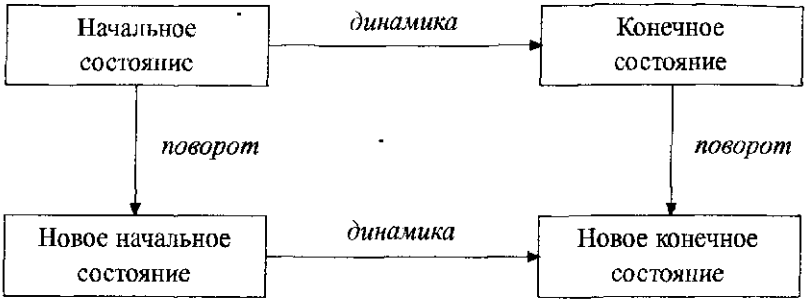
где $\mathbf{U}$ — унитарный оператор (и, в частности, линейный).

Симметрии образуют группу: преобразование симметрии можно обратить, а произведение двух симметрий, в свою очередь, является симметрией. Каждой операции симметрии R, действующей на нашу систему, соответствует унитарное преобразование $\mathbf{U}(R)$. Перемножение этих унитарных операторов должно соответствовать групповому закону перемножения симметрий — применение $R_1 \circ R_2$ должно быть эквивалентно последовательному применению сначала R_2, а затем R_1. Таким образом, мы требуем

$$\mathbf{U}(R_1)\mathbf{U}(R_2) = Phase(R_1, R_2)\mathbf{U}(R_1 \circ R_2). \tag{2.15}$$

В уравнении (2.15) допускается фазовый множитель, поскольку квантовыми состояниями являются *лучи*; нам нужно требовать лишь того, чтобы $\mathbf{U}(R_1 \circ R_2)$ действовал так же, как и $\mathbf{U}(R_1)\mathbf{U}(R_2)$, на лучи, а не на векторы. $\mathbf{U}(R)$ обеспечивает унитарное (с точностью до фазы) представление группы симметрии.

До сих пор наше понятие симметрии не имело связи с динамикой. Обычно мы требуем от симметрии, чтобы она сохраняла динамическую эволюцию системы. Это означает, что не должно иметь значения, преобразуем ли мы сначала систему, а затем она эволюционирует, или наоборот, сначала происходит эволюция системы, а затем мы преобразуем ее. Другими словами, диаграмма



коммутативна. Это означает, что оператор эволюции во времени должен коммутировать с преобразованиями симметрии $\mathbf{U}(R)$

$$\mathbf{U}(R)e^{-it\mathbf{H}} = e^{-it\mathbf{H}}\mathbf{U}(R). \tag{2.16}$$

Разлагая это уравнение до линейного порядка по t, получаем

$$\mathbf{U}(R)\mathbf{H} = \mathbf{H}\mathbf{U}(R). \tag{2.17}$$

В случае непрерывной симметрии операция R может быть выбрана сколь угодно близкой к единице $R = 1 + \epsilon T$, тогда $\mathbf{U}$ также близок к единичному оператору $\mathbf{1}$:

$$\mathbf{U}(R) = \mathbf{1} - i\epsilon\mathbf{Q} + O(\epsilon^2). \tag{2.18}$$

Из унитарности (в линейном порядке по ϵ) $\mathbf{U}$ следует, что $\mathbf{Q}$ является наблюдаемой $\mathbf{Q} = \mathbf{Q}^\dagger$. Разлагая уравнение (2.17) до линейных по ϵ слагаемых, находим

$$[\mathbf{Q}, \mathbf{H}] = 0\,; \tag{2.19}$$

наблюдаемая $\mathbf{Q}$ коммутирует с гамильтонианом.

Уравнение (2.19) представляет собой *закон сохранения*. Он говорит, например, что если мы приготовили собственное состояние оператора $\mathbf{Q}$, то управляемая уравнением Шредингера эволюция во времени будет сохранять это собственное состояние. Таким образом, симметрии влекут за

собой законы сохранения. И наоборот, по заданной сохраняющейся величине $\mathbf{Q}$, удовлетворяющей уравнению (2.19), можно построить соответствующее преобразование симметрии. Конечное преобразование может быть построено как произведение множества ифинитезимальных преобразований

$$R = \left(1 + \frac{\theta}{N} T\right)^N \Rightarrow \mathbf{U}(R) = \left(\mathbf{1} + i\frac{\theta}{N}\mathbf{Q}\right)^N \to e^{i\theta\mathbf{Q}} \tag{2.20}$$

(в пределе $N \to \infty$). Выяснив, как выглядит унитарное представление инфинитезимальных преобразований, мы тем самым определили представление конечных преобразований; они могут быть построены как произведения инфинитезимальных преобразований. Мы говорим, что $\mathbf{Q}$ – *генератор* симметрии.

Кратко напомним, как эта общая теория применяется к пространственным поворотам и моменту количества движения (импульса). Бесконечно малый поворот на угол $d\theta$ вокруг оси, определяемой единичным вектором $\vec{n} = (n_1, n_2, n_3)$, может быть представлен в виде

$$\mathbf{U}(\vec{n}, d\theta) = 1 - id\theta\, \vec{n} \cdot \vec{\mathbf{J}}, \tag{2.21}$$

где $(\mathbf{J}_1, \mathbf{J}_2, \mathbf{J}_3)$ – компоненты момента импульса. Конечный поворот выражается как

$$\mathbf{U}(\vec{n}, \theta) = \exp(-i\theta\, \vec{n} \cdot \vec{\mathbf{J}}). \tag{2.22}$$

Повороты вокруг разных осей не коммутируют между собой. Из их элементарных свойств вытекают коммутационные соотношения

$$\left[\mathbf{J}_k, \mathbf{J}_l\right] = i\varepsilon_{klm}\mathbf{J}_m, \tag{2.23}$$

где ε_{klm} – полностью антисимметричный единичный псевдотензор ($\varepsilon_{123} = 1$), а по повторяющимся индексам предполагается суммирование. Чтобы совершать повороты квантовой системы, найдем удовлетворяющие коммутационным соотношениям (2.23) самосопряженные операторы $\mathbf{J}_1$, $\mathbf{J}_2, \mathbf{J}_3$ в гильбертовом пространстве.

«Определяющее» представление группы поворотов трехмерно, однако простейшее нетривиальное неприводимое представление является двумерным и задается генераторами

$$\mathbf{J}_k = \frac{1}{2}\sigma_k, \tag{2.24}$$

где

$$\boldsymbol{\sigma}_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \boldsymbol{\sigma}_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad \boldsymbol{\sigma}_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{2.25}$$

— матрицы Паули. С точностью до унитарного преобразования базиса это единственное двумерное неприводимое представление. Поскольку собственные числа операторов $\mathbf{J}_k$ равны $\pm 1/2$, мы называем его представлением спина-1/2. (Отождествляя $\mathbf{J}$ с моментом импульса, мы неявно выбрали единицы, в которых $\hbar = 1$). Матрицы Паули также обладают свойствами взаимной антикоммутации и идемпотентности

$$\boldsymbol{\sigma}_k \boldsymbol{\sigma}_l + \boldsymbol{\sigma}_l \boldsymbol{\sigma}_k = 2\delta_{kl}\mathbf{1}. \tag{2.26}$$

Таким образом, $(\vec{n}\cdot\vec{\boldsymbol{\sigma}})^2 = n_k n_l \boldsymbol{\sigma}_k \boldsymbol{\sigma}_l = n_k n_k \mathbf{1} = \mathbf{1}$. Разлагая экспоненту в ряд, мы видим, что конечный поворот представляется как

$$\mathbf{U}(\vec{n},\theta) = \exp\Big(-i\frac{\theta}{2}\vec{n}\cdot\vec{\boldsymbol{\sigma}}\Big) = \mathbf{1}\cos\frac{\theta}{2} - i(\vec{n}\cdot\vec{\boldsymbol{\sigma}})\sin\frac{\theta}{2}. \tag{2.27}$$

В такой форме можно представить наиболее общую унитарную 2×2-матрицу с единичным определителем. Это позволяет думать о кубите как о состоянии объекта со спином-1/2, а о произвольном унитарном преобразовании (кроме возможного поворота общей фазы), действующем на это состояние (кубит), — как о *повороте* спина.

Необычным свойством представления $\mathbf{U}(\vec{n},\theta)$ является его *двузначность*. В частности, нетривиально представляется поворот на угол 2π вокруг любой оси:

$$\mathbf{U}(\vec{n},\theta = 2\pi) = -\mathbf{1}. \tag{2.28}$$

Наше представление группы вращений в действительности является представлением «с точностью до знака»

$$\mathbf{U}(R_1)\mathbf{U}(R_2) = \pm\mathbf{U}(R_1 \circ R_2). \tag{2.29}$$

Но, как уже отмечалось, это вполне приемлемо, *поскольку групповое умножение относится к лучам*, а не к векторам. Эти двузначные представления группы вращений называются *спинорными* представлениями. (Существование спиноров следует из топологического свойства группы — она не односвязна.)

Несмотря на то, что поворот на угол 2π действительно не ведет к наблюдаемому изменению состояния объекта со спином-1/2, было бы ошибкой считать, что спинорное свойство не имеет наблюдаемых следствий.

Допустим, у меня есть машина, которая действует на пару спинов. Если первый спин направлен вверх, то она ничего не меняет, но если первый спин направлен вниз, она поворачивает второй спин на угол 2π. Пусть теперь эта машина действует на состояние, в котором первый спин находится в суперпозиции состояний «вверх» и «вниз». Тогда

$$\frac{1}{\sqrt{2}}(|\uparrow\rangle_1 + |\downarrow\rangle_1)|\uparrow\rangle_2 \rightarrow \frac{1}{\sqrt{2}}(|\uparrow\rangle_1 - |\downarrow\rangle_1)|\uparrow\rangle_2. \tag{2.30}$$

Несмотря на отсутствие наблюдаемого влияния на состояние второго спина, состояние первого спина стало ортогональным его исходному состоянию, что очень даже наблюдаемо.

В повернутой системе отсчета поворот $R(\vec{n},\theta)$ превращается в поворот на тот же самый угол, но вокруг повернутой оси. Отсюда следует, что три компоненты момента количества движения при поворотах преобразуются как вектор

$$\mathbf{U}(R)\mathbf{J}_k\mathbf{U}^\dagger(R) = R_{kl}\mathbf{J}_l. \tag{2.31}$$

Таким образом, если состояние $|m\rangle$ является собственным состоянием оператора $\mathbf{J}_3$

$$\mathbf{J}_3|m\rangle = m|m\rangle, \tag{2.32}$$

тогда $\mathbf{U}(R)|m\rangle$ является собственным состоянием оператора $R\mathbf{J}_3$ с тем же самым собственным значением:

$$\begin{aligned} R\mathbf{J}_3\mathbf{U}(R)|m\rangle &= \mathbf{U}(R)\mathbf{J}_3\mathbf{U}^\dagger(R)\mathbf{U}(R)|m\rangle \\ &= \mathbf{U}(R)\mathbf{J}_3|m\rangle = m(\mathbf{U}(R)|m\rangle). \end{aligned} \tag{2.33}$$

Следовательно, мы можем построить собственные состояния оператора проекции момента импульса на ось $\vec{n} = (\sin\theta\cos\varphi, \sin\theta\sin\varphi, \cos\theta)$, применяя поворот на угол θ вокруг оси $\vec{n}' = (-\sin\varphi, \cos\varphi, 0)$ к собственному состоянию оператора $\mathbf{J}_3$. Для нашего представления спина-1/2 таким поворотом является

$$\begin{aligned} \exp\left[-i\frac{\theta}{2}\vec{n}'\cdot\vec{\boldsymbol{\sigma}}\right] &= \exp\left[\frac{\theta}{2}\begin{pmatrix} 0 & -e^{-i\varphi} \\ e^{i\varphi} & 0 \end{pmatrix}\right] = \\ &= \begin{pmatrix} \cos\frac{\theta}{2} & -e^{-i\varphi}\sin\frac{\theta}{2} \\ +e^{+i\varphi}\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}. \end{aligned} \tag{2.34}$$

Применяя его к $\binom{1}{0}$ — собственному состоянию оператора $\mathbf{J}_3$ с собственным значением $+1$, получим (с точностью до общей фазы)

$$|\psi(\theta,\varphi)\rangle = \begin{pmatrix} e^{-i\varphi/2}\cos\dfrac{\theta}{2} \\ e^{+i\varphi/2}\sin\dfrac{\theta}{2} \end{pmatrix}. \tag{2.35}$$

Мы можем непосредственно проверить, что этот вектор является собственным состоянием оператора

$$\vec{n}\cdot\vec{\boldsymbol{\sigma}} = \begin{pmatrix} \cos\theta & e^{-i\varphi}\sin\theta \\ e^{i\varphi}\sin\theta & -\cos\theta \end{pmatrix} \tag{2.36}$$

с собственным значением $+1$. Итак, мы видим, что уравнение (2.11) с $a = e^{-i\varphi/2}\cos\dfrac{\theta}{2}$, $b = e^{+i\varphi/2}\sin\dfrac{\theta}{2}$ может интерпретироваться как состояние спина, ориентированного вдоль направления (θ,φ).

Мы уже отмечали, что невозможно определить a и b с помощью одного измерения. Более того, даже имея множество идентичных копий данного состояния, мы не можем полностью его определить, измеряя каждую копию только вдоль оси z. Это могло бы позволить нам оценить $|a|$ и $|b|$, но не дало бы возможности получить информацию об относительной фазе a и b. Эквивалентно мы могли бы найти значение проекции спина на ось z

$$\langle\psi(\theta,\varphi)|\boldsymbol{\sigma}_3|\psi(\theta,\varphi)\rangle = \cos^2\frac{\theta}{2} - \sin^2\frac{\theta}{2} = \cos\theta, \tag{2.37}$$

но ничего не смогли бы узнать о его компонентах в плоскости xy. Проблема определения $|\psi\rangle$ путем измерения спина аналогична проблеме определения единичного вектора $\vec{n}$ путем измерения его компонент вдоль различных осей. В общем необходимы измерения вдоль трех различных осей. Например, из $\langle\boldsymbol{\sigma}_3\rangle$ и $\langle\boldsymbol{\sigma}_1\rangle$ мы можем определить n_3 и n_1, но знак n_2 останется неопределенным. Измерение $\langle\boldsymbol{\sigma}_2\rangle$ могло бы устранить эту двусмысленность.

Конечно, если мы позволили поворачивать спин, тогда будет достаточно измерений только вдоль оси z. То есть измерение спина вдоль оси $\vec{n}$ эквивалентно предварительному совершению поворота, совмещающего ось $\vec{n}$ с осью z, а затем — измерению вдоль оси z.

В частном случае $\theta = \pi/2$, $\varphi = 0$ (ось x) наше спиновое состояние имеет вид

$$|\uparrow_x\rangle = \frac{1}{\sqrt{2}}\bigl(|\uparrow_z\rangle + |\downarrow_z\rangle\bigr), \tag{2.38}$$

(«спин вверх вдоль оси x»). Ортогональным ему состоянием («спин вниз вдоль оси x») является

$$|\downarrow_x\rangle = \frac{1}{\sqrt{2}}(|\uparrow_z\rangle - |\downarrow_z\rangle). \tag{2.39}$$

Для этих обоих состояний, измеряя спин вдоль оси z, мы получим $|\uparrow_z\rangle$ с вероятностью 1/2 и $|\downarrow_z\rangle$ с вероятностью 1/2.

Рассмотрим теперь комбинацию

$$\frac{1}{\sqrt{2}}(|\uparrow_x\rangle + |\downarrow_x\rangle). \tag{2.40}$$

Это состояние обладает тем свойством, что если мы измеряем спин вдоль оси x, то с вероятностями, равными 1/2, получаем $|\uparrow_x\rangle$ или $|\downarrow_x\rangle$. Можно спросить, что мы получим, измеряя состояние (2.40) вдоль оси z?

Если бы это были классические вероятностные биты, то ответ был бы очевиден. Состояние (2.40) представляет собой одно из двух состояний, и для *каждого* из них вероятность направления вверх или вниз вдоль оси z равна 1/2. Таким образом, измеряя состояние (2.40) вдоль оси z, мы, конечно, должны с вероятностью 1/2 обнаружить спин, направленным вверх.

Но для кубитов это не так! Складывая уравнения (2.38) и (2.39), мы обнаруживаем, что в состоянии, описываемом уравнением (2.40), в действительности замаскировано состояние $|\uparrow_z\rangle$. Измеряя его вдоль оси z, мы всегда будем получать $|\uparrow_z\rangle$ и никогда — $|\downarrow_z\rangle$.

Таким образом, для кубитов, в противоположность классическим вероятностным битам, вероятности могут складываться довольно неожиданным образом. В этом и состоит (в его простейшей форме) явление, называемое «квантовой интерференцией», важная особенность квантовой информации.

Следует подчеркнуть, что, хотя *формальная* эквивалентность объекту со спином-1/2 применима к любой двухуровневой квантовой системе, конечно, не каждая двухуровневая система преобразуется при поворотах как спинор.

2.2.2. Поляризации фотона

Другую важную систему, имеющую два состояния, представляет *фотон*, который может иметь одну из двух независимых поляризаций. Состояния поляризации фотона тоже преобразуются при поворотах, однако фотоны отличаются от объектов со спином-1/2 в двух важных отношениях:

(1) Фотоны являются безмассовыми частицами. (2) Фотоны имеют спин-1 (это не спинорные частицы).

Мы не располагаем временем для детального обсуждения унитарных представлений группы Пуанкаре. Достаточно сказать, что спин частицы определяет, как преобразуется ее состояние под действием преобразований *малой* группы — сохраняющей импульс частицы подгруппы группы Лоренца. В случае массивной частицы мы всегда можем перейти в ее систему покоя и тогда малой группой является группа вращений.

Для безмассовых частиц не существует системы покоя. Конечномерные унитарные представления малой группы превращаются в представления группы вращений в *двумерном* пространстве, вращений вокруг направления импульса. Конечно, в случае с фотоном это соответствует знакомому свойству классического света — волны поляризованы перпендикулярно направлению распространения.

При повороте вокруг направления распространения два состояния линейной поляризации ($|x\rangle$ и $|y\rangle$ для горизонтальной и вертикальной поляризации) преобразуются как

$$\begin{aligned} |x\rangle &\to +\cos\theta\,|x\rangle + \sin\theta\,|y\rangle, \\ |y\rangle &\to -\sin\theta\,|x\rangle + \cos\theta\,|y\rangle. \end{aligned} \tag{2.41}$$

Это двумерное представление в действительности приводимо. Матрица

$$\begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \tag{2.42}$$

имеет собственные состояния

$$|R\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix}, \qquad |L\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} i \\ 1 \end{pmatrix}, \tag{2.43}$$

отвечающие собственным значениям $e^{+i\theta}$ и $e^{-i\theta}$, состояния правой и левой циркулярной поляризации. То есть они являются собственными состояниями генератора поворотов

$$\mathrm{J} = \begin{pmatrix} 0 & -i \\ +i & 0 \end{pmatrix} = \boldsymbol{\sigma}_y \tag{2.44}$$

с собственными значениями ± 1. Поскольку собственные значения равны ± 1 (а не $\pm 1/2$), мы говорим, что фотон имеет спин-1.

В этом контексте явление квантовой интерференции может быть описано следующим образом. Предположим, что мы имеем анализатор поляризации, который позволяет пройти через него фотону только с одной из двух линейных поляризаций. Тогда вероятность прохождения x- или y-поляризованного фотона через повернутый на 45° анализатор равна 1/2; 1/2-ой равна и вероятность прохождения поляризованного под углом 45° фотона через x- или y-анализатор. Однако x-фотон *никогда* не пройдет через y-анализатор. Если мы поместим повернутый на 45° анализатор между x- и y-анализаторами, тогда через каждый анализатор пройдет половина падающих на него фотонов. Но если мы удалим промежуточный анализатор, то *ни один* фотон не пройдет через y-анализатор.

Очевидно, можно сконструировать прибор, который поворачивает плоскость поляризации фотона и, следовательно, применяет преобразование (2.41) к нашему кубиту. Как уже отмечалось, это не самое общее унитарное преобразование. Но если мы имеем также и прибор, который изменяет относительную фазу двух ортогональных, линейно поляризованных состояний

$$\begin{aligned} |x\rangle &\to e^{+i\omega/2}|x\rangle, \\ |y\rangle &\to e^{-i\omega/2}|y\rangle, \end{aligned} \tag{2.45}$$

то эти два прибора можно использовать вместе, чтобы совершить произвольное 2×2 унитарное преобразование (с определителем, равным единице) состояния поляризации фотона.

2.3. Матрица плотности

2.3.1. Бинарная квантовая система

Последняя лекция была об одном кубите. Эта лекция — о *двух* кубитах. (Догадайтесь, о чем будет следующая лекция!) Переход от одного кубита к двум — более серьезный шаг, чем вы могли бы ожидать. Многое из того, что есть странного и чудесного в квантовой механике, можно понять, рассматривая свойства квантовых состояний двух кубитов.

Аксиомы § 2.1 дают вполне приемлемую общую формулировку квантовой теории. Тем не менее при многих обстоятельствах мы обнаруживаем, что они кажутся нарушенными. Беда в том, что наши аксиомы нацелены на то, чтобы характеризовать поведение всей Вселенной. Но, как правило, у нас нет таких амбиций, как пытаться понять физику всей Вселенной; мы довольствуемся изучением только нашего маленького уголка. На практи-

ке наши исследования всегда ограничены малой частью гораздо большей квантовой системы.

В следующих нескольких лекциях мы увидим, что если мы ограничиваем наше внимание только на части большой системы, то (в противоположность аксиомам § 2.1):

1) состояния *не* являются лучами.

2) измерения *не* являются ортогональными проекторами.

3) эволюция *не* унитарна.

Мы сможем лучше понять эти моменты, рассматривая простейший пример: мир двух кубитов, в котором мы наблюдаем только один из них.

Итак, рассмотрим систему двух кубитов. Кубит A находится здесь, в комнате вместе с нами, и мы вольны наблюдать его или манипулировать им по своему усмотрению. Но кубит B заперт в подвале, где мы не можем до него добраться. Имея некоторое состояние двух кубитов, мы хотели бы найти простой способ описания наблюдений, которые мы можем делать только на кубите A.

Будем использовать $\{|0\rangle_A, |1\rangle_A\}$ и $\{|0\rangle_B, |1\rangle_B\}$ для обозначения ортонормированных базисов для кубитов A и B соответственно. Рассмотрим следующее квантовое состояние двухкубитовой Вселенной:

$$|\psi\rangle_{AB} = a|0\rangle_A \otimes |0\rangle_B + b|1\rangle_A \otimes |1\rangle_B. \tag{2.46}$$

В этом состоянии кубиты A и B *коррелированы*. Допустим, мы измеряем кубит A, проецируя его на базис $\{|0\rangle_A, |1\rangle_A\}$. Тогда с вероятностью $|a|^2$ мы получим результат $|0\rangle_A$, а измерение приготовит состояние

$$|0\rangle_A \otimes |0\rangle_B; \tag{2.47}$$

с вероятностью $|b|^2$ мы получим результат $|1\rangle_A$, а измерение приготовит состояние

$$|1\rangle_A \otimes |1\rangle_B. \tag{2.48}$$

В каждом случае, в результате измерения выбирается определенное состояние кубита B. Если мы сразу за этим измерим кубит B, то наверняка (с вероятностью единица) обнаружим его в состоянии $|0\rangle_B$, если перед этим было получено $|0\rangle_A$, и — в состоянии $|1\rangle_B$, если предыдущим результатом было $|1\rangle_A$. В этом смысле результаты измерений $\{|0\rangle_A, |1\rangle_A\}$ и $\{|0\rangle_B, |1\rangle_B\}$ полностью скоррелированы в состоянии $|\psi\rangle_{AB}$.

Теперь я хотел бы рассмотреть более общие наблюдаемые, действующие на кубит A, и я хотел бы характеризовать результаты измерения только A (независимо от результатов любых измерений недоступного кубита B). Наблюдаемую, действующую только на кубит A, можно представить в виде

$$\mathbf{M}_A \otimes \mathbf{1}_B, \tag{2.49}$$

где $\mathbf{M}_A$ – действующий на A самосопряженный оператор, а $\mathbf{1}_B$ – действующий на B единичный оператор. Ожидаемое значение наблюдаемой в состоянии $|\psi\rangle_{AB}$ равно

$$\begin{aligned} {}_{AB}\langle\psi|\mathbf{M}_A \otimes \mathbf{1}_B|\psi\rangle_{AB} &= (a^*{}_A\langle 0| \otimes {}_B\langle 0| + b^*{}_A\langle 1| \otimes {}_B\langle 1|)\mathbf{M}_A \otimes \mathbf{1}_B \\ &\quad (a|0\rangle_A \otimes |0\rangle_B + b|1\rangle_A \otimes |1\rangle_B) = \\ &= |a|^2{}_A\langle 0|\mathbf{M}_A|0\rangle_A + |b|^2{}_A\langle 1|\mathbf{M}_A|1\rangle_A \end{aligned} \tag{2.50}$$

(где мы воспользовались ортогональностью $|0\rangle_B$ и $|1\rangle_B$). Это выражение можно переписать в форме

$$\langle \mathbf{M}_A \rangle = \mathrm{tr}(\mathbf{M}_A \boldsymbol{\rho}_A), \tag{2.51}$$

$$\boldsymbol{\rho}_A = |a|^2|0\rangle_A{}_A\langle 0| + |b|^2|1\rangle_A{}_A\langle 1|, \tag{2.52}$$

а tr обозначает *след*. Оператор $\boldsymbol{\rho}_A$ называется *оператором плотности* (или *матрицей плотности*) кубита A. Он самосопряжен, положителен (его собственные значения неотрицательны) и имеет единичный след (поскольку $|\psi\rangle$ являются нормированными состояниями).

Поскольку $\langle \mathbf{M}_A \rangle$ имеет вид (2.51) для любой наблюдаемой $\mathbf{M}_A$, действующей на кубит A, то логично интерпретировать $\boldsymbol{\rho}_A$ как *ансамбль* возможных квантовых состояний, каждое из которых возникает с определенной вероятностью. Другими словами, мы получили бы для $\langle \mathbf{M}_A \rangle$ тот же самый результат, если бы предположили, что кубит A находится в одном из двух квантовых состояний. Причем с вероятностью $p_0 = |a|^2$ он находится в состоянии $|0\rangle_A$, а с вероятностью $p_1 = |b|^2$ – в состоянии $|1\rangle_A$. Если нас интересует результат любого возможного измерения, мы можем рассматривать в качестве $\mathbf{M}_A$ проектор $\mathbf{E}_A(a)$ на соответствующее собственное пространство наблюдаемой. Тогда

$$\mathrm{Prob}(a) = p_0\,{}_A\langle 0|\mathbf{E}_A(a)|0\rangle_A + p_1\,{}_A\langle 1|\mathbf{E}_A(a)|1\rangle_A, \tag{2.53}$$

что представляет собой вероятность результата a, взвешенную вероятностью каждого квантового состояния и просуммированную по всему ансамблю.

Мы уже обращали внимание на существенное различие между когерентной суперпозицией состояний $|0\rangle_A$ и $|1\rangle_A$ и вероятностным ансамблем, в котором каждое из состояний $|0\rangle_A$ и $|1\rangle_A$ может появляться с конкретной вероятностью. Например, для объекта со спином-1/2 мы видели, что если мы измеряем σ_1 в состоянии $\frac{1}{\sqrt{2}}(|\uparrow_z\rangle + |\downarrow_z\rangle)$, то с единичной вероятностью получим результат $|\uparrow_x\rangle$. Но ансамбль, в котором каждое из состояний $|\uparrow_z\rangle$ и $|\downarrow_z\rangle$ появляется с вероятностью 1/2, представляется оператором плотности

$$\boldsymbol{\rho} = \frac{1}{2}(|\uparrow_z\rangle\langle\uparrow_z| + |\downarrow_z\rangle\langle\downarrow_z|) = \frac{1}{2}\mathbf{1}, \tag{2.54}$$

тогда проекция на $|\uparrow_x\rangle$ имеет ожидаемое значение

$$\mathrm{tr}(|\uparrow_x\rangle\langle\uparrow_x|\boldsymbol{\rho}) = \frac{1}{2}. \tag{2.55}$$

Фактически мы видели, что любое представляемое лучом состояние одного кубита можно интерпретировать как спин, ориентированный вдоль некоторого определенного направления. Но, поскольку левая часть (2.55) не изменяется при унитарном преобразовании базиса, а состояние $|\psi(\theta,\varphi)\rangle$ можно получить унитарным преобразованием состояния $|\uparrow_z\rangle$, мы видим, что для $\boldsymbol{\rho}$, определяемого уравнением (2.54),

$$\mathrm{tr}(|\psi(\theta,\varphi)\rangle\langle\psi(\theta,\varphi)|\boldsymbol{\rho}) = \frac{1}{2}. \tag{2.56}$$

Следовательно, если приготовлено состояние $|\psi\rangle_{AB}$ (2.46) с $|a|^2 = |b|^2 = 1/2$, то при измерении спина A вдоль любой оси мы получим совершенно случайный результат; каждая из ориентаций спина, вверх или вниз, может появиться с вероятностью 1/2.

Это обсуждение коррелированного двухкубитового состояния $|\psi\rangle_{AB}$ очевидным образом распространяется на произвольное состояние любой бинарной квантовой системы (системы, состоящей из двух частей). Гильбертовым пространством бинарной системы является $\mathbf{H}_A \otimes \mathbf{H}_B$, где $\mathbf{H}_{A,B}$ — гильбертово пространство одной из составляющих систему частей. Это означает, что если $\{|i\rangle_A\}$ — ортонормированный базис в $\mathbf{H}_A$, а $\{|\mu\rangle_B\}$ — ортонормированный базис в $\mathbf{H}_B$, то $\{|i\rangle_A \otimes |\mu\rangle_B\}$ — ортонормированный базис в $\mathbf{H}_A \otimes \mathbf{H}_B$. Таким образом, произвольное чистое состояние в $\mathbf{H}_A \otimes \mathbf{H}_B$ может быть представлено в виде разложения

$$|\psi\rangle_{AB} = \sum_{i,\mu} a_{i,\mu}|i\rangle_A \otimes |\mu\rangle_B, \tag{2.57}$$

где $\sum\limits_{i,\mu} |a_{i,\mu}|^2 = 1$. Ожидаемое значение наблюдаемой $\mathbf{M}_A \otimes 1_B$, действующей только на подсистему A, равно

$$\begin{aligned}\langle \mathbf{M}_A \rangle &= {}_{AB}\langle\psi|\mathbf{M}_A \otimes \mathbf{1}_B|\psi\rangle_{AB} = \\ &= \sum_{j,\nu} a^*_{j,\nu}\, {}_A\langle j| \otimes {}_B\langle\nu|\mathbf{M}_A \otimes \mathbf{1}_B \sum_{i,\mu} a_{i,\mu}|i\rangle_A \otimes |\mu\rangle_B = \\ &= \sum_{i,j,\mu} a^*_{j,\mu} a_{i,\mu}\, {}_A\langle j|\mathbf{M}_A|i\rangle_A = \\ &= \mathrm{tr}(\mathbf{M}_A \boldsymbol{\rho}_A), \end{aligned} \tag{2.58}$$

где

$$\boldsymbol{\rho}_A = \mathrm{tr}_B(|\psi\rangle_{AB}\, {}_{AB}\langle\psi|) \equiv \sum_{i,j,\mu} a_{i,\mu} a^*_{j,\mu} |i\rangle_A\, {}_A\langle j|. \tag{2.59}$$

Мы говорим, что оператор плотности $\boldsymbol{\rho}_A$ подсистемы A получается взятием частичного *следа* от матрицы плотности (в рассматриваемом случае от чистого состояния) составной системы AB по переменным подсистемы B.

Из определяющего уравнения (2.59) непосредственно следует, что $\boldsymbol{\rho}_A$ обладает следующими свойствами:

1) $\boldsymbol{\rho}_A$ — самосопряженый оператор: $\boldsymbol{\rho}_A = \boldsymbol{\rho}_A^\dagger$;

2) $\boldsymbol{\rho}_A$ — положительный оператор: для любого $|\psi\rangle_A$ ${}_A\langle\psi|\boldsymbol{\rho}_A|\psi\rangle_A = \sum\limits_{\mu} |\sum\limits_{i} a_{i,\mu}\, {}_A\langle\psi|i\rangle_A|^2 \geqslant 0$;

3) $\mathrm{tr}\,\boldsymbol{\rho}_A = 1$: мы имеем $\mathrm{tr}\,\boldsymbol{\rho}_A = \sum\limits_{i,\mu} |a_{i,\mu}|^2 = 1$, поскольку состояние $|\psi\rangle_{AB}$ нормировано.

Отсюда следует, что $\boldsymbol{\rho}_A$ может быть диагонализован, что все его собственные значения вещественны и неотрицательны и что сумма его собственных значений равна единице.

Если мы наблюдаем подсистему большей системы, то, даже если состоянием большей системы является луч, состояние подсистемы таковым не будет; в общем случае оно описывается оператором плотности. В том случае, когда состоянием подсистемы является луч, мы называем его *чистым*. В противном случае — состояние является *смешанным*.

Если состоянием является чистое состояние $|\psi\rangle_A$, то матрица плотности $\rho_A = |\psi\rangle_{A\,A}\langle\psi|$ представляет собой *проектор* на одномерное пространство, натянутое на $|\psi\rangle_A$. Следовательно, матрица плотности чистого состояния обладает свойством $\rho_A^2 = \rho_A$. В общем случае матрица плотности, разложенная в базисе, в котором она диагональна, имеет вид

$$\rho_A = \sum_a p_a |\psi_a\rangle\langle\psi_a|, \tag{2.60}$$

где $0 \leqslant p_a \leqslant 1$ и $\sum_a p_a = 1$. Если состояние не является чистым, то эта сумма состоит из двух или большего числа слагаемых и $\rho_A^2 \neq \rho_A$; фактически $\operatorname{tr}\rho_A^2 = \sum p_a^2 < \sum p_a = 1$. Мы говорим, что ρ представляет *некогерентную* суперпозицию состояний $\{|\psi_a\rangle\}$; некогерентность означает, что относительные фазы $|\psi_a\rangle$ экспериментально ненаблюдаемы.

Поскольку ожидаемое значение наблюдаемой M, действующей на подсистему, может быть представлено в виде

$$\langle \mathrm{M}\rangle = \operatorname{tr}\mathrm{M}\rho = \sum_a p_a \langle\psi_a|\mathrm{M}|\psi_a\rangle, \tag{2.61}$$

мы, как и прежде, видим, что ρ можно интерпретировать как *ансамбль* чистых квантовых состояний, в котором состояние $|\psi_a\rangle$ появляется с вероятностью p_a. Таким образом, мы прошли большую часть пути к пониманию того, как в квантовой механике возникают вероятности, когда квантовая система A взаимодействует с другой системой B. Состояния A и B становятся *запутанными*, то есть коррелированными. Запутывание *разрушает когерентность* суперпозиции состояний, так что некоторые фазы становятся ненаблюдаемыми, если мы следим за одной только A. Мы можем описывать эту ситуацию, говоря, что происходит *коллапс* (*редукция*) состояния системы A — она находится в одном из множества альтернативных состояний, каждому из которых может быть приписана вероятность.

2.3.2. Сфера Блоха

Вернемся к случаю, в котором системой A является один кубит, и рассмотрим общую форму матрицы плотности. Наиболее общая самосопряженная 2×2-матрица зависит от четырех вещественных параметров и может быть разложена в базисе $\{1, \sigma_1, \sigma_2, \sigma_3\}$. Поскольку каждая из матриц σ_i является бесследовой, коэффициент перед 1 в разложении матрицы

плотности $\boldsymbol{\rho}$ должен быть равен $1/2$ (так чтобы $\operatorname{tr}\boldsymbol{\rho} = 1$), а $\boldsymbol{\rho}$ может быть разложена как

$$\begin{aligned}\boldsymbol{\rho}(\vec{P}) &= \frac{1}{2}(\mathbf{1} + \vec{P}\cdot\vec{\boldsymbol{\sigma}}) \equiv \\ &\equiv \frac{1}{2}(\mathbf{1} + P_1\boldsymbol{\sigma}_1 + P_2\boldsymbol{\sigma}_2 + P_3\boldsymbol{\sigma}_3) = \\ &= \frac{1}{2}\begin{pmatrix} 1+P_3 & P_1 - iP_2 \\ P_1 + iP_2 & 1 - P_3 \end{pmatrix}. \end{aligned} \tag{2.62}$$

Мы можем вычислить $\det\boldsymbol{\rho} = \frac{1}{4}(1 - \vec{P}^2)$. Следовательно, необходимым условием неотрицательности собственных значений $\boldsymbol{\rho}$ является неравенство $\det\boldsymbol{\rho} \geqslant 0$ или $\vec{P}^2 \leqslant 1$. Это условие также и достаточно; поскольку $\operatorname{tr}\boldsymbol{\rho} = 1$ и $\boldsymbol{\rho}$ не может иметь два отрицательных собственных значения. Таким образом, имеется взаимно однозначное соответствие между возможными матрицами плотности одиночного кубита и точками *единичного трехмерного шара* $0 \leqslant |\vec{P}| \leqslant 1$. Этот шар обычно называют *сферой Блоха* (хотя, конечно, это в действительности шар, а не сфера).

Граница ($|\vec{P}| = 1$) шара (которая как раз и является сферой) содержит матрицы плотности с нулевым детерминантом. Поскольку $\operatorname{tr}\boldsymbol{\rho} = 1$, эти матрицы плотности должны иметь собственные значения 0 и 1. Они представляют собой одномерные проекторы и, следовательно, чистые состояния. Мы уже видели, что каждое чистое состояние одного кубита имеет вид $|\psi(\theta,\varphi)\rangle$ и может рассматриваться как ориентация спина в (θ,φ)-направлении. Действительно, используя свойство

$$(\hat{n}\cdot\vec{\boldsymbol{\sigma}})^2 = 1, \tag{2.63}$$

где $\hat{n}$ — единичный вектор, мы можем легко убедиться в том, что матрица плотности чистого состояния

$$\boldsymbol{\rho}(\hat{n}) = \frac{1}{2}(\mathbf{1} + \hat{n}\cdot\vec{\boldsymbol{\sigma}}) \tag{2.64}$$

обладает свойством

$$(\hat{n}\cdot\vec{\boldsymbol{\sigma}})\boldsymbol{\rho}(\hat{n}) = \boldsymbol{\rho}(\hat{n})(\hat{n}\cdot\vec{\boldsymbol{\sigma}}) = \boldsymbol{\rho}(\hat{n}) \tag{2.65}$$

и, следовательно, является проектором

$$\boldsymbol{\rho}(\hat{n}) = |\psi(\hat{n})\rangle\langle\psi(\hat{n})|\,; \tag{2.66}$$

то есть $\hat{n}$ представляет собой направление, вдоль которого ориентируется спин. И наоборот, из выражения

$$|\psi(\theta,\varphi)\rangle = \begin{pmatrix} e^{-i\varphi/2}\cos\frac{\theta}{2} \\ e^{+i\varphi/2}\sin\frac{\theta}{2} \end{pmatrix} \tag{2.67}$$

можно непосредственно найти, что

$$\begin{aligned} \boldsymbol{\rho}(\theta,\varphi) &= |\psi(\theta,\varphi)\rangle\langle\psi(\theta,\varphi)| = \\ &= \begin{pmatrix} \cos^2\frac{\theta}{2} & \cos\frac{\theta}{2}\sin\frac{\theta}{2}e^{-i\varphi} \\ \cos\frac{\theta}{2}\sin\frac{\theta}{2}e^{+i\varphi} & \sin^2\frac{\theta}{2} \end{pmatrix} = \\ &= \frac{1}{2}\mathbf{1}+\frac{1}{2}\begin{pmatrix} \cos\theta & e^{-i\varphi}\sin\theta \\ e^{+i\varphi}\sin\theta & -\cos\theta \end{pmatrix} = \frac{1}{2}(\mathbf{1}+\hat{n}\cdot\vec{\boldsymbol{\sigma}}), \end{aligned} \tag{2.68}$$

где $\hat{n} = (\sin\theta\cos\varphi, \sin\theta\sin\varphi, \cos\theta)$. Приятным свойством блоховской параметризации чистых состояний является то, что, хотя $|\psi(\theta,\varphi)\rangle$ имеет физически несущественную произвольную общую фазу, в матрице плотности $\boldsymbol{\rho}(\theta,\varphi) = |\psi(\theta,\varphi)\rangle\langle\psi(\theta,\varphi)|$ этой неоднозначности нет; все параметры в $\boldsymbol{\rho}$ имеют физический смысл.

Из свойства

$$\frac{1}{2}\operatorname{tr}\boldsymbol{\sigma}_i\boldsymbol{\sigma}_j = \delta_{ij} \tag{2.69}$$

следует, что

$$(\hat{n}\cdot\vec{\boldsymbol{\sigma}})_{\vec{P}} = \operatorname{tr}\left(\hat{n}\cdot\vec{\boldsymbol{\sigma}}\boldsymbol{\rho}(\vec{P})\right) = \hat{n}\cdot\vec{P}. \tag{2.70}$$

Таким образом, вектор $\vec{P}$ в уравнении (2.62) параметризует *поляризацию* спина. Если в нашем распоряжении имеется множество идентично приготовленных систем, мы можем определить $\vec{P}$ [и, следовательно, полностью матрицу плотности $\boldsymbol{\rho}(\vec{P})$], измеряя $(\hat{n}\cdot\vec{\boldsymbol{\sigma}})$ вдоль каждой из трех линейно независимых осей.

2.3.3. Теорема Глизона

Отправляясь от аксиом квантовой механики и рассматривая описание части большей квантовой системы, мы пришли к понятию матрицы плотности $\boldsymbol{\rho}$ и выражению $\operatorname{tr}(\mathbf{M}\boldsymbol{\rho})$ для ожидаемого значения наблюдаемой $\mathbf{M}$. Тем более приятно узнать, что формализм матрицы плотности является очень

общим и применим в гораздо более широких пределах. В этом состоит содержание *теоремы Глизона* (1957).

Теорема Глизона исходит из предпосылки, что задачей квантовой теории является сопоставление соответствующих вероятностей всем возможным ортогональным проекциям в гильбертовом пространстве (другими словами, всем возможным измерениям наблюдаемых).

Тогда состоянием квантовой системы является отображение, которое каждой проекции ($\mathbf{E}^2 = \mathbf{E}$ и $\mathbf{E} = \mathbf{E}^\dagger$) ставит в соответствие неотрицательное вещественное число, не превосходящее единицу:

$$\mathbf{E} \to p(\mathbf{E}), \qquad 0 \leqslant p(\mathbf{E}) \leqslant 1. \tag{2.71}$$

Это отображение должно обладать свойствами:

(1) $p(0) = 0$.

(2) $p(\mathbf{1}) = 1$.

(3) Если $\mathbf{E}_1\mathbf{E}_2 = 0$, то $p(\mathbf{E}_1 + \mathbf{E}_2) = p(\mathbf{E}_1) + p(\mathbf{E}_2)$.

Решающим здесь является постулат (3). Он утверждает, что (поскольку проекции на взаимно ортогональные пространства могут рассматриваться как взаимно исключающие альтернативы) вероятности, приписываемые взаимно ортогональным проекциям, должны быть аддитивными. Это очень сильное предположение, поскольку существует много различных способов выбора $\mathbf{E}_1$ и $\mathbf{E}_2$. Грубо говоря, первые два предположения утверждают, что, какое бы измерение мы ни делали: (1) всегда есть его результат; (2) вероятность суммы всех возможных (взаимно ортогональных) исходов равна единице.

В этих предположениях Глизон показал, что если размерность гильбертова пространства больше двух, то для любого такого отображения существует эрмитовский, положительный оператор $\boldsymbol{\rho}$ с единичным следом $\mathrm{tr}\,\boldsymbol{\rho} = 1$ такой, что

$$p(\mathbf{E}) = \mathrm{tr}(\boldsymbol{\rho}\mathbf{E}). \tag{2.72}$$

Таким образом, формализм матрицы плотности действительно является *необходимым*, если мы представляем наблюдаемые самосопряженными операторами в гильбертовом пространстве и приписываем определенные вероятности каждому возможному результату измерения. Грубо говоря, требование аддитивности вероятностей взаимно исключающих результатов настолько сильно, что мы с необходимостью приходим к линейному выражению (2.72).

Случай двумерного гильбертова пространства является особым, поскольку именно в двух измерениях оказывается недостаточным взаимно исключающих проекций. Все нетривиальные проекции имеют вид

$$\mathbf{E}(\hat{n}) = \frac{1}{2}(\mathbf{1} + \hat{n} \cdot \hat{\boldsymbol{\sigma}}), \tag{2.73}$$

но

$$\mathbf{E}(\hat{n})\mathbf{E}(\hat{m}) = 0 \tag{2.74}$$

только при $\hat{m} = -\hat{n}$; следовательно, любая определенная на двумерной сфере функция $f(\hat{n})$ такая, что $f(\hat{n}) + f(-\hat{n}) = 1$, удовлетворяет условиям теоремы Глизона, а таких функций существует много. Но в трех измерениях может быть больше альтернативных способов разбиения единицы, так что предположения Глизона гораздо сильнее. Мы не приводим здесь доказательства теоремы. (Для обсуждения см. книгу Переса, стр. 190)[1].

2.3.4. Эволюция оператора плотности

До сих пор мы не обсуждали эволюцию во времени смешанных состояний. В случае бинарной системы, подчиняющейся обычным аксиомам квантовой теории, предположим, что ее гамильтониан в пространстве $\mathcal{H}_A \otimes \mathcal{H}_B$ имеет вид

$$\mathbf{H}_{AB} = \mathbf{H}_A \otimes \mathbf{1}_B + \mathbf{1}_A \otimes \mathbf{H}_B. \tag{2.75}$$

В этом предположении подсистемы A и B не связаны между собой, так что каждая из них эволюционирует независимо. Оператор эволюции комбинированной системы

$$\mathbf{U}_{AB}(t) = \mathbf{U}_A(t) \otimes \mathbf{U}_B(t) \tag{2.76}$$

расщепляется на отдельные унитарные операторы эволюции, действующие каждый на свою систему.

Тогда в шредингеровской картине динамики начальное чистое состояние $|\psi(0)\rangle_{AB}$ бинарной системы, заданное уравнением (2.57), эволюционирует как

$$|\psi(t)\rangle_{AB} = \sum_{i,\mu} a_{i\mu} |i(t)\rangle_A \otimes |\mu(t)\rangle_B, \tag{2.77}$$

где

$$\begin{aligned} |i(t)\rangle_A &= \mathbf{U}_A(t)|i(0)\rangle_A, \\ |\mu(t)\rangle_B &= \mathbf{U}_B(t)|\mu(0)\rangle_A \end{aligned} \tag{2.78}$$

[1] A. Peres, *Quantum Theory: Concepts and Methods*, Kluwer Academic Publishers, New York et al (2002).

определяют новый ортогональный базис в $\mathcal{H}_A$ и $\mathcal{H}_B$ [так как $\mathbf{U}_A(t)$ и $\mathbf{U}_B(t)$ унитарны]. Вычисляя, как и раньше, частичный след, находим

$$\boldsymbol{\rho}_A(t) = \sum_{i,j,\mu} a_{i\mu} a^*_{j\mu} |i(t)\rangle_A \, {}_A\langle j(t)| = \mathbf{U}_A(t) \boldsymbol{\rho}_A(0) \mathbf{U}_A^\dagger(t). \qquad (2.79)$$

Таким образом, $\mathbf{U}_A(t)$ определяет эволюцию матрицы плотности.

В частности, в базисе, в котором $\boldsymbol{\rho}_A(0)$ диагональна, имеем

$$\boldsymbol{\rho}_A(t) = \sum_a p_a \mathbf{U}_A(t) |\psi_a(0)\rangle_A \, {}_A\langle\psi_a(0)| \mathbf{U}_A^\dagger(t). \qquad (2.80)$$

Уравнение (2.80) говорит о том, что эволюция $\boldsymbol{\rho}_A$ полностью согласуется с интерпретацией ансамбля. Эволюция во времени каждого состояния в ансамбле управляется оператором $\mathbf{U}_A(t)$. Если состояние $|\psi_a(0)\rangle_A$ с вероятностью p_a возникает в момент времени $t = 0$, то с той же вероятностью p_a состояние $|\psi_a(t)\rangle_A$ возникает в последующий момент времени t.

С другой стороны, должно быть ясным, что уравнение (2.80) справедливо только в предположении о том, что системы A и B динамически *не связаны* между собой. Ниже мы исследуем, как эволюционирует матрица плотности при более общих условиях.

2.4. Разложение Шмидта

Чистое двухкубитовое состояние может быть представлено в стандартной форме (*разложение Шмидта*), которая часто оказывается полезной.

Чтобы прийти к этой форме, заметим, что произвольный вектор из $\mathcal{H}_A \otimes \mathcal{H}_B$ может быть разложен как

$$|\psi\rangle_{AB} = \sum_{i,\mu} a_{i\mu} |i\rangle_A |\mu\rangle_B \equiv \sum_i |i\rangle_A |\tilde{i}\rangle_B. \qquad (2.81)$$

Здесь $\{|i\rangle_A\}$ и $\{|\mu\rangle_B\}$ — ортогональные базисы в $\mathcal{H}_A$ и $\mathcal{H}_B$ соответственно. Чтобы получить второе равенство в (2.81), мы положили по определению

$$|\tilde{i}\rangle_B \equiv \sum_\mu a_{i\mu} |\mu\rangle_B. \qquad (2.82)$$

Заметим, что векторы $|\tilde{i}\rangle_B$ *не* обязаны быть взаимно ортогональными или нормированными.

Предположим теперь, что $\{|i\rangle_A\}$ – базис, в котором ρ_A диагональна

$$\rho_A = \sum_i p_i |i\rangle_{A\,A}\langle i|. \tag{2.83}$$

Мы можем также вычислить ρ_A, выполняя операцию взятия частичного следа

$$\begin{aligned}\rho_A &= \mathrm{tr}_B\left(|\psi\rangle_{AB\,AB}\langle\psi|\right) = \\ &= \mathrm{tr}_B\left(\sum_{ij}|i\rangle_{A\,A}\langle j|\otimes|\tilde{i}\rangle_{B\,B}\langle\tilde{j}|\right) = \sum_{ij}{}_B\langle\tilde{j}|\tilde{i}\rangle_B\left(|i\rangle_{A\,A}\langle j|\right).\end{aligned} \tag{2.84}$$

Последнее равенство в (2.84) получено с учетом того, что

$$\begin{aligned}\mathrm{tr}_B\left(|\tilde{i}\rangle_{B\,B}\langle\tilde{j}|\right) &= \sum_k {}_B\langle k|\tilde{i}\rangle_{B\,B}\langle\tilde{j}|k\rangle_B = \\ &= \sum_k {}_B\langle\tilde{j}|k\rangle_{B\,B}\langle k|\tilde{i}\rangle_B = {}_B\langle\tilde{j}|\tilde{i}\rangle_B,\end{aligned} \tag{2.85}$$

где $\{|k\rangle_B\}$ – ортонормированный базис в $\mathcal{H}_B$. Сравнивая уравнения (2.83) и (2.84), мы видим, что

$${}_B\langle\tilde{j}|\tilde{i}\rangle_B = p_i\delta_{ij}. \tag{2.86}$$

Следовательно, в конце концов оказалось, что $\{|\tilde{i}\rangle_B\}$ *взаимно ортогональны*. Соответствующим изменением масштаба мы получаем ортонормированные векторы

$$|i'\rangle_B = p_i^{-1/2}|\tilde{i}\rangle_B \tag{2.87}$$

[мы можем полагать $p_i \neq 0$, поскольку уравнение (2.87) необходимо только для фигурирующих в сумме (2.83) слагаемых] и, следовательно, разложение

$$|\psi\rangle_{AB} = \sum_i \sqrt{p_i}|i\rangle_A|i'\rangle_B \tag{2.88}$$

в *специальных* ортонормированных базисах в $\mathcal{H}_A$ и $\mathcal{H}_B$.

Уравнение (2.88) представляет собой разложение Шмидта чистого двухкубитового состояния $|\psi\rangle_{AB}$[1]. Любое чистое двухкубитовое состояние может быть представлено в этой форме, но, естественно, используемые при

[1] Разложение Шмидта было получено задолго до появления квантовой механики: E. Schmidt, *Zur theorie der linearen and nichtlinearen integralgleichungen*, Math. Annalen, **63**, 433–476 (1906). – *Прим. ред.*

этом базисы зависят от разлагаемого состояния. В общем случае мы не можем одновременно разложить $|\psi\rangle_{AB}$ и $|\varphi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ в виде (2.88), используя для этого одни и те же ортонормированные базисы в $\mathcal{H}_A$ и $\mathcal{H}_B$.

Используя уравнение (2.88), мы можем также вычислить частичный след по $\mathcal{H}_A$ и получить

$$\boldsymbol{\rho}_B = \mathrm{tr}_A \left(|\psi\rangle_{AB\ AB}\langle\psi| \right) = \sum_i p_i |i'\rangle_{B\ B}\langle i'|. \tag{2.89}$$

Мы видим, что $\boldsymbol{\rho}_A$ и $\boldsymbol{\rho}_B$ имеют *одинаковые ненулевые собственные числа*. Конечно, при этом совсем не обязательно, чтобы $\mathcal{H}_A$ и $\mathcal{H}_B$ имели одинаковые размерности, так что количество *нулевых* собственных значений $\boldsymbol{\rho}_A$ и $\boldsymbol{\rho}_B$ может различаться.

Если $\boldsymbol{\rho}_A$ (и, следовательно, $\boldsymbol{\rho}_B$) не имеет других вырожденных собственных значений, кроме нулевых, тогда разложение Шмидта состояния $|\psi\rangle_{AB}$ существенно однозначно определяется матрицами плотности $\boldsymbol{\rho}_A$ и $\boldsymbol{\rho}_B$. Мы можем диагонализовать $\boldsymbol{\rho}_A$ и $\boldsymbol{\rho}_B$, чтобы найти векторы $|i\rangle_A$ и $|i'\rangle_B$. После этого мы объединим в пары собственные состояния $\boldsymbol{\rho}_A$ и $\boldsymbol{\rho}_B$, отвечающие одинаковым собственным значениям, чтобы получить (2.88). Мы выбрали фазы наших базисных состояний так, чтобы они не возникали в коэффициентах в суммах; сохранилась лишь свобода переопределения векторов $|i\rangle_A$ и $|i'\rangle_B$ путем умножения их на противоположные фазы (что, конечно, оставляет неизменным выражение (2.88)).

Но если $\boldsymbol{\rho}_A$ имеет вырожденные ненулевые собственные значения, тогда нам необходимо больше информации, чем та, которая позволила определить разложение Шмидта состояния $|\psi\rangle_{AB}$ по $\boldsymbol{\rho}_A$ и $\boldsymbol{\rho}_B$; нам нужно знать, какое состояние $|i'\rangle_B$ объединяется в пару с $|i\rangle_A$. Например, если $\mathcal{H}_A$ и $\mathcal{H}_B$ N-мерны, а $\mathbf{U}_{ij}$ — произвольная унитарная $N \times N$-матрица, то

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{N}} \sum_{i,j=1}^{N} |i\rangle_A \mathbf{U}_{ij} |j'\rangle_B \tag{2.90}$$

будет давать $\boldsymbol{\rho}_A = \boldsymbol{\rho}_B = \frac{1}{N}\mathbf{1}$ после вычисления парциальных частичных следов. Более того, мы можем выполнить одновременно унитарные преобразования в $\mathcal{H}_A$ и $\mathcal{H}_B$:

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{N}} \sum_i |i\rangle_A |i'\rangle_B = \frac{1}{\sqrt{N}} \sum_{ijk} \mathbf{U}^*_{ij} |j\rangle_A \mathbf{U}_{ik} |k'\rangle_B ; \tag{2.91}$$

это сохраняет состояние $|\psi\rangle_{AB}$, но иллюстрирует имеющуюся здесь неоднозначность базиса, используемого в разложении Шмидта состояния $|\psi\rangle_{AB}$.

2.4.1. Запутанность

Каждому чистому двухкубитовому состоянию $|\psi\rangle_{AB}$ можно сопоставить положительное целое число, *число Шмидта*, представляющее собой количество ненулевых собственных значений ρ_A (или ρ_B) и, следовательно, — число слагаемых в разложении Шмидта состояния $|\psi\rangle_{AB}$. С помощью этой величины мы можем определить, что значит быть *запутанным* для чистого двухкубитового состояния: $|\psi\rangle_{AB}$ запутано (или несепарабельно) если его число Шмидта больше единицы; в противном случае оно *сепарабельно* (или не запутано). Таким образом, сепарабельное чистое состояние двух кубитов представляет собой прямое произведение чистых состояний из $\mathcal{H}_A$ и $\mathcal{H}_B$:

$$|\psi\rangle_{AB} = |\varphi\rangle_A \otimes |\chi\rangle_B\,; \tag{2.92}$$

тогда и приведенные матрицы плотности $\rho_A = |\varphi\rangle_{A\,A}\langle\varphi|$, $\rho_B = |\chi\rangle_{B\,B}\langle\chi|$ являются чистыми. Любое состояние, которое не может быть представлено в виде такого прямого произведения, является запутанным; тогда ρ_A и ρ_B представляют собой смешанные состояния.

Одна из наших главных целей этого семестра — лучше понять смысл запутанности. Иногда не совсем строго и корректно говорят, что подсистемы A и B не коррелированы, если состояние $|\psi\rangle_{AB}$ — сепарабельно; в конце концов, два спина в сепарабельном состоянии

$$|\uparrow\rangle_A|\uparrow\rangle_B, \tag{2.93}$$

несомненно, коррелированы — оба они ориентированы в одном направлении. Однако характер корреляций между A и B в запутанном и сепарабельном состояниях различен. Вероятно, решающим различием является то, что *запутанность нелокальна*. Единственным способом запутать A и B является для двух подсистем их непосредственное взаимодействие друг с другом.

Мы можем приготовить состояние (2.93), не приводя спины A и B в контакт друг с другом. Нам нужно только послать сообщение (классическое!) двум ассистентам (Алисе и Бобу[1]), чтобы оба они приготовили спин в состоянии, ориентированном вдоль оси z. Но единственным способом превратить (2.93) в запутанное состояние, типа

$$\frac{1}{\sqrt{2}}(|\uparrow\rangle_A|\uparrow\rangle_B + |\downarrow\rangle_A|\downarrow\rangle_B), \tag{2.94}$$

является применение к нему *коллективного* унитарного преобразования. Локальные унитарные преобразования вида $\mathbf{U}_A \otimes \mathbf{U}_B$ и выполненные Алисой и Бобом локальные измерения *не могут увеличить число Шмидта*

[1] Алиса и Боб (A и B) — традиционные персонажи теории квантовой информации. — *Прим. ред.*

двухкубитового состояния, независимо от того, как долго Алиса и Боб обсуждали свои действия. Чтобы запутать два кубита, мы *должны* собрать их вместе и позволить им взаимодействовать.

Как мы обсудим позже, можно также определить различие между запутанным и сепарабельным двухкубитовыми *смешанными* состояниями. Мы также обсудим различные способы, которыми локальные операции могут модифицировать форму запутанности, а также некоторые возможности использования запутанности.

2.5. Неоднозначность интерпретации ансамблей

2.5.1. Выпуклость

Напомним, что оператор ρ, действующий в гильбертовом пространстве $\mathcal{H}$, может рассматриваться как оператор плотности, если он обладает тремя свойствами:

(1) ρ самосопряжен;

(2) ρ неотрицателен;

(3) $\mathrm{tr}(\rho) = 1$.

Отсюда непосредственно следует, что из двух данных матриц плотности ρ_1 и ρ_2 мы всегда можем построить другую матрицу плотности как выпуклую линейную комбинацию: при любом вещественном λ, удовлетворяющем $0 \leqslant \lambda \leqslant 1$,

$$\rho(\lambda) = \lambda\rho_1 + (1-\lambda)\rho_2 \tag{2.95}$$

представляет собой матрицу плотности. Легко видеть, что $\rho(\lambda)$ удовлетворяет свойствам (1) и (3), если ими обладают ρ_1 и ρ_2. Чтобы проверить (2), вычислим

$$\langle\psi|\rho(\lambda)|\psi\rangle = \lambda\langle\psi|\rho_1|\psi\rangle + (1-\lambda)\langle\psi|\rho_2|\psi\rangle \geqslant 0; \tag{2.96}$$

неотрицательность $\rho(\lambda)$ обеспечивается тем, что таковыми являются ρ_1 и ρ_2. Таким образом, мы показали, что в гильбертовом пространстве $\mathcal{H}$ размерности N операторы плотности образуют *выпуклое подмножество* вещественного векторного пространства эрмитовых $N \times N$-матриц. (Подмножество векторного пространства называется выпуклым, если оно содержит отрезки прямых линий, соединяющие любые две его точки.)

Большинство операторов плотности могут быть многими различными способами представлены в виде сумм других операторов плотности. В этом отношении чистые состояния занимают особое положение — невозможно выразить чистое состояние как выпуклую сумму двух других чистых состояний. Рассмотрим чистое состояние $\rho = |\psi\rangle\langle\psi|$; пусть $|\psi_\perp\rangle$ обозначает вектор, ортогональный $|\psi\rangle$, $\langle\psi_\perp|\psi\rangle = 0$. Предположим, что ρ можно разложить, как в уравнении (2.95); тогда

$$\langle\psi_\perp|\rho|\psi_\perp\rangle = 0 = \lambda\langle\psi_\perp|\rho_1|\psi_\perp\rangle + (1-\lambda)\langle\psi_\perp|\rho_2|\psi_\perp\rangle. \qquad (2.97)$$

Так как правая часть является суммой двух неотрицательных слагаемых, оба они должны быть одновременно равны нулю. Если λ не нуль и не единица, то отсюда следует, что ρ_1 и ρ_2 ортогональны $|\psi_\perp\rangle$. Но поскольку $|\psi_\perp\rangle$ может быть любым вектором, ортогональным $|\psi\rangle$, мы приходим к выводу, что $\rho_1 = \rho_2 = \rho$.

Векторы выпуклого множества, которые не могут быть представлены в виде линейной комбинации других векторов этого множества, называются *крайними точками* множества. Мы только что показали, что чистые состояния являются крайними точками множества матриц плотности. Более того, *только* чистые состояния являются крайними, поскольку любое смешанное состояние может быть записано как $\rho = \sum_i p_i|i\rangle\langle i|$ в базисе, в котором оно диагонально, что является выпуклой суммой чистых состояний.

Мы уже встречались с этой структурой в обсуждении частного случая сферы Блоха. Мы говорили, что операторы плотности заполняют (единичный) шар в трехмерном множестве эрмитовых 2×2-матриц с единичным следом. Шар является выпуклым, а его крайними точками являются точки на поверхности. Аналогично, $N \times N$-операторы плотности образуют выпуклое подмножество (N^2-1)-мерного множества эрмитовых $N \times N$-матриц с единичным следом, крайними точками которого являются чистые состояния.

Однако в одном отношении 2×2-случай нетипичен: при $N > 2$ точки на границе множества матриц плотности не обязательно являются чистыми состояниями. Границу множества образуют все матрицы плотности, имеющие хотя бы одно нулевое собственное значение (поскольку существуют сколь угодно близкие к ним матрицы с отрицательными собственными значениями). Такая матрица плотности при $N > 2$ не является чистой, поскольку число ее ненулевых собственных чисел может превышать единицу.

2.5.2. Приготовление ансамбля

Выпуклость множества матриц плотности имеет простую, проясняющую суть дела, физическую интерпретацию. Допустим, что ассистент со-

сласен приготовить одно из двух возможных состояний; состояние ρ_1 готовится с вероятностью λ, а состояние ρ_2 — с вероятностью $1-\lambda$. (Можно воспользоваться генератором случайных чисел, чтобы осуществить этот выбор.) Чтобы вычислить ожидаемое значение любой наблюдасмой M, мы усредняем ее по *обоим* выборам приготовления, а результат квантового измерения есть

$$\begin{aligned}\langle \mathbf{M} \rangle &= \lambda \langle \mathbf{M} \rangle_1 + (1-\lambda)\langle \mathbf{M} \rangle_2 = \\ &= \lambda \operatorname{tr}(\mathbf{M}\rho_1) + (1-\lambda)\operatorname{tr}(\mathbf{M}\rho_2) = \\ &= \operatorname{tr}(\mathbf{M}\rho(\lambda)). \end{aligned} \tag{2.98}$$

Таким образом, все ожидаемые значения не отличимы от тех, что мы получили бы, если бы вместо этого было приготовлено состояние $\rho(\lambda)$ Таким образом, мы имеем операционную процедуру, данные методы приготовления состояний ρ_1 и ρ_2 для приготовления произвольной выпуклой комбинации.

Действительно, для любого смешанного состояния ρ существует бесконечное множество способов его представления в виде выпуклой комбинации других состояний и, следовательно, бесконечное разнообразие процедур, которые мы могли бы применить для приготовления ρ. И каждая из этих процедур ведет к одним и тем же следствиям для любой мыслимой наблюдаемой рассматриваемой системы. Но чистое состояние совсем другое — оно может быть приготовлено одним единственным способом. (То есть оно «чистое» относительно чистых состояний.) Каждое чистое состояние является собственным состоянием некоторой наблюдаемой, например, для состояния $\rho = |\psi\rangle\langle\psi|$ измерение проекции $\mathbf{E} = |\psi\rangle\langle\psi|$ гарантирует результат 1. (В качестве примера вспомним, что каждое чистое состояние одного кубита представляет собой состояние типа «спин вверх» вдоль некоторой оси). Поскольку ρ является состоянием, для которого результат измерения $\mathbf{E}$ со 100% вероятностью равен единице, нет никакой возможности воспроизвести это наблюдаемое свойство, выбирая один из нескольких возможных способов его приготовления. Таким образом, приготовление чистого состояния совершенно однозначно (мы можем установить этот единственный способ его приготовления, если имеем множество копий состояния, чтобы поэкспериментировать с ними), тогда как в приготовлении смешанного состояния всегда возможны варианты.

Как велика эта неоднозначность? Так как любое ρ можно представить в виде суммы чистых состояний, задержим наше внимание на следующем вопросе: насколько большим числом способов может быть представ-

лен оператор плотности как выпуклая сумма чистых состояний? Математически этот вопрос звучит так: насколько большим числом способов можно записать ρ в виде суммы *крайних состояний*?

В качестве первого примера рассмотрим «максимально смешанное» состояние одного кубита:

$$\rho = \frac{1}{2}\mathbf{1}. \tag{2.99}$$

Такое состояние действительно может быть приготовлено бесконечным числом способов как ансамбль чистых состояний. Например,

$$\rho = \frac{1}{2}|\uparrow_z\rangle\langle\uparrow_z| + \frac{1}{2}|\downarrow_z\rangle\langle\downarrow_z|, \tag{2.100}$$

такое ρ мы получим, если приготовим состояния или $|\uparrow_z\rangle$, или $|\downarrow_z\rangle$, появляющиеся с вероятностью $\frac{1}{2}$ каждое. Но также мы имеем

$$\rho = \frac{1}{2}|\uparrow_x\rangle\langle\uparrow_x| + \frac{1}{2}|\downarrow_x\rangle\langle\downarrow_x|, \tag{2.101}$$

такое ρ мы получим, если приготовим состояния или $|\uparrow_x\rangle$, или $|\downarrow_x\rangle$, появляющиеся с вероятностью $\frac{1}{2}$ каждое. Эта процедура приготовления, бесспорно, *другая*. Тем не менее, наблюдая за одним спином, разницу между ними обнаружить невозможно.

И вообще, центральная точка шара Блоха является суммой любых двух диаметрально противоположных точек на сфере, поэтому, приготовив или $|\uparrow_A\rangle$, или $|\downarrow_A\rangle$, появляющиеся с вероятностью $\frac{1}{2}$ каждое, мы тем самым приготовим состояние $\rho = \frac{1}{2}\mathbf{1}$.

Различные способы приготовления ρ из ансамбля *взаимно ортогональных* чистых состояний существуют только тогда, когда ρ имеет два (или более) вырожденных собственных значения. Однако у нас нет серьезных оснований ограничивать наше внимание этими ансамблях. Мы можем рассмотреть точку внутри шара Блоха

$$\rho(\vec{P}) = \frac{1}{2}(\mathbf{1} + \vec{P}\cdot\vec{\sigma}) \tag{2.102}$$

с $0 < |\vec{P}| < 1$; это состояние также можно выразить как

$$\rho(\vec{P}) = \lambda\rho(\hat{n}_1) + (1-\lambda)\rho(\hat{n}_2), \tag{2.103}$$

если $\vec{P} = \lambda\hat{n}_1 + (1-\lambda)\hat{n}_2$ (или, другими словами, $\vec{P}$ лежит где-нибудь на отрезке прямой, соединяющей точки сферы $\hat{n}_1$ и $\hat{n}_2$). Очевидно, что для любого $\vec{P}$ существует такое решение, связанное с любой хордой сферы, проходящей через точку $\vec{P}$; все такие хорды образуют двухпараметрическое семейство.

Эта высокая степень неоднозначности приготовления смешанного квантового состояния является одной из характерных особенностей квантовой информации, которая резко контрастирует с классическими вероятностными распределениями. Рассмотрим в качестве примера распределение вероятностей одного классического бита. Существует два крайних распределения таких, в которых 0 или 1 возникают со 100% вероятностью. *Любое* распределение вероятностей для бита является выпуклой суммой этих двух крайних точек. Аналогично, если имеется N возможных состояний, то существует N крайних распределений, а любое распределение вероятностей имеет *единственное* разложение по этим крайним распределениям (выпуклое множество распределений вероятностей образует *симплекс*). Если 0 появляется с вероятностью 21%, 1 — с вероятностью 33%, а 2 — с вероятностью 46%, то существует единственная процедура приготовления, которая дает это распределение вероятностей!

2.5.3. Быстрее света?

Вернемся теперь к нашей ранней точке зрения — смешанное состояние системы A возникает вследствие *запутывания* A с системой B — чтобы продолжить рассмотрение последствий неоднозначности приготовления смешанных состояний. Если кубит имеет матрицу плотности

$$\rho_A = \frac{1}{2}|\uparrow_z\rangle_A\,{}_A\langle\uparrow_z| + \frac{1}{2}|\downarrow_z\rangle_A\,{}_A\langle\downarrow_z|, \tag{2.104}$$

эта матрица плотности могла бы возникнуть в результате запутывания двухкубитового чистого состояния $|\psi\rangle_{AB}$, представимого в виде разложения Шмидта:

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|\uparrow_z\rangle_A|\uparrow_z\rangle_B + |\downarrow_z\rangle_A|\downarrow_z\rangle_B\right). \tag{2.105}$$

Следовательно, интерпретация ансамбля ρ_A, в котором приготовлено или состояние $|\uparrow_z\rangle_A$, или состояние $|\downarrow_z\rangle_A$ (каждое с вероятностью $p = 1/2$), может быть реализована выполнением измерения кубита B. Мы измеряем кубит B в базисе $\{|\uparrow_z\rangle_B, |\downarrow_z\rangle_B\}$; если получается результат $|\uparrow_z\rangle_B$, то приготовлено состояние $|\uparrow_z\rangle_A$, если же получается результат $|\downarrow_z\rangle_B$, то приготовлено $|\downarrow_z\rangle_A$.

Но, как уже отмечалось, в этом случае базис Шмидта не единственен, поскольку ρ_A имеет вырожденные собственные значения. Мы можем одновременно применить унитарные преобразования к кубитам A и B (если мы применяем $\mathbf{U}$ к A, то к B мы должны применить $\mathbf{U}^*$), не меняя при этом двухкубитовое чистое состояние $|\psi\rangle_{AB}$. Следовательно, для *любого* единичного трехмерного вектора $\hat{n}$ состояние $|\psi\rangle_{AB}$ имеет разложение Шмидта вида

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|\uparrow_{\hat{n}}\rangle_A|\uparrow_{\hat{n}'}\rangle_B + |\downarrow_{\hat{n}}\rangle_A|\downarrow_{\hat{n}'}\rangle_B\right). \qquad (2.106)$$

Отсюда видно, что, измеряя кубит B в подходящем базисе, мы можем реализовать *любую* интерпретацию ρ_A как ансамбля двух чистых состояний.

Вдумчивые студенты после знакомства с этим свойством иногда загораются идеей предложить механизм сверхсветовой системы связи. Готовится много копий состояния $|\psi\rangle_{AB}$. Алиса забирает кубиты A с собой на туманность Андромеды, а Боб оставляет все кубиты B на Земле. Когда Боб хочет послать Алисе однобитовое сообщение, он выбирает, измерить ли ему σ_1 или σ_3 на всех своих спинах, приготовив таким образом спины Алисы в одном из двух ансамблей: $\{|\uparrow_x\rangle_A, |\downarrow_x\rangle_A\}$ или $\{|\uparrow_z\rangle_A, |\downarrow_z\rangle_A\}$.[1] Чтобы прочитать сообщение, Алиса сразу вслед за этим измеряет свои спины, чтобы увидеть, какой ансамбль был приготовлен.

Но *еще более* вдумчивые студенты (или студенты, слышавшие предыдущую лекцию) могут разглядеть изъян в этой схеме. Несмотря на то, что оба метода приготовления несомненно различны, оба ансамбля описываются в точности одной и той же матрицей плотности ρ_A. Таким образом, Алиса не может сделать никакого мыслимого измерения, чтобы различить эти два ансамбля, и нет возможности сообщить ей, какое действие совершил Боб. Сообщение «нечитабельно».

Почему тогда мы так уверенно утверждаем, что «оба метода приготовления несомненно различны»? Чтобы развеять любые сомнения относительно этого, представим, что Боб: (1) измеряет все свои спины вдоль оси $\hat{x}$ или (2) измеряет все свои спины вдоль оси $\hat{z}$, а затем вызывает Алису по межгалактическому телефону. Он *не говорит* Алисе, какое измерение он выполнил, (1) или (2), но сообщает ей все их результаты: «первый спин направлен вверх, второй — вниз» и т. д.. Теперь Алиса выполняет измерения (1) или (2) со *своими* спинами. Если они оба измеряли вдоль одной и той же оси, то Алиса обнаружит, что каждый из результатов ее измерений согласуется с тем, что нашел Боб. Но если Алиса и Боб выполняли измерения вдоль разных (ортогональных) осей, то Алиса *не обнаружит никаких*

[1] В этом случае $\mathbf{U}$ вещественно, поэтому $\mathbf{U} = \mathbf{U}^*$, а $\hat{n} = \hat{n}'$.

корреляций между их результатами. Примерно половина результатов ее измерений будет согласоваться с результатами Боба, примерно половина — противоречить им. Если Боб обещает выполнить (1) или (2) и предполагается отсутствие ошибок в приготовлении или измерении, тогда Алиса будет знать, что их действия были различными (даже если Боб не сообщал ей этой информации), сразу, как только результат одного из ее измерений вступит в противоречие с тем, что нашел Боб. Если же результаты всех их измерений согласуются, тогда, если было проведено достаточно много измерений, с очень высоким уровнем значимости Алиса будет считать, что она и Боб выполняли измерения вдоль одной и той же оси. (Даже с учетом возможных ошибок измерения этот статистический тест будет оставаться надежным, если частота появления ошибок достаточно низка). Таким образом, Алиса имеет возможность различить два использованных Бобом метода приготовления, однако в этом случае нет сверхсветовой связи, поскольку прежде чем Алиса смогла выполнить свою проверку, ею получен телефонный вызов от Боба.

2.5.4. Квантовое удаление (информации)

Мы говорили, что матрица плотности $\rho_A = \frac{1}{2}\mathbf{1}_A$ описывает спин в *некогерентной* суперпозиции чистых состояний $|\uparrow_z\rangle_A$ и $|\downarrow_z\rangle_A$. Оно отличимо от *когерентной* суперпозиции этих состояний, такой как

$$|\uparrow_x,\downarrow_x\rangle = \frac{1}{2}\left(|\uparrow_z\rangle \pm |\downarrow_z\rangle\right); \tag{2.107}$$

в этом случае относительная фаза двух состояний имеет наблюдаемые следствия (отличает $|\uparrow_x\rangle$ от $|\downarrow_x\rangle$). В случае некогерентной суперпозиции относительная фаза полностью ненаблюдаема. Суперпозиция становится некогерентной, если спин A запутывается с другим спином B, недоступным для наблюдения.

С эвристической точки зрения состояния $|\uparrow_z\rangle_A$ и $|\downarrow_z\rangle_A$ могут *интерферировать* (может быть наблюдаемой относительная фаза этих состояний) только тогда, когда мы не имеем информации о том, находится ли спин в состоянии $|\uparrow_z\rangle_A$ или в состоянии $|\downarrow_z\rangle_A$. Даже более того, интерференция может наблюдаться только тогда, когда *в принципе нет никакой возможности* определить, находится ли спин в состоянии вверх или вниз вдоль оси $\hat{z}$. Запутывание спина A со спином B разрушает интерференцию (по причине *декогерентизации* A), поскольку у нас появляется принципиальная возможность определить, находится ли спин A в состоянии вверх или вниз вдоль оси $\hat{z}$, выполняя соответствующее измерение спина B.

Но сейчас мы увидим, что утверждение о том, что запутывание является причиной декогерентизации, требует оговорки. Допустим, что Боб измеряет спин B вдоль оси $\hat{x}$, получая в качестве результата или $|\uparrow_x\rangle_B$, или $|\downarrow_x\rangle_B$, и посылает результат своего измерения Алисе. *Теперь* спин Алисы находится в чистом состоянии (или в $|\uparrow_x\rangle_A$, или в $|\downarrow_x\rangle_A$), а фактически в когерентной суперпозиции $|\uparrow_z\rangle_A$ и $|\downarrow_z\rangle_A$. Мы сумели восстановить чистоту состояния спина Алисы, прежде чем ее скрыло облако декогерентизации!

Предположим, что Боб позволил своему спину пройти через прибор Штерна–Герлаха, ориентированный вдоль оси $\hat{z}$. Ну, конечно, спин Алисы не может вести себя, как в состоянии когерентной суперпозиции $|\uparrow_z\rangle_A$ и $|\downarrow_z\rangle_A$; всего лишь проследив за тем, по какому пути прошел его спин, Боб будет знать, ориентирован ли спин Алисы вверх или вниз вдоль оси $\hat{z}$. Но допустим, что Боб не производит наблюдений. Вместо этого он вновь тщательно фокусирует два пучка, не делая никакой записи о том, вверх или вниз переместился его спин, после чего позволяет пройти спину через второй прибор Штерна–Герлаха, ориентированный вдоль оси $\hat{x}$. На этот раз он производит наблюдение и сообщает Алисе результат своего измерения σ_1. Теперь когерентность состояния спина Алисы восстановлена!

Эта ситуация была названа *квантовым ластиком*. Запутывание двух спинов создает «ситуацию измерения», в котором теряется когерентность $|\uparrow_z\rangle_A$ и $|\downarrow_z\rangle_A$, вследствие чего, наблюдая за спином B, мы можем выяснить, ориентирован спин A вверх или вниз вдоль оси $\hat{z}$. Но когда мы (вслед за этим) измеряем спин B вдоль оси $\hat{x}$, эта информация «стирается». Ни результат $|\uparrow_x\rangle_B$, ни $|\downarrow_x\rangle_B$ — ничего не сообщают нам о том, ориентирован ли спин A вверх или вниз вдоль оси $\hat{z}$, поскольку Боб не позаботился сохранить информацию «какой путь», что можно было сделать, наблюдая за движением спина в первом приборе Штерна – Герлаха[1]. Следовательно, для спина A вновь возможно поведение типа когерентной суперпозиции $|\uparrow_z\rangle_A$ и $|\downarrow_z\rangle_A$ (и это *после того*, как Алиса узнает о результате Боба).

Мы можем лучше понять квантовый ластик с точки зрения ансамбля. Алиса имеет множество спинов, выбранных из ансамбля $\rho_A = \frac{1}{2}\mathbf{1}_A$, и у нее нет возможности наблюдать интерференцию между состояниями $|\uparrow_z\rangle_A$ и $|\downarrow_z\rangle_A$. Когда Боб выполняет свое измерение вдоль оси $\hat{x}$, реализуется конкретно приготовленный ансамбль. Однако это не дает эффекта, который может почувствовать Алиса, — состояние ее спинов, *как и прежде*, описы-

[1]Часто говорят, что была стерта «welcher weg»-информация, поскольку по-немецки это звучит более изысканно [«welcher weg» (*нем.*) – «какой путь» (перев.)].

вается ансамблем $\rho_A = \frac{1}{2}\mathbf{1}_A$. Но когда Алиса получает телефонное сообщение от Боба, она может отобрать *субансамбль* из тех своих спинов, которые находятся в чистом состоянии $|\uparrow_x\rangle_A$. Сообщенная Бобом информация позволяет Алисе отделить чистые состояния от максимально смешанных.

Другой намек на квантовый ластик иногда называют *отложенным выбором*. Это значит, что описанная нами ситуация в действительности полностью симметрична относительно Алисы и Боба, то есть невозможно определить, кто первым произвел измерение. (Действительно, если измерения Алисы и Боба являются событиями, разделенными пространственно-подобным интервалом, то их следование друг за другом во времени неинвариантно, оно зависит от системы отсчета, используемой наблюдателем.) Алиса могла бы измерить все свои спины сегодня (скажем, вдоль оси $\hat{x}$), прежде чем Боб решит, как он будет измерять свои спины. На следующей неделе Боб решает «приготовить» спины Алисы в состояниях $|\uparrow_{\hat{n}}\rangle_A$ и $|\downarrow_{\hat{n}}\rangle_A$ (это и есть «отложенный выбор»). После этого он сообщает Алисе о том, какие спины были в состоянии $|\uparrow_{\hat{n}}\rangle_A$, а она может проконтролировать запись его измерения, чтобы убедиться, что

$$(\sigma_1)_{\hat{n}} = \hat{n} \cdot \hat{x}. \tag{2.108}$$

Результат будет один и тот же независимо от того, «приготовил» Боб спины до или после измерения Алисы.

Мы утверждали, что матрица плотности представляет полное физическое описание подсистемы A, поскольку она характеризует все возможные измерения, которые на ней могут быть выполнены. Иногда раздаются возражения[1], что явление квантового ластика демонстрирует обратное. Так как полученная от Боба информация даст Алисе возможность извлечь чистое состояние из смеси, то как можно утверждать, что в ρ_A закодировано все, что Алиса может узнать об A?

Я не считаю это правильным выводом. Скорее я хочу сказать, что квантовый ластик предоставляет еще одну возможность повторить наше заклинание: «Информация материальна». Состояние ρ_A системы A и состояние ρ_A, дополненное информацией, полученной Алисой от Боба, — не одно и то же. Эта информация (которая снабжает метками субансамбли) изменяет физическое описание. Чтобы выразить это математически, мы должны включить в наше описание «знание Алисы о состоянии». Ансамбль спинов, о котором Алиса не имеет информации, вверх или вниз направлен каждый

[1] Например, в книге: Roger Penrose, *Shadows of the Mind. A Search for the Missing Science of Consciousness*, Oxford University Press, New York et al, 1994; перевод Роджер Пенроуз, *Тени разума. В поисках науки о сознании*. Москва–Ижевск: ИКИ (2003)

спин, представляет собой другое состояние, нежели ансамбль, в котором Алисе известно состояние каждого спина[1].

2.5.5. Теорема ЖХЙВ

До сих пор мы рассматривали квантовый ластик только в связи с одиночным кубитом, описываемым ансамблем равновероятных, взаимно ортогональных состояний (то есть $\rho_A = \frac{1}{2}1_A$). Это обсуждение можно существенно обобщить.

Мы уже видели, что смешанное состояние любой квантовой системы можно бесконечным числом различных способов реализовать как ансамбль чистых состояний. Рассмотрим одну такую реализацию для матрицы плотности ρ_A

$$\rho_A = \sum_i p_i |\varphi_i\rangle_A \, {}_A\langle\varphi_i|, \qquad \sum_i p_i = 1. \tag{2.109}$$

Здесь все состояния $\{|\varphi_i\rangle_A\}$ являются нормированными, но не обязательно взаимно ортогональными векторами. Тем не менее ρ_A можно понимать как ансамбль, в котором каждое чистое состояние $|\varphi_i\rangle_A \, {}_A\langle\varphi_i|$ возникает с вероятностью p_i.

Конечно, для любого такого ρ_A мы можем построить его «очищение», двухкубитовое чистое состояние $|\Phi_1\rangle_{AB}$, которое дает ρ_A при вычислении частичного следа в пространстве $\mathcal{H}_B$. Такое очищение имеет вид

$$|\Phi_1\rangle_{AB} = \sum_i \sqrt{p_i} |\varphi_i\rangle_A |\alpha_i\rangle_B, \tag{2.110}$$

где векторы $|\alpha_i\rangle_B \in \mathcal{H}_B$ взаимно ортогональны и нормированы:

$${}_B\langle\alpha_i|\alpha_j\rangle_B = \delta_{ij}. \tag{2.111}$$

Очевидно, что

$$\mathrm{tr}_B \left(|\Phi_1\rangle_{AB} \, {}_{AB}\langle\Phi_1| \right) = \rho_A. \tag{2.112}$$

Более того, мы можем представить выполнение ортогонального измерения в системе B, проецирующее на базис $|\alpha_i\rangle_B$.[2] С вероятностью p_i получится результат $|\alpha_i\rangle_B$ и приготовит чистое состояние $|\varphi_i\rangle_A \, {}_A\langle\varphi_i|$ системы A.

[1] Это «знание состояния» не должно быть действительно состоянием человеческого разума; достаточной будет любая (неодушевленная) запись, помечающая субансамбль.

[2] Пространство $\mathcal{H}_B$ может быть и не натянутым на векторы $|\alpha_i\rangle_B$, однако в состоянии $|\Phi_1\rangle_{AB}$ никогда не появляются результаты измерения, ортогональные всем $|\alpha_i\rangle_B$.

Таким образом, для данного очищения $|\Phi_1\rangle_{AB}$ состояния ρ_A существует такое измерение в системе B, при выполнении которого реализуется состояние $|\varphi_i\rangle_A$ ансамбля ρ_A. По известному результату измерения в B мы успешно выделили одно из чистых состояний $|\varphi_i\rangle_A$ смеси ρ_A.

Только что описанное представляет собой обобщение процедуры приготовления состояния $|\uparrow_z\rangle_A$ путем измерения спина B вдоль оси $\hat{z}$ (в нашем обсуждении двух запутанных кубитов). Но чтобы обобщить понятие квантового ластика, мы хотим видеть, что, выполняя разные измерения B в состоянии $|\Phi_1\rangle_{AB}$, можно реализовать *разные* интерпретации ансамбля ρ_A. Пусть

$$\rho_A = \sum_\mu q_\mu |\psi_\mu\rangle_A \, {}_A\langle\psi_\mu| \tag{2.113}$$

— другая реализация той же самой матрицы плотности ρ_A как ансамбля чистых состояний. Для этого ансамбля тоже существует соответствующее очищение

$$|\Phi_2\rangle_{AB} = \sum_\mu \sqrt{q_\mu}|\psi_\mu\rangle_A|\beta_\mu\rangle_B, \tag{2.114}$$

где вновь $\{|\beta_\mu\rangle\}$ — ортонормированные векторы из $\mathcal{H}_B$. Итак, в состоянии $|\Phi_2\rangle_{AB}$ мы можем реализовать ансамбль, выполняя в $\mathcal{H}_B$ измерение, проецирующее на базис $\{|\beta_\mu\rangle_B\}$.

Как связаны состояния $|\Phi_1\rangle_{AB}$ и $|\Phi_2\rangle_{AB}$? Фактически мы можем легко показать, что

$$|\Phi_1\rangle_{AB} = (\mathbf{1}_A \otimes \mathbf{U}_B)|\Phi_2\rangle_{AB}; \tag{2.115}$$

два состояния отличаются унитарным изменением базиса, действующим только в $\mathcal{H}_B$, или

$$|\Phi_1\rangle_{AB} = \sum_\mu \sqrt{q_\mu}|\psi_\mu\rangle_A|\gamma_\mu\rangle_B, \tag{2.116}$$

где

$$|\gamma_\mu\rangle_B = \mathbf{U}_B|\beta_\mu\rangle_B \tag{2.117}$$

— другой ортонормированный базис в $\mathcal{H}_B$. Итак, мы видим, что существует *единственное* очищение $|\Phi_1\rangle_{AB}$ смешанного состояния ρ_A такое что, выбирая измерение соответствующей наблюдаемой в системе B, мы можем реализовать либо $\{|\varphi_i\rangle\}$-ансамбль, либо $\{|\psi_\mu\rangle\}$-ансамбль!

Аналогично мы можем рассмотреть множество ансамблей, реализующих смешанное состояние ρ_A, где максимальное число чистых состояний, возникающих в любом из этих ансамблей, равно n. Тогда мы мо-

жем выбрать гильбертово пространство $\mathcal{H}_B$ размерности n и чистое состояние $|\Phi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ такое, что любой из ансамблей может быть реализован путем измерения соответствующей наблюдаемой в $\mathcal{H}_B$. В этом и состоит *теорема ЖХЙВ*[1]. Она выражает явление квантового ластика в его наиболее общей форме.

Фактически теорема ЖХЙВ является почти тривиальным следствием разложения Шмидта. Оба состояния, $|\Phi_1\rangle_{AB}$ и $|\Phi_2\rangle_{AB}$, имеют разложение Шмидта, а поскольку при вычислении частичного следа по B оба они дают одно и то же смешанное состояние ρ_A, эти разложения должны иметь вид

$$|\Phi_1\rangle_{AB} = \sum_k \sqrt{\lambda_k}|k\rangle_A|k'_1\rangle_B,$$
$$|\Phi_2\rangle_{AB} = \sum_k \sqrt{\lambda_k}|k\rangle_A|k'_2\rangle_B, \qquad (2.118)$$

где λ_k — собственные значения, а $|k\rangle_A$ — соответствующие им собственные векторы ρ_A. Но поскольку $\{|k'_1\rangle_B\}$ и $\{|k'_2\rangle_B\}$ — ортонормированные базисы в $\mathcal{H}_B$, существует такое унитарное преобразование $\mathbf{U}_B$, что

$$|k'_1\rangle_B = \mathbf{U}_B|k'_2\rangle_B, \qquad (2.119)$$

откуда непосредственно следует уравнение (2.115).

В ансамбле чистых состояний, описываемом уравнением (2.109), мы хотели бы сказать, что чистые состояния $|\varphi_i\rangle_A$ образуют в нем *некогерентную* суперпозицию — наблюдатель в системе A не может детектировать относительные фазы этих состояний. С эвристической точки зрения причина того, что эти состояния не могут интерферировать, состоит в том, что, выполняя в системе B измерение, проецирующее на ортонормированный базис $\{|\alpha_i\rangle_B\}$, в принципе мы имеем возможность обнаружить, какой представитель ансамбля реализован на самом деле. Однако проецируя вместо этого на базис $\{|\gamma_\mu\rangle_B\}$ и передавая в систему A информацию о результате измерения, мы можем выделить из ансамбля одно из чистых состояний $|\psi_\mu\rangle_A$, даже если оно может быть когерентной суперпозицией состояний $|\varphi_i\rangle_A$. В сущности, измерение B в базисе $\{|\gamma_\mu\rangle_B\}$ «стирает» «welcher weg»-информацию (состоянием A является либо $|\varphi_i\rangle_A$, либо $|\varphi_j\rangle_A$). В этом смысле теорема ЖХЙВ характеризует обобщенный квантовый «ластик». Еще раз повторим мораль, что *информация материальна* — информация, полученная в системе B, после ее передачи в A изменяет физическое описание состояния A.

[1] ЖХДжВ: Жизан, Хастон, Джозса, Вутерс.

2.6. Резюме

Аксиомы. Ареной квантовой механики служит гильбертово пространство $\mathcal{H}$. Основными предположениями являются:

(1) *Состояние* представляет собой *луч* в $\mathcal{H}$.

(2) *Наблюдаемая* представляется *самосопряженным оператором* в $\mathcal{H}$.

(3) *Измерением* является ортогональная *проекция*.

(4) *Эволюция во времени унитарна*.

Оператор плотности. Если мы ограничиваем наше внимание только на части большей квантовой системы, предположения (1)–(4) не выполняются. В частности, квантовое состояние описывается не лучом, а оператором плотности $\boldsymbol{\rho}$, неотрицательным оператором с единичным следом. Оператор плотности описывает *чистое состояние* (состояние может быть описано лучом), если $\boldsymbol{\rho}^2 = \boldsymbol{\rho}$; в противном случае состояние является *смешанным*. В этом состоянии наблюдаемая M имеет ожидаемое значение $\mathrm{tr}(\mathbf{M}\boldsymbol{\rho})$.

Кубит. Квантовая система, определенная в двумерном гильбертовом пространстве, называется *кубитом*. Наиболее общая матрица плотности кубита имеет вид

$$\boldsymbol{\rho}(\vec{P}) = \frac{1}{2}\left(\mathbf{1} + \vec{P}\cdot\vec{\boldsymbol{\sigma}}\right), \tag{2.120}$$

где $\vec{P}$ — трехкомпонентный вектор длины $|\vec{P}| \leqslant 1$. В чистом состоянии $|\vec{P}| = 1$.

Разложение Шмидта. Для любой квантовой системы, состоящей из двух частей A и B (*бинарная* система), гильбертово пространство является тензорным произведением $\mathcal{H}_A \otimes \mathcal{H}_B$. Для любого чистого состояния $|\psi\rangle_{AB}$ бинарной системы существуют ортонормированные базисы $\{|i\rangle_A\}$ в $\mathcal{H}_A$ и $\{|i'\rangle_B\}$ в $\mathcal{H}_B$ такие, что

$$|\psi\rangle_{AB} = \sum_i \sqrt{p_i}|i\rangle_A|i'\rangle_B. \tag{2.121}$$

Уравнение (2.121) называется *разложением Шмидта* состояния $|\psi\rangle_{AB}$. В двухкубитовом чистом состоянии подсистемы A и B по отдельности описываются операторами плотности $\boldsymbol{\rho}_A$ и $\boldsymbol{\rho}_B$; из уравнения (2.121)

следует, что ρ_A и ρ_B имеют одинаковые ненулевые собственные значения (p_i). Количество ненулевых собственных значений называется *числом Шмидта* состояния $|\psi\rangle_{AB}$. Двухкубитовое чистое состояние называется *запутанным*, если его число Шмидта больше единицы.

Ансамбли. Операторы плотности в гильбертовом пространстве образуют выпуклое множество, а чистые состояния представляют собой *крайние точки* этого множества. Смешанное состояние системы A может быть приготовлено как *ансамбль* чистых состояний многими различными способами, неразличимыми экспериментально, если мы наблюдаем только систему A. Для любого смешанного состояния ρ_A системы A любое приготовление ρ_A как ансамбля чистых состояний, в принципе можно реализовать, выполняя измерение в другой системе B, с которой запутана система A. Фактически для множества таких приготовлений смешанного состояния ρ_A существует единственное запутанное состояние A и B такое, что любое из этих приготовлений может быть реализовано путем измерения соответствующей наблюдаемой в B (*теорема ЖХЙВ*). Выполняя измерение в системе B и сообщая его результат в систему A, мы можем выделить из смеси чистое состояние, выбранное из одного из ансамблей.

2.7. Упражнения

2.1. Точность воспроизведения вероятностной гипотезы. Один кубит (объект со спином-$\frac{1}{2}$) находится в неизвестном *чистом* состоянии $|\psi\rangle$, случайно выбранном из равномерно распределенного по сфере Блоха ансамбля. Мы наугад считаем, что этим состоянием является $|\phi\rangle$. Чему в среднем равна определяемая соотношением

$$F = |\langle\phi|\psi\rangle|^2 \tag{2.122}$$

точность воспроизведения нашей гипотезы?

2.2. Точность воспроизведения после измерения. После случайного выбора однокубитового чистого состояния, как в предыдущей задаче, мы выполняем измерение спина вдоль оси $\hat{z}$. Это измерение приготавливает состояние, описываемое матрицей плотности

$$\rho = \mathbf{P}_\uparrow\langle\psi|\mathbf{P}_\uparrow|\psi\rangle + \mathbf{P}_\downarrow\langle\psi|\mathbf{P}_\downarrow|\psi\rangle \tag{2.123}$$

(где $\mathbf{P}_{\uparrow,\downarrow}$ обозначает проектор на состояние спин-вверх или спин-вниз вдоль оси $\hat{z}$). С какой в среднем точностью

$$F \equiv \langle\psi|\boldsymbol{\rho}|\psi\rangle \tag{2.124}$$

эта матрица плотности воспроизводит начальное состояние $|\psi\rangle$? (Улучшение F по сравнению с ответом к предыдущей задаче является грубой мерой того, как много мы узнаем, выполнив измерение).

2.3. Разложение Шмидта. Для двухкубитового состояния

$$|\Phi\rangle_{AB} = \frac{1}{\sqrt{2}}|\uparrow\rangle_A\left(\frac{1}{2}|\uparrow\rangle_B + \frac{\sqrt{3}}{2}|\downarrow\rangle_B\right) + \\ + \frac{1}{\sqrt{2}}|\downarrow\rangle_A\left(\frac{\sqrt{3}}{2}|\uparrow\rangle_B + \frac{1}{2}|\downarrow\rangle_B\right). \tag{2.125}$$

1) Вычислите $\boldsymbol{\rho}_A = \mathrm{tr}_B(|\Phi\rangle_{AB\ AB}\langle\Phi|)$ и $\boldsymbol{\rho}_B = \mathrm{tr}_A(|\Phi\rangle_{AB\ AB}\langle\Phi|)$.
2) Найдите разложение Шмидта состояния $|\Phi\rangle_{AB}$.

2.4. Трехкубитовое чистое состояние. Существует ли разложение Шмидта произвольного трехкубитового чистого состояния? То есть если $|\psi\rangle_{ABC}$ — произвольный вектор в $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$, то можем ли мы найти ортогональные базисы $\{|i\rangle_A\}$, $\{|i\rangle_B\}$ и $\{|i\rangle_C\}$, такие что

$$|\psi\rangle_{ABC} = \sum_i \sqrt{p_i}|i\rangle_A \otimes |i\rangle_B \otimes |i\rangle_C\,? \tag{2.126}$$

Истолкуйте ваш ответ.

2.5. Квантовые корреляции в смешанном состоянии. Рассмотрим матрицу плотности двух кубитов:

$$\boldsymbol{\rho} = \frac{1}{8}\mathbf{1} + \frac{1}{2}|\psi^-\rangle\langle\psi^-|, \tag{2.127}$$

где $\mathbf{1}$ обозначает единичную 4×4-матрицу, а

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle|\downarrow\rangle - |\downarrow\rangle|\uparrow\rangle\right) \tag{2.128}$$

Пусть мы измеряем первый спин вдоль оси $\hat{n}$, а второй — вдоль оси $\hat{m}$, где $\hat{n} \cdot \hat{m} = \cos\theta$. Какова вероятность того, что оба спина находятся в состоянии «спин-вверх» вдоль соответствующих осей?

Глава 3

Основы II: Измерение и эволюция

3.1. За пределами ортогональных измерений

3.1.1. Ортогональные измерения

Мы хотели бы исследовать свойства *обобщенных* измерений, которые можно реализовать в системе A, выполняя ортогональные измерения в большей системе, содержащей A. Но сначала, следуя классической трактовке фон Неймана, кратко обсудим, как в принципе могут быть выполнены ортогональные измерения произвольной наблюдаемой.

Чтобы измерить наблюдаемую M, мы модифицируем гамильтониан Вселенной, включая в него связь между этой наблюдаемой и «переменной-указателем» («pointer» variable), которая будет играть роль прибора. Связь запутывает собственные состояния наблюдаемой с различимыми состояниями прибора, так что, «наблюдая» за прибором, мы можем приготовить собственное состояние наблюдаемой.

Конечно, это не вполне удовлетворительная модель измерения, поскольку мы не объяснили, как можно измерить «переменную-указатель». Как можно видеть, позиция фон Неймана состояла в том, что в принципе возможно скоррелировать состояния микроскопической квантовой системы со значениями макроскопической классической переменной, которые, само собой разумеется, мы способны различать. Конечно, возможно и желательно более обстоятельное объяснение; мы еще вернемся к этой проблеме ниже.

Мы можем представлять себе прибор как пробную частицу, распространяющуюся свободно, за исключением ее регулируемой связи с измеряемой квантовой системой. Если мы намерены измерять положение этой пробной частицы, то в начальном состоянии должен быть приготовлен достаточно узкий волновой пакет, но не слишком, поскольку очень узкий волновой пакет будет слишком быстро расплываться. Если начальная ширина волнового пакета равна Δx, неопределенность его скорости будет иметь

порядок $\Delta v = \Delta p/m \sim \hbar/m\Delta x$, так что, спустя время t, пакет расползется до ширины

$$\Delta x(t) = \Delta x + \frac{\hbar t}{m\Delta x}, \tag{3.1}$$

минимальное значение которой имеет прядок $[\Delta x(t)]^2 \sim [\Delta x]^2 \sim \hbar t/m$. Следовательно, если эксперимент продолжается в течение времени t, то разрешение, которого мы можем добиться в определении конечного положения пробной частицы, ограничено «стандартным квантовым пределом»:

$$\Delta x \gtrsim (\Delta x)_{SQL} \sim \sqrt{\frac{\hbar t}{m}}. \tag{3.2}$$

Будем считать нашу пробную частицу достаточно тяжелой, чтобы это ограничение было несущественным.

Гамильтониан, описывающий взаимодействие квантовой системы с пробной частицей, имеет вид:

$$\mathbf{H} = \mathbf{H}_0 + \frac{1}{2m}\mathbf{P}^2 + \lambda \mathbf{M}\mathbf{P}, \tag{3.3}$$

где $\mathbf{P}^2/2m$ — гамильтониан свободной пробной частицы (который в дальнейшем будет игнорироваться, поскольку пробная частица настолько тяжела, что расплыванием ее волнового пакета можно пренебречь), $\mathbf{H}_0$ — невозмущенный гамильтониан измеряемой системы, λ — константа связи, которую мы можем менять по своему усмотрению. Измеряемая наблюдаемая $\mathbf{M}$ связана с импульсом $\mathbf{P}$ пробной частицы.

Если $\mathbf{M}$ не коммутирует с $\mathbf{H}_0$, то нас будет беспокоить, как эта наблюдаемая изменяется в процессе измерения. Чтобы упростить анализ, предположим, что или $[\mathbf{M}, \mathbf{H}_0] = 0$, или же измерение выполняется настолько быстро, что в ходе его можно пренебречь свободной эволюцией системы. Тогда гамильтониан (3.3) можно аппроксимировать одним слагаемым $\mathbf{H} \simeq \lambda \mathbf{M}\mathbf{P}$ (где, конечно же, $[\mathbf{M}, \mathbf{P}] = 0$, так как $\mathbf{M}$ — наблюдаемая системы, а $\mathbf{P}$ — наблюдаемая пробной частицы), а оператор эволюции во времени —

$$\mathbf{U}(t) \simeq \exp\big[-i\lambda t \mathbf{M}\mathbf{P}\big]. \tag{3.4}$$

Разлагая в базисе, в котором наблюдаемая $\mathbf{M}$ диагональна

$$\mathbf{M} = \sum_a |a\rangle M_a \langle a|, \tag{3.5}$$

представим $\mathbf{U}(t)$ в виде

$$\mathbf{U}(t) = \sum_a |a\rangle \exp\big[-i\lambda t M_a \mathbf{P}\big]\langle a|. \tag{3.6}$$

Вспомним теперь, что $\mathbf{P}$ генерирует параллельные переносы *положения* пробной частицы: в координатном представлении $\mathbf{P} = -i\frac{d}{dx}$, так что $\exp(-ix_0\mathbf{P}) = \exp\left(-x_0\frac{d}{dx}\right)$ и разложение в ряд Тейлора дает

$$\exp(-ix_0\mathbf{P})\psi(x) = \psi(x - x_0). \tag{3.7}$$

Другими словами, оператор $\exp(-ix_0\mathbf{P})$, действуя на волновой пакет, перемещает его на x_0. Отсюда видно, что если наша квантовая система начинает эволюцию из суперпозиции собственных состояний оператора $\mathbf{M}$, первоначально не запутанной с пространственным волновым пакетом пробной частицы $|\psi(x)\rangle$, то по истечении времени t ее квантовое состояние эволюционирует в

$$\mathbf{U}(t)\left(\sum_a \alpha_a|a\rangle \otimes |\psi(x)\rangle\right) = \sum_a \alpha_a|a\rangle \otimes |\psi(x - \lambda t M_a)\rangle. \tag{3.8}$$

Теперь положение пробной частицы коррелирует со значениями наблюдаемой $\mathbf{M}$. Если волновой пакет достаточно узок, чтобы мы могли разрешить все значения M_a (что имеет место при $|\Delta x| \lesssim |\lambda t M_a|$), тогда всякий раз, измеряя (неважно как!) положение пробной частицы, мы будем готовить собственное состояние наблюдаемой M_a. С вероятностью $|\alpha_a|^2$ мы обнаружим, что положение пробной частицы сместилось на величину $\lambda t M_a$, и, следовательно, приготовим собственное состояние $|a\rangle$ оператора $\mathbf{M}$. Таким образом, мы приходим к выводу, что начальное состояние $|\varphi\rangle$ квантовой системы проецируется на $|a\rangle$ с вероятностью $|\langle a|\varphi\rangle|^2$. Это и есть модель ортогонального измерения фон Неймана.

Классическим примером служит прибор Штерна–Герлаха. Чтобы измерить $\boldsymbol{\sigma}_3$ объекта со спином-$1/2$, мы пропускаем его через область неоднородного магнитного поля

$$B_3 = \lambda z. \tag{3.9}$$

Магнитный момент объекта равен $\mu\vec{\boldsymbol{\sigma}}$, а индуцируемая магнитным полем связь –

$$\mathbf{H} = -\lambda\mu z\boldsymbol{\sigma}_3. \tag{3.10}$$

В этом случае $\boldsymbol{\sigma}_3$ является измеряемой наблюдаемой, связанной с положением z, а не с импульсом пробной частицы. В этом нет ничего страшного, поскольку z генерирует трансляции импульса $\mathbf{P}_z$ и, следовательно, эта

связь сообщает *импульс* пробной частице. Мы можем различить, сдвинулся объект вверх или вниз и таким образом определить спиновое состояние $|\uparrow_z\rangle$ или $|\downarrow_z\rangle$. Конечно, поворачивая магнит, можно измерить наблюдаемую $\hat{n}\cdot\vec{\sigma}$.

Как показало обсуждение квантового ластика, одного только факта возникновения запутанного состояния (3.8) еще *не достаточно* для объяснения, почему процедура измерения готовит собственное состояние оператора $\mathbf{M}$. В принципе измерение пробной частицы могло бы спроецировать ее состояние на некоторую специфическую суперпозицию собственных состояний оператора положения, и таким образом приготовить квантовую систему в суперпозиции собственных состояний оператора $\mathbf{M}$. Чтобы достичь более глубокого понимания процесса измерения, нужно объяснить, почему базис собственных состояний положения пробной частицы имеет особый статус среди других возможных базисов.

Если мы действительно можем, как это только что было описано, связать любую наблюдаемую с измеримой «переменной-указателем», тогда мы в состоянии выполнить любую мыслимую ортогональную проекцию в гильбертовом пространстве. Для данного набора операторов $\{\mathbf{E}_a\}$ таких, что

$$\mathbf{E}_a = \mathbf{E}_a^\dagger, \qquad \mathbf{E}_a\mathbf{E}_b = \delta_{ab}\mathbf{E}_a, \qquad \sum_a \mathbf{E}_a = \mathbf{1}, \tag{3.11}$$

мы можем выполнить процедуру измерения, которое с вероятностью

$$\mathrm{Prob}(a) = \langle\psi|\mathbf{E}_a|\psi\rangle \tag{3.12}$$

преобразует чистое состояние $|\psi\rangle\langle\psi|$ в

$$\frac{\mathbf{E}_a|\psi\rangle\langle\psi|\mathbf{E}_a}{\langle\psi|\mathbf{E}_a|\psi\rangle}. \tag{3.13}$$

Результаты такого измерения можно описать матрицей плотности, которая получается суммированием всех возможных результатов (3.13) (а не выбором одного частного результата), взвешенных вероятностями их появления (3.12). В таком случае измерение преобразует начальное чистое состояние в соответствии с

$$|\psi\rangle\langle\psi| \to \sum_a \mathbf{E}_a|\psi\rangle\langle\psi|\mathbf{E}_a. \tag{3.14}$$

Это *ансамбль* чистых состояний, описывающих результаты измерения. Он описывает состояние, в котором известно выполненное в системе измерение, но неизвестен его результат. Следовательно, начальное чистое состояние превращается в смешанное, за исключением тех случаев, когда оно

оказывается собственным состоянием измеряемой наблюдаемой. Если же начальным состоянием перед измерением было смешанное состояние, описываемое матрицей плотности ρ, тогда, представляя ρ как ансамбль чистых состояний, мы обнаружим, что в результате измерения

$$\rho \to \sum_a \mathbf{E}_a \rho \mathbf{E}_a. \tag{3.15}$$

3.1.2. Обобщенные измерения

Теперь мы хотели бы обобщить понятие измерения, выйдя за пределы рассмотренных фон Нейманом ортогональных измерений. Путь, ведущий к идее обобщенного измерения, состоит в предположении, что наша система A расширена до тензорного произведения $\mathcal{H}_A \otimes \mathcal{H}_B$ и мы выполняем в нем ортогональные измерения, которые в самой системе A уже не обязательно ортогональны. Сначала мы пойдем несколько другим путем, который, хотя и не имеет физической мотивации, выглядит более естественно и просто с математической точки зрения.

Предположим, что гильбертово пространство $\mathcal{H}_A$ является частью более широкого пространства, имеющего структуру *прямой суммы*:

$$\mathcal{H} = \mathcal{H}_A \oplus \mathcal{H}_A^{\perp}. \tag{3.16}$$

Нашим наблюдателям, «живущим» в $\mathcal{H}_A$, доступны только наблюдаемые с носителем в $\mathcal{H}_A$, то есть такие наблюдаемые $\mathbf{M}_A$, что для любого $|\psi^{\perp}\rangle \in \mathcal{H}_A^{\perp}$

$$\mathbf{M}_A|\psi^{\perp}\rangle = 0 = \langle\psi^{\perp}|\mathbf{M}_A. \tag{3.17}$$

Например, в двухкубитовом мире мы можем представить, что наши наблюдаемые имеют носители только в той части пространства, в которой второй кубит находится в состоянии $|0\rangle_2$. Тогда $\mathcal{H}_A = \mathcal{H}_1 \otimes |0\rangle_2$, а $\mathcal{H}_A^{\perp} = \mathcal{H}_1 \otimes |1\rangle_2$, где $\mathcal{H}_1$ — гильбертово пространство первого кубита. (Эта ситуация может показаться несколько искусственной, что я и подразумевал, говоря о немотивированности такого разложения пространства на прямую сумму.) Всякий раз, когда мы выполняем ортогональное измерение в $\mathcal{H}$, приготавливая в нем одно из множества взаимно ортогональных состояний, наш наблюдатель будет знать только о компоненте состояния, принадлежащей его пространству $\mathcal{H}_A$. Поскольку в $\mathcal{H}_A$ эти компоненты не обязательно ортогональны, он придет к выводу, что измерение готовит одно из множества неортогональных состояний.

Пусть $\{|i\rangle\}$ обозначает базис в $\mathcal{H}_A$, а $\{|\mu\rangle\}$ — базис в $\mathcal{H}_A^{\perp}$. Допустим, что начальная матрица плотности ρ_A имеет носитель в $\mathcal{H}_A$ и что мы выполняем ортогональное измерение в $\mathcal{H}$. Рассмотрим случай, когда каждый

оператор $\mathbf{E}_a$ является одномерным проектором, что, вообще говоря, достаточно для наших целей. Таким образом, $\mathbf{E}_a = |u_a\rangle\langle u_a|$, где $|u_a\rangle$ — нормированный вектор в $\mathcal{H}$. Этот вектор имеет единственное ортогональное разложение

$$|u_a\rangle = |\tilde{\psi}_a\rangle + |\tilde{\psi}_a^{\perp}\rangle, \tag{3.18}$$

где $|\tilde{\psi}_a\rangle$ и $|\tilde{\psi}_a^{\perp}\rangle$ — (ненормированные) векторы из $\mathcal{H}_A$ и $\mathcal{H}_A^{\perp}$ соответственно. После измерения новой матрицей плотности будет $|u_a\rangle\langle u_a|$ с вероятностью $\langle u_a|\boldsymbol{\rho}_A|u_a\rangle = \langle\tilde{\psi}_a|\boldsymbol{\rho}_A|\tilde{\psi}_a\rangle$ (поскольку $\boldsymbol{\rho}_A$ не имеет носителя в $\mathcal{H}_A^{\perp}$).

Но для нашего наблюдателя, не подозревающего о существовании $\mathcal{H}_A^{\perp}$, нет физической разницы между $|u_a\rangle$ и $|\tilde{\psi}_a\rangle$ (за исключением нормировки). Если записать $|\tilde{\psi}_a\rangle = \sqrt{\lambda_a}|\psi_a\rangle$, где $|\psi_a\rangle$ — нормированное состояние, тогда вдобавок к этому можно сказать, что для ограниченного пространством $\mathcal{H}_A$ наблюдателя с вероятностью $\langle\tilde{\psi}_a|\boldsymbol{\rho}_A|\tilde{\psi}_a\rangle$ результатом измерения является $|\psi_a\rangle\langle\psi_a|$.

Определим оператор

$$\mathbf{F}_a = \mathbf{E}_A\mathbf{E}_a\mathbf{E}_A = |\tilde{\psi}_a\rangle\langle\tilde{\psi}_a| = \lambda_a|\psi_a\rangle\langle\psi_a| \tag{3.19}$$

(где $\mathbf{E}_A$ — ортогональный проектор, проецирующий $\mathcal{H}$ на $\mathcal{H}_A$). Тогда мы можем сказать, что результат a имеет вероятность $\operatorname{tr}\mathbf{F}_a\boldsymbol{\rho}_A$. Очевидно, что каждый оператор $\mathbf{F}_a$ эрмитов и неотрицателен, но $\mathbf{F}_a$ не является проектором, за исключением случая, когда $\lambda_a = 1$. Более того

$$\sum_a \mathbf{F}_a = \mathbf{E}_A\left(\sum_a \mathbf{E}_a\right)\mathbf{E}_A = \mathbf{E}_A = \mathbf{1}_A; \tag{3.20}$$

сумма всех $\mathbf{F}_a$ равна единичному оператору в $\mathcal{H}_A$.

Разложение единицы на сумму неотрицательных операторов называется *положительной операторно-значной мерой* (ПОЗМ)[1]. (Термин мера несколько неуклюж в нашем конечномерном случае; он более уместен, когда индекс a может меняться непрерывным образом). В этом обсуждении мы пришли к частному случаю ПОЗМ, построенной из одномерных операторов (операторов с одним отличным от нуля собственным значением).

[1]Строгое определение ПОЗМ или, как ее чаще называют в русской литературе, разложения единицы в гильбертовом пространстве напоминает определение вероятностной меры (имеющей, однако, не числовые, а операторные значения). См. в книге: А. С. Холево. *Вероятностные и статистические аспекты квантовой теории*, Москва–Ижевск, ИКИ (2003). *Прим. ред.*]

В обобщенной теории измерений каждый результат имеет вероятность, которую можно представить в виде

$$\text{Prob}(a) = \text{tr}\,\boldsymbol{\rho}_A \mathbf{F}_a. \tag{3.21}$$

Положительность $\mathbf{F}_a$ и равенство $\sum_a \mathbf{F}_a = \mathbf{1}_A$ необходимы, чтобы обеспечить положительность вероятностей и равенство единице их суммы.

Как ПОЗМ общего вида влияет на квантовое состояние? Простого общего ответа на этот чрезвычайно важный вопрос нет, но в случае (только что обсуждавшемся) ПОЗМ, построенной из одномерных операторов, когда результат $|\psi_a\rangle\langle\psi_a|$ возникает с вероятностью $\text{tr}\,\boldsymbol{\rho}_A\mathbf{F}_a$, суммирование по всем исходам дает

$$\begin{aligned}\boldsymbol{\rho}_A \to \boldsymbol{\rho}'_A &= \sum_a |\psi_a\rangle\langle\psi_a|(\lambda_a\langle\psi_a|\boldsymbol{\rho}_A|\psi_a\rangle) \\ &= \sum_a \left(\sqrt{\lambda_a}|\psi_a\rangle\langle\psi_a|\right)\boldsymbol{\rho}_A\left(\sqrt{\lambda_a}|\psi_a\rangle\langle\psi_a|\right) \\ &= \sum_a \sqrt{\mathbf{F}_a}\boldsymbol{\rho}_A\sqrt{\mathbf{F}_a},\end{aligned} \tag{3.22}$$

[что обобщает неймановское $\sum_a \mathbf{E}_a\boldsymbol{\rho}\mathbf{E}_a$ (3.15) на случай, когда $\mathbf{F}_a$ не являются проекторами]. Заметим, что $\text{tr}\,\boldsymbol{\rho}_A = \text{tr}\,\boldsymbol{\rho}'_A = 1$, поскольку $\sum_a \mathbf{F}_a = \mathbf{1}_A$.

3.1.3. Однокубитовая ПОЗМ

В качестве примера рассмотрим один кубит и предположим, что $\{\hat{n}_a\}$ – N единичных трехмерных векторов, удовлетворяющих условию

$$\sum_a \lambda_a \hat{n}_a = 0, \tag{3.23}$$

где λ_a – положительные вещественные числа $0 < \lambda_a < 1$ такие, что $\sum_a \lambda_a = 1$. Пусть

$$\mathbf{F}_a = \lambda_a(\mathbf{1} + \hat{n}_a \cdot \vec{\boldsymbol{\sigma}}) = 2\lambda_a\mathbf{E}(\hat{n}_a) \tag{3.24}$$

[где $\mathbf{E}(\hat{n}_a)$ – проектор $|\uparrow_{\hat{n}_a}\rangle\langle\uparrow_{\hat{n}_a}|$]. Тогда

$$\sum_a \mathbf{F}_a = \left(\sum_a \lambda_a\right)\mathbf{1} + \left(\sum_a \lambda_a\hat{n}_a\right)\cdot\vec{\boldsymbol{\sigma}} = \mathbf{1}, \tag{3.25}$$

следовательно, $\mathbf{F}_a$ определяют ПОЗМ.

В случае $N = 2$ имеем $\hat{n}_1 + \hat{n}_2 = 0$,[1] следовательно, ПОЗМ является ортогональным измерением вдоль оси $\hat{n}_1$. При $N = 3$ в симметричном случае $\lambda_1 = \lambda_2 = \lambda_3 = \frac{1}{3}$ имеем $\hat{n}_1 + \hat{n}_2 + \hat{n}_3 = 0$ и

$$\mathbf{F}_a = \frac{1}{3}\left(\mathbf{1} + \hat{n}_a \cdot \vec{\sigma}\right) = \frac{2}{3}\mathbf{E}(\hat{n}_a). \tag{3.26}$$

3.1.4. Теорема Наймарка

Мы пришли к понятию ПОЗМ, рассматривая ортогональные измерения в более широком, чем $\mathcal{H}_A$, пространстве. Теперь обратим наши рассуждения и покажем, что таким образом может быть реализована любая ПОЗМ.

Рассмотрим произвольную ПОЗМ с n одномерными положительными операторами $\mathbf{F}_a$, удовлетворяющими условию $\sum_{a=1}^{n} \mathbf{F}_a = \mathbf{1}$. Покажем, что эту ПОЗМ всегда можно реализовать путем расширения гильбертова пространства и выполнения ортогонального измерения в этом более широком пространстве. Это утверждение называется *теоремой Наймарка* [2].

Чтобы доказать это, рассмотрим гильбертово пространство $\mathcal{U}$ с $\dim \mathcal{H} = N$ и ПОЗМ $\{\mathbf{F}_a\}$, $a = 1, 2, \ldots, n$ с $n \geqslant N$. Каждый одномерный положительный оператор может быть записан в виде

$$\mathbf{F}_a = |\tilde{\psi}_a\rangle\langle\tilde{\psi}_a|, \tag{3.27}$$

где вектор $|\tilde{\psi}_a\rangle$ не нормирован. Выписывая в явном виде матричные элементы равенства $\sum_{a=1} \mathbf{F}_a = \mathbf{1}$, получим:

$$\sum_{a=1}^{n} \left(\mathbf{F}_a\right)_{ij} = \sum_{a=1}^{n} \tilde{\psi}_{ai}^{*} \tilde{\psi}_{aj} = \delta_{ij}. \tag{3.28}$$

Теперь изменим точку зрения на уравнение (3.28). Будем интерпретировать $\left(\tilde{\psi}_a\right)_i$ не как $n \geqslant N$ векторов в N-мерном пространстве, а как $N \leqslant n$

[1] Конечно, это равенство справедливо лишь в симметричном случае $\lambda_1 = \lambda_2 = \frac{1}{2}$, который здесь по-видимому подразумевается. — *Прим. ред.*

[2] Обсуждение ПОЗМ и теоремы Наймарка можно найти в книге: A. Peres. *Quantum theory: Concepts and Methods*, Kluwer Academic Publishers, New York et al (2002) [На русском языке см.: Н.И. Ахиезер, И.М. Глазман, *Теория операторов в гильбертовом пространстве*, Наука, М.: (1966). — *Прим. ред.*]

векторов $\left(\tilde{\psi}_i^T\right)_a$ в n-мерном пространстве. Тогда уравнение (3.28) утверждает, что эти N векторов образуют ортогональный набор. Естественно, что он может быть расширен до ортогонального базиса в n-мерном пространстве. Другими словами, существует $n \times n$-матрица u_{ai} с $u_{ai} = \tilde{\psi}_{ai}$ при $a = 1, 2, \ldots, N$ такая, что

$$\sum_a u_{ai}^* u_{aj} = \delta_{ij}, \tag{3.29}$$

или, в матричной форме, $\mathbf{U}^\dagger\mathbf{U} = \mathbf{1}$. Отсюда следует, что $\mathbf{U}\mathbf{U}^\dagger = \mathbf{1}$, поскольку для любого вектора $|\psi\rangle$

$$\mathbf{U}(\mathbf{U}^\dagger\mathbf{U})|\psi\rangle = (\mathbf{U}\mathbf{U}^\dagger)\mathbf{U}|\psi\rangle = \mathbf{U}|\psi\rangle, \tag{3.30}$$

а областью действия $\mathbf{U}$ (по крайней мере для конечномерных матриц) является все n-мерное пространство. Возвращаясь к компонентной записи, имеем

$$\sum_j u_{aj} u_{bj}^* = \delta_{ab}. \tag{3.31}$$

Следовательно, $\left(u_a\right)_i$ образуют полный ортонормированный набор векторов[1].

Пусть теперь в пространстве размерности $n \geqslant N$ выполняется ортогональное измерение:

$$\mathbf{E}_a = |u_a\rangle\langle u_a|. \tag{3.32}$$

Мы построили векторы $|u_a\rangle$ так, чтобы каждый из них имел ортогональное разложение

$$|u_a\rangle = |\tilde{\psi}_a\rangle + |\tilde{\psi}_a^\perp\rangle, \tag{3.33}$$

где $|\tilde{\psi}_a\rangle \in \mathcal{H}$, а $|\tilde{\psi}_a^\perp\rangle \in \mathcal{H}^\perp$. Тогда ортогональным проецированием этого базиса на $\mathcal{H}$ мы воспроизводим ПОЗМ $\{\mathbf{F}_a\}$. Этим завершается доказательство теоремы Наймарка.

Чтобы проиллюстрировать теорему Наймарка в действии, рассмотрим еще раз однокубитовую ПОЗМ

$$\mathbf{F}_a = \frac{2}{3}|\uparrow_{\hat{n}_a}\rangle\langle\uparrow_{\hat{n}_a}|, \tag{3.34}$$

$a = 1, 2, 3$, где $\hat{n}_1 + \hat{n}_2 + \hat{n}_3 = 0$. Согласно теореме ПОЗМ может быть реализована как ортогональное измерение «кутрита» — квантовой системы в трехмерном гильбертовом пространстве.

[1] Другими словами, мы показали, что если строки $n \times n$-матрицы ортонормированы, то таковыми же будут их столбцы.

Пусть $\hat{n}_1 = (0,0,1)$, $\hat{n}_2 = (\sqrt{3}/2, 0, -1/2)$, $\hat{n}_3 = (-\sqrt{3}/2, 0, -1/2)$, тогда, вспоминая что

$$|\theta, \varphi = 0\rangle = \begin{pmatrix} \cos\dfrac{\theta}{2} \\ \sin\dfrac{\theta}{2} \end{pmatrix}, \tag{3.35}$$

мы можем записать три вектора $|\tilde{\psi}_a\rangle = \sqrt{2/3}|\theta, \varphi = 0\rangle$ (где $\theta_1, \theta_2, \theta_3 = 0, 2\pi/3, 4\pi/3$) как

$$|\tilde{\psi}_1\rangle, |\tilde{\psi}_2\rangle, |\tilde{\psi}_3\rangle = \begin{pmatrix} \sqrt{2/3} \\ 0 \end{pmatrix}, \begin{pmatrix} \sqrt{1/6} \\ \sqrt{1/2} \end{pmatrix}, \begin{pmatrix} -\sqrt{1/6} \\ \sqrt{1/2} \end{pmatrix}. \tag{3.36}$$

Теперь мы можем интерпретировать эти три двумерных вектора, как 2×3-матрицу, а теорема Наймарка гарантирует, что две ее строки ортонормированы. Следовательно, мы можем добавить еще одну ортонормированную строку:

$$|u_1\rangle, |u_2\rangle, |u_3\rangle = \begin{pmatrix} \sqrt{2/3} \\ 0 \\ \sqrt{1/3} \end{pmatrix}, \begin{pmatrix} \sqrt{1/6} \\ \sqrt{1/2} \\ -\sqrt{1/3} \end{pmatrix}, \begin{pmatrix} -\sqrt{1/6} \\ \sqrt{1/2} \\ \sqrt{1/3} \end{pmatrix}. \tag{3.37}$$

Мы видим, что (как и утверждает теорема) столбцы $|u_a\rangle$ также ортонормированы. Если мы выполним ортогональное измерение в базисе векторов $|u_a\rangle$, то живущий в двумерном подпространстве наблюдатель придет к выводу, что мы реализовали ПОЗМ $\{\mathbf{F}_1, \mathbf{F}_2, \mathbf{F}_3\}$. Мы показали, что если наш кубит фактически является двумя компонентами *кутрита*, то ПОЗМ может быть реализована как ортогональное измерение этого кутрита.

3.1.5. Ортогональное измерение на тензорном произведении

Тем не менее типичный кубит не скрывает никакого секрета. Чтобы выполнить обобщенное измерение, нам необходимо запастись дополнительными кубитами и выполнить совместные ортогональные измерения на нескольких кубитах сразу.

Рассмотрим случай двух (изолированных) систем A и B, описываемых тензорным произведением $\mathcal{H}_A \otimes \mathcal{H}_B$. Предположим, что на этом тензорном произведении мы выполняем ортогональное измерение, характеризуемое полным набором взаимно ортогональных проекторов $\mathbf{E}_a$:

$$\sum_a \mathbf{E}_a = \mathbf{1}. \tag{3.38}$$

Представим, что начальным состоянием квантовой системы является «некоррелированное» тензорное произведение состояний

$$\rho_{AB} = \rho_A \otimes \rho_B. \tag{3.39}$$

Тогда с вероятностью

$$\mathrm{Prob}(a) = \mathrm{tr}_{AB}\left[\mathbf{E}_a(\rho_A \otimes \rho_B)\right] \tag{3.40}$$

результатом измерения будет a. В этом случае новая матрица плотности будет равна[1]

$$\rho'_{AB} = \frac{\mathbf{E}_a(\rho_A \otimes \rho_B)\mathbf{E}_a}{\mathrm{tr}_{AB}\left[\mathbf{E}_a(\rho_A \otimes \rho_B)\right]}. \tag{3.41}$$

Для наблюдателя, имеющего доступ только к системе A, ее новую матрицу плотности дает частичный след только что записанной матрицы плотности, или

$$\rho'_A = \frac{\mathrm{tr}_B\left[\mathbf{E}_a(\rho_A \otimes \rho_B)\mathbf{E}_a\right]}{\mathrm{tr}_{AB}\left[\mathbf{E}_a(\rho_A \otimes \rho_B)\right]}. \tag{3.42}$$

Выражение (3.40) для вероятности результата a также может быть записано в виде

$$\mathrm{Prob}(a) = \mathrm{tr}_A\left[\mathrm{tr}_B\left(\mathbf{E}_a(\rho_A \otimes \rho_B)\right)\right] = \mathrm{tr}_A\left(\mathbf{F}_a\rho_A\right); \tag{3.43}$$

если ввести ортогональные базисы $\{|i\rangle_A\}$ в $\mathcal{H}_A$, а $\{|\mu\rangle_B\}$ в $\mathcal{H}_B$, то

$$\sum_{ij\mu\nu}(\mathbf{E}_a)_{j\nu,i\mu}(\rho_A)_{ij}(\rho_B)_{\mu\nu} = \sum_{ij}(\mathbf{F}_a)_{ji}(\rho_A)_{ij} \tag{3.44}$$

или

$$(\mathbf{F}_a)_{ji} = \sum_{\mu\nu}(\mathbf{E}_a)_{j\nu,i\mu}(\rho_B)_{\mu\nu}. \tag{3.45}$$

Из уравнения (3.45) следует, что каждый оператор обладает $\mathbf{F}_a$ свойствами:

(1) Эрмитовость:

$$(\mathbf{F}_a)^*_{ij} = \sum_{\mu\nu}(\mathbf{E}_a)^*_{i\nu,j\mu}(\rho_B)^*_{\mu\nu} = \sum_{\mu\nu}(\mathbf{E}_a)_{j\mu,i\nu}(\rho_B)_{\nu\mu} = (\mathbf{F}_a)_{ji},$$

поскольку эрмитовы $\mathbf{E}_a$ и ρ_B.

[1] Такой вид матрица плотности будет иметь после измерения, результат которого *зафиксирован* и имеет значение a. Если же результат не был «записан», то при таком измерении матрица плотности эволюционирует в соответствии с уравнением (3.15). — *Прим. ред.*

(2) Положительность: В базисе, диагонализующем $\boldsymbol{\rho}_B = \sum_\mu p_\mu |\mu\rangle_{B\ B}\langle\mu|$,

$$ {}_A\langle\psi|\mathbf{F}_a|\psi\rangle_A = \sum_\mu p_\mu \big({}_A\langle\psi| \otimes {}_B\langle\mu|\big)\mathbf{E}_a\big(|\psi\rangle_A \otimes |\mu\rangle_B\big) \geqslant 0, $$

поскольку положителен $\mathbf{E}_a$.

(3) Полнота:

$$ \sum_a \mathbf{F}_a = \sum_\mu p_\mu \left\langle \mu \middle| \sum_a \mathbf{E}_a \middle| \mu \right\rangle_B = \mathbf{1}_A, $$

поскольку $\sum_a \mathbf{E}_a = \mathbf{1}_{AB}$, а $\operatorname{tr}\boldsymbol{\rho}_B = 1$.

Однако операторы $\mathbf{F}_a$ не обязательно взаимно ортогональны. Фактически количество $\mathbf{F}_a$ ограничено только размерностью $\mathcal{H}_A \otimes \mathcal{H}_B$, большей (и, возможно, гораздо большей) чем размерность $\mathcal{H}_A$.

В общем случае нет простого способа выразить конечную матрицу плотности $\boldsymbol{\rho}'_A$ через $\boldsymbol{\rho}_A$ и $\mathbf{F}_a$. Не будем, однако, обращать внимание на то, как ПОЗМ изменяет матрицу плотности, а вместо этого зададимся вопросом. Допустим, что $\mathcal{H}_A$ имеет размерность N, и рассмотрим ПОЗМ, состоящую из n одномерных неотрицательных операторов $\mathbf{F}_a$, удовлетворяющих условию $\sum_{a=1}^{n} \mathbf{F}_a = \mathbf{1}_A$. Можем ли мы выбрать пространство $\mathcal{H}_B$, матрицу плотности $\boldsymbol{\rho}_B$ в $\mathcal{H}_B$ и проекционные операторы $\mathbf{E}_a$ в $\mathcal{H}_A \otimes \mathcal{H}_B$ (где количество $\mathbf{E}_a$ может превосходить количество $\mathbf{F}_a$) такие, чтобы вероятность результата a ортогонального измерения удовлетворяла условию[1]

$$ \operatorname{tr}\mathbf{E}_a(\boldsymbol{\rho}_A \otimes \boldsymbol{\rho}_B) = \operatorname{tr}\left(\mathbf{F}_a\boldsymbol{\rho}_A\right)? \tag{3.46} $$

(Неважно, как ортогональная проекция модифицирует $\boldsymbol{\rho}_A$!). Мы будем считать это «реализацией» ПОЗМ с помощью ортогонального измерения, поскольку нас не интересует, какова $\boldsymbol{\rho}'_A$ для каждого результата измерения; мы только требуем, чтобы *вероятности* результатов согласовались с определенной таким образом ПОЗМ.

Такая реализация ПОЗМ действительно возможна; чтобы показать это, еще раз обратимся к теореме Наймарка. Каждый одномерный оператор $\mathbf{F}_a$,

[1] Если количество $\mathbf{E}_a$ больше, чем $\mathbf{F}_a$, то почти все n результатов имеют вероятность, *равную нулю*.

$a = 1, 2, \ldots, n$, может быть представлен в виде $\mathbf{F}_a = |\tilde{\psi}_a\rangle\langle\tilde{\psi}_a|$. Согласно Наймарку существуют n ортонормированных n-компонентных векторов $|u_a\rangle$ таких, что

$$|u_a\rangle = |\tilde{\psi}_a\rangle + |\tilde{\psi}_a^{\perp}\rangle. \tag{3.47}$$

Начнем с того, что рассмотрим частный случай $n = rN$, где r – положительное целое число. Тогда удобно разложить $|\tilde{\psi}_a^{\perp}\rangle$ на прямую сумму N-компонентных векторов

$$|\tilde{\psi}_a^{\perp}\rangle = |\tilde{\psi}_{1,a}^{\perp}\rangle \oplus |\tilde{\psi}_{2,a}^{\perp}\rangle \oplus \cdots \oplus |\tilde{\psi}_{r-1,a}^{\perp}\rangle. \tag{3.48}$$

Здесь $|\tilde{\psi}_{1,a}^{\perp}\rangle$ обозначает первые N компонент вектора $|\tilde{\psi}_a^{\perp}\rangle$, $|\tilde{\psi}_{2,a}^{\perp}\rangle$ обозначает следующие N компонент и так далее. Тогда ортонормированность векторов $|u_a\rangle$ означает, что

$$\delta_{ab} = \langle u_a|u_b\rangle = \langle\tilde{\psi}_a|\tilde{\psi}_b\rangle + \sum_{\mu=1}^{r-1}\langle\tilde{\psi}_{\mu,a}^{\perp}|\tilde{\psi}_{\mu,b}^{\perp}\rangle. \tag{3.49}$$

Выберем теперь $\mathcal{H}_B$ имеющим размерность r и обозначим ортонормированный базис в $\mathcal{H}_B$:

$$\{|\mu\rangle_B\}, \qquad \mu = 0, 1, 2, \ldots, r-1. \tag{3.50}$$

Тогда из уравнения (3.49) следует, что

$$|\Phi_a\rangle_{AB} = |\tilde{\psi}_a\rangle_A|0\rangle_B + \sum_{\mu=1}^{r-1}|\tilde{\psi}_{\mu,a}^{\perp}\rangle_A|\mu\rangle_B, \qquad a = 1, 2, \ldots, n, \tag{3.51}$$

– ортонормированный базис в $\mathcal{H}_A \otimes \mathcal{H}_B$.

Предположим теперь, что состоянием в $\mathcal{H}_A \otimes \mathcal{H}_B$ является

$$\boldsymbol{\rho}_{AB} = \boldsymbol{\rho}_A \otimes |0\rangle_{B\,B}\langle 0|, \tag{3.52}$$

и мы выполняем ортогональное проецирование на базис $\{|\Phi_a\rangle_{AB}\}$ в $\mathcal{H}_A \otimes \mathcal{H}_B$. Тогда, поскольку при $\mu \neq 0$ ${}_B\langle 0|\mu\rangle_B = 0$, результат $|\Phi_a\rangle_{AB}$ появляется с вероятностью

$${}_{AB}\langle\Phi_a|\boldsymbol{\rho}_{AB}|\Phi_a\rangle_{AB} = {}_A\langle\tilde{\psi}_a|\boldsymbol{\rho}_A|\tilde{\psi}_a\rangle_A \tag{3.53}$$

и, следовательно,

$${}_{AB}\langle\Phi_a|\boldsymbol{\rho}_{AB}|\Phi_a\rangle_{AB} = \mathrm{tr}\,(\mathbf{F}_a\boldsymbol{\rho}_A). \tag{3.54}$$

Мы действительно успешно «реализовали» ПОЗМ, выполняя ортогональное измерение в $\mathcal{H}_A \otimes \mathcal{H}_B$. Эта конструкция так же эффективна, как и описанная выше конструкция «прямой суммы»; мы выполнили ортогональное измерение в пространстве размерности $n = rN$.

Если появился результат a, тогда с помощью измерения приготовлено состояние

$$\rho'_{AB} = |\Phi_a\rangle_{AB\,AB}\langle\Phi_a|. \tag{3.55}$$

Матрица плотности, видимая наблюдателю, которому доступна только система A, получается взятием частичного следа по $\mathcal{H}_B$:

$$\begin{aligned}\rho'_A &= \mathrm{tr}_B\left(|\Phi_a\rangle_{AB\,AB}\langle\Phi_a|\right) = \\ &= |\tilde{\psi}_a\rangle_{A\,A}\langle\tilde{\psi}_a| + \sum_{\mu=1}^{r-1} |\tilde{\psi}^{\perp}_{\mu,a}\rangle_{A\,A}\langle\tilde{\psi}^{\perp}_{\mu,a}|,\end{aligned} \tag{3.56}$$

что не совсем то же самое, что было получено в нашей конструкции «прямой суммы». Во всяком случае существует множество способов реализовать ПОЗМ с помощью ортогональных измерений, и уравнение (3.56) применимо только к выбранной здесь частной конструкции.

Тем не менее в действительности эта конструкция идеально подходит для реализации ПОЗМ, в которой состояние $|\psi_a\rangle_{A\,A}\langle\psi_a|$ приготавливается в результате появления исхода a. Трудным моментом осуществления ПОЗМ является обеспечение того, что результат a появляется с требуемой вероятностью. После этого уже легко прийти к соглашению о том, что *следствием* появления результата a является состояние $|\psi_a\rangle_{A\,A}\langle\psi_a|$; если угодно, сразу как только измерение выполнено и результат a получен, мы можем просто отбросить ρ_A и приступить к приготовлению требуемого состояния! Фактически, в случае проекции на базис $|\Phi_a\rangle_{AB}$ мы можем полностью построить ПОЗМ, проецируя систему B на базис $\{|\mu\rangle_B\}$ и сообщая результат в систему A. Если результатом является $|0\rangle_B$, тогда не нужно предпринимать никаких действий. Если же результатом является $|\mu\rangle_B$, $\mu > 0$, тогда было приготовлено состояние $|\tilde{\psi}^{\perp}_{\mu,a}\rangle_A$, которое затем может быть преобразовано в $|\psi_a\rangle_A$.

До сих пор мы обсуждали частный случай $n = r \cdot N$. Если в действительности $n = r \cdot N - c$, $0 < c < N$, то нам нужно лишь выбрать равными нулю последние c компонент вектора $|\tilde{\psi}^{\perp}_{r-1,a}\rangle_A$ и состояния $|\Phi\rangle_{AB}$ по-прежнему будут взаимно ортогональными. Чтобы получить полный базис, мы можем добавить c состояний:

$$|e_i\rangle_A|r-1\rangle_B, \qquad i = rN - c + 1, rN - c + 2, \ldots, rN; \tag{3.57}$$

здесь $|e_i\rangle_A$ — вектор, у которого отлична от нуля только одна i-ая компонента, так что $|e_i\rangle_A$ гарантированно ортогонален вектору $|\tilde{\psi}^{\perp}_{r-1,a}\rangle_A$. В этом случае ПОЗМ реализуется как ортогональное измерение в пространстве размерности $rN = n + c$.

В качестве примера конструкции тензорного произведения мы вновь можем рассмотреть однокубитовую ПОЗМ с

$$\mathbf{F}_a = \frac{2}{3}|\uparrow_{\hat{n}_a}\rangle_A\,{}_A\langle\uparrow_{\hat{n}_a}|, \qquad a = 1,2,3. \tag{3.58}$$

Мы можем реализовать эту ПОЗМ, вводя второй кубит B. В двухкубитовом гильбертовом пространстве мы можем проецировать на ортонормированный базис [1]

$$\begin{aligned} |\Phi_a\rangle &= \sqrt{\frac{2}{3}}|\uparrow_{\hat{n}_a}\rangle_A|0\rangle_B + \sqrt{\frac{1}{3}}|0\rangle_A|1\rangle_B, \quad a = 1,2,3, \\ |\Phi_0\rangle &= |1\rangle_A|1\rangle_B. \end{aligned} \tag{3.59}$$

Если начальным состоянием является $\boldsymbol{\rho}_{AB} = \boldsymbol{\rho}_A \otimes |0\rangle_B\,{}_B\langle 0|$, то мы имеем

$$\langle\Phi_a|\boldsymbol{\rho}_{AB}|\Phi_a\rangle = \frac{2}{3}\,{}_A\langle\uparrow_{\hat{n}_a}|\boldsymbol{\rho}_A|\uparrow_{\hat{n}_a}\rangle_A, \tag{3.60}$$

следовательно, эта проекция осуществляет ПОЗМ в $\mathcal{H}_A$. (Здесь мы выполнили ортогональные измерения в четырехмерном пространстве; в предыдущей конструкции «прямой суммы» мы нуждались только в трех измерениях).

3.1.6. ЖХЙВ с ПОЗМ

Обсуждая теорему ЖХЙВ, мы говорили, что, приготовив состояние

$$|\Phi_a\rangle_{AB} = \sum_{\mu} \sqrt{q_\mu}|\psi_\mu\rangle_A|\beta_\mu\rangle_B, \tag{3.61}$$

[1] Здесь фаза $|\tilde{\psi}_2\rangle = \sqrt{2/3}|\uparrow_{\hat{n}_a}\rangle_A$ отличается на -1 от соответствующей фазы в уравнении (3.36); она выбрана таким образом, чтобы ${}_A\langle\uparrow_{\hat{n}_a}|\uparrow_{\hat{n}_b}\rangle_A = -1/2$ при $a \neq b$. Мы сделали этот выбор затем, чтобы коэффициент перед $|0\rangle_A|1\rangle_B$ был положителен во всех трех $|\Phi_1\rangle$, $|\Phi_2\rangle$, $|\Phi_3\rangle$.

мы можем реализовать ансамбль

$$\boldsymbol{\rho}_A = \sum_\mu q_\mu |\psi_\mu\rangle_{A\,A}\langle\psi_\mu|, \tag{3.62}$$

выполняя ортогональные измерения в $\mathcal{H}_B$. Более того, если $\dim \mathcal{H}_B = n$, то, измеряя подходящие наблюдаемые в $\mathcal{H}_B$, мы можем с этим одним чистым состоянием $|\Phi_a\rangle_{AB}$ реализовать любое приготовление $\boldsymbol{\rho}_A$ как ансамбля, содержащего вплоть до n чистых состояний.

Теперь можно видеть, что если мы готовы допустить в $\mathcal{H}_B$ ПОЗМы, а не только ортогональные измерения, то даже при $\dim \mathcal{H}_B = N$ можно реализовать любое приготовление $\boldsymbol{\rho}_A$ с помощью подходящего выбора ПОЗМ в $\mathcal{H}_B$. Суть в том, что $\boldsymbol{\rho}_B$ имеет носитель в пространстве размерности самое большее N. Следовательно, можно переписать

$$|\Phi_a\rangle_{AB} = \sum_\mu \sqrt{q_\mu}|\psi_\mu\rangle_A|\tilde{\beta}_\mu\rangle_B, \tag{3.63}$$

где $|\tilde{\beta}_\mu\rangle_B$ — ортогональная проекция вектора $|\beta_\mu\rangle_B$ на носитель матрицы плотности $\boldsymbol{\rho}_B$. Мы можем выполнить ПОЗМ на носителе $\boldsymbol{\rho}_B$ с $\mathbf{F}_a = |\tilde{\beta}_\mu\rangle_{B\,B}\langle\tilde{\beta}_\mu|$ и таким образом приготовить состояние $|\psi_\mu\rangle_A$ с вероятностью q_μ.

3.2. Супероператоры

3.2.1. Представление операторной суммы

Перейдем к следующему этапу нашей программы понимания поведения части бинарной системы. Мы видели, что чистое состояние бинарной системы может вести себя подобно смешанному состоянию, когда мы наблюдаем только одну ее подсистему A, а ортогональное измерение бинарной системы внутри ее подсистемы A может быть (неортогональной) ПОЗМ. Зададимся вопросом: если состояние бинарной системы совершает унитарную эволюцию, то как тогда описать эволюцию одной только ее подсистемы A?

Пусть начальная матрица плотности бинарной системы представляет собой тензорное произведение состояний вида

$$\boldsymbol{\rho}_A \otimes |0\rangle_{B\,B}\langle 0|; \tag{3.64}$$

система A имеет матрицу плотности $\boldsymbol{\rho}_A$, а система B предполагается находящейся в чистом состоянии, которое мы обозначили $|0\rangle_B$. Бинарная система эволюционирует в течение конечного промежутка времени, управляемая унитарным оператором эволюции

$$\mathbf{U}_{AB}(\boldsymbol{\rho}_A \otimes |0\rangle_{B\,B}\langle 0|)\mathbf{U}_{AB}. \tag{3.65}$$

Выполним вычисление частичного следа в $\mathcal{H}_B$, чтобы найти конечную матрицу плотности системы A:

$$\begin{aligned}\boldsymbol{\rho}'_A &= \mathrm{tr}_B\left(\mathbf{U}_{AB}(\boldsymbol{\rho}_A \otimes |0\rangle_{B\,B}\langle 0|)\mathbf{U}^\dagger_{AB}\right)\\ &= \sum_\mu {}_B\langle\mu|\mathbf{U}_{AB}|0\rangle_B\,\boldsymbol{\rho}_A\,{}_B\langle 0|\mathbf{U}^\dagger_{AB}|\mu\rangle_B,\end{aligned} \tag{3.66}$$

где $\{|\mu\rangle_B\}$ — ортонормированный базис в $\mathcal{H}_B$, а ${}_B\langle\mu|\mathbf{U}_{AB}|0\rangle_B$ — оператор, действующий в $\mathcal{H}_A$. [Если $\{|i\rangle_A \otimes |\mu\rangle_B\}$ — ортонормированный базис в $\mathcal{H}_A \otimes \mathcal{H}_B$, то ${}_B\langle\mu|\mathbf{U}_{AB}|\nu\rangle_B$ обозначает оператор, матричные элементы которого равны

$${}_A\langle i|{}_B\langle\mu|\mathbf{U}_{AB}|\nu\rangle_B|j\rangle_A = ({}_A\langle i| \otimes {}_B\langle\mu|)\mathbf{U}_{AB}(|\nu\rangle_B \otimes |j\rangle_A).] \tag{3.67}$$

Если обозначить

$$\mathbf{M}_\mu = {}_B\langle\mu|\mathbf{U}_{AB}|0\rangle_B, \tag{3.68}$$

то $\boldsymbol{\rho}'_A$ можно представить в виде

$$\$(\boldsymbol{\rho}_A) \equiv \boldsymbol{\rho}'_A = \sum_\mu \mathbf{M}_\mu \boldsymbol{\rho}_A \mathbf{M}^\dagger_\mu. \tag{3.69}$$

Из унитарности $\mathbf{U}_{AB}$ следует, что $\mathbf{M}_\mu$ обладает свойством

$$\begin{aligned}\sum_\mu \mathbf{M}^\dagger_\mu \mathbf{M}_\mu &= \sum_\mu {}_B\langle 0|\mathbf{U}^\dagger_{AB}|\mu\rangle_{B\,B}\langle\mu|\mathbf{U}_{AB}|0\rangle_B =\\ &= {}_B\langle 0|\mathbf{U}^\dagger_{AB}\mathbf{U}_{AB}|0\rangle_B = \mathbf{1}_A.\end{aligned} \tag{3.70}$$

Уравнение (3.69) определяет линейное отображение $\$$, преобразующее один линейный оператор в другой. Если выполняется свойство (3.70), то такое отображение называется *супероператором*, а уравнение (3.69) назы-

вается представлением супероператора операторной суммой (или представлением *Крауса*). Супероператор можно рассматривать как линейное отображение, преобразующее операторы плотности в операторы плотности, поскольку из (3.69) и (3.70) следует, что $\boldsymbol{\rho}'_A$ — оператор плотности, если им является $\boldsymbol{\rho}_A$:

(1) $\boldsymbol{\rho}'_A$ эрмитов: $\boldsymbol{\rho}'^{\dagger}_A = \sum_\mu \mathbf{M}_\mu \boldsymbol{\rho}^\dagger_A \mathbf{M}^\dagger_\mu = \sum_\mu \mathbf{M}_\mu \boldsymbol{\rho}_A \mathbf{M}^\dagger_\mu = \boldsymbol{\rho}'_A$.

(2) $\boldsymbol{\rho}'_A$ имеет единичный след: $\operatorname{tr} \boldsymbol{\rho}'_A = \sum_\mu \operatorname{tr}\left(\boldsymbol{\rho}_A \mathbf{M}^\dagger_\mu \mathbf{M}_\mu\right) = \operatorname{tr} \boldsymbol{\rho}_A = 1$.

(3) $\boldsymbol{\rho}'_A$ положительно определен:

$$ {}_A\langle\psi|\boldsymbol{\rho}'_A|\psi\rangle_A = \sum_\mu \left({}_A\langle\psi|\mathbf{M}_\mu\right)\boldsymbol{\rho}_A\left(\mathbf{M}^\dagger_\mu|\psi\rangle_A\right) \geqslant 0. $$

Мы показали, что представление операторной суммы (3.69) следует из «унитарного представления» (3.66). Более того, по данному представлению супероператора в виде операторной суммы всегда можно построить соответствующее унитарное представление. Выберем в качестве $\mathcal{H}_B$ гильбертово пространство, размерность которого, по крайней мере, больше числа слагаемых в операторной сумме. Если $|\varphi\rangle_A$ — произвольный вектор в $\mathcal{H}_A$, $\{|\mu\rangle_B\}$ — ортонормированный базис в $\mathcal{H}_B$, а $|0\rangle_B$ — некоторое нормированное состояние в $\mathcal{H}_B$, то определим действие $\mathbf{U}_{AB}$ соотношением

$$ \mathbf{U}_{AB}\left(|\varphi\rangle_A \otimes |0\rangle_B\right) = \sum_\mu \mathbf{M}_\mu |\varphi\rangle_A \otimes |\mu\rangle_B. \tag{3.71} $$

Это действие сохраняет внутреннее произведение

$$ \left(\sum_\nu {}_A\langle\varphi_2|\mathbf{M}^\dagger_\nu \otimes {}_B\langle\nu|\right)\left(\sum_\mu \mathbf{M}_\mu|\varphi_1\rangle_A \otimes |\mu\rangle_B\right) = $$

$$ = {}_A\left\langle \varphi_2 \left| \sum_\mu \mathbf{M}^\dagger_\mu \mathbf{M}_\mu \right| \varphi_1 \right\rangle_A = \langle\varphi_2|\varphi_1\rangle_A, \tag{3.72} $$

следовательно, $\mathbf{U}_{AB}$ может быть расширен до унитарного оператора, действующего на всем $\mathcal{H}_A \otimes \mathcal{H}_B$. Взяв частичный след, мы найдем

$$ \operatorname{tr}_B\left(\mathbf{U}_{AB}\left(|\varphi\rangle_A \otimes |0\rangle_B\right)\left({}_A\langle\varphi| \otimes {}_B\langle 0|\right)\mathbf{U}^\dagger_{AB}\right) = \sum_\mu \mathbf{M}_\mu \left(|\varphi\rangle_A\, {}_A\langle\varphi|\right)\mathbf{M}^\dagger_\mu. \tag{3.73} $$

Поскольку любая матрица плотности ρ_A может быть представлена как ансамбль чистых состояний, мы воспроизводим представление операторной суммы, действующей на произвольную ρ_A.

Очевидно, что представление операторной суммы данного супероператора \$ не единственно. Мы можем вычислить частичный след в любом базисе, в каком пожелаем. Если мы используем базис $\left\{ {}_B\langle\nu| = \sum_\mu \mathbf{U}_{\nu\mu}\, {}_B\langle\mu| \right\}$, то получим представление

$$\$(\rho_A) = \sum_\nu \mathbf{N}_\nu \rho_A \mathbf{N}_\nu^\dagger, \tag{3.74}$$

где $\mathbf{N}_\nu = \mathbf{U}_{\nu\mu}\mathbf{M}_\mu$. Вскоре мы увидим, что так связаны *любые* два представления операторных сумм одного супероператора.

Супероператоры важны, поскольку они обеспечивают нас формализмом для обсуждения общей теории *декогерентизации*, эволюции чистых состояний в смешанные. *Унитарная* эволюция ρ_A является частным случаем, когда в операторной сумме имеется только одно слагаемое. Если в ней присутствуют два или более слагаемых, тогда в ходе эволюции, управляемой оператором $\mathbf{U}_{AB}$, чистые начальные состояния из $\mathcal{H}_A$ *запутываются* с $\mathcal{H}_B$. То есть если возникающие в операторной сумме операторы $\mathbf{M}_1$ и $\mathbf{M}_2$ линейно независимы, то существует такой вектор $|\varphi\rangle_A$, что векторы $|\tilde{\varphi}_1\rangle_A = \mathbf{M}_1|\varphi\rangle_A$ и $|\tilde{\varphi}_2\rangle_A = \mathbf{M}_2|\varphi\rangle_A$ линейно независимы, следовательно, состояние $|\tilde{\varphi}_1\rangle_A|1\rangle_B + |\tilde{\varphi}_2\rangle_A|2\rangle_B + \cdots$ имеет число Шмидта больше единицы. Следовательно, чистое состояние $|\varphi\rangle_A\,{}_A\langle\varphi|$ эволюционирует к смешанному *конечному* состоянию ρ'_A.

Из двух супероператоров $\$_1$ и $\$_2$ можно построить композицию, представляющую собой другой супероператор $\$_1 \circ \$_2$; если $\$_1$ описывает эволюцию от вчерашнего дня до сегодняшнего, а $\$_2$ — от сегодняшнего дня до завтрашнего, то $\$_1 \circ \$_2$ описывает эволюцию от вчерашнего дня до завтрашнего. Но является ли обратный супероператор также супероператором? То есть существует ли супероператор, описывающий эволюцию из сегодняшнего дня во вчерашний? Вы покажете в домашнем упражнении, что на самом деле супероператор обратим только тогда, когда он унитарен.

Операторы унитарной эволюции образуют группу, а супероператоры определяют динамическую *полугруппу*. Когда возникает декогерентизация, существует стрела времени; даже на микроскопическом уровне можно говорить о различии между движением вперед и назад во времени. Декогерентизация вызывает неизбежную потерю квантовой информации – однажды вынув (мертвого) кота из ящика, мы не можем вернуть его в исходное состояние.

3.2.2. Линейность

Теперь посмотрим на эту проблему немного шире и обсудим основные свойства, которым должен удовлетворять любой «разумный» закон эволюции матрицы плотности. Мы увидим, что любой такой закон допускает представление операторной суммы, то есть, в известном смысле, выделенное нами динамическое поведение рассматриваемой части бинарной системы действительно является наиболее общим.

Отображение $\$: \rho \to \rho'$, преобразующее исходную матрицу плотности ρ в конечную ρ', представляет собой отображение операторов в операторы, обладающее следующими свойствами:

(1) $\$$ *сохраняет эрмитовость*: ρ' эрмитова, если таковой является ρ.

(2) $\$$ *сохраняет след*: $\operatorname{tr}\rho' = 1$, если $\operatorname{tr}\rho = 1$.

(3) $\$$ *положителен*: ρ' неотрицательна, если таковой является ρ.

Обычно также предполагают, что

(0) $\$$ *линейный оператор*.

В то время как условия (1), (2) и (3) действительно необходимы для того, чтобы ρ' оставалась матрицей плотности, (0) остается открытым вопросом. Почему линейность?

Возможный ответ состоит в том, что нелинейную эволюцию матрицы плотности было бы сложно согласовать с любой интерпретацией ансамбля. Если

$$\$\big[\rho(\lambda)\big] = \$\big[\lambda\rho_1 + (1-\lambda)\rho_2\big] = \lambda\$[\rho_1] + (1-\lambda)\$[\rho_2], \tag{3.75}$$

тогда временная эволюция согласуется с вероятностной интерпретацией $\rho(\lambda)$: или (с вероятностью λ) было приготовлено начальное состояние ρ_1, которое эволюционировало в состояние $\$[\rho_1]$, или (с вероятностью $1-\lambda$) было приготовлено начальное состояние ρ_2, которое эволюционировало в состояние $\$[\rho_2]$. Нелинейный супероператор $\$$, по-видимому, ведет к парадоксальным следствиям.

В качестве примера рассмотрим один кубит, эволюционирующий согласно

$$\$(\rho) = \exp\big[i\pi\sigma_1 \operatorname{tr}(\sigma_1\rho)\big]\rho\exp\big[-i\pi\sigma_1\operatorname{tr}(\sigma_1\rho)\big]. \tag{3.76}$$

Нетрудно проверить, что $ — положительный и сохраняющий след оператор. Предположим, что начальной матрицей плотности является $\rho = \frac{1}{2}\mathbf{1}$, реализованная как ансамбль

$$\rho = \frac{1}{2}|\uparrow_z\rangle\langle\uparrow_z| + \frac{1}{2}|\downarrow_z\rangle\langle\downarrow_z|. \tag{3.77}$$

Поскольку $\mathrm{tr}(\sigma_1\rho) = 0$, эволюция ρ тривиальна и оба представителя ансамбля остаются неизменными. Если спин был приготовлен в состоянии $|\uparrow_z\rangle$, то в нем он и останется.

Теперь представим, что непосредственно после приготовления ансамбля мы ничего не делаем, если было приготовлено состояние $|\uparrow_z\rangle$, но если оказалось, что приготовлено $|\downarrow_z\rangle$, мы поворачиваем его в состояние $|\uparrow_x\rangle$. Теперь матрица плотности равна

$$\rho' = \frac{1}{2}|\uparrow_z\rangle\langle\uparrow_z| + \frac{1}{2}|\uparrow_x\rangle\langle\uparrow_x|, \tag{3.78}$$

так что $\mathrm{tr}(\sigma_1\rho') = \frac{1}{2}$. В результате эволюции, управляемой оператором $, она преобразуется в $\$(\rho') = \sigma_1\rho\sigma_1$. Тогда если спин был приготовлен в состоянии $|\uparrow_z\rangle$, то он эволюционирует в ортогональное состояние $|\downarrow_z\rangle$.

Следуя этим двум сценариям, первоначально приготовленное состояние $|\uparrow_z\rangle$ эволюционирует различным образом. Но в чем разница между этими двумя случаями? Разница в том, что *если* приготовлено начальное состояние спина $|\downarrow_z\rangle$, то мы совершаем различные действия: ничего не делаем в случае (1), но поворачиваем спин в случае (2). Тем не менее, мы обнаружили, что в этих двух случаях спин ведет себя по-разному, даже если первоначально было приготовлено состояние $|\uparrow_z\rangle$!

Мы привыкли говорить, что ρ описывает две (или более) различные альтернативы приготовления чистого состояния, только одна из которых действительно реализуется всякий раз, когда мы готовим кубит. Но мы обнаружили, что если мы готовим $|\uparrow_z\rangle$, то происходящее действительно *зависит от того, что мы были бы должны сделать*, если бы вместо этого было приготовлено $|\downarrow_z\rangle$. По-видимому, становится неразумно рассматривать два возможных приготовления как взаимно исключающие альтернативы. Эволюция альтернатив действительно зависит от других альтернатив, которые предположительно не были реализованы. Джо Полчински назвал это явление «телефоном Эверетта», поскольку различные «ветви волновой функции» выглядят способными «общаться» между собой.

Тогда нелинейная эволюция матрицы плотности имела бы странные, возможно, даже абсурдные следствия. И все-таки это не факт, что нели-

нейная эволюция должна быть исключена. Действительно, Джим Хартл доказывал, что существуют варианты «обобщенных квантовых механик», в которых допустима нелинейная эволюция, но тем не менее можно сохранить последовательную вероятностную интерпретацию. Несмотря на это, здесь мы будем следовать традиции и требовать, чтобы $ был линейным оператором.

3.2.3. Полная положительность

Было бы приятно прийти к выводу, что любой $, удовлетворяющий условиям (0)–(3), имеет представление операторной суммы и, следовательно, может быть реализован унитарной эволюцией подходящей бинарной системы. К сожалению, это не всегда возможно. И все же, к счастью, оказывается, что, добавив одно достаточно безобидно звучащее предположение, можно показать, что $ имеет представление операторной суммы.

Необходимым нам дополнительным предположением [в действительности более сильной версией (3)] является:

(3′) $ *вполне положителен.*

Полная положительность определяется следующим образом. Рассмотрим любое возможное расширение $\mathcal{H}_A$ до тензорного произведения $\mathcal{H}_A \otimes \mathcal{H}_B$; тогда $ вполне положителен в $\mathcal{H}_A$, если $\$_A \otimes \mathbf{1}_B$ является положительным для любого такого расширения.

Полная положительность, несомненно, является разумным свойством, чтобы нуждаться в физических основаниях. Если мы изучаем эволюцию системы A, то никогда нельзя быть уверенным в том, что нет взаимодействующей с ней системы B, о существовании которой мы не подозреваем. Полная положительность (в комбинации с другими предположениями) утверждает лишь то, что если система A эволюционирует, а система B — нет, то любая начальная матрица плотности составной системы эволюционирует в другую матрицу плотности.

Докажем, что предположений (0), (1), (2) и (3′) достаточно для того, чтобы $ был супероператором (имел представление операторной суммы). [Действительно, свойства (0)–(3′) могут рассматриваться как альтернативное определение супероператора.] Однако, прежде чем приступать к доказательству, попробуем пояснить понятие полной положительности на примере положительного, но не вполне положительного оператора. Таким примером служит оператор транспонирования

$$T : \rho \to \rho^T. \tag{3.79}$$

T сохраняет собственные значения оператора ρ и, следовательно, очевидно положителен. Но является ли T *вполне* положительным (положителен ли любой оператор $\mathbf{T}_A \otimes \mathbf{1}_B$)? Выберем $\dim \mathcal{H}_A = \dim \mathcal{H}_B = N$ и рассмотрим максимально запутанное состояние

$$|\Phi\rangle_{AB} = \frac{1}{\sqrt{N}} \sum_{i=1}^{N} |i\rangle_A \otimes |i'\rangle_B, \tag{3.80}$$

где $\{|i\rangle_A\}$ и $\{|i'\rangle_B\}$ – ортонормированные базисы в $\mathcal{H}_A$ и $\mathcal{H}_B$ соответственно. Тогда

$$\mathbf{T}_A \otimes \mathbf{1}_B : \rho|\Phi\rangle_{AB\,AB}\langle\Phi| = \frac{1}{N} \sum_{i,j} \left(|i\rangle_{A\,A}\langle j|\right) \otimes \left(|i'\rangle_{B\,B}\langle j'|\right) \rightarrow$$

$$\rightarrow \rho' = \frac{1}{N} \sum_{i,j} \left(|j\rangle_{A\,A}\langle i|\right) \otimes \left(|i'\rangle_{B\,B}\langle j'|\right). \tag{3.81}$$

Мы видим, что оператор $N\rho'$ действует как

$$N\rho' : \left(\sum_i a_i|i\rangle_A\right) \otimes \left(\sum_j b_j|j'\rangle_B\right) \rightarrow \left(\sum_i a_i|i'\rangle_B\right) \otimes \left(\sum_j b_j|j\rangle_A\right), \tag{3.82}$$

или

$$N\rho'\left(|\varphi\rangle_A \otimes |\psi\rangle_B\right) = |\psi\rangle_A \otimes |\varphi\rangle_B. \tag{3.83}$$

Следовательно, $N\rho'$ – оператор перестановки (квадрат которого является тождественным оператором). Собственными состояниями $N\rho'$ являются *симметричные* относительно $A \leftrightarrow B$ состояния, которым отвечает собственное значение $+1$, и *антисимметричные* состояния, которым отвечает собственное значение -1. Поскольку ρ' имеет отрицательные собственные значения, он не является положительным и (поскольку ρ несомненно положителен), следовательно, $\mathbf{T}_A \otimes \mathbf{1}_B$ не сохраняет положительность. Таким образом, $\mathbf{T}_A$ – положительный оператор, но он не является вполне положительным.

3.2.4. ПОЗМ как супероператор

Унитарное преобразование, запутывающее A с B, после ортогонального измерения B может быть описано как ПОЗМ в A. Фактически положительные операторы, включая ПОЗМ, можно построить из операторов Крауса. Если $|\varphi\rangle_A$ эволюционирует как

$$|\varphi\rangle_A|0\rangle_B \rightarrow \sum_\mu \mathbf{M}_\mu|\varphi\rangle_A|\mu\rangle_B, \tag{3.84}$$

тогда измерение в B, проецирующее на базис $\{|\mu\rangle_B\}$, с вероятностью

$$\text{Prob}(\mu) = {}_A\langle\varphi|\mathbf{M}_\mu^\dagger\mathbf{M}_\mu|\varphi\rangle_A \tag{3.85}$$

дает результат μ. Выражая $\boldsymbol{\rho}_A$ как ансамбль чистых состояний, мы находим вероятность

$$\text{Prob}(\mu) = \text{tr}\left(\mathbf{F}_\mu\boldsymbol{\rho}_A\right), \qquad \mathbf{F}_\mu = \mathbf{M}_\mu^\dagger\mathbf{M}_\mu \tag{3.86}$$

результата μ; очевидно, что $\mathbf{F}_\mu$ положителен, а равенство $\sum\limits_\mu \mathbf{F}_\mu = \mathbf{1}$ следует из нормировки операторов Крауса. Следовательно, это действительно реализация ПОЗМ.

В частности, ПОЗМ, модифицирующая матрицу плотности согласно

$$\boldsymbol{\rho} \to \sum_\mu \sqrt{\mathbf{F}_\mu}\boldsymbol{\rho}\sqrt{\mathbf{F}_\mu}, \tag{3.87}$$

является частным случаем супероператора. Так как каждый $\sqrt{\mathbf{F}_\mu}$ эрмитов, требование

$$\sum_\mu \mathbf{F}_\mu = \mathbf{1} \tag{3.88}$$

в точности совпадает с условием нормировки операторной суммы. Следовательно, ПОЗМ имеет «унитарное представление»; существует унитарный оператор $\mathbf{U}_{AB}$, действующий как

$$\mathbf{U}_{AB} \,:\, |\varphi\rangle_A \otimes |0\rangle_B \to \sum_\mu \sqrt{\mathbf{F}_\mu}|\varphi\rangle_A \otimes |\mu\rangle_B, \tag{3.89}$$

где $|\varphi\rangle_A$ — чистое состояние в A. Очевидно, что, выполняя ортогональное измерение в системе B, проецирующее на базис $\{|\mu\rangle_B\}$, мы можем реализовать ПОЗМ, которая готовит состояние

$$\boldsymbol{\rho}'_A = \frac{\sqrt{\mathbf{F}_\mu}\boldsymbol{\rho}_A\sqrt{\mathbf{F}_\mu}}{\text{tr}\left(\mathbf{F}_\mu\boldsymbol{\rho}_A\right)} \tag{3.90}$$

с вероятностью

$$\text{Prob}(\mu) = \text{tr}\left(\mathbf{F}_\mu\boldsymbol{\rho}_A\right). \tag{3.91}$$

Эта реализация ПОЗМ, возможно, не самая эффективная (мы требуем, чтобы гильбертово пространство $\mathcal{H}_A \otimes \mathcal{H}_B$ имело размерность $N \cdot n$, если ПОЗМ имеет n возможных результатов), но в некоторых отношениях она наиболее удобна. ПОЗМ представляет собой наиболее общее измерение, которое мы можем выполнить в системе A, сначала запутывая ее с системой B, а затем выполняя ортогональное измерение в системе B.

3.3. Теорема о представлении Крауса

Теперь мы практически готовы доказать, что любой $, удовлетворяющий условиям (0), (1), (2) и (3′), имеет представление операторной суммы (теорема о представлении Крауса)[1]. Но сначала мы обсудим полезный трюк, который будет использован в доказательстве. Поскольку этот прием широко применяется, имеет смысл описать его отдельно.

Этот трюк (который мы будем называть «методом соответственного состояния») позволяет полностью охарактеризовать оператор $\mathbf{M}_A$, действующий в $\mathcal{H}_A$, описывая действие оператора $\mathbf{M}_A \otimes \mathbf{1}_B$ на единственное чистое максимально запутанное состояние[2] в $\mathcal{H}_A \otimes \mathcal{H}_B$ (где $\dim \mathcal{H}_B \geqslant \dim \mathcal{H}_A \equiv N$). Рассмотрим состояние

$$|\tilde{\psi}\rangle_{AB} = \sum_{i=1}^{N} |i\rangle_A \otimes |i'\rangle_B, \tag{3.92}$$

где $\{|i\rangle_A\}$ и $\{|i'\rangle_B\}$ — ортонормированные базисы в $\mathcal{H}_A$ и $\mathcal{H}_B$. (Мы выбрали $|\tilde{\psi}\rangle_{AB}$ нормированным таким образом, чтобы ${}_{AB}\langle\tilde{\psi}|\tilde{\psi}\rangle_{AB} = N$; это избавляет нас от необходимости писать множители $\sqrt{N}$ в формулах ниже.) Заметим, что любой вектор

$$|\varphi\rangle_A = \sum_i a_i |i\rangle_A \tag{3.93}$$

в $\mathcal{H}_A$ может быть представлен в виде «частичного» внутреннего произведения

$$|\varphi\rangle_A = {}_B\langle\varphi^*|\tilde{\psi}\rangle_{AB}, \tag{3.94}$$

где

$$|\varphi^*\rangle_B = \sum_i a_i^* |i'\rangle_B. \tag{3.95}$$

Мы говорим, что $|\varphi\rangle_A$ является «соответственным состоянием» «состояния-указателя» $|\varphi^*\rangle_B$. Отображение

$$|\varphi\rangle_A \to |\varphi^*\rangle_B, \tag{3.96}$$

[1] Приводимое здесь доказательство следует работе B. W. Schumacher, *Sending Entanglement Through Noisy Quantum Channels*, Phys. Rev., A54, 2614–2628 (1996); quant-ph/9604023 (см. Appendix A в этой работе).

[2] Мы говорим, что состояние $|\psi\rangle_{AB}$ максимально запутано, если $\mathrm{tr}_B(|\psi\rangle_{AB\,AB}\langle\psi|) \propto \mathbf{1}_A$.

очевидно, является *антилинейным* и фактически *антиунитарным* отображением из $\mathcal{H}_A$ в подпространство $\mathcal{H}_B$. Оператор $\mathbf{M}_A \otimes \mathbf{1}_B$, действуя на $|\tilde{\psi}\rangle_{AB}$, дает

$$(\mathbf{M}_A \otimes \mathbf{1}_B)|\tilde{\psi}\rangle_{AB} = \sum_i \mathbf{M}_A|i\rangle_A \otimes |i'\rangle_B. \tag{3.97}$$

Из этого состояния мы можем выделить $\mathbf{M}_A|\varphi\rangle_A$ в качестве соответственного состояния

$$_B\langle\varphi^*|\mathbf{M}_A \otimes \mathbf{1}_B|\tilde{\psi}\rangle_{AB} = \mathbf{M}_A|\varphi\rangle_A. \tag{3.98}$$

Мы можем интерпретировать формализм соответственного состояния, говоря что можно реализовать ансамбль чистых состояний в $\mathcal{H}_A$, выполняя измерения в $\mathcal{H}_B$ на запутанном состоянии — если измерение в $\mathcal{H}_B$ дает результат $|\varphi^*\rangle_B$, то приготовленным состоянием является $|\varphi\rangle_A$. Если мы намерены применить некоторый линейный оператор в $\mathcal{H}_A$, то обнаружим, что результат не зависит от того, было ли сначала приготовлено состояние, а затем на него подействовали оператором, или сначала был применен оператор, а затем приготовлено состояние. Конечно, этот вывод имеет физический смысл. Можно даже представить, что приготовление и действие оператора являются событиями, разделенными пространственно-подобным интервалом, так что временное упорядочение становится нековариантным (зависящим от наблюдателя).

Мы покажем, что $\$_A$ имеет представление операторной суммы, применяя метод соответственного состояния не к операторам, а к супероператорам. *Поскольку* мы предполагаем, что $\$_A$ вполне положителен, мы знаем, что $\$_A \otimes \mathbf{1}_B$ положителен. Следовательно, если мы применяем $\$_A \otimes \mathbf{1}_B$ к $\tilde{\rho}_{AB} = |\tilde{\psi}\rangle_{AB\,AB}\langle\tilde{\psi}|$, то результатом будет положительный оператор, (ненормированная) матрица плотности $\tilde{\rho}'_{AB}$ в $\mathcal{H}_A \otimes \mathcal{H}_B$. Подобно любой матрице плотности, $\tilde{\rho}'_{AB}$ может быть представлена как ансамбль чистых состояний. Следовательно,

$$(\$_A \otimes \mathbf{1}_B)(|\tilde{\psi}\rangle_{AB\,AB}\langle\tilde{\psi}|) = \sum_\mu q_\mu |\tilde{\Phi}_\mu\rangle_{AB\,AB}\langle\tilde{\Phi}_\mu| \tag{3.99}$$

где $q_\mu > 0$, $\sum_\mu q_\mu = 1$, а каждый вектор $|\tilde{\Phi}_\mu\rangle_{AB}$, подобно $|\tilde{\psi}\rangle_{AB}$, нормирован таким образом, что $_{AB}\langle\tilde{\Phi}_\mu|\tilde{\Phi}_\mu\rangle_{AB} = N$. Применяя метод соответственного состояния, имеем

$$\begin{aligned}\$_A(|\varphi\rangle_{A\,A}\langle\varphi|) &= {}_B\langle\varphi^*|(\$_A \otimes \mathbf{1}_B)(|\tilde{\psi}\rangle_{AB\,AB}\langle\tilde{\psi}|)|\varphi^*\rangle_B = \\ &= \sum_\mu q_\mu {}_B\langle\varphi^*|\tilde{\Phi}_\mu\rangle_{AB\,AB}\langle\tilde{\Phi}_\mu|\varphi^*\rangle_B.\end{aligned} \tag{3.100}$$

Мы почти у цели; определим оператор $\mathbf{M}_\mu$ в $\mathcal{H}_A$ соотношением

$$\mathbf{M}_\mu : |\varphi\rangle_A \to \sqrt{q_\mu}\,{}_B\langle\varphi^*|\tilde{\Phi}_\mu\rangle_{AB}. \tag{3.101}$$

Можно проверить, что

1) Оператор $\mathbf{M}_\mu$ *линеен*, поскольку отображение $|\varphi\rangle_A \to |\varphi^*\rangle_B$ *антилинейно*.

2) $\$_A(|\varphi\rangle_{A\,A}\langle\varphi|) = \sum_\mu \mathbf{M}_\mu(|\varphi\rangle_{A\,A}\langle\varphi|)\mathbf{M}_\mu^\dagger$ для любого чистого состояния $|\varphi\rangle_A \in \mathcal{H}_A$.

3) $\$_A(\boldsymbol{\rho}_A) = \sum_\mu \mathbf{M}_\mu \boldsymbol{\rho}_A \mathbf{M}_\mu^\dagger$ для любой матрицы плотности $\boldsymbol{\rho}_A$, поскольку $\boldsymbol{\rho}_A$ может быть представлена как ансамбль чистых состояний, а $\$_A$ линеен.

4) $\sum_\mu \mathbf{M}_\mu \mathbf{M}_\mu^\dagger = \mathbf{1}_A$, поскольку $\$_A$ сохраняет след для любого $\boldsymbol{\rho}_A$.

Таким образом, мы построили представление операторной суммы для $\$_A$.

Вкратце, доказательство состоит в следующем. Поскольку $\$_A$ вполне положителен, то $\$_A \otimes \mathbf{1}_B$ преобразует максимально запутанную матрицу плотности в $\mathcal{H}_A \otimes \mathcal{H}_B$ в другую матрицу плотности. Эта матрица плотности может быть выражена, как ансамбль чистых состояний. Каждому из этих чистых состояний в $\mathcal{H}_A \otimes \mathcal{H}_B$ можно сопоставить (с помощью метода соответственных состояний) слагаемое операторной суммы.

Рассматривая таким образом представление операторной суммы, можно легко установить два важных следствия:

Как много операторов Крауса? Каждый оператор $\mathbf{M}_\mu$ связан с состоянием $|\Phi_\mu\rangle$ в представлении ансамбля $\boldsymbol{\rho}'_{AB}$. Так как максимальный ранг $\boldsymbol{\rho}'_{AB}$ равен N^2 (где $N = \dim \mathcal{H}_A$), $\$_A$ всегда имеет представление операторной суммы с максимальным числом операторов Крауса, равным N^2.

Какова неоднозначность? Выше мы отмечали, что операторы Крауса

$$\mathbf{N}_a = \mathbf{M}_\mu \mathbf{U}_{\mu a} \tag{3.102}$$

($\mathbf{U}_{\mu a}$ – унитарное преобразование) представляют тот же, что и $\mathbf{M}_\mu$, супероператор $\$_A$. Теперь можно сказать, что любые два представления Крауса должны быть связаны таким образом. (Если число операторов $\mathbf{N}_a$ оказывается больше, чем $\mathbf{M}_\mu$, тогда набору $\mathbf{M}_\mu$, очевидно, нужно добавить соответствующее количество нулевых операторов, так чтобы эти два набора

операторов имели одинаковую мощность.) Это свойство можно рассматривать как следствие теоремы ЖХЙВ.

Описанная выше конструкция соответственного состояния устанавливает взаимно однозначное соответствие между представлениями ансамблей (ненормированной) матрицы плотности $(\$_A \otimes \mathbf{1}_B)(|\tilde{\psi}\rangle_{AB\,AB}\langle\tilde{\psi}|)$ и представлениями операторных сумм $\$_A$. (Мы явно описали, как перейти от представления ансамбля к представлению операторной суммы, но, очевидно, можно пойти и другим путем. Если

$$\$_A(|i\rangle_{A\,A}\langle j|) = \sum_\mu \mathbf{M}_\mu |i\rangle_{A\,A}\langle j|\mathbf{M}_\mu^\dagger, \tag{3.103}$$

то

$$\begin{aligned}(\$_A \otimes \mathbf{1}_B)(|\tilde{\psi}\rangle_{AB\,AB}\langle\tilde{\psi}|) &= \sum_{i,j,\mu} (\mathbf{M}_\mu|i\rangle_A|i'\rangle_B)({}_A\langle j|{}_B\langle j'|\mathbf{M}_\mu^\dagger{}_B\langle j'|) \\ &= \sum_\mu q_\mu |\tilde{\Phi}_\mu\rangle_{AB\,AB}\langle\tilde{\Phi}_\mu|,\end{aligned} \tag{3.104}$$

где

$$\sqrt{q_\mu}|\tilde{\Phi}_\mu\rangle_{AB} = \sum_i \mathbf{M}_\mu|i\rangle_A|i'\rangle_B. \tag{3.105}$$

Рассмотрим теперь два таких ансамбля (или соответственно два представления $\$_A$ операторными суммами) $\{\sqrt{q_\mu}|\tilde{\Phi}_\mu\rangle_{AB}\}$ и $\{\sqrt{p_a}|\tilde{\Upsilon}_a\rangle_{AB}\}$. Для каждого ансамбля в $\mathcal{H}_{AB} \otimes \mathcal{H}_C$ существует соответствующее «очищение»:

$$\begin{aligned}&\sum_\mu \sqrt{q_\mu}|\tilde{\Phi}_\mu\rangle_{AB}|\alpha_\mu\rangle_C, \\ &\sum_a \sqrt{p_a}|\tilde{\Upsilon}_a\rangle_{AB}|\beta_a\rangle_C,\end{aligned} \tag{3.106}$$

где $\{|\alpha_\mu\rangle_C\}$ и $\{|\beta_a\rangle_C\}$ — два разных ортонормированных набора из $\mathcal{H}_C$. Теорема ЖХЙВ утверждает, что эти два «очищения» связаны между собой действующим в $\mathcal{H}_C$ унитарным преобразованием $\mathbf{1}_{AB} \otimes \mathbf{U}'_C$. Следовательно,

$$\begin{aligned}\sum_a \sqrt{p_a}|\tilde{\Upsilon}_a\rangle_{AB}|\beta_a\rangle_C \quad &\sum_\mu \sqrt{q_\mu}|\tilde{\Phi}_\mu\rangle_{AB}\mathbf{U}'_C|\alpha_\mu\rangle_C \\ &= \sum_{\mu,a} \sqrt{q_\mu}|\tilde{\Phi}_\mu\rangle_{AB}U_{\mu a}|\beta_a\rangle_C.\end{aligned} \tag{3.107}$$

Здесь второе равенство мы получили, заметив что ортонормированные базисы $\{|\alpha_\mu\rangle_C\}$ и $\{|\beta_a\rangle_C\}$ связаны между собой унитарным преобразованием, а произведение преобразований, в свою очередь, унитарно. Мы приходим к выводу, что

$$\sqrt{p_a}|\tilde{\Upsilon}_a\rangle_{AB} = \sum_\mu \sqrt{q_\mu}|\tilde{\Phi}_\mu\rangle_{AB} U_{\mu a} \tag{3.108}$$

(где $U_{\mu a}$ — унитарное преобразование), откуда следует, что

$$\mathbf{N}_a = \sum_\mu \mathbf{M}_\mu \mathbf{U}_{\mu a}. \tag{3.109}$$

Замечание. Поскольку мы уже установили, что можем перейти от представления операторной суммы для $\$_A$ к унитарному представлению, мы нашли, что любой «разумный» закон эволюции оператора плотности в $\mathcal{H}_A$ может быть реализован унитарным преобразованием $\mathbf{U}_{AB}$, действующим в $\mathcal{H}_A \otimes \mathcal{H}_B$ как

$$\mathbf{U}_{AB} : |\psi\rangle_A \otimes |0\rangle_B \to \sum_\mu |\varphi\rangle_A \otimes |\mu\rangle_B. \tag{3.110}$$

Является ли этот результат неожиданным? Возможно, да. Мы можем интерпретировать супероператор как *описывающий эволюцию системы* (A), взаимодействующей с окружением (B). В общем случае состояния системы запутаны с ее окружением. Но в (3.110) предполагается, что начальное состояние не запутано. Несмотря на то что реальная система всегда связана запутыванием с ее окружением, при описании эволюции ее матрицы плотности без потери общности можно *представлять*, что в момент, когда мы начинаем ее наблюдать, предварительное запутывание отсутствует!

Замечание. Представление операторной суммы даст очень удобный способ выражения любого вполне положительного $\$$. Но положительный $\$$ не допускает такого представления, если не является вполне положительным. Насколько мне известно, не существует удобного, сопоставимого с представлением Крауса, способа выразить наиболее общий *положительный* $\$$.

3.4. Три квантовых канала

Лучше всего познакомиться с понятием супероператора, изучив несколько примеров. Мы рассмотрим три примера (все они интересны и по-

лезны) супероператоров для одного кубита. Из уважения к традиционной терминологии (классической) теории связи я буду ссылаться на эти супероператоры как на *квантовые каналы*. Мы можем представлять, что $ описывает судьбу квантовой информации, которая с некоторой потерей точности воспроизведения посылается от передатчика к приемнику. Или, если угодно, можно считать (в духе предыдущего обсуждения), что передача идет во времени, а не в пространстве, то есть $ описывает эволюцию квантовой системы, взаимодействующей с ее окружением.

3.4.1. Деполяризующий канал

Деполяризующий канал представляет собой модель декогерентизации кубита, имеющую особенно тонкие свойства симметрии. Мы можем описать его, говоря что с вероятностью $1-p$ кубит остается неповрежденным, тогда как с вероятностью p возникает ошибка. Она может быть любой из трех типов, причем все три типа ошибок равновероятны. Если $\{|0\rangle, |1\rangle\}$ — ортонормированный базис кубита, их можно описать следующим образом:

1. Ошибка инвертирования бита $\begin{matrix}|0\rangle \to |1\rangle \\ |1\rangle \to |0\rangle\end{matrix}$ или $|\psi\rangle \to \sigma_1|\psi\rangle$, $\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

2. Ошибка обращения фазы $\begin{matrix}|0\rangle \to |0\rangle \\ |1\rangle \to -|1\rangle\end{matrix}$ или $|\psi\rangle \to \sigma_3|\psi\rangle$, $\sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

3. Обе ошибки $\begin{matrix}|0\rangle \to +i|1\rangle \\ |1\rangle \to -i|0\rangle\end{matrix}$ или $|\psi\rangle \to \sigma_2|\psi\rangle$, $\sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$.

При появлении ошибки $|\psi\rangle$ превращается в ансамбль трех равновероятных состояний: $\sigma_1|\psi\rangle$, $\sigma_2|\psi\rangle$ и $\sigma_3|\psi\rangle$.

Унитарное представление

Деполяризующий канал может быть представлен унитарным оператором, действующим в $\mathcal{H}_A \otimes \mathcal{H}_E$, где размерность пространства $\mathcal{H}_E$ равна четырем. (Я обозначаю здесь это пространство $\mathcal{H}_E$, чтобы подтолкнуть вас

к мысли о вспомогательной системе как окружении.) Унитарный оператор $\mathbf{U}_{AE}$ действует как

$$\mathbf{U}_{AE}\colon |\psi\rangle_A \otimes |0\rangle_E \to \sqrt{1-p}|\psi\rangle_A \otimes |0\rangle_E + \\ + \sqrt{\frac{p}{3}}\Big[\boldsymbol{\sigma}_1|\psi\rangle_A \otimes |1\rangle_E + \boldsymbol{\sigma}_2|\psi\rangle_A \otimes |2\rangle_E + \boldsymbol{\sigma}_3|\psi\rangle_A \otimes |3\rangle_E\Big]. \quad (3.111)$$

(Поскольку $\mathbf{U}_{AE}$ сохраняет внутреннее произведение, он имеет унитарное расширение на все пространство $\mathcal{H}_A \otimes \mathcal{H}_E$.) Окружение эволюционирует к одному из четырех взаимно ортогональных состояний, «хранящих запись» о том, что произошло; если бы мы могли измерить окружение в базисе $\{|\mu\rangle_E,\ \mu = 0,1,2,3\}$, мы узнали бы, какого сорта ошибка возникла (тогда мы были бы в состоянии вмешаться и устранить ошибку).

Представление Крауса

Чтобы получить представление канала в виде операторной суммы, вычислим частичный след по окружению в базисе $\{|\mu\rangle_E\}$. Тогда

$$\mathbf{M}_\mu = {}_E\langle\mu|\mathbf{U}_{AE}|0\rangle_E, \quad (3.112)$$

где

$$\mathbf{M}_0 = \sqrt{1-p}\,\mathbf{1}, \quad \mathbf{M}_1 = \sqrt{\frac{p}{3}}\,\boldsymbol{\sigma}_1, \quad \mathbf{M}_2 = \sqrt{\frac{p}{3}}\,\boldsymbol{\sigma}_2, \quad \mathbf{M}_3 = \sqrt{\frac{p}{3}}\,\boldsymbol{\sigma}_3. \quad (3.113)$$

Используя $\boldsymbol{\sigma}_i^2 = \mathbf{1}$, можно непосредственно проверить условие нормировки:

$$\sum_\mu \mathbf{M}_\mu^\dagger \mathbf{M}_\mu = \left[(1-p) + 3\cdot\frac{p}{3}\right]\mathbf{1} = \mathbf{1}. \quad (3.114)$$

Произвольная начальная матрица плотности кубита $\boldsymbol{\rho}_A$ преобразуется как

$$\boldsymbol{\rho}_A \to \boldsymbol{\rho}'_A = (1-p)\boldsymbol{\rho}_A + \frac{p}{3}\left(\boldsymbol{\sigma}_1\boldsymbol{\rho}_A\boldsymbol{\sigma}_1 + \boldsymbol{\sigma}_2\boldsymbol{\rho}_A\boldsymbol{\sigma}_2 + \boldsymbol{\sigma}_3\boldsymbol{\rho}_A\boldsymbol{\sigma}_3\right), \quad (3.115)$$

где мы суммируем по четырем (в принципе различимым) путям, по которым могло бы эволюционировать окружение.

Представление соответственного состояния

Канал можно также охарактеризовать, описывая как в нем преобразуется максимально запутанное состояние двух кубитов, если канал действует

только на первый кубит. Существует четыре взаимно ортогональных максимально запутанных состояния, которые можно записать в виде

$$
\begin{aligned}
|\phi^+\rangle_{AB} &= \frac{1}{\sqrt{2}}\left(|00\rangle_{AB} + |11\rangle_{AB}\right),\\
|\phi^-\rangle_{AB} &= \frac{1}{\sqrt{2}}\left(|00\rangle_{AB} - |11\rangle_{AB}\right),\\
|\psi^+\rangle_{AB} &= \frac{1}{\sqrt{2}}\left(|01\rangle_{AB} + |10\rangle_{AB}\right),\\
|\psi^-\rangle_{AB} &= \frac{1}{\sqrt{2}}\left(|01\rangle_{AB} - |10\rangle_{AB}\right).
\end{aligned}
\tag{3.116}
$$

Если начальным состоянием является $|\phi^-\rangle_{AB}$, то, когда деполяризующий канал действует на первый кубит, запутанное состояние эволюционирует как

$$
\begin{aligned}
|\phi^+\rangle_{AB\,AB}\langle\phi^+| \to (1-p)|\phi^+\rangle_{AB\,AB}\langle\phi^+| +\\
+\frac{p}{3}\left(|\psi^+\rangle_{AB\,AB}\langle\psi^+| + |\psi^-\rangle_{AB\,AB}\langle\psi^-| + |\phi^-\rangle_{AB\,AB}\langle\phi^-|\right).
\end{aligned}
\tag{3.117}
$$

В «наихудшем» квантовом канале $p = 3/4$, в этом случае начальное запутанное состояние эволюционирует в

$$
\begin{aligned}
|\phi^+\rangle_{AB\,AB}\langle\phi^+| \to \frac{1}{4}\left(|\phi^+\rangle_{AB\,AB}\langle\phi^+| + |\phi^-\rangle_{AB\,AB}\langle\phi^-| +\right.\\
\left. + |\psi^+\rangle_{AB\,AB}\langle\psi^+| + |\psi^-\rangle_{AB\,AB}\langle\psi^-|\right) = \frac{1}{4}\mathbf{1}_{AB}.
\end{aligned}
\tag{3.118}
$$

Оно становится полностью случайной матрицей плотности в $\mathcal{H}_A \otimes \mathcal{H}_B$. Тогда, применяя метод соответственного состояния, можно увидеть, что чистое состояние $|\varphi\rangle_A$ одного кубита A эволюционирует как

$$
|\varphi\rangle_{A\,A}\langle\varphi| \to {}_B\left\langle\varphi^*\left|2\left(\frac{1}{4}\mathbf{1}_{AB}\right)\right|\varphi^*\right\rangle_B = \frac{1}{2}\mathbf{1}_A; \tag{3.119}
$$

оно становится случайной матрицей в $\mathcal{H}_A$, независимо от значения начального состояния $|\varphi\rangle_A$. Как если бы канал выбросил начальное состояние и заменил его совершенно случайным мусором.

Альтернативным представлением эволюции максимально запутанного состояния является

$$|\phi^+\rangle_{AB\,AB}\langle\phi^+| \to \left(1-\frac{4}{3}p\right)|\phi^+\rangle_{AB\,AB}\langle\phi^+| + \frac{4}{3}p\left(\frac{1}{4}\mathbf{1}_{AB}\right). \quad (3.120)$$

Таким образом, вместо того, чтобы говорить о трех типах равновероятных ошибок, появляющихся с вероятностью p каждая, мы могли бы говорить, что с вероятностью $4p/3$ возникает ошибка, полностью «рандомизирующая» состояние (мы можем так говорить по крайней мере при $p \leqslant 3/4$). Наличие двух естественных способов определения «вероятности ошибки» в этом канале иногда может приводить к путанице и недоразумениям.

Полезной мерой того, насколько хорошо канал сохраняет исходную квантовую информацию, является так называемая «точность воспроизведения запутанности» F_e. Она количественно определяет, насколько конечная матрица плотности «близка» к исходному максимально запутанному состоянию $|\phi^+\rangle$:

$$F_e = \langle\phi^+|\boldsymbol{\rho}'|\phi^+\rangle. \quad (3.121)$$

Для деполяризующего канала мы имеем $F_e = 1-p$ и, следовательно, можем интерпретировать F_e как вероятность отсутствия ошибки.

Представление сферы Блоха

Также поучительно рассмотреть, как деполяризующий канал действует на сфере Блоха. Произвольная матрица плотности одного кубита может быть записана в виде

$$\boldsymbol{\rho} = \frac{1}{2}(\mathbf{1} + \vec{P}\cdot\vec{\boldsymbol{\sigma}}), \quad (3.122)$$

где $\vec{P}$ — «спиновая поляризация» кубита. Повернем оси таким образом, чтобы $\vec{P} = P_3\hat{e}_3$, а $\boldsymbol{\rho} = \frac{1}{2}(\mathbf{1} + P_3\boldsymbol{\sigma}_3)$. Тогда, поскольку $\boldsymbol{\sigma}_3\boldsymbol{\sigma}_3\boldsymbol{\sigma}_3 = \boldsymbol{\sigma}_3$, а $\boldsymbol{\sigma}_1\boldsymbol{\sigma}_3\boldsymbol{\sigma}_1 = -\boldsymbol{\sigma}_3 = \boldsymbol{\sigma}_2\boldsymbol{\sigma}_3\boldsymbol{\sigma}_2$, найдем, что

$$\boldsymbol{\rho}' = \left(1-p+\frac{p}{3}\right)\frac{1}{2}(1+P_3\boldsymbol{\sigma}_3) + \frac{2p}{3}\frac{1}{2}(1-P_3\boldsymbol{\sigma}_3) \quad (3.123)$$

или $P_3' = (1-4p/3)P_3$. С учетом симметрии относительно поворотов видно, что независимо от ориентации $\vec{P}$

$$\vec{P}' = \left(1-\frac{4}{3}p\right)\vec{P}. \quad (3.124)$$

Следовательно, под действием деполяризующего канала происходит однородное сжатие сферы Блоха; спиновая поляризация уменьшается на множитель $(1 - 4p/3)$ (вот почему мы называем этот канал деполяризующим). Этот результат следовало ожидать в связи со сделанным ранее заключением о том, что с вероятностью $4p/3$ в канале происходит полная «рандомизация» спина.

Обратимость?

Почему мы говорим, что супероператор необратим? Очевидно, мы можем обратить однородное сжатие сферы однородным же раздуванием. Но беда в том, что раздувание сферы Блоха не положительно и потому не является супероператором. Раздувание преобразует $\vec{P}$ длины $|\vec{P}| \leqslant 1$ в вектор длины $|\vec{P}| \geqslant 1$, преобразуя таким образом оператор плотности в оператор с отрицательным собственным значением. Декогерентизация может сжать шар, но нет физического процесса, способного снова надуть его! Супероператор, бегущий назад во времени, не является супероператором.

3.4.2. Канал затухания фазы

Нашим следующим примером является канал *затухания фазы*. Этот случай интересен с практической точки зрения, поскольку представляет голую, свободную от несущественных математических деталей, карикатуру декогерентизации в реальной физической ситуации.

Унитарное представление

Унитарным представлением канала является

$$\begin{aligned} |0\rangle_A|0\rangle_E &\to \sqrt{1-p}|0\rangle_A|0\rangle_E + \sqrt{p}|0\rangle_A|1\rangle_E, \\ |1\rangle_A|0\rangle_E &\to \sqrt{1-p}|1\rangle_A|0\rangle_E + \sqrt{p}|1\rangle_A|2\rangle_E. \end{aligned} \tag{3.125}$$

В этом случае, в отличие от деполяризующего канала, кубит A не совершает никаких переходов. Вместо этого он время от времени (с вероятностью p) «рассеивает» окружение, толкая его в состояние $|1\rangle_E$, если A находится в состоянии $|0\rangle_A$, и — в состояние $|2\rangle_E$, если A находится в состоянии $|1\rangle_A$. Более того, также в отличие от деполяризующего канала, этот канал выделяет предпочтительный базис для кубита A; только в базисе $\{|0\rangle_A\ |1\rangle_A\}$ не происходит опрокидывание спина кубита A.

Представление Крауса

Вычисляя частичный след по $\mathcal{H}_E$ в базисе $\{|0\rangle_E, |1\rangle_E, |2\rangle_E\}$, получим операторы Крауса

$$\mathbf{M}_0 = \sqrt{1-p}\,\mathbf{1}, \quad \mathbf{M}_1 = \sqrt{p}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad \mathbf{M}_2 = \sqrt{p}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}. \quad (3.126)$$

Нетрудно проверить, что $\mathbf{M}_0^2 + \mathbf{M}_1^2 + \mathbf{M}_2^2 = \mathbf{1}$. В этом случае не обязательно иметь три оператора Крауса; как вы покажете в домашнем упражнении, возможно представление двумя операторами Крауса.

Начальная матрица плотности $\boldsymbol{\rho}$ эволюционирует к

$$\$(\boldsymbol{\rho}) = \mathbf{M}_0\boldsymbol{\rho}\mathbf{M}_0 + \mathbf{M}_1\boldsymbol{\rho}\mathbf{M}_1 + \mathbf{M}_2\boldsymbol{\rho}\mathbf{M}_2 = \\ = (1-p)\boldsymbol{\rho} + p\begin{pmatrix} \rho_{00} & 0 \\ 0 & \rho_{11} \end{pmatrix} = \begin{pmatrix} \rho_{00} & (1-p)\rho_{01} \\ (1-p)\rho_{10} & \rho_{11} \end{pmatrix}; \quad (3.127)$$

таким образом, диагональные элементы $\boldsymbol{\rho}$ остаются неизменными, тогда как недиагональные — затухают.

Предположим, что отнесенная к единице времени вероятность акта рассеяния Γ такова, что вероятность рассеяния за время Δt гораздо меньше единицы ($p = \Gamma\Delta t \ll 1$). Эволюция в течение времени $t = n\Delta t$ управляется супероператором $\$^n$, так что недиагональные элементы матрицы плотности подавляются по закону $(1-p)^n = (1-\Gamma\Delta t)^{t/\Delta t} \to \exp(-\Gamma t)$ (при $\Delta t \to 0$). Таким образом, если мы приготовили начальное чистое состояние $a|0\rangle + b|1\rangle$, то спустя время $t \gg \Gamma^{-1}$ оно распадается в некогерентную суперпозицию $\boldsymbol{\rho}' = |a|^2|0\rangle\langle 0| + |b|^2|1\rangle\langle 1|$. Декогерентизация возникает в выделенном базисе $\{|0\rangle, |1\rangle\}$.

Представление сферы Блоха

Эту задачу вы исследуете в домашнем упражнении.

Интерпретация

Канал затухания фазы можно интерпретировать как описывающий тяжелую «классическую» частицу (например, частицу межзвездной пыли), взаимодействующую с фоновым газом легких частиц (например, с фотонами реликтового микроволнового излучения). Можно представить, что первоначально пылинка была приготовлена в суперпозиции собственных со-

стояний оператора координаты $|\psi\rangle = \frac{1}{\sqrt{2}}(|x\rangle + |-x\rangle)$ (или в более общей суперпозиции слабо перекрывающихся, пространственно-локализованных волновых пакетов). Можно контролировать поведение частички пыли, но безнадежно пытаться следить за квантовым состоянием всех фотонов, рассеиваемых этой частицей; для наших целей ее квантовое состояние описывается матрицей плотности ρ, полученной после вычисления следа по фотонным степеням свободы.

Наш анализ канала затухания фазы показывает, что если фотоны рассеиваются частицей с частотой Γ, то недиагональные элементы матрицы плотности ρ затухают как $\exp(-\Gamma t)$ и становятся полностью пренебрежимыми при $t \gg \Gamma^{-1}$. Начиная с этого момента, когерентная суперпозиция собственных состояний оператора положения полностью разрушена — нет никакой возможности восстановить волновые пакеты и заставить их интерферировать. (Если мы пытаемся получить с помощью частиц пыли картину интерференции на двух щелях, то мы не увидим ее, если пылинкам необходимо время $t \gg \Gamma^{-1}$, чтобы пройти путь от источника до экрана.)

Частицы пыли тяжелы. Вследствие большой инерции, их состояние движения мало подвержено влиянию со стороны рассеиваемых фотонов. Таким образом, имеется два несоизмеримых временных масштаба, имеющих отношение к динамике частиц пыли. С одной стороны, это время затухания, то есть время, за которое значительная часть импульса частиц передается фотонам: это большое время, если частицы достаточно тяжелы. С другой стороны, существует временной масштаб декогерентизации. В этой модели он имеет порядок Γ^{-1} — времени, в течение которого на частице пыли происходит рассеяние *одного* фотона и которое гораздо короче временного масштаба затухания. В макроскопическом объекте декогерентизация протекает *быстро*.

Как мы уже отмечали, канал затухания фазы выделяет предпочтительный базис для декогерентизации, в нашей «интерпретации» мы предположили, что им является базис собственных состояний оператора положения. С физической точки зрения декогерентизация выделяет пространственно локализованные состояния частиц пыли, поскольку их *взаимодействие* с фотонами локализовано в пространстве. Частицы, находящиеся в различимых пространственных положениях, стремятся рассеивать фотоны во взаимно ортогональные состояния.

Даже если «частицы» разделены настолько мало, что они не разрешаются рассеиваемыми фотонами, процесс декогерентизации все еще работает подобным образом. Возможно, фотоны, рассеянные частицами, находящимися в точках $+x$ и $-x$, не являются взаимно ортогональными, а вместо

этого имеют ненулевое перекрытие

$$\langle \gamma + | \gamma - \rangle = 1 - \varepsilon, \qquad \varepsilon \ll 1. \tag{3.128}$$

Тем не менее канал затухания фазы описывает эту ситуацию, но теперь с p, замененным на εp (если p – по-прежнему вероятность акта рассеяния). Таким образом, темп декогерентизации становится равным $\Gamma_{\rm dec} = \varepsilon \Gamma_{\rm scat}$, где $\Gamma_{\rm scat}$ – частота рассеяния (см. домашнее задание).

Интуитивное понимание, извлекаемое из этой простой модели, применимо к огромному множеству физических ситуаций. Распад когерентной суперпозиции макроскопически различимых состояний «тяжелых» объектов происходит гораздо быстрее их затухания. Пространственная локализация взаимодействия системы с ее окружением делает предпочтительным для декогерентизации «локальный» базис. По-видимому, подобные принципы можно применить к декогерентизации «состояния кота» $\frac{1}{\sqrt{2}}(|\text{dead}\rangle + |\text{alive}\rangle)$, поскольку состояния «мертвый» и «живой» можно различить локальными испытаниями.

3.4.3. Канал затухания амплитуды

Канал затухания амплитуды представляет собой схематическую модель распада возбужденного состояния (двухуровневого) атома вследствие спонтанного излучения фотона. Регистрируя излучаемый фотон («наблюдая за окружением»), мы можем выполнить ПОЗМ, которая дает информацию о начальном состоянии атома.

Унитарное представление

Обозначим как $|0\rangle_A$ основное состояние атома, а интересующее нас возбужденное состояние – $|1\rangle_A$. Роль «окружения» играет электромагнитное поле, начальным состоянием которого предполагается основное $|0\rangle_E$. Существует вероятность p того, что некоторое время спустя возбужденное состояние распадается в основное $|0\rangle_A$, что сопровождается излучением фотона и, следовательно, переходом окружения из состояния $|0\rangle_E$ («нет фотонов») в состояние $|1\rangle_E$ («один фотон»). Эта эволюция описывается унитарным преобразованием, действующим на атом и окружение как

$$\begin{aligned} |0\rangle_A|0\rangle_E &\to |0\rangle_A|0\rangle_E, \\ |1\rangle_A|0\rangle_E &\to \sqrt{1-p}|1\rangle_A|0\rangle_E + \sqrt{p}|0\rangle_A|1\rangle_E. \end{aligned} \tag{3.129}$$

(Естественно, если начальным состоянием атома является основное, а окружение находится при нулевой температуре, то никакие переходы не происходят).

Операторы Крауса

Вычисляя частичный след по окружению в базисе $\{|0\rangle_E, |1\rangle_E\}$, найдем операторы Крауса

$$\mathbf{M}_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-p} \end{pmatrix}, \qquad \mathbf{M}_1 = \begin{pmatrix} 0 & \sqrt{p} \\ 0 & 0 \end{pmatrix}. \tag{3.130}$$

Нетрудно проверить, что

$$\mathbf{M}_0^\dagger \mathbf{M}_0 + \mathbf{M}_1^\dagger \mathbf{M}_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1-p \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & p \end{pmatrix} = \mathbf{1}. \tag{3.131}$$

Оператор $\mathbf{M}_1$ индуцирует «квантовый скачок» — распад состояния $|1\rangle_A$ в $|0\rangle_A$, а $\mathbf{M}_0$ описывает эволюцию состояния в отсутствии скачков. Матрица плотности изменяется как

$$\begin{aligned} \rho \;\to\; \$(\rho) &= \mathbf{M}_0 \rho \mathbf{M}_0^\dagger + \mathbf{M}_1 \rho \mathbf{M}_1^\dagger = \\ &= \begin{pmatrix} \rho_{00} & \sqrt{1-p}\rho_{01} \\ \sqrt{1-p}\rho_{10} & (1-p)\rho_{11} \end{pmatrix} + \begin{pmatrix} p\rho_{11} & 0 \\ 0 & 0 \end{pmatrix} = \\ &= \begin{pmatrix} \rho_{00} + p\rho_{11} & \sqrt{1-p}\rho_{01} \\ \sqrt{1-p}\rho_{10} & (1-p)\rho_{11} \end{pmatrix}. \end{aligned} \tag{3.132}$$

Если мы применим канал n раз подряд, то матричный элемент ρ_{11} уменьшится согласно

$$\rho_{11} \to (1-p)^n \rho_{11}. \tag{3.133}$$

Следовательно, если вероятность перехода в течение времени Δt равна $\Gamma \Delta t$, то вероятность того, что возбужденное состояние проживет в течение времени t равна $(1 - \Gamma\Delta t)^{t/\Delta t} \to e^{-\Gamma t}$, ожидаемый экспоненциальный закон затухания.

При $t \to \infty$ вероятность затухания стремится к единице, следовательно:

$$\$(\rho) = \begin{pmatrix} \rho_{00} + \rho_{11} & 0 \\ 0 & 0 \end{pmatrix}. \tag{3.134}$$

Атом всегда сваливается в свое основное состояние. Этот пример показывает, что иногда оказывается возможным, что супероператор преобразует начальное смешанное состояние, например:

$$\rho = \begin{pmatrix} \rho_{00} & 0 \\ 0 & \rho_{11} \end{pmatrix} \tag{3.135}$$

в чистое конечное состояние.

Контроль окружения

В случае распада возбужденного атомного состояния, сопровождающегося излучением фотона, полезно следить за состоянием окружения с помощью детектора фотонов. Измерение окружения готовит чистое состояние атома и, в сущности, предотвращает процесс декогерентизации.

Возвращаясь к унитарному представлению канала затухания амплитуды, мы видим, что когерентная суперпозиция основного и возбужденного атомных состояний эволюционирует как

$$\left(a|0\rangle_A + b|1\rangle_B\right)|0\rangle_E \to \left(a|0\rangle_A + b\sqrt{1-p}|1\rangle_B\right)|0\rangle_E + b\sqrt{p}|0\rangle_A|1\rangle_E. \tag{3.136}$$

Регистрируя фотон и, следовательно, проецируя окружение на состояние $|1\rangle_E$, мы готовим атомное состояние $|0\rangle_A$. Фактически мы приготовили состояние, относительно которого нам точно известно, что оно было порождено начальным возбужденным атомным состоянием $|1\rangle_A$, — основное состояние не распадается.

С другой стороны, если мы не зарегистрировали фотон, а наш детектор обладает идеальной чувствительностью, то мы спроецировали окружение на состояние $|0\rangle_E$ и, следовательно, приготовили атомное состояние

$$a|0\rangle_A + b\sqrt{1-p}|1\rangle_B. \tag{3.137}$$

Ввиду неудачи в регистрации фотона становится более вероятным, что начальным атомным состоянием было основное!

Как уже отмечалось, унитарное преобразование, которое запутывает A с E вслед за ортогональным измерением E, может быть описано как ПОЗМ в A. Если $|\varphi\rangle_A$ изменяется как

$$|\varphi\rangle_A|0\rangle_E \to \sum_\mu \mathbf{M}_\mu|\varphi\rangle_A|\mu\rangle_E, \tag{3.138}$$

то ортогональное измерение в E, которое проецирует на базис $\{|\mu\rangle_E\}$, для каждого результата μ реализует ПОЗМ с

$$\mathrm{Prob}(\mu) = \mathrm{tr}\left(\mathbf{F}_\mu \rho_A\right), \qquad \mathbf{F}_\mu = \mathbf{M}_\mu^\dagger \mathbf{M}_\mu. \tag{3.139}$$

В случае канала затухания амплитуды находим:

$$\mathbf{F}_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1-p \end{pmatrix}, \qquad \mathbf{F}_1 = \begin{pmatrix} 0 & 0 \\ 0 & p \end{pmatrix}, \tag{3.140}$$

где $\mathbf{F}_0$ определяет вероятность успешного детектирования фотона, а $\mathbf{F}_1$ – дополнительную к ней вероятность того, что фотон не зарегистрирован.

Если мы ожидаем в течение времени $t \gg \Gamma^{-1}$, так что p стремится к единице, наша ПОЗМ приближается к ортогональному измерению, измерению начального атомного состояния в базисе $\{|0\rangle_A, |1\rangle_A\}$. Необычной чертой этого измерения является то, что мы можем проецировать на состояние $|0\rangle_A$, *не регистрируя* фотон. Это пример того, что Дикке называл «измерением без взаимодействия» – наблюдая *отсутствие изменения* в состоянии окружения, мы делаем вывод, каким должно было быть атомное состояние. Термин «измерение без взаимодействия» является общеупотребительным, хотя он в некоторой степени вводит в заблуждение; очевидно, что если бы гамильтониан Вселенной не включал связь атома с электромагнитным полем, то измерение было бы невозможно.

3.5. Основное уравнение

3.5.1. Марковская эволюция

Формализм супероператоров предоставляет общее описание эволюции матрицы плотности, в том числе эволюции чистого состояния в смешанное (декогерентизация). В том же смысле, в каком унитарное преобразование дает общее описание когерентной квантовой эволюции. В последнем случае динамику квантовой системы удобно характеризовать *гамильтонианом*, описывающим эволюцию в бесконечно малом интервале времени. Тогда динамика описывается дифференциальным уравнением, *уравнением Шредингера*. Интегрируя это уравнение или, иначе говоря, складывая эволюции на множестве инфинитезимальных интервалов, мы можем рассчитать эволюцию в течение конечного интервала времени.

Часто, по крайней мере в хорошем приближении, оказывается возможным описание эволюции (не обязательно когерентной) матрицы плотности

дифференциальным уравнением. Это так называемое *основное уравнение* (master equation) будет нашей следующей темой.

В самом деле, непонятно, почему для описания декогерентизации необходимо дифференциальное уравнение. Такое описание возможно, если только эволюция квантовой системы является «марковской» или, другими словами, *локальной* во времени. Если эволюция во времени t оператора плотности $\rho(t)$ управляется дифференциальным уравнением (первого порядка), то это значит, что оператор $\rho(t+dt)$ полностью определяется оператором $\rho(t)$.

Мы видели, что всегда можем описать эволюцию оператора плотности ρ_A в гильбертовом пространстве $\mathcal{H}_A$, если предположить, что в расширенном гильбертовом пространстве $\mathcal{H}_A \otimes \mathcal{H}_B$ она в действительности является унитарной. Но, даже если эволюция в $\mathcal{H}_A \otimes \mathcal{H}_B$ управляется уравнением Шредингера, этого не достаточно, чтобы обеспечить *локальность* во времени эволюции $\rho_A(t)$. Действительно, если мы знаем только $\rho_A(t)$, мы не имеем полной системы начальных условий для уравнения Шредингера; кроме этого нам необходимо знать состояние «окружения». Так как из общей теории супероператоров известно, что мы вправе потребовать, что в момент времени $t = 0$ квантовым состоянием в пространстве $\mathcal{H}_A \otimes \mathcal{H}_B$ является

$$\rho_A \otimes |0\rangle_{E\,E}\langle 0|, \tag{3.141}$$

то наиболее ярким выражением этой трудности является то, что оператор плотности $\rho_A(t+dt)$ зависит не только от $\rho_A(t)$, но также и от ρ_A в более ранние моменты времени, поскольку резервуар E[1] некоторое время сохраняет память об этой информации и может вернуть ее обратно в систему A.

Это затруднение возникает вследствие того, что информация течет по улице с двухсторонним движением. Открытая система (классическая или квантовая) является *диссипативной*, поскольку информация может перетекать из системы в резервуар. Но это значит, что информация может также течь обратно из резервуара в систему, приводя к немарковским *флуктуациям* в системе[2].

Таким образом, за исключением случая когерентной (унитарной) эволюции, флуктуации неизбежны, а строго марковское описание квантовой динамики невозможно. Тем не менее во многих отношениях марковское описание является хорошим приближением. Ключевая идея здесь в том, что возможно разделение между типичным корреляционным временем флукту-

[1] Обсуждая основное уравнение, окружение обычно называют *резервуаром* в знак уважения к глубоко укоренившейся терминологии статистической физики.

[2] Эта неизбежная связь лежит в основе *флуктуационно-диссипационной теоремы*, мощного инструмента статистической физики.

аций и временным масштабом наблюдаемой нами эволюции. Грубо говоря, мы можем обозначить через $(\Delta t)_{\rm res}$ время, которое требуется резервуару, чтобы «забыть» полученную от системы информацию, — спустя время $(\Delta t)_{\rm res}$ мы можем считать, что информация навсегда потеряна, и пренебрегать возможностью того, что она вновь вернется, чтобы повлиять на дальнейшую эволюцию системы.

Наше описание эволюции системы будет включать в себя «сглаживание» («coarse graining») во времени: мы воспринимаем динамику сквозь фильтр, скрывающий высокочастотную часть движения с $\omega \gg (\Delta t)^{-1}_{\rm coarse}$. Тогда марковское описание должно быть приближенно справедливым, если $(\Delta t)_{\rm res} \ll (\Delta t)_{\rm coarse}$; мы можем пренебречь памятью резервуара, поскольку не в состоянии обнаружить ее влияние. Это «марковское приближение» *полезно*, если временной масштаб наблюдаемой нами динамики велик по сравнению с $(\Delta t)_{\rm coarse}$, например, если временной масштаб затухания $(\Delta t)_{\rm damp}$ удовлетворяет неравенству

$$(\Delta t)_{\rm damp} \gg (\Delta t)_{\rm coarse} \gg (\Delta t)_{\rm res}. \tag{3.142}$$

Это условие часто выполняется на практике, например, в атомной физике, где $(\Delta t)_{\rm res} \sim \hbar/kT \sim 10^{-14}$с ($T$ — температура) по порядку величины больше типичного времени жизни возбужденного состояния.

Поучительным примером является случай, в котором система A представляет собой один гармонический осциллятор ($\mathbf{H}_A = \omega \mathbf{a}^\dagger \mathbf{a}$), а резервуар R состоит из множества гармонических осцилляторов ($\mathbf{H}_R = \sum_i \omega_i \mathbf{b}_i^\dagger \mathbf{b}_i$), слабо связанных с рассматриваемой системой возмущением

$$\mathbf{H}' = \sum_i \lambda_i (\mathbf{a}\mathbf{b}_i^\dagger + \mathbf{a}^\dagger \mathbf{b}_i). \tag{3.143}$$

Гамильтониан резервуара может, например, представлять (свободное) электромагнитное поле, тогда $\mathbf{H}'$ в низшем нетривиальном порядке теории возмущений индуцирует переходы, в которых осциллятор излучает или поглощает один фотон, при этом уменьшая или соответственно увеличивая свое число заполнения $\mathbf{n} = \mathbf{a}^\dagger \mathbf{a}$.

Мы могли бы подойти к основному уравнению, анализируя систему с помощью зависящей от времени теории возмущений, аккуратно вводя конечную обрезающую частоту. Детали этого анализа можно найти в книге Говарда Кармайкла[1]. Однако здесь я хотел бы обойтись без него и перепрыгнуть к основному уравнению более эвристическим путем.

[1] Howard Carmichael, *Open Systems Approach to Quantum Optics*, Springer Verlag, Berlin et al 1993. На русском языке см. Ю. Л. Климонтович *Статистическая теория открытых систем*, тт. 1–3, Янус-К М., 1995–2001; Ю. Л. Климонтович *Введение в физику открытых систем*, Янус-К М., 2002. — *Прим. ред.*

3.5.2. Линдбладиан

При унитарной эволюции изменение матрицы плотности во времени управляется уравнением Шредингера[1]

$$\dot{\boldsymbol{\rho}} = -i\big[\mathbf{H}, \boldsymbol{\rho}\big], \tag{3.144}$$

которое, при не зависящем от времени $\mathbf{H}$, можно формально решить и найти

$$\boldsymbol{\rho}(t) = e^{-i\mathbf{H}t}\boldsymbol{\rho}(0)e^{i\mathbf{H}t}. \tag{3.145}$$

Нашей целью является обобщение этого уравнения на случай марковской, но не унитарной, эволюции, в котором мы будем иметь

$$\dot{\boldsymbol{\rho}} = \mathcal{L}[\boldsymbol{\rho}]. \tag{3.146}$$

Линейный оператор $\mathcal{L}$, порождающий конечный супероператор в том же смысле, в каком гамильтониан $\mathbf{H}$ порождает унитарную эволюцию во времени, будет называться *линдбладианом*. Если $\mathcal{L}$ не зависит от времени, то формальное решение уравнения (3.146) имеет вид

$$\boldsymbol{\rho}(t) = e^{\mathcal{L}t}\boldsymbol{\rho}(0). \tag{3.147}$$

Чтобы вычислить линдбладиан, мы начинаем с уравнения Шредингера для системы, связанной с резервуаром

$$\dot{\boldsymbol{\rho}}_A = \mathrm{tr}_R\left(\dot{\boldsymbol{\rho}}_{AR}\right) = -i\,\mathrm{tr}_R\left(\big[\mathbf{H}_{AR}, \boldsymbol{\rho}_{AR}\big]\right), \tag{3.148}$$

но, как уже отмечалось, мы не ожидаем, что эта формула для $\dot{\boldsymbol{\rho}}_A$ может быть выражена лишь через $\boldsymbol{\rho}_A$. Чтобы найти линдбладиан, необходимо явно воспользоваться марковским приближением (как это делает Кармайкл). С другой стороны, предположим, что марковское приближение применимо. Мы уже знаем, что *наиболее общий* супероператор можно записать в представлении Крауса:

$$\boldsymbol{\rho}_A(t) = \$_t\big[\boldsymbol{\rho}(0)\big] = \sum_{\mu} \mathbf{M}_{\mu}(t)\boldsymbol{\rho}(0)\mathbf{M}_{\mu}^{\dagger}(t), \tag{3.149}$$

причем $\$_{t=0} = \mathbf{1}$. Если пролетевшее время является инфинитезимальным интервалом dt и

$$\boldsymbol{\rho}(dt) = \boldsymbol{\rho}(0) + O(dt), \tag{3.150}$$

[1] В статистической физике это уравнение принято называть квантовым уравнением Лиувилля, хотя, конечно, оно непосредственно выводится из уравнения Шредингера. — *Прим. ред.*

тогда одним из операторов Крауса будет $\mathbf{M}_0 = \mathbf{1} + O(dt)$, а все остальные будут иметь порядок $\sqrt{dt}$. Операторы $\mathbf{M}_\mu$ ($\mu > 0$) описывают «квантовые скачки», которые с вероятностью порядка dt может совершать система. Следовательно, мы можем записать

$$\begin{aligned} \mathbf{M}_\mu &= \sqrt{dt}\mathbf{L}_\mu, \qquad \mu = 1, 2, 3, \ldots, \\ \mathbf{M}_0 &= \mathbf{1} + (-i\mathbf{H} + \mathbf{K})dt, \end{aligned} \tag{3.151}$$

где $\mathbf{H}$ и $\mathbf{K}$ эрмитовы, причем $\mathbf{L}_\mu$, $\mathbf{H}$ и $\mathbf{K}$ имеют нулевой порядок по dt. Фактически, оператор $\mathbf{K}$ можно определить, используя условие нормировки Крауса

$$\mathbf{1} = \sum_\mu \mathbf{M}_\mu^\dagger \mathbf{M}_\mu = \mathbf{1} + dt\left(2\mathbf{K} + \sum_{\mu>0} \mathbf{L}_\mu^\dagger \mathbf{L}_\mu\right), \tag{3.152}$$

или

$$\mathbf{K} = -\frac{1}{2}\sum_{\mu>0} \mathbf{L}_\mu^\dagger \mathbf{L}_\mu. \tag{3.153}$$

Подставляя это в уравнение (3.149), выражая $\boldsymbol{\rho}(dt) = \boldsymbol{\rho}(0) + \dot{\boldsymbol{\rho}}(0)dt$ и сравнивая слагаемые порядка dt, получим уравнение Линдблада[1]:

$$\dot{\boldsymbol{\rho}} - \mathcal{L}[\boldsymbol{\rho}] = -i[\mathbf{H}, \boldsymbol{\rho}] + \sum_{\mu>0}\left(\mathbf{L}_\mu \boldsymbol{\rho} \mathbf{L}_\mu^\dagger - \frac{1}{2}\mathbf{L}_\mu^\dagger \mathbf{L}_\mu \boldsymbol{\rho} - \frac{1}{2}\boldsymbol{\rho}\mathbf{L}_\mu^\dagger \mathbf{L}_\mu\right). \tag{3.154}$$

Первый член в $\mathcal{L}[\boldsymbol{\rho}]$ представляет собой обычное слагаемое Шредингера, генерирующее унитарную эволюцию. Остальные слагаемые описывают возможные переходы, которые может испытывать система, вследствие ее взаимодействия с резервуаром. Операторы $\mathbf{L}_\mu$ называются *операторами Линдблада* или *операторами квантовых скачков*. Каждое слагаемое $\mathbf{L}_\mu \boldsymbol{\rho} \mathbf{L}_\mu^\dagger$ индуцирует один из возможных квантовых скачков, тогда как слагаемые $-\frac{1}{2}\mathbf{L}_\mu^\dagger \mathbf{L}_\mu \boldsymbol{\rho} - \frac{1}{2}\boldsymbol{\rho}\mathbf{L}_\mu^\dagger \mathbf{L}_\mu$ необходимы для корректного описания тех случаев, когда скачки не возникают.

Уравнение Линдблада (3.154) и есть то, что мы искали, общая форма (вполне положительной) марковской эволюции матрицы плотности: то есть основное уравнение. Из представления Крауса, с которого мы начинали, следует, что уравнение Линдблада сохраняет матрицу плотности: $\boldsymbol{\rho}(t+dt)$ — матрица плотности, если таковой является $\boldsymbol{\rho}(t)$. Действительно, используя уравнение (3.154), можно непосредственно проверить,

[1] Уравнение Линдблада, описывающее марковскую эволюцию матрицы плотности открытой системы, получено в работе G. Lindblad, *On the Generators of Quantum Dynamical Semigroups*, Commun. Math. Phys., **48**, 119–130 (1976). – *Прим. ред.*

что $\dot{\rho}$ эрмитов, а $\mathrm{tr}\,\dot{\rho} = 0$. То, что $\mathcal{L}[\rho]$ сохраняет положительность, несколько менее очевидно, но, как уже отмечалось, следует из представления Крауса.

Если мы вспомним связь между представлением Крауса и унитарным представлением супероператора, то интерпретацию основного уравнения можно сделать более прозрачной. Представим, что мы непрерывно контролируем резервуар, проецируя его *в каждый момент времени* на базис $|\mu\rangle_R$. С вероятностью $1 - O(dt)$ резервуар остается в состоянии $|0\rangle_R$, а с вероятностью порядка dt он совершает скачок в одно из состояний $|\mu\rangle_R$ ($\mu > 0$). Говоря, что резервуар «забыл» информацию, полученную от системы (так что применимо марковское приближение), мы считаем, что эти переходы происходят с вероятностями, линейно растущими со временем. Напомним, что это *не следует* автоматически из зависящей от времени теории возмущений. На малых временах t вероятности отдельных переходов пропорциональны t^2; мы получаем темп (дифференцируя «золотое правило Ферми») только после суммирования по непрерывному континууму возможных конечных состояний. Поскольку количество доступных состояний в действительности убывает как $1/t$, просуммированная по конечным состояниям вероятность перехода пропорциональна t. Используя марковское описание динамики, мы явно предполагали, что масштаб времени $(\Delta t)_{\mathrm{coarse}}$ настолько велик, что мы можем приписать частоты различным возможным переходам, которые могут быть обнаружены, пока мы контролируем окружение системы (резервуар). В действительности это следует из требования $(\Delta t)_{\mathrm{coarse}} \gg (\Delta t)_{\mathrm{res}}$.

3.5.3. Затухающий гармонический осциллятор

В качестве примера, иллюстрирующего основное уравнение, рассмотрим взаимодействующий с электромагнитным полем гармонический осциллятор

$$\mathbf{H}' = \sum_i \lambda_i (\mathbf{a}\mathbf{b}_i^\dagger + \mathbf{a}^\dagger \mathbf{b}_i). \tag{3.155}$$

Предположим, что температура резервуара равна нулю; тогда будет наблюдаться падение уровня возбуждения осциллятора, сопровождающееся последовательным излучением фотонов, но поглощения фотонов происходить не будет. Следовательно, имеется только один оператор скачка:

$$\mathbf{L}_1 = \sqrt{\Gamma}\mathbf{a}. \tag{3.156}$$

Здесь Γ представляет собой темп распада первого возбужденного ($n = 1$) состояния осциллятора в основное ($n = 0$) состояние; в соответствии со

структурой гамильтониана $\mathbf{H}'$ темп затухания в результате перехода с n-го уровня на $(n-1)$-й равен $n\Gamma$.[1] Основное уравнение в форме Линдблада приобретает вид

$$\dot{\boldsymbol{\rho}} = -i[\mathbf{H}_0, \boldsymbol{\rho}] + \Gamma\left(\mathbf{a}\boldsymbol{\rho}\mathbf{a}^\dagger - \frac{1}{2}\mathbf{a}^\dagger\mathbf{a}\boldsymbol{\rho} - \frac{1}{2}\boldsymbol{\rho}\mathbf{a}^\dagger\mathbf{a}\right), \tag{3.157}$$

где $\mathbf{H}_0 = \omega\mathbf{a}^\dagger\mathbf{a}$ — гамильтониан осциллятора. Это то же самое уравнение, что и полученное Кармайклом с помощью более изощренного анализа. (Мы не учли здесь только *лэмбовский сдвиг*, или радиационную перенормировку частоты осциллятора, имеющую тот же порядок, что и слагаемые скачков в $\mathcal{L}[\boldsymbol{\rho}]$.)

Слагаемые скачков в основном уравнении описывают *затухание* осциллятора вследствие излучения им фотонов[2]. Чтобы исследовать влияние скачков, удобно перейти к *представлению взаимодействия*; определим операторы $\boldsymbol{\rho}_I$ и $\mathbf{a}_I$ в представлении взаимодействия

$$\begin{aligned}\boldsymbol{\rho}(t) &= e^{-i\mathbf{H}_0 t}\boldsymbol{\rho}_I(t)e^{i\mathbf{H}_0 t},\\ \mathbf{a}(t) &= e^{-i\mathbf{H}_0 t}\mathbf{a}_I(t)e^{i\mathbf{H}_0 t},\end{aligned} \tag{3.158}$$

так что

$$\dot{\boldsymbol{\rho}}_I = \Gamma\left(\mathbf{a}_I\boldsymbol{\rho}_I\mathbf{a}_I^\dagger - \frac{1}{2}\mathbf{a}_I^\dagger\mathbf{a}_I\boldsymbol{\rho}_I - \frac{1}{2}\boldsymbol{\rho}_I\mathbf{a}_I^\dagger\mathbf{a}_I\right), \tag{3.159}$$

где фактически $\mathbf{a}_I(t) = \mathbf{a}e^{-i\omega t}$, следовательно, в правой части уравнения (3.159) можно заменить $\mathbf{a}_I$ на $\mathbf{a}$. В отсутствии затухания переменная $\tilde{\mathbf{a}} = e^{-i\mathbf{H}_0 t}\mathbf{a}e^{i\mathbf{H}_0 t} = \mathbf{a}e^{i\omega t}$ остается постоянной. При наличии затухания $\tilde{\mathbf{a}}$ изменяется в соответствии с уравнением

$$\frac{d}{dt}\langle\tilde{\mathbf{a}}\rangle = \frac{d}{dt}\operatorname{tr}(\mathbf{a}\boldsymbol{\rho}_I) = \operatorname{tr}\mathbf{a}\dot{\boldsymbol{\rho}}, \tag{3.160}$$

а из (3.159) мы имеем

$$\begin{aligned}\operatorname{tr}\mathbf{a}\dot{\boldsymbol{\rho}} &= \Gamma\operatorname{tr}\left(\mathbf{a}^2\boldsymbol{\rho}_I\mathbf{a}^\dagger - \frac{1}{2}\mathbf{a}\mathbf{a}^\dagger\mathbf{a}\boldsymbol{\rho}_I - \frac{1}{2}\mathbf{a}\boldsymbol{\rho}_I\mathbf{a}^\dagger\mathbf{a}\right) =\\ &= \Gamma\operatorname{tr}\left(\frac{1}{2}[\mathbf{a}^\dagger, \mathbf{a}]\mathbf{a}\boldsymbol{\rho}_I\right) = -\frac{\Gamma}{2}\operatorname{tr}(\mathbf{a}\boldsymbol{\rho}_I) = -\frac{\Gamma}{2}\langle\tilde{\mathbf{a}}\rangle.\end{aligned} \tag{3.161}$$

[1] n-е возбужденное состояние осциллятора может интерпретироваться как состояние n невзаимодействующих частиц; его темп затухания равен $n\Gamma$, поскольку исчезнуть при этом может любая из n частиц (квантов).

[2] Эта модель распространяет наше обсуждение канала затухания амплитуды, скорее на затухающий осциллятор, а не на затухающий кубит.

Интегрируя это уравнение, получим

$$\langle \tilde{\mathbf{a}}(t) \rangle = e^{-\Gamma t/2} \langle \tilde{\mathbf{a}}(0) \rangle. \tag{3.162}$$

Аналогично, число заполнения осциллятора $\mathbf{n} = \mathbf{a}^\dagger \mathbf{a} = \tilde{\mathbf{a}}^\dagger \tilde{\mathbf{a}}$ затухает согласно

$$\begin{aligned} \frac{d}{dt}\langle \mathbf{n} \rangle = \frac{d}{dt}\langle \mathbf{a}^\dagger \mathbf{a} \rangle = \operatorname{tr}(\mathbf{a}^\dagger \mathbf{a} \boldsymbol{\rho}_I) = \\ = \Gamma \operatorname{tr} \left(\mathbf{a}^\dagger \mathbf{a}^2 \boldsymbol{\rho}_I \mathbf{a}^\dagger - \frac{1}{2} \mathbf{a}^\dagger \mathbf{a} \mathbf{a}^\dagger \mathbf{a} \boldsymbol{\rho}_I - \frac{1}{2} \mathbf{a}^\dagger \mathbf{a} \boldsymbol{\rho}_I \mathbf{a}^\dagger \mathbf{a} \right) = \\ = \Gamma \operatorname{tr} \mathbf{a}^\dagger [\mathbf{a}^\dagger, \mathbf{a}] \mathbf{a} \boldsymbol{\rho}_I = -\Gamma \operatorname{tr} \mathbf{a}^\dagger \mathbf{a} \boldsymbol{\rho}_I = -\Gamma \langle \mathbf{n} \rangle, \end{aligned} \tag{3.163}$$

что после интегрирования дает

$$\langle \tilde{\mathbf{n}}(t) \rangle = e^{-\Gamma t} \langle \tilde{\mathbf{n}}(0) \rangle. \tag{3.164}$$

Таким образом, Γ представляет собой темп затухания осциллятора. Мы можем интерпретировать n-е возбужденное состояние осциллятора как состояние n невзаимодействующих частиц, каждая из которых распадается с отнесенной к единице времени вероятностью Γ; следовательно, уравнение (3.164) и есть тот самый экспоненциальный закон, которому удовлетворяет численность популяции распадающихся частиц.

Более интересно то, что говорит основное уравнение о декогерентизации. Детали этого анализа будут в домашнем задании. А здесь мы проанализируем более простую задачу — осциллятор, испытывающий затухание фазы.

3.5.4. Затухание фазы

Чтобы смоделировать затухание фазы гармонического осциллятора, возьмем другую связь осциллятора с резервуаром:

$$\mathcal{H}' = \left(\sum_i \lambda_i \mathbf{b}_i^\dagger \mathbf{b}_i \right) \mathbf{a}^\dagger \mathbf{a}. \tag{3.165}$$

Таким образом, существует только один оператор Линдблада, а основное уравнение в представлении взаимодействия имеет вид

$$\dot{\boldsymbol{\rho}}_I = \Gamma \left(\mathbf{a}^\dagger \mathbf{a} \boldsymbol{\rho}_I \mathbf{a}^\dagger \mathbf{a} - \frac{1}{2} (\mathbf{a}^\dagger \mathbf{a})^2 \boldsymbol{\rho}_I - \frac{1}{2} \boldsymbol{\rho}_I (\mathbf{a}^\dagger \mathbf{a})^2 \right). \tag{3.166}$$

Здесь Γ может интерпретироваться как частота (отнесенная к единице времени вероятность), с которой фотоны резервуара *рассеиваются* осциллятором, находящимся в первом возбужденном состоянии. Если число заполнения равно n, то частота рассеяния становится равной $n^2\Gamma$. Причина появления множителя n^2 состоит в том, что все вклады в амплитуду рассеяния от каждой из n осцилляторных «частиц» складываются когерентно; амплитуда пропорциональна n, а частота (темп) — n^2.

Уравнение для $\boldsymbol{\rho}_I$ (3.166) легко решить в базисе чисел заполнения. Разлагая

$$\boldsymbol{\rho}_I = \sum_{n,m} \rho_{nm} |n\rangle\langle m| \tag{3.167}$$

(где $\mathbf{a}^\dagger \mathbf{a}|n\rangle = n|n\rangle$), запишем основное уравнение в виде

$$\dot{\rho}_{nm} = \Gamma \left(nm - \frac{1}{2}n^2 - \frac{1}{2}m^2 \right) \rho_{nm} = -\frac{\Gamma}{2}(n-m)^2 \rho_{nm}. \tag{3.168}$$

Его интегрирование дает

$$\rho_{nm}(t) = \rho_{nm}(0) \exp\left[-\frac{1}{2}\Gamma t (n-m)^2 \right]. \tag{3.169}$$

Если мы приготовим подобную «кот-состоянию» суперпозицию собственных состояний оператора чисел заполнения с большой разницей значений n

$$|\mathrm{cat}\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + |n\rangle\big), \qquad n \gg 1, \tag{3.170}$$

то недиагональные элементы матрицы плотности будут затухать как $\exp\left(-\Gamma n^2 t/2\right)$. Фактически это точно такой же тип поведения, что и обнаруженный нами при анализе затухания фазы одного кубита. Темп декогерентизации равен $n^2\Gamma$, так как он равен частоте рассеяния фотонов резервуара осциллятором, возбужденным в состояние $|n\rangle$. Как и ранее, мы видим также, что декогерентизация фазы выбирает предпочтительный базис. Она возникает в базисе собственных состояний оператора чисел заполнения, поскольку это именно тот оператор, который входит в связь осциллятора с резервуаром $\mathbf{H}'$.

Вернемся к затуханию амплитуды. Поскольку в нашей модели затухания амплитуды в связь осциллятора с резервуаром $\mathbf{H}'$ входит оператор уничтожения $\mathbf{a}$ (и сопряженный ему оператор рождения $\mathbf{a}^\dagger$), то можно предположить, что декогерентизация возникает в базисе собственных состояний

оператора $\mathbf{a}$. *Когерентное состояние*

$$|\alpha\rangle = e^{-|\alpha|^2/2} e^{\alpha \mathbf{a}^\dagger} |0\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \tag{3.171}$$

представляет собой собственное состояние оператора $\mathbf{a}$, отвечающее собственному значению α. Два когерентных состояния с разными собственными значениями α_1 и α_2 не ортогональны друг другу:

$$|\langle \alpha_1 | \alpha_2 \rangle|^2 = e^{-|\alpha_1|^2} e^{-|\alpha|_2^2} e^{2\mathrm{Re}(\alpha_1^* \alpha_2)} = \exp\left(-|\alpha_1 - \alpha_2|^2\right), \tag{3.172}$$

следовательно, перекрытие очень мало при большой величине $|\alpha_1 - \alpha_2|^2$.

Представим, что мы приготовили «кот-состояние»

$$|\mathrm{cat}\rangle = \frac{1}{\sqrt{2}} \left(|\alpha_1\rangle + |\alpha_2\rangle \right), \tag{3.173}$$

суперпозицию когерентных состояний с $|\alpha_1 - \alpha_2| \gg 1$. Вы покажете (в домашнем упражнении), что недиагональные элементы матрицы плотности $\boldsymbol{\rho}$ затухают как

$$\exp\left(-\frac{\Gamma t}{2} |\alpha_1 - \alpha_2|^2 \right) \tag{3.174}$$

(при $\Gamma t \ll 1$). Таким образом, темп декогерентизации

$$\Gamma_{\mathrm{dec}} = \frac{1}{2} |\alpha_1 - \alpha_2|^2 \Gamma_{\mathrm{damp}} \tag{3.175}$$

огромен по сравнению с темпом затухания. Такое поведение также легко интерпретируется. В когерентном состоянии ожидаемое значение числа заполнения равно $\langle \alpha | \mathbf{a}^\dagger \mathbf{a} | \alpha \rangle = |\alpha|^2$. Следовательно, если $\alpha_{1,2}$ сравнимы по модулю, но имеют существенно разные фазы (как в суперпозиции волновых пакетов с минимальной неопределенностью, центрированных в точках x и $-x$), темп декогерентизации имеет порядок темпа эмиссии *одного* фотона. Он очень велик по сравнению с темпом диссипации значительной части энергии осциллятора.

Аналогично можно рассмотреть осциллятор, связанный с резервуаром, находящимся при конечной температуре. Вновь темп декогерентизации будет иметь порядок частоты излучения или поглощения одного фотона, но теперь она гораздо выше, чем при нулевой температуре. Поскольку фотонные моды с частотой, сравнимой с частотой осциллятора ω, имеют термически равновесное число заполнения

$$n_\gamma = \frac{T}{\hbar \omega} \tag{3.176}$$

(при $T \gg \hbar\omega$), то интенсивность взаимодействия увеличивается множителем n_γ. Тогда мы имеем

$$\frac{\Gamma_{\rm dec}}{\Gamma_{\rm damp}} \sim n_{\rm osc} n_\gamma \sim \frac{E}{\hbar\omega}\frac{T}{\hbar\omega} \sim \frac{m\omega_2 x^2}{\hbar\omega}\frac{T}{\hbar\omega} \sim x^2\frac{mT}{\hbar^2} \sim \frac{x^2}{\lambda_T^2}, \qquad (3.177)$$

где x – амплитуда осцилляций, а λ_T – тепловая длина волны де Бройля. Декогерентизация протекает *очень быстро*.

3.6. В чем проблема? (Здесь есть проблема?)

Наш обзор оснований квантовой теории почти завершен. Но прежде чем мы займемся своим главным делом, кратко проанализируем состояние этих оснований. Находится ли квантовая теория в «хорошей форме» или в ее корнях имеются фундаментальные проблемы, до сих пор требующие своего решения?

Одной такой потенциально серьезной проблемой, впервые упомянутой в § 2.1, является *проблема измерения*. Мы отмечали странный дуализм, присущий аксиомам квантовой теории. Существует два способа изменения квантового состояния: *детерминистская унитарная эволюция* и *вероятностное измерение*. Но почему измерение должно принципиально отличаться от любого другого физического процесса? Этот дуализм вселяет в некоторых людей подозрение, что современная формулировка квантовой теории все еще не полна.

В этой главе мы многое узнали об измерениях. В § 3.1.1 мы обсудили, как унитарная эволюция может привести к появлению корреляций (запутывания) между системой и «переменной-указателем» измерительного прибора. Таким образом, чистое состояние системы может эволюционировать в смешанное (после взятия следа по состояниям «указателя»), которое допускает интерпретацию как *ансамбля* взаимно ортогональных чистых состояний (собственных состояний оператора плотности рассматриваемой системы), каждое из которых возникает с вполне определенной вероятностью. Таким образом, уже в этом простом высказывании заложены зерна более глубокого понимания того, как исключительно в рамках унитарной эволюции может возникнуть «коллапс» (редукция) вектора состояния. С другой стороны, в § 2.5 мы говорили о том, что интерпретация матрицы плотности как ансамбля неоднозначна. В § 2.5.5 мы особенно ясно видели, что если мы способны измерить «указатель» в любом понравившемся нам базисе, то мы можем приготовить систему в любом из множества «экзотических» состояний, суперпозиций собственных состояний системы ρ (теоре-

ма ЖХЙВ). Следовательно, редукция (*разрушающая* относительные фазы состояний в суперпозиции) не может быть объяснена одним только запутыванием.

В § 3.4 и § 3.5 мы изучали другой важный аспект процесса измерения — *декогерентизацию*. Главная идея состоит в том, что в случае макроскопических систем мы не можем надеяться уследить за всеми микроскопическими степенями свободы. Нам приходится довольствоваться *сглаженным* (*coarse-grained*) описанием, получающимся в результате взятия следа по множеству ненаблюдаемых переменных. В случае макроскопического измерительного прибора мы должны взять след по степеням свободы окружения, с которым прибор неизбежно взаимодействует. Тогда мы обнаружим, что прибор исключительно быстро релаксирует в некоторый предпочтительный базис, определяемый природой связи прибора с его окружением. Похоже, что особенностью гамильтониана Вселенной является то, что фундаментальные взаимодействия хорошо локализованы в пространстве, следовательно, избираемый в процессе декогерентизации базис также хорошо локализован в пространстве. Кот или жив или мертв, а не в суперпозиции состояний $1/\sqrt{2}(|\text{alive}\rangle + |\text{dead}\rangle)$.

Вычисляя след по степеням свободы окружения, мы получаем более полную картину процесса измерения, «редукции». Наша система запутывается с прибором, который, в свою очередь, запутан с окружением. Если мы рассматриваем микросостояние окружения, как недоступное в любой момент времени, то мы вправе говорить, что измерение состоялось. Относительные фазы базисных состояний системы безвозвратно потеряны — ее вектор состояния коллапсировал.

Конечно, с принципиальной точки зрения никакой реальной потери информации о фазах нет. Эволюция системы+прибора+окружения является унитарной и детерминистской. В принципе мы, вероятно, могли бы выполнить в высшей степени нелокальное измерение окружающей среды и восстановить якобы разрушенную фазовую информацию о системе. В этом смысле наше объяснение коллапса, по выражению Белла, годится только «для всех практических целей» (FAPP: «for all practical purposes»). После «измерения» когерентность системы базисных состояний в принципе могла бы быть восстановлена (мы могли бы обратить измерение с помощью «квантового удаления»), но осуществление такого измерения в высшей степени невероятно. В самом деле, коллапс имеет место только «для всех практических целей» (хотя, вероятно, мы могли бы доказать в космологическом смысле, что некоторые измерения действительно принципиально необратимы), но существует ли то, что достойно быть не «для всех практических целей»?

Нашей целью в физике является объяснение наблюдаемых явлений на основе как можно более простых моделей. Не нужно постулировать два фундаментальных процесса (унитарная эволюция *и* измерение), если существенным является только один из них (унитарная эволюция). Тогда примем, по крайней мере временно, такую гипотезу:

Эволюция *замкнутой* квантовой системы *всегда унитарна*.

Конечно, мы видели, что не все супероператоры унитарны. Суть гипотезы в том, что неунитарная эволюция *открытой* системы, в том числе и происходящая в процессе измерения редукция, всегда возникает в результате игнорирования некоторых степеней свободы большей системы. Эта точка зрения была провозглашена Хьюго Эвереттом в 1957 г[1]. Согласно ей эволюция квантового состояния Вселенной является действительно детерминистской!

Но даже если мы согласимся с тем, что редукция объясняется декогерентизацией в системе, то есть на самом деле является детерминированной, мы не избавимся от всех загадок квантовой теории. Для волновой функции Вселенной фактически существует суперпозиция состояния, в котором кот мертв, и состояния, в котором кот жив. Несмотря на это, всякий раз, когда я наблюдаю за котом, он либо жив, либо мертв. Оба исхода возможны, но только один из них реализуется в действительности. Почему это так?

Ваш ответ на этот вопрос может зависеть от вашего понимания квантовой теории. Существует (по меньшей мере) два приемлемых направления рассуждений.

Платоник: Физика описывает *реальность*. В квантовой теории «волновая функция Вселенной» представляет полное описание физической реальности.

Позитивист: Физика описывает наши *ощущения*. Волновая функция кодирует состояние наших знаний, а задача квантовой теории – дать по возможности наилучшие предсказания относительно будущего на основе текущего уровня наших знаний.

Я верю в реальность. Я думаю, что мои доводы прагматичны. Как физик, я стремлюсь к наиболее экономичной модели, «объясняющей» то, что я воспринимаю. По крайней мере для физика, простейшим предположением является то, что мои (и ваши) ощущения скоррелированы с лежащей в их

[1] H. Everett, III *"Relative State" Formulation of Quantum Mechanics*, Rev. Mod. Phys., **29**, 454–462 (1957). — *Прим. ред.*

основе внешней по отношению ко мне реальностью. Серьезному философу эта онтология может показаться безнадежно наивной. Однако я предпочитаю верить в реальность, поскольку это предположение выглядит простейшим из тех, что могли бы успешно объяснить мои ощущения. (В подобном же духе я предпочитаю верить, что наука представляет нечто большее, чем просто консенсус. Я верю, что наука способствует прогрессу и приближает нас к удовлетворительному пониманию Природы — законы физики открыты, а не придуманы. Я верю в это, потому что это наиболее простое объяснение того, почему ученые так легко приходят к взаимопониманию.)

Те, кто придерживается другой точки зрения (даже если существует объективная реальность, вектор состояния описывает не ее, а всего лишь уровень наших знаний о ней), склонны считать, что современная формулировка квантовой теории не вполне удовлетворительна, что существует более глубокое описание, все еще ждущее своего открытия. Пока вы не сможете убедить меня в обратном, мне представляется более разумным предполагать, что волновая функция дает описание реальности.

Если мы полагаем, что волновая функция описывает реальность, и *если* принимаем точку зрения Эверетта, что вся эволюция является унитарной, *то* мы обязаны признать, что все возможные исходы измерения имеют одинаковое право быть «реальными». Как тогда понять, почему в эксперименте реализуется только *один* результат — кот или жив или мертв.

На самом деле здесь нет никакого парадокса, если только мы (в духе интерпретации Эверетта) готовы включить и себя в квантовую систему, описываемую волновой функцией. Эта волновая функция описывает все возможные корреляции между подсистемами, в том числе между котом и состоянием моего сознания. Если мы приготовили «кот-состояние», а затем наблюдаем за ним, то оператор плотности (после взятия следа по всем внешним степеням свободы) приобретает вид

$$\begin{aligned} &|\text{decay}\rangle_{\text{atom}}|\text{dead}\rangle_{\text{cat}}|\text{know it's dead}\rangle_{\text{me}}, \qquad \left(\text{Prob} = \frac{1}{2}\right), \\ &|\text{no decay}\rangle_{\text{atom}}|\text{alive}\rangle_{\text{cat}}|\text{know it's alive}\rangle_{\text{me}}, \qquad \left(\text{Prob} = \frac{1}{2}\right). \end{aligned} \tag{3.178}$$

Эта матрица плотности ρ описывает две альтернативы, но в обоих случаях я имею точное знание о состоянии здоровья кота. Я *никогда* не вижу его полуживым-полумертвым. (В соответствии с опытом, я нахожусь в собственном состоянии «оператора определенности».)

Допуская, что волновая функция описывает реальность и что вся эволюция является унитарной, мы приходим к интерпретации квантовой теории на основе «множественности миров». В этой картине всякий раз, когда

совершается «измерение», волновая функция Вселенной «расщепляется» на две ветви, соответствующие двум возможным исходам. После множества измерений существует множество ветвей (множество миров), каждая из которых с одинаковым правом может описывать реальность. Это размножение миров выглядит насмешкой над нашим намерением разработать наиболее экономичное описание. Но мы следуем одной конкретной ветви и для предсказания того, что мы увидим в следующий момент, множество других миров не имеет значения. Размножение миров ничего нам не стоит. «Множественность миров» может показаться странной, но стоит ли удивляться тому, что полное описание реальности — нечто находящегося полностью за пределами нашего опыта, кажется нам странным?

Включив себя в реальность, описываемую волновой функцией, мы поняли, почему мы воспринимаем определенный результат измерения, но по-прежнему стоит следующий вопрос: «Каким образом в этот (детерминистский) формализм входит понятие *вероятности*?» Этот вопрос продолжает беспокоить, для ответа на него мы должны быть готовы точно сформулировать, что значит «с вероятностью»?

Слово «вероятность» используется в двух различных смыслах. Иногда *вероятность* означает *частоту*. Мы говорим, что вероятность того, что монета выпадет орлом вверх равна $1/2$, если мы ожидаем, что при многократном подбрасывании монеты число выпадений орла, деленное на полное число подбрасываний, сходится к $1/2$. (Это, однако, ненадежное понятие; даже если вероятность равна $1/2$, монета все равно *может* выпасть орлом триллион раз подряд.) При строгом математическом обсуждении теория вероятностей часто формулируется как раздел теории меры — она занимается свойствами бесконечных последовательностей.

Но в повседневной практике, а также в квантовой теории, вероятности обычно *не* являются частотами. Когда мы выполняем измерение, мы не можем повторить его бесконечное число раз на идентично приготовленных системах. С точки зрения Эверетта, или с космологической, существует только одна Вселенная, а не множество одинаково приготовленных ее копий.

Так что же такое вероятность? На практике это число, которое дает количественное определение достоверности утверждения при данном состоянии знаний. Возможно, это удивительно, что такое представление можно положить в основу хорошо определенной математической теории, иногда называемой «бейесовским» подходом к вероятности. Термин «бейесовский» отражает теоретико-вероятностный метод, обычно используемый (в науке и в повседневной практике) для проверки гипотезы при наличии некоторых результатов наблюдения. Проверка гипотезы выполняется с ис-

пользованием правила Бейеса для условной вероятности:

$$P(A_0|B) = P(B|A_0)P(A_0)/P(B). \tag{3.179}$$

Предположим, например, что A_0 — приготовление частного квантового состояния, а B — частный результат измерения состояния. Мы выполнили измерение (получение B) и теперь хотим сделать заключение о том, какое состояние было приготовлено (вычислить $P(A_0|B)$). Квантовая механика позволяет нам вычислить $P(B|A_0)$, но она ничего не говорит о $P(A_0)$ (или $P(B)$). Мы делаем предположение *относительно* $P(A_0)$, что возможно, если принять «принцип безразличия»: если неизвестно, что более или менее вероятно, A_i или A_j, то предполагается, что $P(A_i) = P(A_j)$. Как только множество приготовлений определено, мы можем вычислить

$$P(B) = \sum_i P(B|A_i)P(A_i) \tag{3.180}$$

и, следовательно, применяя правило Бейеса, получить $P(A_0|B)$.

Но если мы будем считать, что теория вероятностей дает количественное определение достоверности при данном состоянии знаний, то мы обязаны спросить «при состоянии чьих знаний»? Чтобы построить объективную теорию, мы должны интерпретировать вероятность в квантовой теории не как предсказание, основанное на нашем *текущем* состоянии знаний, а скорее как предсказание, основанное на самом полном *возможном* знании о квантовом состоянии. Если мы готовим состояние $|\uparrow_x\rangle$, а измеряем σ_3, то мы говорим, что с вероятностью $1/2$ результатом является $|\uparrow_z\rangle$, не потому, что это лучшее предсказание, которое можно сделать, опираясь на то, что нам известно, а потому, что это лучшее предсказание, которое *кто-либо* может сделать, независимо от того, как много он знает. В этом смысле результат истинно *случайный*; его невозможно предсказать с уверенностью, даже если наше знание является полным (в *противоположность* псевдослучайности, возникающей в классической физике вследствие неполноты наших знаний).

Как же теперь нам извлечь вероятности из детерминистской Вселенной Эверетта? Вероятности возникают, потому что мы (часть системы) не можем с уверенностью предсказать наше будущее. Я знаю формализм, мне известны гамильтониан и волновая функция Вселенной, я знаю свою ветвь волновой функции. Теперь я собираюсь следить за котом. Мгновение спустя я буду определенно знать, что кот мертв, или я буду уверен в том, что он жив. Даже со всеми своими знаниями я не могу предсказать будущее. Даже имея полное знание о настоящем, невозможно сказать, каким будет состояние моего знания после того, как я понаблюдаю за котом. Самое лучшее,

что я могу, это приписать вероятности результатам. Итак, несмотря на то, что волновая функция Вселенной детерминистская, я, как часть системы, не способен на большее, чем делать вероятностные предсказания.

Конечно, главным героем этой истории является *декогерентизация*. Мы можем последовательно приписать вероятности альтернативам Dead и Alive, если только интерференция между ними невозможна (или по крайней мере пренебрежима). Вероятности имеют смысл, только когда мы можем исчерпывающим образом идентифицировать множества взаимно исключающих альтернатив. Поскольку это сложный вопрос, реально ли возникновение интерференции в более позднее время, мы не можем решить, приемлема ли теория вероятностей, рассматривая квантовое состояние в данный момент времени; мы должны проверить множество взаимно исключающих (сглаженных) историй или последовательностей событий. Существует утонченная техника («функционалы декогерентизации») определения того, являются ли различные истории в достаточной степени некогерентными, чтобы им можно было корректно приписать вероятности.

Итак, позицию Эверетта *можно* примирить с наблюдаемым квантовым индетерминизмом, однако, насколько я понимаю, в этой картине остается тревожащее белое пятно. Я собираюсь наблюдать за котом, и я знаю, что мгновение спустя матрица плотности примет вид

$$\begin{aligned} |\text{dead}\rangle_{\text{cat}}|\text{know it's dead}\rangle_{\text{me}}, \qquad & \text{Prob} = p_{\text{dead}}, \\ |\text{alive}\rangle_{\text{cat}}|\text{know it's alive}\rangle_{\text{me}}, \qquad & \text{Prob} = p_{\text{alive}}. \end{aligned} \tag{3.181}$$

Но как я узнаю, что p_{dead} и p_{alive} действительно являются теми вероятностями, которые я (в моей бейесовской картине) могу приписать своим будущим ощущениям? Мне *по-прежнему* необходимо правило преобразования этого оператора плотности в приписываемые альтернативам вероятности. *Предположение* о таком правиле выглядит противоречащим философии Эверетта; мы предпочли бы сказать, что единственным правилом, необходимым для формулировки теории, является уравнение Шредингера (и, возможно, предписание, указывающее начальную волновую функцию). Постулирование формулы вероятности находится в опасной близости к допущению, что, в конце концов, существует недетерминированный процесс измерения. Это сложная, касающаяся фундамента теории, проблема, полностью удовлетворительного решения которой я не знаю.

Поскольку, касаясь природы вероятности в квантовой теории, мы не в состоянии полностью избавиться от замешательства, может быть, полезно прокомментировать интересное предложение Хартла. Чтобы осуществить его предложение, мы должны вернуться (возможно, с сожалением) к ча-

стотной интерпретации вероятности. Идея Хартла состоит в том, что нам не нужно считать интерпретацию вероятности как часть постулата об измерении. На самом деле достаточно сделать более слабое предположение:

> Если мы готовим квантовое состояние $|a\rangle$ такое, что $\mathbf{A}|a\rangle = a|a\rangle$, и сразу вслед за этим измеряем $\mathbf{A}$, то результатом измерения является a.

Это выглядит как предположение о том, что во Вселенной Эверетта действует бейесовский подход. Я собираюсь измерить наблюдаемую, и волновая функция будет ветвиться, но если наблюдаемая имеет *одно и то же* значение в каждой ветви, то я *могу* предсказать результат.

Чтобы реализовать частотную интерпретацию вероятности, нам следует, строго говоря, рассмотреть бесконечное множество испытаний. Допустим, мы хотим сделать утверждение относительно вероятности получения результата $|\uparrow_z\rangle$ при измерении $\boldsymbol{\sigma}_3$ в состоянии

$$|\psi\rangle = a|\uparrow_z\rangle + b|\downarrow_z\rangle. \tag{3.182}$$

Тогда мы должны представить, что приготовлено бесконечное число копий, то есть состояние имеет вид

$$|\psi^{(\infty)}\rangle \equiv \big(|\psi\rangle\big)^{\infty} = |\psi\rangle \otimes |\psi\rangle \otimes |\psi\rangle \otimes \cdots, \tag{3.183}$$

и мы мысленно представляем измерение $\boldsymbol{\sigma}_3$ в каждой из копий. Формально случай бесконечного числа испытаний можно сформулировать как N испытаний в пределе $N \to \infty$.

Идея Хартла состоит в том, чтобы рассматривать оператор «среднего спина»

$$\bar{\boldsymbol{\sigma}}_3 = \lim_{N\to\infty} \frac{1}{N} \sum_{i=1}^{N} \boldsymbol{\sigma}_3^{(i)}, \tag{3.184}$$

и доказывать, что $\big(|\psi\rangle\big)^N$ при $N \to \infty$ стремится к *собственному состоянию* оператора $\bar{\sigma}_3$ с собственным значением $|a|^2 - |b|^2$. Тогда мы можем, ссылаясь на слабый постулат измерения, сделать вывод, что измерение $\bar{\boldsymbol{\sigma}}_3$ наверняка даст результат $|a|^2 - |b|^2$, и, следовательно, $|a|^2$ равно той части наших спинов, которые ориентированы вверх. В этом смысле, $|a|^2$ является вероятностью того, что измерение $\boldsymbol{\sigma}_3$ дает результат $|\uparrow_z\rangle$.

Рассмотрим в качестве примера частный случай

$$|\psi_x^{(N)}\rangle \equiv \big(|\uparrow_x\rangle\big)^N = \left[\frac{1}{\sqrt{2}}\big(|\uparrow_z\rangle + |\downarrow_z\rangle\big)\right]^N. \tag{3.185}$$

Мы можем вычислить

$$\langle\psi_x^{(N)}|\bar{\sigma}_3|\psi_x^{(N)}\rangle = 0,$$

$$\langle\psi_x^{(N)}|\bar{\sigma}_3^2|\psi_x^{(N)}\rangle = \frac{1}{N^2}\left\langle\psi_x^{(N)}\left|\sum_{ij}\sigma_3^{(i)}\sigma_3^{(j)}\right|\psi_x^{(N)}\right\rangle =$$

$$= \frac{1}{N^2}\sum_{ij}\delta_{ij} = \frac{N}{N^2} = \frac{1}{N}. \qquad (3.186)$$

Формально переходя к пределу при $N \to \infty$, мы приходим к выводу, что $\bar{\sigma}_3$ имеет исчезающую дисперсию вокруг его среднего значения $\langle\bar{\sigma}_3\rangle = 0$, следовательно, по крайней мере в этом смысле, $|\psi_x^{(\infty)}\rangle$ является «собственным состоянием» оператора $\bar{\sigma}_3$ с нулевым собственным значением.

Коулмен и Лесниевски отметили, что в доказательстве Хартла можно пойти дальше и показать, что результат измерения $|\uparrow_z\rangle$ не только появляется с правильной частотой, но что результаты $|\uparrow_z\rangle$ *случайным образом распределены*. Чтобы придать смысл этому утверждению, мы должны сформулировать определение случайности. Мы говорим, что бесконечная последовательность битов случайна, если она *несжимаема*; нет проще способа генерировать первые N битов, чем просто выписать их. Мы формализуем эту идею, рассматривая длину кратчайшей компьютерной программы (для некоторого компьютера), генерирующей первые N битов последовательности. Тогда для случайного ряда

$$\text{длина кратчайшей программы} > N - \text{const}, \qquad (3.187)$$

где константа может зависеть от конкретного используемого компьютера или от конкретной последовательности, но не от N.

Коулмен и Лесниевски рассмотрели ортогональный проекционный оператор $\mathbf{E}_{\text{random}}$, действие которого на $|\psi\rangle$ — собственное состояние оператора $\sigma_3^{(i)}$ удовлетворяет условиям

$$\mathbf{E}_{\text{random}}|\psi\rangle = |\psi\rangle, \qquad (3.188)$$

если последовательность собственных значений $\sigma_3^{(i)}$ случайна, и

$$\mathbf{E}_{\text{random}}|\psi\rangle = 0, \qquad (3.189)$$

если эта последовательность не случайна. Одного этого свойства недостаточно для определения того, как $\mathbf{E}_{\text{random}}$ действует на всем пространстве $(\mathcal{H}_2)^\infty$, но с учетом дополнительного, имеющего технический характер, предположения они нашли, что $\mathbf{E}_{\text{random}}$ существует, единственный

и обладает свойством

$$\mathbf{E}_{\text{random}}|\psi_x^{(\infty)}\rangle = |\psi_x^{(\infty)}\rangle. \tag{3.190}$$

Таким образом, мы «также можем сказать», что $|\psi_x^{(\infty)}\rangle$ является случайным, что касается измерений σ_3, — процедура, отличающая случайные состояния от неслучайных, которая прекрасно работает для последовательности собственных значений оператора σ_3, столь же надежно будет идентифицировать $|\psi_x^{(\infty)}\rangle$ как случайный вектор.

Эти аргументы интересны, но они не приносят мне полного удовлетворения. Больше всего беспокоит необходимость рассматривать бесконечные последовательности (общая черта любой частотной интерпретации вероятности). При любом конечном N мы не можем применить ослабленный постулат измерения Хартла, и даже в пределе $N \to \infty$ применение этого постулата содержит некоторые тонкости. Желательно было бы иметь *усиленный* слабый постулат измерения, применимый к конечному N, но я не знаю, как сформулировать такой постулат или как его объяснить.

В заключение: Физика должна описывать объективный физический мир, и лучшим из известных нам представлений физической реальности является квантово-механическая волновая функция. Физика должна стремиться объяснять все наблюдаемые явления как можно более экономично, в частности, не апеллируя к постулату, что процесс измерения управляется иными динамическими принципами, нежели другие процессы. К счастью, все, что мы знаем о физике, совместимо с гипотезой о том, что все физические процессы (в том числе измерения) могут быть точно смоделированы унитарной эволюцией волновой функции (или матрицы плотности). Если микроскопическая квантовая система взаимодействует с макроскопическим прибором, то «для всех практических целей» декогерентизация вызывает «коллапс» волновой функции.

Если мы избегаем рассматривать измерение как некий таинственный процесс и принимаем волновую функцию в качестве описания физической реальности, то это ведет нас к Эверетту или интерпретации квантовой теории с позиции «множественности миров». Согласно этой точке зрения все возможные исходы любого «измерения» рассматриваются как «реальные» — но я воспринимаю только один результат, поскольку состояние моего мозга (как части квантовой системы) сильно скоррелировано с ним.

Несмотря на то, что эволюция волновой функции в интерпретации Эверетта является детерминистской, у меня нет возможности однозначно предсказать результат выполняемого в будущем эксперимента — я не знаю, в какой ветви волновой функции окажусь после него, следовательно, я не в состоянии предсказать будущее состояние моего разума. Таким образом,

хотя «глобальная» картина в известной степени детерминистская, из моего собственного локального вида изнутри системы я ощущаю квантово-механическую случайность.

Мой личный взгляд состоит в том, что эверettовская интерпретация квантовой теории дает удовлетворительное объяснение измерения и природы случайности, но все еще не дает полного объяснения квантово-механических правил вычисления вероятностей. Для полного объяснения следует выйти за рамки частотной интерпретации вероятности — в идеале хотелось бы поставить бейесовский взгляд на вероятность на надежное объективное основание.

3.7. Резюме

ПОЗМ. Если мы ограничиваем наше внимание подпространством более широкого гильбертова пространства, то ортогональное измерение (измерение фон Неймана), выполненное в более широком пространстве, вообще говоря, не может быть описано как ортогональное измерение в подпространстве. Это скорее *обобщенное измерение* или *ПОЗМ*, результат которого появляется с вероятностью

$$\mathrm{Prob}(a) = \mathrm{tr}\,(\mathbf{F}_a \rho), \tag{3.191}$$

где ρ — матрица плотности подсистемы, $\mathbf{F}_a$ — положительные эрмитовы операторы, удовлетворяющие условию

$$\sum_a \mathbf{F}_a = \mathbf{1}. \tag{3.192}$$

ПОЗМ в $\mathcal{H}_A$ может быть реализована как унитарное преобразование на тензорном произведении $\mathcal{H}_A \otimes \mathcal{H}_B$ после ортогонального измерения в $\mathcal{H}_B$.

Супероператор. Унитарная в $\mathcal{H}_A \otimes \mathcal{H}_B$ эволюция в общем случае не будет выглядеть унитарной, если мы ограничим свое внимание только пространством $\mathcal{H}_A$. Скорее эволюция в $\mathcal{H}_A$ будет описываться *супероператором* (который обратим только тогда, когда он унитарен). Произвольный супероператор $ имеет представление операторной суммы (представление Крауса)

$$\$: \rho \to \$(\rho) = \sum_\mu \mathbf{M}_\mu \rho \mathbf{M}_\mu^\dagger, \tag{3.193}$$

где

$$\sum_\mu \mathbf{M}_\mu^\dagger \mathbf{M}_\mu = \mathbf{1}. \tag{3.194}$$

Фактически любое разумное (линейное и вполне положительное) отображение матриц плотности в матрицы плотности имеет унитарное представление и представление операторной суммы.

Декогерентизация. Декогерентизация – разрушение квантовой информации вследствие взаимодействия системы с ее окружением – может быть описана супероператором. Если окружение часто «рассеивает» систему и его состояние не контролируется, тогда в некотором выделенном базисе (обычно, в соответствии с природой связи системы с окружением, выбирается пространственно-локализованный базис) недиагональные элементы матрицы плотности системы быстро затухают. Временной масштаб декогерентизации определяется частотой рассеяния, которая может быть гораздо больше темпа затухания состояния.

Основное уравнение. Когда соответствующий динамический временной масштаб открытой квантовой системы велик по сравнению со временем, в течение которого окружение «забывает» квантовую информацию, эволюция системы эффективно локальна во времени (марковское приближение). Подобно тому как общая унитарная эволюция генерируется гамильтонианом, общая марковская эволюция генерируется *супероператором Линдблада* $\mathcal{L}$, как это описывается *основным уравнением*

$$\dot{\rho} = \mathcal{L}\rho = -i[\mathbf{H}, \rho] + \sum_{\mu} \left(\mathbf{L}_{\mu} \rho \mathbf{L}_{\mu}^{\dagger} - \frac{1}{2} \mathbf{L}_{\mu}^{\dagger} \mathbf{L}_{\mu} \rho - \frac{1}{2} \rho \mathbf{L}_{\mu}^{\dagger} \mathbf{L}_{\mu} \right). \qquad (3.195)$$

Здесь каждый *оператор Линдблада* (или *оператор квантового скачка*) представляет «квантовый скачок», который в принципе можно регистрировать, если достаточно тщательно контролировать окружение. Решая основное уравнение, мы можем вычислить темп декогерентизации открытой системы.

3.8. Упражнения

3.1. Реализация ПОЗМ. Рассмотрим ПОЗМ, определенную четырьмя положительными операторами

$$\begin{aligned} P_1 &= \tfrac{1}{2} |\uparrow_z\rangle\langle\uparrow_z|, & P_2 &= \tfrac{1}{2} |\downarrow_z\rangle\langle\downarrow_z|, \\ P_3 &= \tfrac{1}{2} |\uparrow_x\rangle\langle\uparrow_x|, & P_4 &= \tfrac{1}{2} |\downarrow_x\rangle\langle\downarrow_x|. \end{aligned} \qquad (3.196)$$

Покажите, каким образом эту ПОЗМ можно реализовать как ортогональное измерение в двухкубитовом гильбертовом пространстве, если введен один вспомогательный (ancilla) спин.

3.2. Обратимость супероператоров. Цель этого упражнения — показать, что супероператор обратим только тогда, когда он унитарен. Напомним, что любой супероператор может быыть представлен в виде операторной суммы; он действует на чистое состояние как

$$\mathcal{M}(|\psi\rangle\langle\psi|) = \sum_{\mu} \mathbf{M}_{\mu}|\psi\rangle\langle\psi|\mathbf{M}_{\mu}^{\dagger}, \tag{3.197}$$

где $\sum_{\mu} \mathbf{M}_{\mu}^{\dagger}\mathbf{M}_{\mu} = \mathbf{1}$. Другой супероператор $\mathcal{N}$ называется обратным по отношению к $\mathcal{M}$, если $\mathcal{N} \circ \mathcal{M} = 1$, или

$$\sum_{\mu,a} \mathbf{N}_{a}\mathbf{M}_{\mu}|\psi\rangle\langle\psi|\mathbf{M}_{\mu}^{\dagger}\mathbf{N}_{a}^{\dagger} = |\psi\rangle\langle\psi| \tag{3.198}$$

для любого $|\psi\rangle$. Отсюда следует, что

$$\sum_{\mu,a} \left|\langle\psi|\mathbf{N}_{a}\mathbf{M}_{\mu}|\psi\rangle\right|^{2} = 1. \tag{3.199}$$

a) Используя условия нормировки, которым удовлетворяют $\mathbf{N}_a$ и $\mathbf{M}_\mu$, покажите, что $\mathcal{N} \circ \mathcal{M} = 1$ влечет за собой

$$\mathbf{N}_{a}\mathbf{M}_{\mu} = \lambda_{a\mu}\mathbf{1} \tag{3.200}$$

для *всех* a и μ, другими словами, каждое произведение $\mathbf{N}_a\mathbf{M}_\mu$ пропорционально тождественному (единичному) оператору.

b) Используя результат (a), покажите, что для всех μ и ν $\mathbf{M}_{\nu}^{\dagger}\mathbf{M}_{\mu}$ пропорционально тождественному оператору.

c) Покажите, что из (b) следует унитарность $\mathcal{M}$.

3.3. Как много супероператоров? Сколько вещественных параметров необходимо для параметризации супероператора общего вида

$$\$: \rho \rightarrow \rho', \tag{3.201}$$

если ρ — оператор плотности в N-мерном гильбертовом пространстве? [**Указание**: Сколько вещественных чисел параметризует эрмитову $N \times N$-матрицу? Как много линейных отображений эрмитовых матриц на эрмитовы матрицы? Как много *сохраняющих след* отображений эрмитовых матриц на эрмитовы матрицы?]

3.4. Насколько быстра декогерентизация? Очень хороший маятник с массой $m = 1\,\text{г}$ и круговой частотой $\omega = 1\,\text{с}^{-1}$ имеет добротность $Q = 10^9$. Маятник приготовлен в состоянии «кот-суперпозиции»

$$|\text{cat}\rangle = \frac{1}{\sqrt{2}}\big(|x\rangle + |-x\rangle\big) \tag{3.202}$$

волновых пакетов с минимальной неопределенностью, первоначально покоящихся в положениях $\pm x$, где $x = 1\,\text{см}$. Оценить по порядку величины, как быстро произойдет декогерентизация этого «кот-состояния», если окружение находится

a) при нулевой температуре;

b) при комнатной температуре.

3.5. Затухание фазы. На лекции мы получили представление операторной суммы канала затухания фазы для одного кубита с операторами Крауса

$$\mathbf{M}_0 = \sqrt{1-p}\,\mathbf{1},\ \mathbf{M}_1 = \sqrt{p}\,\frac{1}{2}(\mathbf{1}+\boldsymbol{\sigma}_3),\ \mathbf{M}_2 = \sqrt{p}\,\frac{1}{2}(\mathbf{1}-\boldsymbol{\sigma}_3). \tag{3.203}$$

a) Найдите альтернативное представление, используя только два оператора Крауса $\mathbf{N}_0, \mathbf{N}_1$.

b) Найдите унитарную 3×3-матрицу $U_{\mu a}$ такую, что полученные вами в (a) операторы Крауса (дополненные третьим $\mathbf{N}_2 = 0$) связаны с $\mathbf{M}_{0,1,2}$ соотношением

$$\mathbf{M}_\mu = U_{\mu a}\mathbf{N}_a. \tag{3.204}$$

c) Рассмотрите унитарное представление однокубитового канала

$$\begin{aligned} |0\rangle_A|0\rangle_E &\to \sqrt{1-p}\,|0\rangle_A|0\rangle_E + \sqrt{p}\,|0\rangle_A|\gamma_0\rangle_E, \\ |1\rangle_A|0\rangle_E &\to \sqrt{1-p}\,|1\rangle_A|0\rangle_E + \sqrt{p}\,|1\rangle_A|\gamma_1\rangle_E, \end{aligned} \tag{3.205}$$

где $|\gamma_0\rangle_E$ и $|\gamma_1\rangle_E$ — ортогональные $|0\rangle_E$ нормированные состояния, удовлетворяющие условию

$${}_E\langle\gamma_0|\gamma_1\rangle_E = 1-\varepsilon, \qquad 0<\varepsilon<1. \tag{3.206}$$

Покажите, что это тоже канал затухания фазы, и найдите его представление операторной суммы с двумя операторами Крауса.

d) Допустим, что канал из (c) описывает то, что происходит с кубитом, когда на нем рассеивается один фотон. Выразите темп декогерентизации Γ_{decoh} через темп рассеяния Γ_{scatt}.

3.6. Декогерентизация на сфере Блоха. Параметризуйте матрицу плотности одного кубита следующим образом:

$$\boldsymbol{\rho} = \frac{1}{2}\left(\mathbf{1} + \vec{P}\cdot\vec{\boldsymbol{\sigma}}\right). \tag{3.207}$$

a) Опишите, что происходит с $\vec{P}$ под действием канала затухания фазы.

b) Опишите, что происходит с $\vec{P}$ под действием канала затухания амплитуды, определяемого операторами Крауса

$$\mathbf{M}_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-p} \end{pmatrix}, \qquad \mathbf{M}_1 = \begin{pmatrix} 0 & \sqrt{p} \\ 0 & 0 \end{pmatrix}. \tag{3.208}$$

c) Проделайте то же самое для «двойного канала Паули»:

$$\mathbf{M}_0 = \sqrt{1-p}\,\mathbf{1}, \quad \mathbf{M}_1 = \sqrt{\frac{p}{2}}\,\boldsymbol{\sigma}_1, \quad \mathbf{M}_2 = \sqrt{\frac{p}{2}}\,\boldsymbol{\sigma}_3. \tag{3.209}$$

3.7. Декогерентизация затухающего осциллятора. На лекции мы говорили, что в представлении взаимодействия матрица плотности $\boldsymbol{\rho}_I(t)$ осциллятора, который может излучать кванты в находящийся при нулевой температуре резервуар, подчиняется основному уравнению

$$\dot{\boldsymbol{\rho}}_I = \Gamma\left(\mathbf{a}\boldsymbol{\rho}_I\mathbf{a}^\dagger - \frac{1}{2}\mathbf{a}^\dagger\mathbf{a}\boldsymbol{\rho}_I - \frac{1}{2}\boldsymbol{\rho}_I\mathbf{a}^\dagger\mathbf{a}\right), \tag{3.210}$$

где $\mathbf{a}$ — осцилляторный оператор уничтожения.

a) Рассмотрите величину

$$X(\lambda, t) = \operatorname{tr}\left[\boldsymbol{\rho}_I(t)e^{\lambda\mathbf{a}^\dagger}e^{-\lambda^*\mathbf{a}}\right], \tag{3.211}$$

где λ — комплексное число. Используя основное уравнение, выведите и решите дифференциальное уравнение для $X(\lambda, t)$. Найдите

$$X(\lambda, t) = X(\lambda', 0), \tag{3.212}$$

где λ' является функцией от λ, Γ и t. Что это за функция $\lambda'(\lambda, \Gamma, t)$?

b) Предположим, что при $t = 0$ приготовлено «кот-состояние» осциллятора

$$|\mathrm{cat}\rangle = \frac{1}{\sqrt{2}}\left(|\alpha_1\rangle + |\alpha_2\rangle\right), \tag{3.213}$$

где $|\alpha\rangle$ обозначает когерентное состояние

$$|\alpha\rangle = e^{-|\alpha|^2/2}e^{\alpha\mathbf{a}^\dagger}|0\rangle. \tag{3.214}$$

Используйте результат (**a**), чтобы получить матрицу плотности в более поздний момент времени t. Каков темп затухания недиагональных элементов $\boldsymbol{\rho}$ (в этом когерентном базисе) при $\Gamma t \ll 1$?

Глава 4

Квантовое запутывание

4.1. Несепарабельность ЭПР-пар

4.1.1. Скрытая квантовая информация

Глубокие аспекты, отличающие квантовую информацию от классической, включают в себя свойства, привлечение и использование *квантового запутывания*. Вспомним, что, согласно § 2.4.1, бинарное состояние *запутано*, если его число Шмидта больше единицы. Запутанные состояния интересны тем, что в них проявляются не имеющие классических аналогов корреляции.

В качестве примера напомним определенное в § 3.4.1 *максимально запутанное* состояние двух кубитов (или *ЭПР-пара*[1]):

$$|\phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}\big(|00\rangle_{AB} + |11\rangle_{AB}\big). \tag{4.1}$$

«Максимально запутанный» означает, что если мы вычислим след по состояниям кубита B, чтобы найти оператор плотности ρ_A кубита A, то получим оператор, пропорциональный единичному:

$$\rho_A = \mathrm{tr}_B\big(|\phi^+\rangle_{AB\,AB}\langle\phi^+|\big) = \frac{1}{2}\mathbf{1}_A \tag{4.2}$$

(и аналогично $\rho_B = \frac{1}{2}\mathbf{1}_B$). Это значит, что результат измерения спина A вдоль *любой* оси будет полностью случайным: с вероятностью $1/2$ мы найдем его ориентированным вверх, и с вероятностью $1/2$ – вниз. Следовательно, если мы выполним любое локальное измерение A или B, то не получим никакой информации о приготовленном состоянии, лишь

[1] ЭПР – Эйнштейн, Подольский, Розен. – *Прим. перев.*

породив вместо этого случайный бит. Эта ситуация резко контрастирует со случаем одного кубита в чистом состоянии. Приготовив, скажем, $|\uparrow_{\hat{n}}\rangle$ или $|\downarrow_{\hat{n}}\rangle$, мы можем хранить в этом состоянии один бит и достоверно извлекать его, выполняя измерение вдоль оси $\hat{n}$. В случае двух кубитов нам следовало бы уметь хранить два бита, но в состоянии $|\phi^+\rangle_{AB}$ эта информация *скрыта*; по крайней мере, мы не можем извлечь ее, измеряя A или B.

Фактически $|\phi^+\rangle_{AB}$ является одним из представителей введенного в §3.4.1 базиса четырех взаимно ортогональных состояний двух кубитов, каждый из которых также максимально запутан:

$$\begin{aligned} |\phi^\pm\rangle_{AB} &= \frac{1}{\sqrt{2}}\left(|00\rangle_{AB} \pm |11\rangle_{AB}\right), \\ |\psi^\pm\rangle_{AB} &= \frac{1}{\sqrt{2}}\left(|01\rangle_{AB} \pm |10\rangle_{AB}\right). \end{aligned} \tag{4.3}$$

Представим, что Алиса и Боб играют с Чарли. Чарли готовит одно из этих четырех состояний, кодируя таким образом два бита в состоянии двухкубитовой системы. Один из них представляет собой бит *четности* ($|\phi\rangle$ или $|\psi\rangle$): параллельны или антипараллельны состояния двух спинов? Другой — бит *фазы* (+ или −): какой четности выбрана суперпозиция двух состояний? Затем Чарли посылает кубит A Алисе, а кубит B Бобу. Чтобы выиграть, Алиса (или Боб) должна определить, какое из четырех состояний приготовил Чарли.

Конечно, если бы Алиса и Боб соединили свои кубиты вместе, то они смогли бы идентифицировать состояние, выполняя ортогональное измерение, проецирующее на базис $\{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$. Но представим, что они находятся в разных городах и вообще не могут связаться друг с другом. Действуя локально, ни Алиса, ни Боб не могут извлечь никакой информации о состоянии.

Все, что они могут делать локально, это *манипулировать* этой информацией. Алиса может применить преобразование σ_3 к своему кубиту A, изменяя относительную фазу $|0\rangle_A$ и $|1\rangle_A$. Это действие обращает бит фазы, хранящийся в запутанном состоянии:

$$\begin{aligned} |\phi^+\rangle &\leftrightarrow |\phi^-\rangle, \\ |\psi^+\rangle &\leftrightarrow |\psi^-\rangle. \end{aligned} \tag{4.4}$$

С другой стороны, она может применить преобразование σ_1, которое опрокидывает ее спин ($|0\rangle_A \leftrightarrow |1\rangle_A$) и таким образом инвертирует бит четности

запутанного состояния:

$$|\phi^+\rangle \leftrightarrow |\psi^+\rangle,$$
$$|\phi^-\rangle \leftrightarrow -|\psi^-\rangle. \tag{4.5}$$

Аналогично и Боб может манипулировать запутанным состоянием. Фактически, как мы обсуждали в §2.4, или Алиса, или Боб могут выполнить локальное унитарное преобразование, заменяющее одно максимально запутанное состояние на любое другое максимально запутанное состояние[1]. Поскольку их локальные унитарные преобразования *не могут* изменить $\rho_A = \rho_B = \frac{1}{2}\mathbf{1}$, информация, которой они манипулируют, ни одним из них не может быть прочитана.

Предположим теперь, что Алиса и Боб могут обмениваться (классическими) сообщениями о результатах своих измерений; тогда вместе они могут узнать о том, как скоррелированы их измерения. Запутанные состояния базиса удобно характеризовать одновременными собственными значениями двух коммутирующих наблюдаемых

$$\sigma_1^A \otimes \sigma_1^B,$$
$$\sigma_3^A \otimes \sigma_3^B; \tag{4.6}$$

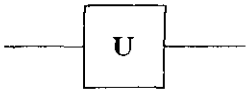
собственное значение оператора $\sigma_3^A \otimes \sigma_3^B$ является битом четности, а собственное значение $\sigma_1^A \otimes \sigma_1^B$ — битом фазы. Так как эти операторы коммутируют, они в принципе могут быть измерены одновременно. Но это невозможно, пока Алиса и Боб выполняют локальные измерения. Они могли бы оба решить измерить свои спины вдоль оси $\hat{z}$, приготовив одновременно собственные состояния операторов σ_3^A и σ_3^B. Поскольку σ_3^A и σ_3^B коммутируют с оператором четности $\sigma_3^A \otimes \sigma_3^B$, их ортогональные измерения не возмущают бит четности, а их результаты можно скомбинировать так, чтобы получить значение этого бита. Однако операторы σ_3^A и σ_3^B *не* коммутируют с оператором $\sigma_1^A \otimes \sigma_1^B$, поэтому выполненное таким способом измерение бита четности возмущает бит фазы. С другой стороны, Алиса и Боб могли бы решить измерить свои спины вдоль оси $\hat{x}$; тогда они могли бы узнать бит фазы ценой возмущения бита четности. Но они не могут одновременно выполнить оба этих измерения. Чтобы можно было надеяться получить бит четности без возмущения бита фазы, Алисе и Бобу нужно получить информацию о произведении $\sigma_3^A \otimes \sigma_3^B$, не изме-

[1] Но, конечно, этого недостаточно для того, чтобы выполнить произвольное унитарное преобразование в четырехмерном пространстве $\mathcal{H}_A \otimes \mathcal{H}_B$, содержащее также и не максимально запутанные состояния. Максимально запутанные состояния *не* образуют подпространства — их суперпозиция обычно *не* является максимально запутанной.

ряя отдельно ни σ_3^A, ни σ_3^B, что не может быть выполнено локальным образом.

Пусть теперь Алиса и Боб соберутся вместе, так чтобы они могли оперировать своими кубитами сообща. Как они могут узнать бит четности и бит фазы их пары? Применив подходящее унитарное преобразование, они могут повернуть запутанный базис $\{|\phi^+\rangle,\ |\psi^-\rangle\}$ таким образом, что он перейдет в незапутанный базис $\{|00\rangle,\ |01\rangle,\ |10\rangle,\ |11\rangle\}$. Тогда Алиса и Боб могут измерить кубиты A и B, чтобы получить искомые ими биты. Как строится это преобразование?

Воспользуемся удобным моментом, чтобы ввести обозначение, которое будет широко использоваться далее в этом курсе, обозначение квантовой схемы. Кубиты изображаются горизонтальными линиями, а однокубитовое унитарное преобразование U —



В частности, ниже нам очень пригодится однокубитовое унитарное *преобразование Адамара*

$$\mathbf{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}}(\boldsymbol{\sigma}_1 + \boldsymbol{\sigma}_3), \tag{4.7}$$

которое обладает свойствами

$$\mathbf{H}^2 = \mathbf{1}, \tag{4.8}$$

и

$$\begin{aligned} \mathbf{H}\boldsymbol{\sigma}_1\mathbf{H} &= \boldsymbol{\sigma}_3, \\ \mathbf{H}\boldsymbol{\sigma}_3\mathbf{H} &= \boldsymbol{\sigma}_1. \end{aligned} \tag{4.9}$$

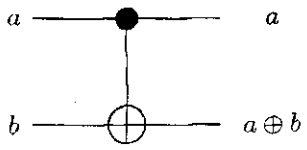
[Мы можем рассматривать $\mathbf{H}$ (с точностью до общей фазы) как поворот на угол $\theta = \pi$ вокруг оси $\hat{n} = \frac{1}{\sqrt{2}}(\hat{n}_1 + \hat{n}_3)$, который переводит друг в друга оси $\hat{x}$ и $\hat{z}$; мы имеем

$$\mathbf{U}(\hat{n}, \theta) = \mathbf{1}\cos\frac{\theta}{2} + i\hat{n}\cdot\vec{\boldsymbol{\sigma}}\sin\frac{\theta}{2} = i\frac{1}{\sqrt{2}}(\boldsymbol{\sigma}_1 + \boldsymbol{\sigma}_3) = i\mathbf{H}.] \tag{4.10}$$

Также полезно двухкубитовое преобразование, известное как обратимое XOR или контролируемое НЕ (CNOT) преобразование; оно действует как

$$\mathbf{CNOT}\ :\ |a, b\rangle \rightarrow |a, a \oplus b\rangle \tag{4.11}$$

на базисных состояниях $a, b = 0, 1$, где $a \oplus b$ обозначает сумму по модулю два. **CNOT** изображается диаграммой

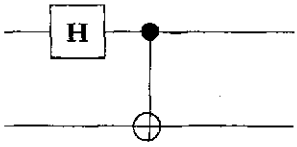


Таким образом, это преобразование инвертирует второй бит, если первый имеет значение 1, и действует тривиально, если первый бит имеет значение 0; оно обладает свойством

$$(\mathbf{CNOT})^2 = \mathbf{1} \otimes \mathbf{1}. \tag{4.12}$$

Мы называем a *контролирующим* битом (или *источником*) операции **CNOT**, а b - *контролируемым* битом (или *целью*).

Комбинируя эти «примитивные» преобразования, или квантовые *вентили*, мы можем построить другие унитарные преобразования. Например, «схема» (читается слева направо)



представляет произведение примененной к первому кубиту операции **H** и следующей за ней **CNOT** с первым кубитом в качестве контролирующего и вторым — в качестве контролируемого. Непосредственно видно, что эта схема преобразует стандартный базис в запутанный:

$$\begin{aligned}
|00\rangle &\to \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big)|0\rangle \to |\phi^+\rangle,\\
|01\rangle &\to \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big)|1\rangle \to |\psi^+\rangle,\\
|10\rangle &\to \frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big)|0\rangle \to |\phi^-\rangle,\\
|11\rangle &\to \frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big)|1\rangle \to |\psi^-\rangle,
\end{aligned} \tag{4.13}$$

так что первый бит становится битом фазы в запутанном базисе, а второй — битом четности.

Аналогично мы можем обратить преобразование, проходя схему в обратном направлении (поскольку и **CNOT**, и **H** идемпотентны); если мы применим обращенную схему к запутанному состоянию, а затем измерим оба бита, то мы узнаем значения бита фазы и бита четности.

Конечно, **H** действует только на один из кубитов; «нелокальной» частью нашей схемы является операция контролируемого НЕ (**CNOT**) – это операция, устанавливающая или устраняющая запутывание. Если бы только мы могли выполнить «межзвездную **CNOT**», то были бы в состоянии запутывать пространственно-разделенные пары или извлекать закодированную в них информацию. Однако мы не можем этого сделать. Чтобы выполнить эту работу, вентиль **CNOT** должен действовать на цель, не открывая значения источника. Локальных операций и классической связи для этого недостаточно.

4.1.2. Эйнштейновская локальность и скрытые переменные

Эйнштейна смущало квантовое запутывание. В конце концов он совместно с Подольским и Розеном (ЭПР) выразил это беспокойство в том, что они рассматривали как парадокс[1]. Согласно более поздней интерпретации Бома, описанная ими ситуация в действительности та же самая, что и обсуждавшаяся в § 2.5.3. Данное максимально запутанное состояние двух кубитов поделено между Алисой и Бобом, Алиса может выбрать одно из нескольких возможных измерений, чтобы выполнить его на своем спине, реализуя тем самым различные возможные интерпретации ансамблей матрицы плотности Боба; например, она может приготовить собственные состояния: или σ_1, или σ_3.

Мы видели, что Алиса и Боб не могут использовать это явление для сверхсветовой связи. Эйнштейн знал это, но оставался неудовлетворенным. Он считал, что теория, дающая *полное* описание физической реальности, должна удовлетворять более строгому критерию, который можно назвать *эйнштейновской локальностью* (иногда известный как *локальный реализм*).

> Предположим, что A и B – разделенные пространственно-подобным интервалом системы. Тогда в *полном* описании физической реальности действие, совершенное над системой A, не должно изменять описание системы B.

[1] A. Einstein, B. Podolsky, N. Rosen, *Can Quantum-mechanical Description of Physical Reality Be Considered Complete?*, Phys. Rev., 47, 777–780 (1935); современная интерпретация мысленного эксперимента ЭПР, использующая максимально запутанное состояние спинов, предложена Д. Бомом: D. Bohm, *Quantum Theory*, Prentice-Hall, Englewood Cliffs< New Jersey (1951); перевод: Д. Бом, *Квантовая теория*, М., Наука (1965). – *Прим. ред.*

Но если A и B запутаны, измерение A выполнено и *конкретный* полученный результат известен, то матрица плотности B обязательно *изменится*. Следовательно, согласно критерию Эйнштейна описание квантовой системы с помощью волновой функции или оператора плотности не может считаться полным.

Эйнштейн пытался представить более полное описание, которое устранило бы индетерминизм квантовой механики. Теории такого рода называются *теориями локальных скрытых переменных*. В теории скрытых переменных измерение в действительности является детерминистским, но выглядит вероятностным, поскольку некоторые степени свободы точно неизвестны. Например, возможно, что для описания приготовленного спинового состояния, которое в квантовой теории рассматривается как чистое состояние $|\uparrow_{\hat{z}}\rangle$, в действительности существует более глубокая теория, в которой оно параметризуется как $(\hat{z}, \lambda)$, где λ $(0 \leqslant \lambda \leqslant 1)$ — скрытая переменная. Допустим, что при современном уровне экспериментальной техники мы не контролируем λ, следовательно, когда мы готовим спиновое состояние, λ может принять любое значение — распределение вероятностей, управляющее ее значениями, является однородным на единичном интервале.

Теперь предположим, что при измерении спина вдоль оси $\hat{n}$, повернутой на угол θ относительно оси $\hat{z}$, будет получен результат

$$\begin{aligned} &|\uparrow_{\hat{z}}\rangle \quad \text{при} \quad 0 \leqslant \lambda \leqslant \cos^2\frac{\theta}{2}, \\ &|\downarrow_{\hat{z}}\rangle \quad \text{при} \quad \cos^2\frac{\theta}{2} < \lambda \leqslant 1. \end{aligned} \tag{4.14}$$

Если мы знаем λ, то результат является детерминистским, но если λ полностью неизвестна, тогда управляющее измерением распределение вероятностей будет согласоваться с предсказаниями квантовой теории. В теории скрытых переменных случайность результата измерения не является ее внутренним свойством; скорее она является следствием невежества — наше описание системы не является максимально возможным полным описанием.

Теперь как насчет запутанных состояний? Когда мы говорим, что теория скрытых переменных является *локальной*, мы подразумеваем, что она удовлетворяет эйнштейновскому требованию локальности. Измерение A не изменяет значения переменных, определяющих измерения B. Когда Алиса измеряет свою половину запутанного состояния, которое она делит с Бобом, она получает информацию о значениях скрытых переменных, увеличивая возможность предсказать, что получит Боб после измерения своей половины. Это кажется похожим на то, что имел в виду Эйнштейн, говоря о более полном описании.

4.2. Неравенство Белла

4.2.1. Три квантовые монеты

Является ли теория скрытых переменных просто переформулировкой квантовой теории, или она представляет собой допускающую проверку гипотезу? Плодотворная идея Джона Белла состояла в том, чтобы проверить эйнштейновскую локальность, рассматривая количественные свойства корреляций между результатами, полученными двумя экспериментаторами, Алисой и Бобом, измерявшими разные части системы, находящейся в запутанном состоянии. Рассмотрим пример корреляций, которые Алиса и Боб хотели бы объяснить.

Изучаемая Алисой и Бобом система могла бы быть описана следующим образом: Алиса в Пасадене имеет в своем распоряжении три выложенные на стол монеты, помеченные как 1, 2, 3. Каждая монета выпадает «орлом» (О) или «решкой» (Р), но они закрыты непрозрачными крышками, так что Алиса не может сказать, что на них выпало. Она может открыть любую одну из трех монет и таким образом узнать ее значение (О или Р). Но как только одна монета оказывается открытой, две другие закрытые монеты мгновенно исчезают облачком дыма и Алиса уже не имеет возможности открыть их. В ее распоряжении множество копий трехмонетного набора и в конце концов она понимает, что, независимо от того, какая монета открывается, вероятности обнаружить О или Р одинаковы. Боб в Чикаго имеет аналогичный набор монет, также помеченных 1, 2 и 3. Он тоже обнаруживает, что каждая из его монет, когда открывается, с одинаковой вероятностью показывает или О, или Р.

Фактически Алиса и Боб имеют множество идентичных копий поделенных между ними наборов монет; они проводят обширную серию экспериментов, чтобы исследовать, как их наборы монет коррелируют между собой. Они быстро делают замечательное открытие: всякий раз, когда Алиса и Боб открывают монеты с одинаковыми метками (1,2 или 3), они *всегда* находят их в одинаковом состоянии - обе показывают или О, или Р. Они проводят миллион испытаний, чтобы быть точно уверенными, что это происходит всегда! Их наборы монет идеально скоррелированы.

Алиса и Боб догадываются, что обнаружили нечто важное, и часто разговаривают по телефону, обсуждая внезапные идеи о смысле своих результатов. Однажды Алиса находилась в особенно задумчивом настроении.

Алиса: Ты знаешь, Боб, мне иногда трудно решить, какую из трех монет открыть. Я знаю, что если я открою, скажем, монету 1, то монеты 2 и 3 исчезнут, и у меня не будет возможности узнать, что выпало на

них. Хотя бы раз мне удалось открыть две из трех монет и узнать, что на них выпало: «орел» (О) или «решка» (Р). Я пыталась, но это действительно невозможно — нет способа увидеть одну монету и не дать исчезнуть другим!

Боб: [*Долгая пауза*]. Эй! ... подожди минутку, Алиса, у меня появилась идея.... Смотри, я думаю, что у тебя *есть* способ в конце концов узнать, что выпало на двух твоих монетах! Допустим, ты хотела бы открыть монеты 1 и 2. Ну, тогда я открою свою монету 2 здесь, в Чикаго, и сообщу тебе, что я обнаружил, пусть, к примеру, на ней выпало О. Тогда мы знаем, что если ты тоже откроешь монету 2, то наверняка найдешь О. В этом нет никаких сомнений, так как мы проверяли это миллион раз. Верно?

Алиса: Верно ....

Боб: Но теперь тебе ни к чему открывать твою монету 2; ты же точно знаешь, что на ней обнаружишь. Вместо этого ты можешь открыть монету 1. Тогда ты узнаешь, что выпало на обеих монетах.

Алиса: Гмм ..., да, может быть. Да, я имею в виду, что раньше, когда мы открывали одни и те же монеты, это всегда срабатывало, но теперь ты открыл свою монету 2 и твои монеты 1 и 3 исчезли, а я открыла свою монету 1, и мои монеты 2 и 3 исчезли. Нет возможности даже попытаться еще раз проверить, что случилось бы, если бы мы оба открыли монету 2.

Боб: Не надо проверять это еще раз, Алиса; мы уже миллион раз проверяли это. Смотри, твои монеты в Пасадене, а мои — в Чикаго. Очевидно, что просто нет способа, которым мое решение открыть мою монету 2 может *повлиять* на то, что ты обнаружишь, когда откроешь свою монету 2. То есть это невозможно. Просто когда я открываю мою монету 2, мы получаем информацию, необходимую нам, чтобы с уверенностью предсказать, что произойдет, когда ты откроешь свою монету 2. Так как мы уже уверены в этом, зачем заботиться о проверке!

Алиса: Хорошо, Боб, я понимаю, что ты имеешь в виду. Почему мы не можем выполнить эксперимент, чтобы увидеть, что действительно происходит, когда ты и я открываем разные монеты?

Боб: Я не знаю, Алиса. Было бы невероятно получить хоть какое-то финансирование такого «глупого» эксперимента. Я имею в виду, интересует

ли кого-нибудь на самом деле, что происходит, когда я открываю монету 2, а ты — монету 1?

Алиса: Я не уверена. Но я слышала о теоретике по имени Белл. Говорят, что у него интересные идеи относительно монет. Возможно, у него есть теория, которая делает предсказание относительно того, что мы обнаружим. Может быть, нам стоит поговорить с ним?

Боб: Хорошая мысль! И даже неважно, имеет его теория смысл или нет. Мы можем тем не менее предложить эксперимент, чтобы проверить его предсказание, и тогда нас, возможно, спонсируют.

Итак, Алиса и Боб отправляются в ЦЕРН[1], чтобы побеседовать с Беллом. Они рассказывают ему об эксперименте, который они предлагают выполнить. Белл внимательно слушает их, но некоторое время с отрешенным видом хранит молчание. Алису и Боба не очень это беспокоит, так как они не много понимают из того, что говорят теоретики. Но наконец Белл говорит:

Белл: Я думаю, что у меня есть идея .... Когда Боб открывает свою монету в Чикаго, он не может оказать никакого *влияния* на монету Алисы в Пасадене. Вместо этого то, что обнаруживает Боб, открывая свою монету, дает некоторую *информацию* о том, что случится, когда Алиса откроет свою монету.

Боб: Ну, то есть что я и говорил ....

Белл: Правильно. Звучит разумно. Итак, допустим, что Боб в этом прав. Теперь Боб может открыть любую одну из его монет и узнать наверняка, что найдет Алиса, когда она откроет соответствующую монету. Он никак не *затронул* ее монеты; он просто получил информацию о ней. Нам придется сделать вывод, что должны существовать некоторые *скрытые переменные*, которые определяют состояние монет Алисы. И если эти переменные полностью известны, тогда состояние каждой из монет Алисы может быть однозначно предсказано.

Боб: [*Раздраженный всей этой абстрактной чепухой*]. Да, ну и что?

Белл: Когда ваши коррелированные наборы монет были приготовлены, значения скрытых переменных не были полностью определены, вот

[1]CERN — Европейский центр ядерных исследований. — *Прим. перев.*

почему на любой одной монете с равной вероятностью может выпасть О, а может и Р. Однако должно существовать некоторое распределение вероятностей $P(x, y, z)$ (с $x, y, z \in \{\text{O,P}\}$), которое характеризует приготовление и управляет тремя монетами Алисы. Эти вероятности должны быть неотрицательны и в сумме равны единице:

$$\sum_{x,y,z\in\{\text{O,P}\}} P(x, y, z) = 1. \tag{4.15}$$

Алиса не может открыть все три ее монеты, следовательно, она не может непосредственно измерить $P(x, y, z)$. Однако с помощью Боба она в действительности может открыть любые две монеты из своего набора. Обозначим как $P_{\text{same}}(i, j)$ вероятность того, что монеты i и j $(i, j = 1, 2, 3)$ показывают одно и то же: или обе О, или обе Р. Тогда мы видим, что

$$\begin{aligned} P_{\text{same}}(1,2) &= P(\text{OOO}) + P(\text{OOP}) + P(\text{PPO}) + P(\text{PPP}), \\ P_{\text{same}}(2,3) &= P(\text{OOO}) + P(\text{POO}) + P(\text{OPP}) + P(\text{PPP}), \\ P_{\text{same}}(1,3) &= P(\text{OOO}) + P(\text{OPO}) + P(\text{POP}) + P(\text{PPP}). \end{aligned} \tag{4.16}$$

Из уравнения (4.15) непосредственно следует, что

$$\begin{aligned} P_{\text{same}}(1,2) + P_{\text{same}}(2,3) + P_{\text{same}}(1,3) = \\ = 1 + 2P(\text{OOO}) + 2P(\text{PPP}) \geqslant 1. \end{aligned} \tag{4.17}$$

Это и есть мое предсказание: P_{same} должны подчиняться неравенству[1]

$$P_{\text{same}}(1,2) + P_{\text{same}}(2,3) + P_{\text{same}}(1,3) \geqslant 1. \tag{4.18}$$

Вы можете проверить мой вывод в вашем эксперименте, в котором «открываются» две монеты сразу.

Боб: Ну, я допускаю, что математика выглядит правильной. Но на самом деле я не понимаю этого. Почему это работает?

Алиса: Мне кажется, что я поняла ... Белл говорит, что если на столе лежат три монеты и на каждой из них либо О, либо Р, тогда по крайней мере на двух из трех выпадает *одно и то же*: или на обеих О, или на обеих Р. Не так ли, Белл?

[1] Неравенства таково типа получены в работе J.S. Bell, *On the Einstein–Podolsky–Rosen Paradox*, Physics, **1**, 195–200 (1964); см. также J.S. Bell, *On the Problem of Hidden Variables in Quantum Mechanics*, Rev. Mod. Phys., **38**, 447–452 (1966). – *Прим. ред.*

Белл с изумлением смотрит на Алису. Его глаза блестят, на некоторое время он теряет дар речи. Наконец он говорит:

Белл: Да.

Итак, Алиса и Боб были счастливы узнать, что Белл, как редкий зверь, — теоретик, от которого есть толк. Благодаря Беллу, их предложение получило одобрение и они выполняют эксперимент, получая обескураживающий результат. После множества тщательных проверок они с очень высокой статистической надежностью делают вывод, что

$$P_{\text{same}}(1,2) \simeq P_{\text{same}}(2,3) \simeq P_{\text{same}}(1,3) \simeq \frac{1}{4} \tag{4.19}$$

и, следовательно,

$$P_{\text{same}}(1,2) + P_{\text{same}}(2,3) + P_{\text{same}}(1,3) \simeq 3 \cdot \frac{1}{4} = \frac{3}{4} < 1. \tag{4.20}$$

Обнаруженные Алисой и Бобом корреляции вопиюще нарушают неравенство Белла!

Алиса и Боб — хорошие экспериментаторы, но они не решаются публиковать столь возмутительный результат до тех пор, пока не смогут найти ему правдоподобное теоретическое истолкование. Наконец, дойдя до полного отчаяния, они идут в библиотеку, чтобы узнать, может ли принести хоть какое-то утешение квантовая механика ....

4.2.2. Квантовое запутывание против эйнштейновской локальности

Там Алиса и Боб читают о квантовом запутывании. В конце концов, они узнают, что их волшебные монеты управляются максимально запутанным состоянием двух кубитов. Алиса и Боб в действительности делят множество копий состояния $|\psi^-\rangle$.[1] Когда Алиса открывает монету, она измеряет свой кубит вдоль одной из трех возможных осей, не перпендикулярных между собой. Поскольку измерения не коммутируют, Алиса может открыть только одну из ее трех монет. Аналогично, когда Боб открывает свою монету, он измеряет свою часть запутанной пары вдоль любой одной из трех осей, следовательно, он тоже имеет возможность открыть только одну из

[1] Судя по тому, что, открывая монеты с одинаковыми номерами, Алиса и Боб *всегда* обнаруживали их в одинаковом состоянии (см. § 4.2.1), их трех-монетные наборы должны управляться максимально запутанным состоянием ЭПР-типа $|\phi^+\rangle_{AB}$ (см. уравнение (4.3)). Однако дальнейшие вычисления в этом параграфе выполняются для состояния $|\psi^-\rangle$. *—Прим. ред.*

его трех монет. Но поскольку измерения Алисы коммутируют с измерениями Боба, каждый из них может открыть одну монету и исследовать, как их монеты коррелируют между собой.

Чтобы помочь Алисе и Бобу интерпретировать их эксперимент, посмотрим, что говорит квантовая механика об этих корреляциях. Состояние $|\psi^-\rangle$ обладает полезным свойством: оно остается неизменным, если Алиса и Боб применяют одно и то же унитарное преобразование (2.27)

$$\mathbf{U} \otimes \mathbf{U}|\psi^-\rangle = |\psi^-\rangle. \tag{4.21}$$

В случае бесконечно малого унитарного преобразования оно превращается в свойство

$$\left(\vec{\sigma}^A + \vec{\sigma}^B\right)|\psi^-\rangle = 0 \tag{4.22}$$

(состояние с равным нулю полным моментом импульса, в чем вы можете легко убедиться с помощью явных вычислений). Рассмотрим ожидаемое значение

$$\langle\psi^-|\left(\vec{\sigma}^A \cdot \hat{a}\right)\left(\vec{\sigma}^B \cdot \hat{b}\right)|\psi^-\rangle, \tag{4.23}$$

где $\hat{a}$ и $\hat{b}$ — единичные трехмерные векторы. Действуя на $|\psi^-\rangle$, мы можем заменить $\vec{\sigma}^B$ на $-\vec{\sigma}^A$; следовательно, ожидаемое значение (4.23) может быть представлено как свойство системы Алисы, которая имеет оператор плотности $\boldsymbol{\rho}_A = \frac{1}{2}\mathbf{1}$:

$$\begin{aligned} -\langle\psi^-|\left(\vec{\sigma}^A \cdot \hat{a}\right)\left(\vec{\sigma}^A \cdot \hat{b}\right)|\psi^-\rangle = \\ = -a_i b_j \operatorname{tr}\left(\boldsymbol{\rho}_A \boldsymbol{\sigma}_i^A \boldsymbol{\sigma}_j^A\right) = -a_i b_j \delta_{ij} = -\hat{a}\cdot\hat{b} = -\cos\theta, \end{aligned} \tag{4.24}$$

где θ — угол между осями $\hat{a}$ и $\hat{b}$. Таким образом, мы нашли, что результаты измерения всегда идеально антикоррелированы, когда оба спина измеряются вдоль одной и той же оси $\hat{a}$, но мы также получили и более общий результат, применимый к случаю, когда две оси различны.

Проекционный оператор на состояние спин-вверх (спин-вниз) вдоль оси $\hat{n}$ имеет вид $\mathbf{E}(\hat{n}, \pm) = \frac{1}{2}(\mathbf{1} \pm \hat{n}\cdot\vec{\sigma})$; следовательно, мы получаем

$$\begin{aligned} P(++) &= \langle\psi^-|\mathbf{E}^A(\hat{a},+)\mathbf{E}^B(\hat{b},+)|\psi^-\rangle = \frac{1}{4}(1-\cos\theta), \\ P(--) &= \langle\psi^-|\mathbf{E}^A(\hat{a},-)\mathbf{E}^B(\hat{b},-)|\psi^-\rangle = \frac{1}{4}(1-\cos\theta), \\ P(+-) &= \langle\psi^-|\mathbf{E}^A(\hat{a},+)\mathbf{E}^B(\hat{b},-)|\psi^-\rangle = \frac{1}{4}(1+\cos\theta), \\ P(-+) &= \langle\psi^-|\mathbf{E}^A(\hat{a},-)\mathbf{E}^B(\hat{b},+)|\psi^-\rangle = \frac{1}{4}(1+\cos\theta); \end{aligned} \tag{4.25}$$

здесь $P(++)$ — вероятность того, что Алиса и Боб, оба получают в результате спин-вверх, когда Алиса выполняет измерение вдоль оси $\hat{a}$, а Боб — вдоль оси $\hat{b}$, и так далее. Вероятность того, что их результаты совпадают, равна

$$P_{\text{same}} = P(++) + P(--) = \frac{1}{2}(1 - \cos\theta), \tag{4.26}$$

а вероятность того, что их результаты различны, —

$$P_{\text{opposite}} = P(+-) + P(-+) = \frac{1}{2}(1 + \cos\theta). \tag{4.27}$$

Теперь предположим, что Алиса измеряет свои спины вдоль одной из трех, симметрично ориентированных в плоскости OXZ, осей

$$\hat{a}_1 = (0, 0, 1), \quad \hat{a}_2 = \left(\frac{\sqrt{3}}{2}, 0, -\frac{1}{2}\right), \quad \hat{a}_3 = \left(-\frac{\sqrt{3}}{2}, 0, -\frac{1}{2}\right), \tag{4.28}$$

так что

$$\hat{a}_1 \cdot \hat{a}_2 = \hat{a}_2 \cdot \hat{a}_3 = \hat{a}_3 \cdot \hat{a}_1 = -\frac{1}{2}. \tag{4.29}$$

Предположим также, что Боб выполняет измерение вдоль одной из трех осей, диаметрально противоположных осям Алисы:

$$\hat{b}_1 = -\hat{a}_1, \qquad \hat{b}_2 = -\hat{a}_2, \qquad \hat{b}_3 = -\hat{a}_3. \tag{4.30}$$

Если Алиса и Боб выбирают противоположные оси, то $\theta = 180^\circ$ и $P_{\text{same}} = 1$. В противном случае $\theta = \pm 60^\circ$, так что $\cos\theta = 1/2$ и $P_{\text{same}} = 1/4$. Это именно то нарушающее предсказание Белла поведение, которое Алиса и Боб обнаружили в своем эксперименте.

Логика Белла выглядит безупречной, но кое-что встало с ног на голову, поэтому мы вынуждены пересмотреть молчаливо подразумеваемые им предположения. Во-первых, Белл предполагает, что существует совместное распределение вероятностей, управляющее возможными исходами всех измерений, которые могут выполнить Алиса и Боб. Это является гипотезой о скрытых переменных. Белл представляет, что если значения скрытых переменных точно известны, то можно с уверенностью предсказать результат любого измерения — результаты измерения описываются вероятностным образом, поскольку значения скрытых переменных извлекаются из некоторого ансамбля возможных значений. Во-вторых, Белл полагает, что решение Боба, какое выполнять измерение в Чикаго, не влияет на скрытые

переменные, управляющие измерением Алисы в Пасадене. Это представляет собой предположение о локальности скрытых переменных. Если мы принимаем эти два предположения, то с неизбежностью приходим к выводу Белла. Мы обнаружили, что корреляции, предсказываемые квантовой теорией, несовместимы с этими предположениями.

Что отсюда следует? Вероятно, урок этой истории в том, что может быть опасно рассуждать о том, что могло бы случиться, но на самом деле не происходит — что иногда называют *контрфактом*. Конечно, в нашей повседневной жизни мы постоянно этим занимаемся и обычно выходим сухими из воды; рассуждения о контрфактах выглядят приемлемыми в классическом мире, но в квантовом мире с ними иногда можно попасть впросак. Мы утверждали, что, поскольку Боб выполнил измерение вдоль оси $\hat{a}_1$, Алиса знала, что произошло бы, если бы она провела измерение вдоль оси $\hat{a}_1$, и сколько бы мы ни проверяли, их результаты всегда идеально скоррелированы. Однако Алиса *не стала* измерять вдоль $\hat{a}_1$; вместо этого она выполнила измерение вдоль $\hat{a}_2$. Мы столкнулись с трудностями, пытаясь приписать вероятности результатам измерений вдоль $\hat{a}_1$, $\hat{a}_2$ и $\hat{a}_3$, несмотря на то, что Алиса может выполнить только одно из них. Предположение о существовании распределения вероятностей, управляющего исходами всех трех измерений, каждое из которых, но только одно, Алиса могла бы выполнить, в квантовой теории ведет к математическим противоречиям, так что нам лучше его не делать. Мы подтвердили принцип *дополнительности* Бора — запрещено одновременно рассматривать исходы двух взаимно исключающих экспериментов.

Тот, кто отвергает принцип дополнительности, может, предпочтет сказать, что (экспериментально подтвержденные) нарушения неравенств Белла продемонстрировали существенную нелокальность, присущую квантовому описанию Природы. *Если* мы действительно настаиваем на законности обсуждения результатов взаимно исключающих экспериментов, *то* неизбежно приходим к выводу, что выбор измерения Боба действительно оказывает тонкое *влияние* на результат измерения Алисы. Таким образом, сторонники этой точки зрения говорят о «квантовой нелокальности».

Исключив локальные скрытые переменные, Белл разбил мечту Эйнштейна о том, что индетерминизм квантовой теории мог бы быть устранен более полным, но все же локальным, описанием Природы. Если мы принимаем локальность как нерушимый принцип, мы вынуждены принять случайность не как следствие неполного знания, а как неизбежное внутреннее свойство квантового измерения.

Некоторые считают, что раскрытые неравенствами Белла специфические корреляции требуют более глубокого объяснения, чем способна дать

квантовая механика. Они рассматривают явление ЭПР как предтечу ожидающей своего открытия новой физики. Но они могут и ошибаться. После ЭПР мы ждали больше 65-ти лет, а новой физики так и нет.

Похоже, человеческий разум плохо подготовлен к тому, чтобы постичь корреляции, демонстрируемые запутанными квантовыми состояниями, и поэтому мы говорим о таинственности квантовой теории. Но какой бы ни была ваша позиция, эксперимент вынуждает вас согласиться с наличием странных корреляций между результатами измерений. Нет большой тайны в том, как эти корреляции были установлены – мы видели, что Алисе и Бобу было необходимо вместе в некоторой точке пространства создать запутывание между их кубитами. Необычность состоит в том, что даже когда A и B пространственно разделены, мы не можем строго рассматривать A и B как два отдельных кубита и использовать классическую информацию для характеристики того, как они коррелируют. Они более, чем просто коррелированы, они представляют собой нечто *единое и неделимое*. Они *запутаны*.

4.3. Еще неравенства Белла

4.3.1. Неравенство КГШХ

Экспериментальные проверки эйнштейновской локальности обычно основываются на другой форме неравенства Белла, применяемого к ситуации, в которой Алиса может измерить одну из двух наблюдаемых $\mathbf{a}$ и $\mathbf{a}'$, в то время как Боб может измерить или $\mathbf{b}$, или $\mathbf{b}'$. Предположим, что наблюдаемые $\mathbf{a}, \mathbf{a}', \mathbf{b}, \mathbf{b}'$ принимают значения $\{\pm 1\}$ и являются функциями скрытых случайных переменных.

Если $\mathbf{a}, \mathbf{a}' = \pm 1$, то отсюда следует, что или $\mathbf{a} + \mathbf{a}' = 0$, тогда $\mathbf{a} - \mathbf{a}' = \pm 2$, или же $\mathbf{a} - \mathbf{a}' = 0$, тогда $\mathbf{a} + \mathbf{a}' = \pm 2$; следовательно:

$$\mathbf{C} = (\mathbf{a} + \mathbf{a}')\mathbf{b} + (\mathbf{a} - \mathbf{a}')\mathbf{b}' = \pm 2. \tag{4.31}$$

(Здесь тайком введено предположение о локальных скрытых переменных – мы представили, что значения $\{\pm 1\}$ могут быть приписаны одновременно всем четырем наблюдаемым, даже если невозможно одновременное измерение $\mathbf{a}$ и $\mathbf{a}'$ или $\mathbf{b}$ и $\mathbf{b}'$.) Очевидно

$$|\langle \mathbf{C} \rangle| \leqslant \langle |\mathbf{C}| \rangle = 2, \tag{4.32}$$

так что

$$|\langle \mathbf{ab} \rangle + \langle \mathbf{a'b} \rangle + \langle \mathbf{ab'} \rangle - \langle \mathbf{a'b'} \rangle| \leqslant 2. \tag{4.33}$$

Этот результат называется *неравенством КГШХ* (Клаузер - Горн - Шимони - Холт). Оно справедливо для любых случайных переменных $\mathrm{a}, \mathrm{a}', \mathrm{b}, \mathrm{b}'$, принимающих значения $\{\pm 1\}$, которые управляются совместным распределением вероятностей.

Чтобы увидеть, что квантовая механика нарушает неравенство КГШХ, допустим, что a, a' обозначают эрмитовы операторы

$$\mathbf{a} = \vec{\sigma}^{(A)} \cdot \hat{a}, \qquad \mathbf{a}' = \vec{\sigma}^{(A)} \cdot \hat{a}', \tag{4.34}$$

действующие на кубит Алисы, где $\hat{a}$, $\hat{a}'$ — трехмерные единичные векторы. Аналогично b, b' обозначают операторы

$$\mathbf{b} = \vec{\sigma}^{(B)} \cdot \hat{b}, \qquad \mathbf{b}' = \vec{\sigma}^{(B)} \cdot \hat{b}', \tag{4.35}$$

действующие на кубит Боба. Каждая наблюдаемая имеет собственные значения ± 1, то есть результатами их измерения являются значения ± 1.

Напомним, что если Алиса и Боб делят максимально запутанное состояние $|\psi^-\rangle$, то

$$\langle \psi^- | (\vec{\sigma}^A \cdot \hat{a})(\vec{\sigma}^B \cdot \hat{b}) | \psi^- \rangle = -\hat{a} \cdot \hat{b} = -\cos\theta, \tag{4.36}$$

где θ — угол между $\hat{a}$ и $\hat{b}$. Рассмотрим случай, когда $\hat{a}'$, $\hat{b}$, $\hat{a}$, $\hat{b}'$ компланарны и располагаются последовательно через $45°$, так что квантовая механика предсказывает:

$$\begin{aligned} \langle \mathbf{ab} \rangle = \langle \mathbf{a}'\mathbf{b} \rangle = \langle \mathbf{ab}' \rangle &= -\cos\frac{\pi}{4} = -\frac{1}{\sqrt{2}}, \\ \langle \mathbf{a}'\mathbf{b}' \rangle &= -\cos\frac{3\pi}{4} = \frac{1}{\sqrt{2}}. \end{aligned} \tag{4.37}$$

Тогда неравенство КГШХ

$$4 \cdot \frac{1}{\sqrt{2}} = 2\sqrt{2} \leqslant 2 \tag{4.38}$$

очевидно нарушается предсказанием квантовой механики.

4.3.2. Максимальное нарушение

Фактически, как мы увидим из следующих аргументов, только что рассмотренный случай представляет максимально возможное квантово-механическое нарушение неравенства КГШХ. Предположим, что $\mathbf{a}, \mathbf{a}', \mathbf{b}, \mathbf{b}'$

эрмитовы операторы с собственными значениями ± 1, так что

$$\mathbf{a}^2 = \mathbf{a}'^2 = \mathbf{b}^2 = \mathbf{b}'^2 = \mathbf{1}; \tag{4.39}$$

допустим также, что «наблюдаемые Алисы» $\mathbf{a}, \mathbf{a}'$ коммутируют с «наблюдаемыми Боба» $\mathbf{b}, \mathbf{b}'$:

$$[\mathbf{a}, \mathbf{b}] = [\mathbf{a}, \mathbf{b}'] = [\mathbf{a}', \mathbf{b}] = [\mathbf{a}', \mathbf{b}'] = 0. \tag{4.40}$$

Определяя

$$\mathbf{C} = \mathbf{ab} + \mathbf{a}'\mathbf{b} + \mathbf{ab}' - \mathbf{a}'\mathbf{b}' \tag{4.41}$$

и учитывая (4.39), вычислим

$$\mathbf{C}^2 = \begin{array}{cccc} \mathbf{1} & +\mathbf{aa}' & +\mathbf{bb}' & -\mathbf{aa}'\mathbf{bb}' \\ +\mathbf{a}'\mathbf{a} & +\mathbf{1} & +\mathbf{a}'\mathbf{abb}' & -\mathbf{bb}' \\ +\mathbf{b}'\mathbf{b} & +\mathbf{aa}'\mathbf{b}'\mathbf{b} & +\mathbf{1} & -\mathbf{aa}' \\ -\mathbf{a}'\mathbf{ab}'\mathbf{b} & -\mathbf{b}'\mathbf{b} & -\mathbf{a}'\mathbf{a} & +\mathbf{1} \end{array}. \tag{4.42}$$

Все квадратичные члены попарно сокращаются, так что мы остаемся с

$$\begin{aligned} \mathbf{C}^2 &= 4 \cdot \mathbf{1} - \mathbf{aa}'\mathbf{bb}' + \mathbf{a}'\mathbf{abb}' + \mathbf{aa}'\mathbf{b}'\mathbf{b} - \mathbf{a}'\mathbf{ab}'\mathbf{b} \\ &= 4 \cdot \mathbf{1} - [\mathbf{a}, \mathbf{a}'][\mathbf{b}, \mathbf{b}']. \end{aligned} \tag{4.43}$$

Теперь вспомним, что *норма* $\|\mathbf{M}\|$ ограниченного оператора $\mathbf{M}$ определяется как[1]

$$\|\mathbf{M}\| = \sup_{|\psi\rangle} \left(\frac{\|\mathbf{M}|\psi\rangle\|}{\||\psi\rangle\|} \right); \tag{4.44}$$

то есть нормой $\mathbf{M}$ является максимальное собственное значение оператора $\sqrt{\mathbf{M}^\dagger \mathbf{M}}$. Нетрудно проверить, что норма оператора обладает свойствами

$$\begin{aligned} \|\mathbf{MN}\| &\leqslant \|\mathbf{M}\| \cdot \|\mathbf{N}\|, \\ \|\mathbf{M} + \mathbf{N}\| &\leqslant \|\mathbf{M}\| + \|\mathbf{N}\|. \end{aligned} \tag{4.45}$$

[1] В оригинале используется обозначение $\|\cdot\|_{\sup}$ и термин *sup norm*, который можно было бы перевести как *супремум-норма*, или *верхняя норма*. На самом деле (4.44) дает определение обычной нормы ограниченного оператора, которая в русской литературе обозначается как $\|\cdot\|$. См., например, М. Рид, Б. Саймон, *Методы современной математической физики*. Т. 1. *Функциональный анализ*, Мир, М., 1977, стр. 21. — *Прим. ред.*

Эрмитовский оператор с собственными значениями ± 1 имеет единичную норму, так что

$$\|\mathbf{C}^2\| \leqslant 4 + 4\|\mathbf{a}\| \cdot \|\mathbf{a}'\| \cdot \|\mathbf{b}\| \cdot \|\mathbf{b}'\| = 8. \tag{4.46}$$

Поскольку оператор $\mathbf{C}$ эрмитов,

$$\|\mathbf{C}^2\| = \|\mathbf{C}\|^2 \tag{4.47}$$

и, следовательно,

$$\|\mathbf{C}\| \leqslant 2\sqrt{2}, \tag{4.48}$$

что известно как неравенство Цирельсона.

Неравенство КГШХ утверждает, что $|\langle \mathbf{C} \rangle| \leqslant 2$. В квантовой механике абсолютная величина ожидаемого значения эрмитовского оператора $\mathbf{C}$ не может быть больше его максимального собственного значения

$$|\langle \mathbf{C} \rangle| \leqslant \|\mathbf{C}\| \leqslant 2\sqrt{2}. \tag{4.49}$$

Мы видим, что верхняя грань достигается в случае, когда $\hat{a}'$, $\hat{b}$, $\hat{a}$, $\hat{b}'$ компланарны и располагаются последовательно через углы $45°$. Таким образом, найденное нами нарушение неравенства КГШХ является наибольшим допустимым в квантовой теории.

4.3.3. Квантовые стратегии действуют лучше классических

Неравенство КГШХ представляет собой ограничение на величину корреляций между двумя частями бинарной классической системы, а неравенство Цирельсона — ограничение на величину корреляций между двумя частями бинарной квантовой системы. Мы можем углубить наше понимание того, чем квантовые корреляции отличаются от классических, рассматрев игру, в которой квантовые стратегии работают лучше классических.

Алиса и Боб играют с Чарли. Чарли готовит два бита $x, y \in \{0, 1\}$; затем он посылает x Алисе, а y Бобу. Получив входящий бит x, Алиса производит выходящий бит $a \in \{0, 1\}$, точно так же, получив y, Боб производит выходящий бит $b \in \{0, 1\}$. Но им запрещено общаться друг с другом, так что Алиса не знает y, а Боб не знает x.

Алиса и Боб побеждают в игре, если их выходящие биты окажутся связанными с входящими соотношением

$$a \oplus b = x \wedge y, \tag{4.50}$$

где $\oplus$ обозначает сложение по модулю два (вентиль XOR), а $\wedge$ обозначает произведение (вентиль AND). Могут ли Алиса и Боб найти стратегию, позволяющую им всегда выигрывать, независимо от того, какие входящие биты выбирает Чарли?

Нет, очевидно, что такой стратегии здесь нет. Пусть a_0, a_1 обозначают значения выходящих битов Алисы, если входящими были $x = 0, 1$, и пусть b_0, b_1 — выходящие биты Боба, соответствующие его входящим битам $y = 0, 1$. Чтобы Алиса и Боб выиграли при всех возможных входах, их выходящие биты должны удовлетворять

$$a_0 \oplus b_0 = 0, \quad a_0 \oplus b_1 = 0, \quad a_1 \oplus b_0 = 0, \quad a_1 \oplus b_1 = 1. \tag{4.51}$$

Однако это невозможно, так как, складывая эти четыре равенства, мы получим $0 = 1$.

Предположим, что Чарли генерирует входящие биты случайным образом. Тогда существует очень простая стратегия, позволяющая Алисе и Бобу выигрывать в трех случаях из четырех: они всегда выбирают выходящие биты $a = b = 0$, так что они проигрывают, если только входящие биты $x = y = 1$. Неравенство КГШХ может рассматриваться как утверждение того, что если Алиса и Боб делят не квантовое запутанное состояние, то лучшей стратегии нет.

Чтобы связать это утверждение с нашей предыдущей формулировкой неравенства КГШХ, определим случайные переменные, принимающие значения ± 1:

$$\begin{aligned} \mathbf{a} &= (-1)^{a_0}, \qquad \mathbf{a}' = (-1)^{a_1}, \\ \mathbf{b} &= (-1)^{b_0}, \qquad \mathbf{b}' = (-1)^{b_1}. \end{aligned} \tag{4.52}$$

Тогда неравенство КГШХ говорит, что при любом совместном распределении вероятностей, управляющем переменными $\mathbf{a}, \mathbf{a}', \mathbf{b}, \mathbf{b}' \in \{0, 1\}$, ожидаемые значения удовлетворяют неравенству

$$\langle \mathbf{ab} \rangle + \langle \mathbf{ab}' \rangle + \langle \mathbf{a}'\mathbf{b} \rangle - \langle \mathbf{a}'\mathbf{b}' \rangle \leqslant 2. \tag{4.53}$$

Более того, если мы обозначим p_{xy} вероятность того, что уравнения (4.51) удовлетворяются, когда входящие биты равны (x, y), то

$$\begin{aligned} \langle \mathbf{ab} \rangle &= 2p_{00} - 1, \qquad \langle \mathbf{ab}' \rangle = 2p_{01} - 1, \\ \langle \mathbf{a}'\mathbf{b} \rangle &= 2p_{10} - 1, \qquad \langle \mathbf{a}'\mathbf{b}' \rangle = 1 - 2p_{11}; \end{aligned} \tag{4.54}$$

Например, $\langle \mathbf{ab} \rangle = p_{00} - (1 - p_{00}) = 2p_{00} - 1$, поскольку значение $\mathbf{ab}$ равно $+1$, когда Алиса и Боб выигрывают, и -1, когда они проигрывают.

Неравенство КГШХ (4.53) приобретает вид

$$2(p_{00} + p_{01} + p_{10} + p_{11}) - 4 \leqslant 2 \tag{4.55}$$

или

$$\langle p \rangle \equiv \frac{1}{4}(p_{00} + p_{01} + p_{10} + p_{11}) \leqslant \frac{3}{4}, \tag{4.56}$$

где $\langle p \rangle$ обозначает вероятность выигрыша, усредненную по однородному ансамблю входящих битов. Таким образом, если входящие биты случайны, то Алиса и Боб не могут достичь вероятности выигрыша, превосходящей $3/4$.

Имеет смысл рассмотреть, как предположение о том, что Алиса и Боб действуют под управлением «*локальных* скрытых переменных», ограничивает их успех в игре. Несмотря на то, что Алиса и Боб не делят квантовое запутанное состояние, им разрешено разделить таблицу случайных чисел, в соответствии с которой они могут генерировать их выходящие биты. Таким образом, мы можем представить, что Алиса и Боб принимают коррелированные решения, руководствуясь скрытыми переменными, извлекаемыми из ансамбля возможных значений. Эти корреляции ограничены локальностью — Алиса не знает входящих битов Боба, а Боб — входящих битов Алисы.

Но если Алиса и Боб делят квантовое запутанное состояние, то они могут изобрести стратегию получше. В зависимости от значения своего входящего бита, Алиса решает измерить одну из двух эрмитовых наблюдаемых с собственными значениями ± 1: $\mathbf{a}$, если $x = 0$, и $\mathbf{a}'$, если $x = 1$. Аналогично, Боб измеряет $\mathbf{b}$, если $y = 0$, и $\mathbf{b}'$, если $y = 1$. Тогда квантово-механические ожидаемые значения этих наблюдаемых удовлетворяют неравенству Цирельсона

$$\langle \mathbf{ab} \rangle + \langle \mathbf{ab}' \rangle + \langle \mathbf{a}'\mathbf{b} \rangle - \langle \mathbf{a}'\mathbf{b}' \rangle \leqslant 2\sqrt{2}, \tag{4.57}$$

а вероятность того, что Алиса и Боб выиграют гейм, ограничена условием

$$2(p_{00} + p_{01} + p_{10} + p_{11}) - 4 \leqslant 2\sqrt{2} \tag{4.58}$$

или

$$\langle p \rangle \equiv \frac{1}{4}(p_{00} + p_{01} + p_{10} + p_{11}) \leqslant \frac{1}{2} + \frac{1}{2\sqrt{2}} \approx 0{,}853. \tag{4.59}$$

Более того, мы видели, что это неравенство может перейти в равенство, если Алиса и Боб делят максимально запутанное состояние двух кубитов, а наблюдаемые $\mathbf{a}, \mathbf{a}', \mathbf{b}, \mathbf{b}'$ выбраны подходящим образом.

Итак, мы обнаружили, что Алиса и Боб могут играть более успешно при наличии квантового запутывания, чем в его отсутствие. По крайней мере для этих целей, разделенное квантовое запутывание является более мощным средством, чем разделенная классическая случайность. Но даже ресурс квантового запутывания имеет свои пределы, устанавливаемые неравенством Цирельсона.

4.3.4. Все запутанные чистые состояния нарушают неравенства Белла

Сепарабельные состояния не нарушают неравества Белла. Например, если $\mathbf{a}$ является наблюдаемой, действующей на кубит Алисы, а $\mathbf{b}$ — наблюдаемой, действующей на кубит Боба, то в случае сепарабельного *чистого* состояния

$$\langle \mathbf{ab} \rangle = \langle \mathbf{a} \rangle \langle \mathbf{b} \rangle. \tag{4.60}$$

Никакого нарушения неравеств Белла не может быть, поскольку, как мы уже видели, действительно *существует* (локальная) теория скрытых переменных, которая корректно воспроизводит предсказания квантовой теории для чистого состояния одного кубита. Общее сепарабельное состояние представляет просто вероятностную смесь сепарабельных чистых состояний, так что корреляции между подсистемами являются полностью классическими и неравенства Белла применимы.

С другой стороны, мы видели, что максимально запутанное состояние, такое как $|\psi^-\rangle$, *нарушает* неравенства Белла. Но что можно сказать относительно чистого состояния, запутанного лишь частично, такого как

$$|\phi\rangle = \alpha|00\rangle + \beta|11\rangle\,? \tag{4.61}$$

Любое чистое состояние двух кубитов может быть выражено таким способом в базисе Шмидта; при подходящем соглашении относительно фаз α и β вещественные и неотрицательные.

Предположим, что Алиса и Боб выполняют измерение вдоль оси, лежащей в плоскости OXZ, так что их наблюдаемыми являются

$$\begin{aligned} \mathbf{a} &= \boldsymbol{\sigma}_3^{(A)} \cos\theta_A + \boldsymbol{\sigma}_1^{(A)} \sin\theta_A, \\ \mathbf{b} &= \boldsymbol{\sigma}_3^{(B)} \cos\theta_B + \boldsymbol{\sigma}_1^{(B)} \sin\theta_B. \end{aligned} \tag{4.62}$$

Состояние $|\phi\rangle$ обладает свойствами

$$\begin{aligned} \langle\phi|\boldsymbol{\sigma}_3 \otimes \boldsymbol{\sigma}_3|\phi\rangle = 1, \qquad \langle\phi|\boldsymbol{\sigma}_1 \otimes \boldsymbol{\sigma}_1|\phi\rangle = 2\alpha\beta, \\ \langle\phi|\boldsymbol{\sigma}_3 \otimes \boldsymbol{\sigma}_1|\phi\rangle = \langle\phi|\boldsymbol{\sigma}_1 \otimes \boldsymbol{\sigma}_3|\phi\rangle = 0, \end{aligned} \tag{4.63}$$

так что квантово-механическое ожидаемое значение переменной $\mathbf{ab}$ равно

$$\langle \mathbf{ab} \rangle = \langle \phi | \mathbf{ab} | \phi \rangle = \cos\theta_A \cos\theta_B + 2\alpha\beta \sin\theta_A \sin\theta_B \tag{4.64}$$

[и мы воспроизводим $\cos(\theta_A - \theta_B)$ в максимально запутанном случае $\alpha = \beta = 1/\sqrt{2}$]. Теперь для простоты рассмотрим частный (не оптимальный!) случай

$$\theta_A = 0, \quad \theta'_A = \frac{\pi}{2}, \quad \theta'_B = -\theta_B, \tag{4.65}$$

так что квантовые предсказания равны

$$\begin{aligned} \langle \mathbf{ab} \rangle &= \cos\theta_B = \langle \mathbf{ab}' \rangle, \\ \langle \mathbf{a}'\mathbf{b} \rangle &= 2\alpha\beta \sin\theta_B = -\langle \mathbf{a}'\mathbf{b}' \rangle. \end{aligned} \tag{4.66}$$

Подставляя в неравенство КГШХ, получаем

$$|\cos\theta_B - 2\alpha\beta \sin\theta_B| \leqslant 1, \tag{4.67}$$

что очевидно нарушается при значениях θ_B, близких к 0 и π. Разлагая левую часть в линейном порядке по θ_B, имеем

$$\simeq 1 - 2\alpha\beta\theta_B, \tag{4.68}$$

что, конечно же, превосходит единицу при $\alpha\beta > 0$ и малом отрицательном θ_B.

Мы показали, что *любое* запутанное чистое состояние двух кубитов нарушает некоторое неравенство Белла. Это доказательство нетрудно обобщить на произвольное бинарное чистое состояние. То есть для бинарных чистых состояний «запутывание» эквивалентно «нарушению неравенства Белла». Однако, как мы увидим ниже, для бинарных смешанных состояний ситуация более тонкая.

4.3.5. Фотоны

Эксперименты по проверке неравенства Белла обычно выполняются на запутанных фотонах, а не на объектах со спином-1/2. Каковы квантово-механические предсказания для фотонов?

Вспомним из §2.2.2, что в случае фотонов, распространяющихся в направлении $\hat{z}$, мы используем обозначения $|x\rangle$, $|y\rangle$ для состояний, линейно поляризованных вдоль осей OX и OY соответственно. На языке этих базисных состояний, поляризованных вдоль «горизонтальной» и «вертикальной»

осей, состояния, повернутые на угол θ относительно OX и OY осей, могут быть выражены как

$$|H(\theta)\rangle = \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix}, \qquad |V(\theta)\rangle = \begin{pmatrix} -\sin\theta \\ \cos\theta \end{pmatrix}. \tag{4.69}$$

Мы можем построить 2×2-матрицу, собственными состояниями которой являются $|H(\theta)\rangle$ и $|V(\theta)\rangle$ с соответствующими собственными значениями ± 1; она имеет вид

$$\tau(\theta) \equiv |H(\theta)\rangle\langle H(\theta)| - |V(\theta)\rangle\langle V(\theta)| = \begin{pmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{pmatrix}. \tag{4.70}$$

Генератором поворотов вокруг оси $\hat{z}$ является $\mathbf{J} = \boldsymbol{\sigma}_2$, а собственными состояниями оператора $\mathbf{J}$ с собственными значениями ± 1 — циркулярно поляризованные состояния

$$|+\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}, \qquad |-\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} i \\ 1 \end{pmatrix}. \tag{4.71}$$

Предположим, что возбужденный атом излучает два фотона, которые вылетают в противоположных направлениях в состоянии с равным нулю суммарным угловым моментом и положительной четностью. Двухфотонные состояния

$$|+\rangle_A|-\rangle_B, \qquad |-\rangle_A|+\rangle_B \tag{4.72}$$

инвариантны относительно поворотов вокруг оси $\hat{z}$. Фотоны имеют противоположные значения J_z, но одинаковые *спиральности* (угловые моменты вдоль направления распространения), так как они распространяются в противоположных направлениях. При отражении в плоскости OYZ поляризованные состояния преобразуются согласно

$$|x\rangle \to -|x\rangle, \qquad |y\rangle \to |y\rangle \tag{4.73}$$

или

$$|+\rangle \to +i|-\rangle, \qquad |-\rangle \to -i|+\rangle; \tag{4.74}$$

следовательно, собственными состояниями четности являются запутанные состояния

$$\frac{1}{\sqrt{2}}\left(|+\rangle_A|-\rangle_B \pm |-\rangle_A|+\rangle_B\right). \tag{4.75}$$

Тогда состояние с $J_z = 0$ и положительной четностью, выраженное через линейно поляризованные состояния, имеет вид

$$-\frac{i}{\sqrt{2}}\left(|+-\rangle_{AB} + |-+\rangle_{AB}\right) = \frac{1}{\sqrt{2}}\left(|xx\rangle_{AB} + |yy\rangle_{AB}\right) \equiv |\phi^+\rangle_{AB}. \tag{4.76}$$

Вследствие инвариантности относительно поворотов вокруг оси $\hat{z}$, оно имеет такой вид независимо от того, как мы ориентируем OX и OY оси.

Алиса и Боб могут использовать анализатор поляризации, чтобы спроецировать состояния поляризации фотона на базис $\{|H(\theta)\rangle, |V(\theta)\rangle\}$ и, следовательно, измерить $\tau(\theta)$. Для двух фотонов в состоянии $|\phi^+\rangle$, если Алиса ориентирует свой анализатор под углом θ_A, а Боб – под углом θ_B, тогда корреляции результатов их измерений закодированы в ожидаемом значении

$$\langle\phi^+|\tau^{(A)}(\theta_A)\tau^{(B)}(\theta_B)|\phi^+\rangle. \tag{4.77}$$

С учетом вращательной симметрии:

$$\begin{aligned}
&= \langle\phi^+|\tau^{(A)}(0)\tau^{(B)}(\theta_B-\theta_A)|\phi^+\rangle = \\
&= \frac{1}{2}\langle x|\tau^{(B)}(\theta_B-\theta_A)|x\rangle - \frac{1}{2}\langle y|\tau^{(B)}(\theta_B-\theta_A)|y\rangle = \\
&= \cos 2(\theta_B-\theta_A).
\end{aligned} \tag{4.78}$$

Напомним, что в случае измерения кубитов на сфере Блоха мы находили подобное выражение $\cos\theta$, где θ – угол между направлениями поляризации у Алисы и Боба. Здесь вместо этого мы имеем $\cos 2\theta$, поскольку фотоны имеют спин-1, а не спин-1/2.

Если Алиса измеряет одну из двух наблюдаемых $\mathbf{a} = \tau^{(A)}(\theta_A)$ или $\mathbf{a}' = \tau^{(A)}(\theta'_A)$, а Боб измеряет или $\mathbf{b} = \tau^{(B)}(\theta_B)$, или $\mathbf{b}' = \tau^{(B)}(\theta'_B)$, то в предположении о существовании локальных скрытых переменных применимо неравенство КГШХ. Если мы подставляем квантовые предсказания для ожидаемых значений, то получим

$$|\cos 2(\theta_B-\theta_A)+\cos 2(\theta_B-\theta'_A)+\cos 2(\theta'_B-\theta_A)-\cos 2(\theta'_B-\theta'_A)| \leqslant 2. \tag{4.79}$$

Максимальное нарушение этого неравенства, при котором неравенство Цирельсона превращается в равенство, – левая часть равна $2\sqrt{2}$ – возникает, когда θ'_A, θ_B, θ_A и θ'_B последовательно разделены углами $22\frac{1}{2}^\circ$, так что

$$\begin{aligned}
\frac{1}{\sqrt{2}} &= \cos 2(\theta_B-\theta_A) = \cos 2(\theta_B-\theta'_A) = \\
&= \cos 2(\theta'_B-\theta_A) = -\cos 2(\theta'_B-\theta'_A).
\end{aligned} \tag{4.80}$$

4.3.6. Эксперименты и лазейки

Лазейка локальности. Экспериментами с запутанными парами фотонов было проверено неравенство КГШХ в форме (4.79). Эксперименты

подтвердили квантовые предсказания и убедительно продемонстрировали, что неравенство КГШХ нарушается. Следовательно, эти эксперименты, по всей видимости, показывают, что Природа не может корректно описываться теорией локальных скрытых переменных.

Но так ли это? Скептик может выдвинуть возражения. Например, при выводе неравенства КГШХ мы предполагали, что после того как Алиса решит, что измерять: a или a′, Боб не получает информации о ее решении прежде, чем он выполнит свои измерения (а также, если первым измерения выполняет Боб, то мы предполагаем, что информация о его решении не доходит до Алисы прежде, чем она выполнит свои измерения). С другой стороны, маргинальное распределение вероятностей для результатов измерений Боба может быть дополнено после измерений Алисы, но до измерений Боба, так что неравенство КГШХ становится неприменимым. Предположение о невозможности такого дополнения подтверждается релятивистской причинностью, если решение и измерение Алисы, как события, отделены от решения и измерения Боба пространственно-подобными интервалами. Скептик упорно настаивает, чтобы эксперимент удовлетворял этому условию, которое называется *лазейкой локальности*.

В 1982 г. Аспек с сотрудниками выполнили эксперимент с целью проверки лазейки локальности. Два запутанных фотона рождаются в результате распада возбужденного состояния атома кальция и поляризация каждого фотона ориентируется включением одного из двух псевдо-случайно выбранного анализатора поляризации. Фотоны регистрируются на удалении около 12 м от источника, что соответствует времени распространения света около 40 нс. Это время гораздо больше времени включения или разности времен прибытия обоих фотонов. Следовательно, «решение» о том, какую наблюдаемую измерять, принимается, когда фотоны уже находятся в полете, а события, состоящие в выборе осей для измерения поляризации фотонов A и B, разделены пространственно-подобным интервалом. Результаты согласуются с квантовыми предсказаниями и нарушают неравенство КГШХ на пять стандартных отклонений. После Аспека этот результат был подтвержден в других экспериментах, включая те, в которых детекторы A и B были удалены на километры.

Лазейка детектирования. Другое возражение, которое может выдвинуть скептик, называется *лазейкой детектирования*. В экспериментах с фотонами эффективность детектирования исключительно низкая. Большинство запутанных фотонных пар не регистрируются обоими детекторами A и B. Среди событий, ведущих к ошибке: фотон может быть поглощен, прежде чем он достигнет детектора, фотон может пролететь мимо детектора, или фотон может достичь детектора, но не быть им зарегистрирован-

ным. В эксперименте принимаются только те данные, которые получены при совпадении регистрации двух фотонов, поскольку, проверяя неравенство КГШХ, мы должны предполагать, что полученные данные представляют объективную выборку из всех запутанных пар.

Но что если локальные скрытые переменные управляют не только тем, *какое* состояние поляризации детектируется, но также и тем, *сработает ли вообще* детектор? Тогда полученные нами данные могут быть необъективной (смещенной) выборкой, а неравенство КГШХ — неприменимым.

В упражнении 4.2 мы покажем, что лазейку детектирования можно закрыть, если фотоны регистрируются с эффективностью около 82,84%. Современные эксперименты с фотонами далеки от требуемой эффективности. В экспериментах с ионными ловушками неравенство КГШХ было проверено с эффективностью детектирования, близкой к 100%, однако в этих экспериментах открыта (для скрытых переменных (перев.)) лазейка локальности. До сих пор не поставлено эксперимента, в котором одновременно были бы закрыты обе лазейки — локальности и детектирования.

Лазейка свободы воли. Предположим, что выполнен эксперимент, в котором фотоны регистрируются с идеальной эффективностью, а решения, принимаемые Алисой и Бобом, выглядят разделенными пространственно-подобным интервалом. Но скептик может продолжать сопротивляться выводу о том, что теории локальных скрытых переменных исключены, обращаясь к *лазейке свободы воли*. Предполагается, что принимаемые Алисой и Бобом решения о том, что измерять, сами управляются скрытыми переменными. Тогда их решения могут коррелировать со значениями скрытых переменных, которые определяют результаты измерения, следовательно, они не в состоянии получить объективную выборку из распределения скрытых переменных, а неравенство КГШХ может быть нарушено.

Каждый из нас сам решает для себя, насколько серьезно относиться к этому возражению.

4.4. Использование запутывания

После работы Белла квантовое запутывание стало предметом интенсивных исследований среди тех, кто интересуется основаниями квантовой теории. Постепенно сформировалась новая точка зрения: запутывание не только уникальный инструмент для демонстрации странностей квантовой механики, но и потенциально полезный *ресурс*. Используя запутывание квантовых состояний, мы можем решить задачи, сложные или неразрешимые при других подходах.

4.4.1. Плотное кодирование

Нашим первым примером является использование запутывания для связи. Алиса хочет послать сообщение Бобу. Она может послать классические биты (типа точек и тире азбуки Морзе), но предположим, что Алиса и Боб связаны *квантовым* каналом связи. Например, Алиса может приготовить кубиты (фотоны) в любом состоянии поляризации, в каком пожелает, и послать их Бобу, который измеряет поляризацию вдоль выбранной им оси. Существует ли какое-нибудь преимущество в отправлении кубитов вместо классических битов?

В принципе, если их квантовый канал имеет идеальную точность воспроизведения, а Алиса и Боб выполняют приготовление и измерение с идеальной эффективностью, тогда они *не будут испытывать затруднений*, используя кубиты вместо классических битов. Скажем, Алиса может приготовить или $|\uparrow_z\rangle$, или $|\downarrow_z\rangle$, а Боб может измерить вдоль $\hat{z}$, чтобы определить сделанный ей выбор. Таким образом, с каждым кубитом Алиса может послать один классический бит. Но фактически это максимум того, что она может сделать. Посылая по одному кубиту независимо от того, как она их готовит, и независимо от того, как Боб их измеряет, с каждым кубитом можно передать не более одного классического бита (даже если кубиты запутаны между собой). Это утверждение, частный случай предела Холево способности квантового канала пропускать классическую информацию, будет доказано в главе 5.

Теперь немного изменим правила — предположим, что Алиса и Боб делят запутанную пару кубитов в состоянии $|\phi^+\rangle_{AB}$. Пара была приготовлена в прошлом году; один кубит был отправлен Алисе, а другой — Бобу в надежде, что разделенное запутывание однажды пригодится. Использование квантового канала весьма дорого, так что Алиса может позволить себе послать Бобу только один кубит. Тем не менее для нее крайне важно сообщить Бобу *два* классических бита информации.

К счастью, Алиса помнит о запутанном состоянии $|\phi^+\rangle_{AB}$, которое она делит с Бобом, и выполняет протокол, который они с Бобом приготовили как раз для такого случая. На своей части запутанной пары она может выполнить одно из четырех возможных унитарных преобразований:

1) $\mathbf{1}$ (она ничего не делает),

2) σ_1 (поворот на 180° вокруг оси $\hat{x}$),

3) σ_2 (поворот на 180° вокруг оси $\hat{y}$),

4) σ_3 (поворот на 180° вокруг оси $\hat{z}$).

Как мы видели, делая это, она преобразует $|\phi^+\rangle_{AB}$ к одному из четырех взаимно ортогональных состояний:

1) $|\phi^+\rangle_{AB}$,

2) $|\psi^+\rangle_{AB}$,

3) $|\psi^-\rangle_{AB}$ (с точностью до фазы),

4) $|\phi^-\rangle_{AB}$.

Теперь она посылает свой кубит Бобу, который получает его и выполняет ортогональное коллективное измерение на паре, проецируя ее на максимально запутанный базис. Результат измерения недвусмысленно различает четыре возможных действия, которые Алиса могла выполнить. Следовательно, *один кубит*, посланный Алисой Бобу, успешно переносит два бита классической информации! Поэтому такая процедра называется «плотным кодированием».

Приятной особенностью этого протокола является то, что если сообщение строго конфиденциальное, то Алиса может не беспокоиться о том, что пересылаемый кубит перехватят враги и расшифруют ее сообщение. Перехваченный кубит имеет матрицу плотности $\boldsymbol{\rho}_A = \frac{1}{2}\mathbf{1}_A$ и не несет информации вообще. Вся информация в корреляциях между кубитами A и B, а она недоступна, до тех пор пока враг не заполучит обе части запутанной пары. (Но, конечно, он может «перекрыть» канал, препятствуя получению информации Бобом.)

С одной точки зрения Алисе и Бобу в действительности *нужно* дважды воспользоваться каналом для обмена двумя битами информации. Например, мы можем представить, что Алиса сама приготовила состояние $|\phi^-\rangle_{AB}$. В прошлом году она послала Бобу половину состояния, а теперь посылает вторую. То есть на самом деле Алиса посылала два кубита Бобу в одном из четырех взаимно ортогональных состояний, чтобы передать ему два классических бита информации, что допускает предел Холево.

Плотное кодирование является странным по ряду причин. Во-первых, Алиса послала Бобу первый кубит задолго до того, как узнала, каким будет ее сообщение. Во-вторых, каждый кубит сам по себе не несет никакой информации; она целиком закодирована в корреляциях между кубитами. В-третьих, это сработало бы с тем же успехом, если бы запутанную пару приготовил Боб и половину ее послал Алисе; тогда два классических бита передаются от Алисы к Бобу путем пересылки одного кубита от Боба к Алисе и обратно.

Так или иначе, если бы возникла необходимость и понадобилось немедленно послать два бита, в то время как каналом связи можно воспользоваться только один раз, Алиса и Боб могли бы использовать предварительно приготовленное запутывание для более эффективной связи. Они использовали бы запутывание как ресурс.

4.4.2. Квантовая телепортация

В плотном кодировании квантовая информация может быть использована для увеличения передачи классической информации. В частности, если Алиса и Боб делят запутанное состояние, то для передачи двух классических битов достаточно послать один кубит. Интересно обратное утверждение. Если Алиса и Боб делят запутанное состояние, то достаточно ли послать два классических бита, чтобы передать один кубит?

Представим, что Чарли приготовил для Алисы кубит в состоянии $|\psi\rangle$, но Алиса ничего не знает о том, какое состояние приготовил Чарли. Бобу отчаянно нужен этот кубит, и Алиса хочет помочь ему. Но проклятый квантовый канал снова закрыт! Алиса может послать Бобу только *классическую* информацию.

Она могла бы попытаться измерить $\vec{\sigma} \cdot \hat{n}$, проецируя свой кубит или на $|\uparrow_{\hat{n}}\rangle$, или на $|\downarrow_{\hat{n}}\rangle$, и послать однобитовый результат измерения Бобу, который тогда мог бы приступить к приготовлению обнаруженного Алисой состояния. Но, как вы покажете в упражнении 4.7, состояние Боба не будет идеальной копией состояния Алисы; в среднем он будет соответствовать кубиту Алисы с точностью воспроизведения

$$F = |\langle\varphi|\psi\rangle|^2 = \frac{2}{3}. \tag{4.81}$$

Эта точность воспроизведения выше той, которой Боб мог бы добиться просто случайным образом выбирая состояние $\left(F = \frac{1}{2}\right)$, но она далека от той, что ему требуется. Более того, как мы увидим в главе 5, не существует алгоритма, позволяющего таким способом (Алиса измеряет кубит и посылает классическую информацию Бобу) достичь точности воспроизведения выше, чем $2/3$.

К счастью, Алиса и Боб помнят, что они делят максимально запутанное состояние $|\phi^+\rangle_{AB}$, которое они приготовили в прошлом году. Почему бы им не использовать запутывание как *ресурс*? Если они готовы израсходовать разделенное запутанное состояние и общаться классическим образом, то может ли Алиса послать свой кубит Бобу с точностью воспроизведения выше, чем $2/3$?

На самом деле они могут добиться точности воспроизведения $F = 1$, выполняя следующий протокол: Алиса соединяет неизвестный кубит $|\psi\rangle_C$, который она хочет послать Бобу, с ее половиной $|\phi^+\rangle_{AB}$-пары, которую она делит с Бобом. Она измеряет две коммутирующие наблюдаемые

$$\boldsymbol{\sigma}_1^{(C)} \otimes \boldsymbol{\sigma}_1^{(A)}, \qquad \boldsymbol{\sigma}_3^{(C)} \otimes \boldsymbol{\sigma}_3^{(A)}, \tag{4.82}$$

выполняя таким образом *измерение Белла* – проекцию двух кубитов на одно из четырех максимально запутанных состояний $|\phi^\pm\rangle_{CA}$, $|\psi^\pm\rangle_{CA}$. Затем она посылает результаты своих измерений (два бита классической информации) Бобу по классическому каналу. Получив эту информацию, Боб выполняет одну из четырех операций над своим кубитом:

$$\begin{aligned}
&\text{Алиса измеряет } |\phi^+\rangle_{CA} \to \text{Боб применяет } \mathbf{1}^{(B)},\\
&\text{Алиса измеряет } |\psi^+\rangle_{CA} \to \text{Боб применяет } \boldsymbol{\sigma}_1^{(B)},\\
&\text{Алиса измеряет } |\psi^-\rangle_{CA} \to \text{Боб применяет } \boldsymbol{\sigma}_2^{(B)},\\
&\text{Алиса измеряет } |\phi^-\rangle_{CA} \to \text{Боб применяет } \boldsymbol{\sigma}_3^{(B)}.
\end{aligned} \tag{4.83}$$

Это действие преобразует кубит Боба (его часть запутанной пары, предварительно поделенной с Алисой) в идеальную копию $|\psi\rangle_C$. Этот магический трюк называется *квантовой телепортацией*.

Как она работает? Заметим, что для $|\psi\rangle = a|0\rangle + b|1\rangle$ мы можем записать

$$\begin{aligned}
|\psi\rangle_C|\phi^+\rangle_{AB} &= (a|0\rangle_C + b|1\rangle_C)\frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}) =\\
&= \frac{1}{\sqrt{2}}(a|000\rangle_{CAB} + a|011\rangle_{CAB} + b|100\rangle_{CAB} + b|111\rangle_{CAB}) =\\
&= \frac{a}{2}(|\phi^+\rangle_{CA} + |\phi^-\rangle_{CA})|0\rangle_B + \frac{a}{2}(|\psi^+\rangle_{CA} + |\psi^-\rangle_{CA})|1\rangle_B +\\
&+ \frac{b}{2}(|\psi^+\rangle_{CA} - |\psi^-\rangle_{CA})|0\rangle_B + \frac{b}{2}(|\phi^+\rangle_{CA} - |\phi^-\rangle_{CA})|1\rangle_B =\\
&= \frac{1}{2}|\phi^+\rangle_{CA}(a|0\rangle_B + b|1\rangle_B) + \frac{1}{2}|\psi^+\rangle_{CA}(a|1\rangle_B + b|0\rangle_B) +\\
&+ \frac{1}{2}|\psi^-\rangle_{CA}(a|1\rangle_B - b|0\rangle_B) + \frac{1}{2}|\phi^-\rangle_{CA}(a|0\rangle_B - b|1\rangle_B) =\\
&= \frac{1}{2}|\phi^+\rangle_{CA}|\psi\rangle_B + \frac{1}{2}|\psi^+\rangle_{CA}\boldsymbol{\sigma}_1|\psi\rangle_B +\\
&+ \frac{1}{2}|\psi^-\rangle_{CA}(-i\boldsymbol{\sigma}_2)|\psi\rangle_B + \frac{1}{2}|\phi^-\rangle_{CA}\boldsymbol{\sigma}_3|\psi\rangle_B.
\end{aligned} \tag{4.84}$$

Таким образом, мы видим, что, когда Алиса выполняет измерение Белла на кубитах C и A, все четыре исхода равновероятны. Как только Боб узнает результат ее измерения, он получает в свое распоряжение чистое состояние $\sigma|\psi\rangle$, где σ — известный оператор Паули, один из $\{1, \sigma_1, \sigma_2, \sigma_3\}$. Действие, предписываемое уравнением (4.83), восстанавливает кубит Боба в начальном состоянии $|\psi\rangle$.

Квантовая телепортация — любопытная процедура. Первоначально кубит Боба полностью некоррелирован с неизвестным кубитом $|\psi\rangle_C$, но выполненное Алисой измерение Белла устанавливает корреляцию между A и C. Результат ее измерения фактически совершенно случаен, следовательно, выполняя это измерение, Алиса (и Боб) в действительности не получают никакой информации относительно $|\psi\rangle$. Это особенно приятно. Ведь как известно, если бы они получили любую информацию о состоянии, то неизбежно внесли бы в него возмущение.

Как же в таком случае квантовому состоянию удается перейти от Алисы к Бобу? Это довольно загадочно. С одной стороны, мы едва ли можем уверенно сказать, что два отправленых классических бита несли эту информацию, поскольку они были случайными. Следовательно, невольно хочется сказать, что разделенная запутанная пара сделала возможной телепортацию. Вспомним, однако, что запутанная пара в действительности была приготовлена еще в прошлом году, когда Алисе даже не снилось, что она будет посылать кубит Бобу ...

Следует также заметить, что процесс телепортации полностью согласуется с принципом невозможности клонирования. В самом деле, в руках Боба оказалась копия состояния $|\psi\rangle_B$. Но прежде, чем она могла возникнуть, оригинал $|\psi\rangle_C$ был разрушен измерением Алисы.

Наши сведения о плотном кодировании и квантовой телепортации можно подытожить как утверждения о том, как ресурс одного типа может моделировать другой. Введем термины *забит* для разделенной на две части запутанной пары кубитов[1] и *с-бит* для классического бита (*с* от слова *classical* — классический). Мы телепортируем один кубит от Алисы к Бобу, расходуя один забит и посылая два *с*-бита, а с помощью плотного кодирования мы посылаем два *с*-бита от Алисы к Бобу, расходуя один забит и транспортируя один кубит. Таким образом, можно сказать, что

$$\begin{aligned} &1 \text{ забит} + 2\,c\text{-бита} \rightarrow 1 \text{ кубит}, \\ &1 \text{ забит} + 1 \text{ кубит} \rightarrow 2\,c\text{-бита} \end{aligned} \tag{4.85}$$

означает, что ресурсов левых частей достаточно для копирования правых частей. В этих алгоритмах существенно запутывание. Без забитов кубит

[1] В оригинале *ebit* (*e* от слова *entangled* — *запутанный*). — *Прим. перев.*

стоит не больше одного c-бита и без них же «телепортируемый» кубит имеет точность воспроизведения $F \leqslant 2/3$.

4.4.3. Квантовая телепортация и максимальное запутывание

Идея телепортации выглядит довольно таинственно. Хотелось бы глубже разобраться, почему она работает. Полезным ключом к разгадке является то, что для телепортации с точностью воспроизведения $F = 1$ расходуемое запутанное состояние согласно протоколу должно быть *максимально* запутанным. А основной особенностью бинарных максимально запутанных состояний является то, что *или Алиса, или Боб* могут преобразовывать одно такое состояние в другое, применяя локальное унитарное преобразование.

Чтобы лучше увидеть, как работает квантовая телепортация, рассмотрим телепортирование N-мерной системы, используя максимально запутанное $N \times N$-состояние вида

$$|\Phi\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle \otimes |i\rangle. \tag{4.86}$$

Полезным свойством этого состояния является

$$\begin{aligned} {}_{CA}\langle\Phi|\Phi\rangle_{AB} &= \frac{1}{N} \sum_{i,j} \left({}_C\langle i| \otimes {}_A\langle j| \right) \left(|j\rangle_A \otimes |i\rangle_B \right) = \\ &= \frac{1}{N} \sum_i |i\rangle_B \, {}_C\langle i| = \frac{1}{N} \mathbf{T}_{BC}. \end{aligned} \tag{4.87}$$

Здесь мы определили *трансфер-оператор* (или *оператор переноса*) $\mathbf{T}_{BC}$, который обладает свойством

$$\mathbf{T}_{BC}|\varphi\rangle_C = \mathbf{T}_{BC} \left(\sum_i a_i |i\rangle_C \right) = \sum_i a_i |i\rangle_B = |\varphi\rangle_B ; \tag{4.88}$$

он отображает состояние из C на идентичное состояние в B. Это свойство не имеет инвариантного смысла, независимого от выбора базиса в B и C; скорее $\mathbf{T}_{BC}$ просто описывает произвольный способ связать ортонормированные базисы двух систем. Конечно, Алисе и Бобу придется определенным образом ориентировать свои базисы, чтобы проверить, что телепортация действительно состоялась.

Теперь вспомним, что любое другое максимально запутанное $N \times N$-состояние имеет разложение Шмидта вида

$$\frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i'\rangle \otimes |i\rangle \tag{4.89}$$

и может быть выражено как

$$|\Phi(\mathbf{U})\rangle \equiv \mathbf{U} \otimes \mathbf{1}|\Phi\rangle, \tag{4.90}$$

где

$$\mathbf{U}|i\rangle = |i'\rangle = \sum_j |j\rangle U_{ji}. \tag{4.91}$$

Записывая

$$|\Phi(\mathbf{U})\rangle_{AB} = \frac{1}{\sqrt{N}} \sum_{i,j} |j\rangle_A \otimes |i\rangle_B U_{ji}, \tag{4.92}$$

можно легко проверить, что

$${}_{CA}\langle\Phi(\mathbf{U})|\Phi(\mathbf{V}^T)\rangle_{AB} = \frac{1}{N}(\mathbf{V}\mathbf{U}^{-1})_B \mathbf{T}_{BC}, \tag{4.93}$$

где $\mathbf{V}^T$ обозначает транспонированную матрицу $\mathbf{V}$ в стандартном базисе ($V_{ij}^T = V_{ji}$); тогда, *в частности, для любой* унитарной матрицы $\mathbf{U}$ трансфер-оператор может быть представлен в виде

$$\frac{1}{N}\mathbf{T}_{BC} = {}_{CA}\langle\Phi(\mathbf{U})|\Phi(\mathbf{U}^T)\rangle_{AB}. \tag{4.94}$$

Предположим теперь, что Алиса и Боб делят $|\Phi\rangle_{AB}$, а Чарли приготовил состояние $|\psi\rangle_C$ и оставил его на хранение в лаборатории Алисы. Алиса выполняет измерение, которое проецирует CA на базис максимально запутанных состояний, получая результат $|\Phi(\mathbf{U}_a)\rangle_{CA}$ для некоторого унитарного преобразования $\mathbf{U}_a$. Тогда из уравнения (4.94) известно, что *если бы* Алиса и Боб вместо $|\Phi\rangle_{AB}$ поделили состояние $|\Phi(\mathbf{U}_a^T)\rangle_{CA}$, то измерение Алисы приготовило бы в лаборатории Боба идеальную копию (реплику) состояния $|\psi\rangle$. К сожалению, они не догадались с самого начала поделить подходящее состояние. Но еще не все потеряно! Боб понимает, что

$$|\Phi(\mathbf{U}_a^T)\rangle_{AB} = \mathbf{1}_A \otimes (\mathbf{U}_a)_B |\Phi\rangle_{AB}, \tag{4.95}$$

и, конечно, $(\mathbf{U}_a)_B$ коммутирует с измерением Алисы. Следовательно, когда Боб узнает у Алисы, что результатом ее измерения было $|\Phi(\mathbf{U}_a^T)\rangle_{AB}$, он применит $(\mathbf{U}_a)_B$ к своей половине поделенного с Алисой состояния. Тогда протокол станет эквивалентным тому, в котором они с самого начала делили именно то, какое нужно, максимально запутанное состояние, а состояние Боба преобразуется в $|\psi\rangle_B$!

Этот подход к телепортации имеет некоторые концептуальные преимущества. Во-первых, можно легко убедиться в том, что Алисе не требуется выполнять ортогональное измерение. Чтобы осуществить телепортацию с точностью воспроизведения $F = 1$, ей достаточно выполнить ПОЗМ с операторами $\mathbf{M}_a$, где каждый $\mathbf{M}_a$ обладает свойством

$$\mathbf{M}_a^\dagger \mathbf{M}_a \propto |\Phi(\mathbf{U}_a)\rangle\langle\Phi(\mathbf{U}_a)| \tag{4.96}$$

для некоторого унитарного преобразования $\mathbf{U}_a$. Так же легко можно увидеть, как должен быть модифицирован протокол телепортации, если начальным максимально запутанным состоянием, которое делят Алиса и Боб, является не $|\Phi\rangle_{AB}$, а

$$|\Phi(\mathbf{V}^T)\rangle_{AB} = \mathbf{1}_A \otimes \mathbf{V}_B |\Phi\rangle_{AB}. \tag{4.97}$$

Если результатом измерения Алисы является $|\Phi(\mathbf{U}_a)\rangle_{CA}$, то уравнение (4.93) говорит нам, что состояние Боба принимает вид

$$\mathbf{V}\mathbf{U}_a^{-1}|\psi\rangle_B. \tag{4.98}$$

Чтобы воспроизвести $|\psi\rangle_B$, Боб должен применить преобразование $\mathbf{U}_a\mathbf{V}^{-1}$.

Порядок следования операторов в уравнении (4.98) на первый взгляд может показаться интуитивно непонятным — он выглядит так, как если бы измерение Алисы $(\mathbf{U}_a)$ предшествовало приготовлению разделяемого запутанного состояния $(\mathbf{V})$. Однако это «обращение времени» имеет непосредственное толкование. Если результатом измерения Алисы является $|\Phi(\mathbf{U}_a)\rangle_{CA}$, то Боб получил бы идеальную копию $|\psi\rangle$, если бы начальным состоянием было $\mathbf{1}_A \otimes (\mathbf{U}_a)_B |\Phi\rangle_{AB}$. Чтобы смоделировать ситуацию, в которой сразу было подходящим образом выбрано запутанное состояние, Боб сначала применяет $\mathbf{V}^{-1}$, чтобы скомпенсировать «поворот» в $|\Phi(\mathbf{V}^T)\rangle_{AB}$ и восстановить $|\Phi\rangle_{AB}$, а затем применяет $\mathbf{U}_a$, чтобы преобразовать запутанное состояние к требуемому виду.

Существует более фантастическая интерпретация уравнения (4.98), которая хотя и необязательна, но тем не менее неопровержима. Мы можем «объяснить», как квантовая информация переносится от Алисы к Бобу, следуя движению кубита вдоль мировой линии в пространстве-времени. Кубит движется вперед во времени от его приготовления Чарли до измерения Алисой, затем – назад от измерения до первоначального приготовления запутанной пары и, наконец, снова вперед во времени от приготовления пары до лаборатории Боба. Поскольку эта мировая линия посещает измерение Алисы прежде чем добирается до приготовления запутанной пары, $\mathbf{U}_a^{-1}$ действует «первым», а $\mathbf{V}$ – «позднее».

4.4.4. Квантовый программный продукт

Телепортация имеет некоторые интересные приложения. Представим, например, что Алиса и Боб хотят применить «квантовый вентиль» $\mathbf{V}$ к неизвестному состоянию $|\psi\rangle_C$. Но применение $\mathbf{V}$ требует сложного оборудования, которое они себе не могут позволить.

Более экономичная альтернатива – *приобрести квантовый программный продукт* – бинарное состояние, которым, как уверяет продавец, является

$$|\Phi(\mathbf{V}^T)\rangle_{AB} = \mathbf{1}_A \otimes \mathbf{V}_B |\Phi\rangle_{AB}. \tag{4.99}$$

Аппаратное обеспечение Алисы достаточно мощное, чтобы выполнить измерение, проецирующее на базис $\{|\Phi(\mathbf{U}_a)\rangle_{CA}\}$; коль скоро результат a известен, состояние $\mathbf{V}\mathbf{U}_a^{-1}|\psi\rangle_B$ – приготовлено. Тогда Боб может завершить выполнение $\mathbf{V}$ на $|\psi\rangle_B$, применяя преобразование $\mathbf{V}\mathbf{U}_a\mathbf{V}^{-1}$.

Эта процедура может показаться неразумной – почему мы считаем, что Боб может применить преобразование $\mathbf{V}\mathbf{U}_a\mathbf{V}^{-1}$, но не способен применить $\mathbf{V}$? В действительности это не так глупо, а имеет важные применения к отказоустойчивым квантовым вычислениям, которые мы будем изучать позднее в главе 8[1]. В некоторых случаях *выполнение* $\mathbf{V}\mathbf{U}_a\mathbf{V}^{-1}$ в действительности несколько проще, нежели применение $\mathbf{V}$. Более того, вместо того, чтобы приобретать квантовое программное обеспечение, Алиса и Боб могут сами приготовить его, даже несмотря на то, что они не могут надежно применить $\mathbf{V}$. Это возможно, поскольку проще проверить, что было должным образом приготовлено *известное* квантовое состояние, чем проверять, что известное унитарное преобразование было успешно применено

[1] В это издание вошли первые шесть глав лекций Прескилла. Редакция РХД предполагает издание второй части, которая будет посвящена теории квантовых кодов, исправляющих ошибки, отказоустойчивых вычислений, топологических квантовых вычислений и другим вопросам. – *Прим. ред.*

к неизвестному состоянию. Если нельзя положиться на применяющее **V** аппаратное обеспечение, то мы предпочтем использовать его автономно для подготовки компьютерной программы, чтобы применить ее с гарантированной надежностью, нежели рисковать нанести неустранимое повреждение нашему неизвестному состоянию вследствие ошибочного выполнения **V**.

С каждым применением **V** расходуется одна копия квантового программного обеспечения. Таким образом, протокол выполнения преобразования **V** с его помощью использует запутывание как ресурс.

4.5. Квантовая криптография

4.5.1. Распределение квантового ЭПР-ключа

У каждого есть свои секреты, Алиса и Боб не исключение. Алисе нужно передать Бобу очень личное сообщение, но у них есть очень любопытная подружка, Ева, которая наверняка попытается их подслушать. Могут ли они связаться, будучи уверенными, что Еве это не удастся?

Очевидно, им нужно воспользоваться каким-то кодом. Но беда в том, что Ева не только очень любопытна, но и весьма ловка. Алиса и Боб не уверены, что им хватит ума придумать такой код, который Ева не сможет взломать, за исключением одной схемы кодирования, которая абсолютно надежна. Если Алиса и Боб поделят *тайный ключ*, известную только им случайную последовательность битов, тогда Алиса может конвертировать свое письмо в кодах ASCII (ряд битов не длиннее ключа), *сложив* (по модулю два) каждый бит своего сообщения с соответствующим битом ключа, и послать результат Бобу. Получив этот ряд, Боб может добавить ключ, чтобы извлечь сообщение Алисы.

Эта схема надежна, так как, даже если Ева перехватит сообщение, она ничего не сможет узнать, поскольку передаваемая последовательность сама по себе не несет никакой информации — сообщение закодировано в корреляции между передаваемой строкой и *ключом* (который Ева не знает).

Тем не менее проблема все еще остается, поскольку Алисе и Бобу необходимо установить общий случайный ключ и они должны быть уверены, что Ева не сможет его узнать. Они могли бы встретиться, чтобы обменяться ключом, но это может оказаться невыполнимо. Они могли бы доверить третьему лицу передать этот ключ, но что если оно состоит в тайном сговоре с Евой? Они могли бы использовать протоколы распределения «открытых ключей», но их надежность опирается на предположения относительно вычислительных ресурсов, доступных потенциальному противнику. Действительно, в главе 6 мы увидим, что протоколы открытых

ключей беззащитны перед атакой хакера, располагающего квантовым компьютером.

Могут ли Алиса и Боб использовать *квантовую* информацию (и особенно запутывание) для решения проблемы передачи ключа? Могут! Можно придумать протоколы *распределения квантовых ключей*, которые будут неуязвимы для любой, допустимой законами физики, атаки.

Предположим, что Алиса и Боб делят запас запутанных пар, приготовленных в состоянии $|\phi^+\rangle$. Чтобы приготовить известный только им тайный ключ, они должны выполнить следующий протокол.

Для каждого находящегося в их распоряжении кубита Алиса и Боб решают измерять или σ_1, или σ_3. Это решение является псевдо-случайным, каждый выбор реализуется с вероятностью $1/2$. Затем, после того как измерения выполнены, они открыто объявляют о том, какие наблюдаемые были измерены, но не открывают полученные ими результаты. В тех случаях (примерно в половине), в которых они измерили свои кубиты вдоль разных осей, их результаты отбрасываются (поскольку в них получены нескоррелированные результаты). В тех же случаях, в которых они выполнили измерения вдоль одних и тех же осей, их результаты хотя и случайны, но *идеально скоррелированы*. Следовательно, они установили между собой случайный ключ.

Но действительно ли этот протокол неуязвим перед коварной атакой Евы? В частности, еще раньше Ева могла тайком исказить пары. Тогда пары, которыми располагают Алиса и Боб, могут и не находиться в идеальных $|\phi^+\rangle$-состояниях, а скорее они будут запутаны с кубитами Евы (без ведома Алисы и Боба). Тогда Ева может подождать до тех пор, пока Алиса и Боб не сделают своего заявления, чтобы соответствующим образом выполнить измерение своих кубитов и получить максимальную информацию о полученных ими результатах. Алиса и Боб должны защититься от подобной атаки.

Если Ева действительно исказила пары Алисы и Боба, тогда наиболее общее возможное состояние AB-пары и множества E-кубитов имеет вид

$$|\Upsilon\rangle_{ABE} = |00\rangle_{AB}|e_{00}\rangle_E + |01\rangle_{AB}|e_{01}\rangle_E + \\ + |10\rangle_{AB}|e_{10}\rangle_E + |11\rangle_{AB}|e_{11}\rangle_E, \qquad (4.100)$$

где состояния кубитов Евы $|e_{ij}\rangle_E$ ни нормированы, ни взаимно ортогональны. Вспомним теперь, что определяющим свойством $|\phi^+\rangle$ является то, что оно представляет собой собственное состояние как $\sigma_1^{(A)} \otimes \sigma_1^{(B)}$, так и $\sigma_3^{(A)} \otimes \sigma_3^{(B)}$ с собственным значением $+1$. Предположим, что Алиса и Боб

могут проверить, обладают ли этим свойством имеющиеся у них кубиты. Чтобы удовлетворялось $\boldsymbol{\sigma}_3^{(A)} \otimes \boldsymbol{\sigma}_3^{(B)} = 1$, мы должны иметь

$$|\Upsilon\rangle_{ABE} = |00\rangle_{AB}|e_{00}\rangle_E + |11\rangle_{AB}|e_{11}\rangle_E, \tag{4.101}$$

а чтобы выполнялось $\boldsymbol{\sigma}_1^{(A)} \otimes \boldsymbol{\sigma}_1^{(B)} = 1$, мы должны иметь

$$|\Upsilon\rangle_{ABE} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})|e\rangle_E = |\phi^+\rangle_{AB}|e\rangle_E. \tag{4.102}$$

Мы видим, что AB-пары могут быть собственными состояниями операторов $\boldsymbol{\sigma}_1^{(A)} \otimes \boldsymbol{\sigma}_1^{(B)}$ и $\boldsymbol{\sigma}_3^{(A)} \otimes \boldsymbol{\sigma}_3^{(B)}$, если только они полностью незапутаны с кубитами Евы. Следовательно, измеряя свои кубиты, она не сможет что-либо узнать о результатах измерений Алисы и Боба. Случайный ключ надежен.

Чтобы проверить свойства $\boldsymbol{\sigma}_1^{(A)} \otimes \boldsymbol{\sigma}_1^{(B)} = 1 = \boldsymbol{\sigma}_3^{(A)} \otimes \boldsymbol{\sigma}_3^{(B)}$, Алиса и Боб могут пожертвовать частью своего общего ключа и открыто сравнить результаты своих измерений. Они должны обнаружить, что их результаты действительно идеально скоррелированы. Если это так, то с высокой статистической надежностью они будут уверены в том, что Ева не в состоянии перехватить ключ. Если нет, то они зарегистрировали гнусную деятельность Евы. Тогда они могут выбросить этот ключ и сделать новую попытку установить надежный ключ.

Как я только что это представил, протокол распределения квантового ключа, казалось бы, требует наличия разделенных между Алисой и Бобом запутанных пар, но на самом деле это не так. Мы можем представить, что Алиса сама готовит пары $|\phi^+\rangle$, а затем измеряет один кубит в каждой паре, прежде чем послать другой Бобу. Это полностью эквивалентно схеме, в которой Алиса готовит одно из четырех состояний

$$|\uparrow_z\rangle, \quad |\downarrow_z\rangle, \quad |\uparrow_x\rangle, \quad |\downarrow_x\rangle \tag{4.103}$$

(выбираемое случайным образом, каждое из них возникает с вероятностью 1/4) и посылает кубит Бобу. Тогда измерение Боба и проверка выполняются, как и раньше. Эта схема (известная как протокол распределения квантового ключа BB84 [1]) так же надежна, как и схема, основанная на запутывании[2].

[1] Предложен Беннетом и Брассаром в 1984 г.: C.H. Bennett, G. Brassard, in *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing*, IEEE, New York (1984). Экспериментально реализован в экспериментах с поляризованными фотонами. Детальное обсуждение можно найти в книге *Физика квантовой информации*, под ред. Д. Боумейстера, А. Экерта и А. Цайлингера, Постмаркет, М.: (2002). — *Прим. ред.*

[2] За исключением того, что в ЭПР-схеме Алиса и Боб могут подождать с созданием ключа до тех пор, пока им не понадобится поговорить, сокращая таким образом риск того, что в какой-то момент Ева может совершить взлом, чтобы узнать, какие состояния приготовила Алиса (и таким образом извлечь ключ).

Другой интригующий вариант называется «обращенной во времени ЭПР» схемой. Здесь и Алиса и Боб готовят по одному из четырех состояний (4.103) и отсылают свои кубиты Чарли. Тогда Чарли выполняет измерение Белла на паре, то есть он измеряет $\sigma_1^{(A)} \otimes \sigma_1^{(B)}$ и $\sigma_3^{(A)} \otimes \sigma_3^{(B)}$, совершая ортогональную проекцию на одно из состояний $|\phi^{\pm}\rangle$, $|\psi^{\pm}\rangle$, и открыто объявляет о результате. Поскольку все четыре из этих состояний одновременно являются собственными состояниями операторов $\sigma_1^{(A)} \otimes \sigma_1^{(B)}$ и $\sigma_3^{(A)} \otimes \sigma_3^{(B)}$, когда Алиса и Боб приготовили свои спины ориентированными вдоль одной и той же оси (что они делают примерно в половине случаев), они делят один бит[1]. Конечно, Чарли может оказаться в союзе с Евой, но, как и прежде, путем сравнения части своих кодов, Алиса и Боб могут проверить, что те не имели доступа к информации. Эта схема имеет то преимущество, что Чарли мог бы заведовать центральной коммутаторной станцией, храня кубиты, полученные от многих людей, и выполняя измерение Белла, когда двое из абонентов запросят установить безопасную связь. (Здесь мы предполагаем, что Чарли имеет устойчивую квантовую память, в которой кубит может храниться надежно и сколь угодно долго.) Безопасный ключ может быть установлен даже при временно закрытой линии квантовой связи, если оба абонента догадались послать свои кубиты Чарли раньше (когда квантовый канал был открыт).

До сих пор мы делали нереалистичное предположение о том, что квантовый канал связи идеален, но, конечно, в реальном мире будут возникать ошибки. Следовательно, даже если Ева не причинила никакого ущерба, Алиса и Боб иногда будут обнаруживать, что их проверочный тест терпит неудачу. Но как им отличить ошибки, возникающие из-за дефектов канала, от ошибок, возникающих в результате вторжения Евы?

Обращаясь к этой проблеме, Алиса и Боб могут усовершенствовать их протокол в двух отношениях. Во-первых, они могут осуществить (классическую) коррекцию ошибок, чтобы сократить эффективную частоту их появления. Например, чтобы установить каждый бит их общего ключа, они могут в действительности заменить его блоком трех случайных битов. Если среди трех битов не все одинаковые, то Алиса может сообщить Бобу, какой из них отличается от двух других; Боб может инвертировать этот бит в своем блоке, а *затем* использовать подсчет большинства голосов для определения значения бита для блока. Таким способом Алиса и Боб разделят одинаковый бит ключа, даже если для одного бита в блоке из трех возникла ошибка.

[1]Пока Чарли не выполнил свое измерение, состояния, приготовленные Алисой и Бобом, полностью некоррелированы. Определенная корреляция (или антикорреляция) устанавливается после того, как Чарли выполнит свое измерение.

Однако одной лишь коррекции ошибок недостаточно для уверенности в том, что Ева не получила информацию о ключе — коррекция ошибок должна быть дополнена (классическим) секретным усилением. Например, после выполнения коррекции ошибок, когда Алиса и Боб уже уверены, что располагают одинаковыми ключами, они могут выделить бит «суперключа», например, *четность* n битов ключа. Чтобы узнать *что-нибудь* о четности n битов, Еве нужно *хотя бы что-нибудь* узнать о каждом бите. Следовательно, бит четности в среднем существенно более надежен, чем каждый из отдельных битов ключа.

Если частота ошибок в канале достаточно низка, то можно показать, что распределение квантового ключа, дополненное коррекцией ошибок и секретным усилением, неуязвимо для любой атаки, которую может предпринять Ева (в том смысле, что можно гарантировать, что полученная ею информация будет сколь угодно мала). Мы вернемся к проблеме обеспечения безопасности распределения квантового ключа в главе 7.

4.5.2. Невозможность клонирования

Безопасность распределения квантового ключа основана на существенном различии между квантовой и классической информацией. Невозможно получить информацию, *определяющую различие* между неортогональными квантовыми состояниями, не *внося возмущение* в эти состояния.

Например, в протоколе BB84 Алиса посылает Бобу любое из четырех состояний, $|\uparrow_z\rangle$, $|\downarrow_z\rangle$, $|\uparrow_x\rangle$, $|\downarrow_x\rangle$: и они имеют возможность проверить, что ни одно из этих состояний не возмущено попыткой подслушивания со стороны Евы. В более общем виде предположим, что $|\varphi\rangle$ и $|\psi\rangle$ — два неортогональных состояния в $\mathcal{H}$ ($\langle\psi|\varphi\rangle \neq 0$) и что в $\mathcal{H}\otimes\mathcal{H}_E$ (где $\mathcal{H}_E$ — доступное Еве гильбертово пространство) применяется унитарное преобразование U, не возмущающее $|\varphi\rangle$ и $|\psi\rangle$. Тогда

$$U\colon \begin{cases} |\psi\rangle\otimes|0\rangle_E \to |\psi\rangle\otimes|e\rangle_E, \\ |\varphi\rangle\otimes|0\rangle_E \to |\varphi\rangle\otimes|f\rangle_E, \end{cases} \tag{4.104}$$

а унитарность предполагает, что

$$\begin{aligned} \langle\psi|\varphi\rangle &= \big({}_E\langle 0|\otimes\langle\psi|\big)\big(|\varphi\rangle\otimes|0\rangle_E\big) = \\ &= \big({}_E\langle e|\otimes\langle\psi|\big)\big(|\varphi\rangle\otimes|f\rangle_E\big) = \langle\psi|\varphi\rangle\langle e|f\rangle. \end{aligned} \tag{4.105}$$

Таким образом, при $\langle\psi|\varphi\rangle \neq 0$ мы имеем $\langle e|f\rangle = 1$ и, поскольку состояния нормированы, $|e\rangle = |f\rangle$. Это означает, что ни одно измерение в $\mathcal{H}_E$ не

может дать информацию, отличающую $|\psi\rangle$ от $|\varphi\rangle$. В случае BB84 это доказательство показывает, что если Ева не вносит возмущения в состояния, посланные Алисой, то состояния в $\mathcal{H}_E$ остаются неизменными, независимо от того, какое из четырех состояний $|\uparrow_z\rangle$, $|\downarrow_z\rangle$, $|\uparrow_x\rangle$, $|\downarrow_x\rangle$ было послано, и, следовательно, Ева ничего не узнает о разделенном Алисой и Бобом ключе. С другой стороны, если Алиса посылает Бобу одно из двух ортогональных состояний $|\uparrow_z\rangle$ или $|\downarrow_z\rangle$, то ничто не мешает Еве получить копию информации (как в случае с классическими битами).

Ранее мы отмечали, что если у нас есть множество идентичных копий кубита, то можно измерить средние значения некоммутирующих наблюдаемых типа σ_1, σ_2 и σ_3, чтобы полностью определить матрицу плотности кубита. Неотъемлемым в выводе о том, что неортогональные состояния нельзя различить не возмутив их, является неявное утверждение, что невозможно сделать идеальную копию кубита. (Если бы мы могли, мы сделали бы столько копий, сколько их необходимо для определения $\langle\sigma_1\rangle$, $\langle\sigma_2\rangle$ и $\langle\sigma_3\rangle$ с любой наперед заданной точностью.) Сформулируем это в явном виде: не существует квантового ксерокса.

Ортогональные квантовые состояния (подобные классической информации) *могут* надежно копироваться. Например, унитарное преобразование, действующее как

$$U\colon \begin{cases} |0\rangle_A|0\rangle_E \to |0\rangle_A|0\rangle_E, \\ |1\rangle_A|0\rangle_E \to |1\rangle_A|1\rangle_E, \end{cases} \tag{4.106}$$

копирует первый кубит на второй, если первый является одним из двух состояний: $|0\rangle_A$ или $|1\rangle_A$. Но если вместо этого первый кубит находится в состоянии $|\psi\rangle = a|0\rangle_A + b|1\rangle_A$, то

$$U\colon \big(a|0\rangle_A + b|1\rangle_A\big)|0\rangle_E \to a|0\rangle_A|0\rangle_E + b|1\rangle_A|1\rangle_E. \tag{4.107}$$

Это не состояние $|\psi\rangle \otimes |\psi\rangle$ (тензорное произведение исходного состояния и его копии); скорее это нечто совершенно отличное — запутанное состояние двух кубитов.

Чтобы рассмотреть наиболее общий квантовый ксерокс, допустим, что полное гильбертово пространство шире тензорного произведения исходного пространства и пространства копий. Тогда наиболее общее «копирующее» унитарное преобразование действует как

$$U\colon \begin{cases} |\psi\rangle_A|0\rangle_E|0\rangle_F \to |\psi\rangle_A|\psi\rangle_E|e\rangle_F, \\ |\varphi\rangle_A|0\rangle_E|0\rangle_F \to |\varphi\rangle_A|\varphi\rangle_E|f\rangle_F. \end{cases} \tag{4.108}$$

Тогда унитарность предполагает, что

$$ {}_A\langle\psi|\varphi\rangle_A = {}_A\langle\psi|\varphi\rangle_A \, {}_E\langle\psi|\varphi\rangle_E \, {}_F\langle e|f\rangle_F ; \tag{4.109} $$

следовательно, если ${}_A\langle\psi|\varphi\rangle_A \neq 0$, то

$$ 1 = {}_E\langle\psi|\varphi\rangle_E \, {}_F\langle e|f\rangle_F . \tag{4.110} $$

Поскольку состояния нормированы, мы приходим к выводу, что

$$ |\langle\psi|\varphi\rangle| = 1, \tag{4.111} $$

то есть $|\psi\rangle$ и $|\varphi\rangle$ в действительности представляют один и тот же луч. Ни одна унитарная машина не может сделать копии $|\varphi\rangle$ и $|\psi\rangle$, если они являются *различными неортогональными состояниями*. Этот результат называется теоремой о невозможности клонирования.

4.6. Многокомпонентное запутывание

4.6.1. Три квантовых ящика

После безумно успешного эксперимента с тремя монетами на столе Алиса и Боб стали всемирно известными. Они стали профессорами, Алиса в КАЛТЕХе, а Боб в Чикаго. Они слишком занятые, чтобы проводить много времени в лабораториях, но у них достаточно аспирантов и они продолжают активно заниматься наукой.

Их лучший студент, Чарли, который выполнял всю черновую работу в эксперименте с монетами, закончил образование и теперь он доцент в Принстоне. Алиса и Боб хотели бы содействовать карьере Чарли и помочь ему занять постоянную должность. Однажды они болтали по телефону.

Алиса: Знаешь, Боб, мы, конечно, должны помочь Чарли. Ты можешь придумать подходящий эксперимент, который мы можем выполнить втроем?

Боб: Ну, я не знаю, Алиса. Есть множество экспериментов, которые я хотел бы выполнить с нашими запутанными парами кубитов. Но в каждом эксперименте есть один кубит для меня, а другой — для тебя. Похоже, что Чарли — третий лишний.

Алиса: [*Длинная пауза*]. Боб... А ты когда-нибудь думал о постановке эксперимента с тремя кубитами?

У Боба отвисла челюсть и подскочил пульс. Во внезапном прозрении он словно увидел перед собой всю свою будущую карьеру. По правде говоря, Боб уже начинал задумываться о том, что их эксперименты с двумя кубитами порядком устарели. Теперь он знает, что в ближайшие пять лет он всецело посвятит себя выполнению полного трехкубитового эксперимента. К тому времени он, Алиса и Чарли обучат другого блестящего студента и будут готовы подступиться к четырем кубитам. Затем еще один студент и еще один кубит. И так до самой пенсии.

Вот как выглядит эксперимент с тремя кубитами, который Алиса и Боб решили попробовать осуществить: Алиса поручает сотруднику своей лаборатории в КАЛТЕХе тщательно приготовить состояние трех квантовых ящиков. (Но Алиса не знает точно, как он это сделает.) Она оставляет один ящик у себя, а два других отправляет срочной квантовой почтой Бобу и Чарли. В каждом ящике находится шар, который может быть или черным, или белым, но ящик плотно закрыт. Единственная возможность узнать, что находится внутри, — это открыть ящик, но открыть его можно двумя различными способами — ящик имеет две дверцы, промаркированные как X и Y. Определить цвет шара можно, когда открывается одна из двух дверок. Но невозможно открыть обе дверцы сразу.

Алиса, Боб и Чарли собираются исследовать, как скоррелированы ящики. Они проводят множество тщательно контролируемых испытаний. Каждый раз один из них, выбранный жребием, открывает дверцу X, тогда как двое других открывают дверцу Y. Удачливые, как всегда, Алиса, Боб и Чарли делают удивительное открытие. Они обнаруживают, что *всякий раз*, когда они открывают ящики в таком порядке, они находят нечетное количество черных шаров.

То есть Алиса, Боб и Чарли обнаружили, что когда они открывают дверцу X на одном ящике и дверцы Y на двух других, то гарантированно наблюдают одно из сочетаний цветов:

$$0_A0_B1_C, \quad 0_A1_B0_C, \quad 1_A0_B0_C, \quad 1_A1_B1_C \tag{4.112}$$

(0 обозначает белый, 1 — черный). Они ни разу не наблюдали ни одного сочетания из

$$1_A1_B0_C, \quad 1_A0_B1_C, \quad 0_A1_B1_C, \quad 0_A0_B0_C. \tag{4.113}$$

независимо от того, у какого из трех ящиков была открыта дверца X.

Некоторое время спустя Алиса, Боб и Чарли понимают, что после открытия двух ящиков они всегда могут предсказать, что произойдет, когда

будет открыт третий ящик. Если первые два шара одного цвета, то третий шар, разумеется, будет черным, а если первые два — разных цветов, то последний шар обязательно будет белым. Они проверяли это несметное количество раз, но так происходило всегда!

Даже после признания эксперимента с тремя монетами Алиса, Боб и Чарли не усомнились в своей приверженности к эйнштейновской локальности. Однажды между ними состоялся трехсторонний разговор.

Алиса: Знаете, парни, иногда я просто не могу решиться открыть ли дверцу X или дверцу Y своего ящика. Я знаю, я должна выбирать аккуратно . . . . Если я открою дверцу X, то я несомненно внесу возмущение в ящик; следовательно, я никогда не узнаю, что случилось бы, если бы вместо этого я открыла дверцу Y. А если я открою дверцу Y, я никогда не узнаю, что нашла бы, если бы открыла дверцу X. Это так огорчает!

Боб: Алиса, ты не права! Наш эксперимент показывает, что ты можешь знать оба эти случая. Неужели ты не видишь? Допустим, что ты хочешь знать, что произойдет, когда ты откроешь дверцу X. Тогда ты просто просишь Чарли и меня открыть дверцы Y наших ящиков и сообщить тебе, что мы обнаружили. Ты будешь знать абсолютно точно, без сомнения, что случится, если ты откроешь дверцу X. Мы проверяли это много раз, и это всегда работает. Так зачем же беспокоиться и открывать дверцу X? Ты можешь пойти дальше и вместо этого открыть дверцу Y и узнать, что ты найдешь. Таким образом ты реально узнаешь результаты открывания *обеих* дверок!

Чарли: Но как можно быть в этом уверенным? Если Алиса открывает дверцу Y, она теряет возможность открыть дверцу X. Она же не может реально получить оба этих случая. После того, как она открывает дверцу Y, мы не можем проверить, произойдет ли ожидаемый результат при открывании дверцы X.

Боб: Да ну, как может случиться другое? Смотри, ты же на самом деле не думаешь, что ты со своим ящиком в Принстоне, а я со своим — в Чикаго можем оказать какое-то влияние на то, что найдет Алиса, когда она откроет свой ящик в Пасадене, не так ли? Когда мы открываем наши ящики, мы ничего не можем изменить в ящике Алисы; мы только узнаем информацию, необходимую для того, чтобы с уверенностью предсказать, что обнаружит Алиса.

Чарли: Ну, может быть, нам следовало бы выполнить несколько больше экспериментов, чтобы выяснить, что вы в этом правы.

Действительно, открытие корреляции трех ящиков сделало Алису и Боба даже более знаменитыми, чем раньше, но Чарли еще не получил той репутации, которой заслуживает, – он все еще без должности. Не удивительно, что он хочет выполнить больше экспериментов! Он продолжает:

Чарли: Здесь есть нечто такое, что мы можем проверить. Во всех выполненных до сих пор экспериментах мы всегда открывали дверцу Y на двух ящиках и дверцу X на одном. Может быть, нам нужно проверить нечто другое. Например, может быть, нам стоит посмотреть, что произойдет, если мы откроем одни и те же дверцы на всех трех ящиках. Мы могли бы проверить открытие трех X-дверок.

Боб: Да ну! Мне надоели эти три ящика. Мы уже все о них знаем. Пора двигаться дальше, и, я думаю, Диана уже готова нам помогать. Давайте перейдем к четырем ящикам!

Алиса: Нет, я считаю, что Чарли прав. Мы действительно не можем сказать, что мы все знаем о трех ящиках, пока не поэкспериментируем с другими способами открывания дверок.

Боб: Забудьте об этом! Нас ни за что не финансируют. После того как мы вложили столько усилий в открывание двух Y-ов и одной X, мы скажем, что теперь мы хотим открывать три X. Нам скажут, что сначала вы занимались ерундой, а теперь вы предлагаете заняться чепухой. Да нас просто поднимут на смех.

Алиса: Боб прав. Я думаю, что только одним способом мы сможем получить финансирование этого эксперимента, если мы сможем сделать предсказание относительно его исхода. Тогда мы сможем сказать, что выполняем эксперимент для проверки предсказания. Я слышала о неких теоретиках, Гринбергере, Горне, Цайлингере и Мермине (ГГЦМ). Они много размышляли о наших экспериментах с тремя ящиками; может, они смогут что-нибудь предложить.

Боб: Ну, в этих ящиках вся моя жизнь, а они просто банда теоретиков. Сомневаюсь, что они скажут что-нибудь интересное или полезное. Но на самом деле не важно, имеет ли их теория какой-нибудь смысл, я поддерживаю это предложение. Если мы сможем проверить ее, то я даже соглашусь с тем, что есть смысл выполнить новый эксперимент с тремя ящиками.

Итак, Алиса, Боб и Чарли совершают путешествие, чтобы познакомиться с ГГЦМ. И, несмотря на глубокий скептицизм Боба, ГГЦМ действительно делают очень интересное предложение.

ГГЦМ: Боб говорит, что, открывая ящики в Принстоне и в Чикаго, никак не возможно повлиять на то, что происходит, когда Алиса открывает ящик в Пасадене. Ну, допустим, что он прав. Теперь вы, парни, отправляетесь выполнять эксперимент, в котором вы все открываете X-дверцы. Никто не может сказать, что из этого получится, но мы можем рассуждать следующим образом: предположим, что если бы вы открыли три Y-дверцы, то обнаружили бы три белых шара. Тогда можно использовать аргументы Боба, чтобы понять, что если вместо этого вы откроете три X-дверцы, то найдете три черных шара. Это аналогично такому рассуждению: если Алиса открывает X, а Боб и Чарли открывают Y, тогда вы знаете наверняка, что количество черных шаров будет нечетным. Следовательно, если вы знаете, что Боб и Чарли, открыв дверцы Y, нашли по белому шару, то Алиса найдет черный, когда откроет дверцу X. Аналогично, если Алиса и Чарли, открыв дверцы Y, нашли по белому шару, то Боб найдет черный, когда откроет дверцу X. Наконец, если Алиса и Боб, открыв дверцы Y, нашли по белому шару, то Чарли должен найти черный, когда откроет дверцу X. Итак, мы видим, что[1]

$$Y_A Y_B Y_C = 000 \rightarrow X_A X_B X_C = 111. \tag{4.114}$$

Не так ли?

Боб: Ну, возможно, это достаточно логично, но насколько это полезно? Мы не знаем, что обнаружим внутри ящика, пока не откроем его. Вы предположили, что $Y_A Y_B Y_C = 000$, но мы никогда не знаем это заранее.

ГГЦМ: Безусловно, но подождите. Да, вы правы, что мы не можем знать заранее, что мы найдем, если откроем дверцу Y на каждом ящике. Но для трех ящиков имеется только восемь возможностей, и мы можем легко их все перечислить. А для каждой из этих восьми возможностей для $Y_A Y_B Y_C$ мы можем использовать те же рассуждения, что и раньше, чтобы сделать вывод о значении $X_A X_B X_C$. Мы получаем таблицу

[1] Здесь 0 обозначает белый шар, а 1 — черный; Y_A означает то, что находит Алиса, когда открывает дверцу Y на своем ящике, *и так далее*.

типа этой:

$$\begin{aligned}
Y_A Y_B Y_C = 000 &\rightarrow X_A X_B X_C = 111 \\
Y_A Y_B Y_C = 001 &\rightarrow X_A X_B X_C = 001 \\
Y_A Y_B Y_C = 010 &\rightarrow X_A X_B X_C = 010 \\
Y_A Y_B Y_C = 100 &\rightarrow X_A X_B X_C = 100 \\
Y_A Y_B Y_C = 011 &\rightarrow X_A X_B X_C = 100 \\
Y_A Y_B Y_C = 101 &\rightarrow X_A X_B X_C = 010 \\
Y_A Y_B Y_C = 110 &\rightarrow X_A X_B X_C = 001 \\
Y_A Y_B Y_C = 111 &\rightarrow X_A X_B X_C = 111
\end{aligned} \tag{4.115}$$

Боб: Хорошо, ну и что?

ГГЦМ: Есть нечто замечательное в этой таблице, Боб! Взгляни на значения $X_A X_B X_C$... Каждое из них имеет нечетное количество единиц. Это и есть наше предсказание. Когда вы все будете открывать дверцу X на ваших ящиках, вы всегда будете находить нечетное количество черных шаров! Может быть один, может быть три, но всегда *нечетное количество*.

Конечно же, Алиса, Боб и Чарли восхищены проницательностью ГГЦМ. Они предложили продолжить эксперимент, который был одобрен и щедро профинансирован. Наконец, наступает долгожданный день, когда они в первый раз выполняют эксперимент. И когда Алиса, Боб и Чарли, каждый, открывает дверцу X на своем ящике, можете ли вы угадать, что они обнаруживают? Три белых шара. Вах!!!

Подозревая ошибку, Алиса, Боб и Чарли очень тщательно повторяют эксперимент, снова и снова, и снова... Но в каждом испытании, всякий раз, они находят четное количество черных шаров, когда они открывают дверцу X на всех трех ящиках. Иногда — ни одного, иногда — два, но никогда — один, и никогда — три. То, что они обнаруживали, всегда было прямо противоположно тому, что предсказывали ГГЦМ, исходя из принципа эйнштейновской локальности!

Снова отчаяние приводит жаждущих просвещения Алису, Боба и Чарли в библиотеку. После некоторого изучения учебника по квантовой механике и основательного допроса сотрудника лаборатории Алисы они понимают, что их три ящика были приготовлены в квантовом ГГЦМ-состоянии:

$$|\psi\rangle_{ABC} = \frac{1}{\sqrt{2}}\left(|000\rangle_{ABC} + |111\rangle_{ABC}\right), \tag{4.116}$$

являющемся одновременно собственным состоянием трех наблюдаемых

$$\mathbf{Z}_A \otimes \mathbf{Z}_B \otimes \mathbf{1}_C, \quad \mathbf{1}_A \otimes \mathbf{Z}_B \otimes \mathbf{Z}_C, \quad \mathbf{X}_A \otimes \mathbf{X}_B \otimes \mathbf{X}_C \tag{4.117}$$

с единичным собственным значением. А так как $\mathbf{ZX} = i\mathbf{Y}$, они понимают, что это состояние обладает свойствами:[1]

$$\begin{aligned} \mathbf{Y}_A \otimes \mathbf{Y}_B \otimes \mathbf{X}_C &= -1, \\ \mathbf{X}_A \otimes \mathbf{Y}_B \otimes \mathbf{Y}_C &= -1, \\ \mathbf{Y}_A \otimes \mathbf{X}_B \otimes \mathbf{Y}_C &= -1, \\ \mathbf{X}_A \otimes \mathbf{X}_B \otimes \mathbf{X}_C &= 1. \end{aligned} \tag{4.118}$$

Открывая ящик с помощью дверцы X или дверцы Y, Алиса, Боб и Чарли выполняют измерение наблюдаемых $\mathbf{X}$ или $\mathbf{Y}$, результат которого $+1$ означает белый шар, а результат -1 — черный шар. Таким образом, если приготовлено трехкубитовое состояние (4.116), то уравнение (4.118) говорит, что нечетное количество черных шаров будет обнаруживаться, если дверца Y открывается на двух ящиках, а дверца X — на третьем, в то время как четное количество черных шаров будет обнаруживаться, если на всех трех ящиках открывается дверца X. Это поведение, недвусмысленно предсказываемое квантовой механикой, именно то, что казалось таким обескураживающим Алисе, Бобу и Чарли и их консервативным собратьям, приверженцам эйнштейновской локальности.

После дополнительного глубокого изучения учебника по квантовой механике Алиса, Боб и Чарли постепенно приходят к пониманию изъяна в их рассуждениях. Они знакомятся с принципом дополнительности Бора, принципом непримиримой несовместимости некоммутирующих наблюдаемых. Они поняли, что для того чтобы прийти к своему предсказанию, они должны были *постулировать* результат измерения $\mathbf{YYY}$, а затем делать заключение о результатах измерения $\mathbf{XXX}$. Пренебрегая требующими серьезного отношения предостережениями Нильса Бора, они пали жертвой самого пагубного заблуждения.

Как они и надеялись, эксперимент с тремя ящиками принес дальнейшее признание Алисе и Бобу, а также должность Чарли. Конечно, эксперимент с тремя монетами уже убедительно опроверг эйнштейновскую локальность; несмотря на это, эксперимент с тремя ящиками имел другой характер. В эксперименте с монетами Алиса и Боб могли открыть только

[1] Здесь используются обозначения $\mathbf{X}_A = \boldsymbol{\sigma}_1^{(A)}$, $\mathbf{Y}_B = \boldsymbol{\sigma}_2^{(B)}$ и так далее. Равенства в уравнении (4.118) следует понимать как символические. Они обозначают, что (4.116) является собственным состоянием соответствующих наблюдаемых с собственными значениями ∓ 1. — *Прим. ред.*

две из трех монет, обнаруживая любую из четырех возможных конфигураций: ОО, ОР, РО, РР. Лишь выполнив множество испытаний, они смогли накопить убедительные статистические доказательства нарушения неравенства Белла. В противоположность этому в эксперименте с тремя ящиками Алиса, Боб и Чарли нашли результат, не согласующийся с эйнштейновской локальностью в каждом отдельном испытании, в котором они открывали дверцу X на всех трех ящиках!

4.7. Упражнения

4.1. Теорема Харди. Боб (в Бостоне) и Клер (в Чикаго) делят множество идентично приготовленных копий двухкубитового состояния

$$|\psi\rangle = \sqrt{1-2x}\,|00\rangle + \sqrt{x}\,|01\rangle + \sqrt{x}\,|10\rangle, \qquad (4.119)$$

где x — вещественное число, лежащее между 0 и $1/2$. Они проводят множество испытаний, в которых каждый измеряет свой кубит в базисе $\{|0\rangle, |1\rangle\}$, и узнают, что если результатом Боба является $|1\rangle$, то результат Клер всегда $|0\rangle$, а если результатом Клер является $|1\rangle$, тогда у Боба всегда $|0\rangle$.

Боб и Клер проводят дальнейшие эксперименты, в которых Боб выполняет измерение в базисе $\{|0\rangle, |1\rangle\}$, а Клер — в ортонормированном базисе $\{|\varphi\rangle, |\varphi^\perp\rangle\}$. Они обнаруживают, что если результат Боба $|0\rangle$, то результатом Клер всегда является $|\varphi\rangle$ и никогда — $|\varphi^\perp\rangle$. Аналогично, если Клер измеряет в базисе $\{|0\rangle, |1\rangle\}$, а Боб — в базисе $\{|\varphi\rangle, |\varphi^\perp\rangle\}$, тогда если результат Клер $|0\rangle$, то результатом Боба всегда является $|\varphi\rangle$ и никогда — $|\varphi^\perp\rangle$.

а) Выразить базис $\{|\varphi\rangle, |\varphi^\perp\rangle\}$ через $\{|0\rangle, |1\rangle\}$.

Теперь Боб и Клер интересуются, что произойдет, если они оба будут измерять в базисе $\{|\varphi\rangle, |\varphi^\perp\rangle\}$. Их друг Альберт, ярый сторонник локального реализма, предсказывает, что невозможно обоим получить результат $|\varphi^\perp\rangle$ (предсказание известное как *теорема Харди*). Альберт аргументирует это следующим образом.

> Когда Боб и Клер выполняют измерение в базисе $\{|\varphi\rangle, |\varphi^\perp\rangle\}$, имеет смысл рассмотреть, что могло бы случиться, если бы вместо этого кто-то один из них выполнил измерение в базисе $\{|0\rangle, |1\rangle\}$.

Итак, предположим, что Боб и Клер оба измеряют в базисе $\{|\varphi\rangle, |\varphi^\perp\rangle\}$ и что они оба получают результат $|\varphi^\perp\rangle$. Теперь, если бы Боб вместо этого измерял в базисе $\{|0\rangle, |1\rangle\}$, то мы могли бы быть уверены в том, что его результат — $|1\rangle$, так как эксперимент показывает, что если бы Боб получил $|0\rangle$, то Клер не могла бы получить $|\varphi^\perp\rangle$. Аналогично, если бы Клер измеряла в базисе $\{|0\rangle, |1\rangle\}$, то она наверняка получила бы результат $|1\rangle$. Мы приходим к выводу, что если бы Боб и Клер оба измеряли в базисе $\{|0\rangle, |1\rangle\}$, то они оба получили бы результат $|1\rangle$. Но это противоречит эксперименту, который показывает, что если Боб и Клер оба выполняют измерение в базисе $\{|0\rangle, |1\rangle\}$, то невозможно им обоим получить результат $|1\rangle$. Следовательно, мы вынуждены сделать вывод, что если Боб и Клер измеряют в базисе $\{|\varphi\rangle, |\varphi^\perp\rangle\}$, то они не могут одновременно получить результат $|\varphi^\perp\rangle$.

Несмотря на впечатляющую аргументацию Альберта, Боб и Клер решают исследовать, какое предсказание может быть получено из квантовой механики.

a) Если Боб и Клер оба измеряют в базисе $\{|\varphi\rangle, |\varphi^\perp\rangle\}$, каково квантово-механическое предсказание для вероятности $P(x)$ того, что они оба получат результат $|\varphi^\perp\rangle$?

b) Найдите «максимальное нарушение» теоремы Харди: покажите, что максимальным значением $P(x)$ является $P[(3-\sqrt{5})/2] = (5\sqrt{5}-11)/2 \approx 0{,}0902$.

c) Боб и Клер проводят эксперимент, подтверждающий предсказание квантовой механики. Что ошибочно в рассуждениях Альберта?

4.2. Закрытие лазейки детектирования. Напомним, что *неравенство КГШХ*

$$|\langle ab\rangle + \langle a'b\rangle + \langle ab'\rangle - \langle a'b'\rangle| \leqslant 2 \tag{4.120}$$

справедливо, если случайные переменные a, b, a', b' принимают значения ± 1 и подчиняются совместному распределению вероятностей. Максимальное нарушение этого неравенства квантово-механическими предсказаниями имеет место, когда левая часть равна $2\sqrt{2}$, что достигается, когда Алиса и Боб делят максимально запутанное состояние $|\phi^+\rangle$, a, a' — результаты измерения кубита Алисы вдоль осей $\hat{x}$

и $\hat{z}$, а b, b' — результаты измерения кубита Боба вдоль осей $(\hat{x}+\hat{z})/\sqrt{2}$ и $(\hat{x}-\hat{z})/\sqrt{2}$.

Алиса и Боб выполнили замечательный эксперимент, измерив поляризацию запутанной фотонной пары и подтвердили предсказываемое квантовой механикой нарушение неравенства КГШХ. Альберт настроен скептически. Он обращает внимание на то, что используемые в их эксперименте детекторы не очень эффективны. По большей части, если Алиса регистрирует фотон, то Боб — нет, а если Боб регистрирует фотон, то Алиса – нет. Следовательно, они отбрасывают данные для большинства фотонных пар и оставляют результаты только при совпадении детектирования двух фотонов. В своем анализе данных Алиса и Боб предполагают, что их результаты основаны на репрезентативной выборке измеряемых наблюдаемых, подчиняющихся некоторому распределению вероятностей. Однако Альберт доказывает, что их выводы могут оказаться недостоверными, если состояние детектируемого фотона скоррелировано с результатом измерения поляризации.

Алиса и Боб интересуются, насколько им необходимо поднять эффективность детекторов, чтобы выполнить эксперимент, который убедит Альберта.

Алиса может ориентировать свой детектор вдоль любой оси, и если она направила его вдоль оси $\hat{a}$, то в идеале ее детектор будет щелкать, когда спин ее кубита направлен вверх вдоль оси $\hat{a}$, но ввиду неэффективности детектора иногда он не срабатывает, даже если кубит ориентирован вверх. Пусть теперь для каждого номера i фотонной пары: $x_i \in \{0,1\}$ - переменная, обозначающая сработал ли детектор Алисы, ориентированный вдоль оси $\hat{a}$, а именно, если щелчок был, то $x_i = 1$, а если нет, то $x_i = 0$. Поскольку детектор неидеальный, то x_i может быть равно нулю, даже если кубит ориентирован вверх вдоль $\hat{a}$. Аналогично $x'_i \in \{0,1\}$ обозначает, сработал ли детектор Алисы, ориентированный вдоль оси $\hat{a}'$, $y_i \in \{0,1\}$ обозначает, сработал ли детектор Боба, ориентированный вдоль $\hat{b}$, а $y'_i \in \{0,1\}$ обозначает, сработал ли детектор Боба, ориентированный вдоль $\hat{b}'$. В предположении локального реализма каждой паре можно сопоставить значения x, x', y, y', определяемые локальными скрытыми переменными.

Алиса и Боб свободны в выборе ориентации своих детекторов в каждом измерении; следовательно, их выборка значений x, x', y, y' репре-

зентативна и они выводят из своих измерений следующие значения:

$$\begin{aligned} P_{++}(ab) &= \frac{1}{N}\sum_{i=1}^{N} x_i y_i, \\ P_{-+}(a'b) &= \frac{1}{N}\sum_{i=1}^{N} x'_i y_i, \\ P_{+-}(ab') &= \frac{1}{N}\sum_{i=1}^{N} x_i y'_i, \\ P_{--}(a'b') &= \frac{1}{N}\sum_{i=1}^{N} x'_i y'_i, \end{aligned} \tag{4.121}$$

где N — полное количество испытанных пар. Здесь, например, $P_{++}(ab)$ — вероятность того, что оба детектора сработают, когда Алиса и Боб ориентируют их вдоль осей $\hat{a}$ и $\hat{b}$, соответственно (с учетом влияния несовершенства детекторов).

a) Покажите, что если $x, x', y, y' \in \{0, 1\}$, то

$$xy + xy' + x'y - x'y' \leqslant x + y. \tag{4.122}$$

b) Покажите, что

$$P_{++}(ab) + P_{-+}(a'b) + P_{+-}(ab') - P_{--}(a'b') \leqslant P_{+\cdot}(a) + P_{\cdot+}(b); \tag{4.123}$$

здесь $P_{+\cdot}(a)$ обозначает вероятность того, что детектор Алисы щелкнет, если он ориентирован вдоль оси $\hat{a}$, а $P_{\cdot+}(b)$ обозначает вероятность того, что детектор Боба щелкнет, если он ориентирован вдоль оси $\hat{b}$.

c) Теперь сравним это с предсказаниями квантовой механики, где детектор Алисы имеет эффективность η_A, а детектор Боба — η_B. Это означает, что детектор Алисы щелкает с вероятностью $P = \eta_A P_{\text{perf}}$, где P_{perf} — вероятность щелчка идеального детектора, и аналогично для детектора Боба. Выбирая a, b, a', b' максимально нарушающими неравенство КГШХ, покажите, что предсказания квантовой механики нарушают неравенство (4.123), если только

$$\frac{\eta_A \eta_B}{\eta_A + \eta_B} > \frac{1}{1 + \sqrt{2}}. \tag{4.124}$$

Таким образом, если $\eta_A = \eta_B$, то Алисе и Бобу необходимы детекторы с эффективностью выше 82,84%, чтобы преодолеть возражения Альберта.

4.3. Телепортация с помощью непрерывных переменных. Один полный ортонормированный базис в гильбертовом пространстве двух частиц на вещественной прямой представляет собой базис (сепарабельных) собственных состояний оператора положения $\{|q_1\rangle \otimes |q_2\rangle\}$. Другой – запутанный базис $\{|Q, P\rangle\}$, где

$$|Q, P\rangle = \frac{1}{\sqrt{2\pi}} \int dq\, e^{iPq} |q\rangle \otimes |q + Q\rangle\,; \tag{4.125}$$

они являются одновременными собственными состояниями оператора относительного положения $\mathbf{Q} = \mathbf{q}_2 - \mathbf{q}_1$ и оператора полного импульса $\mathbf{P} = \mathbf{p}_1 + \mathbf{p}_2$.

a) Проверьте, что

$$\langle Q', P' | Q, P\rangle = \delta(Q' - Q)\delta(P' - P). \tag{4.126}$$

b) Поскольку состояния $\{|Q, P\rangle\}$ образуют базис, мы можем разложить собственные состояния положений как

$$|q_1\rangle \otimes |q_2\rangle = \int dQ\, dP\, |Q, P\rangle\langle Q, P|\big(|q_1\rangle \otimes |q_2\rangle\big). \tag{4.127}$$

Вычислите коэффициенты разложения $\langle Q, P|\big(|q_1\rangle \otimes |q_2\rangle\big)$.

c) Алиса и Боб приготовили запутанное состояние $|Q, P\rangle_{AB}$ двух частиц A и B; Алиса оставила себе частицу A, а Боб – частицу B. Алиса получила неизвестный волновой пакет $|\psi\rangle_C = \int dq\, |q\rangle_C\, {}_C\langle q|\psi\rangle_C$, который она намерена телепортировать Бобу. Составьте протокол, который они могут выполнить, чтобы осуществить телепортацию. Что должна измерить Алиса? Какую информацию она должна послать Бобу? Что должен сделать Боб, получив эту информацию, чтобы частица B была приготовлена в состоянии $|\psi\rangle_B$?

4.4. Телепортация со смешанными состояниями. Операциональный способ определения запутанного состояния заключается в том, что оно может быть использовано для телепортации неизвестного квантового состояния с лучшей точностью воспроизведения, чем этого можно было бы добиться с помощью одних только локальных операций и классической связи. В этом упражнении вы покажете, что существуют смешанные состояния, в этом смысле запутанные, но тем не менее не нарушающие никакого неравенства Белла. Следовательно, для смешанных

состояний (в противоположность чистым состояниям) понятия «запутанный» и «нарушающий неравенство Белла» не эквивалентны.

Рассмотрите «шумящую» запутанную пару с матрицей плотности

$$\boldsymbol{\rho}(\lambda) = (1-\lambda)|\psi^-\rangle\langle\psi^-| + \frac{\lambda}{4}\mathbf{1}. \tag{4.128}$$

a) Найдите точность воспроизведения F, которой можно достичь, если состояние $\boldsymbol{\rho}(\lambda)$ используется для телепортации одного кубита от Алисы к Бобу. [**Указание**. Вспомните, что вы показали в одном из предыдущих упражнений, что «случайное гадание» имеет точность воспроизведения $F = 1/2$.]

b) При каких значениях λ найденная в (a) точность воспоизведения лучше той, которой можно добиться, если Алиса измеряет свой кубит и посылает Бобу классическое сообщение? [**Указание.** Раньше вы показали, что можно достичь значения $F = 2/3$, если Алиса измеряет свой кубит. Фактически это наилучшее возможное значение F, достижимое в классической связи.]

c) Вычислите

$$\mathrm{Prob}(\uparrow_{\hat{n}}\uparrow_{\hat{m}}) \equiv \mathrm{tr}\left(\mathbf{E}_A(\hat{n})\mathbf{E}_B(\hat{m})\boldsymbol{\rho}(\lambda)\right), \tag{4.129}$$

где $\mathbf{E}_A(\hat{n})$ — проекция кубита Алисы на состояние $|\uparrow_{\hat{n}}\rangle$, а $\mathbf{E}_B(\hat{m})$ — проекция кубита Боба на состояние $|\uparrow_{\hat{m}}\rangle$.

d) Рассмотрите случай $\lambda = 1/2$. Покажите, что в этом случае состояние $\boldsymbol{\rho}(\lambda)$ не нарушает неравенства Белла. [**Указание.** Достаточно построить модель локальных скрытых переменных, которая при $\lambda = 1/2$ корректно воспроизводит найденные в (c) спиновые корреляции.] Предположите, что скрытая переменная $\hat{\alpha}$ однородно распределена на единичной сфере и что существуют функции f_A и f_B такие, что

$$\mathrm{Prob}_A(\uparrow_{\hat{n}}) = f_A(\hat{\alpha}\cdot\hat{n}), \qquad \mathrm{Prob}_B(\uparrow_{\hat{m}}) = f_B(\hat{\alpha}\cdot\hat{m}). \tag{4.130}$$

Задача состоит в том, чтобы найти f_A и f_B (где $0 \leqslant f_{A,B} \leqslant 1$), обладающие свойствами

$$\int_{\hat{\alpha}} f_A(\hat{\alpha}\cdot\hat{n}) = \frac{1}{2}, \qquad \int_{\hat{\alpha}} f_B(\hat{\alpha}\cdot\hat{m}) = \frac{1}{2},$$

$$\int_{\hat{\alpha}} f_A(\hat{\alpha}\cdot\hat{n}) f_B(\hat{\alpha}\cdot\hat{m}) = \mathrm{Prob}(\uparrow_{\hat{n}}\uparrow_{\hat{m}}). \tag{4.131}$$

4.5. Распределение квантового ключа. Алиса и Боб хотят выполнить протокол распределения квантового ключа. Алиса имеет все необходимое, чтобы приготовить любое из двух состояний: $|u\rangle$ или $|v\rangle$. В подходящем базисе эти два состояния могут быть представлены как

$$|u\rangle = \begin{pmatrix} \cos\alpha \\ \sin\alpha \end{pmatrix}, \qquad |v\rangle = \begin{pmatrix} \sin\alpha \\ \cos\alpha \end{pmatrix}, \tag{4.132}$$

где $0 < \alpha < \pi/4$. Алиса выбирает наугад, что послать Бобу, $|u\rangle$ или $|v\rangle$, а Боб должен выполнить измерение, чтобы определить, что она послала. Так как эти два состояния не ортогональны, Боб не может различить их с абсолютной точностью.

a) Боб понимает, что он не может рассчитывать на то, что всякий раз он сможет идентифицировать кубит Алисы, поэтому он довольствуется процедурой, которая лишь иногда обеспечивает успех. Он выполняет ПОЗМ с тремя возможными исходами: $\neg|u\rangle$, $\neg|v\rangle$, или НЕ ЗНАЮ. Если он получает результат $\neg|u\rangle$, он уверен, что было послано $|v\rangle$, а если он получает результат $\neg|v\rangle$, он уверен, что было послано $|u\rangle$. Если получен результат НЕ ЗНАЮ, тогда его измерение неубедительно (не позволяет сделать определенного вывода). Эта ПОЗМ определяется операторами

$$\begin{gathered} \mathbf{F}_{\neg u} = A(\mathbf{1} - |u\rangle\langle u|), \quad \mathbf{F}_{\neg v} = A(\mathbf{1} - |v\rangle\langle v|), \\ \mathbf{F}_{\mathrm{DK}} = (1 - 2A)\mathbf{1} + A(|u\rangle\langle u| + |v\rangle\langle v|) \end{gathered} \tag{4.133}$$

(DK — Don't Know — НЕ ЗНАЮ), где A — положительное вещественное число. Какое значение A должен выбрать Боб, чтобы минимизировать вероятность результата НЕ ЗНАЮ, и чему равна эта минимальная вероятность НЕ ЗНАЮ (при условии, что Алиса выбирает $|u\rangle$ или $|v\rangle$ с равной вероятностью)? [**Указание.** Если A слишком велико, то $\mathbf{F}_{\mathrm{DK}}$ будет иметь отрицательные собственные значения, а уравнения (4.133) не будут представлять ПОЗМ.]

b) Разработайте протокол распределения квантового ключа, используя исходные данные Алисы и ПОЗМ Боба.

c) Конечно, Ева тоже хочет знать, что Алиса посылает Бобу. Надеясь на то, что Алиса и Боб не заметят, она перехватывает каждый посылаемый Алисой кубит, выполняя ортогональное измерение, проецирующее его на базис $\left\{\binom{1}{0}, \binom{0}{1}\right\}$. Если она получает результат $\binom{1}{0}$, то она пересылает Бобу $|u\rangle$, а если — $\binom{0}{1}$, то пересылает ему $|v\rangle$. Следовательно, всякий раз, когда ПОЗМ Боба имеет

убедительный результат, Ева знает, каков он. Но вмешательство вызывает обнаруживаемые ошибки; иногда Боб получает «убедительный» результат, который на самом деле отличается от того, что посылала Алиса. Какова вероятность такой ошибки?

4.6. Минимальное возмущение. В упражнении 2.1 вы исследовали игру, в которой Алиса решает наудачу (равновероятно), какое чистое состояние одного кубита приготовить из двух возможных:

$$|\psi\rangle = \begin{pmatrix} \cos\alpha \\ \sin\alpha \end{pmatrix} \quad \text{или} \quad |\tilde{\psi}\rangle = \begin{pmatrix} \sin\alpha \\ \cos\alpha \end{pmatrix}, \tag{4.134}$$

и посылает это состояние Бобу. Выполняя ортогональное измерение в базисе $\{|0\rangle, |1\rangle\}$, Боб может идентифицировать состояние с минимальной вероятностью ошибки

$$(P_{\text{error}})_{\text{optimal}} = \sin^2\alpha = \frac{1}{2}(1 - \sin\theta), \tag{4.135}$$

где мы определили θ соотношением

$$\langle\psi|\tilde{\psi}\rangle \equiv \cos\theta = \sin(2\alpha). \tag{4.136}$$

Но допустим теперь, что Ева хочет *перехватить* это состояние, пока оно движется от Алисы к Бобу. Как и Боб, она желает извлечь оптимальную информацию, отличающую $|\psi\rangle$ от $|\tilde{\psi}\rangle$, и при этом минимизировать вносимое ее вмешательством возмущение, так чтобы Алисе и Бобу было невозможно заметить, что здесь что-то не так.

Ева понимает, что оптимальную ПОЗМ можно осуществить с помощью операторов измерений

$$\mathbf{M}_0 = |\phi_0\rangle\langle 0|, \qquad \mathbf{M}_1 = |\phi_1\rangle\langle 1| \tag{4.137}$$

с произвольными векторами $|\phi_0\rangle$ и $|\phi_1\rangle$. Если Ева выполняет это измерение, то Боб получает состояние

$$\rho' = \cos^2\alpha|\phi_0\rangle\langle\phi_0| + \sin^2\alpha|\phi_1\rangle\langle\phi_1|, \tag{4.138}$$

если Алиса послала $|\psi\rangle$, и состояние

$$\tilde{\rho}' = \sin^2\alpha|\phi_0\rangle\langle\phi_0| + \cos^2\alpha|\phi_1\rangle\langle\phi_1|, \tag{4.139}$$

если Алиса послала $|\tilde{\psi}\rangle$.

Ева хочет, чтобы средняя точность воспроизведения получаемого Бобом состояния была как можно больше. Величина, которую она хочет минимизировать, называемая в дальнейшем «возмущением» D, измеряет, насколько близка к единице эта средняя точность воспроизведения

$$D = 1 - \frac{1}{2}(F + \tilde{F}), \tag{4.140}$$

где

$$F = \langle\psi|\rho'|\psi\rangle, \qquad \tilde{F} = \langle\tilde{\psi}|\tilde{\rho}'|\tilde{\psi}\rangle. \tag{4.141}$$

Целью этого упражнения является проверить, насколько эффективно Ева может сократить возмущение с помощью подходящего выбора своих измерительных операторов.

a) Покажите, что $F + \tilde{F}$ может быть представлено в виде

$$F + \tilde{F} = \langle\phi_0|A|\phi_0\rangle + \langle\phi_1|B|\phi_1\rangle, \tag{4.142}$$

где

$$\begin{aligned} A &= \begin{pmatrix} 1 - 2\cos^2\alpha\,\sin^2\alpha & \cos\alpha\,\sin\alpha \\ \cos\alpha\,\sin\alpha & 2\cos^2\alpha\,\sin^2\alpha \end{pmatrix}, \\ B &= \begin{pmatrix} 2\cos^2\alpha\,\sin^2\alpha & \cos\alpha\,\sin\alpha \\ \cos\alpha\,\sin\alpha & 1 - 2\cos^2\alpha\,\sin^2\alpha \end{pmatrix}. \end{aligned} \tag{4.143}$$

b) Покажите, что если $|\phi_0\rangle$ и $|\phi_1\rangle$ выбраны оптимально, то минимальное возмущение, которое может быть достигнуто, равно

$$D_{\min}(\cos^2\theta) = \frac{1}{2}\left(1 - \sqrt{1 - \cos^2\theta + \cos^4\theta}\right). \tag{4.144}$$

[**Указание.** Мы можем выбрать $|\phi_0\rangle$ и $|\phi_1\rangle$, чтобы независимо максимизировать два слагаемых в уравнении (4.142). Максимальным значением является максимальное собственное значение оператора A, которое может быть выражено как $\lambda_{\max} = \frac{1}{2}(1 + \sqrt{1 - 4\det A})$, поскольку сумма собственных значений равна единице.] Конечно, Ева могла бы сделать возмущение еще меньшим, если ее устроит меньшая, чем оптимальная, вероятность правильного определения сообщения Алисы.

c) Изобразите график функции $D_{\min}(\cos^2\theta)$. Истолкуйте ее значения при $\cos\theta = 1$ и $\cos\theta = 0$. При каком значении θ $D_{\min}$ максимальна? Найдите $D_{\min}$ и $(p_{\text{error}})_{\text{optimal}}$ для этого значения θ.

4.7. Приближенное клонирование. Теорема о невозможности клонирования показывает, что невозможно построить унитарную машину, которая будет делать идеальные копии неизвестного квантового состояния. Но допустим, что нас устроит *неидеальная* копия — какой точности воспроизведения мы можем добиться?

Рассмотрим машину, действующую на трехкубитовое состояние в соответствии с

$$\begin{aligned} |000\rangle_{ABC} &\to \sqrt{\frac{2}{3}}|00\rangle_{AB}|0\rangle_C + \sqrt{\frac{1}{3}}|\psi^+\rangle_{AB}|1\rangle_C, \\ |100\rangle_{ABC} &\to \sqrt{\frac{2}{3}}|11\rangle_{AB}|1\rangle_C + \sqrt{\frac{1}{3}}|\psi^-\rangle_{AB}|0\rangle_C. \end{aligned} \tag{4.145}$$

a) Являются ли такой прибор в принципе физически реализуемым?

Если машина действует на начальное состояние $|\psi\rangle_A|00\rangle_{BC}$, то она производит чистое запутанное состояние трех кубитов $|\Psi\rangle_{ABC}$. Но если мы наблюдаем один только кубит A, то его конечным состоянием является оператор плотности $\rho'_A = \mathrm{tr}_{BC}\left(|\Psi\rangle_{ABC\,ABC}\langle\Psi|\right)$. Аналогично конечным состоянием отдельно наблюдаемого кубита B является ρ'_B. Нетрудно видеть, что $\rho'_A = \rho'_B$ — идентичные, но не идеальные копии исходного чистого состояния $|\psi\rangle_A$.

b) Отображение начального состояния $|\psi\rangle_{A\,A}\langle\psi|$ кубита A на конечное состояние ρ'_A определяет супероператор \$. Найдите его представление операторной суммы.

c) Найдите ρ'_A для $|\psi\rangle_A = a|0\rangle_A + b|1\rangle_A$ и вычислите его точность воспроизведения $F \equiv {}_A\langle\psi|\rho'_A|\psi\rangle_A$.

4.8. Прости нас, дядюшка Альберт. Рассмотрим n-кубитовое «кот-состояние»

$$|\psi\rangle_n = \frac{1}{2}\left(|000\ldots0\rangle + |111\ldots1\rangle\right). \tag{4.146}$$

Это состояние можно охарактеризовать как одновременное собственное состояние (с единичным собственным значением) n операторов

$$\begin{aligned} &\sigma_3 \otimes \sigma_3 \otimes 1 \otimes 1 \otimes \cdots \otimes 1 \otimes 1 \otimes 1, \\ &1 \otimes \sigma_3 \otimes \sigma_3 \otimes 1 \otimes \cdots \otimes 1 \otimes 1 \otimes 1, \\ &\qquad\cdots \\ &1 \otimes 1 \otimes 1 \otimes 1 \otimes \cdots \otimes 1 \otimes \sigma_3 \otimes \sigma_3, \\ &\sigma_1 \otimes \sigma_1 \otimes \sigma_1 \otimes \cdots \otimes \sigma_1 \otimes \sigma_1 \otimes \sigma_1. \end{aligned} \tag{4.147}$$

a) Покажите, что $|\psi\rangle_n$ является собственным состоянием оператора

$$(\boldsymbol{\sigma}_1 + i\boldsymbol{\sigma}_2)^{\otimes n} + (\boldsymbol{\sigma}_1 - i\boldsymbol{\sigma}_2)^{\otimes n}, \tag{4.148}$$

и вычислите его собственное значение.

b) Если мы верим в локальные скрытые переменные, тогда мы верим, что для каждого из n-кубитов $\boldsymbol{\sigma}_1$ и $\boldsymbol{\sigma}_2$ имеют определенные значения, коль скоро скрытые переменные определены. Если это так, то что можно сказать относительно *модулей* $(\boldsymbol{\sigma}_1 + i\boldsymbol{\sigma}_2)^{\otimes n}$ или $(\boldsymbol{\sigma}_1 - i\boldsymbol{\sigma}_2)^{\otimes n}$, предполагая определенные значения скрытых переменных?

c) Из (b) выведите верхнюю границу для

$$\frac{1}{2}\left|(\boldsymbol{\sigma}_1 + i\boldsymbol{\sigma}_2)^{\otimes n} + (\boldsymbol{\sigma}_1 - i\boldsymbol{\sigma}_2)^{\otimes n}\right|, \tag{4.149}$$

следующую из гипотезы о локальных скрытых переменных.

d) Сравните это с (a). Что сказал бы Эйнштейн?

4.9. Манипулирование запутыванием. a) Двадцать пять игроков команды Янки из Нью-Йорка и двадцать пять игроков комады Святых Отцов из Сан-Диего хотят разделить пятьдесят кубитов «кот-состояния». Янки готовят 26-кубитовое «кот-состояние» и дают один из кубитов Алисе; то же делают и Святые Отцы. Теперь Алиса должна соединить эти и приготовить 50-кубитовое состояние. Как ей это сделать? [**Указание.** Подумайте о стабилизаторе.]

b) Присоединившись к Янки, Алиса приняла на хранение один из кубитов их 25-кубитового «кот-состояния». Но ее подкупили! Алисе поручено извлечь имеющийся у ней кубит из «кот-состояния», сохранив неповрежденным 24-кубитовое состояние остальных игроков. Как ей это сделать? [**Указание.** Подумайте о стабилизаторе.]

4.10. Критерий Переса — Городецки в d измерениях. Напомним, что *состояние Вернера* пары кубитов может быть представлено как

$$\boldsymbol{\rho}(\lambda) = \lambda|\phi^+\rangle\langle\phi^+| + \frac{1}{4}(1-\lambda)\mathbf{1} \tag{4.150}$$

и что *частичное транспонирование* $\boldsymbol{\rho}_{AB}^{PT}$ парного оператора плотности $\boldsymbol{\rho}_{AB}$ определяется как

$$\boldsymbol{\rho}_{AB}^{PT} \equiv (\mathbf{1}_A \otimes \mathbf{T}_B)\boldsymbol{\rho}_{AB}, \tag{4.151}$$

где $\mathbf{T}$ – операция транспонирования, действующая в базисе $\{|i\rangle\}$ как

$$\mathbf{T}(|i\rangle\langle j|) = |j\rangle\langle i|. \tag{4.152}$$

На лекции мы видели, что частичное транспонирование состояния Вернера $\rho(\lambda)$ отрицательно при $\lambda > 1/3$; следовательно, согласно *критерию Переса–Городецки* состояние Вернера несепарабельно при $\lambda > 1/3$.

a) Естественный способ обобщения состояния Вернера на пару d-мерных систем – рассмотреть

$$\rho_\Phi(\lambda) = \lambda|\Phi\rangle\langle\Phi| + \frac{1}{d^2}(1-\lambda)\mathbf{1}, \tag{4.153}$$

где $|\Phi\rangle$ – максимально запутанное состояние

$$|\Phi\rangle = \frac{1}{\sqrt{d}}\sum_{i=1}^{d}|i\rangle\otimes|i\rangle. \tag{4.154}$$

Покажите, что

$$(|\Phi\rangle\langle\Phi|)^{PT} = \frac{1}{d}(\mathbf{1} - 2\mathbf{E}_{\text{antisym}}), \tag{4.155}$$

где $\mathbf{E}_{\text{antisym}}$ – проектор на пространство, антисимметричное относительно перестановки двух систем: A и B.

b) При каких значениях λ частичное транспонирование $\rho_\Phi(\lambda)$ отрицательно?

c) Если состояние Вернера двух кубитов выбрано в виде

$$\rho(\lambda) = \lambda|\psi^-\rangle\langle\psi^-| + \frac{1}{4}(1-\lambda)\mathbf{1}, \tag{4.156}$$

тогда другой естественный способ обобщить состояние Вернера на пару d-мерных систем – рассмотреть

$$\rho_{\text{anti}}(\lambda) = \frac{2\lambda}{d(d-1)}\mathbf{E}_{\text{antisym}} + \frac{1}{d^2}(1-\lambda)\mathbf{1}. \tag{4.157}$$

При каких значениях λ частичное транспонирование $\rho_{\text{anti}}(\lambda)$ отрицательно?

Глава 5

Теория квантовой информации

Теория квантовой информации настолько обширный предмет, что вполне могла бы занимать нас весь семестр. Но вследствие недостатка времени (мне не терпится перейти к квантовым вычислениям) я не смогу осветить этот предмет так глубоко, как мне бы этого хотелось. Мы удовольствуемся отрывочным введением в некоторые основные идеи и результаты. Возможно, лекции будут носить более описательный характер, нежели в первом семестре, с более частыми рассуждениями на пальцах и с большим количеством деталей, оставленных для домашних упражнений. Вероятно, эту главу следовало бы назвать: «Теория квантовой информации для нетерпеливых» [1].

Теория квантовой информации имеет дело с четырьмя главными темами.

(1) Передача классической информации по квантовым каналам связи (будет обсуждаться).

(2) Компромисс между получением информации о квантовом состоянии и его возмущением (этот вопрос мы кратко обсуждали в главе 4 в связи с квантовой криптографией, но здесь разберемся с ним основательно).

(3) Количественная характеристика квантового запутывания (которой мы кратко коснемся).

(4) Передача квантовой информации по квантовым каналам связи. (Мы обсудим случай канала без помех, отложив обсуждение канала с помехами до тех пор, пока не познакомимся с квантовыми корректирующими кодами.)

Эти темы объединяет часто повторяющийся лейтмотив: интерпретация и применения энтропии фон Неймана.

---

[1] Читателю, интересующемуся более строгим математическим изложением основных результатов квантовой теории информации, можно порекомендовать книгу А.С. Холево, *Введение в квантовую теорию информации*, МЦНМО, М.: 2002; более подробное изложение теории классической и квантовой информации на физическом уровне строгости можно найти в книге M.A. Nielsen, I.L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2001; перевод на русский язык М. Нильсен, И. Чанг, *Квантовые вычисления и квантовая информация*, М.: Мир, 2006. – *Прим. ред.*

5.1. Шеннон для «чайников»

Прежде чем мы сможем понять энтропию фон Неймана и ее значение для квантовой информации, мы должны обсудить энтропию Шеннона и ее значение для информации классической.

В своей основополагающей статье 1948 г. Клод Шеннон установил два основных результата теории классической информации. Им были решены две центральных проблемы.

(1) Насколько можно *сжать* сообщение, то есть насколько избыточна информация? («Теорема кодирования без помех»).

(2) С какой *скоростью* мы можем надежно передавать сообщения по каналу с помехами; то есть насколько избыточным должно быть содержание сообщения, чтобы быть защищенным от ошибок? («Теорема кодирования для канала с помехами (шумом)».)

Оба вопроса касаются *избыточности* — насколько, в среднем, *неожиданна* следующая буква сообщения. Согласно одной из ключевых идей Шеннона, удобную количественную меру избыточности предоставляет *энтропия*.

Я назвал этот раздел «Шеннон для чайников», поскольку я попытаюсь быстро объяснить основные идеи Шеннона с минимальным количеством ε-ов и δ. Таким образом, я смогу втиснуть теорию классической информации примерно в двенадцать страниц.

5.1.1. Энтропия Шеннона и сжатие данных

Сообщением называется строка из букв, выбранных из содержащего k букв алфавита

$$\{a_1, a_2, \ldots, a_k\}. \tag{5.1}$$

Предположим, что буквы a_x в сообщении статистически независимы и каждая из них появляется с заданной *a priori* вероятностью $p(a_x)$, где $\sum_{x=1}^{k} p(a_x) = 1$. Простейшим примером служит двоичный алфавит, в котором 0 появляется с вероятностью $1 - p$, а 1 — с вероятностью p (где $0 \leqslant p \leqslant 1$).

Рассмотрим длинные, содержащие n букв ($n \gg 1$), сообщения. Нас интересует, можно ли сжать сообщение до более короткой строки, несущей, по существу, ту же информацию?

Согласно закону больших чисел при очень больших n типичные строки содержат (в двоичном случае) примерно $n(1-p)$ нулей и примерно np единиц. Количество различных строк такого типа (типичных строк) по порядку величины равно биномиальному коэффициенту $\binom{n}{np}$ и из формулы Стирлинга $\log n! = n\log n - n + O(\log n)$ мы получаем

$$\begin{aligned}\log\binom{n}{np} &= \log\left(\frac{n!}{(np)![n(1-p)]!}\right) \simeq n\log n - n - \\ &- [np\log np - np + n(1-p)\log n(1-p) - n(1-p)] = \\ &= nH(p), \end{aligned} \tag{5.2}$$

где

$$H(p) = -p\log p - (1-p)\log(1-p) \tag{5.3}$$

— функция, называемая *энтропией*. Следовательно, количество типичных строк имеет порядок $2^{nH(p)}$. (Логарифмы здесь понимаются по основанию два, если не оговаривается иное.)

Чтобы передать, по существу, всю информацию, переносимую строкой из n битов, достаточно выбрать блоковый код, присваивающий положительное целое число каждой типичной строке. Этот блоковый код имеет около $2^{nH(p)}$ слов (появляющихся с *a priori* одинаковой вероятностью), так что любое из них мы можем идентифицировать, используя двоичную строку длиной $nH(p)$. Поскольку $0 \leqslant H(p) \leqslant 1$ при $0 \leqslant p \leqslant 1$ и $H(p) = 1$ только при $p = 1/2$, блоковый код сокращает сообщение при любом $p \neq 1/2$ (когда 0 и 1 не равновероятны). Это результат Шеннона. Главная идея заключается в том, что нам не нужно кодовое слово для каждой последовательности букв, а только для *типичных* последовательностей. Вероятность того, что действительное сообщение атипично, асимптотически (то есть в пределе $n \to \infty$) мала.

Это рассуждение очевидным образом обобщается на случай k букв, когда буква x появляется с вероятностью $p(x)$.[1] В строке, содержащей n букв, x обычно возникает приблизительно $np(x)$ раз, а количество типичных строк имеет порядок

$$\frac{n!}{\prod_x (np(x))!} \simeq 2^{nH(X)}, \tag{5.4}$$

[1] Ансамбль, в котором каждая из n букв извлекается из распределения X, будет обозначаться как X^n.

где мы вновь воспользовались асимптотической формулой Стирлинга, а

$$H(X) = -\sum_x p(x) \log p(x) \tag{5.5}$$

– *энтропия Шеннона* (или просто энтропия) ансамбля $X = \{x, p(x)\}$. Выбирая блоковый код, присваивающий целые числа типичным последовательностям, можно сжать до $nH(X)$ битов информацию, содержащуюся в строке из n букв. В этом смысле выбранная из ансамбля буква x несет в среднем $H(X)$ битов информации.

Это рассуждение полезно переформулировать на несколько ином языке. Отдельное n-буквенное сообщение

$$x_1 x_2 \ldots x_n \tag{5.6}$$

возникает с вероятностью, *a priori* равной

$$P(x_1 x_2 \ldots x_n) = p(x_1)p(x_2)\cdots p(x_n), \tag{5.7}$$

$$\log P(x_1 x_2 \ldots x_n) = \sum_{i=1}^{n} \log p(x_i). \tag{5.8}$$

Применяя к этой сумме центральную предельную теорему, мы приходим к выводу, что для «большинства последовательностей»

$$-\frac{1}{n} \log P(x_1 x_2 \ldots x_n) \sim \langle -\log p(x) \rangle \equiv H(X), \tag{5.9}$$

где угловые скобки обозначают среднее значение по распределению вероятностей, управляющему случайной переменной x.

Конечно, на языке ε-ов и δ можно дать точную формулировку этого утверждения. Для любых $\varepsilon, \delta > 0$ и для достаточно больших n каждая «типичная последовательность» имеет вероятность P, удовлетворяющую неравенству

$$H(X) - \delta < -\frac{1}{n} \log P(x_1 x_2 \ldots x_n) < H(X) + \delta, \tag{5.10}$$

а суммарная вероятность всех типичных последовательностей превышает $1 - \varepsilon$.[1] Или, другими словами, каждая из последовательностей букв, возникающих с превосходящей $1 - \varepsilon$ суммарной вероятностью («типичные

[1] Фактически это один из вариантов *закона больших чисел*. Его строгую математическую формулировку можно найти в любом учебнике по теории вероятностей или в книге А. С. Холево, *Введение в квантовую теорию информации*, МЦНМО, М.: 2002. – *Прим. ред.*

последовательности»), появляется с вероятностью P такой, что

$$2^{-n(H+\delta)} \leqslant P \leqslant 2^{-n(H-\delta)}. \tag{5.11}$$

Из уравнения (5.11) можно вывести верхнюю и нижнюю грани для *количества* $N(\varepsilon, \delta)$ типичных последовательностей (так как сумма вероятностей всех типичных последовательностей должна лежать между $1-\varepsilon$ и единицей):

$$(1-\varepsilon)2^{n(H-\delta)} \leqslant N(\varepsilon, \delta) \leqslant 2^{n(H+\delta)}. \tag{5.12}$$

С помощью блокового кода длиной $n(H+\delta)$ битов мы можем закодировать все типичные последовательности. Тогда, независимо от того, как закодированы атипичные последовательности, вероятность ошибки (декодирования) будет меньше, чем ε.

И наоборот, если мы попытаемся сжать сообщение до меньшего, чем $H-\delta'$, количества битов на одну букву, то не сможем добиться малой частоты ошибок при $n \to \infty$, так как будем не в состоянии однозначно присвоить кодовые слова всем типичным последовательностям. Вероятность успешного декодирования сообщения P_{success} будет ограничена сверху

$$P_{\text{success}} \leqslant 2^{n(H-\delta')}2^{-n(H-\delta)} + \varepsilon' = 2^{-n(\delta'-\delta)} + \varepsilon'. \tag{5.13}$$

Мы можем корректно декодировать только $2^{n(H-\delta')}$ типичных сообщений, каждое из которых возникает с вероятностью, меньшей чем $2^{-n(H-\delta)}$ (ε' добавлена, чтобы учесть вероятность того, что нам удается корректно декодировать атипичные сообщения). А так как δ может быть выбрана сколь угодно малой, то при $n \to \infty$ малой становится и эта вероятность успеха.

Таким образом, оптимальный код асимптотически сжимает каждую букву до $H(X)$ битов. Это и есть теорема Шеннона о кодировании в отсутствии шума.

5.1.2. Взаимная информация

Энтропия Шеннона $H(X)$ количественно определяет, сколько в среднем информации передается буквой, извлеченной из ансамбля X. То есть сообщает, сколько (асимптотически при $n \to \infty$, где n — количество извлеченных букв) необходимо битов, чтобы закодировать эту информацию.

Взаимная информация $I(X;Y)$ количественно определяет степень корреляции двух сообщений. Как много мы узнаем о сообщении, извлеченном из X^n, прочитав сообщение, извлеченное из Y^n?

Допустим, например, что мы хотим послать сообщение от отправителя к получателю. Однако в канале связи имеется шум, так что полученное

сообщение (y) может отличаться от посланного (x). Канал с шумом можно характеризовать условной вероятностью $p(y|x)$ — вероятностью того, что будет получено y, если послано x. Предположим, что буква x посылается с *a priori* известной вероятностью $p(x)$. Мы хотим количественно определить, что мы узнаем об x, получив y; какой объем информации мы приобретаем?

Как уже говорилось, энтропия $H(X)$ дает отнесенную к одной букве количественную меру моего априорного незнания сообщения до его получения; то есть вам необходимо передать мне (без искажений) nH битов, чтобы (асимптотически) точно определить конкретное сообщение из n букв. Но после ознакомления с сообщением y, я могу использовать теорему Бейеса, чтобы скорректировать распределение вероятностей для x:

$$p(x|y) = \frac{p(y|x)p(x)}{p(y)}. \tag{5.14}$$

[Мне известны $p(y|x)$, если я знаком со свойствами канала, и $p(x)$, если я знаю априорные вероятности появления букв; таким образом, я могу вычислить $p(y) = \sum_x p(y|x)p(x)$.] Благодаря приобретенному новому знанию я стал более осведомлен относительно x, чем ранее. С полученными мной y-ми, используя оптимальный код, вы можете полностью определить конкретную строку из n букв, посылая мне

$$H(X|Y) = \langle -\log p(x|y) \rangle \tag{5.15}$$

битов на каждую букву[1]. $H(X|Y)$ называется «условной энтропией». Из $p(x|y) = p(x,y)/p(y)$ мы видим, что

$$\begin{aligned} H(X|Y) &= \langle -\log p(x,y) + \log p(y) \rangle = \\ &= H(X,Y) - H(Y) \end{aligned} \tag{5.16}$$

[1] Вряд ли следует понимать это утверждение в буквальном смысле. Для того, чтобы отправитель мог восстановить посылаемую им строку из n букв X, он должен получать по параллельному каналу *без шума* информацию о каждой букве выходящего сообщения Y и по нему же отправлять исправления, если произошла ошибка передачи. [См. C. Shannon, A mathematical theory of communication, Bell System Techn. J., **27**, № 3, 379–423; № 4, 623–656 (1948). Русский перевод: К. Шеннон, Математическая теория связи, в книге К. Шеннон, *Работы по теории информации и кибернетике*, ИЛ, Москва (1063), стр. 243–332.] Скорее условную энтропию $H(X|Y)$ следует интерпретировать как количество информации, *теряемой* при передаче сообщения X через канал с шумом.

Кроме этого, обратим внимание на то, что в (5.15), а также в уравнениях (5.16), (5.17) и (5.19), угловые скобки обозначают усреднение по совместному распределению вероятностей $p(x,y)$. Следовательно все эти величины определяют информационные характеристики не конкретных n-буквенных строк, а всего совместного ансамбля входящих и выходящих сообщений. — *Прим. ред.*

и аналогично

$$H(Y|X) \equiv \langle -\log p(y|x) \rangle = \\ = \left\langle -\log \frac{p(x,y)}{p(x)} \right\rangle = H(X,Y) - H(X). \qquad (5.17)$$

Таким образом, $H(X|Y)$ можно интерпретировать как количество *дополнительных* битов на одну букву, необходимых для полного определения x и y при известном y. Очевидно, что эта величина не может быть отрицательной.

Информация об X, приобретаемая при знакомстве с Y, измеряется тем, насколько *сокращается* отнесенное к одной букве количество битов, необходимое для идентификации X при известном Y. Таким образом:

$$I(X;Y) \equiv H(X) - H(X|Y) = \\ = H(X) + H(Y) - H(X,Y) = \\ = H(Y) - H(Y|X). \qquad (5.18)$$

$I(X;Y)$ называется взаимной информацией. Она, очевидно, симметрична относительно перестановки X и Y; количество информации об X, получаемое при знакомстве с Y, равно количеству информации об Y, получаемому при знакомстве с X. Знакомство с Y не может *уменьшить* мое знание об X, следовательно, $I(X;Y)$ очевидно неотрицательна. (Неравенства $H(X) \geqslant H(X|Y) \geqslant 0$ легко доказываются с учетом свойства выпуклости логарифмической функции[1].)

Конечно, если X и Y полностью некоррелированы, то мы имеем $p(x,y) = p(x)p(y)$ и

$$I(X;Y) \equiv \left\langle \log \frac{p(x,y)}{p(x)p(y)} \right\rangle = 0; \qquad (5.19)$$

естественно, что, знакомясь с Y, мы ничего не можем узнать об X, если между ними нет корреляции!

5.1.3. Теорема о кодировании для канала с шумом

Если мы хотим установить связь через канал с шумом, то мы, очевидно, можем повысить надежность передачи посредством избыточности

[1] См., например, T. M. Cover, and J. A. Thomas, *Elements of Information Theory*, J. Wiley & Sons, New York, 1991.

информации. Например, я могу многократно посылать каждый бит, а получатель – прислушиваться к голосу большинства, чтобы его декодировать.

Но всегда ли для данного канала можно найти код, гарантирующий сколь угодно высокую надежность (при $n \to \infty$)? А что можно сказать о *быстродействии* таких кодов; сколько битов потребуется для каждой буквы сообщения?

Фактически Шеннон показал, что любой канал может быть использован для сколь угодно надежной связи с конечной (ненулевой) скоростью, пока существует хоть *какая-нибудь* корреляция между его входом и выходом. Более того, он нашел полезное выражение для оптимальной скорости коммуникации, которая может быть достигнута. Эти результаты составляют содержание «теоремы о кодировании для канала связи с шумом».

Предположим для определенности, что мы пользуемся двоичным алфавитом, каждая буква которого (0 и 1) появляется с априорной вероятностью $1/2$. Предположим также, что канал является «двоичным симметричным каналом» – он действует на каждый бит независимо, с вероятностью p инвертируя его значение и оставляя невредимым с вероятностью $1-p$. То есть условные вероятности равны

$$\begin{aligned} p(0|0) &= 1-p, \quad p(0|1) = p, \\ p(1|0) &= p, \quad p(1|1) = 1-p. \end{aligned} \tag{5.20}$$

Мы хотим построить семейство кодов растущего блочного размера n такого, чтобы вероятность ошибки декодирования стремилась к нулю при $n \to \infty$. Если количество закодированных в блоке битов равно k, то код заключается в выборе 2^k «кодовых слов» из 2^n возможных n-битовых строк. Определим быстродействие кода R (число битов информации, приходящихся на один передаваемый бит) как

$$R = \frac{k}{n}. \tag{5.21}$$

Нам нужно разработать такой код, чтобы кодовые строки находились как можно «дальше друг от друга». Другими словами, для данного быстродействия R мы хотим максимизировать количество битов, которые должны инвертироваться, чтобы одно кодовое слово заменилось другим (это количество называется «расстоянием Хэмминга» между двумя кодовыми словами).

Для любой входящей строки длиной n битов, ошибки, как правило, будут вызывать инвертирование примерно np битов – следовательно, вход

обычно рассеивается в одну из примерно $2^{nH(p)}$ типичных выходящих строк (заполняющих «сферу радиуса Хэмминга» np, окружающую входящую строку). Для надежного декодирования, входящие кодовые слова следует выбирать таким образом, чтобы было маловероятным перекрытие сфер ошибок двух разных кодовых слов. В противном случае два разных входа иногда будут давать один и тот же выход, что с неизбежностью приведет к ошибкам декодирования. Если мы хотим избавиться от таких двусмысленностей декодирования, полное число строк, содержащихся во всех 2^{nR} сферах ошибок, не должно превышать полного количества битов 2^n в выходящем сообщении; мы требуем выполнения

$$2^{nH(p)}2^{nR} \leqslant 2^n \tag{5.22}$$

или

$$R \leqslant 1 - H(p) \equiv C(p). \tag{5.23}$$

Если надежность передачи достаточно высока, мы не можем ожидать, что быстродействие кода превзойдет $C(p)$. Но достижимо ли на самом деле быстродействие $R = C(p)$ (асимптотически)?

Фактически возможна передача с R, сколь угодно близким к $C(p)$ и сколь угодно малой вероятностью ошибки. По-видимому, самой остроумной из идей Шеннона была демонстрация того, что $C(p)$ может быть достигнуто учетом среднего по «случайным кодам». [Очевидно, что случайный выбор кода — не самый разумный способ, но, возможно это покажется удивительным, оказывается, что случайное кодирование достигает такого же высокого быстродействия (асимптотически при больших n), как и любая другая схема кодирования.] Поскольку C представляет собой оптимальное быстродействие при надежной передаче данных по каналу с шумом, она называется *емкостью канала связи* или *пропускной способностью канала связи*.

Предположим, что 2^{nR} кодовых слов представляют собой случайную выборку из ансамбля X^n. Сообщение (одно из кодовых слов) послано. Чтобы его декодировать, изобразим вокруг полученного сообщения «сферу Хэмминга», содержащую

$$2^{n[H(p)+\delta]} \tag{5.24}$$

строк. Сообщение декодируется содержащимся в этой сфере кодовым словом в предположении, что оно существует и единственно. Если такое кодовое слово не существует или оно не единственно, то будем считать, что произошла ошибка декодирования.

Насколько вероятна ошибка декодирования? Мы выбрали сферу декодирования достаточно большой, так что отсутствие достоверного кодового

слова внутри сферы атипично, следовательно, мы должны беспокоиться лишь о том, что ее займут более одного достоверного кодового слова. Поскольку всего имеется 2^n возможных строк, то окружающая выходящую строку сфера Хэмминга содержит долю

$$\frac{2^{n[H(p)+\delta]}}{2^n} = 2^{-n[C(p)-\delta]} \tag{5.25}$$

от общего количества строк. Таким образом, вероятность того, что одно из 2^{nR} случайно выбранных кодовых слов «по несчастью» займет эту сферу, равна

$$2^{-n[C(p)-R-\delta]}. \tag{5.26}$$

А так как δ мы можем выбрать сколь угодно малым, то R можно взять настолько близким к $C(p)$ [но все же меньшим, чем $C(p)$], насколько это необходимо, чтобы вероятность такой ошибки оставалась экспоненциально малой при $n \to \infty$.

Пока мы показали, что мала *средняя* вероятность ошибки, которую мы усредняем по выбору случайного кода, а для каждого конкретного кода — еще и по всем кодовым словам. Таким образом, должен существовать один частный код со средней (усредненной по кодовым словам) вероятностью ошибки, меньшей чем ε. Но нам хотелось бы иметь более сильный результат — вероятность ошибки мала для *каждого* кодового слова.

Чтобы установить этот более сильный результат, обозначим через P_i вероятность ошибки декодирования i-го посланного кодового слова. Мы продемонстрировали существование кода такого, что

$$\frac{1}{2^{nR}} \sum_{i=1}^{2^{nR}} P_i < \varepsilon. \tag{5.27}$$

Пусть $N_{2\varepsilon}$ обозначает количество кодовых слов с $P_i > 2\varepsilon$. Тогда мы приходим к выводу, что

$$\frac{1}{2^{nR}}(N_{2\varepsilon})2\varepsilon < \varepsilon \quad \text{или} \quad N_{2\varepsilon} < 2^{nR-1}, \tag{5.28}$$

то есть можно отбросить максимум половину кодовых слов, чтобы добиться $P_i < 2\varepsilon$ для *каждого* кодового слова. Быстродействие сконструированного нами нового кода равно

$$\text{Rate} = R - \frac{1}{n}, \tag{5.29}$$

что стремится к R при $n \to \infty$.

Таким образом, $C(p) = 1 - H(p)$ представляет собой максимальное быстродействие, которое может быть достигнуто асимптотически со сколь угодно малой вероятностью ошибки.

Рассмотрим теперь, как обобщить эти доказательства на более общие алфавиты и каналы. Пусть имеется канал связи, характеризуемый набором $p(y|x)$, и определенное распределение вероятностей $X = \{x, p(x)\}$ для входящих букв. Мы посылаем строки из n букв и предполагаем, что канал действует на каждую букву независимо. (О действующем таким образом канале говорят как о «канале без памяти».) Конечно, как только заданы $p(y|x)$ и $X = \{x, p(x)\}$, так сразу определены $p(x|y)$ и $Y = \{y, p(y)\}$.

Чтобы установить достижимое быстродействие, вновь рассмотрим усреднение по случайным кодам, где кодовые слова выбираются с *априорной* вероятностью, определяемой ансамблем X^n. Таким образом, с высокой вероятностью они будут выбраны из типичного набора строк букв, содержащего около $2^{nH(X)}$ таких типичных строк.

Для типичного, принадлежащего Y^n, получаемого сообщения существует около $2^{nH(X|Y)}$ сообщений, которые могли бы быть посланы. Мы можем декодировать полученное сообщение, сопоставляя ему «сферу», содержащую $2^{n[H(X|Y)+\delta]}$ возможных входов. Если внутри этой сферы имеется единственное кодовое слово, то им декодируется полученное сообщение.

Как и раньше, маловероятно, что внутри сферы не окажется ни одного кодового слова, однако мы должны исключить возможность того, что их там больше одного. Каждая сфера декодирования содержит долю

$$\frac{2^{n[H(X|Y)+\delta]}}{2^{nH(X)}} \cdot 2^{-n[H(X)-H(X|Y)-\delta]} = \\ = 2^{-n[I(X;Y)-\delta]} \tag{5.30}$$

от общего числа типичных входов. Если имеется 2^{nR} кодовых слов, то вероятность того, что одно из них случайно окажется внутри сферы декодирования, равна

$$2^{nR}2^{-n[I(X;Y)-\delta]} = 2^{-n[I(X;Y)-R-\delta]}. \tag{5.31}$$

Поскольку δ может быть выбрана сколь угодно малой, то R можно взять настолько близким к I (но все же меньшим, чем I), насколько это необходимо, чтобы вероятность ошибки декодирования оставалась экспоненциально малой при $n \to \infty$.

Это доказательство показывает, что, когда мы усредняем по случайным кодам и по кодовым словам, вероятность ошибки остается малой при любом быстродействии $R < I$. Тогда те же самые рассуждения, что и выше, показывают существование особого кода с вероятностью ошибки $< \varepsilon$ для каждого кодового слова. Это приемлемый результат, поскольку он согласуется с нашей интерпретацией I, как информации, которую мы приобретаем о входящем X, получая сигнал Y. То есть I представляет собой отнесенную к одной букве информацию, которую мы можем послать по данному каналу связи.

Взаимная информация $I(X;Y)$ зависит не только от условных вероятностей $p(y|x)$, характеризующих канал связи, но также и от априорных вероятностей $p(x)$ появления букв. Приведенное выше доказательство случайного кодирования применимо при любом выборе вероятностей $p(x)$, следовательно, мы показали, что безошибочная передача возможна при любом быстродействии R, меньшем чем

$$C = \max_{\{p(x)\}} I(X;Y). \tag{5.32}$$

C называется *емкостью канала* или *пропускной способностью канала* и зависит только от условных вероятностей, определяющих данный канал.

Мы показали, что достижимо любое быстродействие $R < C$, но может ли R превзойти C (при условии, что по-прежнему вероятность ошибки стремится к нулю при $n \to \infty$)? Доказательство того, что C является верхней границей быстродействия, в общем случае может показаться более тонким, чем для двоичного симметричного канала — вероятности ошибок для разных букв различны, и мы свободны в использовании этого при создании кода. Будем, однако, рассуждать следующим образом:

Допустим, что мы выбрали 2^{nR} строк из n букв в качестве кодовых слов. Рассмотрим ансамбль (обозначаемый как $\tilde{X}^n$), в котором каждое кодовое слово возникает с одинаковой вероятностью ($= 2^{-nR}$). Тогда очевидно, что

$$H(\tilde{X}^n) = nR. \tag{5.33}$$

Посылая кодовые слова через канал связи, мы получаем ансамбль $\tilde{Y}^n$ выходящих состояний.

Поскольку мы предполагаем, что канал действует на каждую букву независимо, условная вероятность для строки из n букв факторизуется:

$$p(y_1 y_2 \ldots y_n | x_1 x_2 \ldots x_n) = p(x_1|y_1)p(x_2|y_2)\cdots p(x_n|y_n), \tag{5.34}$$

а отсюда следует, что условная энтропия удовлетворяет условию

$$H(\tilde{Y}^n|\tilde{X}^n) = \langle -\log p(y^n|x^n)\rangle = \sum_i \langle -\log p(y_i|x_i)\rangle = \\ = \sum_i H(\tilde{Y}_i|\tilde{X}_i), \tag{5.35}$$

где $\tilde{X}_i$ и $\tilde{Y}_i$ – частные (маргинальные) распределения вероятностей для i-ой буквы, определяемые нашим распределением по кодовым словам. Напомним, что нам также известно, что $H(X,Y) \leqslant H(X) + H(Y)$ или

$$H(\tilde{Y}^n) \leqslant \sum_i H(\tilde{Y}_i). \tag{5.36}$$

Отсюда следует, что

$$I(\tilde{Y}^n;\tilde{X}^n) = H(\tilde{Y}^n) - H(\tilde{Y}^n|\tilde{X}^n) \leqslant \sum_i \left[H(\tilde{Y}_i) - H(\tilde{Y}_i|\tilde{X}_i)\right] = \\ = \sum_i I(\tilde{Y}_i;\tilde{X}_i) \leqslant nC; \tag{5.37}$$

взаимная информация посланного и полученного сообщений ограничена сверху суммой отнесенных к каждой букве взаимных информаций, а взаимная информация для каждой буквы ограничена сверху емкостью канала связи [поскольку C определяется как максимум $I(X;Y)$].

Вспоминая о симметрии взаимной информации, мы имеем

$$I(\tilde{X}^n;\tilde{Y}^n) = H(\tilde{X}^n) - H(\tilde{X}^n|\tilde{Y}^n) = \\ = nR - H(\tilde{X}^n|\tilde{Y}^n) \leqslant nC. \tag{5.38}$$

Теперь если мы в состоянии надежно декодировать при $n \to \infty$, то это означает, что входящее кодовое слово полностью определяется получаемым сигналом или что условная энтропия входа (в расчете на одну букву) должна стать малой:

$$\frac{1}{n} H(\tilde{X}^n|\tilde{Y}^n) \to 0. \tag{5.39}$$

Если безошибочность передачи возможна, то в пределе $n \to \infty$ уравнение (5.38) принимает вид

$$R \leqslant C. \tag{5.40}$$

Быстродействие не может превзойти емкость канала связи. [Вспомним, что условная энтропия, в отличие от взаимной информации, *не симметрична*. Действительно, $H(\tilde{Y}^n|\tilde{X}^n)/n$ *не становится* малым, поскольку канал вносит неопределенность в то, какое сообщение будет получено. Но если мы можем декодировать точно, то, коль скоро сигнал получен, исчезает неопределенность в том, какое кодовое слово было послано.]

Мы показали, что емкость C представляет собой максимальное достижимое быстродействие связи через канал с шумом, при котором вероятность ошибки декодирования стремится к нулю при стремящемся к бесконечности количестве букв в сообщении. В этом состоит теорема Шеннона о кодировании для канала связи с шумом.

Конечно, использованный нами метод (усреднение по случайным кодам) доказательства того, что равенство $R = C$ асимптотически достижимо, не очень конструктивен. Так как случайный код не имеет структуры или схемы, то кодирование и декодирование будут довольно громоздкими (нам нужна экспоненциально большая книга кодов). Тем не менее эта теорема важна и полезна, поскольку она говорит о том, что в принципе достижимо и, более того, что недостижимо, даже в принципе. К тому же, поскольку $I(X;Y)$ является вогнутой функцией от $X = \{x, p(x)\}$ (при фиксированном $\{p(y|x)\}$), то она имеет единственный локальный максимум, а C для интересуемого канала связи часто может быть вычислена (по крайней мере численно).

5.2. Энтропия фон Неймана

В теории классической информации мы часто рассматриваем источник, который готовит сообщения из n букв ($n \gg 1$), причем каждая буква независимо извлекается из ансамбля $X = \{x, p(x)\}$. Мы видели, что информационная энтропия Шеннона $H(X)$ (асимптотически при $n \to \infty$) представляет собой количество приходящихся на одну букву несжимаемых битов информации.

Нас также могут интересовать корреляции между сообщениями. Корреляции между двумя ансамблями букв X и Y характеризуются условными вероятностями $p(y|x)$. Мы видели, что взаимная информация

$$I(X;Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) \tag{5.41}$$

представляет собой приходящееся на одну букву количество битов информации об X, которую мы можем получить, читая Y (и наоборот). Если условные вероятности $p(y|x)$ характеризуют канал с шумом, то $I(X;Y)$ –

приходящееся на одну букву количество информации, которое может быть передано через канал связи (при *a priori* заданном распределении вероятностей для X-ов).

Мы хотели бы распространить эти понятия на *квантовую* информацию. Представим источник, который готовит сообщения из n букв, но теперь каждая буква выбирается из ансамбля квантовых состояний. Алфавит сигналов представляет собой множество квантовых состояний $\boldsymbol{\rho}_x$, каждое из которых появляется с определенной *априорной* вероятностью p_x.

Как мы уже подробно обсуждали, если наблюдателю неизвестно, какая буква приготовлена, то вероятность любого результата любого измерения буквы, выбранной из этого ансамбля, можно полностью охарактеризовать матрицей плотности

$$\boldsymbol{\rho} = \sum_x p_x \boldsymbol{\rho}_x; \tag{5.42}$$

для ПОЗМ $\{\mathbf{F}_a\}$ мы имеем

$$\mathrm{Prob}(a) = \mathrm{tr}\left(\mathbf{F}_a \boldsymbol{\rho}\right). \tag{5.43}$$

Для этой (или любой другой) матрицы плотности можно определить энтропию фон Неймана

$$S(\boldsymbol{\rho}) = -\,\mathrm{tr}\left(\boldsymbol{\rho}\log\boldsymbol{\rho}\right). \tag{5.44}$$

Конечно, если мы выберем ортонормированный базис $\{|a\rangle\}$, диагонализующий $\boldsymbol{\rho}$:

$$\boldsymbol{\rho} = \sum_a \lambda_a |a\rangle\langle a|, \tag{5.45}$$

то

$$S(\boldsymbol{\rho}) = H(A), \tag{5.46}$$

где $H(A)$ — энтропия Шеннона ансамбля $A = \{a, \lambda_a\}$.

В том случае, когда алфавит сигналов состоит из взаимно ортогональных чистых состояний, квантовый источник сводится к классическому; все сигнальные состояния идеально различимы и $S(\boldsymbol{\rho}) = H(A)$. Более интересен квантовый источник, сигнальные состояния которого $\boldsymbol{\rho}$ взаимно не коммутируют. Мы докажем, что энтропия фон Неймана является количественной мерой несжимаемой информации, содержащейся в квантовом источнике (в том случае, когда сигнальные состояния являются чистыми), почти как энтропия Шеннона является количественной мерой информации, содержащейся в классическом источнике.

На самом деле мы обнаружим, что энтропия фон Неймана играет двойственную роль. Она является количественной мерой не только *квантовой* информации, содержащейся в одной букве ансамбля (минимальное количество приходящихся на одну букву кубитов, необходимое для надежного кодирования информации), но и содержащейся в ней *классической* информации (максимальное количество приходящейся на одну букву информации — в битах, а не в кубитах — которое можно получить с помощью наилучшего измерения). Мы увидим, что энтропия фон Неймана входит в квантовую информацию еще одним, третьим способом, количественно определяя запутывание бинарного чистого состояния. Таким образом, теория квантовой информации в значительной мере занимается интерпретацией и применениями энтропии фон Неймана, подобно тому как классическая теория информации главным образом занимается интерпретацией и применениями энтропии Шеннона.

Фактически необходимый для развития квантовой теории информации математический аппарат очень похож на математику Шеннона (типичные последовательности, случайное кодирование,...); похож настолько, что временами скрывается то, что в концептуальном плане они на самом деле весьма различны. Центральной проблемой квантовой теории информации является то, что неортогональные чистые квантовые состояния нельзя идеально различить — особенность, не имеющая классического аналога.

5.2.1. Математические свойства $S(\rho)$

Имеется несколько часто используемых свойств $S(\rho)$ [многие из которых являются близкими аналогами свойств $H(X)$]. Ниже я привожу список некоторых из этих свойств. Большей частью их доказательства не сложны (заметным исключением является доказательство сильной субаддитивности) и включены в упражнения в конце главы[1].

(1) Чистота. Чистое состояние $\rho = |\varphi\rangle\langle\varphi|$ имеет $S(\rho) = 0$.

(2) Инвариантность. Энтропия не изменяется при унитарных преобразованиях базиса

$$S(\mathbf{U}\rho\mathbf{U}^{-1}) = S(\rho). \tag{5.47}$$

[1]Некоторые доказательства можно также найти в обзоре A. Wehrl, *General Properties of Entropy*, Rev. Mod. Phys. **50**, 221 (1978); или в главе 9 книги A. Peres, *Quantum Theory: Concept and Methods*, Kluwer Academic Publishers, New York et al 2002. [Подробное обсуждение математических свойств энтропии фон Неймана можно найти в книге М. Нильсен, И. Чанг, *Квантовые вычисления и квантовая информация*, М.: Мир, 2006. — *Прим. ред.*]

Это очевидно, поскольку $S(\boldsymbol{\rho})$ зависит только от собственных значений $\boldsymbol{\rho}$.

(3) Максимум. Если $\boldsymbol{\rho}$ имеет D ненулевых собственных значений, то

$$S(\boldsymbol{\rho}) \leqslant \log D, \tag{5.48}$$

где равенство достигается, когда все ненулевые собственные значения равны между собой. (Энтропия максимальна, когда квантовые состояния *равновероятны*.)

(4) Вогнутость. Для $\lambda_1, \lambda_2, \ldots \lambda_n \geqslant 0$ и $\lambda_1 + \lambda_2 + \ldots + \lambda_n = 1$

$$S(\lambda_1\boldsymbol{\rho}_1 + \lambda_2\boldsymbol{\rho}_2 + \ldots + \lambda_n\boldsymbol{\rho}_n) \geqslant \lambda_1 S(\boldsymbol{\rho}_1) + \lambda_2 S(\boldsymbol{\rho}_2) + \ldots \lambda_n S(\boldsymbol{\rho}_n). \tag{5.49}$$

То есть энтропия фон Неймана тем больше, чем нам *меньше известно* о том, как было приготовлено состояние. Это свойство является следствием выпуклости логарифмической функции.

(5) Энтропия измерения. Предположим, что в состоянии $\boldsymbol{\rho}$ измеряется наблюдаемая

$$\mathbf{A} = \sum_y |a_y\rangle a_y \langle a_y|, \tag{5.50}$$

так что результат a_y появляется с вероятностью

$$p(a_y) = \langle a_y|\boldsymbol{\rho}|a_y\rangle. \tag{5.51}$$

Тогда энтропия Шеннона ансамбля всех исходов измерения $Y = \{a_y, p(a_y)\}$ удовлетворяет

$$H(Y) \geqslant S(\boldsymbol{\rho}), \tag{5.52}$$

где равенство достигается для коммутирующих $\mathbf{A}$ и $\boldsymbol{\rho}$. Математически это утверждение означает, что в любом базисе $S(\boldsymbol{\rho})$ возрастает при замене нулями всех недиагональных матричных элементов $\boldsymbol{\rho}$. Физически это означает, что случайность результата измерения минимизируется, если выбирается измерение наблюдаемой, коммутирующей с матрицей плотности. Но если мы измеряем «плохую» наблюдаемую, то результат будет менее предсказуем.

(6) Энтропия приготовления. Если чистое состояние случайным образом извлекается из ансамбля $\{|\varphi_x\rangle, p_x\}$, так что матрица плотности равна

$$\boldsymbol{\rho} = \sum_x p_x |\varphi_x\rangle\langle\varphi_x|, \tag{5.53}$$

то

$$H(Y) \geqslant S(\rho), \tag{5.54}$$

где равенство достигается, если сигнальные состояния $|\varphi_x\rangle$ взаимно ортогональны. Это утверждение указывает на то, что перемешивание неортогональных чистых состояний ведет к *потере различимости*. [Мы не можем полностью восстановить информацию о том, какое состояние было приготовлено, поскольку, как мы обсудим позже, достижимый при выполнении измерения прирост информации не может превзойти $S(\rho)$.]

(7) Субаддитивность. Рассмотрим бинарную систему AB в состоянии ρ_{AB}. Тогда

$$S(\rho_{AB}) \leqslant S(\rho_A) + S(\rho_B), \tag{5.55}$$

где $\rho_A = \mathrm{tr}_B\, \rho_{AB}$, $\rho_B = \mathrm{tr}_A\, \rho_{AB}$, а равенство достигается при $\rho_{AB} = \rho_A \otimes \rho_B$. Таким образом, энтропия *аддитивна* для некоррелированных систем, в противном случае энтропия всей системы меньше суммы энтропий ее частей. Это свойство является аналогом свойства энтропии Шеннона

$$H(X,Y) \leqslant H(X) + H(Y), \tag{5.56}$$

(или $I(X;Y) \geqslant 0$); оно имеет место, поскольку некоторая информация в XY (или AB) закодирована в корреляциях между X и Y (A и B).

(8) Сильная субаддитивность. Для любого состояния ρ_{ABC} трехкомпонентной системы

$$S(\rho_{ABC}) + S(\rho_B) \leqslant S(\rho_{AB}) + S(\rho_{BC}). \tag{5.57}$$

Это свойство называется «сильной» субаддитивностью, поскольку оно сводится к (обычной) субаддитивности в случае одномерной B. Доказательство соответствующего свойства энтропии Шеннона довольно просто, однако для энтропии фон Неймана оно оказывается на удивление трудным[1]. Свойство сильной субаддитивности легче запомнить, если интерпретировать его следующим образом: AB и BC можно рассматривать как две *перекрывающиеся* подсистемы. Энтропия их объединения (ABC) плюс энтропия их пересечения (B) не превышает

[1] Набросок доказательства сильной субаддитивности энтропии фон Неймана приведен в статье A. Wehrl, *General Properties of Entropy*, Rev. Mod. Phys. **50**, 221 (1978); [На русском языке см. М. Нильсен, И. Чанг, *Квантовые вычисления и квантовая информация*, М.: Мир, 2006. — *Прим. ред.*]

сумму энтропий подсистем (AB и BC). Мы увидим, что сильная субаддитивность имеет глубокие и важные следствия.

(9) Неравенство треугольника (Неравенство Араки – Либа). Для бинарной системы

$$S(\rho_{AB}) \geqslant |S(\rho_A) - S(\rho_B)|. \tag{5.58}$$

Неравенство треугольника резко контрастирует с аналогичным свойством энтропии Шеннона

$$H(X,Y) \geqslant H(X), H(Y) \tag{5.59}$$

или

$$H(X|Y), H(Y|X) \geqslant 0. \tag{5.60}$$

Энтропия Шеннона классической бинарной системы превосходит энтропию Шеннона любой ее части - во всей системе содержится больше информации о ней, нежели в ее части! Но это не так для энтропии фон Неймана. В предельном случае бинарного чистого квантового состояния мы имеем $S(\rho_A) = S(\rho_B)$ (не равные нулю, если состояние запутано), в то время как $S(\rho_{AB}) = 0$. Бинарное состояние определенным образом приготовлено, но если мы измеряем наблюдаемые различных подсистем, то результаты измерений с неизбежностью становятся случайными и непредсказуемыми. Мы не можем различить, как было приготовлено состояние, наблюдая две подсистемы отдельно, поскольку информация закодирована скорее в нелокальных квантовых корреляциях. Сопоставление положительности условной энтропии Шеннона (в классическом случае) с неравенством треугольника (в квантовом случае) замечательно характеризует ключевое различие между квантовой и классической информацией.

5.2.2. Энтропия и термодинамика

Конечно, понятие энтропии впервые было введено в науку в термодинамике. Здесь я ненадолго отвлекусь на некоторые термодинамические приложения математических свойств $S(\rho)$.

Существует два различных (но связанных между собой) возможных подхода к основаниям квантовой статистической физики. В первом мы рассматриваем эволюцию изолированной (замкнутой) квантовой системы, но производим некоторое *сглаживание* (*coarse graining*), чтобы определить термодинамические переменные. Во втором подходе, который, возможно, физически более мотивирован, мы рассматриваем *открытую* систе-

му, квантовую систему в контакте с окружением, и следим за ее эволюцией, не контролируя окружение.

Для открытой системы определяющим математическим свойством энтропии фон Неймана является ее *субаддитивность*. Если система (A) и окружение (E) первоначально не коррелированы друг с другом

$$\boldsymbol{\rho}_{AE} = \boldsymbol{\rho}_A \otimes \boldsymbol{\rho}_E, \tag{5.61}$$

то энтропия аддитивна

$$S(\boldsymbol{\rho}_{AE}) = S(\boldsymbol{\rho}_A) + S(\boldsymbol{\rho}_E). \tag{5.62}$$

Предположим теперь, что открытая система эволюционирует в течение некоторого времени. Эволюция описывается унитарным оператором $\mathbf{U}_{AE}$, действующим на комбинированную систему $A + E$:

$$\boldsymbol{\rho}_{AE} \to \boldsymbol{\rho}'_{AE} = \mathbf{U}_{AE}\boldsymbol{\rho}_{AE}\mathbf{U}_{AE}^{-1}, \tag{5.63}$$

а поскольку унитарная эволюция сохраняет S, то

$$S(\boldsymbol{\rho}'_{AE}) = S(\boldsymbol{\rho}_{AE}). \tag{5.64}$$

Наконец, применим свойство субаддитивности к состоянию $S(\boldsymbol{\rho}'_{AE})$, получая в результате

$$S(\boldsymbol{\rho}_A) + S(\boldsymbol{\rho}_E) = S(\boldsymbol{\rho}'_{AE}) \leqslant S(\boldsymbol{\rho}'_A) + S(\boldsymbol{\rho}'_B), \tag{5.65}$$

где равенство имеет место в случае, когда A и E остаются некоррелированными. Если мы определим «полную» энтропию Вселенной как сумму энтропии системы и энтропии окружения, то придем к выводу, что *энтропия Вселенной не может убывать*. Это одна из формулировок второго закона термодинамики. Заметим, однако, чтобы вывести этот «закон», мы предположили, что в начальном состоянии система и окружение были некоррелированы.

Обычно взаимодействие системы и окружения *будет* генерировать корреляции, так что (в предположении *отсутствия* начальных корреляций) энтропия действительно *будет нарастать*. Вспомните из нашего обсуждения основного уравнения в § 3.5, что обычно окружение быстро «забывает», так что, если наше время разрешения достаточно велико, то в каждый момент времени систему и окружение (фактически) можно рассматривать как

«первоначально» некоррелированные (марковское приближение). В этом предположении «полная» энтропия будет монотонно возрастать, асимптотически приближаясь к своему теоретическому максимуму, максимальному достижимому значению, согласующемуся со всеми законами сохранения (энергии, заряда, барионного числа и т. д.).

Действительно, обычное предположение, лежащее в основании квантовой статистической физики, состоит в том, что система и окружение находятся в «наиболее вероятной конфигурации», максимизирующей $S(\rho_A) + S(\rho_E)$. В этой конфигурации все «доступные» состояния равновероятны.

С микроскопической точки зрения первоначально закодированная в системе информация (наша способность отличать одно начальное состояние от другого, первоначально ортогонального, состояния) теряется; она оказывается закодированной в квантовом запутывании системы и окружения. В принципе эта информация могла бы быть восстановлена, но на практике локальным наблюдателям это совершенно недоступно. Следовательно, мы наблюдаем термодинамическую необратимость.

Конечно, мы можем применить эти рассуждения к большой замкнутой системе (всей Вселенной?). Мы можем разделить систему на малую ее часть и остаток (окружение малой части). Тогда сумма энтропий этих частей будет неубывающей. Это частный тип сглаживания. Эта часть замкнутой системы ведет себя подобно открытой системе, поэтому для больших систем микроканонический и канонический ансамбли статистической механики дают одинаковые предсказания.

5.3. Сжатие квантовых данных

Что является квантовым аналогом теоремы о кодировании без шума?

Рассмотрим длинное сообщение, состоящее из n букв, где каждая буква случайным образом выбирается из ансамбля чистых состояний

$$\{|\varphi_x\rangle, p_x\}, \tag{5.66}$$

а сами $|\varphi_x\rangle$ не обязательно ортогональны. (Например, $|\varphi_x\rangle$ может представлять собой состояние поляризации одного фотона.) Таким образом, каждая буква описывается матрицей плотности

$$\rho = \sum_x p_x |\varphi_x\rangle\langle\varphi_x|, \tag{5.67}$$

а все сообщение целиком — матрицей плотности

$$\rho^n = \rho \otimes \rho \otimes \cdots \otimes \rho. \tag{5.68}$$

Зададим вопрос: насколько *избыточна* эта квантовая информация? Мы хотели бы придумать *квантовый код*, который *позволит* сжать сообщение в более узкое гильбертово пространство без потери точности его воспроизведения. Например, допустим, что у нас есть устройство квантовой памяти (жесткий диск квантового компьютера?), и нам известны *статистические* свойства записанных данных (то есть мы знаем ρ). Сжимая данные, мы хотим сэкономить объем памяти.

Оптимальное сжатие, которое может быть достигнуто, было найдено Беном Шумахером. Можете ли вы угадать ответ? Наилучшим возможным сжатием, совместимым со сколь угодно высокой точностью воспроизведения при $n \to \infty$ является сжатие в гильбертово пространство $\mathcal{H}$ с

$$\log(\dim \mathcal{H}) \sim nS(\rho). \tag{5.69}$$

В этом отношении энтропия фон Неймана представляет собой количество *кубитов* квантовой информации, переносимых одной буквой сообщения. Например, если сообщение состоит из n фотонных состояний поляризации, то мы можем сжать его до $m = nS(\rho)$ фотонов – сжатие всегда возможно, за исключением случая $\rho = \frac{1}{2}1$. (Мы не можем сжать случайные кубиты точно так же, как не можем сжать случайные биты.)

Доказательство теоремы Шумахера не составляет труда, если известны и понятны результаты Шеннона. Большой заслугой Шумахера была правильная постановка вопроса, что позволило впервые дать точную (квантово-) информационную теоретическую интерпретацию энтропии фон Неймана[1].

5.3.1. Сжатие квантовых данных: пример

Прежде чем обсуждать в общем виде протокол Шумахера сжатия квантовых данных, полезно рассмотреть простой пример. Предположим, что нашими буквами являются отдельные кубиты, извлекаемые из ансамбля

$$\begin{aligned} |\uparrow_z\rangle &= \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad p = \frac{1}{2}, \\ |\uparrow_x\rangle &= \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix}, \quad p = \frac{1}{2}, \end{aligned} \tag{5.70}$$

[1] Как мы вскоре увидим, интерпретация $S(\rho)$ на языке *классической* информации, закодированной в квантовых состояниях, действительно была известна раньше.

так что матрица плотности каждой буквы имеет вид

$$\boldsymbol{\rho} = \frac{1}{2}|\uparrow_z\rangle\langle\uparrow_z| + \frac{1}{2}|\uparrow_x\rangle\langle\uparrow_x| = \\ = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix} = \begin{pmatrix} 3/4 & 1/4 \\ 1/4 & 1/4 \end{pmatrix}. \tag{5.71}$$

Как очевидно из симметрии, собственными состояниями $\boldsymbol{\rho}$ являются кубиты, ориентированные вверх и вниз вдоль оси $\hat{n} = \frac{1}{\sqrt{2}}(\hat{x} + \hat{z})$:

$$|0'\rangle \equiv |\uparrow_{\hat{n}}\rangle = \begin{pmatrix} \cos\frac{\pi}{8} \\ \sin\frac{\pi}{8} \end{pmatrix}, \\ |1'\rangle \equiv |\downarrow_{\hat{n}}\rangle = \begin{pmatrix} \sin\frac{\pi}{8} \\ -\cos\frac{\pi}{8} \end{pmatrix}; \tag{5.72}$$

соответствующие им собственные значения:

$$\lambda(0') = \frac{1}{2} + \frac{1}{2\sqrt{2}} = \cos^2\frac{\pi}{8}, \\ \lambda(1') = \frac{1}{2} - \frac{1}{2\sqrt{2}} = \sin^2\frac{\pi}{8}; \tag{5.73}$$

[очевидно, что $\lambda(0') + \lambda(1') = 1$, а $\lambda(0')\lambda(1') = 1/8 = \det\boldsymbol{\rho}$]. Собственное состояние $|0'\rangle$ одинаково (и довольно сильно) перекрывается с обоими сигнальными состояниями

$$|\langle 0'|\uparrow_z\rangle|^2 = |\langle 0'|\uparrow_x\rangle|^2 = \cos^2\frac{\pi}{8} = 0{,}8535; \tag{5.74}$$

перекрытия состояния $|1'\rangle$ тоже одинаковы (но относительно слабы)

$$|\langle 1'|\uparrow_z\rangle|^2 = |\langle 1'|\uparrow_x\rangle|^2 = \sin^2\frac{\pi}{8} = 0{,}1465. \tag{5.75}$$

Таким образом, если мы не знаем, какое состояние было послано, $|\uparrow_z\rangle$ или $|\uparrow_x\rangle$, то лучшей нашей догадкой является $|\psi\rangle = |0'\rangle$. Это предположение имеет максимальную *точность воспроизведения*

$$F = \frac{1}{2}|\langle\uparrow_z|\psi\rangle|^2 + \frac{1}{2}|\langle\uparrow_x|\psi\rangle|^2 \tag{5.76}$$

среди всех возможных состояний кубита $|\psi\rangle$ ($F = 0{,}8535$).

Теперь представим, что Алисе нужно послать Бобу три буквы. Но она может позволить себе послать только два кубита (квантовые каналы требуют очень больших расходов!). Тем не менее она хочет, чтобы Боб реконструировал ее состояние с максимально возможной точностью воспроизведения.

Она могла бы послать Бобу две из имеющихся у нее трех букв и предложить Бобу угадать $|0'\rangle$ для третьей. Тогда Боб получает две буквы с $F = 1$ и имеет $F = 0{,}8535$ для третьей; следовательно, полная $F = 0{,}8535$. Но существует ли более разумная процедура, достигающая более высокой точности воспроизведения?

Лучшая процедура действительно *существует*. Диагонализовав ρ, мы разложили гильбертово пространство одного кубита на «вероятное» (натянутое на $|0'\rangle$) и «маловероятное» (натянутое на $|1'\rangle$) одномерные подпространства. Подобным образом мы можем разложить гильбертово пространство трех кубитов на вероятное и маловероятное подпространства. Если произвольное сигнальное состояние имеет вид $|\psi\rangle = |\psi_1\rangle|\psi_2\rangle|\psi_3\rangle$ (с каждым из трех кубитов, находящихся в состоянии $|\uparrow_z\rangle$ или $|\uparrow_x\rangle$), то

$$
\begin{aligned}
|\langle 0'0'0'|\psi\rangle|^2 &= \cos^6\frac{\pi}{8} = 0{,}6219,\\
|\langle 0'0'1'|\psi\rangle|^2 &= |\langle 0'1'0'|\psi\rangle|^2 = |\langle 1'0'0'|\psi\rangle|^2 = \cos^4\frac{\pi}{8}\sin^2\frac{\pi}{8} = 0{,}1067,\\
|\langle 0'1'1'|\psi\rangle|^2 &= |\langle 1'0'1'|\psi\rangle|^2 = |\langle 1'1'0'|\psi\rangle|^2 = \cos^2\frac{\pi}{8}\sin^4\frac{\pi}{8} = 0{,}0183,\\
|\langle 1'1'1'|\psi\rangle|^2 &= \sin^6\frac{\pi}{8} = 0{,}0031.
\end{aligned}
\tag{5.77}
$$

Таким образом, мы можем разложить пространство на вероятное подпространство Λ, натянутое на $\{|0'0'0'\rangle, |0'0'1'\rangle, |0'1'0'\rangle, |1'0'0'\rangle\}$, и его ортогональное дополнение $\Lambda^\perp$. Если мы выполняем («грубое») измерение, проецирующее сигнальное состояние на Λ или $\Lambda^\perp$, то вероятность проецирования на вероятное подпространство равна

$$P_{\text{likely}} = 0{,}6219 + 3 \times 0{,}1067 = 0{,}9419, \tag{5.78}$$

тогда как вероятность проецирования на маловероятное подпространство —

$$P_{\text{unlikely}} = 3 \times 0{,}0183 + 0{,}0031 = 0{,}0581. \tag{5.79}$$

Чтобы выполнить это грубое измерение, Алиса могла бы, например, сначала применить унитарное преобразование U, превращающее четыре высоко вероятных базисных состояния в

$$|\cdot\rangle|\cdot\rangle|0\rangle, \tag{5.80}$$

а четыре маловероятных базисных состояния в

$$|\cdot\rangle|\cdot\rangle|1\rangle\,; \tag{5.81}$$

затем Алиса измеряет третий кубит, чтобы закончить грубое измерение. Если результатом является $|0\rangle$, то ее входящее состояние было спроецировано (в действительности) на Λ. Она посылает Бобу два оставшихся (неизмеренные) кубита. Когда Боб получает это (сжатое) двухкубитовое состояние $|\psi_{\rm comp}\rangle$, он развертывает его, присоединяя $|0\rangle$ и применяя $\mathbf{U}^{-1}$,

$$|\psi'\rangle = \mathbf{U}^{-1}(|\psi_{\rm comp}\rangle|0\rangle). \tag{5.82}$$

Если измерение Алисы третьего кубита дает $|1\rangle$, то она спроецировала свое входящее состояние на маловероятное подпространство $\Lambda^{\perp}$. Лучшее, что она может сделать в этом случае, это послать состояние, которое Боб развертывает в самое вероятное состояние $|0'0'0'\rangle$; то есть она посылает такое состояние $|\psi_{\rm comp}\rangle$, что

$$|\psi'\rangle = \mathbf{U}^{-1}(|\psi_{\rm comp}\rangle|0\rangle) = |0'0'0'\rangle. \tag{5.83}$$

Таким образом, если Алиса кодирует трехкубитовое сигнальное состояние $|\psi\rangle$, посылает два кубита Бобу, а Боб декодирует как только что описано, тогда он получает состояние

$$|\psi\rangle\langle\psi| \;\longrightarrow\; \boldsymbol{\rho} = \mathbf{E}|\psi\rangle\langle\psi|\mathbf{E} + |0'0'0'\rangle\langle\psi|(\mathbf{1}-\mathbf{E})|\psi\rangle\langle 0'0'0'|, \tag{5.84}$$

где $\mathbf{E}$ – проекционный оператор на Λ. Достигаемая в этой процедуре точность воспроизведения равна

$$F = \langle\psi|\boldsymbol{\rho}|\psi\rangle = \big(\langle\psi|\mathbf{E}|\psi\rangle\big)^2 + \big(\langle\psi|(\mathbf{1}-\mathbf{E})|\psi\rangle\big)\big(\langle\psi|0'0'0'\rangle\big)^2 = \\ = (0{,}9419\dot{})^2 + 0{,}0581 \times 0{,}6219 = 0{,}9234. \tag{5.85}$$

Это действительно лучше наивной процедуры посылки двух из трех кубитов, каждого с идеальной точностью воспроизведения.

Когда мы посылаем более длинные сообщения с большим количеством букв, точность воспроизведения сжатия улучшается. Энтропия фон Неймана однокубитового ансамбля равна

$$S(\boldsymbol{\rho}) = H\left(\cos^2\frac{\pi}{8}\right) = 0{,}60088\ldots \tag{5.86}$$

Следовательно, согласно теореме Шумахера мы можем сократить длинное сообщение на фактор (скажем) 0,6009 и тем не менее достичь очень высокой точности воспроизведения.

5.3.2. Кодирование Шумахера в общем

Ключом к теореме Шеннона о кодировании в отсутствии шума является то, что мы без большой потери точности воспроизведения можем кодировать типичные последовательности и игнорировать остальные. Чтобы количественно описать сжимаемость квантовой информации, перейдем от понятия типичной *последовательности* к понятию типичного *подпространства*. Ключом к теореме Шумахера о квантовом кодировании в отсутствии шума является то, что мы без большой потери точности воспроизведения можем кодировать типичные подпространства и игнорировать их ортогональные дополнения.

Рассмотрим сообщение, состоящее из n букв, где каждая буква является чистым квантовым состоянием, извлекаемым из ансамбля $\{|\varphi_x\rangle, p_x\}$, так что матрица плотности одной буквы равна

$$\rho = \sum_x p_x |\varphi_x\rangle\langle\varphi_x|. \tag{5.87}$$

Более того, буквы извлекаются независимо, так что матрица плотности всего сообщения

$$\rho^n = \rho \otimes \rho \otimes \cdots \otimes \rho. \tag{5.88}$$

Мы хотим доказать, что для больших n почти все носители этой матрицы плотности занимают подпространство полного гильбертова пространства сообщений, причем размерность этого подпространства асимптотически стремится к $2^{nS(\rho)}$.

Этот вывод непосредственно следует из соответствующего классического утверждения, если мы рассматриваем ортонормированный базис, в котором ρ диагональна. Работая в этом базисе, по существу, мы можем рассматривать наш квантовый источник информации как эффективный классический источник, производящий сообщения, которые представляют собой строки из собственных состояний ρ. Вероятность каждого такого сообщения определяется произведением соответствующих собственных значений ρ. Для заданных n и δ определим типичное подпространство Λ как пространство, натянутое на собственные векторы ρ^n, с собственными значениями, удовлетворяющими

$$2^{-n(S+\delta)} \leqslant \lambda \leqslant 2^{-n(S-\delta)}. \tag{5.89}$$

Непосредственно пользуясь результатом Шеннона, мы приходим к выводу, что для любых δ, $\varepsilon > 0$ и при достаточно большом n сумма подчиняющихся

этому условию собственных значений $\boldsymbol{\rho}^n$ удовлетворяет неравенству

$$\mathrm{tr}(\boldsymbol{\rho}^n \mathbf{E}) > 1 - \varepsilon \tag{5.90}$$

(где $\mathbf{E}$ обозначает проекционный оператор на типичное подпространство), а количество $\dim \Lambda$ таких собственных значений удовлетворяет неравенству

$$(1-\varepsilon)2^{n(S-\delta)} \leqslant \dim \Lambda \leqslant 2^{n(S+\delta)}. \tag{5.91}$$

Наша стратегия кодирования состоит в том, чтобы отправлять состояния, действительно принадлежащие типичному подпространству. Например, мы можем выполнить грубое измерение, проецирующее входящее сообщение на Λ или на $\Lambda^\perp$; с вероятностью $P_\Lambda = \mathrm{tr}(\boldsymbol{\rho}^n \mathbf{E}) > 1 - \varepsilon$ результат будет принадлежать Λ. В таком случае спроецированное состояние кодируется и посылается. Асимптотически вероятность другого результата пренебрежимо мала, поэтому не так уж важно, что мы будем делать в этом случае.

Кодирование спроецированного состояния просто упаковывает его, чтобы оно могло переноситься минимальным количеством кубитов. Например, мы применяем унитарное преобразование базиса $\mathbf{U}$, которое превращает каждое состояние $|\psi_{\mathrm{typ}}\rangle$ из Λ в состояние вида

$$\mathbf{U}|\psi_{\mathrm{typ}}\rangle = |\psi_{\mathrm{comp}}\rangle|0_{\mathrm{rest}}\rangle, \tag{5.92}$$

где $|\psi_{\mathrm{comp}}\rangle$ — состояние $n(S+\delta)$ кубитов, а $|0_{\mathrm{rest}}\rangle$ обозначает состояние $|0\rangle\otimes\ldots\otimes|0\rangle$ остальных кубитов. Алиса посылает $|\psi_{\mathrm{comp}}\rangle$ Бобу, который декодирует его, присоединяя $|0_{\mathrm{rest}}\rangle$ и применяя $\mathbf{U}^{-1}$.

Предположим, что

$$|\varphi_i\rangle = |\varphi_{x_1(i)}\rangle|\varphi_{x_2(i)}\rangle\cdots|\varphi_{x_n(i)}\rangle \tag{5.93}$$

обозначает произвольное сообщение, представляющее собой одно из n-буквенных чистых состояний, которое может быть послано. После того как выполнены только что описанные кодирование, передача и декодирование, Боб получает реконструированное состояние

$$|\varphi_i\rangle\langle\varphi_i| \to \boldsymbol{\rho}_i' = \mathbf{E}|\varphi_i\rangle\langle\varphi_i|\mathbf{E} + \boldsymbol{\rho}_{i,Junk}\langle\varphi_i|(\mathbf{1}-\mathbf{E})|\varphi_i\rangle, \tag{5.94}$$

где $\boldsymbol{\rho}_{i,Junk}$ — состояние, выбираемое нами для отправления, если грубое измерение дает результат $\Lambda^\perp$. Что можно сказать относительно точности воспроизведения этой процедуры?

Точность воспроизведения изменяется от сообщения к сообщению (в противоположность обсуждавшемуся выше примеру), поэтому мы рассматриваем точность воспроизведения, усредненную по ансамблю возможных сообщений:

$$F = \sum_i p_i \langle\varphi_i|\boldsymbol{\rho}_i'|\varphi_i\rangle = \sum_i p_i \langle\varphi_i|\mathbf{E}|\varphi_i\rangle\langle\varphi_i|\mathbf{E}|\varphi_i\rangle + \\ + \sum_i p_i \langle\varphi_i|\boldsymbol{\rho}_{i,Junk}'|\varphi_i\rangle\langle\varphi_i|\mathbf{1}-\mathbf{E}|\varphi_i\rangle \geqslant \sum_i p_i \|\mathbf{E}|\varphi_i\rangle\|^4, \quad (5.95)$$

где последнее неравенство справедливо, поскольку вклад «мусора» неотрицателен. Так как для любого вещественного числа

$$(x-1)^2 \geqslant 0 \quad \text{или} \quad x^2 \geqslant 2x-1, \quad (5.96)$$

мы имеем (полагая $x = \|\mathbf{E}|\varphi_i\rangle\|^2$)

$$\|\mathbf{E}|\varphi_i\rangle\|^4 \geqslant 2\|\mathbf{E}|\varphi_i\rangle\|^2 - 1 \quad (5.97)$$

и, следовательно,

$$F \geqslant \sum_i p_i \big(2\langle\varphi_i|\mathbf{E}|\varphi_i\rangle - 1\big) = 2\,\mathrm{tr}\,(\boldsymbol{\rho}^n\mathbf{E}) - 1 > 2(1-\varepsilon) - 1 = 1 - 2\varepsilon. \quad (5.98)$$

Итак, мы показали, что можно сжать сообщение до объема, несколько меньшего, чем $n(S+\delta)$ кубитов, обеспечивая в то же время сколь угодно высокую при больших n усредненную точность воспроизведения.

Следовательно, мы установили, что с несущественной потерей точности воспроизведения сообщение может быть сжато до $S+\delta$ кубитов в расчете на одну букву. Возможно ли дальнейшее сжатие?

Допустим, что Боб декодирует полученное сообщение $\boldsymbol{\rho}_{\mathrm{comp,i}}$ путем присоединения кубитов и применения преобразования $\mathbf{U}^{-1}$, получая при этом

$$\boldsymbol{\rho}' = \mathbf{U}^{-1}(\boldsymbol{\rho}_{\mathrm{comp,i}} \otimes |0\rangle\langle 0|)\mathbf{U} \quad (5.99)$$

(«унитарное декодирование»). Допустим, что $\boldsymbol{\rho}_{\mathrm{comp,i}}$ было сжато до $n(S-\delta)$ кубитов. Тогда, *независимо от того, как было закодировано входящее сообщение*, все декодированные сообщения будут принадлежать подпространству Λ' размерности $2^{n(S-\delta)}$ гильбертова пространства Боба. (Мы не предполагаем здесь, что Λ' не имеет ничего общего с типичным подпространством.)

Если входящим сообщением является $|\varphi_i\rangle$, то реконструированное Бобом сообщение — $\boldsymbol{\rho}'_i$, которое может быть диагонализовано

$$\boldsymbol{\rho}'_i = \sum_{a_i} |a_i\rangle \lambda_{a_i} \langle a_i|, \tag{5.100}$$

где векторы $|a_i\rangle$ — взаимно ортогональные состояния из Λ'. Точность воспроизведения реконструированного сообщения равна

$$F_i = \langle \varphi_i | \boldsymbol{\rho}'_i | \varphi_i \rangle = \sum_{a_i} \lambda_{a_i} \langle \varphi_i | a_i \rangle \langle a_i | \varphi_i \rangle \leqslant$$

$$\leqslant \sum_{a_i} \langle \varphi_i | a_i \rangle \langle a_i | \varphi_i \rangle \leqslant \langle \varphi_i | \mathbf{E}' | \varphi_i \rangle, \tag{5.101}$$

где $\mathbf{E}'$ — ортогональный проектор на подпространство Λ'. Следовательно, усредненная точность воспроизведения удовлетворяет

$$F = \sum_i p_i F_i \leqslant \sum_i p_i \langle \varphi_i | \mathbf{E}' | \varphi_i \rangle = \mathrm{tr}(\boldsymbol{\rho}^n \mathbf{E}'). \tag{5.102}$$

Но поскольку $\mathbf{E}'$ проецирует на пространство размерности $2^{n(S-\delta)}$, то $\mathrm{tr}(\boldsymbol{\rho}^n \mathbf{E}')$ не может быть больше суммы $2^{n(S-\delta)}$ наибольших собственных значений $\boldsymbol{\rho}^n$. Из свойств типичных подпространств следует, что эта сумма принимает сколь угодно малое значение; при достаточно большом n

$$F \leqslant \mathrm{tr}(\boldsymbol{\rho}^n \mathbf{E}') < \epsilon. \tag{5.103}$$

Таким образом, мы показали, что если мы попытаемся сжать сообщение до $S - \delta$ кубитов на одну букву, тогда при достаточно большом n точность воспроизведения неизбежно станет плохой. Итак, мы приходим к выводу, что $S(\boldsymbol{\rho})$ кубитов на одну букву является оптимальным сжатием квантовой информации, которое может быть достигнуто, если мы хотим получить хорошую точность воспроизведения при n стремящемся к бесконечности. В этом состоит теорема Шумахера о кодировании в отсутствии шума.

Приведенное выше доказательство применимо к любой мыслимой схеме кодирования, но только к ограниченному классу схем декодирования (унитарное декодирование). Конечно, может быть рассмотрена более общая схема декодирования, описываемая *супероператором*. Тогда потребуется более высокая техника для доказательства того, что невозможно лучшее сжатие, чем S кубитов на одну букву. Но вывод остается неизменным. Суть в том, что $S - \delta$ кубитов недостаточно для того, чтобы различить все типичные состояния.

Подводя итог, отметим тесную аналогию между теоремами Шеннона и Шумахера о кодировании в отсутствии шума. В классическом случае почти все длинные сообщения являются типичными последовательностями, так что мы можем кодировать только их и тем не менее иметь малую вероятность ошибки. В квантовом случае почти все длинные сообщения имеют почти единичное перекрытие с типичным подпространством, так что мы можем кодировать только его и тем не менее достигать высокой точности воспроизведения.

Фактически Алиса могла бы послать Бобу эффективно классическую информацию — строку $x_1 x_2 \ldots x_n$, закодированную во взаимно ортогональных квантовых состояниях — тогда Боб, следуя этим классическим инструкциям, мог бы реконструировать состояние Алисы. Таким способом они могли бы добиться высоко надежного сжатия до $H(X)$ битов (или кубитов) в расчете на одну букву. Но если буквы извлекаются из ансамбля *неортогональных* чистых состояний, то эта степень сжатия не оптимальна; часть классической информации о приготовлении состояния становится избыточной, поскольку неортогональные состояния не могут быть идеально различимыми. Таким образом, кодирование Шумахера может продвинуться дальше, достигая оптимального сжатия $S(\rho)$ кубитов на одну букву сообщения. Информация упакована более эффективно, но дорогой ценой — Боб получил то, что имела ввиду Алиса, но он не может узнать — что. В противоположность классическому случаю, Боб не может выполнить никакого измерения, чтобы корректно дешифровать сообщение Алисы. Попытка прочитать сообщение неизбежно внесет в него возмущение.

5.3.3. Кодирование смешанного состояния: информация Холево

Теорема Шумахера характеризует сжимаемость ансамбля чистых состояний. Но что если буквы извлекаются из ансамбля смешанных состояний? В этом случае сжимаемость надежно не установлена и является предметом текущих исследований[1].

Нетрудно видеть, что для смешанных состояний $S(\rho)$ уже не будет ответом. Чтобы привести тривиальный пример, предположим, что некоторое смешанное состояние ρ_0 с энтропией $S(\rho_0) \neq 0$ выбирается с вероятностью $p_0 = 1$. Тогда сообщение всегда равно $\rho_0 \otimes \rho_0 \otimes \cdots \otimes \rho_0$ и не несет никакой информации; Боб может идеально реконструировать сообщение, *ничего не получая* от Алисы. Следовательно, это сообщение можно сжать до нуля кубитов на одну букву, что меньше, чем $S(\rho_0) > 0$.

[1] См. M. Horodecki, *Limits for Compression of Quantum Information Carried by Ensembles of Mixed States*, Phys. Rev., **A57**, 3364–3369 (1997); quant-ph/9712035.

Чтобы построить менее тривиальный пример, вспомним, что для ансамбля взаимно ортогональных чистых состояний энтропия Шеннона равна энтропии фон Неймана:

$$H(X) = S(\rho), \tag{5.104}$$

так что классическая и квантовая сжимаемости совпадают. Это справедливо, поскольку ортогональные состояния идеально различимы. Фактически, если Алиса хочет послать Бобу сообщение

$$|\varphi_{x_1}\rangle|\varphi_{x_2}\rangle\cdots|\varphi_{x_n}\rangle, \tag{5.105}$$

то она может послать классическое сообщение $x_1 \ldots x_n$, а Боб может реконструировать состояние с идеальной точностью воспроизведения.

Теперь предположим, что буквы извлекаются из ансамбля взаимно ортогональных *смешанных* состояний $\{\rho_x, p_x\}$:

$$\operatorname{tr} \rho_x \rho_y = 0, \qquad x \neq y; \tag{5.106}$$

то есть ρ_x и ρ_y имеют носители во взаимно ортогональных подпространствах гильбертова пространства. Эти смешанные состояния также идеально различимы, то есть опять сообщения, по существу, классические и, следовательно, могут быть сжаты до $H(X)$ кубитов на одну букву. Например, мы можем расширить гильбертово пространство наших букв $\mathcal{H}_A$ до более широкого пространства $\mathcal{H}_A \otimes \mathcal{H}_B$ и выбрать очищение каждого ρ_x, то есть чистое состояние $|\varphi_x\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$, такое что

$$\operatorname{tr}_B \left(|\varphi_x\rangle_{AB\ AB}\langle\varphi_x|\right) = (\rho_x)_A. \tag{5.107}$$

Эти чистые состояния взаимно ортогональны, а ансамбль $\{|\varphi_x\rangle_{AB}, p_x\}$ имеет энтропию фон Неймана $H(X)$; следовательно, мы можем выполнить сжатие сообщения

$$|\varphi_{x_1}\rangle_{AB}\cdots|\varphi_{x_n}\rangle_{AB} \tag{5.108}$$

по Шумахеру до $H(X)$ кубитов на одну букву (асимптотически). После развертывания этого состояния Боб может взять частичный след, «выбрасывая» подсистему B, и таким образом реконструировать сообщение Алисы.

Чтобы сделать разумное предположение о том, какое выражение характеризует сжимаемость сообщения, построенного из алфавита смешанных состояний, мы могли бы поискать выражение, которое сводится к $S(\rho)$ для ансамбля чистых состояний, и — к $H(X)$ для ансамбля взаимно ортогональных смешанных состояний. Выбирая базис, в котором

$$\rho = \sum_x p_x \rho_x \tag{5.109}$$

является блочно-диагональным, мы видим, что

$$\begin{aligned} S(\rho) &= -\operatorname{tr}\rho\log\rho = -\sum_x \operatorname{tr}\left(p_x\rho_x\right)\log\left(p_x\rho_x\right) = \\ &= -\sum_x p_x\log p_x - \sum_x p_x \operatorname{tr}\rho_x\log\rho_x = \\ &= H(X) + \sum_x p_x S(\rho_x) \end{aligned} \tag{5.110}$$

(вспоминая, что $\operatorname{tr}\rho_x = 1$ для каждого x). Следовательно, мы можем записать энтропию Шеннона в виде

$$H(X) = S(\rho) - \sum_x p_x S(\rho_x) \equiv \chi(\mathcal{E}). \tag{5.111}$$

Величина $\chi(\mathcal{E})$ называется *информацией Холево* ансамбля $\mathcal{E} = \{\rho_x, p_x\}$. Очевидно, она зависит не только от матрицы плотности ρ, но и от конкретного способа реализации ρ как ансамбля смешанных состояний. Мы нашли, что как для ансамбля чистых состояний, так и для ансамбля *взаимно ортогональных* смешанных состояний информация Холево $\chi(\mathcal{E})$ представляет собой оптимальное количество кубитов на одну букву, которого можно достичь, если мы сжимаем сообщение, сохраняя высокую точность воспроизведения при больших n.

Информация Холево может рассматриваться как обобщение энтропии фон Неймана, переходящее в $S(\rho)$ для ансамбля чистых состояний. Она также является близким аналогом взаимной информации

$$I(Y;X) = H(Y) - H(Y|X) \tag{5.112}$$

в классической теории информации, сообщающей нам, насколько в среднем уменьшается энтропия Шеннона ансамбля Y, когда мы узнаем значение X; аналогично

$$\chi(\mathcal{E}) = S(\rho) - \sum_x p_x S(\rho_x) \tag{5.113}$$

говорит нам, насколько в среднем уменьшается энтропия фон Неймана ансамбля, когда мы узнаем, как он был приготовлен. Подобно классической взаимной информации, информация Холево всегда неотрицательна, как это следует из свойства вогнутости $S(\rho)$

$$S\left(\sum p_x\rho_x\right) \geqslant \sum p_x S(\rho_x). \tag{5.114}$$

Теперь мы хотим исследовать связь между информацией Холево и сжимаемостью сообщений, построенных из алфавита *неортогональных* смешанных состояний. Фактически можно показать, что в общем случае невозможно сжатие с высокой точностью воспроизведения до объема, меньшего чем χ на одну букву сообщения.

Чтобы установить этот результат, воспользуемся свойством «монотонности» χ, доказанным Линдбладом и Ульманом: супероператор не может увеличивать информацию Холево. То есть если \$ — произвольный супероператор, действующий на ансамбль смешанных состояний как

$$\$: \mathcal{E} = \{\boldsymbol{\rho}_x, p_x\} \rightarrow \mathcal{E}' = \{\$(\boldsymbol{\rho}_x), p_x\}, \tag{5.115}$$

то

$$\chi(\mathcal{E}') \leqslant \chi(\mathcal{E}). \tag{5.116}$$

Монотонность Линдблада – Ульмана тесно связана с сильной субаддитивностью энтропии фон Неймана, что вы покажете в домашнем упражнении.

Монотонность χ обеспечивает еще одно свидетельство того, что χ характеризует количество информации, закодированной в квантовой системе. Декогерентизация, описываемая супероператором, может лишь сохранить или сократить эту величину информации, но не увеличить ее. Заметим, что в противоположность этому энтропия фон Неймана не монотонна. Супероператор может преобразовать начальное чистое состояние в смешанное, увеличивая $S(\boldsymbol{\rho})$. Однако другой супероператор преобразует любое смешанное состояние в «основное» $|0\rangle\langle 0|$ и, следовательно, уменьшает энтропию начального смешанного состояния до нуля. Было бы ошибкой интерпретировать это уменьшение S как «приобретение информации», так как наша способность отличить разные возможные приготовления полностью утрачена. Соответственно распад в основное состояние сокращает до нуля информацию Холево, отражая то, что мы потеряли возможность реконструировать начальное состояние.

Рассмотрим теперь сообщения из n букв, независимо извлекаемых из ансамбля $\mathcal{E} = \{\boldsymbol{\rho}_x, p_x\}$; ансамбль всех таких входящих сообщений обозначается как $\mathcal{E}^{(n)}$. Пусть разработан код, который сжимает сообщения так, что они все занимают гильбертово пространство $\tilde{\mathcal{H}}^{(n)}$; ансамбль сжатых сообщений обозначается как $\tilde{\mathcal{E}}^{(n)}$. Тогда развертывание выполняется супероператором \$

$$\$: \tilde{\mathcal{E}}^{(n)} \rightarrow \mathcal{E}'^{(n)}, \tag{5.117}$$

чтобы получить ансамбль $\mathcal{E}'^{(n)}$ выходящих сообщений.

Теперь предположим, что эта схема кодирования имеет высокую точность воспроизведения. Чтобы свести к минимуму техническую сторону, не будем вдаваться в детали того, как следует охарактеризовать количественно точность воспроизведения $\mathcal{E}'^{(n)}$ относительно $\mathcal{E}^{(n)}$. Мы просто примем, что если $\mathcal{E}'^{(n)}$ имеет высокую точность воспроизведения, то для любого δ и при достаточно больших n

$$\frac{1}{n}\chi\bigl(\mathcal{E}^{(n)}\bigr) - \delta \leqslant \frac{1}{n}\chi\bigl(\mathcal{E}'^{(n)}\bigr) \leqslant \frac{1}{n}\chi\bigl(\mathcal{E}^{(n)}\bigr) + \delta; \tag{5.118}$$

отнесенная к одной букве информации Холево выходящего и входящего сообщений приближаются друг к другу. Поскольку входящие сообщения являются произведениями состояний, то из аддитивности $S(\rho)$ следует, что

$$\chi\bigl(\mathcal{E}^{(n)}\bigr) = n\chi(\mathcal{E}), \tag{5.119}$$

а из монотонности Линдблада – Ульмана мы знаем, что

$$\chi\bigl(\mathcal{E}'^{(n)}\bigr) \leqslant \chi\bigl(\tilde{\mathcal{E}}^{(n)}\bigr). \tag{5.120}$$

Комбинируя уравнения (5.118)–(5.120), находим, что

$$\frac{1}{n}\chi\bigl(\tilde{\mathcal{E}}^{(n)}\bigr) \geqslant \chi(\mathcal{E}) - \delta. \tag{5.121}$$

Наконец, $\chi\bigl(\tilde{\mathcal{E}}^{(n)}\bigr)$ ограничена сверху величиной $S\bigl(\tilde{\rho}^{(n)}\bigr)$, которая, в свою очередь, ограничена сверху числом $\log\dim\tilde{\mathcal{H}}^{(n)}$. Так как δ можно выбрать сколь угодно малой, мы приходим к выводу, что асимптотически при $n \to \infty$

$$\frac{1}{n}\log\dim\tilde{\mathcal{H}}^{(n)} \geqslant \chi(\mathcal{E}); \tag{5.122}$$

хорошо воспроизводимое сжатие, до менее чем $\chi(\mathcal{E})$ кубитов на одну букву, невозможно.

Нередко возникает соблазн предположить, что сжатие до $\chi(\mathcal{E})$ кубитов на одну букву сообщения асимптотически достижимо. С середины января 1998 г. это предположение все еще ждет своего доказательства или опровержения.

5.4. Доступная информация

Тесная аналогия между информацией Холево $\chi(\mathcal{E})$ и классической взаимной информацией $I(X;Y)$, а также монотонность χ наводят на мысль,

что χ связана с количеством *классической* информации, которая может храниться в квантовой системе и извлекаться из нее. В этом разделе мы дадим точную формулировку этой связи.

Предыдущий раздел был посвящен количественному определению объема *квантовой* информации — измеряемой в кубитах — в сообщениях, построенных из алфавита квантовых состояний. Теперь же мы обратимся к совсем другому вопросу. Мы хотим количественно определить объем *классической* информации — измеряемой в битах — которую можно извлечь из таких сообщений, в частности, в случае, когда алфавит включает взаимно неортогональные буквы.

Но почему мы должны быть столь неразумны, чтобы хранить классическую информацию в неортогональных квантовых состояниях, которые нельзя идеально различить? Несомненно, следует избегать такого способа хранения информации, так как это ведет к деградации классического сигнала. Но, возможно, мы не можем обойтись без него. Допустим, например, я инженер связи и интересуюсь существенными физическими ограничениями классической емкости широкополосного оптического волокна. Чтобы получить наилучшую пропускную способность классической информации на единицу мощности, нам, очевидно, следует выбрать кодирование информации в отдельных фотонах, а чтобы добиться высокого темпа, мы должны увеличивать количество передаваемых за одну секунду фотонов. Но если мы сжимаем фотонные волновые пакеты достаточно тесно друг с другом, они начнут перекрываться и мы не сможем их идеально различать. Как максимизировать передаваемую в этом случае классическую информацию? Другой важный пример: допустим, что я — физик-экспериментатор и хочу использовать тонкую квантовую систему, чтобы сконструировать очень чувствительный прибор, измеряющий действие классической силы на систему. Мы можем моделировать силу как свободный параметр x в гамильтониане системы $\mathbf{H}(x)$. В зависимости от значения x состояние системы будет эволюционировать к различным возможным конечным (неортогональным) состояниям $\boldsymbol{\rho}_x$. Как много информации относительно x может получить наш прибор?

Несмотря на то, что с точки зрения физики эта проблема сильно отличается от сжимаемости квантовой информации, математически они связаны между собой. Мы обнаружим, что центральную роль в нашем обсуждении играют энтропия фон Неймана и ее обобщение, информация Холево.

Предположим, например, что Алиса готовит чистое квантовое состояние, извлекая его из ансамбля $\mathcal{E} = \{|\varphi_x\rangle, p_x\}$. Бобу известен ансамбль, но не конкретное выбранное Алисой состояние. Он хочет получить максимально возможную информацию относительно x.

Боб собирает информацию, выполняя обобщенное измерение, ПОЗМ $\{\mathbf{F}_y\}$. Если Алиса приготовила x, то Боб получит результат измерения y с условной вероятностью

$$p(y|x) = \langle\varphi_x|\mathbf{F}_y|\varphi_x\rangle. \tag{5.123}$$

Эти условные вероятности вместе с ансамблем X определяют количество в среднем получаемой Бобом информации, взаимную информацию $I(X;Y)$ приготовления и результата измерения.

Боб свободен в выборе своего измерения. «Наилучшее» возможное измерение, максимизирующее получение информации, называется *оптимальным измерением*, определяемым ансамблем. Максимальное получение информации равно

$$\mathrm{Acc}(\mathcal{E}) = \max_{\{\mathbf{F}_y\}} I(X;Y), \tag{5.124}$$

где max определяется по всем возможным ПОЗМ-ам. Эта величина называется *доступной информацией* ансамбля $\mathcal{E}$.

Конечно, если состояния $|\varphi_x\rangle$ взаимно ортогональны, то они идеально различимы. Условная вероятность результата ортогонального измерения

$$\mathbf{E}_y = |\varphi_y\rangle\langle\varphi_y| \tag{5.125}$$

равна

$$p(y|x) = \delta_{y,x}, \tag{5.126}$$

так что $H(X|Y) = 0$, а $I(X;Y) = H(X)$. Это измерение, очевидно, оптимально — приготовление полностью определено — так что для ансамбля взаимно ортогональных (чистых или смешанных) состояний

$$\mathrm{Acc}(\mathcal{E}) = H(X). \tag{5.127}$$

Однако проблема становится гораздо интереснее, когда сигнальными состояниями являются неортогональные чистые состояния. Для этого случая не известно ни одного полезного общего выражения для $\mathrm{Acc}(\mathcal{E})$, но существует верхняя граница

$$\mathrm{Acc}(\mathcal{E}) \leqslant S(\boldsymbol{\rho}). \tag{5.128}$$

Мы видели, что эта граница достигается в случае ортогональных сигнальных состояний, когда $S(\boldsymbol{\rho}) = H(X)$. В общем случае из классической теории информации известно, что $I(X;Y) \leqslant H(X)$; но для неортогональных

состояний $S(\rho) < H(X)$, так что неравенство (5.128) определяет наилучшую границу. Тем не менее эта граница не является точной, во многих случаях $\mathrm{Acc}(\mathcal{E})$ строго меньше $S(\rho)$.

Более определенное соотношение между $\mathrm{Acc}(\mathcal{E})$ и $S(\rho)$ мы получим, если рассмотрим доступную информацию в расчете на одну букву в сообщении, содержащем n букв. Теперь Боб имеет большую свободу — он может решить выполнить коллективное измерение всех n букв и таким образом получить больше информации, чем если бы он ограничивался измерением только по одной букве за один раз. Более того, Алиса может решить приготовить скорее ансамбль частных, максимально различимых, сообщений (код), нежели произвольные сообщения, каждая буква которых извлечена из ансамбля $\mathcal{E}$.

Тогда мы увидим, что Алиса и Боб могут найти такой код, чтобы маргинальным (частным) ансамблем каждой буквы был $\mathcal{E}$, а отнесенная к одной букве доступная информация асимптотически стремилась к $S(\rho)$ при $n \to \infty$. В этом смысле $S(\rho)$ характеризует доступную информацию в ансамбле *чистых* квантовых состояний.

Более того, заменой энтропии фон Неймана на информацию Холево эти результаты обобщаются на ансамбли смешанных квантовых состояний. Доступная информация ансамбля смешанных состояний $\{\rho_x, p_x\}$ удовлетворяет неравенству

$$\mathrm{Acc}(\mathcal{E}) \leqslant \chi(\mathcal{E}), \tag{5.129}$$

результат, известный как *граница Холево*. Эта граница в общем случае не является точной (хотя она достигается для ансамблей взаимно ортогональных смешанных состояний). Однако если Алиса и Боб выбирают n-буквенный код, в котором частным ансамблем для каждой буквы является $\mathcal{E}$, а Боб выполняет коллективное оптимальное обобщенное измерение (ПОЗМ) всех n букв, тогда максимальной достижимой информацией на одну букву является $\chi(\mathcal{E})$, если потребовать, чтобы все кодовые слова представляли собой *произведения* состояний. В этом смысле $\chi(\mathcal{E})$ характеризует доступную информацию в ансамбле *смешанных* квантовых состояний.

Алфавит из смешанных квантовых состояний может возникнуть, если Алиса попытается послать Бобу чистые квантовые состояния через квантовый канал с шумом. Вследствие декогерентизации в канале связи, Боб получает смешанные состояния, которые он должен декодировать. В этом случае $\chi(\mathcal{E})$ характеризует максимальное количество классической информации, которое может быть передано Бобу через квантовый канал с шумом.

Например, Алиса может послать Бобу n фотонов в определенных состояниях поляризации. Если предположить, что шум действует на каждый

фотон независимо и что Алиса посылает фотоны в незапутанных состояниях, тогда $\chi(\mathcal{E})$ – максимальное количество информации, которое может быть передано Бобу с каждым фотоном. Поскольку

$$\chi(\mathcal{E}) \leqslant S(\boldsymbol{\rho}) \leqslant 1, \tag{5.130}$$

отсюда, в частности, следует, что отдельный (незапутанный) фотон может переносить, самое большее, один бит классической информации.

5.4.1. Граница Холево

Граница Холево для доступной информации не относится к разряду очевидных теорем, но подобно многим интересным результатам квантовой теории информации, она становится очевидной, коль скоро установлена сильная субаддитивность энтропии фон Неймана. Здесь мы предположим наличие свойства сильной субаддитивности и покажем, что отсюда следует граница Холево.

Напомним исходные данные: Алиса готовит квантовое состояние, извлекаемое из ансамбля $\mathcal{E} = \{\boldsymbol{\rho}_x, p_x\}$, а затем Боб выполняет ПОЗМ $\{\mathbf{F}_y\}$. Совместным распределением вероятностей, управляющим приготовлением Алисы x и результатом Боба y является

$$p(x, y) = p_x \operatorname{tr}\left(\mathbf{F}_y \boldsymbol{\rho}_x\right). \tag{5.131}$$

Мы хотим показать, что

$$I(X;Y) \leqslant \chi(\mathcal{E}). \tag{5.132}$$

Поскольку сильная субаддитивность является свойством трех подсистем, нам нужно определить три системы, к которым оно будет применяться. Наша стратегия состоит в приготовлении входящей системы X, в которой хранится классическая запись того, какое приготовление было выбрано, и выходящей системы Y, классические корреляции которой с X управляются совместным распределением $p(x, y)$. Тогда, применяя свойство сильной субаддитивности к X, Y и нашей квантовой системе Q, мы сможем связать $I(X;Y)$ с $\chi(\mathcal{E})$.

Допустим, что начальным состоянием системы XQY является

$$\boldsymbol{\rho}_{XQY} = \sum_x p_x |x\rangle\langle x| \otimes \boldsymbol{\rho}_x \otimes |0\rangle\langle 0|, \tag{5.133}$$

где векторы $|x\rangle$ - взаимно ортогональные чистые состояния входящей системы X, а $|0\rangle$ – частное чистое состояние выходящей системы Y. Вычис-

ляя частичные следы, мы видим, что

$$\rho_X = \sum_x p_x |x\rangle\langle x| \rightarrow S(\rho_X) = H(X),$$
$$\rho_Q = \sum_x p_x \rho_x \equiv \rho \rightarrow S(\rho_{QY}) = S(\rho_Q) = S(\rho), \qquad (5.134)$$

а так как векторы $|x\rangle$ взаимно ортогональны, мы также имеем

$$S(\rho_{XQY}) = S(\rho_{XQ}) = -\sum_x \mathrm{tr}\left(p_x \rho_x \log p_x \rho_x\right) =$$
$$= H(X) + \sum_x p_x S(\rho_x). \qquad (5.135)$$

Теперь выполним унитарное преобразование, которое «отпечатывает» результат измерения Боба на выходящей системе Y. Предположим пока, что Боб выполняет ортогональное измерение $\{\mathbf{E}_y\}$, где

$$\mathbf{E}_y \mathbf{E}_{y'} = \delta_{y,y'} \mathbf{E}_y \qquad (5.136)$$

(вскоре мы кратко рассмотрим более общие ПОЗМ-ы). Наше унитарное преобразование $\mathbf{U}_{QY}$ действует на QY согласно

$$\mathbf{U}_{QY} : |\varphi\rangle_Q \otimes |0\rangle_Y = \sum_y \mathbf{E}_y |\varphi\rangle_Q \otimes |y\rangle_Y \qquad (5.137)$$

(где векторы $|y\rangle_Y$ взаимно ортогональны) и, следовательно, преобразует ρ_{XQY} как

$$\mathbf{U}_{QY} : \rho_{XQY} \rightarrow \rho'_{XQY} = \sum_{x,y,y'} p_x |x\rangle\langle x| \otimes \mathbf{E}_y \rho_x \mathbf{E}_{y'} \otimes |y\rangle\langle y'|. \qquad (5.138)$$

Поскольку энтропия фон Неймана инвариантна относительно унитарного изменения базиса, то

$$S(\rho'_{XQY}) = S(\rho_{XQY}) = H(X) + \sum_x p_x S(\rho_x),$$
$$S(\rho'_{QY}) = S(\rho_{QY}) = S(\rho), \qquad (5.139)$$

а вычисляя частичный след уравнения (5.138) и используя (5.136), мы находим

$$\boldsymbol{\rho}'_{XY} = \sum_{x,y} p_x \operatorname{tr}\left(\mathbf{E}_y \boldsymbol{\rho}_x\right) |x\rangle\langle x| \otimes |y\rangle\langle y| = \\ = \sum_{x,y} p(x,y) |x,y\rangle\langle x,y| \;\rightarrow\; S(\boldsymbol{\rho}'_{XY}) = H(X,Y). \tag{5.140}$$

Отсюда, очевидно, следует, что

$$\boldsymbol{\rho}'_Y = \sum_y p(y) |y\rangle\langle y| \;\rightarrow\; S(\boldsymbol{\rho}'_Y) = H(Y). \tag{5.141}$$

Применим теперь свойство сильной субаддитивности в форме

$$S(\boldsymbol{\rho}'_{XQY}) + S(\boldsymbol{\rho}'_Y) \leqslant S(\boldsymbol{\rho}'_{XY}) + S(\boldsymbol{\rho}'_{QY}), \tag{5.142}$$

которая принимает вид

$$H(X) + \sum_x p_x S(\boldsymbol{\rho}_x) + H(Y) \leqslant H(X,Y) + S(\boldsymbol{\rho}) \tag{5.143}$$

или

$$I(X;Y) = H(X) + H(Y) - H(X,Y) \leqslant S(\boldsymbol{\rho}) - \sum_x p_x S(\boldsymbol{\rho}_x) = \chi(\mathcal{E}). \tag{5.144}$$

Это и есть граница Холево.

Одним из способов рассмотрения более общих ПОЗМ является расширение системы путем присоединения к ней еще одной подсистемы Z. Тогда мы конструируем унитарное преобразование $\mathbf{U}_{QYZ}$, действующее как

$$\mathbf{U}_{QYZ} : |\varphi\rangle_Q \otimes |0\rangle_Y \otimes |0\rangle_Z = \sum_y \sqrt{\mathbf{F}_y} |\varphi\rangle_Q \otimes |y\rangle_Y \otimes |y\rangle_Z, \tag{5.145}$$

так что

$$\boldsymbol{\rho}'_{XQYZ} = \sum_{x,y,y'} p_x |x\rangle\langle x| \otimes \sqrt{\mathbf{F}_y}\boldsymbol{\rho}_x\sqrt{\mathbf{F}_{y'}} \otimes |y\rangle\langle y'| \otimes |y\rangle\langle y'|. \tag{5.146}$$

Тогда вычисление частичного следа по Z дает

$$\boldsymbol{\rho}'_{XQY} = \sum_{x,y} p_x |x\rangle\langle x| \otimes \sqrt{\mathbf{F}_y}\boldsymbol{\rho}_x\sqrt{\mathbf{F}_y} \otimes |y\rangle\langle y| \tag{5.147}$$

и

$$\rho'_{XY} = \sum_{x,y} p_x \operatorname{tr}\left(\mathbf{F}_y \rho_x\right) |x\rangle\langle x| \otimes |y\rangle\langle y| =$$
$$= \sum_{x,y} p(x,y) |x,y\rangle\langle x,y| \to S(\rho'_{XY}) = H(X,Y). \qquad (5.148)$$

Оставшаяся часть доказательства проводится так же, как и выше.

5.4.2. Улучшение различимости: метод Переса — Вутерса

Чтобы лучше познакомиться с концепцией доступной информации, рассмотрим однокубитовый пример. Алиса готовит одно из трех возможных чистых состояний:

$$|\varphi_1\rangle = |\uparrow_{\hat{n}_1}\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix},$$
$$|\varphi_2\rangle = |\uparrow_{\hat{n}_2}\rangle = \begin{pmatrix} -\frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{pmatrix}, \qquad (5.149)$$
$$|\varphi_3\rangle = |\uparrow_{\hat{n}_3}\rangle = \begin{pmatrix} -\frac{1}{2} \\ -\frac{\sqrt{3}}{2} \end{pmatrix};$$

объект со спином-$1/2$ ориентирован в одном из трех направлений, симметрично распределенных в xz-плоскости. Каждое состояние *a priori* имеет вероятность $1/3$. Очевидно, что «сигнальные состояния» Алисы не ортогональны:

$$\langle\varphi_1|\varphi_2\rangle = \langle\varphi_1|\varphi_3\rangle = \langle\varphi_2|\varphi_3\rangle = -\frac{1}{2}. \qquad (5.150)$$

Задачей Боба является: выполняя подходящее измерение, как можно больше узнать о том, что приготовлено Алисой. Матрицей плотности ансамбля Алисы является

$$\rho = \frac{1}{3}\left(|\varphi_1\rangle\langle\varphi_1| + |\varphi_2\rangle\langle\varphi_2| + |\varphi_3\rangle\langle\varphi_3|\right) = \frac{1}{2}\mathbf{1}, \qquad (5.151)$$

энтропия которой $S(\rho) = 1$. Следовательно, граница Холево говорит нам, что взаимная информация приготовления Алисы и результата измерения Боба не может превышать одного бита.

Хотя фактически доступная информация существенно меньше допускаемого границей Холево одного бита. В этом случае ансамбль Алисы достаточно симметричен, поэтому нетрудно угадать оптимальное измерение. Боб может выбрать ПОЗМ с тремя результатами, где

$$\mathbf{F}_a = \frac{2}{3}\bigl(\mathbf{1} - |\varphi_a\rangle\langle\varphi_a|\bigr), \qquad a = 1, 2, 3; \tag{5.152}$$

мы видим, что

$$p(a|b) = \langle\varphi_b|\mathbf{F}_a|\varphi_b\rangle = \begin{cases} 0, & a = b, \\ \frac{1}{2}, & a \neq b. \end{cases} \tag{5.153}$$

Следовательно, результат измерения a *исключает* возможность того, что Алиса приготовила a, но оставляет *a posteriori* равными вероятности ($p = 1/2$) двух других состояний. Полученная Бобом информация равна

$$I = H(X) - H(X|Y) = \log_2 3 - 1 = 0{,}58496. \tag{5.154}$$

Чтобы показать, что это измерение действительно оптимально, мы можем сослаться на вариант теоремы Дэвиса, которая гарантирует, что оптимальная ПОЗМ может быть выбрана с тремя $\mathbf{F}_a$, образующими, как и три состояния входящего ансамбля, семейство симметрии третьего порядка. Этот результат серьезно ограничивает возможные ПОЗМ, так что можно проверить с помощью явных вычислений, что (5.152) оптимальна. Таким образом, мы нашли, что доступная информация в ансамбле $\mathcal{E} = \{|\varphi_a\rangle, p_a = 1/3\}$ равна

$$\mathrm{Acc}(\mathcal{E}) = \log_2 \frac{3}{2} = 0{,}58496\ldots. \tag{5.155}$$

Граница Холево не достигается.

Допустим теперь, что у Алисы достаточно много денег и она может позволить себе послать Бобу два кубита, каждый из которых снова извлечен из ансамбля $\mathcal{E}$. Ее естественным решением будет приготовить для этого одно из *девяти* состояний

$$|\varphi_a\rangle|\varphi_b\rangle, \qquad a, b = 1, 2, 3, \tag{5.156}$$

с вероятностью $p_{ab} = 1/9$ каждое. Тогда наилучшая стратегия Боба, дающая, как и раньше, взаимную информацию 0,58496 битов на один кубит, состоит в выполнении ПОЗМ (5.152) на каждом из двух кубитов.

Но Алиса и Боб намерены поступить лучше. После обсуждения проблемы с А. Пересом и В. Вутерсом они выбирают другую стратегию. Алиса приготовит одно из *трех* двухкубитовых состояний

$$|\Phi_a\rangle = |\varphi_a\rangle|\varphi_a\rangle, \qquad a = 1, 2, 3, \tag{5.157}$$

каждое из которых появляется с априорной вероятностью $p_a = 1/3$. Рассматриваемый как один кубит, выбор Алисы управляется ансамблем $\mathcal{E}$, но теперь между ее двумя кубитами имеется (классическая) корреляция – оба они приготовлены одним способом.

Три вектора $|\Phi_a\rangle$ линейно независимы и, следовательно, образуют линейную оболочку трехмерного подпространства четырехмерного гильбертова пространства двух кубитов. В домашнем упражнении вы покажете, что матрица плотности

$$\boldsymbol{\rho} = \frac{1}{3}\sum_{a=1}^{3} |\Phi_a\rangle\langle\Phi_a| \tag{5.158}$$

имеет ненулевые собственные значения $1/2$, $1/4$ и $1/4$, так что

$$S(\boldsymbol{\rho}) = -\frac{1}{2}\log\frac{1}{2} - 2\left(\frac{1}{4}\log\frac{1}{4}\right) = \frac{3}{2}. \tag{5.159}$$

Граница Холево требует, чтобы доступная информация на *один кубит* была меньше, чем $3/4$ бита. По крайней мере это согласуется с тем, что можно превзойти ее значение 0,58496 на один кубит, достигнутое в методе девяти состояний.

На первый взгляд, может показаться, что Алиса не в состоянии передать такое количество классической информации Бобу, если она решает послать одно из всего лишь трех, вместо девяти, возможных состояний. Однако после некоторых размышлений этот вывод становится не очевидным. Действительно, Алиса имеет меньший выбор сигналов, но эти сигналы *более различимы*; вместо (5.150) мы имеем

$$\langle\Phi_a|\Phi_b\rangle = \frac{1}{4}, \qquad a \neq b. \tag{5.160}$$

Бобу следует использовать эту улучшенную различимость при выборе своего измерения. В частности, он найдет более выгодным выполнить *коллективное* измерение двух кубитов вместо измерения их по одному.

Теперь уже не очевидно, каким будет оптимальное измерение Боба. Но он может привлечь общую процедуру, которая, хотя и не обязательно оптимальна, но по крайней мере обычно достаточно хороша. Назовем

построенную с помощью этой процедуры ПОЗМ «достаточно хорошим измерением» (или ДХИ).

Рассмотрим некоторый набор векторов $|\tilde{\Phi}_a\rangle$, которые не предполагаются ортогональными или нормированными. Мы хотим придумать ПОЗМ, которая может достаточно хорошо различать эти векторы. Прежде всего, построим

$$\mathbf{G} = \sum_a |\tilde{\Phi}_a\rangle\langle\tilde{\Phi}_a|. \tag{5.161}$$

Это положительный оператор в подпространстве, натянутом на векторы $|\tilde{\Phi}_a\rangle$. Следовательно, в этом подпространстве он имеет обратный оператор $\mathbf{G}^{-1}$, а обратный оператор имеет положительный квадратный корень $\mathbf{G}^{-1/2}$. Теперь мы определяем

$$\mathbf{F}_a = \mathbf{G}^{-1/2}|\tilde{\Phi}_a\rangle\langle\tilde{\Phi}_a|\mathbf{G}^{-1/2} \tag{5.162}$$

и видим, что в линейной оболочке векторов $|\tilde{\Phi}_a\rangle$

$$\sum_a \mathbf{F}_a = \mathbf{G}^{-1/2}\left(\sum_a |\tilde{\Phi}_a\rangle\langle\tilde{\Phi}_a|\right)\mathbf{G}^{-1/2} = \\ = \mathbf{G}^{-1/2}\mathbf{G}\mathbf{G}^{-1/2} = \mathbf{1}. \tag{5.163}$$

Если необходимо, мы можем присоединить к этим $\mathbf{F}_a$ еще один положительный оператор, проектор $\mathbf{F}_0$ на ортогональное дополнение рассматриваемого подпространства и таким образом построить ПОЗМ. Она представляет собой ДХИ, связанное с данным набором векторов $|\tilde{\Phi}_a\rangle$.

В частном случае, когда векторы $|\tilde{\Phi}_a\rangle$ ортогональны

$$|\tilde{\Phi}_a\rangle = \sqrt{\lambda_a}|\Phi_a\rangle \tag{5.164}$$

(где $|\Phi_a\rangle$ ортонормированы), мы имеем

$$\mathbf{F}_a = \sum_{a,b,c}\left(|\Phi_b\rangle\lambda_b^{-1/2}\langle\Phi_b|\right)\left(\lambda_a|\Phi_a\rangle\langle\Phi_a|\right)\left(|\Phi_c\rangle\lambda_c^{-1/2}\langle\Phi_c|\right) = \\ = |\Phi_a\rangle\langle\Phi_a|, \tag{5.165}$$

то есть идеально различающее векторы $|\Phi_a\rangle$ ортогональное и, следовательно, оптимальное измерение. Если векторы $|\Phi_a\rangle$ линейно независимы, но

не ортогональны, то ДХИ снова является ортогональным измерением (поскольку n одномерных операторов в n-мерном пространстве могут образовать ПОЗМ, если только они взаимно ортогональны), но в этом случае измерение может оказаться не оптимальным.

В домашней работе вы построите ДХИ для векторов $|\Phi_a\rangle$ из (5.157) и покажете, что

$$p(a|a) = \langle\Phi_a|\mathbf{F}_a|\Phi_a\rangle = \frac{1}{3}\left(1+\frac{1}{\sqrt{2}}\right)^2 = 0{,}971405,$$

$$p(b|a) = \langle\Phi_a|\mathbf{F}_b|\Phi_a\rangle = \frac{1}{6}\left(1-\frac{1}{\sqrt{2}}\right)^2 = 0{,}0142977 \qquad (5.166)$$

(при $b \neq a$). Отсюда следует, что условная энтропия входа

$$H(X|Y) = 0{,}215893, \qquad (5.167)$$

а поскольку $H(X) = \log_2 3 = 1{,}58496$, то приобретаемая информация

$$I = H(X) - H(X|Y) = 1{,}36907, \qquad (5.168)$$

взаимная информация равна 0,684535 битов на один кубит. Таким образом, улучшенная различимость сигналов Алисы действительно оправдала себя — мы превзошли 0,58496 битов, которые можно было извлечь из одного кубита. Мы все еще не достигли границы Холево ($I < 1{,}5$ в этом случае), хотя и подошли к ней несколько ближе, чем раньше.

Этот пример, впервые описанный Пересом и Вутерсом, преподносит несколько полезных уроков. Во-первых, Алиса в состоянии послать Бобу большее количество информации, «сократив» свой набор кодовых слов. Ей лучше сделать выбор из меньшего количества более различимых сигналов, чем из большего количества менее различимых сигналов. Алфавит из трех букв кодирует больше, чем алфавит из девяти букв.

Во-вторых, Боб способен считать больше информации, если он выполняет коллективное измерение, вместо измерения каждого кубита по отдельности. Его оптимальное ортогональное измерение проецирует сигнал Алисы на базис *запутанных* состояний.

Описанное здесь ДХИ «оптимально» в том смысле, что оно дает наибольшее приобретение информации по сравнению с любым *известным* измерением. Скорее всего это действительно максимальное значение I, которое может быть достигнуто при любом измерении, но я не доказал этого.

5.4.3. Достижимость границы Холево: чистые состояния

Усвоив эти уроки, мы можем показать, что для заданного ансамбля чистых состояний можно построить n-буквенные кодовые слова, которые асимптотически достигают доступной информации $S(\rho)$ на одну букву.

Мы должны выбрать код, ансамбль кодовых слов, которые может приготовить Алиса, и «декодирующую наблюдаемую» — ПОЗМ, которую будет использовать Боб, пытаясь различить кодовые слова. Наша задача состоит в том, чтобы показать, что Алиса может выбрать $2^{n(S-\delta)}$ таких кодовых слов, что с пренебрежимо малой вероятностью ошибки при $n \to \infty$ Боб может определить, какое из них было послано. Мы не будем вникать во все детали доказательства, а удовольствуемся пониманием того, почему этот результат весьма правдоподобен.

Конечно, главной идеей является привлечение случайного кодирования. Алиса выбирает произведение сигнальных состояний

$$|\varphi_{x_1}\rangle|\varphi_{x_2}\rangle\cdots|\varphi_{x_n}\rangle, \tag{5.169}$$

случайным образом извлекая каждую букву из ансамбля $\mathcal{E} = \{|\varphi_x\rangle, p_x\}$. Как мы видели, для типичного кода каждое типичное кодовое слово имеет большое перекрытие с типичным подпространством $\Lambda^{(n)}$, размерность которого $\dim\Lambda^{(n)} > 2^{n[S(\rho)-\delta]}$. Более того, для типичного кода управляющий каждой буквой частный ансамбль близок к $\mathcal{E}$.

Поскольку при больших n типичное подпространство очень велико, Алиса может выбрать много кодовых слов, тем не менее оставаясь уверенной в том, что характерное перекрытие двух типичных кодовых слов очень мало. С эвристической точки зрения типичные кодовые слова случайным образом распределены в типичном подпространстве, а в среднем два случайных единичных вектора в пространстве размерности D имеют перекрытие $1/D$. Следовательно, если $|u\rangle$ и $|w\rangle$ — два кодовых слова, то

$$\langle|\langle u|w\rangle|^2\rangle_\Lambda < 2^{-n(S-\delta)}. \tag{5.170}$$

Здесь $\langle\cdot\rangle_\Lambda$ обозначает среднее по случайным типичным кодовым словам.

Вы можете убедиться в том, что типичные кодовые слова действительно однородно распределены в типичном подпространстве, как видно из дальнейшего: усредненное по ансамблю перекрытие случайных кодовых слов $|\varphi_{x_1}\rangle\ldots|\varphi_{x_n}\rangle$ и $|\varphi_{y_1}\rangle\ldots|\varphi_{y_n}\rangle$ равно

$$\begin{aligned} &= \sum p_{x_1}\cdots p_{x_n}p_{y_1}\cdots p_{y_n}\left(|\langle\varphi_{x_1}|\varphi_{y_1}\rangle|^2\cdots|\langle\varphi_{x_n}|\varphi_{y_n}\rangle|^2\right) = \\ &= \operatorname{tr}\left(\rho\otimes\cdots\otimes\rho\right)^2. \end{aligned} \tag{5.171}$$

Теперь предположим, что мы ограничили след типичным подпространством $\Lambda^{(n)}$; это пространство имеет размерность $\dim\Lambda^{(n)} < 2^{n(S+\delta)}$, а собственные значения сужения оператора $\boldsymbol{\rho}^{(n)} = \boldsymbol{\rho} \otimes \cdots \otimes \boldsymbol{\rho}$ в подпространство $\Lambda^{(n)}$ удовлетворяют неравенству $\lambda < 2^{-n(S-\delta)}$. Следовательно:

$$\langle |\langle u|w\rangle|^2\rangle_\Lambda = \mathrm{tr}_\Lambda \left[\boldsymbol{\rho}^{(n)}\right]^2 < 2^{n(S+\delta)}\left[2^{-n(S-\delta)}\right]^2 = 2^{-n(S-3\delta)}, \qquad (5.172)$$

где tr_Λ обозначает след по типичному подпространству.

Теперь предположим, что выбрано $2^{n(S-\delta)}$ случайных кодовых слов $\{|u_i\rangle\}$. Тогда если $|u_j\rangle$ - произвольное фиксированное кодовое слово, то

$$\sum_{i\neq j}\langle |\langle u_i|u_j\rangle|^2\rangle < 2^{n(S-\delta)}2^{-n(S-\delta')} = 2^{-n(\delta-\delta')} + \varepsilon; \qquad (5.173)$$

здесь суммирование ведется по всем кодовым словам, а усреднение больше не ограничивается типичными кодовыми словами $\cdots\ \varepsilon$ в правой части возникает от атипичного случая. Теперь при любом фиксированном δ и при достаточно большом n мы можем выбрать δ' и ε настолько малыми, насколько нам это нужно; таким образом, при усреднении по кодам и кодовым словам внутри кода последние становятся хорошо различимыми при $n \to \infty$.

Теперь призовем на помощь несколько стандартных «шеннонизмов»: так как уравнение (5.173) справедливо в среднем по кодам, то оно справедливо и для некоторого частного кода. [Более того, поскольку почти все коды обладают тем свойством, что частный (маргинальный) ансамбль каждой буквы близок к $\mathcal{E}$, то существует код с таким свойством, удовлетворяющий (5.173).] Теперь уравнение (5.173) справедливо, если мы усредняем по частному кодовому слову $|u_j\rangle$. Но, отбрасывая не больше половины кодовых слов, можно быть уверенными в том, что любое *и* каждое кодовое слово хорошо отличимо от всех остальных.

Итак, Алиса может выбрать $2^{n(S-\delta)}$ хорошо различимых кодовых слов, которые становятся взаимно ортогональными в пределе $n \to \infty$. При конечном n Боб может выполнить ДХИ, которое стремится к оптимальному ортогональному измерению при $n \to \infty$. Следовательно, отнесенная к одной букве доступная информация

$$\frac{1}{n}\mathrm{Acc}(\tilde{\mathcal{E}}^{(n)}) = S(\boldsymbol{\rho}) - \delta \qquad (5.174)$$

достижима, где $\tilde{\mathcal{E}}^{(n)}$ обозначает ансамбль n-буквенных кодовых слов Алисы.

Конечно, при любом конечном n ПОЗМ Боба будет представлять собой сложное коллективное измерение, выполняемое на всех n буквах. Чтобы дать настоящее доказательство достижимости, необходимо тщательно проанализировать ПОЗМ и пределы вероятности ее ошибки. Это было выполнено Хаусленденом и др[1]. Приведенное здесь доказательство на пальцах, по крайней мере, показывает, почему их вывод не удивителен.

Из границы Холево и субаддитивности энтропии следует также, что отнесенная к одной букве доступная информация асимптотически не может превзойти $S(\boldsymbol{\rho})$. Граница Холево утверждает, что

$$\mathrm{Acc}(\tilde{\mathcal{E}}^{(n)}) \leqslant S(\tilde{\boldsymbol{\rho}}^{(n)}), \tag{5.175}$$

где $\tilde{\boldsymbol{\rho}}^{(n)}$ обозначает матрицу плотности кодовых слов, а субаддитивность энтропии предполагает, что

$$S(\tilde{\boldsymbol{\rho}}^{(n)}) \leqslant \sum_{i=1}^{n} S(\tilde{\boldsymbol{\rho}}_i), \tag{5.176}$$

где $\tilde{\boldsymbol{\rho}}_i$ — приведенная матрица плотности i-ой буквы. А так как каждая $\tilde{\boldsymbol{\rho}}_i$ асимптотически стремится к $\boldsymbol{\rho}$, то

$$\lim_{n\to\infty} \frac{1}{n}\mathrm{Acc}(\tilde{\mathcal{E}}^{(n)}) \leqslant \lim_{n\to\infty} \frac{1}{n} S(\tilde{\boldsymbol{\rho}}^{(n)}) \leqslant S(\boldsymbol{\rho}). \tag{5.177}$$

Чтобы получить это ограничение, мы не делали никаких предположений относительно кода, за исключением того, что частный ансамбль каждой буквы асимптотически стремится к $\mathcal{E}$. В частности, это ограничение справедливо, даже если кодовые слова являются не сепарабельными, а запутанными состояниями. Таким образом, мы показали, что $S(\boldsymbol{\rho})$ является оптимальной доступной информацией на одну букву.

Можно определить разновидность емкости канала связи, связанной с конкретным алфавитом чистых квантовых состояний, «емкость для заданного алфавита». Предположим, что Алиса обеспечена источником квантовых состояний. Она может создать любое из состояний $|\varphi_x\rangle$, но выбор априорных вероятностей этих состояний зависит от нее. Емкость для заданного алфавита C_{f_a} представляет собой максимальную доступную информацию на одну букву, которой она может достичь при наилучшем возможном

[1] P. Hausladen, R. Jozsa, B. Schumacher, M. Westmoreland and W. K. Wooters. Classical information capacity of a quantum channel. *Phys. Rev.* A 54 (1996) 1869–1876. [См. также А. С. Холево. *Введение в квантовую теорию информации.* МЦНМО, М.: 2002. *Прим. ред.*]

распределении $\{p_x\}$. Мы нашли, что

$$C_{f_a} = \max_{\{p_x\}} S(\rho). \tag{5.178}$$

C_{f_a} представляет собой оптимальное количество классических битов, которое можно (асимптотически) закодировать в одной букве данного конкретного алфавита квантовых состояний из источника.

5.4.4. Достижимость границы Холево: смешанные состояния

Теперь мы хотели бы распространить предыдущие рассуждения на более общий случай. Будем рассматривать n-буквенные сообщения, в которых частным ансамблем для каждой буквы является ансамбль *смешанных* состояний

$$\mathcal{E} = \{\rho_x, p_x\}. \tag{5.179}$$

Мы хотим показать, что в расчете на одну букву (асимптотически при $n \to \infty$) можно переслать $\chi(\mathcal{E})$ битов классической информации. Вновь нашей задачей является: (1) конкретизировать код, которым могут пользоваться Алиса и Боб, ансамбль которого (по крайней мере асимптотически) буква за буквой создает ансамбль $\mathcal{E}$; (2) конкретизировать декодирующую наблюдаемую Боба, ПОЗМ, которую он будет использовать, пытаясь различить кодовые слова; (3) показать, что при $n \to \infty$ вероятность ошибки Боба стремится к нулю. Как и при обсуждении случая чистых состояний, я не буду здесь представлять полное доказательство (см. Холево[1], а также Шумахер и Вестморленд[2]). Вместо этого я предложу вашему вниманию аргументы (даже с большим, чем ранее, количеством объяснений на пальцах, если такое возможно), показывающие, что их вывод разумен.

Как обычно, мы будем демонстрировать достижимость с помощью метода случайного кодирования. Алиса выбирает кодовые слова из смешанных состояний, каждая буква которых извлекается из ансамбля $\mathcal{E}$. То есть кодовое слово

$$\rho_{x_1} \otimes \rho_{x_2} \otimes \cdots \otimes \rho_{x_n} \tag{5.180}$$

[1] A. S. Holevo. The Capacity of the Quantum Channel with General Signal States. *IEEE Trans. Inf. Theory*, **44** (1998) 269–273; quant-ph/9611023.

[2] B. Schumacher and M. D. Westmoreland. Sending Classical Information Via Noisy Quantum Channels. *Phys. Rev.* **A 56** (1997) 131–138. [На русском языке доказательство теоремы Холево–Шумахера–Вестморленда (ХШВ) можно найти в книге М. Нильсен, И. Чанг, *Квантовые вычисления и квантовая информация*, М.: Мир, 2006. – *Прим. ред.*]

выбирается с вероятностью $p_{x_1}p_{x_2}\cdots p_{x_n}$. Идея в том, что *каждое* типичное кодовое слово может рассматриваться как ансамбль чистых состояний, почти все носители которого находятся в определенном типичном подпространстве. Если перекрытия типичных подпространств различных кодовых слов малы, тогда Боб будет в состоянии выполнить ПОЗМ, которая с малой вероятностью ошибки идентифицирует характеристику типичного подпространства сообщения Алисы.

Какова размерность типичного подпространства типичного кодового слова? Если мы *усредняем* по кодовым словам, то средняя энтропия кодового слова равна

$$\langle S^{(n)}\rangle = \sum_{x_1,\ldots x_n} p_{x_1}p_{x_2}\cdots p_{x_n} S(\boldsymbol{\rho}_{x_1}\otimes\boldsymbol{\rho}_{x_2}\otimes\cdots\otimes\boldsymbol{\rho}_{x_n}). \tag{5.181}$$

Используя аддитивность энтропии произведения состояний и $\sum_x p_x = 1$, мы получаем

$$\langle S^{(n)}\rangle = n\sum_x p_x S(\boldsymbol{\rho}_x) \equiv n\langle S\rangle. \tag{5.182}$$

При больших n энтропия кодового слова с большой вероятностью близка к ее среднему значению, более того, велика вероятность того, что собственные значения $\boldsymbol{\rho}_{x_1}\otimes\cdots\otimes\boldsymbol{\rho}_{x_n}$ близки к $2^{-n\langle S\rangle}$. Другими словами, типичное кодовое слово $\boldsymbol{\rho}_{x_1}\otimes\cdots\otimes\boldsymbol{\rho}_{x_n}$ имеет носитель в типичном подпространстве размерности $2^{n\langle S\rangle}$.

Это утверждение является близким аналогом высказывания (ключевого в доказательстве теоремы Шеннона о кодировании для канала связи с шумом) о том, что если через классический канал связи с шумом послано типичное сообщение, то количество типичных сообщений, которые могут быть получены, равно $2^{nH(Y|X)}$.

Далее доказательство следует знакомым путем. Для каждого типичного сообщения $x_1x_2\ldots x_n$ Боб может построить «декодирующее подпространство» размерности $2^{n(\langle S\rangle+\delta)}$ с уверенностью, что почти все носители сообщения Алисы принадлежат этому подпространству. Его ПОЗМ будет предназначена для определения, в каком декодирующем подпространстве находится сообщение Алисы. Ошибки декодирования будут маловероятны, если малы перекрытия типичных декодирующих подпространств.

Несмотря на то, что на самом деле Боба интересует только оценка декодирующего подпространства (и, следовательно, $x_1x_2\ldots x_n$), предположим, что он выполняет полное ДХИ, определяемое всеми векторами, образующими линейную оболочку всех типичных подпространств кодовых

слов Алисы. (При больших n это ДХИ будет стремиться к ортогональному измерению, пока число кодовых слов не слишком велико.) Он получает конкретный результат, который, вероятно, находится в типичном подпространстве размерности $2^{nS(\rho)}$, определяемом источником $\rho \otimes \rho \otimes \cdots \otimes \rho$. Более того, этот результат, вероятно, находится в декодирующем подпространстве сообщения, которое Алиса на самом деле послала. Поскольку результаты измерения Боба однородно распределены в пространстве размерности 2^{nS}, а ансамбль чистых состояний, определяемый частным декодирующим подпространством, имеет размерность $2^{n((S)+\delta)}$, то среднее перекрытие вектора, определенного результатом Боба, с типичным декодирующим подпространством равно:

$$\frac{2^{n((S)+\delta)}}{2^{nS}} = 2^{-n(S-(S)-\delta)} = 2^{-n(\chi-\delta)}. \tag{5.183}$$

Если Алиса выбирает 2^{nR} кодовых слов, то средняя вероятность ошибки декодирования будет

$$2^{nR}2^{-n(\chi-\delta)} = 2^{-n(\chi-R-\delta)}. \tag{5.184}$$

Мы можем выбрать R любым, меньшим χ, тогда эта вероятность ошибки будет очень мала при $n \to \infty$.

Эти доводы показывают, что *усредненная по случайным кодам и кодовым словам* вероятность ошибки мала. Как обычно, мы выбираем конкретный код и отбрасываем некоторые кодовые слова, чтобы получить малую вероятность ошибки для каждого кодового слова. Более того, конкретный код может быть выбран типичным, так что частный ансамбль каждого кодового слова стремится к $\mathcal{E}$ при $n \to \infty$. Мы приходим к выводу, что отнесенная к одной букве доступная информация χ асимптотически достижима.

По своей структуре это доказательство близко к аналогичному доказательству соответствующей классической теоремы о кодировании. В частности, величина χ здесь играет такую же роль, как I в теореме Шеннона. В то время как 2^{-nI} является вероятностью того, что конкретная типичная последовательность лежит в определенной сфере декодирования, $2^{-n\chi}$ представляет собой перекрытие конкретного типичного состояния с определенным декодирующим подпространством.

5.4.5. Емкость канала связи

Комбинируя границу Холево с выводом о том, что достижимы χ битов на одну букву, можно получить выражение для *классической* емкости

квантового канала связи. (Но с предупреждением: мы уверены, что эту «емкость» нельзя превысить, если только мы отказываемся от использования запутанных кодовых слов.)

Алиса готовит n-буквенные сообщения и посылает их Бобу через квантовый канал связи с шумом, описываемый супероператором \$. Предположим, что упомянутый супероператор \$ действует на каждую букву независимо (квантовый канал *без памяти*). Боб выполняет ПОЗМ, которая оптимизирует получаемую им информацию относительно того, что приготовила Алиса.

Фактически окажется, что лучше всего Алиса готовит сообщения из чистых состояний (это следует из субаддитивности энтропии). Если конкретная буква приготовлена как чистое состояние $|\varphi_x\rangle$, то Боб получит

$$|\varphi_x\rangle\langle\varphi_x| \to \$(|\varphi_x\rangle\langle\varphi_x|) \equiv \boldsymbol{\rho}_x. \tag{5.185}$$

А если Алиса посылает чистое состояние $|\varphi_{x_1}\rangle\cdots|\varphi_{x_n}\rangle$, то Боб получит смешанное состояние $\boldsymbol{\rho}_{x_1}\otimes\cdots\otimes\boldsymbol{\rho}_{x_n}$. Таким образом, ансамбль кодовых слов Алисы определяет ансамбль смешанных состояний $\tilde{\mathcal{E}}^{(n)}$, получаемых Бобом. Следовательно, оптимальное количество получаемой Бобом информации по определению равно $\mathrm{Acc}(\tilde{\mathcal{E}}^{(n)})$, что удовлетворяет границе Холево:

$$\mathrm{Acc}(\tilde{\mathcal{E}}^{(n)}) \leqslant \chi(\tilde{\mathcal{E}}^{(n)}). \tag{5.186}$$

Теперь ансамблем Боба является

$$\{\boldsymbol{\rho}_{x_1}\otimes\cdots\otimes\boldsymbol{\rho}_{x_n},\ p(x_1,x_2,\ldots,x_n)\}, \tag{5.187}$$

где $p(x_1,x_2,\ldots,x_n)$ совершенно произвольное распределение вероятностей кодовых слов Алисы. Вычислим χ для этого ансамбля. Заметим, что

$$\begin{aligned}
&\sum_{x_1,\ldots,x_n} p(x_1,x_2,\ldots,x_n)S(\boldsymbol{\rho}_{x_1}\otimes\cdots\otimes\boldsymbol{\rho}_{x_n}) = \\
&= \sum_{x_1,\ldots,x_n} p(x_1,x_2,\ldots,x_n)\Big[S(\boldsymbol{\rho}_{x_1}) + S(\boldsymbol{\rho}_{x_2}) + \ldots + S(\boldsymbol{\rho}_{x_n})\Big] = \\
&= \sum_{x_1} p_1(x_1)S(\boldsymbol{\rho}_{x_1}) + \sum_{x_2} p_2(x_2)S(\boldsymbol{\rho}_{x_2}) + \ldots + \\
&\qquad + \sum_{x_n} p_n(x_n)S(\boldsymbol{\rho}_{x_n}).
\end{aligned} \tag{5.188}$$

где, например, $p_1(x_1) = \sum_{x_2,\ldots,x_n} p(x_1, x_2, \ldots, x_n)$ — частное распределение вероятностей для первой буквы. Более того, из субаддитивности энтропии мы имеем:

$$S(\tilde{\boldsymbol{\rho}}^{(n)}) \leqslant S(\tilde{\boldsymbol{\rho}}_1) + S(\tilde{\boldsymbol{\rho}}_2) + \ldots + S(\tilde{\boldsymbol{\rho}}_n), \tag{5.189}$$

где $\tilde{\boldsymbol{\rho}}_i$ — приведенная матрица плотности i-ой буквы. Комбинируя (5.188) и (5.189), мы находим, что

$$\chi(\tilde{\mathcal{E}}^{(n)}) \leqslant \chi(\tilde{\mathcal{E}}_1) + \chi(\tilde{\mathcal{E}}_2) + \ldots + \chi(\tilde{\mathcal{E}}_n), \tag{5.190}$$

где $\tilde{\mathcal{E}}_i$ — маргинальный ансамбль, управляющий i-ой буквой, полученной Бобом. Неравенство (5.190) применимо к любому ансамблю факторизуемых состояний.

Теперь для канала, описываемого супероператором $\$$, определим *емкость канала* по отношению к факторизуемым состояниям

$$C(\$) = \max_{\mathcal{E}} \chi(\$(\mathcal{E})). \tag{5.191}$$

Следовательно, для каждого слагаемого в (5.190) $\chi(\tilde{\mathcal{E}}_i) \leqslant C$ и мы получаем

$$\chi(\tilde{\mathcal{E}}^{(n)}) \leqslant nC, \tag{5.192}$$

где $\tilde{\mathcal{E}}^{(n)}$ — произвольный ансамбль факторизуемых состояний. В частности, из границы Холево мы приходим к заключению, что количество получаемой Бобом информации ограничено сверху величиной nC. Но мы видели, что для любого $\mathcal{E}$ можно асимптотически достичь $\chi(\$(\mathcal{E}))$ битов на одну букву сообщения при правильном выборе кода и декодирующей наблюдаемой. Следовательно, C представляет собой оптимальное количество битов на одну букву, которое может быть передано через канал с шумом с исчезающе малой вероятностью ошибки *при условии*, что сообщения, которые готовит Алиса, представляют собой факторизуемые состояния.

Мы оставили открытой возможность того, что емкость относительно факторизуемых состояний $C(\$)$ может быть превышена, если позволить Алисе готовить *запутанные* состояния из ее n букв. Неизвестно (на январь 1998 г.), существуют ли квантовые каналы, более высокая пропускная способность которых может быть достигнута при использовании запутанных сообщений. Это один из многих интересных открытых вопросов теории квантовой информации[1].

[1] Обзор некоторых результатов относительно пропускной способности квантового канала при использовании запутанных сообщений см. в книге А. С. Холево, *Введение в квантовую теорию информации*, МЦНМО, М., (2002). — *Прим. ред.*

5.5. Плотность запутывания

Прежде чем завершить наш обзор теории квантовой информации, обратимся к еще одной теме, в которой центральную роль играет энтропия фон Неймана: количественное определение запутывания.

Рассмотрим два бинарных чистых состояния. Одно из них — *максимально* запутанное состояние двух кубитов

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \tag{5.193}$$

Другое — *частично* запутанное состояние двух *кутритов*

$$|\Psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{2}|11\rangle + \frac{1}{2}|22\rangle. \tag{5.194}$$

Какое из них более запутано?

Непосредственно не видно, что ответ на этот вопрос имеет глубокий смысл. Почему можно найти однозначный способ упорядочения всего континуума бинарных состояний в соответствии со степенью их запутывания? Можем ли мы сравнивать пару кубитов с парой кутритов иным способом, нежели яблоко с апельсином?

Определяющим свойством запутывания является то, что оно не может быть создано локальными операциями. В частности, если Алиса и Боб делят бинарное чистое состояние, то они не могут увеличить его число Шмидта никакими локальными операциями — никаким унитарным преобразованием или ПОЗМ, выполняемыми Алисой или Бобом, даже если они обмениваются классическими сообщениями о своих действиях и результатах измерений. Таким образом, число, используемое для количественого определения запутывания, должно обладать тем свойством, что локальные операции его не увеличивают. Очевидным кандидатом является число Шмидта, но после некоторого размышления оно уже не кажется достаточно удовлетворительным. Рассмотрим состояние

$$|\Psi_\varepsilon\rangle = \sqrt{1-2|\varepsilon|^2}|00\rangle + \varepsilon|11\rangle + \varepsilon|22\rangle, \tag{5.195}$$

имеющее число Шмидта, равное трем при любом $|\varepsilon| > 0$. Можем ли мы на самом деле сказать, что $|\Psi_\varepsilon\rangle$ «более запутано», чем $|\phi^+\rangle$? В конце концов, запутывание может рассматриваться как ресурс — мы можем планировать использовать его, например, для телепортации. Кажется очевидным, что $|\Psi_\varepsilon\rangle$ (при $|\varepsilon| \ll 1$) менее ценный, чем $|\phi^+\rangle$, ресурс.

Тем не менее оказывается, что существует естественный и разумный способ количественного описания запутывания любого бинарного чистого состояния. Чтобы сравнить два состояния, выполним локальные операции, чтобы обменять их запутывание на тот «валютный эталон», который можно сравнивать непосредственно. Таким «валютным эталоном» является максимально запутанное состояние.

Точное утверждение о взаимозаменяемости (посредством локальных операций) различных форм запутывания неизбежно будет *асимптотическим*. То есть для того чтобы дать точное количественное описание запутывания конкретного бинарного чистого состояния $|\psi\rangle_{AB}$, представим, что мы хотим приготовить n идентичных копий этого состояния. В нашем распоряжении имеется большой запас максимально запутанных *пар Белла*, поделенных между Алисой и Бобом. Они должны использовать k пар Белла $\left(|\phi\rangle_{AB}\right)^k$ и с помощью локальных операций и классических средств связи приготовить n копий требуемого состояния $\left(|\psi\rangle_{AB}\right)^n$. Чему равно минимальное число $k_{\min}$ пар Белла, необходимое для решения этой задачи?

А теперь предположим, что n копий $|\psi\rangle_{AB}$ уже приготовлены. Алиса и Боб должны выполнить локальные операции, которые преобразуют запутывание $\left(|\psi_{AB}\rangle\right)^n$ назад к стандартной форме; то есть они должны извлечь k' пар Белла $\left(|\phi\rangle_{AB}\right)^{k'}$. Чему равно максимальное количество $k'_{\max}$ пар Белла, которые могут быть выделены (локальным образом) из $\left(|\psi\rangle_{AB}\right)^n$?

Поскольку невозможность порождения запутывания с помощью локальных операций является непушимым принципом, то несомненно, что

$$k'_{\max} \leqslant k_{\min}. \tag{5.196}$$

Однако можно показать, что

$$\lim_{n\to\infty} \frac{k_{\min}}{n} = \lim_{n\to\infty} \frac{k'_{\max}}{n} \equiv E(|\psi\rangle_{AB}). \tag{5.197}$$

В этом смысле локальное преобразование n копий бинарного чистого состояния $|\psi\rangle_{AB}$ в k' запутанных пар является асимптотически *обратимым* процессом. Так как n копий $|\psi\rangle_{AB}$ можно заменить k парами Белла и наоборот, то отсюда следует, что $\frac{k}{n}$ пар Белла однозначно характеризуют степень запутывания, переносимого состоянием $|\psi\rangle_{AB}$. Будем называть отношение k/n (в пределе $n \to \infty$) *запутыванием* E состояния $|\psi\rangle_{AB}$. Величина E измеряет, какие требуются затраты (в парах Белла), чтобы создать $|\psi\rangle_{AB}$,

а также значение $|\psi\rangle_{AB}$ как ресурса (то есть количество кубитов, которые можно телепортировать с помощью $|\psi\rangle_{AB}$).

Чему равно E для данного конкретного чистого состояния $|\psi\rangle_{AB}$? Можете ли вы угадать ответ? Это

$$E = S(\rho_A) = S(\rho_B); \tag{5.198}$$

запутывание является энтропией фон Неймана матрицы плотности Алисы ρ_A (или матрицы плотности Боба ρ_B). Это, очевидно, правильный ответ в том случае, когда $|\psi\rangle_{AB}$ является произведением k пар Белла. В этом случае ρ_A (или ρ_B) равна $\frac{1}{2}1$ для каждого имеющегося в распоряжении Алисы кубита

$$\rho_A = \frac{1}{2}1 \otimes \frac{1}{2}1 \otimes \cdots \otimes \frac{1}{2}1 \tag{5.199}$$

и

$$S(\rho_A) = kS\left(\frac{1}{2}1\right) = k. \tag{5.200}$$

Теперь нужно понять, почему $E = S(\rho_A)$ является правильным ответом для любого бинарного чистого состояния.

Прежде всего, мы хотим показать, что если Алиса и Боб делят $k = n[S(\rho_A) + \delta]$ пар Белла, то они могут (с помощью локальных операций) с высокой точностью воспроизведения приготовить $\left(|\psi\rangle_{AB}\right)^n$. Они могут решить эту задачу, комбинируя квантовую телепортацию со сжатием Шумахера. Во-первых, локальным образом манипулируя находящейся в ее распоряжении бинарной системой AC, Алиса конструирует состояние $|\psi\rangle_{AC}$ (n его копий). Таким образом, состояние системы C можно рассматривать как чистое состояние, извлеченное из ансамбля, описываемого матрицей плотности ρ_C, где $S(\rho_C) = S(\rho_A)$. Затем Алиса выполняет сжатие Шумахера над ее n копиями C, сохраняя хорошую точность воспроизведения, несмотря на то, что типичные состояния из $(\mathcal{H}_C)^n$ сжимаются в пространство $\tilde{\mathcal{H}}_C^{(n)}$ с

$$\dim \tilde{\mathcal{H}}_C^{(n)} = 2^{n[S(\rho_A)+\delta]}. \tag{5.201}$$

Теперь Алиса и Боб могут использовать $n[S(\rho_A) + \delta]$ поделенных между ними пар Белла, чтобы телепортировать сжатое состояние из пространства Алисы $(\tilde{\mathcal{H}}_C)^n$ в пространство Боба $(\tilde{\mathcal{H}}_B)^n$. Телепортация, которая в принципе имеет идеальную точность воспроизведения, требует только локальных операций и классических средств связи, если Алиса и Боб делят необходимое количество пар Белла. Наконец, Боб развертывает (декомпрессия

Шумахера) полученное им состояние; тогда Алиса и Боб делят $\left(|\psi\rangle_{AB}\right)^n$ (со сколь угодно высокой точностью воспроизведения при $n \to \infty$).

Предположим теперь, что Алиса и Боб приготовили состояние $\left(|\psi\rangle_{AB}\right)^n$. Так как $|\psi\rangle_{AB}$, вообще говоря, *частично* запутанное состояние, то поделенное между ними запутывание находится в разбавленном виде. Алиса и Боб хотят *концентрировать* поделенное между ними запутывание, сжимая его до минимально возможного гильбертова пространства; то есть они хотят конвертировать его в максимально запутанные пары. Мы покажем, что с высокой вероятностью успеха Алиса и Боб могут «выпарить» из $\left(|\psi\rangle_{AB}\right)^n$ как минимум

$$k' = n[S(\boldsymbol{\rho}_A) - \delta] \tag{5.202}$$

пар Белла.

Поскольку мы знаем, что Алиса и Боб не могут локальным образом порождать запутывание, то они не могут с помощью локальных операций превратить k пар Белла в $k' > k$ пар, по крайней мере не с высокими точностью воспроизведения и вероятностью успеха. Тогда отсюда следует, что $nS(\boldsymbol{\rho}_A)$ является минимальным количеством пар Белла, необходимым для создания n копий $|\psi\rangle_{AB}$, и что $nS(\boldsymbol{\rho}_A)$ — максимальное количество пар Белла, которое может быть извлечено из n копий $|\psi\rangle_{AB}$. Если бы мы могли более эффективно создавать $|\psi\rangle_{AB}$ из пар Белла или более эффективно извлекать пары Белла из $|\psi\rangle_{AB}$, тогда у Алисы и Боба был бы способ, которым они увеличили бы свой запас пар Белла с помощью локальных операций, что, как известно, невозможно. Следовательно, если мы можем найти способ выделить $k' = n[S(\boldsymbol{\rho}_A) - \delta]$ пар Белла из n копий $|\psi\rangle_{AB}$, то мы знаем, что $E = S(\boldsymbol{\rho}_A)$.

Чтобы проиллюстрировать плотность запутывания, представим, что Алиса и Боб имеют n копий частично запутанного чистого состояния двух кубитов:

$$|\psi(\theta)\rangle_{AB} = \cos\theta|00\rangle + \sin\theta|11\rangle. \tag{5.203}$$

(Подобным образом можно записать любое бинарное чистое состояние, если выбрать базис Шмидта и подходящее соглашение относительно фазы.) То есть Алиса и Боб делят состояние

$$\left(|\psi(\theta)\rangle_{AB}\right)^n = \left(\cos\theta|00\rangle + \sin\theta|11\rangle\right)^n. \tag{5.204}$$

Пусть теперь Алиса (или Боб) выполняет локальное преобразование ее (его) n кубитов. Алиса измеряет вдоль оси z *полный* спин ее n кубитов

$$\boldsymbol{\sigma}_{3,A}^{\text{total}} = \sum_{i=1}^{n} \boldsymbol{\sigma}_{3,A}^{i}. \tag{5.205}$$

Главной чертой этого измерения является его «грубость». Наблюдаемая $\sigma_{3,A}^{\text{total}}$ является сильно *вырожденной*. Алиса проецирует состояние ее n спинов на одно из больших собственных пространств этой наблюдаемой. Она не измеряет спин каждого кубита; фактически она старается не получить никакой другой информации, кроме значения $\sigma_{3,A}^{\text{total}}$, или, что эквивалентно, количества ориентированных «вверх» спинов.

Если мы разложим (5.204), то получим всего 2^n слагаемых. Среди них – $\binom{n}{m}$ слагаемых, в которых ровно m из имеющихся у Алисы кубитов имеют значение $+1$. Каждое из этих слагаемых содержит коэффициент $(\cos\theta)^{n-m}(\sin\theta)^m$. Таким образом, вероятность того, что измерение Алисы обнаружит m направленных «вверх» спинов, равна

$$P(m) = \binom{n}{m} (\cos^2\theta)^{n-m}(\sin^2\theta)^m. \tag{5.206}$$

Более того, если она получила этот результат, то ее измерение приготовило *равновзвешенную* суперпозицию всех $\binom{n}{m}$ состояний, имеющих m ориентированных «вверх» спинов. (Конечно, поскольку спины Алисы и Боба идеально скоррелированы, то если бы Боб измерил $\sigma_{3,B}^{\text{total}}$, то он получил бы точно такой же, как и Алиса, результат. Альтернативно о своем результате Алиса могла бы доложить Бобу в классическом сообщении и тем самым избавить его от хлопот выполнять измерение самому.) Независимо от результата измерения Алиса и Боб теперь делят новое состояние $|\psi'\rangle_{AB}$, в котором все ненулевые собственные значения ρ'_A (и ρ'_B) равны.

При большом n распределение вероятностей $P(m)$ в (5.206) имеет резкий пик – вероятность близка к единице, когда m/n близко к $\sin^2\theta$ и

$$\binom{n}{m} \sim \binom{n}{n\sin^2\theta} \sim 2^{nH(\sin^2\theta)}, \tag{5.207}$$

где $H(p) = -p\log p - (1-p)\log(1-p)$ – функция энтропии. То есть с вероятностью, большей чем $1-\varepsilon$, поделенное теперь между Алисой и Бобом запутанное состояние имеет число Шмидта $\binom{n}{m}$, удовлетворяющее

$$2^{n[H(\sin^2\theta)-\delta]} < \binom{n}{m} < 2^{n[H(\sin^2\theta)+\delta]}. \tag{5.208}$$

Теперь Алиса и Боб хотят превратить поделенное ими запутывание в стандартную пару Белла $|\phi^+\rangle$. Это было бы просто, если бы число Шмидта их максимально запутанного состояния оказалось степенью двойки. Тогда Алиса и Боб могли бы выполнить унитарное преобразование, которое

перевело бы 2^k-мерный носитель его/ее матрицы плотности в гильбертово пространство k кубитов, а затем они могли бы отбросить остаток их кубитов. Тогда оставленные ими k пар были бы максимально запутанными.

Конечно, $\binom{n}{m}$ не обязано быть близким к степени двух. Но если Алиса и Боб разделили множество партий из n копий частично запутанного состояния, то они могут концентрировать запутывание в каждой партии. После такой обработки ℓ партий они получат максимально запутанное состояние с числом Шмидта

$$N_{\text{Schm}} = \binom{n}{m_1}\binom{n}{m_2}\binom{n}{m_3}\cdots\binom{n}{m_\ell}, \tag{5.209}$$

где каждое m_i, как правило, близко к $n\sin^2\theta$. Для любого $\varepsilon > 0$ найдется некоторое ℓ такое, что это число Шмидта в конечном счете окажется близким к степени двух

$$2^{k_\ell} < N_{\text{Schm}} < 2^{k_\ell}(1+\varepsilon). \tag{5.210}$$

При этих условиях Алиса или Боб могут выполнить измерение, которое пытается проецировать носитель размерности $2^{k_\ell}(1+\varepsilon)$ его/ее матрицы плотности на подпространство размерности 2^{k_ℓ}, достигая цели с вероятностью $1-\varepsilon$. *Затем* они переводят носитель в гильбертово пространство k_ℓ кубитов и отбрасывают остаток их кубитов. Обычно k_ℓ близко к $n\ell H(\sin^2\theta)$, так что с близкой к единице вероятностью успеха они выделят около $H(\sin^2\theta)$ максимально запутанных пар из каждого частично запутанного состояния.

Конечно, несмотря на то, что количество ориентированных вверх спинов, которые Алиса (или Боб) находит в своем измерении, обычно близко к $n\sin^2\theta$, оно может флуктуировать около этого значения. Иногда, если повезет, они смогут выделить больше, чем $H(\sin^2\theta)$, пар Белла на одну копию $|\psi(\theta)\rangle_{AB}$. Но вероятность такого существенно лучшего результата пренебрежимо мала при $n \to \infty$.

Эти рассуждения легко распространяются на бинарные чистые состояния в более широких гильбертовых пространствах. Бинарное чистое состояние с числом Шмидта s может быть представлено в базисе Шмидта как

$$|\psi(a_1, a_2, \ldots, a_s)\rangle_{AB} = a_1|11\rangle + a_2|22\rangle + \ldots a_s|ss\rangle. \tag{5.211}$$

Тогда Алиса (или Боб) может измерить полное число векторов $|1\rangle$, полное число векторов $|2\rangle$ и так далее в имеющемся в ее (его) распоряжении состоянии $\left(|\psi\rangle_{AB}\right)^n$. Если она (он) находит m_1 векторов $|1\rangle$, m_2 векторов $|2\rangle$

и т. д., тогда ее (его) измерение готовит максимально запутанное состояние с числом Шмидта

$$N_{\text{Schm}} = \frac{n!}{(m_1)!(m_2)!\cdots(m_s)!}. \tag{5.212}$$

При больших m Алиса обычно будет находить

$$m_i \sim |a_i|^2 n \tag{5.213}$$

и, следовательно,

$$N_{\text{Schm}} \sim 2^{nH}, \tag{5.214}$$

где

$$H = -\sum_i |a_i|^2 \log |a_i|^2 = S(\rho_A). \tag{5.215}$$

Таким образом, из n копий состояния $|\psi\rangle_{AB}$ асимптотически при $n \to \infty$ может быть выделено близкое к $S(\rho_A)$ количество пар Белла.

5.5.1. Запутывание смешанного состояния

Мы нашли хорошо мотивированный и однозначный способ количественного описания запутывания бинарного чистого состояния $|\psi\rangle_{AB}$: $E = S(\rho_A)$, где

$$\rho_A = \text{tr}_B \left(|\psi\rangle_{AB\ AB}\langle\psi|\right). \tag{5.216}$$

Значительный интерес также представляет количественное описание запутывания бинарного смешанного состояния. К сожалению, запутывание смешанного состояния не так хорошо понято, как запутывание чистого состояния, и является предметом текущих исследований.

Допустим, что ρ_{AB} – поделенное Алисой и Бобом смешанное состояние и что они имеют n идентичных копий этого состояния. Предположим также, что, используя локальные операции и классические средства связи, Алиса и Боб могут приготовить $(\rho_{AB})^n$ из k пар Белла с асимптотически (при $n \to \infty$) хорошей точностью воспроизведения и высокой вероятностью успеха. Определим F — *запутывание формирования* ρ_{AB} как

$$F(\rho_{AB}) = \lim_{n\to\infty} \frac{k_{\min}}{n}. \tag{5.217}$$

Далее, предположим, что Алиса и Боб могут использовать локальные операции и классическую связь, чтобы выделить k' пар Белла из n копий ρ_{AB}.

Определим D — *запутывание выделения* ρ_{AB} как

$$D(\rho_{AB}) = \lim_{n\to\infty} \frac{k'_{\max}}{n}. \tag{5.218}$$

Для чистых состояний мы нашли $D = E = F$. Но для смешанных состояний явные общие формулы для D или F неизвестны. Поскольку запутывание не может создаваться локально, мы знаем, что $D \leqslant F$, но (по состоянию на январь 1998 г.) не известно, выполняется ли равенство $D = F$. Однако имеются сильные подозрения, что для смешанных состояний $D < F$. Чтобы приготовить смешанное состояние $(\rho_{AB})^n$ из чистого $\left(|\phi^+\rangle_{AB}\langle\phi^+|\right)^k$, мы должны пренебречь некоторой квантовой информацией. Было бы удивительно, если бы этот процесс оказался (асимптотически) обратимым.

Полезно различать два разных типа запутывания выделения. D_1 обозначает количество пар Белла, которые могут быть выделены, если разрешена только односторонняя классическая связь (например, Алиса *может посылать* сообщения Бобу, но *не может получать* сообщения от него). $D_2 = D$ обозначает запутывание выделения, если классическая связь ничем не ограничена. Известно, что для некоторых смешанных состояний $D_1 < D_2$ и, следовательно, $D_1 < F$ (тогда как для чистых состояний $D_1 = D_2 = F$).

Одной из причин интереса к запутыванию смешанных состояний (и, в частности, к D_1) является его связь с передачей квантовой информации через квантовые каналы с шумом. Если в квантовом канале связи, описываемом супероператором \$, уровень шума не *слишком* высок, то можно построить n-буквенный блоковый код такой, что квантовая информация может быть закодирована, послана через канал $(\$)^n$, декодирована и воспроизведена со сколь угодно высокой точностью при $n \to \infty$. Оптимальное количество закодированных кубитов на одну букву, которое может быть послано через канал, называется емкостью квантового канала $C(\$)$. Оказывается, что $C(\$)$ может быть связана с D_1 частного смешанного состояния, связанного с каналом, — но мы пока отложим дальнейшее обсуждение емкости квантового канала.

5.6. Резюме

Энтропия Шеннона и сжатие классических данных. *Энтропия Шеннона* ансамбля $X = \{x, p(x)\}$ равна $H(X) \equiv -\langle \log p(x)\rangle$; она количественно определяет сжимаемость классической информации. Сообщение

длиной в n букв, каждая буква которого независимо извлекается из X, может быть сжато до $H(X)$ на одну букву (но не более) и, несмотря на это, все же может быть декодировано со сколь угодно высокой точностью при $n \to \infty$.

Взаимная информация и емкость классического канала связи. *Взаимная информация* $I(X;Y) = H(X) + H(Y) - H(X,Y)$ количественно определяет, насколько коррелированы ансамбли X и Y; если мы узнаем значение y, то приобретаем (в среднем) $I(X;Y)$ битов информации об x. Емкость классического шумящего канала связи без памяти равна $C = \max_{\{p(x)\}} I(X;Y)$. Это максимальное количество битов на одну букву, которое может быть передано через канал (используя наилучший возможный код) с пренебрежимо малой вероятностью ошибки при $n \to \infty$.

Энтропия фон Неймана, информация Холево и сжатие квантовых данных. *Энтропия фон Неймана* матрицы плотности ρ равна

$$S(\rho) = -\operatorname{tr} \rho \log \rho, \tag{5.219}$$

а *информация Холево* ансамбля $\mathcal{E} = \{\rho_x, p_x\}$ квантовых состояний равна

$$\chi(\mathcal{E}) = S\left(\sum_x p_x \rho_x\right) - \sum_x p_x S(\rho_x). \tag{5.220}$$

Энтропия фон Неймана количественно определяет сжимаемость ансамбля чистых квантовых состояний. Сообщение длиной в n букв, каждая буква которого независимо извлекается из ансамбля $\{|\varphi_x\rangle, p_x\}$, может быть сжато до $S(\rho)$ кубитов на одну букву (но не более) и, несмотря на это, все же может быть декодировано со сколь угодно высокой точностью воспроизведения при $n \to \infty$. Если буквы извлекаются из ансамбля $\mathcal{E}$ смешанных квантовых состояний, то невозможно сжатие с высокой точностью воспроизведения до менее чем $\chi(\mathcal{E})$ кубитов на одну букву.

Доступная информация. *Доступная информация* ансамбля $\mathcal{E}$ квантовых состояний представляет собой максимальное количество битов информации, которое (в среднем) можно получить о приготовлении состояния с помощью наилучшего возможного измерения. Доступная информация не может превысить информацию Холево ансамбля. Можно построить такой n-буквенный код, что частный ансамбль каждой буквы будет близок к $\mathcal{E}$, а доступная информация на одну букву – к $\chi(\mathcal{E})$. Емкость квантового канала связи \$ по отношению к факторизуемым состояниям равна

$$C(\$) = \max_{\mathcal{E}} \chi(\$(\mathcal{E})). \tag{5.221}$$

Это максимальное количество классических битов на одну букву, которое может быть передано через квантовый канал с пренебрежимо малой вероятностью ошибки при $n \to \infty$ при условии, что каждое кодовое слово является тензорным произведением букв-состояний.

Плотность запутывания. *Запутывание* E бинарного чистого состояния $|\psi\rangle_{AB}$ равна $E = S(\boldsymbol{\rho}_A)$, где $\boldsymbol{\rho}_A = \mathrm{tr}_B\left(|\psi\rangle_{AB\,AB}\langle\psi|\right)$. С помощью локальных операций и классических средств связи можно приготовить n копий $|\psi\rangle_{AB}$ из nE (но не из чуть меньшего количества) пар Белла, а также можно выделить nE (но не больше) пар Белла из n копий $|\psi\rangle_{AB}$ (асимптотически при $n \to \infty$).

5.7. Упражнения

5.1. Различимость неортогональных состояний. Алиса приготовила один кубит в одном из двух (неортогональных) состояний

$$|u\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad |v\rangle = \begin{pmatrix} \cos\dfrac{\theta}{2} \\ \sin\dfrac{\theta}{2} \end{pmatrix}, \tag{5.222}$$

где $0 < \theta < \pi$. Бобу известно значение θ, но он не знает, приготовила Алиса $|u\rangle$ или $|v\rangle$, и ему нужно выполнить измерение, чтобы как можно больше узнать о приготовленном Алисой состоянии.

Боб рассматривает три возможных измерения.

a) Ортогональное измерение с

$$\mathbf{E}_1 = |u\rangle\langle u|, \qquad \mathbf{E}_2 = \mathbf{1} - |u\rangle\langle u|. \tag{5.223}$$

(В этом случае, если Боб получит результат 2, то он будет знать, что Алиса должна была приготовить $|v\rangle$.)

b) ПОЗМ с тремя исходами

$$\begin{aligned} &\mathbf{F}_1 = A(\mathbf{1} - |u\rangle\langle u|), \quad \mathbf{F}_2 = A(\mathbf{1} - |v\rangle\langle v|), \\ &\mathbf{F}_3 = (1 - 2A)\mathbf{1} + A\big(|u\rangle\langle u| + |v\rangle\langle v|\big), \end{aligned} \tag{5.224}$$

где A имеет максимальное совместимое с положительностью $\mathbf{F}_3$ значение. (В этом случае Боб однозначно определит приготовленное состояние, если получит результат 1 или 2, но ничего не узнает из результата 3.)

c) Ортогональнос измерение с

$$\mathbf{E}_1 = |w\rangle\langle w|, \qquad \mathbf{E}_2 = \mathbf{1} - |w\rangle\langle w|, \tag{5.225}$$

где

$$|w\rangle = \begin{pmatrix} \cos\left[\frac{1}{2}\left(\frac{\theta}{2} + \frac{\pi}{2}\right)\right] \\ \sin\left[\frac{1}{2}\left(\frac{\theta}{2} + \frac{\pi}{2}\right)\right] \end{pmatrix}. \tag{5.226}$$

(В этом случае $\mathbf{E}_1$ и $\mathbf{E}_2$ представляют собой проекторы на спиновые состояния, ориентированные в плоскости OXZ перпендикулярно оси, направленной вдоль биссектрисы угла между $|u\rangle$ и $|v\rangle$.)

Найдите среднюю информацию $I(\theta)$, приобретаемую Бобом (взаимную информацию между приготовленным состоянием и результатом измерения) во всех трех случаях, и изобразите графики всех их, как функций θ. Какос измерение следует выбрать Бобу?

5.2. Относительная энтропия. *Относительная энтропия* $S(\boldsymbol{\rho}|\boldsymbol{\sigma})$ двух матриц плотности $\boldsymbol{\rho}$ и $\boldsymbol{\sigma}$ определяется соотношением

$$S(\boldsymbol{\rho}|\boldsymbol{\sigma}) = \operatorname{tr} \boldsymbol{\rho}\big(\log \boldsymbol{\rho} - \log \boldsymbol{\sigma}\big). \tag{5.227}$$

Покажите, что $S(\boldsymbol{\rho}|\boldsymbol{\sigma})$ неотрицательна, и выведите некоторые следствия этого свойства.

a) Дифференцируемая вещественная функция вещественной переменной называется *вогнутой*, если для всех x и y

$$f(y) - f(x) \leqslant (y - x) f'(x). \tag{5.228}$$

Покажите, что если $\mathbf{a}$ и $\mathbf{b}$ — наблюдаемые, а f – вогнутая, то

$$\operatorname{tr}\big[f(\mathbf{b}) - f(\mathbf{a})\big] \leqslant \operatorname{tr}\big[(\mathbf{b} - \mathbf{a}) f'(\mathbf{a})\big]. \tag{5.229}$$

b) Покажите, что $f(x) = -x \log x$ является вогнутой функцией при $x > 0$.

c) Используя (a) и (b), покажите, что $S(\boldsymbol{\rho}|\boldsymbol{\sigma}) \geqslant 0$ для любых двух матриц плотности $\boldsymbol{\rho}$ и $\boldsymbol{\sigma}$.

d) Используя неотрицательность $S(\boldsymbol{\rho}|\boldsymbol{\sigma})$, покажите, что если $\boldsymbol{\rho}$ имеет носитель в пространстве размерности D, то

$$S(\boldsymbol{\rho}) \leqslant \log D. \tag{5.230}$$

e) Используя неотрицательность относительной энтропии, докажите *субаддитивность* энтропии

$$S(\rho_{AB}) \leqslant S(\rho_A) + S(\rho_B). \tag{5.231}$$

[**Указание**. Рассмотрите относительную энтропию $\rho_A \otimes \rho_B$ и ρ_{AB}.]

f) Используя субаддитивность, докажите *вогнутость* энтропии

$$S\left(\sum_i \lambda_i \rho_i\right) \geqslant \sum_i \lambda_i S(\rho_i), \tag{5.232}$$

где λ_i — вещественные положительные числа, сумма которых равна единице. [**Указание**. Примените свойство субаддитивности к

$$\rho_{AB} = \sum_i \lambda_i (\rho_i)_A \otimes (|e_i\rangle\langle e_i|)_B.] \tag{5.233}$$

g) Используя свойство субаддитивности, докажите *неравенство треугольника* (также называемое неравенством Араки – Либа):

$$S(\rho_{AB}) \geqslant |S(\rho_A) - S(\rho_B)|. \tag{5.234}$$

[**Указание**. Рассмотрите очищение ρ_{AB}: то есть постройте чистое состояние $|\psi\rangle_{ABC}$ такое, что $\rho_{AB} = \mathrm{tr}_C\left(|\psi\rangle_{ABC\,ABC}\langle\psi|\right)$. Затем примените свойство субаддитивности к ρ_{BC}.]

5.3. Монотонность Линдблада — Ульмана. Согласно теореме, доказанной Линдбладом и Ульманом, относительная энтропия на $\mathcal{H}_A \otimes \mathcal{H}_B$ обладает свойством, называемым *монотонностью*

$$S(\rho_A|\sigma_A) \leqslant S(\rho_{AB}|\sigma_{AB}). \tag{5.235}$$

Относительная энтропия двух матриц плотности системы AB не может быть меньше, чем редуцированная относительная энтропия подсистемы A.

a) Используя монотонность Линдблада — Ульмана, докажите свойство сильной субаддитивности энтропии фон Неймана. [**Указание**. Рассмотрите относительную энтропию $\rho_A \otimes \rho_{BC}$ и ρ_{ABC} в тройной системе ABC.]

b) Используя монотонность Линдблада – Ульмана, покажите, что действие супероператора не может увеличить относительную энтропию, то есть

$$S(\$\rho|\$\sigma) \leqslant S(\rho|\sigma), \tag{5.236}$$

где $\$$ — произвольный супероператор (вполне положительное отображение). [**Указание**. Вспомните, что произвольный супероператор имеет унитарное представление.]

c) Покажите, что из (b) вытекает, что супероператор не может увеличивать информацию Холево ансамбля $\mathcal{E} = \{\rho_x, p_x\}$ смешанных состояний:

$$\chi(\$(\mathcal{E})) \leqslant \chi(\mathcal{E}), \tag{5.237}$$

где

$$\chi(\mathcal{E}) = S\Big(\sum_x p_x \rho_x\Big) - \sum_x p_x S(\rho_x). \tag{5.238}$$

5.4. ПОЗМ Переса–Вутерса. Рассмотрите источник информации Переса–Вутерса, описанный в § 5.4.2. Он приготавливает одно из трех состояний

$$|\Phi_a\rangle = |\varphi_a\rangle|\varphi_a\rangle, \qquad a = 1, 2, 3, \tag{5.239}$$

каждое из которых появляется с априорной вероятностью $1/3$, где состояния $|\varphi_a\rangle$ определены в (5.149).

a) Выразите матрицу плотности

$$\rho = \frac{1}{3}\sum_a |\Phi_a\rangle\langle\Phi_a| \tag{5.240}$$

в базисе Белла максимально запутанных состояний $\{|\phi^{\pm}\rangle, |\psi^{\pm}\rangle\}$ и вычислите $S(\rho)$.

b) Для трех векторов $|\Phi_a\rangle$, $a = 1, 2, 3$ постройте определенное в (5.162) «достаточно хорошее измерение». (Вновь разложите векторы $|\Phi_a\rangle$ в базисе Белла.) В этом случае ДХИ является ортогональным измерением. Выразите элементы базиса ДХИ в базисе Белла.

c) Вычислите взаимную информацию результатов ДХИ и приготовления состояний.

Глава 6

Квантовые вычисления

6.1. Классические (вычислительные) схемы

В первой главе было введено понятие квантового компьютера. Здесь мы более строго определим модель квантовых вычислений и отметим ее некоторые основные свойства. Но прежде чем объяснять, что делает квантовый компьютер, возможно, следовало бы поговорить о том, что делает классический компьютер.

6.1.1. Универсальные вентили

Классический (детерминистский) компьютер вычисляет функции: по данным n битам на входе он производит m битов на выходе, которые однозначно определены входом. То есть он находит значение

$$f\colon \{0,1\}^n \to \{0,1\}^m \tag{6.1}$$

для определенного, состоящего из n битов, аргумента. Функция, имеющая m-битовое значение, эквивалентна m функциям с однобитовым значением каждая, поэтому вполне можно сказать, что основной задачей, выполняемой классическим компьютером, является вычисление

$$f\colon \{0,1\}^n \to \{0,1\}. \tag{6.2}$$

Нетрудно подсчитать количество таких функций. Существует 2^n возможных входов, и для каждого из них имеется два возможных выхода. Итак, всего имеется 2^{2^n} функций, переводящих n битов в один.

Вычисление любой такой функции можно свести к последовательности элементарных логических операций. Разделим возможные значения входа

$$x = x_1\, x_2 \ldots x_n \tag{6.3}$$

на множество значений, для которых $f(x) = 1$, и дополнительное ему множество, для которого $f(x) = 0$. Для каждого $x^{(a)}$ такого, что $f(x^{(a)}) = 1$, рассмотрим функцию $f^{(a)}$ такую, что

$$f^{(a)}(x) = \begin{cases} 1, & x = x^{(a)}, \\ 0, & x \neq x^{(a)}. \end{cases} \tag{6.4}$$

Тогда

$$f(x) = f^{(1)}(x) \vee f^{(2)}(x) \vee f^{(3)}(x) \vee \dots . \tag{6.5}$$

f — логическое OR ($\vee$) всех функций $f^{(a)}$. В двоичной арифметике двухбитовая операция $\vee$ может быть представлена как

$$x \vee y = x + y - x \cdot y; \tag{6.6}$$

она имеет значение 0, если x и y оба равны нулю, и значение 1 в противном случае.

Рассмотрим вычисление $f^{(a)}$. В том случае, когда $x^{(a)} = 111\dots1$, мы можем записать

$$f^{(a)}(x) = x_1 \wedge x_2 \wedge x_3 \wedge \dots \wedge x_n; \tag{6.7}$$

это логическое AND ($\wedge$) всех n битов. В двоичной арифметике AND представляет собой произведение

$$x \wedge y = x \cdot y. \tag{6.8}$$

Для любого другого $x^{(a)}$ функция $f^{(a)}$ вновь строится как логическое AND n битов, в котором к каждому равному нулю $x_i^{(a)}$ предварительно применяется операция логического NOT ($\neg$), например:

$$f^{(a)}(x) = (\neg x_1) \wedge x_2 \wedge x_3 \wedge (\neg x_4) \wedge \dots, \tag{6.9}$$

если

$$x^{(a)} = 0110\dots. \tag{6.10}$$

Логическая операция NOT в двоичной арифметике представляется как

$$\neg x = 1 - x. \tag{6.11}$$

Мы построили функцию $f(x)$ из трех элементарных логических отношений: NOT, AND, OR. Полученное выражение (6.5) называется «дизъюнктивной нормальной формой» $f(x)$. Мы также неявно использовали еще одну операцию, COPY, превращающую один бит в два:

$$\text{COPY} : x \to xx. \tag{6.12}$$

Операция COPY необходима, поскольку каждая $f^{(a)}$ в разложении f по дизъюнктивным нормальным формам требует свою собственную копию x, на которую она будет действовать.

Фактически мы можем сократить набор элементарных логических отношений до меньшего. Определим операцию NAND («NOT-AND») соотношением

$$x \uparrow y = \neg(x \wedge y) = (\neg x) \vee (\neg y). \tag{6.13}$$

В двоичной арифметике операцией NAND служит

$$x \uparrow y = 1 - x \cdot y. \tag{6.14}$$

Если мы можем выполнять COPY, то NAND можно использовать для выполнения операции NOT:

$$x \uparrow x = 1 - x^2 = 1 - x = \neg x. \tag{6.15}$$

(Или если мы можем приготовить константу $y = 1$, тогда $x \uparrow 1 = 1 - x = \neg x$.) Аналогично

$$(x \uparrow y) \uparrow (x \uparrow y) = \neg(x \uparrow y) = 1 - (1 - x \cdot y) = x \cdot y = x \wedge y, \tag{6.16}$$

а

$$(x \uparrow x) \uparrow (y \uparrow y) = (\neg x) \uparrow (\neg y) = 1 - (1 - x) \cdot (1 - y) = x + y - x \cdot y = x \vee y. \tag{6.17}$$

Итак, если мы можем выполнять COPY, то NAND выполняет AND и OR. Таким образом, одного логического отношения NAND вместе с COPY достаточно для вычисления любой функции f. [Вы можете убедиться в том, что возможной альтернативой в выборе универсального логического отношения является NOR («NOT-OR»):[1]

$$x \downarrow y = \neg(x \vee y) = (\neg x) \wedge (\neg y).] \tag{6.18}$$

Если мы можем приготовить постоянный бит ($x = 0$ или $x = 1$), то количество элементарных операций может быть сокращено с двух до одной. Операция NAND/NOT

$$(x, y) \to (1 - x, 1 - x \cdot y) \tag{6.19}$$

[1] Обратим внимание на то, что вторые равенства в (6.13) и (6.18) фактически являются следствиями известного в теории множеств *принципа двойственности*: (1) Дополнение пересечения равно сумме дополнений и (2) Дополнение суммы равно пересечению дополнений. См., например, А.Н. Колмогоров, С.В. Фомин, *Элементы теории функций и функционального анализа*, М.: Наука, 1976. — *Прим. ред.*

вычисляет NAND (если мы игнорируем первый выходящий бит) и снимает копию (если возьмем в качестве второго входящего бита $y = 1$, а затем применим NOT к обоим выходящим битам)[1]. Таким образом, можно сказать, что NAND/NOT является универсальным логическим вентилем. Если в нашем распоряжении имеется запас постоянных битов, а вентили NAND/NOT могут применяться к любой выбранной паре входящих битов, то мы можем выполнить последовательность операций NAND/NOT для вычисления любой функции $f\colon \{0,1\}^n \to \{0,1\}$ при любом значении входа $x = x_1 x_2 \ldots x_n$.

Этими соображениями мотивируется модель вычислительной схемы. Компьютер имеет несколько основных компонентов, которые могут выполнять элементарные операции с битами или парами битов, такие как COPY, NOT, AND, OR. Он также может готовить постоянные биты или входящие переменные биты. Вычисление представляет собой конечную последовательность таких операций, *схему*, применяемую к точно определенной строке входящих битов[2]. Результатом вычисления является конечное значение всех битов, оставшихся после выполнения всех элементарных операций.

То, что для вычисления любой функции, зависящей от конечного входа, достаточно лишь нескольких элементарных операций, является фундаментальным результатом теории вычислений. Он означает, что с помощью очень простых аппаратных средств можно выполнять сколь угодно сложные вычисления.

До сих пор мы обсуждали вычисления, применяющиеся к частному фиксированному входу, но можно рассматривать и *семейства* схем, действующих на входы переменной длины. Семейства схем предоставляют полезную модель для анализа и классификации *сложности* вычислений, которая будет естественным образом обобщена, когда мы обратимся к квантовым вычислениям.

6.1.2. Сложность схем

Исследуя сложность, мы часто будем интересоваться функциями с однобитовым выходом

$$f : \{0,1\}^n \to \{0,1\}. \tag{6.20}$$

О такой функции f можно сказать, что она кодирует решение «проблемы принятия решения» — функция проверяет вход и выдает ответ ДА или НЕТ.

[1] Можно предложить более простую реализацию операции COPY путем последовательного применения вентиля NAND/NOT: $(x,0) \to (1-x,1) \to (x, 1-(1-x)\cdot 1) = (x,x)$. — *Прим. ред.*

[2] Схемы должны быть *апериодическими*, в том смысле, что *полностью* замкнутые циклы в них недопустимы.

Часто оказывается, что вопрос, который не хотелось бы формулировать словесно как вопрос, имеющий ответ ДА/НЕТ, может быть «переформулирован» как проблема принятия решения. Например, функция, определяющая FACTORING-проблему (задача факторизации):

$$f(x,y) = \begin{cases} 1, & \text{если целое } x \text{ имеет делитель, меньший чем } y, \\ 0 & \text{в противном случае;} \end{cases} \tag{6.21}$$

знание $f(x,y)$ для всех $y < x$ эквивалентно знанию *наименьшего* нетривиального множителя x. Другим важным примером проблемы принятия решения служит HAMILTONIAN-проблема (задача нахождения гамильтонова обхода): рассмотрим ℓ-вершинный граф, представленный $\ell \times \ell$-матрицей смежности (равенство единице ее ij-элемента означает, что существует ребро, связывающее вершины i и j); функция

$$f(x) = \begin{cases} 1, & \text{если граф } x \text{ имеет гамильтонов обход,} \\ 0 & \text{в противном случае.} \end{cases} \tag{6.22}$$

(Обход называется гамильтоновым, если он проходит через каждую вершину графа только один раз.)

Мы хотим оценивать трудность проблемы, количественно определяя необходимые для ее решения ресурсы. Сложность проблемы принятия решения разумно измерять *размером* минимальной схемы, вычисляющей соответствующую функцию $f\colon \{0,1\}^n \to \{0,1\}$. Под размером мы понимаем количество элементарных операций или компонентов, которые нужно объединить в схему, чтобы вычислить f. Также можно интересоваться тем, какого *времени* требует вычисление, если многие операции могут выполняться параллельно. *Глубина* схемы представляет собой необходимое количество шагов при условии, что операции, действующие на различные биты, могут выполняться одновременно (то есть глубиной является максимальная длина прямого пути от входа схемы до ее выхода). *Ширина* схемы — это максимальное количество операций, выполняемых на любом из ее этапов.

Мы хотели бы разделить проблемы принятия решения на два класса: легкие и трудные. Но где следует провести границу? Рассмотрим с этой целью бесконечные семейства проблем принятия решения с переменным размером входа; то есть количество битов на входе может быть любым целым n. Тогда можно проверить, как соизмеряется с n размер схемы, решающей проблему.

Однако в использовании масштабного поведения семейства схем в качестве характеристики сложности задачи имеется одна тонкость. Было бы

обманом скрывать сложность проблемы в *конструкции* схемы. Следовательно, мы должны ограничиться семействами, обладающими приемлемыми свойствами «однородности» — должно быть «просто» построить схему с $n+1$-битовым входом, коль скоро схема с n-битовым входом уже построена.

Пусть с данным семейством функций $\{f_n\}$ (где f_n имеет n-битовый вход) сопоставлены вычисляющие их схемы $\{C_n\}$. Мы говорим, что $\{C_n\}$ является семейством схем «полиномиального размера», если размер C_n растет с n не быстрее некоторой степени n:

$$\text{size}(C_n) \leqslant \text{poly}(n), \tag{6.23}$$

где poly обозначает полином. Тогда определим:

$$P = \left\{ \begin{array}{l} \text{проблема принятия решения, решаемая семействами схем} \\ \text{полиномиального размера} \end{array} \right\}$$

(P означает разрешимость за «полиномиальное время»). Проблемы принятия решения, принадлежащие P, являются «простыми», остальные — «сложными». Заметим, что C_n вычисляет $f_n(x)$ для любого возможного n-битового входа и, следовательно, если проблема принятия решения принадлежит P, то даже «в худшем случае» мы можем найти ответ, используя схему, размер которой не превышает $\text{poly}(n)$. (Как отмечалось выше, мы неявно предполагаем, что семейство схем «однородно», так что проблема *разработки* схемы сама может быть решена с помощью алгоритма, требующего полиномиального времени. В этом предположении разрешимость за полиномиальное время с помощью семейства схем эквивалентна разрешимости за полиномиальное время с помощью универсальной машины Тьюринга.)

Конечно, чтобы определить размер схемы, вычисляющей f_n, мы должны знать, что представляют собой ее элементарные компоненты. К счастью, принадлежность проблемы к P не зависит от выбора набора вентилей, до тех пор пока они универсальны, их множество конечно, а каждый вентиль действует на ограниченное множество битов. Один универсальный набор вентилей может *моделироваться* другим.

Огромное большинство семейств функций $f\colon \{0,1\}^n \to \{0,1\}$ не принадлежит P. Для большей части функций выход существенно случаен, и нет лучшего способа «вычислить» $f(x)$, чем обратиться к таблице ее значений. Но поскольку имеется 2^n n-битовых входов, то эта таблица имеет *экспоненциальный* размер, такой же размер должна иметь и схема, кодирующая эту таблицу. Проблемы из P принадлежат очень частному классу —

они имеют такую структуру, что функция f может быть эффективно вычислена.

Особый интерес представляют проблемы принятия решения, на которые можно ответить, приведя легко проверяемый пример. Пусть, например, для данных x и $y < x$ трудно (в худшем случае) определить, имеет ли x множитель, меньше чем y. Но если кто-нибудь любезно предоставит такое $z < y$, на которое делится x, то нам просто проверить, что z действительно является множителем x. Аналогично трудно определить, имеет ли граф гамильтонов обход, но если кто-нибудь нам его показал, то легко убедиться в том, что он и в самом деле гамильтонов.

Эту идею, что проблема может быть трудно разрешимой, но ее решение, коль скоро оно найдено, легко проверяемо, можно формализовать с помощью понятия «недетерминированной» схемы. Ассоциированная с $C_n(x^{(n)})$ недетерминированная схема $\tilde{C}_{n,m}(x^{(n)}, y^{(m)})$ обладает свойством[1]:

$$C_n(x^{(n)}) = 1, \quad \text{если} \quad \tilde{C}_{n,m}(x^{(n)}, y^{(m)}) = 1, \quad \text{для } \textit{некоторого } y^{(m)} \tag{6.24}$$

(где $x^{(n)}$ представляет n битов, а $y^{(m)}$ — m битов). Таким образом, если $y^{(m)}$ оказалось удачно подобранным для некоторого $x^{(n)}$, то мы можем использовать $\tilde{C}_{n,m}$ для *проверки* того, что $C_n(x^{(n)}) = 1$. Определим

$$NP = \left\{ \begin{array}{l} \text{проблемы принятия решения, допускающие семейство } \textit{недетерминированных} \\ \text{схем полиномиального размера} \end{array} \right\}$$

(NP означает разрешимость за «недетерминированное полиномиальное время»). Если проблема принадлежит NP, то нет гарантии, что она простая. Это означает лишь то, что ее решение легко проверить, если мы располагаем правильной информацией. Очевидно, что $P \subseteq NP$. Подобно P, NP-проблемы образуют малый подкласс всех проблем принятия решения.

---

[1] Согласно одному из определений проблема *принадлежит* классу сложности NP, если существует схема полиномиального по n размера, проверяющая предложенное решение за полиномиальное время. Проверяющая схема [в данном случае это $\tilde{C}(x^{(n)}, y^{(m)})$] является *детерминированной*. Термин *недетерминированный* происходит от того, что согласно другому определению (см. следующее чуть ниже определение в основном тексте) NP-проблема допускает решение за полиномиальное время на так называемой *недетерминированной* машине Тьюринга, способной в некоторых состояниях выбирать различные варианты вычисления. См. А. Китаев, А. Шень, М. Вялый, Классические и квантовые вычисления, М., МЦНМО, ЧеРо (1999). — *Прим. ред.*

Многое в теории сложности опирается на фундаментальное предположение

$$\text{Предположение:} \quad P \neq NP; \tag{6.25}$$

существуют сложные проблемы принятия решения, решения которых легко проверяемы. К сожалению, эта важная гипотеза все еще ждет своего доказательства. Однако после 30-ти лет попыток показать обратное – большинство специалистов в теории сложности твердо уверены в ее справедливости[1].

Важным примером NP-проблемы является CIRCUIT-SAT[2]. В этом случае вход представляет собой состоящая из n вентилей схема C с m-битовым входом и однобитовым выходом. Проблема состоит в том, чтобы найти, существует ли *какой-нибудь* m-битовый вход, для которого выход равен единице. Функция, которую необходимо вычислить, представляет собой

$$f(C) = \begin{cases} 1, & \text{если существует } x^{(m)} \text{ } \textit{такое, что } C(x^{(m)}) = 1, \\ 0 & \text{в противном случае.} \end{cases} \tag{6.26}$$

Это NP-проблема, поскольку *данную* схему легко *смоделировать* и вычислить ее выход для любого частного входа.

Я перехожу к формулировке некоторых важных результатов теории сложности, которые будут для нас важны. Здесь не будет времени для доказательств. Вы можете почерпнуть больше, обратившись к одному из многих учебников по этому предмету. [3]

Многие идеи, порожденные теорией сложности, вытекают из теоремы Кука (1971). Она утверждает, что *любая* NP-проблема *полиномиально приводима* к CIRCUIT-SAT. Это означает, что для любой PROBLEM $\in NP$ существует семейство схем полиномиального размера, которое отображает «ситуацию» $x^{(n)}$ для PROBLEM на «ситуацию» $y^{(m)}$ для CIRCUIT-SAT, то есть

$$\text{CIRCUIT-SAT}(y^{(m)}) = 1, \text{ если } \text{PROBLEM}(x^{(n)}) = 1. \tag{6.27}$$

Отсюда следует, что если бы в нашем распоряжении имелось магическое устройство, которое могло бы эффективно решать CIRCUIT-SAT

[1] Проблема соотношения классов сложности P и NP остается нерешенной и в настоящее время (начало 2007г.). Более того она входит в список важнейших задач математики XXI в. – *Прим. ред.*

[2] CIRCUIT-SAT (circuit-satisfyability) problem – проблема выполнимости схемы. (перев.)

[3] Одной из лучших является книга M.R. Garey, D.S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Competeness*, русский перевод М. Гэри, Д. Джонсон, *Вычислительные машины и трудноразрешаемые задачи*, М.: Мир (1982). [Краткий, но достаточно полный, обзор классов сложности и их иерархии можно найти в первой части книги: А. Китаев, А. Шень, М. Вялый, *Классические и квантовые вычисления*, М.: МЦНМО, ЧеРо (1999). – *Прим. ред.*]

(CIRCUIT-SAT «оракул»), то с помощью полиномиальной редукции мы могли бы связаться с ним, чтобы эффективно решить PROBLEM. Из теоремы Кука следует, что если вдруг окажется, что CIRCUIT-SAT $\in P$, то $P = NP$.

Проблема, которая, подобно CIRCUIT-SAT, обладает тем свойством, что к ней полиномиально приводится любая проблема из NP, называется NP-полной (NPC). После Кука было найдено множество других примеров NPC-проблем. Чтобы показать, что PROBLEM $\in NP$ является NP-полной, достаточно найти другую, полиномиально приводимую к ней проблему, о которой уже известно, что она NP-полная. Например, можно продемонстрировать полиномиальную приводимость CIRCUIT-SAT к HAMILTONIAN. Тогда из теоремы Кука следует, что HAMILTONIAN тоже NP-полна.

Если мы предположим, что $P \neq NP$, то отсюда следует, что в NP существуют проблемы промежуточной трудности (класс NPI). Это ни P, ни NPC.

Другой важный класс сложности называется со-NP. Эвристически NP-проблемами разрешимости являются те, на которые мы можем ответить, приведя пример, если ответом является ДА, в то время как на со-NP-проблему можно ответить *контрпримером*, если ответом является НЕТ. Более формально

$$\{C\} \in NP\colon C(x) = 1, \quad \text{если} \quad C(x, y) = 1 \quad \text{для некоторого } y; \tag{6.28}$$

$$\{C\} \in \text{со-}NP\colon C(x) = 1, \quad \text{если} \quad C(x, y) = 1 \quad \text{для всех } y. \tag{6.29}$$

Очевидно, что между классами NP и со-NP существует симметрия — рассматриваем ли мы проблему из NP или из со-NP зависит от того, как был сформулирован вопрос. (Проблема «Существует ли гамильтонов обход?» принадлежит классу NP. Проблема «Действительно ли, что гамильтонова обхода не существует?» принадлежит классу со-NP.) Однако интересен вопрос: существует ли проблема ($\notin P$), одновременно принадлежащая *обоим* классам: NP и со-NP. Если да, то мы можем легко проверить ответ (коль скоро имеем подходящий пример) независимо от того является им ДА или НЕТ. Считается (хотя и не доказано), что $NP \neq$ со-NP. (Приведя пример, мы можем показать, что граф имеет гамильтонов обход, но мы не знаем, как подобным образом показать, что он *не* имеет гамильтоновых обходов!) При условии, что $NP \neq$ со-NP, существует теорема, которая утверждает, что ни одна со-NP-проблема не принадлежит NPC. Следовательно, проблемы, принадлежащие пересечению NP и со-NP и при этом не входящие в P, являются хорошими кандидатами для включения их в NPI.

Фактически такой проблемой, принадлежащей $NP \cap$co-NP, относительно которой считается, что она не входит в P, является FACTORING-проблема. Как уже отмечалось, FACTORING-проблема принадлежит классу NP, поскольку мы можем легко проверить правильность предоставленного множителя числа x. Но она также принадлежит и co-NP, поскольку известно, что если нам дано простое число, то (по крайней мере в принципе) мы можем эффективно проверить его простоту. Таким образом, если некто сообщает нам простые множители числа x, то мы можем эффективно проверить, что разложение на простые множители правильно, и можем *исключить*, что любое целое, меньшее y, является делителем числа x. Следовательно, похоже на то, что FACTORING-проблема принадлежит классу NPI[1].

Мы пришли к грубой (гипотетической) картине структуры $NP \cap$ co-NP. Классы NP и co-NP не совпадают, но имеют нетривиальное пересечение. Класс P принадлежит пересечению $NP \cap$ co-NP (поскольку $P =$ co-P), но кроме этого оно содержит проблемы, не входящие в P (подобные FACTORING-проблеме). Ни NPC ни co-NPC не пересекаются с $NP \cap$ co-NP.

Можно было бы гораздо больше рассказать о теории сложности, но мы ограничимся здесь упоминанием еще одного элемента, связанного с обсуждением квантовой сложности. Иногда полезно рассматривать *вероятностные* схемы, которые имеют доступ к генератору случайных чисел. Например, вентиль в вероятностной схеме может действовать одним из двух способов и «подбрасывает монету», чтобы решить, какое *действие выполнить*. При одном фиксированном входе такая схема может избрать один из множества вычислительных путей. Об алгоритме, выполняемом вероятностной схемой, говорят как о «рандомизированном».

Если мы приступаем к проблеме принятия решения, используя вероятностный компьютер, то получаем распределение вероятностей результатов. Таким образом, мы не будем всегда получать обязательно правильный ответ. Но если для любого возможного входа вероятность получения правильного ответа больше, чем $\frac{1}{2} + \delta$ ($\delta > 0$), то такая машина полезна. Фактически мы можем многократно повторить вычисление и, учитывая

[1] В 2002 г. группой индийских математиков предложен полиномиальный детерминированный алгоритм проверки целых чисел на простоту. Его асимптотическая сложность $O((\log n)^k)$, где n — проверяемое число, k — целое число $\sim$ 10. Таким образом, проблема распознавания простоты целого числа принадлежит классу сложности P. M. Agrawal, N. Kayal, N. Saxena, *Primes is in P*, Annals of Math., **160**, 781–793 (2004), http://www.math.princeton.edu/$\sim$annals/ . См. также Л. Ю. Бараш, *Алгоритм AKS проверки чисел на простоту и поиск констант генераторов псевдослучайных чисел*, Безопасность информационных технологий, **2**, 27–38 (2005). — *Прим. ред.*

«голос большинства», достичь вероятности ошибки, меньшей ε. Более того, количество необходимых для этого повторений вычисления всего лишь полилогарифмически зависит от ε^{-1}[1].

Если проблема допускает решение с помощью семейства вероятностных схем полиномиального размера, которые всегда дают правильный ответ с вероятностью, большей $\frac{1}{2} + \delta$ (для любого входа и при фиксированном $\delta > 0$), то мы говорим, что она принадлежит классу BPP («вероятностное полиномиальное время с ограниченной ошибкой»). Очевидно, что

$$P \subset BPP, \tag{6.30}$$

но соотношение между NP и BPP не известно. В частности, не доказано, что BPP содержится в NP.

6.1.3. Обратимые вычисления

Разрабатывая модель квантового компьютера, мы обобщим модель классических вычислительных схем. Но нашими квантовыми логическими вентилями будут унитарные и, следовательно, обратимые преобразования, тогда как классические логические вентили типа NAND необратимы. Прежде чем обсуждать квантовые схемы, полезно рассмотреть некоторые особенности классических обратимых вычислений.

Помимо их связи с квантовыми вычислениями, другие побудительные причины для изучения обратимых классических вычислений обсуждались в первой главе. Как заметил Ландауэр, поскольку необратимые логические элементы стирают информацию, они с необходимостью диссипативны и, следовательно, требуют постоянного расхода энергии. Но если компьютер оперирует обратимо, то в принципе не должно быть никакой потребности в энергии. Мы можем вычислять даром!

Обратимый компьютер вычисляет обратимую функцию, преобразуя n битов в другие n битов:

$$f: \{0,1\}^n \rightarrow \{0,1\}^n; \tag{6.31}$$

функция должна быть обратимой, то есть для каждого выхода существует единственный вход; тогда мы в принципе в состоянии пройти вычисление в обратном порядке и, зная выход, воспроизвести вход. Поскольку это взаимно-однозначная функция, ее можно рассматривать как перестановку 2^n строк из n битов – всего таких функций $(2^n)!$.

[1] То есть количество необходимых повторений ограничено сверху полиномом $\mathrm{poly}(\log(\varepsilon^{-1}))$. – *Прим. ред.*

Конечно, любое необратимое вычисление можно «оформить» как вычисление обратимой функции. Например, для любой $f: \{0,1\}^n \to \{0,1\}^m$ мы можем сконструировать $\tilde{f}: \{0,1\}^{n+m} \to \{0,1\}^{n+m}$ такую, что

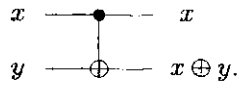
$$\tilde{f}(x; 0^{(m)}) = (x; f(x)) \tag{6.32}$$

(где $0^{(m)}$ обозначает m битов, первоначально положенных равными нулю). Поскольку $\tilde{f}$ преобразует каждое $(x; 0^{(m)})$ к своему, отличному от других, результату, она может быть расширена до обратимой функции от $n+m$ битов. Следовательно, для любой f, преобразующей n битов в m, существует обратимая функция $\tilde{f}$, преобразующая $n+m$ битов в $n+m$ битов, которая вычисляет $f(x)$, действуя на $(x; 0^{(m)})$.

Как теперь построить сложные обратимые вычисления из элементарных компонентов — то есть что образует набор универсальных вентилей? Мы увидим, что одно- и двухбитовых обратимых вентилей не достаточно; для универсальных обратимых вычислений нам понадобятся трехбитовые вентили.

Из четырех 1-бит $\to$ 1-бит вентилей обратимы два — тривиальный и NOT. Из $(2^4)^2 = 256$ возможных 2-бит $\to$ 2-бит вентилей обратимы $4! = 24$. Одним из особенно интересных является вентиль контролируемое NOT или XOR, с которым мы уже сталкивались в четвертой главе:

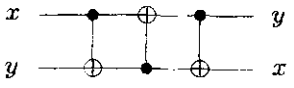
$$XOR: (x, y) \to (x, x \oplus y), \tag{6.33}$$



Этот вентиль инвертирует второй бит, если первый равен единице, и ничего не делает, если первый бит равен нулю (отсюда его название: контролируемое NOT). Его квадрат является тривиальным, то есть он обратен по отношению к самому себе. Конечно, этот вентиль выполняет операцию NOT на втором бите, если первый бит положить равным единице, и выполняет операцию копирования, если начальным значением y является нуль:

$$XOR: (x, 0) \to (x, x), \tag{6.34}$$

С помощью схемы



построенной из трех XOR-ов, мы можем поменять местами два бита[1]:

$$(x, y) \to (x, x \oplus y) \to (y, x \oplus y) \to (y, x). \tag{6.35}$$

С помощью этих обменов можно тасовать биты внутри схемы, собирая их вместе, если мы хотим подействовать на них конкретным компонентом в фиксированном положении.

Чтобы увидеть, что одно- и двухбитовые вентили неуниверсальны, заметим, что все они *линейны*. Каждый обратимый двухбитовый вентиль действует по правилу

$$\begin{pmatrix} x \\ y \end{pmatrix} \to \begin{pmatrix} x' \\ y' \end{pmatrix} = \mathcal{M} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} a \\ b \end{pmatrix}, \tag{6.36}$$

где константа $\binom{a}{b}$ принимает одно из четырех возможных значений, а $\mathcal{M}$ — одна из шести обратимых матриц

$$\mathcal{M} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}. \tag{6.37}$$

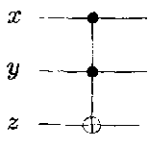
[Все суммирования в (6.36) выполняются по модулю 2.] Комбинируя шесть вариантов $\mathcal{M}$ с четырьмя возможными константами, мы получаем 24 различных вентиля, которыми исчерпывается набор всех обратимых $2 \to 2$ вентилей.

Поскольку линейные преобразования замкнуты относительно композиции, любая схема, скомбинированная из обратимых $2 \to 2$ (и $1 \to 1$) вентилей, будет вычислять линейную функцию

$$x \to \mathcal{M}x + a. \tag{6.38}$$

Однако при $n \geqslant 3$ существуют нелинейные обратимые функции n битов. Важным примером служит *вентиль Тоффоли* $\theta^{(3)}$ (или дважды контролируемое NOT)

$$\theta^{(3)} : (x, y, z) \to (x, y, z \oplus x \cdot y); \tag{6.39}$$



[1] В двоичной арифметике сложение по модулю 2 определяется как $x \oplus y = x + y - 2x \cdot y$. Эта операция, очевидно, коммутативна $x \oplus y = y \oplus x$ и ассоциативна $(x \oplus y) \oplus z = x \oplus (y \oplus z) = x \oplus y \oplus z$. — *Прим. ред.*

он инвертирует третий бит, если два первых равны единице, и ничего не делает в противном случае. Подобно XOR-вентилю он обратен по отношению к самому себе.

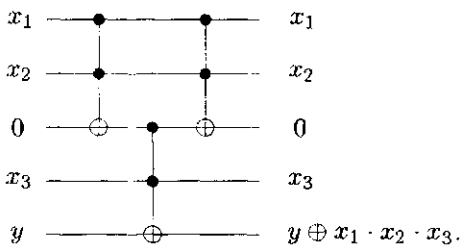
В отличие от обратимых двухбитовых вентилей, $\theta^{(3)}$ является универсальным вентилем булевой логики, если мы можем фиксировать некоторые входящие биты и игнорировать некоторые выходящие биты. Если начальное значение z равно единице, то на третьем выходе возникает $x \uparrow y = 1 - x \cdot y$ — мы можем выполнить NAND. Если же мы фиксируем $x = 1$, то вентиль Тоффоли функционирует подобно XOR-вентилю и может использоваться для копирования.

Вентиль Тоффоли $\theta^{(3)}$ универсален в том смысле, что, используя только его, можно построить схему, вычисляющую любую обратимую функцию (при условии, что можно фиксировать входящие биты и игнорировать выходящие). Полезно показать это непосредственно, не опираясь на наше более раннее доказательство того, что NAND/NOT является универсальным для вычисления любой булевой функции. Фактически можно показать следующее: из вентилей NOT и Тоффоли $\theta^{(3)}$ мы можем построить универсальную функцию n битов при условии, что мы имеем доступ к одному дополнительному биту в памяти.

В качестве первого шага покажем, что из трехбитовых вентилей Тоффоли $\theta^{(3)}$ можно построить n-битовый вентиль Тоффоли $\theta^{(n)}$, действующий по правилу

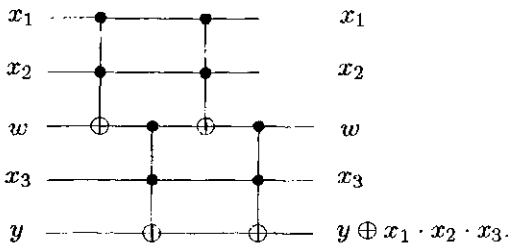
$$(x_1, x_2, \ldots, x_{n-1}, y) \to (x_1, x_2, \ldots, x_{n-1}, y \oplus x_1 x_2 \ldots x_{n-1}). \qquad (6.40)$$

Эта конструкция требует дополнительного бита из вспомогательного пространства. Например, мы конструируем $\theta^{(4)}$ из вентилей $\theta^{(3)}$ с помощью схемы



Цель последнего $\theta^{(3)}$-вентиля — вернуть вспомогательному биту его начальное значение, равное нулю. В действительности, добавив еще один $\theta^{(3)}$-вен-

тиль, можно реализовать $\theta^{(4)}$, который работает независимо от начального значения вспомогательного бита:



Снова мы можем *исключить* последний вентиль, если нас не беспокоит изменение значения вспомогательного бита[1].

Мы можем убедиться в том, что вспомогательный бит действительно необходим. Поскольку $\theta^{(4)}$ представляет собой нечетную перестановку (фактически подстановку) 16-ти четырехбитовых строк, он переставляет 1111 и 1110. Однако $\theta^{(3)}$, действуя на любые три бита из четырех, осуществляет четную перестановку; например, действуя на последние три бита, он переставляет 0111 с 0110 или 1111 с 1110[2]. Поскольку произведение четных перестановок также является четным, мы не можем получить $\theta^{(4)}$ как произведение вентилей $\theta^{(3)}$, действующее только на четыре бита.

Конструкцию $\theta^{(4)}$ из четырех $\theta^{(3)}$ можно непосредственно обобщить на конструкцию $\theta^{(n)}$ из двух $\theta^{(n-1)}$ и двух $\theta^{(3)}$ (только расширив x_1 в приведенной выше диаграмме до нескольких битов). Итерируя эту конструкцию, мы получим $\theta^{(n)}$-схему, состоящую из $2^{n-2} + 2^{n-3} - 2$ вентилей $\theta^{(3)}$. Более того, для этого достаточно только одного вспомогательного бита[3]. (Если нам необходимо построить $\theta^{(n)}$, то для этого подойдет любой доступный вспомогательный бит, так как схема возвращает ему его начальное значение.) Следующим шагом заметим, что, соединяя $\theta^{(n)}$ с вентилями NOT, мы можем в действительности менять значение контрольной строки,

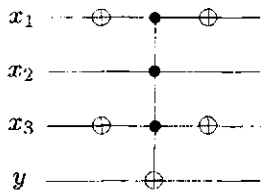
---

[1]На самом деле *восстановление* начального значения вспомогательного бита w, осуществляемое в этой схеме вторым верхним $\theta^{(3)}$-вентилем, является *необходимой* операцией. Именно благодаря этому на выходе второго нижнего $\theta^{(3)}$-вентиля получается $[y \ominus (wx_3 \oplus x_1x_2x_3)] \oplus wx_3 = y \oplus x_1x_2x_3$. Последнее равенство легко проверяется с учетом коммутативности и ассоциативности сложения по модулю 2. — *Прим. ред.*

[2]По-видимому автор имеет ввиду, что $\theta^{(4)}$-вентиль осуществляет нечетное количество нетривиальных подстановок (одну), а $\theta^{(3)}$-вентиль — четное (две). — *Прим. ред.*

[3]С большим вспомогательным пространством можно значительно эффективнее построить $\theta^{(n)}$ из $\theta^{(3)}$ вентилей (см. упражнения).

«управляющей» вентилем. Например, схема



инвертирует значение y, если $x_1x_2x_3 = 010$, и действует тривиально в противном случае. Таким образом, эта схема переставляет две строки: 0100 и 0101. Подобным образом, с помощью вентилей $\theta^{(n)}$ и NOT можно придумать схему, которая переставляет любые две n-битовые строки, отличающиеся только одним битом. (Расположение бита, которым они отличаются, выбирается в качестве *цели* вентиля $\theta^{(n)}$.)

Но фактически подстановка, обменивающая любые две n-битовые строки, может быть представлена как произведение подстановок, которые обменивают строки, отличающиеся только одним битом. Если a_0 и a_s — две строки, расстояние Хемминга между которыми равно s (отличаются s позициями), то существует цепь

$$a_0,\ a_1,\ a_2,\ a_3,\ \ldots,\ a_s \tag{6.41}$$

такая, что каждая строка в этой последовательности удалена от ближайших соседей на равное единице расстояние Хемминга. Следовательно, каждая из подстановок

$$(a_0, a_1),\ (a_1, a_2),\ (a_2, a_3),\ \ldots,\ (a_{s-1}, a_s) \tag{6.42}$$

может быть реализована как вентиль $\theta^{(n)}$, соединенный вентилями NOT. Комбинируя подстановки, находим

$$\begin{aligned}(a_0, a_s) = {} & (a_{s-1}, a_s)(a_{s-2}, a_{s-1})\ldots \\ & \ldots(a_2, a_3)(a_1, a_2)(a_0, a_1)(a_1, a_2)(a_2, a_3)\ldots \\ & \ldots(a_{s-2}, a_{s-1})(a_{s-1}, a_s);\end{aligned} \tag{6.43}$$

мы можем сконструировать подстановку с равным s расстоянием Хемминга из $2s-1$ подстановки с единичным расстоянием Хемминга. Отсюда следует, что мы можем построить (a_0, a_s) из вентилей $\theta^{(n)}$ и NOT.

Наконец, поскольку каждая перестановка является произведением подстановок, мы показали, что любая обратимая функция n-битов (каждая перестановка n-битовых строк) представляет собой произведение вентилей $\theta^{(3)}$ и вентилей NOT, использующее только один бит вспомогательного пространства.

Конечно, операция NOT может быть выполнена с помощью вентиля $\theta^{(3)}$, если мы фиксируем два входящих бита равными единицам. Таким образом, вентиль Тоффоли $\theta^{(3)}$ является универсальным для обратимых вычислений, если мы можем фиксировать входящие биты и отбрасывать выходящие.

6.1.4. Компьютер бильярдных шаров

Двухбитовых вентилей достаточно для универсальных необратимых вычислений, но для универсальных обратимых вычислений необходимы трехбитовые вентили. Возникает соблазн сказать, что для их реализации необходимы «трехчастичные взаимодействия», так что создание обратимого аппаратного обеспечения является более сложной проблемой, чем создание необратимого. Однако это утверждение в какой-то мере может быть обманчивым.

Фредкин описал, как можно построить универсальный обратимый компьютер, в котором фундаментальным взаимодействием является упругое столкновение между двумя бильярдными шарами. Шары радиуса $1/\sqrt{2}$ движутся по квадратной решетке, период которой равен единице. В каждый целочисленный момент времени центр каждого шара находится в узле решетки; наличие или отсутствие шара в данном узле (в этот момент времени) кодирует бит информации. В течение каждого единичного интервала времени каждый (подвижный) шар проходит единичное расстояние вдоль одного из направлений решетки. Иногда, в целочисленные моменты времени, происходит упругое рассеяние на $90°$ двух шаров, занимающих узлы, удаленные друг от друга на расстояние $\sqrt{2}$ (соединенные диагональю ячейки решетки).

Прибор программируется закреплением части шаров в некоторых узлах, которые действуют как идеальные отражатели. После задания начальных положений и направлений движения подвижных шаров система выполняет программу, эволюционируя в течение конечного интервала времени в соответствии с механикой Ньютона. Результат считывается путем наблюдения конечных положений подвижных шаров. Столкновения недиссипативны, так что после обращения всех скоростей вычисление может быть пройдено в обратном порядке.

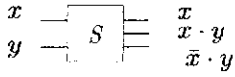
Чтобы показать, что эта машина является универсальным обратимым компьютером, мы должны объяснить, как в ней реализовать универсальный вентиль. Удобно рассмотреть трехбитовый *вентиль Фредкина*

$$(x, y, z) \to (x, xz + \bar{x}z, xz + \bar{x}y), \tag{6.44}$$

который меняет местами y и z, если $x = 0$ (мы ввели обозначение $\bar{x} = \neg x$). Вы можете убедиться в том, что вентиль Фредкина может моделировать вентиль NAND/NOT, если мы фиксируем входы и игнорируем выходы.

Мы можем построить вентиль Фредкина из более примитивного объекта, *вентиля-переключателя*. Переключатель преобразует два бита в три, действуя по правилу

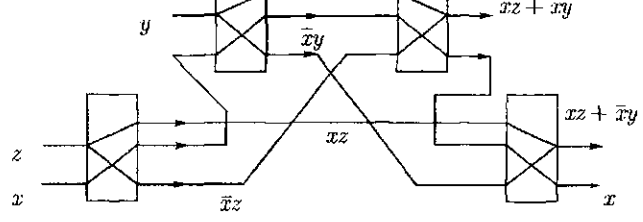
$$(x, y) \to (x, x \cdot y, \bar{x} \cdot y). \tag{6.45}$$



Этот вентиль «обратим» в том смысле, что его можно пройти в обратном направлении, действуя на ограниченный трехбитовый вход, принимающий одно из четырех значений:

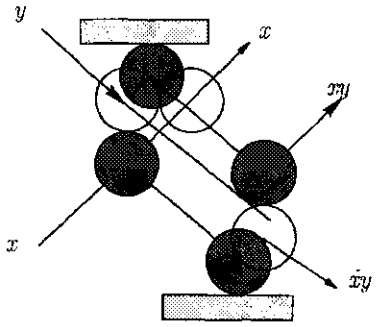
$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}. \tag{6.46}$$

Более того, переключатель сам по себе универсален; фиксируя входы и игнорируя выходы, он может выполнить операцию NOT ($y = 1$, третий выход), AND (второй выход) и COPY ($y = 1$, первый и второй выходы). Тогда не удивительно, что, комбинируя переключатели, можно построить универсальный $3 \to 3$ *вентиль*. Действительно, схема



образует вентиль Фредкина из четырех переключателей (два из них проходятся в прямом направлении, два других — в обратном). Время задержки, необходимое для синхронизации, явно не показано.

В компьютере бильярдных шаров переключатель строится из таких двух отражателей, чтобы (в случае $x = y = 1$) два движущихся шара столкнулись дважды. В этом случае траектории шаров имеют вид



Шар, помеченный как x, вылетает из вентиля вдоль той же траектории (и в то же самое время) независимо от наличия или отсутствия другого шара. Однако при $x = 1$ положение другого шара (если он имеется) смещается вниз по сравнению с его конечным положением при $x = 0$ — это и есть переключатель. Коль скоро мы можем построить переключатель, то можем построить и вентиль Фредкина и, таким образом, реализовать универсальную обратимую логику на компьютере бильярдных шаров.

Очевидной слабостью схемы бильярдных шаров является то, что начальные ошибки положений и скоростей шаров будут быстро накапливаться и в конце концов компьютер окажется несостоятельным. Как отмечалось в первой главе (а Ландауэр настоятельно подчеркивал это), подобным недостатком будет страдать любая предлагаемая схема недиссипативных вычислений. Чтобы контролировать ошибки, мы должны быть в состоянии сжимать фазовое пространство прибора, что с необходимостью будет диссипативным процессом.

6.1.5. Экономия пространства

Но кроме проблемы контроля ошибок, есть еще один ключевой вопрос, касающийся обратимых вычислений. Как распорядиться вспомогательным пространством, необходимым для того, чтобы сделать вычисление обратимым?

Обсуждая универсальность вентиля Тоффоли, мы видели, что в принципе можно выполнить любое обратимое вычисление, используя очень малое вспомогательное пространство. Но на практике может оказаться невероятно сложно понять, как выполнить конкретное вычисление, используя минимальное пространство, и во всяком случае экономия пространства может обернуться непомерным расходом времени.

Существует общая стратегия моделирования необратимого вычисления на обратимом компьютере. Каждый необратимый вентиль, NOT или COPY, можно моделировать вентилем Тоффоли, фиксируя входы и игнорируя выходы. Мы накапливаем и сохраняем весь «мусор» выходящих битов, которые необходимы, чтобы обратить этапы вычисления. Вычисление выполняется вплоть до завершения, после чего делается копия выхода. (Эта COPY-операция логически обратима.) Затем вычисление производится в обратном порядке, чтобы избавиться от «мусора» и вернуть все регистры в их начальные состояния. С помощью этой процедуры обратимая схема осуществляется примерно дважды, до тех пор, пока не будет выполнена моделируемая необратимая схема, а весь генерируемый при этом мусор – выброшен без какой-либо диссипации и, следовательно, энергетических затрат.

Эта процедура работает, но требует огромного пространства памяти – ее необходимый объем растет линейно с продолжительностью T моделируемого необратимого вычисления. Фактически пространство можно использовать гораздо более эффективно (лишь с минимальным замедлением), так что его необходимый объем растет как $\log T$ вместо T. (То есть существует универсальная схема, требующая пространства $\propto \log T$; конечно, моделируя конкретное вычисление, можно добиться даже лучшего результата.)

Чтобы эффективнее использовать пространство, разделим вычисление на более мелкие шаги приблизительно одинакового размера и, когда это возможно, будем обращать их в процессе вычисления. Однако, подобно тому как мы не в состоянии выполнить k-ый шаг вычисления до тех пор, пока не завершен $k-1$-ый шаг, мы не сможем *обратить* k-ый шаг, если предварительно был обращен $k-1$-ый шаг[1]. Необходимый объем пространства (чтобы хранить наш мусор) будет расти как максимальное значение числа шагов вперед за вычетом количества выполненных шагов назад.

Проблему, с которой мы столкнулись, можно сравнить с *обратимой иг-*

[1]Мы скромно предполагаем, что не настолько прозорливы, чтобы предвидеть, какая часть выхода $k-1$-го шага может потребоваться позже. Следовательно, мы сохраняем полную запись состояния машины после $k-1$-го шага, которая не должна удаляться до тех пор, пока не будет обновлена запись после завершения следующего шага.

рой камешками[1]. Выполняемые шаги образуют одномерный ориентированный граф с узлами, пронумерованными как $1, 2, 3, \ldots, T$. Выполнение k-го шага моделируется помещением камешка в k-ый узел графа, а выполнение k-го шага в обратном направлении моделируется удалением камешка из k-го узла. В начале игры нет узлов, занятых камешками, а с каждым ходом мы их добавляем или удаляем. Однако мы не можем поместить камешек в k-ый узел (за исключением $k = 1$) до тех пор, пока не заполнен $k-1$-ый, а также мы не можем удалить камешек из k-го узла (за исключением $k = 1$), если свободен $k-1$-ый узел. Задача в том, чтобы заполнить узел T (завершить вычисление), не используя большего, чем это необходимо, количества камешков (генерируя минимальный объем мусора).

Фактически с помощью n камешков мы можем достичь узла $T = 2^n - 1$, но продвинуться дальше не сможем.

Можно построить рекурсивную процедуру, позволяющую добраться до $T = 2^{n-1}$-го узла с помощью n камешков, оставляя в игре только один камешек. Пусть $F_1(k)$ обозначает помещение камешка в k-й узел, а $F_1^{-1}(k)$ — удаление камешка из k-го узла. Тогда[2]

$$F_2(1,2) = F_2(1)F_1(2)F_1^{-1}(1) \tag{6.47}$$

оставляет камешек в узле $k = 2$, используя максимум два камешка на промежуточных этапах. Аналогично

$$F_3(1,4) = F_2(1,2)F_2(3,4)F_2^{-1}(1,2) \tag{6.48}$$

достигает узла $k = 4$, используя максимум три камешка, а

$$F_4(1,8) = F_3(1,4)F_3(5,8)F_3^{-1}(1,4) \tag{6.49}$$

достигает узла $k = 8$, используя четыре камешка. Очевидно, можно построить процедуру $F_n(1, 2^{n-1})$, которая использует максимум n камешков и оставляет в игре один. [Программа

$$F_n(1,2^{n-1})F_{n-1}(2^{n-1}+1, 2^{n-1}+2^{n-2})\ldots F_1(2^n-1) \tag{6.50}$$

оставляет в игре все n камешков и позволяет заполнить максимально удаленный узел $k = 2^n - 1$.]

---

[1] Как было отмечено Беннетом. Относительно последнего обсуждения см.: M. Li and P. Vitanyi, *Reversibility and Adiabatic Computation: Trading Time and Space for Energy*, Proc. R. Soc. London, **A 452**, 769–789 (1996); quant-ph/9703022.

[2] Правые части (6.47) – (6.50) следует читать слева направо. Именно в этом порядке выполняются описываемые ими действия. — *Прим. ред.*

Понимаемая как программа для выполнения $T = 2^{n-1}$ шагов вычисления, эта стратегия игрока в камешки представляет собой моделирование, требующее роста пространства как $n \sim \log T$. Насколько продолжительным может быть это моделирование? На каждом этапе описанной выше рекурсивной процедуры два шага вперед заменялись двумя шагами вперед и одним назад. Следовательно, $T_{\text{irr}} = 2^n$ шагов необратимого вычисления моделируются $T_{\text{rev}} = 3^n$ шагами обратимого вычисления или

$$T_{\text{rev}} = \left(T_{\text{irr}}\right)^{\log 3/\log 2} = \left(T_{\text{irr}}\right)^{1,58}; \tag{6.51}$$

мы имеем умеренный степенной закон замедления.

В действительности мы можем уменьшить замедление до

$$T_{\text{rev}} \sim \left(T_{\text{irr}}\right)^{1+\varepsilon} \tag{6.52}$$

при любом $\varepsilon > 0$. Вместо того чтобы заменять два шага вперед двумя шагами вперед и одним назад, заменим ℓ шагов вперед ℓ шагами вперед и $\ell - 1$-им шагом назад. Состоящая из n этапов рекурсивная процедура достигает узла ℓ^n, используя максимум $n(\ell-1)+1$ камешков. Теперь мы имеем $T_{\text{irr}} = \ell^n$, а $T_{\text{rev}} = (2\ell-1)^n$, так что

$$T_{\text{rev}} \sim \left(T_{\text{irr}}\right)^{\log(2\ell-1)/\log \ell}; \tag{6.53}$$

показатель степени замедления равен

$$\frac{\log(2\ell-1)}{\log \ell} = \frac{\log 2\ell + \log\left(1-\frac{1}{2\ell}\right)}{\log \ell} \simeq 1 + \frac{\log 2}{\log \ell}, \tag{6.54}$$

а требуемое пространство растет как

$$S \simeq n\ell \simeq \ell \frac{\log T}{\log \ell}. \tag{6.55}$$

Таким образом, для любого фиксированного $\varepsilon > 0$ мы можем добиться S, растущего как $\log T$, и замедления, не большего чем $\left(T_{\text{irr}}\right)^{1+\varepsilon}$. (Для игры в камешки это не оптимальный способ, если наша цель — продвинуться как можно дальше, используя минимально возможное количество камешков. Мы используем больше камешков, чтобы добраться до T-го шага, зато делаем это быстрее.)

Итак, мы видим, что обратимая схема может успешно моделировать схему, построенную из необратимых вентилей, не требуя нереальных ресурсов памяти и не вызывая неразумно большого замедления. Почему это важно? Вас может беспокоить, что поскольку обратимое вычисление «труднее» необратимого, то классификация сложности зависит от того, какими вычислениями мы пользуемся, обратимыми или необратимыми. Однако это не так, поскольку необратимый компьютер легко моделируется обратимым.

6.2. Квантовые схемы

Теперь мы готовы сформулировать математическую модель квантового компьютера. Мы обобщим модель классической вычислительной схемы на модель квантовой вычислительной схемы.

Классический компьютер оперирует битами. Он оснащен конечным набором вентилей, которые могут применяться к множеству битов. Квантовый компьютер оперирует кубитами. Будем предполагать, что он тоже оснащен дискретным набором фундаментальных компонентов, называемых *квантовыми вентилями*. Каждый квантовый вентиль представляет собой унитарное преобразование, действующее на определенное число кубитов. В квантовых вычислениях конечное количество n кубитов первоначально полагаются имеющими значение $|00\ldots0\rangle$. Выполняемая схема построена из конечного числа квантовых вентилей, действующих на эти кубиты. Наконец, выполняется измерение фон Неймана всех кубитов (или некоторого подмножества кубитов), проецирующее каждый из них на базис $\{|0\rangle, |1\rangle\}$. Результат этого измерения является результатом вычисления.

Некоторые особенности этой модели требуют комментария.

(1) Неявно подразумевается, но очень важно, что гильбертово пространство прибора имеет естественное разложение на тензорное произведение пространств более низкой размерности, в данном случае – двумерных пространств кубитов. Конечно, вместо этого мы могли бы рассматривать тензорное произведение, допустим, кутритов. Но в любом случае мы считаем, что существует естественное разложение на подсистемы, которое соответствует квантовым вентилям, действующим одновременно только на несколько подсистем. С математической точки зрения это свойство вентилей является решающим для формулировки хорошо определенного понятия квантовой сложности. С физической точки зрения фундаментальной причиной естественного разложе-

ния на подсистемы является *локальность*; реальные квантовые вентили должны действовать в ограниченной области пространства, то есть компьютер разбивается на подсистемы, взаимодействующие только со своими ближайшими соседями.

(2) Так как унитарные преобразования образуют континуум, может показаться необязательным постулировать, что машина может выполнять только выбранные из дискретного множества квантовые операции. Тем не менее мы принимаем это ограничение, поскольку не хотим, сталкиваясь с выполнением нового вычисления, всякий раз изобретать его новую физическую реализацию.

(3) Мы могли бы допустить, чтобы наши квантовые вентили были супероператорами, а конечным измерением — ПОЗМ. Но поскольку мы можем просто моделировать супероператор, выполняя унитарное преобразование в расширенной системе, или — ПОЗМ, выполняя измерение фон Неймана в расширенной системе, сформулированная модель обладает достаточной общностью.

(4) Мы могли бы допустить, чтобы заключительное измерение было коллективным измерением или проектором на другой базис. Но любое такое измерение можно реализовать, выполняя подходящее унитарное преобразование после проецирования на стандартный базис $\{|0\rangle, |1\rangle\}^n$. Конечно, сложные коллективные измерения лишь с некоторыми затруднениями можно преобразовать в измерения в стандартном базисе и при характеристике сложности алгоритма эти трудности следует иметь в виду.

(5) Мы могли бы допустить наличие измерений на промежуточных этапах вычислений с последующим выбором квантовых вентилей, обусловленным результатами этих измерений. Но фактически тот же результат всегда может быть достигнут с помощью квантовой схемы, в которой все измерения отложены вплоть до ее окончания. (Хотя в принципе мы можем отложить измерения, на практике может оказаться полезным их выполнение на промежуточных этапах квантового алгоритма.)

Будучи унитарным преобразованием, квантовый вентиль обратим. Фактически классический обратимый компьютер представляет собой частный случай квантового компьютера. Классический обратимый вентиль

$$x^{(n)} \to y^{(n)} = f\left(x^{(n)}\right), \tag{6.56}$$

выполняющий перестановку n-битовых строк, может рассматриваться как унитарное преобразование, действующее на «вычислительный» базис $\{|x_i\rangle\}$ как

$$U : |x_i\rangle \rightarrow |y_i\rangle. \tag{6.57}$$

Это действие унитарно, поскольку все 2^n строк $|y_i\rangle$ взаимно ортогональны. Квантовое вычисление, построенное из таких классических вентилей, преобразует $|0\ldots0\rangle$ в одно из состояний вычислительного базиса, так что конечное измерение является детерминированным.

Имеется три главные проблемы, касающиеся нашей модели, к которым мы хотели бы обратиться. Первой из них является *универсальность*. Самое общее унитарное преобразование, которое может быть выполнено на n кубитах, является элементом $U(2^n)$. Наша модель могла бы оказаться неполной, если бы в $U(2^n)$ существовали такие преобразования, которые мы не могли бы выполнить. На самом деле мы увидим, что существует множество способов выбрать дискретный набор *универсальных квантовых вентилей*. Используя набор универсальных вентилей, можно построить схемы, вычисляющие унитарное преобразование, сколь угодно близкое к любому элементу $U(2^n)$.

Благодаря универсальности, существует также аппаратно-независимое понятие *квантовой сложности*. Мы можем определить новый класс сложности BQP — класс проблем принятия решения, которые с высокой вероятностью могут быть решены с помощью квантовой схемы полиномиального размера. Так как один универсальный квантовый компьютер может эффективно моделироваться другим, то этот класс не зависит от деталей аппаратного обеспечения (от выбранного нами набора универсальных вентилей).

Заметим, что квантовый компьютер может легко моделировать классический вероятностный компьютер: он может приготовить состояние $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, а затем спроецировать его на $\{|0\rangle, |1\rangle\}$, генерируя случайный бит. Следовательно, класс BPP несомненно содержится в BQP. Однако, как обсуждалось в первой главе, представляется достаточно разумным ожидать, что в действительности BQP шире, чем BPP, поскольку классический вероятностный компьютер не может легко моделировать квантовый компьютер. Фундаментальная трудность состоит в том, что гильбертово пространство n кубитов огромно, размерности 2^n, и, следовательно, математическое описание типичного вектора в этом пространстве исключительно сложно.

Вторая проблема — наилучшим образом характеризовать ресурсы, необходимые для моделирования квантового компьютера классическим.

Мы увидим, что, несмотря на обширность гильбертова пространства, классический компьютер может моделировать n-кубитовый квантовый компьютер, даже если его запас памяти ограничен, то есть полиномиален по n. Это означает, что BQP содержится в классе сложности $PSPACE$ проблем принятия решения, которые могут быть решены с использованием пространства полиномиального размера, но могут потребовать для этого экспоненциального времени. [Мы знаем, что NP также содержится в $PSPACE$, так как проверка $\tilde{C}(x^{(n)}, y^{(m)}) = 1$ для всех $y^{(m)}$ может быть выполнена с использованием полиномиального пространства.][1]

Третьей важной проблемой, к которой следует обратиться, является *точность*. Класс BQP формально определен при идеализированном предположении, что квантовые вентили могут выполняться с идеальной точностью. Ясно, что при любой реализации квантового вычисления очень важно ослабить это предположение. Семейство квантовых схем полиномиального размера, которое решает трудную проблему, не представляло бы большого интереса, если бы от используемых в схемах вентилей требовалась экспоненциальная точность. Мы покажем, что на самом деле это не так. Идеализированная квантовая схема из T вентилей с приемлемой точностью может моделироваться вентилями с шумом при условии, что вероятность ошибки на один вентиль пропорциональна $1/T$.

Таким образом, квантовые компьютеры бросают серьезный вызов сильному тезису Черча–Тьюринга, утверждающему, что любая физически разумная модель вычисления может быть смоделирована вероятностными классическими схемами с полиномиальным замедлением в худшем случае. Но до сих пор нет строгого доказательства того, что

$$BQP \neq BPP, \tag{6.58}$$

и в ближайшем будущем оно не предвидится[2]. Действительно, следствием было бы

$$BPP \neq PSPACE, \tag{6.59}$$

что решило бы один из давно стоящих, кардинальных открытых вопросов теории сложности.

Возможно, более реалистично надеяться на доказательство того, что $BPP \neq BQP$ вытекает из другого стандартного предположения теории сложности, такого как $P \neq NP$. Такое доказательство до сих пор

[1] В действительности в иерархии сложности существует еще одна ступенька, которая может разделять BQP и $PSPACE$; можно показать, что $BQP \subseteq P^{\#P} \subseteq PSPACE$, но ниже мы не будем рассматривать $P^{\#P}$.

[2] То есть не следует ожидать «переляпгивизированного доказательства». Разделение между BPP и BQP «относительно оракула» будет установлено ниже в этой главе.

не найдено. Но хотя мы все еще не в состоянии доказать, что квантовые компьютеры имеют возможности, выходящие далеко за пределы возможностей обычных компьютеров, тем не менее можно привести свидетельства, указывающие на то, что $BPP \neq BQP$. Мы увидим, что существуют проблемы, которые выглядят сложными (для классического вычисления), но тем не менее могут быть успешно решены с помощью квантовых схем.

Таким образом, кажется вероятным то, что классификация сложности будет зависеть от того, какой компьютер для решения задачи используется, классический или квантовый. Если такое разделение действительно существует, то именно квантовая классификация должна рассматриваться как более фундаментальная, поскольку она в большей степени опирается на физические законы, управляющие Вселенной.

6.2.1. Точность

Обсудим проблему точности. Представим, что мы хотим выполнить вычисление, в котором квантовые вентили $\mathbf{U}_1$, $\mathbf{U}_2, \ldots, \mathbf{U}_T$ последовательно применяются к начальному состоянию $|\varphi_0\rangle$. Состояние, приготовленное идеальной квантовой схемой, имеет вид

$$|\varphi_T\rangle = \mathbf{U}_T \mathbf{U}_{T-1} \ldots \mathbf{U}_2 \mathbf{U}_1 |\varphi_0\rangle. \tag{6.60}$$

Но в действительности наши вентили не являются идеально точными. Пытаясь применить унитарное преобразование $\mathbf{U}_t$, мы вместо этого применяем некоторое «близкое» унитарное преобразование $\tilde{\mathbf{U}}_t$. (Конечно, это не самый общий тип ошибки, который можно предположить, — унитарное преобразование $\mathbf{U}_t$ может оказаться замененным *супероператором*. В этом случае применимы рассуждения, подобные следующим ниже, но здесь мы ограничим наше внимание «унитарными ошибками».)

Ошибки приводят к тому, что действительное состояние компьютера удаляется от идеального. Как сильно оно удаляется? Пусть $|\varphi_t\rangle$ обозначает идеальное состояние после применения t квантовых вентилей, так что

$$|\varphi_t\rangle = \mathbf{U}_t |\varphi_{t-1}\rangle. \tag{6.61}$$

Но если мы применяем действительное преобразование $\tilde{\mathbf{U}}_t$, то

$$\tilde{\mathbf{U}}_t |\varphi_{t-1}\rangle = |\varphi_t\rangle + |E_t\rangle, \tag{6.62}$$

где

$$|E_t\rangle = (\tilde{\mathbf{U}}_t - \mathbf{U}_t)|\varphi_{t-1}\rangle \tag{6.63}$$

— ненормированный вектор. Если $|\tilde{\varphi}_t\rangle$ обозначает действительное состояние после t шагов, то

$$\begin{aligned} |\tilde{\varphi}_1\rangle &= |\varphi_1\rangle + |E_1\rangle, \\ |\tilde{\varphi}_2\rangle &= \tilde{\mathbf{U}}_2|\tilde{\varphi}_1\rangle = |\varphi_2\rangle + |E_2\rangle + \tilde{\mathbf{U}}_2|E_1\rangle \end{aligned} \tag{6.64}$$

и так далее; в конечном счете мы получим

$$\begin{aligned} |\tilde{\varphi}_T\rangle = |\varphi_T\rangle &+ |E_T\rangle + \tilde{\mathbf{U}}_T|E_{T-1}\rangle + \tilde{\mathbf{U}}_T\tilde{\mathbf{U}}_{T-1}|E_{T-2}\rangle \\ &+ \ldots + \tilde{\mathbf{U}}_T\tilde{\mathbf{U}}_{T-1}\ldots\tilde{\mathbf{U}}_2|E_1\rangle. \end{aligned} \tag{6.65}$$

Итак, мы представили разность между $|\tilde{\varphi}_T\rangle$ и $|\varphi_T\rangle$ в виде суммы T оставшихся слагаемых. Наихудший случай, дающий наибольшее отклонение $|\tilde{\varphi}_T\rangle$ от $|\varphi_T\rangle$, возникает, если все оставшиеся слагаемые ориентированы в одном направлении, так что ошибки интерферируют конструктивно. Следовательно,

$$\begin{aligned} \||\tilde{\varphi}_T\rangle - |\varphi_T\rangle\| \leqslant \||E_T\rangle\| + \||E_{T-1}\rangle\| + \\ + \ldots + \||E_2\rangle\| + \||E_1\rangle\|, \end{aligned} \tag{6.66}$$

где учтено, что $\|\mathbf{U}|E_i\rangle\| = \||E_i\rangle\|$ для любого унитарного $\mathbf{U}$.

Пусть $\|\mathbf{A}\|$ обозначает норму оператора $\mathbf{A}$, то есть максимум модуля его собственных значений. Тогда

$$\||E_t\rangle\| = \|(\tilde{\mathbf{U}}_t - \mathbf{U}_t)|\varphi_{t-1}\rangle\| \leqslant \|(\tilde{\mathbf{U}}_t - \mathbf{U}_t)\| \tag{6.67}$$

(поскольку $|\varphi_{t-1}\rangle$ нормирован). Предположим теперь, что при каждом значении t ошибка нашего квантового вентиля ограничена неравенством

$$\|(\tilde{\mathbf{U}}_t - \mathbf{U}_t)\| < \varepsilon. \tag{6.68}$$

Тогда после применения T квантовых вентилей мы имеем

$$\||\tilde{\varphi}_T\rangle - |\varphi_T\rangle\| < T\varepsilon; \tag{6.69}$$

в этом смысле накопление ошибки в состоянии растет пропорционально продолжительности вычисления.

Отклонение, ограниченное неравенством (6.68), может быть представлено в эквивалентной форме $\|\mathbf{W}_t - \mathbf{1}\|$, где $\mathbf{W}_t = \tilde{\mathbf{U}}_t \mathbf{U}_t^\dagger$. Так как оператор $\mathbf{W}_t$ унитарен, каждое его собственное число имеет вид фазы $e^{i\theta}$, а соответствующее собственное значение оператора $\mathbf{W}_t - \mathbf{1}$ имеет модуль

$$|e^{i\theta} - 1| = (2 - 2\cos\theta)^{1/2}, \tag{6.70}$$

так что (6.68) требует, чтобы каждое собственное значение удовлетворяло неравенству

$$\cos\theta > 1 - \frac{\varepsilon^2}{2} \tag{6.71}$$

(или $|\theta| \lesssim \varepsilon$ для малых ε). Природа неравенства (6.69) понятна. В каждый момент времени $|\tilde{\varphi}\rangle$ поворачивается относительно $|\varphi\rangle$ на угол порядка ε (в худшем случае), а расстояние между векторами возрастает максимум на величину порядка ε.

Какая точность является достаточно хорошей? На последнем этапе вычисления мы выполняем ортогональное измерение, а вероятность результата a в идеальном случае равна

$$P(a) = |\langle a|\varphi_T\rangle|^2. \tag{6.72}$$

Вследствие ошибок действительной вероятностью будет

$$\tilde{P}(a) = |\langle a|\tilde{\varphi}_T\rangle|^2. \tag{6.73}$$

Если действительный вектор близок к идеальному, то и распределения вероятностей тоже близки. Если мы просуммируем по ортонормированному базису $\{|a\rangle\}$, то получим

$$\sum_a |\tilde{P}(a) - P(a)| \leqslant 2\||\tilde{\varphi}_T\rangle - |\varphi_T\rangle\|, \tag{6.74}$$

как вы покажете в домашнем упражнении. Следовательно, если при больших T мы сохраняем неизменным (и малым) $T\varepsilon$, то ошибка в распределении вероятностей также остается фиксированной. В частности, если мы разработали квантовый алгоритм, который с вероятностью выше $\frac{1}{2} + \delta$ правильно решает проблему принятия решения (в идеальном случае), тогда с вероятностью, превышающей $\frac{1}{2}$, мы можем добиться успеха и с помощью наших шумящих вентилей, если действие этих вентилей может быть выполнено с точностью $T\varepsilon < O(\delta)$. Семейство квантовых схем может реально решать сложные проблемы в классе BQP до тех пор, пока мы в состоянии улучшать точность выполнения вентилей пропорционально объему вычислений.

6.2.2. $BQP \subseteq PSPACE$

Конечно, классический компьютер может моделировать любую квантовую схему. Но какой объем памяти ему для этого потребуется? Поскольку моделирование n-кубитовой схемы включает в себя манипулирование матрицами размера 2^n, то с наивной точки зрения может показаться, что для этого необходим экспоненциальный по n запас памяти. Однако теперь мы покажем, что с приемлемой точностью (хотя и очень медленно!) моделирование может быть выполнено в пространстве полиномиального размера. Это означает, что класс квантовой сложности BQP содержится в классе $PSPACE$ задач, которые могут быть решены с использованием пространства *полиномиального* размера.

Объектом классического моделирования является вычисление вероятности каждого возможного результата a заключительного измерения

$$\text{Prob}(a) = |\langle a|\mathbf{U}^{(T)}|0\rangle|^2, \tag{6.75}$$

где

$$\mathbf{U}^{(T)} = \mathbf{U}_T\mathbf{U}_{T-1}\ldots\mathbf{U}_2\mathbf{U}_1 \tag{6.76}$$

— произведение T квантовых вентилей. Каждый $\mathbf{U}_t$, действующий на n кубитов, может быть представлен унитарной $2^n \times 2^n$-матрицей, характеризуемой комплексными матричными элементами

$$\langle y|\mathbf{U}_t|x\rangle, \tag{6.77}$$

где $x, y \in \{0, 1, \ldots, 2^n - 1\}$. Явно выписывая произведение матриц, мы имеем

$$\langle a|\mathbf{U}^{(T)}|0\rangle = \sum_{x_t}\langle a|\mathbf{U}_T|x_{T-1}\rangle\langle x_{T-1}|\mathbf{U}_{T-1}|x_{T-2}\rangle\ldots \\ \ldots\langle x_2|\mathbf{U}_2|x_1\rangle\langle x_1|\mathbf{U}_1|0\rangle. \tag{6.78}$$

Уравнение (6.78) представляет собой вариант представления квантового вычисления «интегралом по траекториям» — амплитуда вероятности конечного результата a выражается в виде когерентной суммы амплитуд каждого из огромного количества $2^{n(T-1)}$ возможных вычислительных путей, начинающихся в точке 0 и после T шагов заканчивающихся в a.

Чтобы вычислить $\langle a|\mathbf{U}^{(T)}|0\rangle$, наш классический симулятор должен сложить $2^{n(T-1)}$ комплексных чисел в уравнении (6.78). Первая проблема, с которой мы встречаемся, состоит в том, что классические схемы конечного размера реализуют целочисленную арифметику, тогда как матричные

элементы $\langle y|\mathbf{U}_i|x\rangle$ не обязаны быть рациональными числами. Следовательно, классический симулятор должен выполнять приближенные вычисления с разумной точностью. Каждое из $2^{n(T-1)}$ слагаемых суммы представляет собой произведение T комплексных сомножителей. Накапливаемые ошибки непременно должны быть малыми, если мы выражаем матричные элементы с помощью m точных битов, где m велико по сравнению с $n(T-1)$. Следовательно, мы можем заменить каждый комплексный матричный элемент парой целых чисел определенного знака, принимающих значения $\{0, 1, 2, \ldots, 2^{m-1}\}$. Эти целые числа дают двоичное разложение вещественной и мнимой частей матричного элемента, выраженного с точностью 2^{-m}.

Нашему симулятору потребуется вычислить каждое слагаемое в (6.78) и накопить их полную сумму. Но каждое добавление требует только умеренного объема пространства памяти, и, более того, поскольку для следующего сложения необходимо сохранять только накопленную частичную сумму, не очень большое пространство требуется для суммирования всех слагаемых, даже если их экспоненциально много.

Итак, остается лишь рассмотреть вычисление типичного слагаемого суммы, произведения T матричных элементов. Нам потребуется классическая схема, вычисляющая

$$\langle y|\mathbf{U}_i|x\rangle; \tag{6.79}$$

эта схема принимает $2n$ входящих битов (x, y) и выдает на выходе $2m$-битовое (комплексное) значение матричного элемента. Имея схему, выполняющую эту функцию, легко построить схему, которая перемножает комплексные числа, не используя большого пространства.

Наконец, обратимся к свойствам, которые мы потребовали от набора квантовых вентилей, — это дискретное множество вентилей, каждый из которых действует на ограниченное количество кубитов. Поскольку имеется фиксированное (и конечное) количество вентилей, то существует лишь конечное количество вентилей-подпрограмм, с которым нашему симулятору необходимо уметь обращаться. А поскольку вентили действуют только на несколько кубитов, почти все их матричные элементы исчезают (если n велико), а значение $\langle y|\mathbf{U}|x\rangle$ может быть определено (с требуемой точностью) с помощью простой схемы, требующей незначительной памяти.

Например, в случае однокубитового вентиля, действующего на первый кубит,

$$\langle y_1 y_2 \ldots y_n|\mathbf{U}|x_1 x_2 \ldots x_n\rangle = 0, \quad \text{если} \quad x_2 x_3 \ldots x_n \neq y_2 y_3 \ldots y_n. \tag{6.80}$$

Простая схема может сравнить x_2 с y_2, x_3 с y_3 и так далее и дать на выходе

нуль, если равенство не выполняется. В случае равенства она выдает одно из четырех комплексных чисел

$$\langle y_1|\mathbf{U}_i|x_1\rangle \tag{6.81}$$

с m точными битами. Простая схема может закодировать $8m$ битов этой комплекснозначной 2×2-матрицы. Подобным образом простая схема, требующая пространство лишь полиномиального по n и m размера, может вычислить матричные элементы любого вентиля фиксированного размера.

Таким образом, классический компьютер с пространством, ограниченным сверху размером $\mathrm{poly}(n)$, может моделировать n-кубитовый универсальный квантовый компьютер и, следовательно, BQP $\subseteq$ PSPACE. Конечно, также очевидно, что описанное нами моделирование требует экспоненциального времени, так как нам необходимо вычислить сумму $2^{n(T-1)}$ комплексных чисел. (В действительности большинство слагаемых исчезает, но количество неисчезающих слагаемых остается экспоненциально большим.)

6.2.3. Универсальные квантовые вентили

Мы должны обратиться к еще одному фундаментальному вопросу, касающемуся квантовых вычислений, как построить адекватный набор квантовых вентилей? Другими словами, что образует универсальный квантовый компьютер?

Ответ вам понравится. Для реализации универсальных квантовых вычислений достаточно любого типичного двухкубитового вентиля. То есть, если мы можем применять эти вентили к любой паре кубитов, то любого из них, кроме множества меры нуль унитарных 4×4-матриц, достаточно, чтобы построить n-кубитовую схему, вычисляющую преобразование, сколь угодно близкое к любому элементу $U(2^n)$.

Математически это не особенно глубокий результат, но с физической точки зрения он очень интересен. Это означает, что в квантовом мире, пока мы можем придумывать типичные двухкубитовые взаимодействия и осуществлять их точно между любыми двумя кубитами, мы в состоянии вычислять что угодно, независимо от сложности. Нетривиальные вычисления в квантовой теории встречаются повсюду.

Кроме этого общего результата, интересно продемонстрировать и конкретные наборы универсальных вентилей, которые очень легко могут быть реализованы физически. Обсудим несколько примеров.

Существует несколько основных элементов, входящих в состав любого набора универсальных квантовых вентилей.

(1) Степени типичного вентиля. Рассмотрим «типичный» k-битовый вентиль. Это унитарная $2^k \times 2^k$-матрица $\mathbf{U}$ с собственными значениями $e^{i\theta_1}$, $e^{i\theta_2}, \ldots e^{i\theta_{2^k}}$. Для всех, кроме множества меры нуль, таких матриц каждое θ_i представляет собой иррациональное число, кратное π, и все θ_i несоизмеримы (каждое θ_i/θ_j тоже иррационально). Положительная целая степень $\mathbf{U}^n$ матрицы $\mathbf{U}$ имеет собственные значения

$$e^{in\theta_1}, \quad e^{in\theta_2}, \quad \ldots \quad e^{in\theta_{2^k}}. \tag{6.82}$$

Каждый такой список собственных значений определяет точку на 2^k-мерном торе (произведении 2^k окружностей). Так как n принимает целые положительные значения, эти точки плотно заполняют весь тор, если $\mathbf{U}$ является типичной. Если $\mathbf{U} = e^{i\mathbf{A}}$, то для любого вещественного λ положительные целые степени $\mathbf{U}$ сколь угодно близки к $\mathbf{U}(\lambda) = e^{i\lambda\mathbf{A}}$. Мы утверждаем, что любое $\mathbf{U}(\lambda)$ *достигается* положительными целыми степенями $\mathbf{U}$.

(2) Переключение входов и выходов. Имеется несколько (классических) преобразований, которые можно выполнить, всего лишь переставив метки k кубитов или, другими словами, применяя вентиль $\mathbf{U}$ к кубитам в другом порядке. Из $(2^k)!$ перестановок строк длиной k путем обмена кубитами можно реализовать $k!$ Если вентилем, применяемым к k кубитам в стандартном порядке является $\mathbf{U}$, а P – перестановка, осуществляемая путем обмена кубитами, то мы можем построить вентиль

$$\mathbf{U}' = P\mathbf{U}P^{-1} \tag{6.83}$$

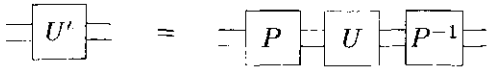
только с помощью переключения входов и выходов исходного вентиля. Например, обмен двумя кубитами осуществляет перестановку

$$P : |01\rangle \leftrightarrow |10\rangle \tag{6.84}$$

или

$$P = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \tag{6.85}$$

действующую в базисе $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. Переключая входы и выходы, мы получаем вентиль



Мы можем также построить любую целую положительную степень $\mathbf{U}'$: $\left(P\mathbf{U}P^{-1}\right)^n = P\mathbf{U}^nP^{-1}$.

(3) Замкнутая алгебра Ли. Мы уже замечали, что если вентиль $\mathbf{U} = e^{i\mathbf{A}}$ является типичным, то его степени плотны на торе $\left\{e^{i\lambda\mathbf{A}}\right\}$. Мы можем далее доказать, что если $\mathbf{U} = e^{i\mathbf{A}}$ и $\mathbf{U}' = e^{i\mathbf{B}}$ типичные вентили, то для любых вещественных α, β, γ из них можно составить вентиль, сколь угодно близкий к

$$e^{i(\alpha\mathbf{A}+\beta\mathbf{B})} \quad \text{или} \quad e^{-\gamma[\mathbf{A},\mathbf{B}]}. \tag{6.86}$$

Таким образом, «достижимые» преобразования образуют замкнутую *алгебру Ли*. Мы говорим, что $\mathbf{U} = e^{i\mathbf{A}}$ генерируется преобразованием $\mathbf{A}$; тогда если $\mathbf{A}$ и $\mathbf{B}$ являются типичными генераторами достижимых преобразований, то этим же свойством обладают их вещественные линейные комбинации и (умноженный на i) коммутатор.

Сначала заметим, что

$$\lim_{n\to\infty}\left(e^{i\alpha\mathbf{A}/n}e^{i\beta\mathbf{B}/n}\right)^n = \lim_{n\to\infty}\left(1+\frac{i}{n}(\alpha\mathbf{A}+\beta\mathbf{B})\right)^n = e^{i(\alpha\mathbf{A}+\beta\mathbf{B})}. \tag{6.87}$$

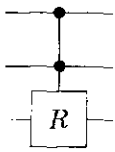
Следовательно, любое преобразование $e^{i(\alpha\mathbf{A}+\beta\mathbf{B})}$ достижимо, если таковыми являются $e^{i\alpha\mathbf{A}/n}$ и $e^{i\beta\mathbf{B}/n}$. Более того,

$$\lim_{n\to\infty}\left(e^{i\mathbf{B}/\sqrt{n}}e^{-i\mathbf{A}/\sqrt{n}}e^{-i\mathbf{B}/\sqrt{n}}e^{i\mathbf{A}/\sqrt{n}}\right)^n = \\ = \lim_{n\to\infty}\left[1-\frac{1}{n}(\mathbf{AB}-\mathbf{BA})\right]^n = e^{-[\mathbf{A},\mathbf{B}]}, \tag{6.88}$$

так что $e^{-[\mathbf{A},\mathbf{B}]}$ также достижимо.

Применяя результаты (1), (2) и (3), можно показать, что типичный двухкубитовый вентиль является универсальным.

1. Вентиль Дойча. Первым, обратившим внимание на существование универсального квантового вентиля, был Дэвид Дойч (1989 г.). Трехкубитовый универсальный вентиль Дойча является квантовым кузеном вентиля Тоффоли. Это дважды контролируемое $\mathbf{R}$-преобразование



которое применяет $\mathbf{R}$ к третьему кубиту, если два первых имеют значение, равное единице; в противном случае — действует тривиально. Здесь

$$\mathbf{R} = -i\mathbf{R}_x(\theta) = -i\exp\left(i\frac{\theta}{2}\boldsymbol{\sigma}_x\right) = -i\left(\cos\frac{\theta}{2} + i\boldsymbol{\sigma}_x\sin\frac{\theta}{2}\right) \tag{6.89}$$

представляет, с точностью до фазы, поворот на θ вокруг оси x, где θ некоторый несоизмеримый с π угол.

n-ая степень вентиля Дойча представляет собой дважды контролируемое $\mathbf{R}^n$. В частности, $\mathbf{R}^4 = \mathbf{R}_x(4\theta)$, так что все однокубитовые преобразования, генерируемые $\boldsymbol{\sigma}_x$, достигаются целыми степенями $\mathbf{R}$. Более того, его $(4n+1)$-ой степенью является преобразование

$$-i\left[\cos\frac{(4n+1)\theta}{2} + i\boldsymbol{\sigma}_x\sin\frac{(4n+1)\theta}{2}\right], \tag{6.90}$$

сколь угодно близкое к $\boldsymbol{\sigma}_x$. Следовательно, вентиль Тоффоли достигается целыми степенями вентиля Дойча, то есть вентиль Дойча является универсальным для классических вычислений.

Действуя на трехкубитовый вычислительный базис

$$\{|000\rangle,\ |001\rangle,\ |010\rangle,\ |011\rangle,\ |100\rangle,\ |101\rangle,\ |110\rangle,\ |111\rangle\}, \tag{6.91}$$

генератор вентиля Дойча переставляет два его последних элемента:

$$|110\rangle \leftrightarrow |111\rangle. \tag{6.92}$$

Изобразим эту 8×8-матрицу как

$$(\boldsymbol{\sigma}_x)_{67} = \left(\begin{array}{c|c} 0 & 0 \\ \hline 0 & \boldsymbol{\sigma}_x \end{array}\right). \tag{6.93}$$

С помощью вентиля Тоффоли можно выполнить перестановку любых этих восьми элементов, в частности, для любых m и n

$$P = (6m)(7n). \tag{6.94}$$

Следовательно, нам доступно любое преобразование, генерируемое

$$P(\boldsymbol{\sigma}_x)_{67}P^{-1} = (\boldsymbol{\sigma}_x)_{mn}. \tag{6.95}$$

Более того,

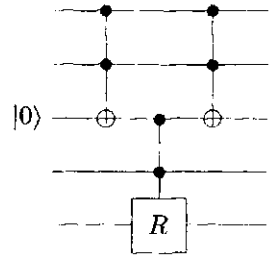
$$\left[(\sigma_x)_{56},(\sigma_x)_{67}\right]=\left[\begin{pmatrix}0&1&0\\1&0&0\\0&0&0\end{pmatrix},\begin{pmatrix}0&0&0\\0&0&1\\0&1&0\end{pmatrix}\right]=\begin{pmatrix}0&0&1\\0&0&0\\-1&0&0\end{pmatrix}=i(\sigma_y)_{57}. \tag{6.96}$$

Аналогично мы можем реализовать любое унитарное преобразование, генерируемое $(\sigma_y)_{mn}$. Наконец,

$$\left[(\sigma_x)_{mn},(\sigma_y)_{mn}\right]=2i(\sigma_z)_{mn}. \tag{6.97}$$

Следовательно, нам доступно любое преобразование, генерируемое линейной комбинацией матриц $(\sigma_{x,y,z})_{mn}$. Они образуют линейную оболочку алгебры Ли $SU(8)$, следовательно, мы можем генерировать любое трехкубитовое унитарное преобразование (за исключением несущественной общей фазы).

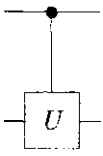
Вспомним теперь, что мы уже обнаружили, что, комбинируя трехбитовые вентили Тоффоли, можно построить n-битовый вентиль Тоффоли. Схема



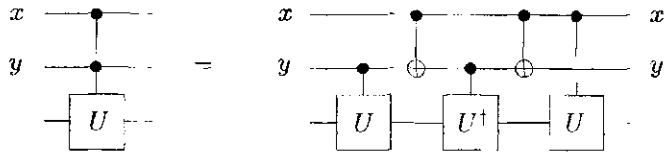
использует один вспомогательный бит, чтобы построить четырехбитовый вентиль Дойча (трижды контролируемое **R**) из одного трехбитового вентиля Дойча и двух трехбитовых вентилей Тоффоли. Аналогичная схема реализует n-битовый вентиль Дойча из одного трехбитового вентиля Дойча и двух $n-1$-битовых вентилей Тоффоли. Коль скоро мы имеем n-битовый вентиль Дойча, а также универсальное классическое вычисление, точно те же аргументы, что и выше, показывают, что можно реализовать любое преобразование из $SU(2^n)$.

2. Универсальные двухкубитовые вентили. Мы видели, что для универсальности классических обратимых вычислений необходимы трехбитовые универсальные вентили. Однако в квантовых вычислениях оказываются адекватными двухкубитовые вентили. Поскольку мы уже знаем, что вентиль Дойча универсален, мы можем установить это, показав, что он может быть образован комбинацией двухкубитовых вентилей.

Фактически, если



обозначает вентиль контролируемое U (унитарное 2×2-преобразование U применяется ко второму кубиту, если первый имеет значение, равное единице; в противном случае вентиль действует тривиально), то вентиль дважды контролируемое U получается с помощью схемы



Степенью U, примененной к третьему кубиту, является

$$y - (x \oplus y) + x - x + y - (x + y - 2xy) = 2xy. \tag{6.98}$$

Следовательно, вентиль Дойча можно построить из вентилей контролируемого U, контролируемого U^{-1} и контролируемого NOT, где

$$\mathrm{U}^2 = -i\mathrm{R}_x(\theta); \tag{6.99}$$

мы можем выбрать

$$\mathrm{U} = e^{-i\pi/4}\mathrm{R}_x\left(\frac{\theta}{2}\right). \tag{6.100}$$

Так как положительные степени U сколь угодно близко приближаются к σ_x и U^{-1}, то вентиль Дойча можно сконструировать из одного лишь контролируемого U. Следовательно, при иррациональном θ/π контролируемое $e^{-i\pi/4}\mathrm{R}_x\left(\frac{\theta}{2}\right)$ само по себе является универсальным вентилем.

(Заметим, что приведенная выше конструкция показывает, что, несмотря на то, что мы не можем построить вентиль Тоффоли из классических двухбитовых обратимых вентилей, его *можно* сконструировать из контролируемого «квадратного корня из NOT», то есть контролируемого U, квадрат которого $\mathrm{U}^2 = \sigma_x$.)

3. Типичные двухбитовые вентили. Итак, мы нашли конкретные двухбитовые вентили (контролируемые повороты), являющиеся универсальными. Следовательно, для универсальности вполне достаточно, если мы можем строить плотные в $U(4)$ преобразования, действующие на пары кубитов.

Однако на самом деле достаточно любого типичного двухкубитового вентиля, чтобы генерировать все преобразования из $U(4)$. Как мы видели, если $e^{i\mathbf{A}}$ – типичный элемент $U(4)$, то можно реализовать любое преобразование, генерируемое $\mathbf{A}$. Более того, можно реализовать любые преобразования, генерируемые элементом минимальной алгебры Ли, содержащей $\mathbf{A}$ и

$$\mathbf{B} = P\mathbf{A}P^{-1}, \tag{6.101}$$

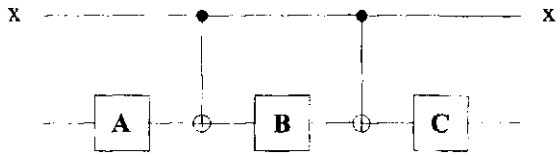
где P – перестановка ($|01\rangle \leftrightarrow |10\rangle$), получаемая переключением входов и выходов.

Рассмотрим теперь общее преобразование $\mathbf{A}$ [разложенное в базисе алгебры Ли $U(4)$], а также рассмотрим конкретную схему построения 16-ти элементов алгебры Ли путем последовательных коммутаций исходя из $\mathbf{A}$ и $\mathbf{B}$. Конструируемые таким образом элементы линейно независимы [а отсюда следует, что любое преобразование в $U(4)$ достижимо], если определитель конкретной 16×16-матрицы не равен нулю. Если этот определитель не обращается в нуль тождественно, то его нули появляются только на подмногообразии меры нуль. Фактически мы можем выбрать, допустим,

$$\mathbf{A} = (\alpha \mathbf{1} + \beta \boldsymbol{\sigma}_x + \gamma \boldsymbol{\sigma}_y)_{23} \tag{6.102}$$

(при несоизмеримых α, β, γ) и с помощью явных вычислений показать, что действительно, начиная с $\mathbf{A}$ и $\mathbf{B}$, последовательными коммутациями можно генерировать всю 16-мерную алгебру Ли. Следовательно, мы приходим к заключению, что неуспех генерирования всей алгебры $U(4)$ нетипичен, и обнаруживаем, что почти все двухкубитовые вентили универсальны.

4. Другие достаточные наборы вентилей. Очевидно также, что универсальные квантовые вычисления можно реализовать с помощью набора вентилей, состоящих из *классических* многокубитовых и квантовых однокубитовых вентилей. Например, можно увидеть, что универсальный набор образуется вентелем XOR, комбинируемым с однокубитовыми вентилями. Рассмотрим схему



применяющую ко второму кубиту преобразование $\mathbf{ABC}$, если $x = 0$, и $\mathbf{A}\sigma_x\mathbf{B}\sigma_x\mathbf{C}$, если $x = 1$. Если мы можем подобрать такие $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$, что

$$\begin{aligned} \mathbf{ABC} &= \mathbf{1}, \\ \mathbf{A}\sigma_x\mathbf{B}\sigma_x\mathbf{C} &= \mathbf{U}, \end{aligned} \tag{6.103}$$

тогда эта схема функционирует как вентиль контролируемое $\mathbf{U}$. Фактически для любого унитарного $\mathbf{U}$ с единичным определителем существуют унитарные 2×2-преобразования $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$ с такими свойствами (как вы покажете в упражнении). Следовательно, XOR в совокупности с произвольными однокубитовыми преобразованиями образуют универсальный набор. Конечно, двух типичных (некоммутирующих) однокубитовых преобразований достаточно, чтобы добиться чего угодно. В действительности с помощью XOR-а и *единственного* типичного однокубитового поворота мы можем построить второй однокубитовый поворот, не коммутирующий с первым. Таким образом, XOR вместе со всего лишь одним однокубитовым вентилем образует универсальный набор вентилей.

Если мы способны реализовать вентиль Тоффоли, тогда для универсальных вычислений достаточно даже некоторых нетипичных однокубитовых преобразований. Например (еще одно упражнение), вентиль Тоффоли совместно с поворотами на $\pi/2$ вокруг осей x и z представляет собой универсальный набор.

5. Точность. Наше обсуждение универсальности сфокусировалось на *достижимости*, оставив без внимания *сложность*. Мы всего лишь установили, что можем построить квантовую схему, сколь угодно близкую к требуемому элементу из $U(2^n)$, но не рассмотрели размер необходимой нам схемы. Однако с точки зрения теории квантовой сложности универсальность очень важна, поскольку она означает, что с приемлемой точностью и разумным замедлением один квантовый компьютер может моделировать другой.

В действительности до сих пор мы были не очень точны в вопросе о том, что означает для одного унитарного преобразования быть «близким» к другому; для этого следует определить топологию. Одна возможность представляет собой использование той же нормы, что и в предыдущем обсуждении точности. Тогда расстоянием между матрицами $\mathbf{U}$ и $\mathbf{W}$ является $\|\mathbf{U} - \mathbf{W}\|$. Еще одна естественная топология связана с внутренним произведением

$$\langle \mathbf{W}|\mathbf{U}\rangle = \operatorname{tr} \mathbf{W}^\dagger\mathbf{U} \tag{6.104}$$

(если $\mathbf{U}$ и $\mathbf{W}$ являются $N \times N$-матрицами, то это в точности обычное внутреннее произведение в $\mathbb{C}^{N^2}$, в котором $\mathbf{U}$ рассматривается как N^2-компонентный вектор). Тогда мы можем определить квадрат расстояния между матрицами как

$$\|\mathbf{U} - \mathbf{W}\|^2 = (\mathbf{U} - \mathbf{W}|\mathbf{U} - \mathbf{W}). \tag{6.105}$$

Для анализа сложности подходит практически любая разумная топология.

Решающим моментом является то, что, имея любой универсальный набор вентилей, мы можем подойти на расстояние ε к любому желаемому преобразованию, действующему на фиксированное количество кубитов, используя квантовую схему, размер которой ограничен сверху полиномиально по ε^{-1}. Следовательно, один универсальный квантовый компьютер может моделировать другой с точностью ε и не хуже, чем с полиномиальным по ε^{-1} фактором замедления. Теперь нам уже понятно: чтобы иметь высокую вероятность получения правильного ответа при выполнении квантовой схемы размера T, необходимо обеспечить выполнение каждого квантового вентиля с точностью порядка T^{-1}. Следовательно, если вы имеете семейство квантовых схем полиномиального размера, которые выполняет ваш квантовый компьютер, то я могу изобрести семейство схем полиномиального размера, которые выполняет моя машина и с приемлемой точностью эмулирует вашу.

Почему схема $\mathrm{poly}(\varepsilon^{-1})$-размера может достичь данного k-кубитового преобразования $\mathbf{U}$ в пределах расстояния ε? Мы знаем, например, что положительные целые степени типичного k-кубитового $e^{i\mathbf{A}}$ плотны на 2^k-торе $\{e^{i\lambda\mathbf{A}}\}$. Область тора в пределах расстояния ε до любой заданной точки имеет объем порядка ε^{2^k}. Следовательно, с помощью $\left(e^{i\mathbf{A}}\right)^n$ при некотором целом n порядка ε^{-2^k} мы можем асимптотически (при достаточно малом ε) достичь любого преобразования $\{e^{i\lambda\mathbf{A}}\}$ с точностью не хуже ε. Нам также известно, что, используя схемы фиксированного размера (независимого от ε), мы можем получить преобразования $\{e^{i\mathbf{A}_a}\}$, где $\mathbf{A}_a$ образуют линейную оболочку полной алгебры Ли $U(2^k)$. Тогда также с полиномиальной сходимостью мы можем аппроксимировать любое $\exp\left(i\sum_a \alpha_a \mathbf{A}_a\right)$, как в уравнении (6.87).

В принципе мы способны добиться гораздо лучшего результата, достигая желаемого k-кубитового унитарного преобразования с точностью не хуже ε с помощью только $\mathrm{poly}\left(\log(\varepsilon^{-1})\right)$ квантовых вентилей. Так как количество схем размера T, которые мы можем построить, действуя на k кубитов, экспоненциально по T, а схемы заполняют $U(2^k)$ примерно однородно,

то должна существовать схема размера T, достигающая в пределах расстояния порядка ϵ^{-T} любой точки в $U(2^k)$. Однако это может оказаться трудной вычислительной задачей – *классическим способом* разработать схему, экспоненциально близко подходящую к унитарному преобразованию, которого мы пытаемся достичь. Поэтому было бы нечестно опираться на эту более эффективную конструкцию в асимптотическом анализе квантовой сложности.

6.3. Некоторые квантовые алгоритмы

Хотя мы по-прежнему не в состоянии показать, что $BPP \neq BQP$, существует три подхода, которым можно последовать, чтобы изучить различия между возможностями классических и квантовых компьютеров.

(1) Неэкспоненциальное ускорение. Мы можем найти квантовые алгоритмы, которые заметно быстрее лучших классических алгоритмов, но *не экспоненциально* быстрее. Эти алгоритмы не проливают свет на общепринятую классификацию сложности. Но они демонстрируют характер разделения между задачами, которые могут выполнять классические и квантовые компьютеры. Пример: гроверовское квантовое ускорение поиска в неструктурированной базе данных.

(2) «Релятивизированное» экспоненциальное ускорение. Мы можем рассмотреть проблему анализа содержимого «квантового черного ящика». Ящик выполняет *a priori* неизвестное унитарное преобразование. Мы можем приготовить для него входные данные и измерить его результат; наша задача – определить, что делает ящик. Оказывается возможным доказать, что существуют квантовые ящики (специалисты по теории вычислений называют их оракулами[1]), обладающие следующим свойством: загружая ящик квантовыми суперпозициями, можно узнать, что находится внутри него, с *экспоненциальным* ускорением по сравнению с тем, как много времени пришлось бы потратить, если бы нам были разрешены только классические входные данные. Специалист по теории вычислений сказал бы, что $BPP \neq BQP$ «относительно оракула». Пример: саймоновское экспоненциальное квантовое ускорение отыскания периода функции «2 в 1».

[1]Термин «оракул» означает, что ящик отвечает на вопрос *немедленно*; то есть время, затрачиваемое на его работу, не включается в анализ сложности.

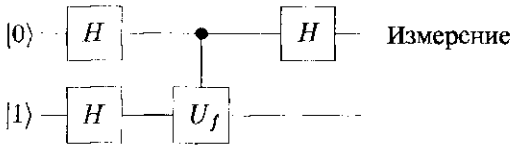
(3) Экспоненциальное ускорение для «по-видимому» трудных задач. Мы можем продемонстрировать квантовый алгоритм, решающий в течение полиномиального времени задачу, которая с классической точки зрения выглядит сложной, то есть серьезно подозревается (хотя и не доказано), что эта задача не принадлежит BPP. Пример: алгоритм факторизации Шора.

1. Проблема Дойча. Мы обсудим примеры из всех трех подходов. Но для начала разомнемся, вспомнив пример простого квантового алгоритма, который предварительно обсуждался в разделе 1.5: алгоритм Дойча для различения между постоянной и сбалансированной функциями $f: \{0,1\} \to \{0,1\}$. Нам предоставлен квантовый черный ящик, вычисляющий $f(x)$; то есть приводящий в действие двухкубитовое унитарное преобразование

$$U_f : |x\rangle|y\rangle \to |x\rangle|y \oplus f(x)\rangle, \tag{6.106}$$

которое инвертирует второй кубит, если $f(\text{первый кубит}) = 1$. Наша задача состоит в том, чтобы определить, выполняется ли $f(0) = f(1)$. Если мы ограничены «классическими» входными данными $|0\rangle$ и $|1\rangle$, то, чтобы получить ответ, нам необходимо обратиться к ящику дважды ($x = 0$ и $x = 1$). Но если нам позволено ввести когерентную суперпозицию этих «классических» состояний, то достаточно одного раза.

Квантовой схемой, решающей эту проблему (обсуждавшуюся в разделе 1.5), является



Здесь H обозначает преобразование Адамара

$$\mathbf{H} : |x\rangle \to \frac{1}{\sqrt{2}} \sum_y (-1)^{xy} |y\rangle \tag{6.107}$$

или

$$\begin{aligned} \mathbf{H} : |0\rangle &\to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \\ |1\rangle &\to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle); \end{aligned} \tag{6.108}$$

то есть **H** представляет собой 2×2-матрицу

$$\mathbf{H} : \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{6.109}$$

Схема преобразует вход $|0\rangle|1\rangle$ в

$$\begin{aligned} |0\rangle|1\rangle &\to \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) \\ &\to \frac{1}{2}\Big[(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\Big](|0\rangle - |1\rangle) \\ &\to \frac{1}{2}\Big\{\Big[(-1)^{f(0)} + (-1)^{f(1)}\Big]|0\rangle \\ &\quad + \Big[(-1)^{f(0)} - (-1)^{f(1)}\Big]|1\rangle\Big\}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \end{aligned} \tag{6.110}$$

Тогда при измерении первого кубита с вероятностью единица будет получен результат $|0\rangle$, если $f(0) = f(1)$ (постоянная функция), и с вероятностью единица — результат $|1\rangle$, если $f(0) \neq f(1)$ (сбалансированная функция).

Квантовый компьютер обладает преимуществом перед классическим компьютером, поскольку он может привлечь *квантовый параллелизм*. Так как мы вводим суперпозицию состояний $|0\rangle$ и $|1\rangle$, выход чувствителен к обоим значениям $f(0)$ и $f(1)$, даже если мы обратились к ящику только один раз.

2. Проблема Дойча–Йожы. Рассмотрим теперь некоторые обобщения проблемы Дойча. По-прежнему будем предполагать, что нам нужно анализировать квантовый черный ящик («квантовый оракул»). Но в надежде узнать что-нибудь о сложности мы будем представлять, что имеем семейство черных ящиков с переменным размером входа. Нас интересует, как время, необходимое для определения того, что происходит внутри ящика, зависит от размера входа (где «время» измеряется тем, сколько раз мы обращаемся к ящику с вопросом).

В *задаче Дойча–Йожы* нам предоставлен квантовый черный ящик, который вычисляет функцию, преобразуя n битов в один:

$$f : \{0,1\}^n \to \{0,1\}, \tag{6.111}$$

причем у нас есть все основания полагать, что f — постоянная [$f(x) = c$ для всех x] или сбалансированная [$f(x) = 0$ для ровно половины возможных значений входа]. Мы должны решить проблему принятия решения: является ли f постоянной или сбалансированной?

Фактически, используя ту же схему, что и для решения проблемы Дойча (но с x, расширенным от одного до n битов), мы также можем решить и эту проблему, обращаясь к ящику только один раз. Заметим, что если n вентилей Адамара параллельно применяются к n кубитам

$$\mathbf{H}^{(n)} = \mathbf{H} \otimes \mathbf{H} \otimes \ldots \otimes \mathbf{H}, \tag{6.112}$$

то n-кубитовое состояние преобразуется как

$$\mathbf{H}^{(n)}\colon |x\rangle \to \prod_{i=1}^{n} \left[\frac{1}{\sqrt{2}} \sum_{y_i=\{0,1\}} (-1)^{x_i y_i} |y_i\rangle \right] \equiv \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} (-1)^{x\cdot y} |y\rangle, \tag{6.113}$$

где x, y представляют n-битовые строки, а $x \cdot y$ обозначает *побитовое* AND (или скалярное произведение по модулю два):

$$x \cdot y = (x_1 \wedge y_1) \oplus (x_2 \wedge y_2) \oplus \ldots \oplus (x_n \wedge y_n). \tag{6.114}$$

Действуя на вход $(|0\rangle)^n|1\rangle$, схема преобразует его следующим образом:

$$\begin{aligned} (|0\rangle)^n|1\rangle &\to \left(\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle \right) \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ &\to \left(\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle \right) \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ &\to \left(\frac{1}{2^n} \sum_{x=0}^{2^n-1} \sum_{y=0}^{2^n-1} (-1)^{f(x)} (-1)^{x\cdot y} |y\rangle \right) \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \end{aligned} \tag{6.115}$$

Теперь вычислим сумму

$$\frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)} (-1)^{x\cdot y}. \tag{6.116}$$

Если f — постоянная функция, то эта сумма равна

$$(-1)^{f(x)} \left(\frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{x\cdot y} \right) = (-1)^{f(x)} \delta_{y,0}; \tag{6.117}$$

она обращается в нуль, за исключением случая, когда $y = 0$. Следовательно, при измерении n-битового выходного регистра с вероятностью единица будет получен результат $|y = 0\rangle \equiv (|0\rangle)^n$. Но если функция f сбалансирована, то при $y = 0$ сумма (6.116) становится равной

$$\frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)} = 0 \tag{6.118}$$

[поскольку половина слагаемых равны $(+1)$, а другая половина $-(-1)$]. Следовательно, вероятность получения результата измерения $|y = 0\rangle$ равна нулю.

Мы приходим к выводу, что квантовому оракулу достаточно одного вопроса, чтобы со 100% уверенностью различить постоянную и сбалансированную функции. Результат измерения $y = 0$ означает, что f — постоянная, любой другой результат — сбалансированная.

Итак, квантовое вычисление изящно решает эту задачу, но действительно ли это трудная проблема с классической точки зрения? Ограничиваясь вводом классических состояний $|x\rangle$, мы можем задавать вопрос оракулу неоднократно, всякий раз выбирая ввод x случайным образом (без возврата). Как только будут получены различные ответы на два различных вопроса, мы определим, что функция сбалансирована (не постоянная). Но если функция фактически является постоянной, мы не будем *уверены* в том, что это действительно так, до тех пор пока не предложим $2^{n-1} + 1$ вопросов, получая всякий раз один и тот же ответ. В противоположность этому квантовое вычисление дает определенный ответ всего лишь в один прием. В этом смысле (если мы требуем абсолютной определенности) классическое вычисление требует экспоненциального по n количества вопросов, тогда как квантовое вычисление — нет, следовательно, можно говорить об экспоненциальном ускорении.

Но может быть неразумно требовать абсолютной определенности от классического вычисления (в частности, так как любой реальный компьютер подвержен ошибкам, то и квантовый компьютер также будет не способен достигать абсолютной надежности). Допустим, что нас удовлетворяет предположение о сбалансированности или постоянстве с вероятностью успеха

$$P(\text{success}) > 1 - \varepsilon. \tag{6.119}$$

Если функция действительно сбалансирована, то вероятность получения всякий раз одного и того же ответа на k заданных вопросов равна $p = 2^{-(k-1)}$. Если после получения одного и того же ответа k раз под-

ряд мы сделаем предположение, что функция постоянна, быстрый бейесовский анализ показывает, что вероятность того, что наша догадка ошибочна, равна $\frac{1}{2^{k-1}+1}$ (в предположении, что сбалансированность и постоянство *a priori* равновероятны). Итак, если мы высказываем догадку после k вопросов, то вероятность ее ошибочности

$$1 - P(\text{success}) = \frac{1}{2^{k-1}(2^{k-1}+1)}. \tag{6.120}$$

Следовательно, мы можем достичь вероятности успеха $1-\varepsilon$ при $\varepsilon^{-1} = 2^{k-1}(2^{k-1}+1)$ или при $k \sim \frac{1}{2}\log\frac{1}{\varepsilon}$. А так как экспоненциально высокая вероятность успеха достигается с помощью полиномиального количества попыток, то на самом деле незаконно говорить, что проблема является трудной.

3. Задача Бернштейна–Вазирани. Точно такая же схема может быть использована для решения другого варанта задачи Дойча–Йожы. Предположим, что наш квантовый черный ящик вычисляет одну из функций f_a, где

$$f_a(x) = a \cdot x, \tag{6.121}$$

а a представляет собой n-битовую строку. Наше задача — определить a.

Квантовый алгоритм может с определенностью решить эту задачу, получив только один (n-кубитовый) квантовый вопрос. Для этой конкретной функции квантовое состояние в уравнении (6.115) имеет вид

$$\frac{1}{2^n}\sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1}(-1)^{a\cdot x}(-1)^{x\cdot y}|y\rangle. \tag{6.122}$$

Но фактически

$$\frac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{a\cdot x}(-1)^{x\cdot y} = \delta_{a,y}, \tag{6.123}$$

то есть этим состоянием является $|a\rangle$. Мы можем выполнить схему один раз и измерить n-кубитовый регистр, обнаружив с вероятностью единица n-битовую строку a.

Если разрешены только классические вопросы, то на каждый из них мы получаем только один бит информации и для определения значения a требуется n вопросов. Следовательно, мы имеем четкую границу между квантовой и классической сложностью задачи. Правда, этот пример не

вскрывает соотношения между BPP и BQP, поскольку классическая задача не является трудной. Количество вопросов, необходимых с классической точки зрения, всего лишь линейно, а не экспоненциально по размеру входа.

4. Задача Саймона. Бернштейну и Вазирани удалось сформулировать вариант предыдущей задачи, который *является* классически трудным, и, таким образом, впервые установить «релятивизированную» границу между квантовой и классической сложностью. Мы найдем более поучительным рассмотреть более простой пример, несколько позднее предложенный Даниэлем Саймоном.

Снова нам предоставлен квантовый черный ящик, и на этот раз мы уверены в том, что он вычисляет функцию «2 в 1»

$$f: \{0,1\}^n \rightarrow \{0,1\}^n. \tag{6.124}$$

Более того, функция имеет период, определяемый n-битовой строкой a; то есть

$$f(x) = f(y), \quad \text{если} \quad y = x \oplus a, \tag{6.125}$$

где $\oplus$ — побитовая XOR-операция. [То есть a является периодом, если мы рассматриваем x принимающим значения из $(Z_2)^n$, а не из Z_{2^n}.[1]] Это все, что нам известно об f. Наша задача — определить значение a.

Эта задача классически *трудная*. Нам необходимо обратиться к оракулу экспоненциально большое количество раз, чтобы иметь какую-нибудь разумную вероятность определения a. Мы ничего не узнаем, пока нам не повезет выбрать два вопроса x и y, которые случайно окажутся удовлетворяющими $x \oplus a = y$. Допустим, например, что мы выбираем $2^{n/4}$ вопросов. Количество пар вопросов меньше чем $\left(2^{n/4}\right)^2$, и для каждой пары $\{x, y\}$ вероятность того, что $x \oplus a = y$, равна 2^{-n}. Следовательно, вероятность успешного отыскания a меньше, чем

$$2^{-n}\left(2^{n/4}\right)^2 = 2^{-n/2}; \tag{6.126}$$

даже при экспоненциально большом количестве вопросов вероятность успеха экспоненциально мала.

Если угодно, эту задачу можно сформулировать как проблему принятия решения: функция f является или одно-однозначной (1 в 1), или отображает два в одно (2 в 1) с некоторым случайно выбранным периодом a;

[1] $(Z_2)^n$ — группа, элементами которой являются двоичные строки длины n. Групповая операция представляет собой побитовое сложение по модулю 2. Z_{2^n} — группа остатков от сложения по модулю 2^n. — *Прим. ред.*

обе эти возможности имеют априорные вероятности $1/2$. Нам нужно определить, является ли функция 1 в 1 или 2 в 1. Тогда после $2^{n/4}$ классических вопросов вероятность корректной догадки удовлетворяет неравенству

$$P(\text{success}) < \frac{1}{2} + \frac{1}{2^{n/2}} \tag{6.127}$$

и не удаляется от $1/2$ при больших значениях n.

Но для квантовых вопросов проблема является простой! Используемая нами схема, по существу, та же, что и выше, но теперь *оба* регистра расширены до n кубитов. Мы готовим равновзвешенную суперпозицию всех n-битовых строк (действуя на $|0\rangle$ преобразованием $\mathbf{H}^{(n)}$), а затем обращаемся к оракулу:

$$U_f : \left(\sum_{x=0}^{2^n-1} |x\rangle \right) |0\rangle \rightarrow \sum_{x=0}^{2^n-1} |x\rangle |f(x)\rangle. \tag{6.128}$$

Теперь мы измеряем второй регистр. (Этот этап на самом деле не обязателен, но для ясности изложения я включаю его сюда.) Результатом измерения является значение, случайно выбранное из 2^n равновероятных значений $f(x)$. Допустим, результатом является $f(x_0)$. Тогда, поскольку оба значения, x_0 и $x_0 \oplus a$, и только они отображаются функцией f на $f(x_0)$, мы приготовили состояние

$$\frac{1}{\sqrt{2}}(|x_0\rangle + |x_0 \oplus a\rangle) \tag{6.129}$$

в первом регистре.

Теперь мы хотим извлечь некоторую информацию относительно a. Очевидно, что на этом этапе было бы бесполезно измерять регистр (в вычислительном базисе). Мы получили бы результат x_0 или $x_0 \oplus a$ с вероятностью $1/2$ каждый, но ни тот, ни другой ничего не сказал бы о значении a.

Но представим теперь, что непосредственно перед измерением мы применили к регистру преобразование Адамара $\mathbf{H}^{(n)}$:

$$\begin{aligned}
\mathbf{H}^{(n)} : \frac{1}{\sqrt{2}} (|x_0\rangle + |x_0 \oplus a\rangle) &\rightarrow \\
&\rightarrow \frac{1}{2^{(n-1)/2}} \sum_{y=0}^{2^n-1} \left[(-1)^{x_0 \cdot y} + (-1)^{(x_0 \oplus a) \cdot y} \right] |y\rangle = \\
&= \frac{1}{2^{(n-1)/2}} \sum_{a \cdot y = 0} (-1)^{x_0 \cdot y} |y\rangle.
\end{aligned} \tag{6.130}$$

Если $a \cdot y = 1$, то слагаемые в коэффициенте перед $|y\rangle$ интерферируют деструктивно. Следовательно, в сумме по y выживают только состояния с $a \cdot y = 0$. Тогда результатом измерения является случайным образом выбранное из всех возможных значений y, появляющихся с вероятностью $2^{-(n-1)}$, таких, что $a \cdot y = 0$.

Мы многократно повторяем этот алгоритм, получая всякий раз еще одно значение y, удовлетворяющее $a \cdot y = 0$. Как только мы найдем n таких линейно независимых значений $\{y_1, y_2, y_3, \ldots y_n\}$ [то есть линейно независимых над $(Z_2)^n$], мы можем решить уравнения

$$\begin{aligned} y_1 \cdot a &= 0, \\ y_2 \cdot a &= 0, \\ &\vdots \\ y_n \cdot a &= 0, \end{aligned} \tag{6.131}$$

чтобы определить единственное значение a, и, таким образом, решить поставленную задачу. Нетрудно видеть, что с помощью $O(n)$ повторений мы можем достичь вероятности успеха, экспоненциально близкой к единице.

Итак, наконец-то мы нашли пример задачи, которую можно решить за полиномиальное время, используя квантовые суперпозиции для данного частного типа оракула, тогда как если ограничиться классическими вопросами, то для этого потребуется экспоненциальное время. Специалист по теории вычислений мог бы сказать:

Существует оракул, относительно которого $BQP \neq BPP$

Заметим, что всякий раз, когда мы сравниваем классическую и квантовую сложность относительно оракула, мы рассматриваем квантовый оракул (вопросами и ответами являются состояния в гильбертовом пространстве), но с выделенным ортонормированным базисом. Если мы предлагаем классический вопрос (элемент выделенного базиса), то всегда получаем классический ответ (другой элемент базиса). Проблема в том, можем ли мы достичь существенного ускорения, выбирая более общие, квантовые, вопросы.

6.4. Квантовый поиск в базе данных

Следующий алгоритм, который мы изучим, подобно алгоритму Саймона, также демонстрирует ускорение по отношению к тому, чего мы мо-

жем достичь с помощью классических вычислений. Однако в противоположность экспоненциальному ускорению решения задачи Саймона в этом случае ускорение только квадратично (квантовое время растет как квадратный корень классического времени). Несмотря на это, результат (открытый Л. Гровером) чрезвычайно интересен ввиду большой полезности этого алгоритма[1].

Рассматриваемая эвристически, проблема, к которой мы обратимся, выглядит так: мы столкнулись с очень большой неструктурированной базой данных, содержащей $N \gg 1$ отдельных объектов, а нам необходимо локализовать один конкретный объект, одним словом, найти иголку в стоге сена. С математической точки зрения база данных представлена таблицей или функцией $f(x)$ с $x \in \{0, 1, 2, \ldots N-1\}$. Мы уверены в том, что отдельная запись a появляется в таблице только один раз, то есть что $f(x) = a$ только при одном значении x. Проблема состоит в том, чтобы по данному a отыскать это значение x.

Если база данных подходящим образом *структурирована*, то поиск x прост. Возможно, кто-то был настолько любезен, что записал значения a в возрастающем порядке. Тогда мы можем найти x, просмотрев только $\log_2 N$ отдельных записей в таблице. Предположим, что $N = 2^n$ является степенью двойки. Мы сначала найдем $f(x)$ при $x = 2^{n-1} - 1$ и проверим, больше ли $f(x)$, чем a. Если да, то мы найдем следующее f при $x = 2^{n-2} - 1$ *и так далее*. С каждым взглядом на таблицу мы вдвое сокращаем количество кандидатов среди значений x, так что достаточно n взглядов, чтобы просмотреть все 2^n рассортированных записей. Вы можете использовать этот алгоритм, чтобы отыскать номер в телефонной книге Лос Анжелеса, поскольку в ней имена записаны в алфавитном порядке.

Но допустим, что вы знаете чей-то номер телефона, и вы хотите узнать его *имя*. Если у вас нет возможности заглянуть в обратный справочник, то процедура поиска будет утомительна. Ваши шансы таковы: вам придется проверить порядочное количество отдельных записей в телефонной книге, прежде чем вы наткнетесь на известный вам номер.

Фактически, если N номеров записаны в случайном порядке, то вам необходимо просмотреть $N/2$ номеров, прежде чем с вероятностью $P = 1/2$ найти его номер (и, следовательно, его имя). Обнаруженное Гровером состоит в том, что если вы имеете квантовую телефонную книгу, то, обратившись к ней примерно только $\sqrt{N}$ раз, вы можете с высокой вероятностью узнать интересующее вас имя.

Эта задача тоже может быть сформулирована как проблема оракула

[1] L. K. Grover, *Quantum Mechanics Helps in Searching for a Needle in a Haystack*, Phys. Rev. Lett., **79**, 325–328 (1997); quant-ph/9706033.

или «черного ящика». В этом случае оракулом является телефонная книга или справочная таблица. Мы можем ввести имя (значение x), а оракул – выдать нуль, если $f(x) \neq a$, или единицу, если $f(x) = a$. Наша задача – как можно быстрее найти значение x, при котором

$$f(x) = a. \tag{6.132}$$

Почему эта проблема важна? Возможно, вы никогда не пытались найти в телефонной книге имя, которое соответствует данному номеру, но если бы это не было так трудно, то вы, может быть, гораздо чаще пытались бы делать это. Более широко метод быстрого поиска в неструктурированной базе данных можно было бы привлечь к решению любой задачи из NP. Нашим оракулом может быть подпрограмма, которая опрашивает каждого потенциального «свидетеля» y, который потенциально мог бы подтвердить решение проблемы. Например, если мы сталкиваемся с графом и нам необходимо узнать, существует ли на нем гамильтонов обход, мы можем представить обход «оракулу», а он – быстро ответить, является этот обход гамильтоновым или нет. Если бы нам был известен быстрый способ спросить оракул обо всех возможных обходах, то мы были бы способны эффективно найти гамильтонов обход (если он существует).

6.4.1. Оракул

Итак, «оракулом» кратко называют подпрограмму, которая быстро вычисляет функцию, чтобы проверить предлагаемое решение проблемы принятия решения, однако продолжим рассматривать оракул абстрактно, как «черный ящик». Оракул «знает», что из 2^n возможных строк длины n одна («помеченная» строка или «решение» ω) особенная. Мы предлагаем оракулу вопрос x, а он сообщает нам или $x = \omega$, или нет. Другими словами, он сообщает значение функции .

$$\begin{aligned} f_\omega(x) &= 0, \qquad x \neq \omega, \\ f_\omega(x) &= 1, \qquad x = \omega. \end{aligned} \tag{6.133}$$

Даже более того, это *квантовый оракул*, следовательно, он может отвечать на вопросы, представляющие собой суперпозиции строк. Оракулом является квантовый черный ящик, выполняющий унитарное преобразование

$$\mathbf{U}_{f_\omega} : |x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f_\omega(x)\rangle, \tag{6.134}$$

где $|x\rangle$ – n-кубитовое состояние, а $|y\rangle$ – однокубитовое состояние.

Как мы видели раньше в других контекстах, состояние однокубитового регистра может быть выбрано равным $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, так что оракул действует как

$$\begin{aligned}\mathbf{U}_{f_\omega} \; : \; & |x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ & \rightarrow (-1)^{f_\omega(x)}|x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).\end{aligned} \tag{6.135}$$

Теперь мы можем игнорировать второй регистр и получить

$$\mathbf{U}_\omega \; : \; |x\rangle \rightarrow (-1)^{f_\omega(x)}|x\rangle \tag{6.136}$$

или

$$\mathbf{U}_\omega = \mathbf{1} - 2|\omega\rangle\langle\omega|. \tag{6.137}$$

Оракул обращает знак состояния $|\omega\rangle$, но на любое другое состояние, ортогональное $|\omega\rangle$, действует тривиально. Это преобразование имеет простую геометрическую интерпретацию. Действуя на любой вектор в 2^n-мерном гильбертовом пространстве, $\mathbf{U}_\omega$ *отражает* его в гиперплоскости, перпендикулярной $|\omega\rangle$ (он сохраняет компоненты в гиперплоскости и обращает компоненту вдоль $|\omega\rangle$).

Мы знаем, что оракул выполняет это отражение для некоторого частного состояния вычислительного базиса $|\omega\rangle$, но *a priori* нам ничего не известно относительно значения строки ω. Наша задача – обращаясь к оракулу минимальное количество раз, определить ω с максимальной вероятностью.

6.4.2. Итерация Гровера

В качестве первого шага приготовим состояние

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle. \tag{6.138}$$

Равновзвешенная суперпозиция всех состояний вычислительного базиса может быть легко получена применением преобразования Адамара к каждому кубиту начального состояния $|x = 0\rangle$. Хотя нам не известно значение ω, мы знаем, что $|\omega\rangle$ является состоянием из вычислительного базиса, так что независимо от значения ω

$$|\langle\omega|s\rangle| = \frac{1}{\sqrt{N}}. \tag{6.139}$$

Если бы мы измерили состояние $|s\rangle$, проецируя его на вычислительный базис, то мы «нашли» бы маркированное состояние $|\omega\rangle$, с вероятностью, равной всего лишь $1/N$. Однако, следуя алгоритму Гровера, мы можем многократно итерировать преобразование, повышая амплитуду вероятности неизвестного искомого состояния $|\omega\rangle$ и одновременно подавляя амплитуды всех ненужных состояний $|x \neq \omega\rangle$. Сконструируем эту итерацию Гровера, комбинируя выполняемое оракулом неизвестное отражение $\mathbf{U}_\omega$ с известным отражением, которое мы можем выполнить сами. Этим известным отражением является преобразование

$$\mathbf{U}_s = 2|s\rangle\langle s| - \mathbf{1}, \tag{6.140}$$

которое сохраняет $|s\rangle$, но обращает знак любого вектора, ортогонального $|s\rangle$. Геометрически, действуя на произвольный вектор, оно сохраняет его компоненту вдоль $|s\rangle$ и обращает знаки компонент в гиперплоскости, ортогональной $|s\rangle$.

Ниже мы вернемся к проблеме построения схемы, выполняющей $\mathbf{U}_s$; а пока лишь предположим, что можем эффективно выполнять $\mathbf{U}_s$.

Одна итерация Гровера представляет собой унитарное преобразование

$$\mathbf{R}_{\text{grov}} = \mathbf{U}_s\mathbf{U}_\omega, \tag{6.141}$$

в котором наше отражение следует за вопросом оракулу. Рассмотрим, как $\mathbf{R}_{\text{grov}}$ действует в плоскости, натянутой на векторы $|\omega\rangle$ и $|s\rangle$. Проще всего понять это действие, представив его геометрически. Вспомним, что

$$|\langle\omega|s\rangle| = \frac{1}{\sqrt{N}} = \sin\theta, \tag{6.142}$$

так что $|s\rangle$ лежит в плоскости, натянутой на ортогональные векторы $|\omega\rangle$ и $|\omega^\perp\rangle$, и наклонен к последнему из них под углом θ. В этой плоскости $\mathbf{U}_\omega$ отражает вектор относительно оси $|\omega^\perp\rangle$, а $\mathbf{U}_s$ — относительно оси $|s\rangle$. Совместно два этих отражения поворачивают вектор на угол 2θ:

$$U_{s0}U_\omega = 2\theta.$$

Тогда итерация Гровера является ничем иным, как поворотом на угол 2θ в плоскости, определяемой векторами $|s\rangle$ и $|\omega\rangle$.

6.4.3. Поиск одного из четырех

Предположим, например, что в базе данных $N = 4$ объекта, среди которых один маркированный. С помощью классических вопросов маркированный объект может быть найден с 1-го, 2-го, 3-го или 4-го раза; в среднем для достижения цели необходимо $2\frac{1}{2}$ вопроса, а в худшем случае —

четыре[1]. Но так как $\sin\theta = \frac{1}{\sqrt{N}} = \frac{1}{2}$, то $\theta = 30°$, $2\theta = 60°$ и, следовательно, после итерации Гровера $|s\rangle$ поворачивается в направлении, перпендикулярном $|\omega^\perp\rangle$, то есть вдоль оси $|\omega\rangle$. Теперь измерение, проецирующее на вычислительный базис, с *полной определенностью* дает результат $|\omega\rangle$. Достаточно всего одного квантового вопроса, чтобы найти маркированное состояние, заметное улучшение по сравнению с классическим случаем.

Иногда полезно альтернативное представление итерации Гровера как «инверсии относительно среднего». Если разложить состояние $|\psi\rangle$ в вычислительном базисе

$$|\psi\rangle = \sum_x a_x |x\rangle, \tag{6.143}$$

то его внутреннее произведение с $|s\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle$ можно представить в виде

$$\langle s|\psi\rangle = \frac{1}{\sqrt{N}} \sum_x a_x = \sqrt{N}\langle a\rangle, \tag{6.144}$$

где

$$\langle a\rangle = \frac{1}{N} \sum_x a_x \tag{6.145}$$

— средняя амплитуда. Тогда применение $\mathbf{U}_s = 2|s\rangle\langle s| - \mathbf{1}$ к $|\psi\rangle$ дает

$$\mathbf{U}_s|\psi\rangle = \sum_x (2\langle a\rangle - a_x)|x\rangle\,; \tag{6.146}$$

амплитуды преобразуются как

$$\mathbf{U}_s : \; a_x - \langle a\rangle \;\longrightarrow\; \langle a\rangle - a_x, \tag{6.147}$$

то есть коэффициент перед $|x\rangle$ инвертируется относительно среднего значения амплитуды.

Возвращаясь к случаю $N = 4$, заметим, что в состоянии $|s\rangle$ каждая амплитуда равна $\frac{1}{2}$. Один вопрос оракулу обращает знак амплитуды маркированного состояния и, таким образом, сокращает среднюю амплитуду

[1] Конечно, если мы знаем, что один маркированный объект здесь обязательно присутствует, то четвертый вопрос на самом деле является излишним, так что можно быть точнее и говорить, что необходимо самое большее три вопроса, а в среднем — $2\frac{1}{4}$.

до $\frac{1}{4}$. Тогда инверсия относительно среднего значения переводит амплитуды всех немаркированных состояний от $\frac{1}{2}$ в нуль и увеличивает амплитуду маркированного состояния от $-\frac{1}{2}$ до $+1$. Итак, мы воспроизвели наш вывод о том, что достаточно одного вопроса, чтобы с полной определенностью найти маркированное состояние.

Также легко понять, что одного вопроса достаточно для того, чтобы найти маркированное состояние, если в базе данных имеется N записей и ровно $\frac{1}{4}$ из них маркирована. Тогда, как и выше, один вопрос сокращает среднюю амплитуду от $\frac{1}{\sqrt{N}}$ до $\frac{1}{2\sqrt{N}}$, а *инверсия относительно среднего* сокращает амплитуды немаркированных состояний до нуля.

(Сравнивая количество квантовых и классических вопросов, с которыми нужно обратиться к оракулу, возможно, не совсем справедливо говорить, что в квантовом случае необходим только один вопрос. Если оракул выполняет программу, которая вычисляет функцию, то в процессе вычисления некоторое вспомогательное пространство будет заполнено мусором. Нам будет необходимо удалить мусор, пройдя вычисление в обратном направлении для того, чтобы сохранить квантовую когерентность. Если классическое вычисление необратимо, то нет необходимости возвращать оракул в исходное состояние. В этом смысле, на языке теории сложности, один вопрос квантовому оракулу может быть примерно эквивалентным двум вопросам классическому оракулу.)

6.4.4. Поиск одного из N

Вернемся теперь к случаю, в котором база данных содержит N объектов, среди которых ровно один маркирован. Каждая итерация Гровера поворачивает квантовое состояние в плоскости, определяемой векторами $|s\rangle$ и $|\omega\rangle$; после T итераций состояние оказывается наклоненным к оси $|\omega^{\perp}\rangle$ под углом $\theta + 2T\theta$. Чтобы оптимизировать вероятность обнаружения маркированного состояния при выполнении заключительного измерения, итерировать следует до угла, близкого к 90°, или

$$(2T+1)\theta \simeq \frac{\pi}{2} \;\Rightarrow\; 2T+1 \simeq \frac{\pi}{2\theta}; \tag{6.148}$$

вспомним, что $\sin\theta = \frac{1}{\sqrt{N}}$, или, при больших N,

$$\theta \simeq \frac{1}{\sqrt{N}}. \tag{6.149}$$

Если выбрать

$$T = \frac{\pi}{4}\sqrt{N}[1 + O(N^{-1/2})], \tag{6.150}$$

то вероятность получения $|\omega\rangle$ в качестве результата измерения будет равна

$$\text{Prob}(\omega) = \sin^2\left((2T+1)\theta\right) = 1 - O\left(\frac{1}{N}\right). \tag{6.151}$$

Таким образом, необходимо лишь около $\frac{\pi}{4}\sqrt{N}$ вопросов, чтобы с высокой вероятностью определить ω, квадратичное ускорение по сравнению с классическим результатом.

6.4.5. Множество решений

Если существует $r > 1$ маркированных состояний и r известно, то количество итераций можно модифицировать так, чтобы вероятность отыскания одного из них оставалась очень близкой к единице. Анализ такой же, как и выше, за исключением того, что теперь оракул индуцирует отражение в гиперплоскости, ортогональной вектору

$$|\tilde{\omega}\rangle = \frac{1}{\sqrt{r}}\sum_{i=1}^{r}|\omega_i\rangle \tag{6.152}$$

— равновзвешенной суперпозиции маркированных состояний вычислительного базиса $|\omega_i\rangle$. Теперь

$$\langle s|\tilde{\omega}\rangle = \sqrt{\frac{r}{N}} \equiv \sin\theta, \tag{6.153}$$

а итерация Гровера поворачивает вектор на угол 2θ в плоскости, натянутой на векторы $|s\rangle$ и $|\tilde{\omega}\rangle$; мы снова приходим к выводу, что после количества итераций

$$T = \frac{\pi}{4\theta} = \frac{\pi}{4}\sqrt{\frac{N}{r}} \tag{6.154}$$

состояние близко к $|\tilde{\omega}\rangle$. Тогда если мы выполним измерение, проецируя на вычислительный базис, то с вероятностью, близкой к единице, найдем одно из маркированных (равновероятных) состояний. (С ростом количества решений время, необходимое для отыскания одного из них, падает как $r^{-1/2}$, в противоположность к r^{-1} в классическом случае.)

Обратим внимание на то, что если продолжить выполнение итераций Гровера, то вектор продолжит поворачиваться, и, таким образом, вероятность отыскания маркированного состояния (в результате заключительного измерения) начнет падать. Алгоритм Гровера подобен выпечке суфле – стоит передержать его в духовке, как оно начнет опадать. Следовательно, если нам ничего неизвестно о количестве маркированных состояний, то поиск одного из них может оказаться безуспешным. Например, $T \sim \frac{\pi}{4}\sqrt{N}$ итераций оптимально при $r = 1$, но при $r = 4$ вероятность отыскания маркированного состояния после этого количества итераций довольно близка к нулю.

Но даже если r *a priori* неизвестно, мы все же можем найти решение с квадратичным, по сравнению с классическими алгоритмами (при $r \ll N$), ускорением. Например, мы можем выбрать количество итераций случайным в интервале от нуля до $\frac{\pi}{4}\sqrt{N}$. Тогда для каждого r, ожидаемая вероятность отыскания маркированного состояния близка к $\frac{1}{2}$. Следовательно, маловероятно, что нам не удастся найти маркированное состояние после нескольких повторений. А при каждом измерении мы можем предлагать оракулу найденное нами состояние в качестве классического вопроса, чтобы получить подтверждение того, является ли оно действительно маркированным.

В частности, если решение не было найдено после нескольких попыток, то вполне возможно, что оно не существует. Таким образом, с высокой вероятностью можно дать корректный ответ ДА/НЕТ на вопрос «Есть ли здесь маркированные состояния?». Следовательно, мы можем принять алгоритм Гровера, в котором оракул проверяет предложенное решение, чтобы решить любую NP-проблему с квадратичным ускорением по сравнению с классическим методом исчерпывающего поиска.

6.4.6. Осуществление отражения

Чтобы выполнить итерацию Гровера, необходимо (кроме вопроса оракулу) унитарное преобразование

$$\mathbf{U}_s = 2|s\rangle\langle s| - \mathbf{1}, \tag{6.155}$$

которое отражает вектор относительно оси, определяемой вектором $|s\rangle$. Как эффективно построить это преобразование из квантовых вентилей? Так как $|s\rangle = \mathbf{H}^{(n)}|0\rangle$, где $\mathbf{H}^{(n)}$ – побитовое преобразование Адамара, то можно записать

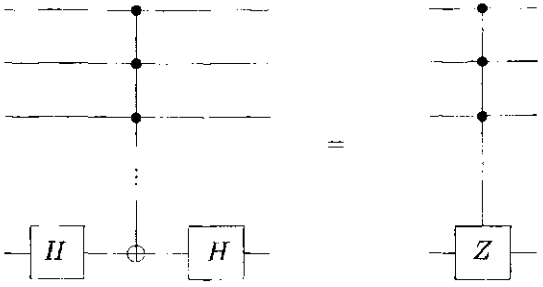
$$\mathbf{U}_s = \mathbf{H}^{(n)}\big(2|0\rangle\langle 0| - \mathbf{1}\big)\mathbf{H}^{(n)}, \tag{6.156}$$

то есть для этого достаточно построить отражение относительно оси $|0\rangle$. Мы легко можем построить это отражение из n-битового вентиля Тоффоли $\theta^{(n)}$.

Вспомним, что

$$\mathbf{H}\sigma_x\mathbf{H} = \sigma_z\,; \tag{6.157}$$

инвертирование бита с адамаровским поворотом базиса эквивалентно обращению относительной фазы векторов $|0\rangle$ и $|1\rangle$. Следовательно:



после сопряжения последнего бита преобразованием $\mathbf{H}$ вентиль $\theta^{(n)}$ становится $(n-1)$-кратно контролируемым σ_z, который обращает фазу вектора $|11\ldots\rangle|1\rangle$ и действует тривиально на все другие состояния вычислительного базиса. Сопрягая с помощью $\mathrm{NOT}^{(n)}$, мы получаем $\mathbf{U}_s$ с точностью до несущественного общего знака минус.

В упражнении вы покажете, что n-битовый вентиль Тоффоли $\theta^{(n)}$ можно построить из $(2n-5)$-ти трехбитовых вентилей Тоффоли $\theta^{(3)}$ (если доступно достаточное вспомогательное пространство). Следовательно, образующая $\mathbf{U}_s$ схема имеет *линейный* по $n = \log N$ размер. Гроверовский поиск в базе данных (при условии, что оракул мгновенно отвечает на вопрос) требует времени порядка $\sqrt{N}\log N$. Если мы рассматриваем оракул как подпрограмму, которая вычисляет функцию за полилогарифмическое время, тогда поиск требует времени порядка $\sqrt{N}\mathrm{poly}\big(\log N\big)$.

6.5. Оптимальность алгоритма Гровера

Гроверовское квадратичное квантовое ускорение поиска в базе данных уже интересно и потенциально важно, но конечно же, действуя более искусно, мы можем добиться лучшего результата, не так ли? Нет, оказывается не можем. Алгоритм Гровера обеспечивает максимально быстрый квантовый поиск в неструктурированной базе данных, если «время» измеряется в соответствии с количеством задаваемых оракулу вопросов.

Рассмотрим случай одного маркированного состояния $|\omega\rangle$, пусть $\mathbf{U}(\omega, T)$ обозначает квантовую схему, T раз обращающуюся к оракулу. Мы не накладываем на эту схему *никаких* ограничений, за исключением количества задаваемых ей вопросов; в частности, мы не ограничиваем количество квантовых вентилей. Эта схема применяется к начальному состоянию $|\psi(0)\rangle$, производя конечное состояние

$$|\psi_\omega(T)\rangle = \mathbf{U}(\omega, T)|\psi(0)\rangle. \tag{6.158}$$

Теперь мы должны выполнить измерение, предназначенное выделить $|\omega\rangle$ среди N его возможных значений. Для того чтобы мы были в состоянии идеально различать возможные состояния $|\psi_\omega(t)\rangle$, они должны быть взаимно ортогональными, а чтобы их можно было корректно различать с высокой вероятностью, они должны быть почти ортогональны.

Если состояния $\{|\psi_\omega\rangle\}$ образуют ортонормированный базис, то для любого фиксированного нормированного вектора $|\varphi\rangle$

$$\sum_{\omega=0}^{N-1} \| |\psi_\omega\rangle - |\varphi\rangle \|^2 \geqslant 2N - 2\sqrt{N}. \tag{6.159}$$

[Сумма минимизируется, если $|\varphi\rangle$ является равновзвешенной суперпозицией всех элементов базиса $|\varphi\rangle = \frac{1}{\sqrt{N}} \sum_\omega |\psi_\omega\rangle$, как вы можете показать, привлекая метод неопределенных множителей Лагранжа нахождения условных экстремумов.] Наша стратегия состоит в подходящем выборе состояния $|\varphi\rangle$, позволяющем с помощью неравенства (6.159) что-нибудь узнать о количестве обращений к оракулу T.

Наша схема с T вопросами образует унитарное преобразование

$$\mathbf{U}(\omega, T) = \mathbf{U}_\omega \mathbf{U}_T \mathbf{U}_\omega \mathbf{U}_{T-1} \ldots \mathbf{U}_\omega \mathbf{U}_1, \tag{6.160}$$

где $\mathbf{U}_\omega$ — преобразование оракула, а $\mathbf{U}_t$ — произвольные преобразования не-оракула. Выберем в качестве $|\varphi(T)\rangle$ результат применения к состоянию $|\psi(0)\rangle$ преобразования $\mathbf{U}(\omega, T)$, в котором каждое $\mathbf{U}_\omega$ заменено на $\mathbf{1}$; то есть результат применения той же схемы, но со всеми вопросами, задаваемыми «пустому оракулу». Следовательно,

$$|\varphi(T)\rangle = \mathbf{U}_T \mathbf{U}_{T-1} \ldots \mathbf{U}_2 \mathbf{U}_1 |\psi(0)\rangle, \tag{6.161}$$

в то время как

$$|\psi_\omega(T)\rangle = \mathbf{U}_\omega \mathbf{U}_T \mathbf{U}_\omega \mathbf{U}_{T-1} \ldots \mathbf{U}_\omega \mathbf{U}_1 |\psi(0)\rangle. \tag{6.162}$$

Чтобы сравнить $|\varphi(T)\rangle$ с $|\psi_\omega(T)\rangle$, воспользуемся нашим предыдущим анализом влияния ошибок на точность схемы, рассматривая ω-оракул как ошибочное применение пустого оракула. Норма вектора ошибки после t-го шага [ср. уравнение (6.63)] равна

$$\||E(\omega,t)\rangle\| = \|(\mathbf{U}_\omega - \mathbf{1})|\varphi(t)\rangle\| = 2\|\langle\omega|\varphi(t)\rangle\|, \tag{6.163}$$

поскольку $\mathbf{U}_\omega = \mathbf{1} - 2|\omega\rangle\langle\omega|$. После T вопросов мы имеем [ср. уравнение (6.66)]

$$\||\psi_\omega(T)\rangle - |\varphi(T)\rangle\| \leqslant 2\sum_{t=1}^{T}|\langle\omega|\varphi(t)\rangle|. \tag{6.164}$$

Из тождества

$$\begin{aligned}&\left(\sum_{t=1}^{T}c_t\right)^2 + \frac{1}{2}\sum_{s,t=1}^{T}(c_s - c_t)^2\\ &= \sum_{s,t=1}^{T}\left(c_tc_s + \frac{1}{2}c_s^2 - c_tc_s + \frac{1}{2}c_t^2\right) = T\sum_{t=1}^{T}c_t^2\end{aligned} \tag{6.165}$$

следует неравенство

$$\left(\sum_{t=1}^{T}c_t\right)^2 \leqslant T\sum_{t=1}^{T}c_t^2, \tag{6.166}$$

применение которого к (6.164) дает

$$\||\psi_\omega(T)\rangle - |\varphi(T)\rangle\|^2 \leqslant 4T\left(\sum_{t=1}^{T}|\langle\omega|\varphi(t)\rangle|^2\right). \tag{6.167}$$

Суммируя по ω, мы находим

$$\sum_\omega \||\psi_\omega(T)\rangle - |\varphi(T)\rangle\|^2 \leqslant 4T\sum_{t=1}^{T}\langle\varphi(t)|\varphi(t)\rangle = 4T^2. \tag{6.168}$$

Привлекая неравенство (6.159), мы приходим к выводу, что

$$4T^2 \geqslant 2N - 2\sqrt{N}, \tag{6.169}$$

если состояния $|\psi_\omega(T)\rangle$ взаимно ортогональны. Следовательно, мы показали, что любой квантовый алгоритм, способный различить все возможные значения маркированного состояния, должен обратиться к оракулу T раз, где

$$T \geqslant \sqrt{\frac{N}{2}} \tag{6.170}$$

(без учета малых при $N \to \infty$ поправок). Алгоритм Гровера находит ω с помощью $\frac{\pi}{4}\sqrt{N}$ вопросов, что превышает эту границу всего примерно на 11%. В действительности можно усовершенствовать доказательство, чтобы улучшить границу до $\frac{\pi}{4}\sqrt{N}(1-\varepsilon)$, что асимптотически насыщается алгоритмом Гровера[1]. Более того, можно показать, что схема Гровера достигает оптимальной вероятности успеха с помощью $T \leqslant \frac{\pi}{4}\sqrt{N}$ вопросов.

Испытываешь приступ разочарования (и одновременно волну восхищения перед Гровером) от осознания того, что алгоритм поиска в базе данных не может быть улучшен. Какое отношение это имеет к квантовой сложности?

Для многих проблем оптимизации в NP-классе не известно лучшего метода, чем исчерпывающий поиск всех возможных решений. Используя *квантовый параллелизм*, можно достичь квадратичного ускорения исчерпывающего поиска. Теперь мы знаем, что квадратичное ускорение является наилучшим, если мы полагаемся на силу явного квантового параллелизма и не разрабатываем наш квантовый алгоритм, используя специфическую структуру решаемой задачи. Тем не менее при достаточной изобретательности можно добиться и лучшего результата.

Оптимальность алгоритма Гровера может быть истолкована как свидетельство того, что $BQP \not\supseteq NP$. *По крайней мере, если окажется*, что $NP \subseteq BQP$, а $P \neq NP$, то тогда NP-проблемы должна объединять глубокая внутренняя структура (свидетельств которой в настоящее время нет), хорошо подходящая к возможностям квантовых схем.

Даже квадратичное ускорение может оказаться полезным для различных NP-полных проблем оптимизации. Однако квадратичное ускорение, в отличие от экспоненциального, реально не перемещает границу между разрешимостью и сложностью. В один прекрасный день квантовые компьютеры смогут превзойти классические компьютеры в выполнении исчер-

[1] C. Zalka, *Grover's Quantum Searching Algorithm is Optimal*, Phys. Rev., **A60**, 2746–2751 (1999); quant-ph/9711070. [Впервые оптимальность алгоритма Гровера была доказана в работе: C. H. Bennet, E. Bernstein, G. Brassard, U. Vazirani, *Strengths and Weaknesses of Quantum Computing*, SIAM J. Comput., **26(5)**, 1510–1523 (1997); quant-phys/9701001 – *Прим. ред.*

нывающего поиска, но только в том случае, если часы квантовых приборов не будут слишком сильно отставать от их классических прототипов.

6.6. Обобщенный поиск и структурированный поиск

В итерации Гровера мы выполняем преобразование $\mathbf{U}_s = 2|s\rangle\langle s| - \mathbf{1}$, отражение относительно оси, определяемой вектором $|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$. Почему именно относительно нее? Преимущество состояния $|s\rangle$ состоит в том, что оно имеет одинаковые перекрытия с каждым состоянием вычислительного базиса. Таким образом, перекрытие любого маркированного состояния $|\omega\rangle$ с $|s\rangle$ гарантированно равно $|\langle\omega|s\rangle| = 1/\sqrt{N}$. Следовательно, если нам известно количество маркированных состояний, то мы можем определить, сколько потребуется итераций, чтобы с высокой вероятностью отыскать одно из них — количество необходимых итераций не зависит от того, какое состояние маркировано.

Но, конечно, мы могли бы выбрать отражение относительно другой оси. Если мы можем построить унитарное преобразование $\mathbf{U}$ (с разумной эффективностью), тогда мы можем образовать

$$\mathbf{U}(2|0\rangle\langle 0| - \mathbf{1})\mathbf{U}^\dagger = 2\mathbf{U}|0\rangle\langle 0|\mathbf{U}^\dagger - \mathbf{1} \tag{6.171}$$

преобразование, отражающее относительно оси $\mathbf{U}|0\rangle$.

Предположим, что

$$|\langle\omega|\mathbf{U}|0\rangle| = \sin\theta, \tag{6.172}$$

где $|\omega\rangle$ — маркированное состояние. Тогда, если мы заменим в итерации Гровера $\mathbf{U}_s$ на отражение (6.171), то одна итерация будет выполнять поворот на угол 2θ в плоскости, определяемой векторами $|\omega\rangle$ и $\mathbf{U}|0\rangle$ (в соответствии с теми же аргументами, что мы использовали для $\mathbf{U}_s$). Таким образом, после T итераций с $(2T+1)\theta \simeq \pi/2$ измерение в вычислительном базисе с высокой вероятностью найдет $|\omega\rangle$. Следовательно, если мы заменим в квантовой схеме Гровера $\mathbf{H}^{(n)}$ на $\mathbf{U}$, мы по-прежнему сможем выполнять поиск в базе данных до тех пор, пока $\mathbf{U}|0\rangle$ остается не ортогональным маркированному состоянию[1]. Но если мы не имеем никакой *априорной* информации о том, какое состояние маркировано, то $\mathbf{H}^{(n)}$ является наилучшим выбором не только потому, что $|s\rangle$ имеет известное перекрытие

[1] L. K. Grover, *Quantum Computers Can Search Rapidly By Using Almost Any Transformation*, Phys. Rev. Lett., **80**, 4329–4332 (1998); quant-ph/9712011.

с каждым маркированным состоянием, но также и потому, что оно имеет максимальное *среднее* перекрытие со всеми возможными маркированными состояниями.

Но иногда, выполняя поиск в базе данных, мы *имеем* некоторую информацию о том куда следует заглянуть, а в этом случае может оказаться полезной описанная выше стратегия обобщенного поиска[1].

В качестве примера проблемы с некоторой вспомогательной структурой предположим, что $f(x, y)$ — функция с однобитовым значением, зависящая от двух n-битовых строк x и y, и нам нужно найти единственное решение $f(x, y) = 1$. С помощью алгоритма Гровера мы можем искать среди N^2 возможных значений ($N = 2^n$) пар (x, y) и с высокой вероятностью найти решение (x_0, y_0) после $\frac{\pi}{4}N$ итераций, квадратичное ускорение по сравнению с классическим поиском.

Но предположим далее, что $g(x)$ — функция только от x, и известно, что $g(x) = 1$ при ровно M значениях x, где $1 \ll M \ll N$. Более того, известно, что $g(x_0) = 1$. Следовательно, мы можем воспользоваться функцией g, чтобы помочь в поиске решения (x_0, y_0).

Теперь для консультаций у нас есть два оракула, один выдает значение $f(x, y)$, а другой значение $g(x)$. Наша задача - найти (x_0, y_0), задав минимальное количество вопросов.

С классической точки зрения нам необходимо около NM вопросов для того, чтобы с разумной вероятностью найти решение. Сначала мы вычисляем $g(x)$ для каждого x; затем мы ограничиваем наш поиск решения $f(x, y) = 1$ только такими M значениями x, при которых $g(x) = 1$. Естественно поинтересоваться, существует ли способ выполнить квантовый поиск за время порядка квадратного корня от классического времени. Исчерпывающий поиск, который обращается только к f-оракулу, требует времени $N \gg \sqrt{NM}$ и, следовательно, не решает проблемы. Нам необходимо пересмотреть наш метод квантового поиска, чтобы воспользоваться преимуществом структуры, предоставляемой функцией g.

Лучший метод — сначала применить алгоритм Гровера к $g(x)$. Примерно за $\frac{\pi}{4}\sqrt{\frac{N}{M}}$ итераций мы приготовим состояние, близкое к равновзвешенной суперпозиции из M решений $g(x) = 1$. В частности, состояние $|x_0\rangle$ возникает с амплитудой $\frac{1}{\sqrt{M}}$. Затем мы применяем алгоритм

[1] E. Farhi and S. Gutmann, *Quantum-Mechanical Square Root Speedup in a Structured Search Problem*, quant-ph/9711035; L. K. Grover, *Quantum Search On Structured Problems*, quant-ph/9802035.

Гровера к $f(x,y)$ при фиксированном x. Приблизительно после $\frac{\pi}{4}\sqrt{N}$ итераций состояние $|x_0\rangle|s\rangle$ эволюционирует достаточно близко к состоянию $|x_0\rangle|y_0\rangle$. Следовательно, $|x_0, y_0\rangle$ появляется с амплитудой $\frac{1}{\sqrt{M}}$.

Образованное из $\frac{\pi}{4}\sqrt{N}$ вопросов унитарное преобразование, которое мы до сих пор строили, может рассматриваться как преобразование $\mathbf{U}$, определяющее обобщенный поиск. Более того, нам известно, что

$$\langle x_0, y_0|\mathbf{U}|0,0\rangle \simeq \frac{1}{\sqrt{M}}. \tag{6.173}$$

Следовательно, если мы итерируем обобщенный поиск примерно $\frac{\pi}{4}\sqrt{M}$ раз, то приготовим состояние, достаточно близкое к $|x_0, y_0\rangle$. В совокупности примерно после

$$\left(\frac{\pi}{4}\right)^2 \sqrt{NM} \tag{6.174}$$

вопросов мы можем с высокой вероятностью найти решение. Это действительно квадратичное ускорение по сравнению с классическим поиском.

6.7. Некоторые задачи не допускают ускорения

Пример структурированного квантового поиска иллюстрирует, что квадратичные квантовые ускорения по сравнению с классическими алгоритмами могут быть достигнуты для различных проблем, а не только для исчерпывающего поиска в неструктурированной базе данных. Можно даже надеяться, что квантовый параллелизм позволяет существенно ускорить любой классический алгоритм. Сейчас эта надежда будет разбита — для многих задач квантовое ускорение невозможно.

Продолжим рассматривать задачи с квантовым черным ящиком, оракулом, который вычисляет функцию f, отображающую n битов в один. Но мы немного модифицируем наши обозначения. Функция f может быть представлена строкой из $N = 2^n$ битов:

$$X = X_{N-1}X_{N-2}\ldots X_1X_0, \tag{6.175}$$

где X_i обозначает $f(i)$. Наша задача — вычислить некоторую зависящую от X функцию с однобитовым значением, то есть ответить на ДА/НЕТ-вопрос о свойствах оракула. То, что сейчас будет показано, означает, что некоторые функции от X не могут быть вычислены с низкой вероятностью

ошибки, используя квантовый алгоритм, за исключением алгоритма, обращающегося к оракулу столько раз (или почти столько же раз), сколько требуется классическому алгоритму[1].

Главная идея состоит в том, что булева функция от переменных X_i может быть представлена полиномом от X_i. Более того, распределение вероятностей для квантового измерения может быть выражено через полином от X_i, где степень полинома равна $2T$, если измерение следует после T вопросов оракулу. Проблема в том, может ли полином степени $2T$ обеспечить разумную аппроксимацию интересующей нас булевой функции.

Действие оракула может быть представлено как

$$\mathbf{U}_O\colon |i, y; z\rangle \to |i, y \oplus X_i; z\rangle, \tag{6.176}$$

где i принимает значения из $\{0, 1, \ldots, N-1\}$, $y \in \{0, 1\}$, а z обозначает состояние вспомогательного кубита, не изменяемого оракулом. Следовательно, в каждом 2×2-блоке, натянутом на $|i, 0; z\rangle$ и $|i, 1; z\rangle$, $\mathbf{U}_O$ представляет собой 2×2-матрицу

$$\begin{pmatrix} 1 - X_i & X_i \\ X_i & 1 - X_i \end{pmatrix}. \tag{6.177}$$

Квантовые вентили, в отличие от вопросов к оракулу, не зависят от X. Следовательно, после того как схема из T вопросов подействует на любое начальное состояние, результирующее состояние $|\psi\rangle$ будет иметь амплитуды, которые (по крайней мере) являются полиномами степени T от X. Если мы выполним ПОЗМ на $|\psi\rangle$, то связанная с положительным оператором $\mathbf{F}$ вероятность результата $\langle\psi|\mathbf{F}|\psi\rangle$ может быть выражена через полином от X степени, не меньшей чем $2T$.

Любая булева функция от X_i может быть выражена (единственным образом) через полином степени $\leqslant N$ по X_i. Например, рассмотрим функцию OR от N переменных X_i; это

$$\mathrm{OR}(X) = 1 - (1 - X_0)(1 - X_1)\cdots(1 - X_{N-1}), \tag{6.178}$$

полином степени N.

Допустим, мы хотим применить нашу квантовую схему для того, чтобы *с полной определенностью* вычислить функцию OR. Тогда мы должны

[1] E. Farhi, *et al*, *A Limit on the Speed of Quantum Computation in Determining Parity*, Phys. Rev. Lett., **81**, 5442–5444 (1998); quant-ph/9802045; R. Beals, *et al*, *Quantum Lower Bounds by Polynomials*. In *Proceedings of the 39th Annual Symposium on Foundamentals of Computer Science* (FOCS'98), 352-361, IEEE, Los Alamos, California, November, 1998; quant-ph/9802049.

быть в состоянии выполнить измерение с двумя результатами 0 и 1, где

$$\begin{aligned} \mathrm{Prob}(0) &= 1 - \mathrm{OR}(X), \\ \mathrm{Prob}(1) &= \mathrm{OR}(X). \end{aligned} \tag{6.179}$$

Но эти выражения являются полиномами степени N, которые могут быть вычислены только после как минимум T-кратного обращения схемы к оракулу, где

$$T \geqslant \frac{N}{2}. \tag{6.180}$$

Мы приходим к выводу, что не существует квантовой схемы, которая менее чем за $N/2$ обращений к оракулу может точно вычислить OR. Фактически для этой функции (или любой функции, принимающей значение 0 только для одного из N ее возможных аргументов) существует более сильное заключение (см. упражнение): требуется $T \geqslant N$, чтобы *с полной определенностью* вычислить OR.

С другой стороны, вычисляя функцию OR (отвечая на ДА/НЕТ-вопрос «Имеется ли маркированное состояние?»), именно алгоритм Гровера может достичь количества вопросов порядка $\sqrt{N}$. Таким образом, вывод о том, что для *детерминированного* вычисления OR необходимо N вопросов, хотя и корректен, но несколько обманчив. Мы можем вычислить OR *вероятностным образом* с помощью гораздо меньшего количества вопросов. По-видимому, алгоритм Гровера может построить полином от X, который, имея степень только $O(\sqrt{N})$, тем не менее обеспечивает весьма адекватную аппроксимацию полинома N-ой степени $\mathrm{OR}(X)$.

Однако OR, принимающая значение 1 для каждого значения X, кроме $X = \vec{0}$, является очень простой булевой функцией. Нам следует рассмотреть другие функции, которые могут предложить квантовому компьютеру более серьезные проблемы.

Первое, что приходит в голову — это функция $\mathrm{PARITY}(X)$, принимающая значение 0, если строка X содержит четное количество единиц, и — значение 1, если строка X содержит нечетное количество единиц. Очевидно, чтобы определить четность, классический алгоритм должен обратиться к оракулу N раз. Насколько лучше это можно сделать, предлагая квантовые вопросы? Фактически мы вообще не можем добиться лучшего результата — необходимо по крайней мере $N/2$ квантовых вопросов, чтобы с вероятностью успеха, большей $\frac{1}{2} + \delta$, найти правильное значение $\mathrm{PARITY}(X)$.

При обсуждении PARITY удобно использовать новые переменные

$$\tilde{X}_i = 1 - 2X_i, \tag{6.181}$$

принимающие значения ± 1, так что

$$\mathrm{PARITY}(\tilde{X}) = \prod_{i=0}^{N-1} \tilde{X}_i \tag{6.182}$$

также принимает значения ± 1. Теперь, после того как выполнена квантовая схема со всеми T вопросами оракулу, мы должны выполнить ПОЗМ с двумя возможными исходами $\mathbf{F}_{\mathrm{even}}$ и $\mathbf{F}_{\mathrm{odd}}$; результатом будет наша оценка $\mathrm{PARITY}(\tilde{X})$. Как мы уже отмечали, вероятность получения результата (к примеру) «even» («четный») может быть выражена через полином $P^{(2T)}_{\mathrm{even}}(\tilde{X})$ степени (самое большее) $2T$ по $\tilde{X}_i$:

$$\langle \mathbf{F}_{\mathrm{even}} \rangle = P^{(2T)}_{\mathrm{even}}(\tilde{X}). \tag{6.183}$$

Как часто наша догадка будет верна? Рассмотрим сумму

$$\sum_{\{\tilde{X}\}} P^{(2T)}_{\mathrm{even}}(\tilde{X}) \cdot \mathrm{PARITY}(\tilde{X}) = \sum_{\{\tilde{X}\}} P^{(2T)}_{\mathrm{even}}(\tilde{X}) \prod_{i=0}^{N-1} \tilde{X}_i. \tag{6.184}$$

Поскольку каждое слагаемое полинома $P^{(2T)}_{\mathrm{even}}(\tilde{X})$ содержит самое большее $2T$ из переменных $\tilde{X}_i$, то можно воспользоваться тождеством

$$\sum_{X_i \in \{0,1\}} \tilde{X}_i = 0, \tag{6.185}$$

чтобы понять, что сумма в (6.184) должна обращаться в нуль при $N > 2T$. Таким образом,

$$\sum_{\mathrm{par}(\tilde{X})=1} P^{(2T)}_{\mathrm{even}}(\tilde{X}) = \sum_{\mathrm{par}(\tilde{X})=-1} P^{(2T)}_{\mathrm{even}}(\tilde{X}); \tag{6.186}$$

то есть при $T < N/2$ мы с одинаковой вероятностью можем угадать «even», как в случае, когда на самом деле $\mathrm{PARITY}(\tilde{X})$ является нечетной, так и в том случае, когда она действительно четная (в среднем). Наш квантовый алгоритм ничего не может сообщить о значении $\mathrm{PARITY}(\tilde{X})$; то есть в среднем по возможным (*a priori* равновероятным) значениям X_i мы с равной вероятностью будем как правы, так и неправы.

Мы можем также показать, демонстрируя явный алгоритм (см. упражнение), что для определения PARITY (или вероятностного, или детерминированного) *достаточно* $N/2$ вопросов (при условии, что N четное). В этом смысле мы достигаем двукратного ускорения по сравнению с классическими вопросами. Но это лучшее из того, чего мы можем добиться.

6.8. Поиск в распределенной базе данных

Поучительно взглянуть на квантовый алгоритм поиска в базе данных с новой точки зрения. Представим, что двум участникам, Алисе и Бобу, необходимо договориться о встрече в удобный для обоих день. У Алисы есть календарь, в который внесено $N = 2^n$ дней, каждый из которых отмечен нулем, если в этот день она занята, или единицей, если она свободна. Аналогичный календарь имеется у Боба. Их задача найти день, в который они оба будут свободны.

Алиса и Боб имеют квантовые компьютеры, но они находятся очень далеко друг от друга. (Алиса на Земле, а Боб путешествует по туманности Андромеды.) Следовательно, для них слишком дорого связываться друг с другом. Им нужно срочно определить дату, но они должны экономить на объеме посылаемой туда и обратно информации.

Даже если существует день, когда они оба свободны, может оказаться, что найти его нелегко. Если Алиса и Боб связываются, посылая туда и обратно классические биты, тогда в худшем случае им будет необходимо обменяться порядка $N = 2^n$ записями календаря, чтобы иметь разумный шанс успешно договориться о встрече. Мы спросим: может быть, вместо этого им лучше обмениваться кубитами?[1] (От Земли до Андромеды тщательно спроектирован и построен квантовый информационный хайвей, так что посылать кубиты вместо битов не намного дороже.)

Для знакомого с основами теории квантовой информации этот вопрос выглядит странным. Теорема Холево раз и навсегда сказала, что один кубит может переносить не более одного бита классической информации. Хотя, немного подумав, мы увидим, что теорема Холево фактически не решает проблему. Хотя она ограничивает взаимную информацию приготовления состояния и результата измерения, она не гарантирует (по крайней мере не прямо), что Алисе и Бобу необходимо обменяться таким же количеством

[1] В ранней версии этих лекций я предлагал другой сценарий, в котором Алиса и Боб имели почти идентичные таблицы, но с одной несовпадающей записью; их задачей было найти положение несовпадающего бита. Однако этот пример был неудачен, поскольку задача могла быть решена с помощью всего лишь $\log N$ битов классической связи. (Я благодарен Ричарду Кливу, указавшему на эту ошибку.) Мы хотели, чтобы Алиса узнала адрес (двоичную строку длиной n) одной записи, которой ее таблица отличается от таблицы Боба. Для этого Боб вычисляет четность $N/2$ записей своей таблицы с меткой, принимающей значение 0 в ее самом младшем значащем бите, и посылает Алисе только бит четности. Алиса сравнивает четность тех же записей ее таблицы и находит один бит (самый младший значащий бит) адреса несовпадающей записи. Затем они повторяют то же самое для каждого из оставшихся $n - 1$ битов до тех пор, пока Алиса не узнает полный адрес «ошибки». Всего послано только n битов (и все от Боба к Алисе).

кубитов, что и битов, чтобы сравнить их календари. Тем не менее это приятный сюрприз — узнать, что Алиса и Боб могут выполнить задание, обменявшись $O(\sqrt{N}\log N)$ кубитами по сравнению с $O(N)$ классическими битами[1].

Чтобы добиться этого, Алиса и Боб должны действовать сообща, осуществляя распределенную версию поиска в базе данных. Алиса имеет доступ к оракулу (ее календарь), вычисляющему функцию $f_A(x)$, а Боб имеет оракул (его календарь), вычисляющий $f_B(x)$. Вместе они могут предложить оракулу

$$f_{AB}(x) = f_A(x) \wedge f_B(x). \tag{6.187}$$

Один из них может осуществить отражение $\mathbf{U}_s$, так что они могут выполнить полную итерацию Гровера и произвести исчерпывающий поиск подходящего дня x такого, что $f_{AB}(x) = 1$ (когда Алиса и Боб оба свободны). Если взаимоприемлемый день действительно существует, они достигнут цели в его поиске после порядка $\sqrt{N}$ вопросов.

Но как Алисе и Бобу задать вопрос $f_{AB}(x)$? Опишем, как им это сделать, действуя на любое одно из состояний вычислительного базиса $|x\rangle$. Сначала Алиса выполняет

$$|x\rangle|0\rangle \rightarrow |x\rangle|f_A(x)\rangle, \tag{6.188}$$

а затем посылает $n+1$ кубитов Бобу. Боб выполняет

$$|x\rangle|f_A(x)\rangle \rightarrow (-1)^{f_A(x)\wedge f_B(x)}|x\rangle|f_A(x)\rangle. \tag{6.189}$$

Это преобразование, очевидно, унитарно, и вы можете легко проверить, что Боб может осуществить его, обратившись к своему оракулу. Теперь, как и требовалось, фазовый множитель перед $|x\rangle$ равен $(-1)^{f_{AB}(x)}$, но в другом регистре продолжает храниться $|f_A(x)\rangle$, что будет портить когерентность суперпозиции значений x. Боб не может удалить этот регистр, но это может сделать Алиса. Тогда Боб посылает $n+1$ кубитов обратно Алисе, а она еще раз консультируется со своим оракулом, чтобы выполнить

$$(-1)^{f_A(x)\wedge f_B(x)}|x\rangle|f_A(x)\rangle \rightarrow (-1)^{f_A(x)\wedge f_B(x)}|x\rangle|0\rangle. \tag{6.190}$$

Обменявшись $2(n+1)$ кубитами, они завершили один вопрос из f_{AB} оракулу и, таким образом, могут выполнить одну итерацию Гровера.

---

[1] H. Burhman, *et. al.*, *Quantum vs. Classical Communication and Computation*, In *Proceedings of the 30th Annual ACM Symposium of Theory of Computing*, ACM Press, 1998; quant-ph/9802040.

Допустим, например, что Алиса и Боб знают, что имеется только одна взаимоприемлемая дата, но у них нет *априорной* информации о том, что это за день. После примерно $\frac{\pi}{4}\sqrt{N}$ итераций, требующих обменяться всего

$$Q \simeq \frac{\pi}{4}\sqrt{N} \cdot 2(\log N + 1) \tag{6.191}$$

кубитами, Алиса выполняет измерение, получая удобную дату с вероятностью, близкой к единице.

Таким образом, по крайней мере в этом частном случае, обмен $O(\sqrt{N}\log N)$ кубитами так же хорош, как и обмен $O(N)$ классическими битами. По-видимому, нужно быть осторожнее в интерпретации границы Холево, которая явно утверждает, что кубит имеет не большую способность переносить информацию, чем бит!

Если Алисе и Бобу заранее неизвестно, сколько имеется подходящих дат, то они тем не менее могут выполнить поиск Гровера (как мы отмечали в § 6.4.5) и с разумной вероятностью найти решение. С помощью $2 \cdot \log N$ битов классического сообщения они могут проверить, действительно ли найденная дата устраивает их обоих.

6.8.1. Сложность квантовой связи

В более общем виде можно представить, что каждый из нескольких участников обладает n-битовым входом; им необходимо вычислить функцию, зависящую от всех входов, с тем, чтобы ее значение в конце концов стало известно одному из них. Какой минимальный объем сообщений необходим для вычисления функции (детерминированного или вероятностного)? Хорошо изученный раздел классической теории сложности, которому адресуется этот вопрос, называется *сложностью связи*. То, что мы установили выше, является квадратичной границей между квантовой и классической сложностями связи для частного класса функций двух участников.

Помимо перехода от обмена классическими битами к обмену кубитами существуют другие интересные пути обобщения классической сложности связи. Например, предположим, что участники делят некоторое заранее подготовленное запутанное состояние (пары Белла или многокомпонентное запутывание) и могут использовать его наряду с классической связью, чтобы выполнить вычисление функции. Вновь непосредственно не очевидно, что разделенное запутывание упростит задачу, так как само по себе оно еще не позволяет участникам обмениваться классическими сообщени-

ями. Но оказывается, что запутывание *оказывает* помощь, по крайней мере небольшую[1].

В последнее время анализ сложности связи популярен среди теоретиков в области сложности, но эта дисциплина пока еще не представляется занимающей важное положение в практической технике связи. Возможно, это удивительно, принимая во внимание важность эффективного распределения вычислительной нагрузки в параллельных вычислениях, которые стали обычным делом. Более того, похоже, что в реальной жизни практически вся связь может рассматриваться как форма дистанционных вычислений. На самом деле мне не нужно получать все биты, дошедшие до меня по телефонной линии, особенно потому, что я скорее всего запомню только несколько битов информации, имеющих отношение к звонку в ближайшем будущем (фильм, на который мы решили сходить). Как менее прозаический пример, нам на Земле может быть необходимо связаться с роботом в глубоком космосе, чтобы проинструктировать, выходить ли ему на орбиту вокруг удаленной звездной системы. Так как ширина полосы предельно ограничена, то мы хотели бы вычислить правильный ответ на ДА/НЕТ-вопрос «Выходить ли на орбиту?» с помощью минимального обмена информацией между Землей и роботом.

Возможно, будущая цивилизация будет использовать известное квадратичное разделение между классической и квантовой сложностью связи, обмениваясь, скорее, кубитами, чем битами, со своей флотилией космических сил. А возможно, будет найдено экспоненциальное разделение, по крайней мере в определенных ситуациях, что существенно повысило бы стимул для развития необходимой технологии квантовой связи.

6.9. Периодичность

Проблема Саймона до сих пор является единственным примером, в котором мы нашли экспоненциальное разделение между скоростью квантового алгоритма и скоростью соответствующего классического алгоритма. Алгоритм Саймона использует квантовый параллелизм, чтобы ускорить поиск периода функции. Его успех вдохновляет нас искать другие квантовые алгоритмы, предназначенные для отыскания других разновидностей периода.

[1] R. Cleve, *et. al.*, *Quantum Entanglement and the Communication Complexity of the Inner Product Function*, Lect. Notes Comput. Sci., **1509**, 61–74 (1998), quant-ph/9708019; H. Buhrman, *et al*, ... *Complexity*, Phys. Rev., **A60**, 2737–2741 (1998), quant-ph/9710054.

Саймон изучал периодические функции, принимающие значения в $(Z_2)^n$. Для этой цели мощным инструментом служило n-битовое преобразование Адамара $\mathbf{H}^{(n)}$. Если вместо этого мы хотим изучать периодические функции, принимающие значения в Z_{2^n}, то инструментом сопоставимой силы будет (дискретное) преобразование Фурье.

Урок задачи Саймона в том, что, хотя поиск иголок в стоге сена может быть трудным, отыскание *периодически* распределенных иголок в стоге сена может оказаться гораздо проще. Например, если мы рассеиваем фотон на периодическом массиве иголок, он вероятнее всего рассеется в одном из преимущественных направлений, в котором удовлетворяется условие брэгговского отражения. Эти преимущественные направления зависят от расстояния между иголками. Таким образом, рассеяв только один фотон, мы уже приобретаем некоторую полезную информацию о периоде. При построении эффективных квантовых алгоритмов следует и дальше пользоваться смысловым подтекстом этой метафоры.

Итак, представим квантовый оракул, вычисляющий функцию

$$f\colon \{0,1\}^n \to \{0,1\}^m, \tag{6.192}$$

которая имеет неизвестный период r, где r – положительное целое число, удовлетворяющее

$$1 \ll r \ll 2^n. \tag{6.193}$$

То есть

$$f(x) = f(x + mr), \tag{6.194}$$

где m – произвольное целое число такое, что x и $x + mr$ лежат в $\{0, 1, 2, \ldots, 2^n - 1\}$. Мы должны найти период r. Рассматриваемая классически, эта проблема *трудная*. Если r, скажем, порядка $2^{n/2}$, нам необходимо обратиться к оракулу порядка $2^{n/2}$ раз, прежде чем мы, возможно, найдем два значения x, отображаемых на одно и то же значение $f(x)$, и, следовательно, что-нибудь узнаем о периоде r. Но, как мы увидим, существует квантовый алгоритм, определяющий r за время $\mathrm{poly}(n)$.

Даже если нам известно, как эффективно вычислять функцию $f(x)$, определение ее периода может оказаться трудной задачей. Наш квантовый алгоритм может быть применен для отыскания за $\mathrm{poly}(n)$ время периода любой функции, которую мы умеем вычислять за $\mathrm{poly}(n)$ время. Эффективное отыскание периода позволяет эффективно решать множество (по-видимому) трудных задач, таких как факторизация целого числа или вычисление дискретного логарифма[1].

[1] Дискретный логарифм определяется как минимальный положительный корень x уравне-

Ключевая идея, лежащая в основе квантового поиска периода, заключается в том, что преобразование Фурье может быть вычислено с помощью эффективной квантовой схемы (что было обнаружено Питером Шором). Квантовое преобразование Фурье (QFT) использует мощь квантового параллелизма, чтобы достичь экспоненциального ускорения хорошо известного (классического) быстрого преобразования Фурье (FFT). Поскольку FFT имеет такое широкое поле применений, то, возможно, однажды и QFT станет столь же широко распространенным.

6.9.1. Отыскание периода

QFT является унитарным преобразованием, действующим в вычислительном базисе согласно

$$\mathrm{QFT}\ :\ |x\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i x y/N} |y\rangle, \tag{6.195}$$

где $N = 2^n$. Будем пока предполагать, что мы эффективно выполняем QFT, и посмотрим, как это позволяет извлекать период функции $f(x)$.

Эмулируя алгоритм Саймона, мы сначала обратимся к оракулу с $\frac{1}{\sqrt{N}} \sum_x |x\rangle$ (легко приготавливаемым применением $\mathbf{H}^{(n)}$ к $|0\rangle$) и, таким образом, приготовим состояние

$$\frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} |x\rangle |f(x)\rangle. \tag{6.196}$$

Затем *измерим выходной* регистр, получая результат $|f(x_0)\rangle$ при некотором $0 \leqslant x_0 < r$. Это измерение готовит во входном регистре когерентную суперпозицию A значений x, которые отображаются на $f(x_0)$:

$$\frac{1}{\sqrt{A}} \sum_{j=0}^{A-1} |x_0 + jr\rangle, \tag{6.197}$$

где

$$N - r \leqslant x_0 + (A-1)r < N \tag{6.198}$$

ния $a^x = b (\mathrm{mod}\, p)$, где все переменные являются целыми числами. Вычисление дискретного логарифма является сложной вычислительной проблемой, что находит применение в криптографии. Квантовый алгоритм решения этой задачи см. в книге М. Нильсен, И. Чанг, *Квантовые вычисления и квантовая информация*, М., Мир (2006). — *Прим. ред.*

или

$$A - 1 < \frac{N}{r} < A + 1. \tag{6.199}$$

На самом деле измерение выходного регистра не обязательно. Если его пропустить, то состоянием входного регистра будет некогерентная суперпозиция (просуммированная по $x_0 \in \{0, 1, 2, \ldots, r-1\}$) состояний вида (6.197). Остальная часть алгоритма также хорошо работает, действуя на это начальное состояние.

Теперь наша задача состоит в том, чтобы извлечь значение r из состояния (6.197). Если бы мы на этом этапе измерили входной регистр, проецируя его на вычислительный базис, то мы бы ничего не узнали относительно r. Вместо этого (ср. с алгоритмом Саймона) следует сначала выполнить преобразование Фурье, а *уже затем* проводить измерение.

Применяя QFT к состоянию (6.197), получим

$$\frac{1}{\sqrt{NA}} \sum_{y=0}^{N-1} e^{2\pi i x_0 y/N} \sum_{j=0}^{A-1} e^{2\pi i j r y/N} |y\rangle. \tag{6.200}$$

Если мы теперь выполним измерение в вычислительном базисе, то вероятность получения результата y будет равна

$$\mathrm{Prob}(y) = \frac{A}{N} \left| \frac{1}{A} \sum_{j=0}^{A-1} e^{2\pi i j r y/N} \right|^2. \tag{6.201}$$

Это распределение резко выделяет такие значения y, при которых yr/N близко к целому числу. Например, если N/r оказывается целым (и, следовательно, равным A), то

$$\mathrm{Prob}(y) = \frac{1}{r} \left| \frac{1}{A} \sum_{j=0}^{A-1} e^{2\pi i j y/A} \right|^2 = \begin{cases} \frac{1}{r}, & y = A \cdot (\text{целое}), \\ 0 & \text{в противном случае.} \end{cases} \tag{6.202}$$

В более общем случае мы можем просуммировать геометрическую прогрессию

$$\sum_{j=0}^{A-1} e^{i\theta j} = \frac{e^{iA\theta} - 1}{e^{i\theta} - 1}, \tag{6.203}$$

где

$$\theta = \frac{2\pi yr(\mathrm{mod\,N})}{N}. \tag{6.204}$$

Существует точно r значений $y \in \{0, 1, 2, \ldots, N-1\}$, удовлетворяющих

$$-\frac{r}{2} \leqslant yr(\mathrm{mod\,N}) \leqslant \frac{r}{2}. \tag{6.205}$$

(Чтобы убедиться в этом, представим промаркированные кратные r и N в ряду чисел, простирающемся от 0 до $rN-1$. Для каждого кратного N существует кратное r, удаленное от него не более чем на расстояние $r/2$) Для каждого из этих значений соответствующее θ удовлетворяет

$$-\pi\frac{r}{N} \leqslant \theta \leqslant \pi\frac{r}{N}. \tag{6.206}$$

Теперь, поскольку $A-1 < \frac{N}{r}$, то при этих значениях θ все слагаемые в сумме по j в уравнении (6.203) лежат в одной полуплоскости, следовательно, они интерферируют конструктивно и сумма становится значительной.

Мы знаем, что

$$|1 - e^{i\theta}| \leqslant |\theta|, \tag{6.207}$$

поскольку расстояние по прямой от начала координат меньше, чем длина дуги вдоль окружности, а при $A|\theta| \leqslant \pi$

$$|1 - e^{iA\theta}| \geqslant \frac{2A|\theta|}{\pi}, \tag{6.208}$$

так как мы можем увидеть (графически или вычислив его производную), что это расстояние является выпуклой функцией. На самом деле $A < \frac{N}{r} + 1$ и, следовательно, $A\theta < \pi\left(1 + \frac{r}{N}\right)$, но, применяя вышеуказанную границу к

$$\left|\frac{e^{i(A-1)\theta} - 1}{e^{i\theta} - 1} + e^{i(A-1)\theta}\right| \geqslant \left|\frac{e^{i(A-1)\theta} - 1}{e^{i\theta} - 1}\right| - 1, \tag{6.209}$$

мы тем не менее можем прийти к выводу, что

$$\left|\frac{e^{iA\theta} - 1}{e^{i\theta} - 1}\right| \geqslant \frac{2(A-1)|\theta|}{\pi|\theta|} - 1 = \frac{2}{\pi}A - \left(1 + \frac{2}{\pi}\right). \tag{6.210}$$

Пренебрегая возможной поправкой порядка $2/A$, мы находим

$$\text{Prob}(y) \geqslant \left(\frac{4}{\pi^2}\right)\frac{1}{r} \tag{6.211}$$

для каждого из r значений y, удовлетворяющих неравенству (6.205). Следовательно, с вероятностью, не ниже чем $4/\pi^2$ измеренное значение y будет удовлетворять

$$k\frac{N}{r} - \frac{1}{2} \leqslant y \leqslant k\frac{N}{r} + \frac{1}{2}, \tag{6.212}$$

или

$$\frac{k}{r} - \frac{1}{2N} \leqslant \frac{y}{N} \leqslant \frac{k}{r} + \frac{1}{2N}, \tag{6.213}$$

где k — целое число, выбранное из $\{0, 1, 2, \ldots, r-1\}$. Результат вычисления с разумной вероятностью находится не дальше чем на расстоянии $1/2$ от целого кратного числа N/r.

Пусть нам известно, что $r < M \ll N$. Таким образом, N/r — рациональное число со знаменателем, меньше m. Два различных рациональных числа, знаменатель каждого из которых меньше M, не могут быть ближе друг к другу чем на $1/M^2$, так как $\frac{a}{b} - \frac{c}{d} = \frac{ad-bc}{bd}$. Если результат измерения y удовлетворяет неравенству (6.212), то существует *единственное* значение k/r (при $r < M$), определяемое y/N, при условии, что $N \geqslant M^2$. Это значение k/r может быть успешно извлечено из измеренного y/N с помощью метода цепных дробей.

С вероятностью, превышающей $4/\pi^2$, мы нашли значение k/r, где k выбирается (примерно равновероятно) из $\{0, 1, 2, \ldots, r-1\}$. С приемлемой вероятностью k и r являются взаимно простыми (не имеющими общего множителя), так что мы добились успеха в отыскании r. Обратившись к оракулу, мы можем проверить, действительно ли $f(x) = f(x+r)$. Но если $\text{GCD}(k, r) \neq 1$,[1] то мы нашли всего лишь r_1, множитель r.

Если мы не достигли успеха, то мы могли бы проверить некоторые близкие значения y [измеренное значение могло оказаться вблизи интервала $-r/2 \leqslant yr(\text{mod}N) \leqslant r/2$, в действительности не находясь внутри его] или проверить несколько множителей r [значение $\text{GCD}(k, r)$, если оно не равно единице, по-видимому, невелико]. Если не удается и это, то мы прибегнем к повторению квантовой схемы, получая (с вероятностью не ни-

[1] GCD (Greatest Common Divisor) — наибольший общий делитель. — *Прим. перев.*

же $4/\pi^2$) на этот раз значение k'/r. Теперь k' также может иметь общий множитель с r, в таком случае наша процедура вновь определяет r_2, множитель r. Но с достаточно высокой вероятностью $\mathrm{GCD}(k, k') = 1$, в таком случае $r = \mathrm{LCM}(r_1, r_2)$.[1] Действительно, мы можем вычислить вероятность того, что случайно выбранные k и k' являются взаимно простыми, следующим образом. Так как вероятность того, что простое число p делит случайно выбранное число, равна $1/p$, то вероятность того, что p делит без остатка оба k и k', равна $1/p^2$. А k и k' являются взаимно простыми тогда и только тогда, когда не существует простого числа p, делящего их обоих без остатка. Следовательно,

$$\text{Prob}(k, k' \text{ взаимно простые}) = \prod_{\text{простые } p} \left(1 - \frac{1}{p^2}\right) = \frac{1}{\zeta(2)} = \frac{6}{\pi^2} \simeq 0{,}607 \quad (6.214)$$

[где $\zeta(z)$ обозначает дзета-функцию Римана]. Таким образом, после некоторого постоянного (не зависящего от N) количества повторений алгоритма мы наверняка добьемся успеха в поиске периода r.

6.9.2. От FFT к QFT

Рассмотрим теперь реализацию квантового преобразования Фурье. Преобразование Фурье

$$\sum_x f(x)|x\rangle \to \sum_y \left(\frac{1}{\sqrt{N}} \sum_x e^{2\pi i xy/N} f(x)\right) |y\rangle \quad (6.215)$$

представляет собой перемножение унитарных $N \times N$-матриц, где матричный (x, y)-элемент равен $\left(e^{2\pi i/N}\right)^{xy}$. С наивной точки зрения это преобразование требует $O(N^2)$ элементарных операций. Существует, однако, хорошо известная и очень полезная (классическая) процедура, сокращающая количество операций до $O(N \log N)$. Предполагая, что $N = 2^n$, представим x и y в виде двоичных разложений

$$\begin{aligned} x &= x_{n-1} \cdot 2^{n-1} + x_{n-2} \cdot 2^{n-2} + \ldots + x_1 \cdot 2 + x_0, \\ y &= y_{n-1} \cdot 2^{n-1} + y_{n-2} \cdot 2^{n-2} + \ldots + y_1 \cdot 2 + y_0. \end{aligned} \quad (6.216)$$

[1] LCM (Least Common Multiple) — наименьшее общее кратное. — *Прим. перев.*

В произведении x и y можно отбросить любые слагаемые, содержащие n-ю и более высокие степени двух, поскольку они не вносят вклада в $e^{2\pi i xy/2^n}$. Следовательно,

$$\frac{xy}{2^n} \equiv y_{n-1}(.x_0) + y_{n-2}(.x_1x_0) + y_{n-3}(.x_2x_1x_0) + \ldots + \\ + y_1(.x_{n-2}x_{n-3}\ldots x_0) + y_0(.x_{n-1}x_{n-2}\ldots x_0), \tag{6.217}$$

где множители в круглых скобках представляют собой значения соответствующих двоичных разрядов, например:

$$x_2x_1x_0 = \frac{x_2}{2} + \frac{x_1}{2^2} + \frac{x_0}{2^3}. \tag{6.218}$$

Теперь мы можем вычислить

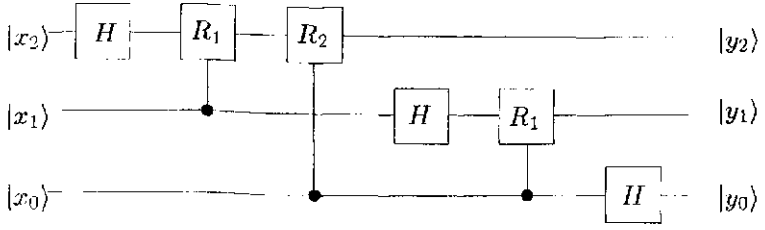
$$\tilde{f}(x) = \frac{1}{\sqrt{N}} \sum_y e^{2\pi i xy/N} f(y) \tag{6.219}$$

для каждого из N значений x. Но сумма по y факторизуется на n сумм по $y_k = 0, 1$, которые могут быть последовательно вычислены за время порядка n.

С помощью квантового параллелизма можно добиться гораздо лучшего результата. Из (6.217) мы получим

$$\begin{aligned} \mathrm{QFT} : |x\rangle \rightarrow & \frac{1}{\sqrt{N}} \sum_y e^{2\pi i xy/N} |y\rangle \\ = & \frac{1}{\sqrt{2^n}} \left(|0\rangle + e^{2\pi i(.x_0)}|1\rangle\right)\left(|0\rangle + e^{2\pi i(.x_1x_0)}|1\rangle\right) \\ & \ldots \left(|0\rangle + e^{2\pi i(.x_{n-1}x_{n-2}\ldots x_0)}|1\rangle\right). \end{aligned} \tag{6.220}$$

QFT преобразует каждое состояние вычислительного базиса в *незапутанное* состояние n кубитов; таким образом, мы ожидаем, что оно может быть эффективно реализовано. Действительно, рассмотрим случай $n = 3$. Нетрудно понять, что эту работу выполняет схема



(но обратим внимание на то, что порядок следования битов на выходе инвертировался). Каждый вентиль Адамара действует как

$$\mathbf{H}\colon |x_k\rangle \to \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i(.x_k)}|1\rangle\right). \tag{6.221}$$

Другие вклады в относительную фазу векторов $|0\rangle$ и $|1\rangle$ в k-ом кубите обеспечиваются двухкубитовыми условными поворотами, где

$$\mathbf{R}_d = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/2^d} \end{pmatrix}, \tag{6.222}$$

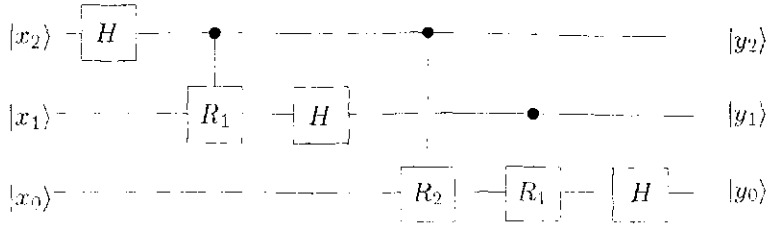
а $d = (k-j)$ – «расстояние» между кубитами.

В случае $n = 3$ QFT строится из трех вентилей $\mathbf{H}$ и трех вентилей контролируемое $\mathbf{R}$. В общем случае очевидное обобщение этой схемы требует n вентилей $\mathbf{H}$ и $\binom{n}{2} = \frac{1}{2}n(n-1)$ контролируемых $\mathbf{R}$. Вновь двухкубитовый вентиль применяется к каждой паре кубитов с контролируемой относительной фазой $\pi/2^d$, где d – «расстояние» между кубитами. Таким образом, семейство схем, осуществляющее QFT, имеет размер порядка $(\log N)^2$.

Мы можем сократить сложность схемы до линейной по $\log N$, если готовы ограничиться реализацией фиксированной точности, поскольку двухкубитовые вентили, действуя на значительно разделенные кубиты, вносят лишь экспоненциально малые фазы. Если мы опустим вентили, действующие на пары, разделенные более чем на m, тогда каждое слагаемое в (6.217) заменяется приближением с m-битовой точностью; полная ошибка в $xy/2^n$ наверняка не хуже, чем $n2^{-m}$, следовательно, мы можем достичь точности ε в $xy/2^n$ при $m \geqslant \log n/\varepsilon$. Если мы сохраним вентили, действующие только на пары кубитов с расстоянием m или менее, то размер схемы будет равен $mn \sim n \log n/\varepsilon$.

Фактически, если мы собираемся измерять в вычислительном базисе непосредственно после выполнения QFT (или его обращения), то возможно дальнейшее упрощение – двухкубитовые вентили не нужны вообще! Заметим, во-первых, что вентиль контролируемое $\mathbf{R}_d$ действует симметричным образом на два кубита — он действует тривиально на $|00\rangle$, $|01\rangle$ и $|10\rangle$ и изменяет фазу $|11\rangle$ на $e^{i\theta_d}$. Таким образом, без модификации вентиля можно менять местами «контрольный» и «целевой» биты. С учетом этой замены наша схема для трехкубитового QFT может быть изображена

заново как



Коль скоро $|y_0\rangle$ измерено, нам *известно* значение бита, который управляет вентилем $\mathbf{R}_1$, действующим на два первых кубита. Следовательно, мы получим то же самое распределение вероятностей результатов измерений, если вместо применения контролируемого $\mathbf{R}_1$ и последующего измерения мы сначала измерим y_0, а затем применим к следующему кубиту поворот $(\mathbf{R}_1)^{y_0}$, обусловленный результатом измерения первого кубита. Аналогично можно заменить вентили контролируемое $\mathbf{R}_1$ и контролируемое $\mathbf{R}_2$ однокубитовым поворотом

$$(\mathbf{R}_2)^{y_0}(\mathbf{R}_1)^{y_1} \tag{6.223}$$

[то есть поворотом с относительной фазой $\pi(.y_1y_0)$], действующим на третий кубит *после* того, как были измерены значения y_1 и y_0.

В общем случае, если мы собираемся измерять после выполнения QFT, то для его осуществления необходимо только n вентилей Адамара и $n-1$ однокубитовых поворотов. Процедура QFT замечательно проста!

6.10. Факторизация

6.10.1. Факторизация как отыскание периода

Что связывает проблему факторизации (поиск простых множителей большого составного положительного целого числа) с периодичностью? Существует хорошо известная (рандомизованная) редукция факторизации к определению периода функции. Хотя эта редукция непосредственно не связана с квантовыми вычислениями, мы обсудим ее здесь для полноты, а также и потому, что перспектива использования квантового компьютера как инструмента факторизации вызывает столь сильное волнение.

Допустим, мы хотим найти множитель n-битового числа N. Выберем псевдослучайным образом $a < N$ и вычислим наибольший общий дели-

тель $\mathrm{GCD}(a, N)$, что можно эффективно [за время порядка $(\log N)^3$] выполнить с помощью алгоритма Евклида. Если $\mathrm{GCD}(a, N) \neq 1$, тогда GCD является нетривиальным множителем числа N и задача решена. Но предположим, что $\mathrm{GCD}(a, N) = 1$.

Отступление: алгоритм Евклида. Чтобы вычислить $\mathrm{GCD}(N_1, N_2)$ (при $N_1 > N_2$) разделим сначала N_1 на N_2, получая остаток R_1. Затем разделим N_2 на R_1, получая остаток R_2. Разделим R_1 на R_2 *и так далее* до тех пор, пока не получим в остатке нуль. Последний ненулевой остаток и есть $R = \mathrm{GCD}(N_1, N_2)$. Чтобы убедиться в том, что алгоритм работает, заметим лишь, что: (1) на R делятся все предыдущие остатки и, следовательно, N_1 и N_2; (2) *любое* число, на которое делятся N_1 и N_2, делит все остатки, включая R. Общий делитель N_1 и N_2, который в свою очередь делится на все остальные общие делители этих чисел, есть не что иное как $\mathrm{GCD}(N_1, N_2)$. Чтобы понять, сколько времени занимает алгоритм Евклида, заметим, что

$$R_j = qR_{j+1} + R_{j+2}, \tag{6.224}$$

где $q \geqslant 1$, а $R_{j+2} < R_{j+1}$; следовательно, $R_{j+2} < \frac{1}{2}R_j$. Два деления сокращают остаток как минимум в два раза, так что требуется не более чем $2\log N_1$ делений, каждое из которых использует $O\big((\log N)^2\big)$ элементарных операций; полное количество операций имеет порядок $O\big((\log N)^3\big)$.

Числа $a < N$, взаимно простые с N (не имеющие общего множителя с N), образуют конечную группу относительно умножения по модулю N. [Почему? Нам нужно установить, что каждый элемент a имеет обратный. Но для данного $a < N$, взаимно простого с N, и каждого $b < N$, пробегающего все взаимно простые с N значения, все произведения $ab \pmod N$ различны[1]. Следовательно, для некоторого b мы должны иметь $ab \equiv 1 \pmod N$; таким образом, число, обратное к a, существует.] Каждый элемент a этой конечной группы имеет конечный *порядок* r, наименьшее положительное целое число такое, что

$$a^r \equiv 1 \pmod N. \tag{6.225}$$

Порядок a по модулю N является периодом функции

$$f_{N,a}(x) = a^x \pmod N. \tag{6.226}$$

[1] Если N — делитель числа $ab - ab'$, то оно должно делителем и $b - b'$.

Мы знаем, что существует эффективный квантовый алгоритм, позволяющий найти период функции; следовательно, если мы можем эффективно вычислить $f_{N,a}$, то также эффективно можем найти и порядок a.

На первый взгляд, вычисление $f_{N,a}$ может показаться трудным, поскольку показатель степени x может быть очень большим. Но если $x < 2^m$ и мы представляем x в виде двоичного разложения

$$x = x_{m-1} \cdot 2^{m-1} + x_{m-2} \cdot 2^{m-2} + \ldots + x_1 \cdot 2 + x_0, \tag{6.227}$$

то

$$a^x (\mathrm{mod}\, N) = \left(a^{2^{m-1}}\right)^{x_{m-1}} \left(a^{2^{m-2}}\right)^{x_{m-2}} \cdots (a)^{x_0} (\mathrm{mod}\, N). \tag{6.228}$$

Каждое a^{2^j} имеет большой показатель степени, тем не менее оно может быть эффективно вычислено *классическим* компьютером путем повторного возведения в квадрат:

$$a^{2^j} (\mathrm{mod}\, N) = \left(a^{2^{j-1}}\right)^2 (\mathrm{mod}\, N). \tag{6.229}$$

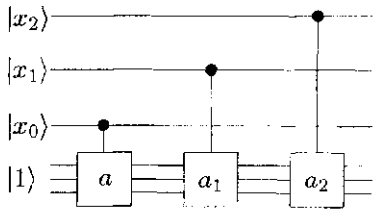
То есть необходимо только $m-1$ (классических) умножений по модулю N, чтобы собрать таблицу всех a^{2^j}.

Вычисление $a^x (\mathrm{mod}\, N)$ выполняет программа

INPUT 1

For $j = 0$ to $m-1$, if $x_j = 1$, MULTIPLY a^{2^j}.

Она требует максимум m умножений по модулю N, каждое из которых требует порядка $(\log N)^2$ элементарных операций[1]. Поскольку $r < N$, у нас будут неплохие шансы успешно выделить период, если выбрать $m \sim 2 \log N$. Следовательно, вычисление $f_{N,a}$ может быть выполнено семейством схем размера $O\left((\log N)^3\right)$, имеющих следующую структуру:



[1] Используя разные трюки для выполнения эффективного перемножения очень больших чисел, количество элементарных операций можно сократить до $O(\log N \log\log N \times \times \log\log\log N)$; таким образом, асимптотически при больших N семейство схем размера $O(\log^2 N \log\log N \log\log\log N)$ может вычислить $f_{N,a}$.

Умножение на a^{2^j} выполняется, если контрольный кубит x_j имеет значение 1.

Предположим, что мы нашли r, период a по модулю N. Тогда, *если* r четное, то

$$N \text{ является делителем числа } \left(a^{r/2}+1\right)\left(a^{r/2}-1\right). \tag{6.230}$$

Очевидно, что N не делит $\left(a^{r/2}-1\right)$; если бы это было так, то порядок a был бы $\leqslant r/2$. Таким образом, *если* наряду с этим N не является делителем $\left(a^{r/2}+1\right)$ или

$$a^{r/2} \neq -1 (\mathrm{mod}\, N), \tag{6.231}$$

тогда N должен иметь нетривиальный общий множитель с каждым из $a^{r/2}\pm 1$. Следовательно, $\mathrm{GCD}(N, a^{r/2}+1) \neq 1$ является множителем N (что можно эффективно определить с помощью классических вычислений), то есть задача решена.

Таким образом, коль скоро найдено r, мы успешно факторизовали N, за исключением случаев, когда (1) r нечетное или (2) r четное и $a^{r/2} \equiv -1 (\mathrm{mod}\, N)$. Насколько вероятен этот успех?

Допустим, что N является произведением двух простых множителей $p_1 \neq p_2$:

$$N = p_1 p_2 \tag{6.232}$$

(это фактически самый неблагоприятный случай). Для каждого $a < p_1 p_2$ существуют единственные $a_1 < p_1$ и $a_2 < p_2$ такие, что

$$\begin{aligned} a &\equiv a_1 (\mathrm{mod}\, p_1), \\ a &\equiv a_2 (\mathrm{mod}\, p_2). \end{aligned} \tag{6.233}$$

Следовательно, случайный выбор $a < N$ эквивалентен случайному выбору $a_1 < p_1$ и $a_2 < p_2$.

Отступление: мы используем **Китайскую теорему об остатках**. Решение a уравнений (6.233) единственно, поскольку если a и b являются решениями, то p_1 и p_2 должны быть делителями $a-b$. Решение существует, поскольку каждое $a < p_1 p_2$ решает уравнения (6.233) при *некоторых* a_1 и a_2. А так как имеется ровно $p_1 p_2$ способов выбрать a_1 и a_2 и ровно $p_1 p_2$ способов выбрать a, то единственность означает, что для каждой пары a_1, a_2 существует соответствующее ей a.

Пусть теперь r_1 обозначает порядок a_1 по модулю p_1, а r_2 – порядок a_2 по модулю p_2. Китайская теорема об остатках утверждает, что $a^r \equiv 1 (\mathrm{mod}\, p_1 p_2)$ эквивалентно тому, что

$$\begin{aligned} a_1^r &\equiv 1 (\mathrm{mod}\, p_1), \\ a_2^r &\equiv 1 (\mathrm{mod}\, p_2). \end{aligned} \tag{6.234}$$

Следовательно, $r = \mathrm{LCM}(r_1, r_2)$. Если r_1 и r_2 оба нечетны, то таковым же является r, и мы проигрываем.

Но если *одно* из двух чисел, r_1 или r_2, четное, то таковым же является r, и мы продолжаем игру. Если

$$\begin{aligned} a_1^{r/2} &\equiv -1 (\mathrm{mod}\, p_1), \\ a_2^{r/2} &\equiv -1 (\mathrm{mod}\, p_2), \end{aligned} \tag{6.235}$$

то $a^{r/2} \equiv -1 (\mathrm{mod}\, p_1 p_2)$, и мы снова проигрываем. Но если или

$$\begin{aligned} a_1^{r/2} &\equiv -1 (\mathrm{mod}\, p_1), \\ a_2^{r/2} &\equiv 1 (\mathrm{mod}\, p_2), \end{aligned} \tag{6.236}$$

или

$$\begin{aligned} a_1^{r/2} &\equiv 1 (\mathrm{mod}\, p_1), \\ a_2^{r/2} &\equiv -1 (\mathrm{mod}\, p_2), \end{aligned} \tag{6.237}$$

то $a^{r/2} \not\equiv -1 (\mathrm{mod}\, p_1 p_2)$, и мы выигрываем. [Конечно, одновременное равенство $a_1^{r/2} \equiv 1 (\mathrm{mod}\, p_1)$ и $a_2^{r/2} \equiv 1 (\mathrm{mod}\, p_2)$ невозможно, что означало бы $a^{r/2} \equiv 1 (\mathrm{mod}\, p_1 p_2)$, то есть r не могло бы быть порядком a.]

Допустим, что

$$\begin{aligned} r_1 &= 2^{c_1} \cdot (\text{нечетное число}), \\ r_2 &= 2^{c_2} \cdot (\text{нечетное число}), \end{aligned} \tag{6.238}$$

где $c_1 > c_2$. Тогда $r = \mathrm{LCM}(r_1, r_2) = 2r_2 \cdot (\text{целое число})$, так что $a^{r/2} \equiv 1 (\mathrm{mod}\, p_2)$, а уравнения (6.236) удовлетворяются – мы победили! Аналогично $c_2 > c_1$ подразумевает уравнение (6.237) – мы снова в выигрыше! Но при $c_1 = c_2$ имеет место $r = r_1 \cdot (\text{нечетное число}) = r_1 \cdot (\text{нечетное число}')$, так что удовлетворяются уравнения (6.235) – в таком случае мы проиграли.

Итак, все сводится к альтернативе: при $c_1 = c_2$ мы проигрываем, а при $c_1 \neq c_2$ – побеждаем. Насколько вероятно, что $c_1 \neq c_2$?

Полезно знать, что мультипликативная группа по модулю p является циклической — она имеет такой образующий элемент порядка $p-1$, что все элементы являются его степенями. [Почему? Множество целых чисел по модулю p образуют конечное *поле*. Если бы группа не была циклической, то максимальный порядок ее элементов был бы $q < p-1$, так что $x^q \equiv 1 (\mathrm{mod}\, p)$ имело бы $p-1$ решений. Но это невозможно: на конечном поле существует не более чем q корней q-ой степени из единицы.]

Допустим, что $p - 1 = 2^k \cdot s$, где s — нечетное, и рассмотрим порядки всех элементов циклической группы порядка $p-1$. Для краткости мы обсудим только самый неблагоприятный для нас случай $k = 1$. Тогда, если b является образующим элементом (имеет порядок $2s$), то четные степени b имеют нечетный порядок, а нечетные — порядок $2 \cdot$ (нечетное число). Тогда в этом случае $r = 2^c \cdot$ (нечетное число), где c с равной вероятностью принимает одно из значений $\{0, 1\}$. Следовательно, если p_1 и p_2 оба такого (неподходящего) типа, а a_1, a_2 выбираются случайно, вероятность того, что $c_1 \neq c_2$, равна $1/2$. Следовательно, раз мы нашли r, то вероятность успешного отыскания множителя как минимум равна $1/2$, если N является произведением двух простых чисел. Если же N имеет больше двух различных простых множителей, то наши нечетные числа даже лучше. Этот метод терпит неудачу, если N является степенью простого числа $N = p^\alpha$, но степени простых чисел успешно факторизуются другими методами.

6.10.2. RSA

Интересует ли кого-нибудь, простой или трудной является факторизация? Некоторых это очень интересует.

Предполагаемая сложность факторизации является основой надежности широко используемой схемы RSA для криптографии с открытым ключом[1], которой вы можете воспользоваться, даже если посылаете через интернет номер своей кредитной карточки.

Идея криптографии с открытым ключом заключается в том, чтобы избежать необходимости обмена секретным ключом (который может быть перехвачен и скопирован) между желающими установить связь с партнерами. Шифрующий ключ общеизвестен. Но его использование для того,

[1] R. L. Rivest, A. Shamir, L. M. Adleman, *A Method of Obtaining Digital Signatures and Public-Key Cryptosystems*, Comm. ACM, **21(2)**, 120–126 (1978).

чтобы извлечь дешифрующий ключ, требует непомерно сложных вычислений. Следовательно, Боб может послать шифрующий ключ Алисе и кому угодно, но только он будет в состоянии декодировать сообщение, которое Алиса (или кто-нибудь другой) закодирует с помощью этого ключа. Кодирование является «односторонней функцией», которую легко вычислить, но очень трудно обратить.

(Конечно, Алиса и Боб могли бы избежать необходимости обмена открытым ключом, если бы они выбрали конфиденциальный ключ во время их предыдущей тайной встречи. Например, они могли бы договориться использовать длинную случайную строку в качестве разового шифра для кодирования и декодирования. Но, возможно, Алиса и Боб никогда не задумывались о том, что однажды им понадобится тайно связаться друг с другом. Или, возможно, ранее они договорились использовать разовый шифр, но уже израсходовали свои тайные ключи и не имеют желания вновь пользоваться ими, опасаясь, что тогда их код смогут взломать шпионы. Сейчас они слишком далеко друг от друга, чтобы безопасно обменяться новым тайным ключом; их самым надежным выбором оказывается криптография с открытым ключом.)

Чтобы построить открытый ключ, Боб выбирает два больших простых числа p и q. Но он не открывает их значения, а вместо этого вычисляет произведение

$$N = pq. \tag{6.239}$$

Поскольку Боб знает разложение N на простые множители, то ему известно и значение функции Эйлера $\varphi(N)$ — количества чисел, меньших чем N, являющихся взаимно простыми с N. В случае произведения двух простых чисел это

$$\varphi(N) = N - p - q + 1 = (p-1)(q-1) \tag{6.240}$$

(только числа, кратные p и q, имеют общий множитель с N). Найти $\varphi(N)$ несложно, если вы знаете разложение N на простые множители, но это трудно, если вам известно только N.

Затем Боб псевдослучайным образом выбирает $e < \varphi(N)$, взаимно простое с $\varphi(N)$. Он открывает Алисе (и любому подслушивающему) значения N и e, но ничего сверх этого.

Алиса преобразует свое сообщение в ASCII[1], число $a < N$. Она кодирует сообщение, вычисляя

$$b = f(a) = a^e (\mathrm{mod}\, N), \tag{6.241}$$

[1] ASCII — American Standard Code for Information Interchange — американский стандарт кода для обмена информацией. — *Прим. перев.*

что можно быстро выполнить путем повторного возведения в квадрат. Как теперь Бобу декодировать это сообщение?

Допустим, что a является взаимно простым с N (что имеет подавляющую вероятность, если p и q очень большие — во всяком случае Алиса может проверить это прежде, чем кодировать). Тогда

$$a^{\varphi(N)} \equiv 1 (\mathrm{mod}\, N) \tag{6.242}$$

(теорема Эйлера). Это так, поскольку числа, меньшие N и взаимно простые с N, образуют группу [порядка $\varphi(N)$] относительно умножения по модулю N. Порядок любого элемента группы должен быть делителем порядка группы (степени a образуют подгруппу). Поскольку $\mathrm{GCD}(e, \varphi(N)) = 1$, то нам известно, что e имеет мультипликативное обратное $d = e^{-1}$ по модулю $\varphi(N)$:

$$ed \equiv 1 (\mathrm{mod}\, \varphi(N)). \tag{6.243}$$

Значение d является строго сохраняемым секретом Боба; он использует его для декодирования, вычисляя

$$\begin{aligned} f^{-1}(b) &= b^d (\mathrm{mod}\, N) = \\ &= a^{ed} (\mathrm{mod}\, N) = \\ &= a\left(a^{\varphi(N)}\right)^{(\text{целое число})} (\mathrm{mod}\, N) = \\ &= a (\mathrm{mod}\, N). \end{aligned} \tag{6.244}$$

Отступление. Как Бобу вычислить $d = e^{-1}$? Мультипликативное обратное является побочным продуктом выполнения алгоритма Евклида вычисления $\mathrm{GCD}(e, \varphi(N)) = 1$. Проследим цепочку остатков снизу вверх, начиная с $R_n = 1$:

$$\begin{aligned} 1 = R_n &= R_{n-2} - q_{n-1} R_{n-1}, \\ R_{n-1} &= R_{n-3} - q_{n-2} R_{n-2}, \\ R_{n-2} &= R_{n-4} - q_{n-3} R_{n-3} \\ &\qquad \text{и так далее} \ldots \end{aligned} \tag{6.245}$$

(где q_j — частные), так что

$$\begin{aligned} 1 &= (1 + q_{n-1} q_{n-2}) R_{n-2} - q_{n-1} R_{n-3}, \\ 1 &= \left(-q_{n-1} - q_{n-3}(1 + q_{n-1} q_{n-2})\right) R_{n-3} + (1 + q_{n-1} q_{n-2}) R_{n-4} \\ &\qquad \text{и так далее} \ldots. \end{aligned} \tag{6.246}$$

Продолжая, мы можем выразить единицу через линейную комбинацию любых двух следующих друг за другом остатков; в конце концов, мы пройдем весь путь вплоть до

$$1 = d \cdot e + q \cdot \varphi(N) \tag{6.247}$$

и идентифицируем d как $e^{-1}(\mathrm{mod}\,\varphi(N))$.

Конечно, если Ева имеет средство сверхбыстрой факторизации, то RSA-схема ненадежна. Она факторизует N, найдет $\varphi(N)$ и быстро вычислит d. На самом деле ей даже не нужно факторизовать N; достаточно вычислить порядок по модулю N закодированного сообщения $a^e(\mathrm{mod}\,N)$. Так как e является взаимно простым с $\varphi(N)$, то порядок $a^e(\mathrm{mod}\,N)$ тот же самый, что и порядок a (оба элемента генерируют одну и ту же *орбиту* или циклическую подгруппу). Как только порядок $\mathrm{Ord}(a)$ становится известен, Ева вычисляет $\tilde{d}$ такое, что

$$\tilde{d}e \equiv 1(\mathrm{mod}\,\mathrm{Ord}(a)), \tag{6.248}$$

так что

$$\left(a^e\right)^{\tilde{d}} \equiv a \cdot \left(a^{\mathrm{Ord}(a)}\right)^{(\text{целое число})} \equiv a(\mathrm{mod}\,N), \tag{6.249}$$

и Ева может дешифровать сообщение. Если нашей единственной целью является взлом RSA, то мы обратимся к алгоритму Шора, чтобы найти $r = \mathrm{Ord}(a^e)$, и нас не должно беспокоить то, можем мы или нет использовать r, чтобы выделить множитель N.

Насколько важна такая перспектива криптографических применений квантовых вычислений? Когда быстрые квантовые компьютеры станут доступной реальностью, заинтересованные стороны могут прекратить использование RSA или могут использовать более длинные ключи, чтобы оставаться на шаг впереди современной техники. Однако люди, имеющие секреты, иногда хотят, чтобы их сообщения до поры (лет 30?) оставались конфиденциальными. Их могут не устроить более длинные ключи, если они не уверены относительно темпов будущих технологических достижений.

А если они избегают RSA, то чем они будут пользоваться вместо этого? Известно не так много подходящих односторонних функций, да и они, а не только RSA, (могут быть) беззащитны перед квантовой атакой. То есть на самом деле многое поставлено на карту. Если станут доступными быстрые большие квантовые компьютеры, то зашифрованная информация станет легко доступной.

Но квантовая теория, одной рукой отбирая, другой дает; квантовые компьютеры могут скомпрометировать схемы открытых ключей, но вместе с этим — предложить альтернативу: обсуждавшееся в четвертой главе безопасное распределение квантового ключа.

6.11. Определение фазы

Существует альтернативный взгляд на алгоритм факторизации (предложенный Китаевым), углубляющий наше понимание того, как он работает: мы можем факторизовать, поскольку можем эффективно и точно измерять собственные значения некоторого унитарного оператора.

Рассмотрим $a < N$, взаимно простое с N. Пусть x принимает значения из $\{0, 1, 2, \ldots, N-1\}$ и пусть $\mathbf{U}_a$ обозначает унитарный оператор

$$\mathbf{U}_a \; : \; |x\rangle \; \rightarrow \; |ax(\mathrm{mod}\, N)\rangle. \tag{6.250}$$

Этот оператор унитарен (перестановка вычислительного базиса), поскольку умножение на a по модулю N обратимо.

Если порядок a по модулю N равен r, то

$$\mathbf{U}_a^r = \mathbf{1}. \tag{6.251}$$

Отсюда следует, что все собственные значения $\mathbf{U}_a$ являются корнями степени r из единицы:

$$\lambda_k = e^{2\pi i k/r}, \quad k \in \{0, 1, 2, \ldots, r-1\}. \tag{6.252}$$

Соответствующими собственными состояниями являются

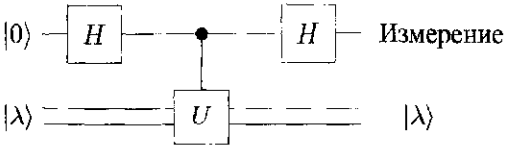
$$|\lambda_k\rangle = \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} e^{-2\pi i k j/r} |a^j x_0 (\mathrm{mod}\, N)\rangle; \tag{6.253}$$

существует r взаимно ортогональных состояний, связанных с каждой орбитой длины r, генерируемой умножением на a.

Оператор $\mathbf{U}_a$ не эрмитов, но его *фаза* (эрмитов оператор, генерирующий $\mathbf{U}_a$) является наблюдаемой величиной. Предположим, что мы можем выполнить измерение, которое проецирует на базис собственных состояний $\mathbf{U}_a$ и определяет значение λ_k, с равной вероятностью выбираемое из возможных собственных значений. Следовательно, измерение определяет

значение k/r, что делает процедура Шора, и мы можем с приемлемо высокой вероятностью успеха получить множитель N. Но как измерить собственные значения унитарного оператора?

Допустим, что мы можем выполнить унитарное преобразование U, обусловленное контрольным битом, и рассмотрим схему



Здесь $|\lambda\rangle$ обозначает собственное состояние U, соответствующее собственному значению λ ($\mathrm{U}|\lambda\rangle = \lambda|\lambda\rangle$). Тогда действие схемы на контрольный бит имеет вид

$$|0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + \lambda|1\rangle) \rightarrow$$
$$\rightarrow \frac{1}{2}(1+\lambda)|0\rangle + \frac{1}{2}(1-\lambda)|1\rangle). \tag{6.254}$$

Тогда результат измерения контрольного кубита имеет распределение вероятностей

$$\begin{aligned} \mathrm{Prob}(0) &= \left|\frac{1}{2}(1+\lambda)\right|^2 = \cos^2 \pi\phi, \\ \mathrm{Prob}(1) &= \left|\frac{1}{2}(1-\lambda)\right|^2 = \sin^2 \pi\phi, \end{aligned} \tag{6.255}$$

где $\lambda = e^{2\pi i\phi}$.

Как мы обсуждали ранее (например, в связи с проблемой Дойча), эта процедура с уверенностью различает собственные значения $\lambda = 1$ ($\phi = 0$) и $\lambda = -1$ ($\phi = 1/2$). Но также могут быть различимы и другие возможные значения λ, хотя и с меньшей статистической достоверностью. Например, предположим, что состояние, на которое действует U, является суперпозицией его собственных состояний

$$\alpha_1|\lambda_1\rangle + \alpha_2|\lambda_2\rangle. \tag{6.256}$$

Предположим также, что мы n раз выполняем изображенную выше схему с n индивидуальными контрольными битами. Таким образом, мы готовим

состояние

$$\alpha_1|\lambda_1\rangle\left(\frac{1+\lambda_1}{2}|0\rangle+\frac{1-\lambda_1}{2}|1\rangle\right)^{\otimes n}+ \\ +\alpha_2|\lambda_2\rangle\left(\frac{1+\lambda_2}{2}|0\rangle+\frac{1-\lambda_2}{2}|1\rangle\right)^{\otimes n}. \quad (6.257)$$

Если $\lambda_1 \neq \lambda_2$, то при больших n перекрытие между двумя состояниями n контрольных битов экспоненциально мало; измеряя контрольные биты, мы можем, как минимум в отличном приближении, выполнить ортогональное проецирование на базис $\{|\lambda_1\rangle, |\lambda_2\rangle\}$.

Если мы используем достаточно контрольных битов, то в нашем распоряжении имеется достаточно большая выборка, чтобы с приемлемой статистической надежностью измерить $\mathrm{Prob}(0) = \frac{1}{2}(1+\cos 2\pi\phi)$. Выполняя контролируемое $i\mathbf{U}$, мы можем также измерить $\frac{1}{2}(1+\sin 2\pi\phi)$, что достаточно для определения ϕ по модулю целое число.

Однако в алгоритме факторизации нам необходимо измерять фазу $e^{2\pi ik/r}$ с экспоненциальной точностью, что, похоже, требует экспоненциального количества испытаний. Допустим все же, что мы можем эффективно вычислять высокие степени $\mathbf{U}$ (как в случае с $\mathbf{U}_a$), такие как

$$\mathbf{U}^{2^j}. \quad (6.258)$$

С помощью описанной выше процедуры измерения $\mathbf{U}^{2^j}$ мы определяем

$$\exp\left(2\pi i 2^j\phi\right), \quad (6.259)$$

где $e^{2\pi i\phi}$ — собственное значение оператора $\mathbf{U}$. Следовательно, измерение $\mathbf{U}^{2^j}$ с точностью до одного бита эквивалентно измерению j-го бита собственного значения $\mathbf{U}$.

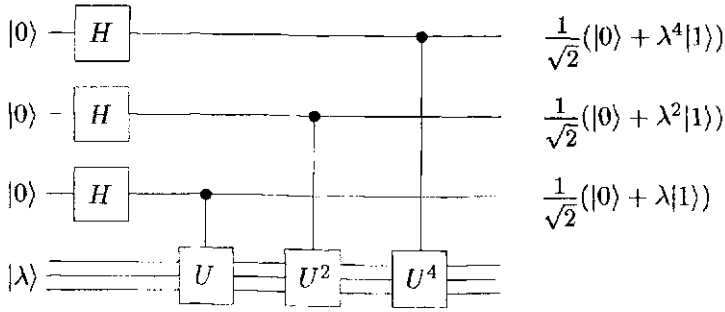
Мы можем использовать эту процедуру определения фазы для отыскания порядка и, следовательно, факторизации. Обратим уравнение (6.253), чтобы получить

$$|x_0\rangle = \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}|\lambda_k\rangle\,; \quad (6.260)$$

каждое состояние вычислительного базиса (при $x_0 \neq 0$) является равновзвешенной суперпозицией r собственных состояний $\mathbf{U}_a$.

Измеряя собственное значение, мы получаем $\lambda_k = e^{2\pi i k/r}$ с k, равновероятно выбирающимся из $\{0, 1, 2, \ldots, r-1\}$. Если $r < 2^n$, то, чтобы определить k/r, мы измеряем с точностью до $2n$ битов. В принципе мы можем выполнять эту процедуру на компьютере, который хранит меньше кубитов, чем это необходимо для вычисления QFT, потому что всякий раз мы можем приступать к определению только одного бита из k/r.

Но поучительно представить, что мы включаем QFT в процедуру определения фазы. Предположим, что схема



действует на собственное состояние $|\lambda\rangle$ унитарного преобразования $\mathbf{U}$. Условный оператор $\mathbf{U}$ готовит состояние $\frac{1}{\sqrt{2}}(|0\rangle + \lambda|1\rangle)$, условный оператор $\mathbf{U}^2$ готовит $\frac{1}{\sqrt{2}}(|0\rangle + \lambda^2|1\rangle)$, а условный оператор $\mathbf{U}^4$ — $\frac{1}{\sqrt{2}}|0\rangle + \lambda^4|1\rangle)$ и так далее. Мы могли бы выполнить преобразование Адамара и измерить каждый из этих кубитов, чтобы получить распределение вероятностей, управляющее j-м битом ϕ, где $\lambda = e^{2\pi i\phi}$. Но целесообразнее заметить, что приготовленное схемой состояние равно

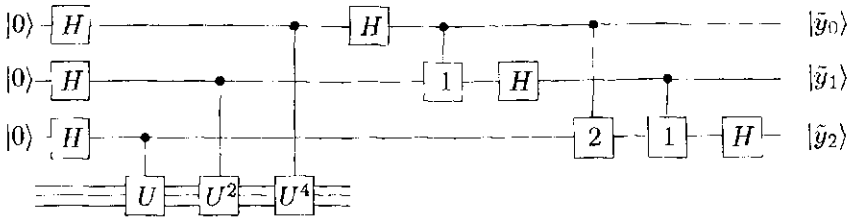
$$\frac{1}{\sqrt{2^m}} \sum_{y=0}^{2^m-1} e^{2\pi i \phi y} |y\rangle. \tag{6.261}$$

Лучший способ узнать значение ϕ — выполнить перед измерением $\mathrm{QFT}^{(m)}$, а не преобразование Адамара $\mathbf{H}^{(m)}$.

Рассмотрим для ясности случай $m = 3$. Схема, которая готовит состояние

$$|x_0\rangle = \frac{1}{\sqrt{8}} \sum_{k=0}^{7} e^{2\pi i \phi y} |y\rangle, \tag{6.262}$$

а затем выполняет его Фурье-анализ, имеет вид



Эта схема почти полностью выполняет описанную выше стратегию определения фазы, но со значительной модификацией. Прежде чем мы выполняем завершающее преобразование Адамара и измеряем $\tilde{y}_1$ и $\tilde{y}_2$, выполняются некоторые условные фазовые повороты. Это те фазовые повороты, которые отличают $\mathrm{QFT}^{(3)}$ от преобразования Адамара $\mathbf{H}^{(3)}$ и резко повышают эффективность, с которой мы можем извлечь значение ϕ.

Мы можем лучше понять, что делают условные повороты, если предположим, что $\phi = k/8$ при $k \in \{0, 1, 2, \ldots, 7\}$; в этом случае нам известно, что преобразование Фурье будет с вероятностью единица генерировать на выходе $\tilde{y} = k$. Мы можем представить k в виде двоичного разложения

$$k = k_2 k_1 k_0 = k_2 \cdot 4 + k_1 \cdot 2 + k_0. \tag{6.263}$$

Фактически схема для самого младшего значащего бита $\tilde{y}_0$ преобразования Фурье является в точности измерительной схемой Китаева, применяемой к унитарному преобразованию $\mathbf{U}^4$, собственные значения которого равны

$$\left(e^{2\pi i\phi}\right)^4 = e^{i\pi k} = e^{i\pi k_0} = \pm 1. \tag{6.264}$$

Измерительная цепь идеально различает собственные значения ± 1, так что $\tilde{y}_0 = k_0$.

Схема для следующего бита $\tilde{y}_1$ почти такая же, как и измерительная схема для $\mathbf{U}^2$ с собственным значением

$$\left(e^{2\pi i\phi}\right)^2 = e^{i\pi k/2} = e^{i\pi(k_1.k_0)}, \tag{6.265}$$

за исключением того, что добавлен условный фазовый поворот, который умножает фазу на $\exp[-i\pi(.k_0)]$, давая в результате $e^{i\pi k_1}$. Вновь, применяя вслед за измерением преобразование Адамара, мы с определенностью получаем результат $\tilde{y}_1 = k_1$. Аналогично схема для $\tilde{y}_2$ измеряет собственное значение

$$e^{2\pi i\phi} = e^{i\pi k/4} = e^{i\pi(k_2.k_1k_0)}, \tag{6.266}$$

за исключением того, что условный поворот удаляет $e^{i\pi(.k_1k_0)}$, так что результатом с определенностью является $\tilde{y}_2 = k_2$.

Таким образом, QFT наилучшим образом осуществляет программу определения фазы. Сначала мы измеряем значащие биты младших разрядов фазы ϕ и используем приобретенную в измерениях информацию, чтобы улучшить достоверность определения значащих битов следующих разрядов. Имея в виду эту интерпретацию, вы сможете просто запомнить схему для $\mathrm{QFT}^{(n)}$!

6.12. Резюме

Классические схемы. Сложность задачи можно характеризовать размером однородного семейства логических схем, решающих эту задачу. Задача трудная, если размер схемы является суперполиномиальной функцией от размера входа. Один классический универсальный компьютер может эффективно моделировать другой, так что классификация сложности аппаратно-независима. Трехбитовый вентиль Тоффоли является универсальным для классических обратимых вычислений. Обратимый компьютер может моделировать необратимый без значительного замедления и неприемлемых затрат памяти.

Квантовые схемы. Хотя это не доказано, но выглядит правдоподобным, что квантовые схемы полиномиального размера не могут моделироваться классическими вероятностными схемами полиномиального размера ($BQP \neq BPP$); однако для этого достаточно полиномиального пространства ($BQP \subseteq PSPACE$). Квантовая схема с шумом может с приемлемой точностью моделировать идеальную квантовую схему размера T, если каждый квантовый вентиль имеет точность порядка $1/T$. Один универсальный квантовый компьютер может эффективно моделировать другой, так что класс сложности BQP аппаратно независим. Типичный двухкубитовый квантовый вентиль, если он может действовать на любую пару кубитов в приборе, адекватен для универальных квантовых вычислений. Также адекватны вентиль контролируемое NOT плюс типичный однокубитовй вентиль.

Быстрый квантовый поиск. Исчерпывающий поиск маркированного элемента в неструктурированной базе данных из N элементов может быть выполнен с помощью квантового компьютера за время порядка $\sqrt{N}$, но не быстрее. Квадратичное квантовое ускорение также может быть достигнуто для некоторых проблем структурированного поиска, но некоторые проблемы оракула не допускают существенного квантового ускорения. Два участника, каждый из которых имеет в распоряжении таблицу из N

записей, могут локализовать совпадающие строки в их таблицах, обменявшись $O(\sqrt{N}\log N)$ кубитами, явно вступая в конфликт с духом (но не буквой) границы Холево.

Отыскание периода. Используя квантовый параллелизм, можно вычислить квантовое преобразование Фурье в N-мерном пространстве за время порядка $(\log N)^2$ (по сравнению со временем $N\log N$ для классического быстрого преобразования Фурье); если нам нужно сразу после этого выполнять измерение, то для вычисления QFT достаточно однокубитовых вентилей. Таким образом, квантовые компьютеры могут эффективно решать некоторые задачи с периодической структурой, такие как факторизация и задача о дискретном логарифме.

6.13. Упражнения

6.1. Линейное моделирование вентиля Тоффоли. На лекции мы построили n-битовый вентиль Тоффоли $\theta^{(n)}$ из трехбитовых вентилей Тоффоли $\theta^{(3)}$. Схема требовала только одного бита вспомогательного пространства, но количество вентилей было экспоненциально велико по n. Используя более широкое вспомогательное пространство, можно существенно сократить количество вентилей.

a) Найдите вычисляющее $\theta^{(n)}$ семейство схем из $2n-5$ вентилей $\theta^{(3)}$. (Здесь используется $n-3$ вспомогательных битов, которые в конце вычисления возвращаются к своим исходным, равным нулю, значениям.)

b) Найдите вычисляющее $\theta^{(n)}$ семейство схем из $4n-12$ вентилей $\theta^{(3)}$, которое работает независимо от начальных значений вспомогательных битов. (Вновь $n-3$ вспомогательных битов в конце вычисления возвращаются к своим начальным, не обязательно равным нулю, значениям.)

6.2. Универсальный набор квантовых вентилей. Цель этого упражнения — завершить демонстрацию того, что контролируемое NOT и произвольные однокубитовые вентили образуют универсальный набор.

a) Пусть $\mathbf{U}$ — произвольная унитарная 2×2-матрица с единичным определителем. Найдите унитарные преобразования $\mathbf{A}$, $\mathbf{B}$ и $\mathbf{C}$ такие, что

$$\mathbf{ABC} = \mathbf{1}, \tag{6.267}$$

$$\mathbf{A}\sigma_x\mathbf{B}\sigma_x\mathbf{C} = \mathbf{U}. \tag{6.268}$$

[**Указание.** Из конструкции углов Эйлера мы знаем, что

$$\mathbf{U} = \mathbf{R}_z(\psi)\mathbf{R}_y(\theta)\mathbf{R}_z(\phi), \tag{6.269}$$

где, например, $\mathbf{R}_z(\phi)$ обозначает поворот вокруг оси z на угол ϕ. Нам также известно, что, например,

$$\boldsymbol{\sigma}_x\mathbf{R}_z(\phi)\boldsymbol{\sigma}_x = \mathbf{R}_z(-\phi).] \tag{6.270}$$

b) Рассмотрите двухкубитовый *вентиль контролируемой фазы*: он применяет $\mathbf{U} = e^{i\alpha}\mathbf{1}$ ко второму кубиту, если первый кубит имеет значение $|1\rangle$, и действует тривиально в противном случае. Покажите, что фактически он является однокубитовым вентилем.

c) Используя вентили контролируемое NOT и однокубитовые вентили, изобразите схему, реализующую контролируемое U, где U — произвольное унитарное 2×2-преобразование.

6.3. Точность. Цель этого упражнения — установить связь между точностью квантового состояния и точностью соответствующего распределения вероятностей.

a) Пусть $\|\mathbf{A}\|$ обозначает норму оператора $\mathbf{A}$, а

$$\|\mathbf{A}\|_{\mathrm{tr}} = \mathrm{tr}\left[(\mathbf{A}\mathbf{A}^\dagger)^{1/2}\right] \tag{6.271}$$

обозначает *следовую норму*. Покажите, что

$$\|\mathbf{AB}\|_{\mathrm{tr}} \leqslant \|\mathbf{B}\| \cdot \|\mathbf{A}\|_{\mathrm{tr}} \quad \text{и} \quad |\mathrm{tr}\,\mathbf{A}| \leqslant \|\mathbf{A}\|_{\mathrm{tr}}. \tag{6.272}$$

b) Предположим, что $\boldsymbol{\rho}$ и $\tilde{\boldsymbol{\rho}}$ — две матрицы плотности, а $\{|a\rangle\}$ — полный ортонормированный базис. Так что

$$\begin{aligned} P_a &= \langle a|\boldsymbol{\rho}|a\rangle, \\ \tilde{P}_a &= \langle a|\tilde{\boldsymbol{\rho}}|a\rangle \end{aligned} \tag{6.273}$$

— соответствующие распределения вероятностей. Используя (a), покажите, что

$$\sum_a |P_a - \tilde{P}_a| \leqslant \|\boldsymbol{\rho} - \tilde{\boldsymbol{\rho}}\|_{\mathrm{tr}}. \tag{6.274}$$

c) Предположим, что $\boldsymbol{\rho} = |\psi\rangle\langle\psi|$ и $\tilde{\boldsymbol{\rho}} = |\tilde{\psi}\rangle\langle\tilde{\psi}|$ — чистые состояния. Используя (b), покажите, что

$$\sum_a |P_a - \tilde{P}_a| \leqslant 2\||\psi\rangle - |\tilde{\psi}\rangle\|. \tag{6.275}$$

6.4. Поиск в базе данных с непрерывным временем. Квантовая система с n-кубитовым гильбертовым пространством имеет гамильтониан

$$\mathbf{H}_\omega = E|\omega\rangle\langle\omega|, \tag{6.276}$$

где $|\omega\rangle$ — неизвестное состояние вычислительного базиса. Вам нужно найти значение ω с помощью следующей процедуры. Включите не зависящее от времени возмущение $\mathbf{H}'$, так что полным гамильтонианом будет

$$\mathbf{H} = \mathbf{H}_\omega + \mathbf{H}'. \tag{6.277}$$

Приготовьте начальное состояние $|\psi_0\rangle$ и позвольте ему эволюционировать в течение времени T под управлением $\mathbf{H}$. Затем измерьте состояние. По результату измерения вы должны сделать вывод относительно ω.

a) Допустим, что в качестве начального состояния выбрано

$$|s\rangle = \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle, \tag{6.278}$$

а в качестве возмущения

$$\mathbf{H}' = E|s\rangle\langle s|. \tag{6.279}$$

Решите зависящее от времени уравнение Шредингера

$$i\frac{d}{dt}|\psi\rangle = \mathbf{H}|\psi\rangle, \tag{6.280}$$

чтобы найти состояние в момент времени T. Каким следует выбрать T, чтобы оптимизировать вероятность успешного определения ω?

b) Теперь предположим, что $|\psi_0\rangle$ и $\mathbf{H}'$ можно выбрать какими угодно, но мы требуем, чтобы спустя время T состоянием системы было $|\omega\rangle$, так чтобы измерение определяло ω с единичной вероятностью успеха. Выведите нижнюю границу, которой должно удовлетворять T, и сравните с вашим результатом в (a). [**Указание.** Как и в нашем анализе на лекции, сравните эволюцию, управляемую $\mathbf{H}$, с эволюцией, управляемой $\mathbf{H}'$ (случай «пустого оракула»), и используйте уравнение Шредингера, чтобы найти, как быстро состояние, эволюционирующее в соответствии с $\mathbf{H}$, отклоняется от состояния, эволюционирующего в соответствии с $\mathbf{H}'$.]

Часть II

Решение упражнений[1]

[1] Решения упражнений выполнены Эндрю Лэндалом и Джимом Харрингтоном (упр. 4.1, 4.2, 4.6).

Решения упражнений к главе 2

2.1. Точность воспроизведения вероятностной гипотезы

Операторы (матрицы) плотности чистого состояния двухуровневой системы находятся во взаимно однозначном соответствии с точками на поверхности сферы Блоха. Благодаря этому соответствию, мы можем выбрать меру Хаара таких матриц плотности равной обычной евклидовой мере на S^2.[1]

$$d\mu = \frac{\sin\theta d\theta d\varphi.}{4\pi}$$

Если мы извлекаем $|\psi\rangle$ из однородного ансамбля чистых состояний и предполагаем, что извлеченным вслед за ним из того же ансамбля состоянием является $|\phi\rangle$, то усредненная ожидаемая точность воспроизведения нашей гипотезы дается (классическим) математическим ожиданием по обоим выборам:

$$\begin{aligned}
\langle F\rangle &= E_{|\psi\rangle}E_{|\phi\rangle}\left[|\langle\phi|\psi\rangle|^2\right] = E_{|\psi\rangle}E_{|\phi\rangle}\left[\langle\phi|\psi\rangle\langle\psi|\phi\rangle\right] = \\
&= E_{|\psi\rangle}E_{|\phi\rangle}\left[\operatorname{tr}\left(|\phi\rangle\langle\phi|\psi\rangle\langle\psi|\right)\right] = \operatorname{tr}\left(E_{|\psi\rangle}E_{|\phi\rangle}\left[|\phi\rangle\langle\phi|\psi\rangle\langle\psi|\right]\right) = \\
&= \operatorname{tr}\left(E_{|\psi\rangle}\left[|\psi\rangle\langle\psi|\right]E_{|\phi\rangle}\left[|\phi\rangle\langle\phi|\right]\right) = \\
&= \operatorname{tr}\left[\left(\int \tfrac{1}{2}\left(\mathbf{1} + \hat{n}_{|\psi\rangle}\cdot\vec{\boldsymbol{\sigma}}\right)\frac{\sin\theta d\theta d\varphi}{4\pi}\right)\times\right. \\
&\qquad \left.\times\left(\int \tfrac{1}{2}\left(\mathbf{1} + \hat{n}_{|\phi\rangle}\cdot\vec{\boldsymbol{\sigma}}\right)\frac{\sin\theta d\theta d\varphi}{4\pi}\right)\right] = \\
&= \operatorname{tr}\left[\left(\tfrac{1}{2}\mathbf{1}\right)\left(\tfrac{1}{2}\mathbf{1}\right)\right] = \frac{1}{4}\operatorname{tr}\mathbf{1} = \frac{1}{2}.
\end{aligned}$$

То, что усредненная точность воспроизведения равна $\frac{1}{2}$, интуитивно понятно, но мы должны честно выполнить вычисления, чтобы подтвердить правильность нашей интуиции. Особенно работая в квантовом мире!

Прежде чем приступать к решению, я хотел бы объяснить, почему приготовленная измерением матрица плотности может быть записана в виде,

[1] В общем случае отыскание меры Хаара для матриц плотности может оказаться трудной задачей.

данном в условии задачи. Вспомним, что если начальным состоянием квантовой системы является чистое состояние $|\psi\rangle$, то, согласно третьей аксиоме (см. раздел 2.1), измерение наблюдаемой $\mathbf{A}$ с вероятностью $p_n = \langle\psi|\mathbf{P}_n|\psi\rangle$ выбирает проектор $\mathbf{P}_n$ на одно из собственных состояний $\mathbf{A}$ и переводит систему в нормированное чистое состояние

$$|\psi_n\rangle = \frac{\mathbf{P}_n|\psi\rangle}{\langle\psi|\mathbf{P}_n|\psi\rangle^{1/2}}.$$

Это наводит на мысль, что матрица плотности чистого состояния должна трансформироваться в *ансамбль* всех возможных результатов измерения:

$$|\psi\rangle\langle\psi| \to \sum_n p_n|\psi_n\rangle\langle\psi_n|.$$

Но $|\psi_n\rangle\langle\psi_n|$ является именно проектором $\mathbf{P}_n$, так что приготавливаемая измерением матрица плотности с тем же основанием может быть записана в виде

$$|\psi\rangle\langle\psi| \to \sum_n \langle\psi|\mathbf{P}_n|\psi\rangle \boldsymbol{P}_n. \qquad \square$$

Однако следует предостеречь, что такая эволюция верна, если только начальным состоянием системы является чистое состояние. В общем случае, как было показано на лекциях, эволюция матрицы плотности $\boldsymbol{\rho}$ под влиянием измерения (фон Неймана) имеет вид $\boldsymbol{\rho} \to \sum_n \mathbf{P}_n \operatorname{tr}(\boldsymbol{\rho}\mathbf{P}_n)$ (см. раздел 3.1.1).

С данной выше матрицей плотности вычисление точности воспроизведения сравнительно просто:

$$\begin{aligned} F &= \langle\psi|\boldsymbol{\rho}|\psi\rangle = \langle\psi|\big(\mathbf{P}_\uparrow\langle\psi|\mathbf{P}_\uparrow|\psi\rangle + \mathbf{P}_\downarrow\langle\psi|\mathbf{P}_\downarrow|\psi\rangle\big)|\psi\rangle = \\ &= \langle\psi|\mathbf{P}_\uparrow|\psi\rangle\langle\psi|\mathbf{P}_\uparrow|\psi\rangle + \langle\psi|\mathbf{P}_\downarrow|\psi\rangle\langle\psi|\mathbf{P}_\downarrow|\psi\rangle = \\ &= \langle\psi|\mathbf{P}_\uparrow|\psi\rangle^2 + \langle\psi|\mathbf{P}_\downarrow|\psi\rangle^2 = p_\uparrow^2 + p_\downarrow^2 = \\ &= p^2 + (1-p)^2 \qquad\qquad (p \equiv p_\uparrow) \\ &= 2p^2 - 2p + 1. \end{aligned}$$

Чтобы найти *усредненную* точность воспроизведения, необходимо вычислить (классическое) математическое ожидание по всем возможным реализациям состояния $|\psi\rangle$. Поскольку состояния $|\psi\rangle$ распределены *однород-*

но, усредненную точность воспроизведения $\langle F\rangle = E_{|\psi\rangle}[F]$ можно найти, *полагая* однородным распределение $p \in [0,1]$. (Длинный путь состоит в замене $|\psi\rangle$ спинорами или проекторами и усреднении по всем углам.) Это дает следующее значение усредненной точности воспроизведения:

$$\langle F\rangle = \int_0^1 (2p^2 - 2p + 1)dp = \frac{2}{3} - \frac{1}{2} + \frac{1}{6}.$$

Таким образом, выполнение измерения увеличивает точность воспроизведения на $\frac{1}{6}$. Эвристически это можно запомнить, заметив, что с вероятностью $\frac{1}{3}$ состояние $|\psi\rangle$ ориентировано вдоль оси измерения, а соответствующий результат измерения дает $|\psi\rangle$ вдоль этой оси имеет вероятность $\frac{1}{2}$. Вероятность того, что гипотеза верна, равна $\frac{1}{3}\cdot\frac{1}{2}$.

Следует заметить, что, хотя выражения для точности воспроизведения в задачах 2.1 и 2.2 выглядят различными, на самом деле оба они являются частными случаями общего выражения

$$F = \operatorname{tr}\rho_1\rho_2.$$

В задаче 2.1 обе ρ_1 и ρ_2 были чистыми состояниями, а в задаче 2.2 чистое только ρ_1. В общем случае F описывает, насколько подобны два квантовых состояния. Непосредственно видно, что точность воспроизведения является не самой лучшей метрикой, так как, например, $\operatorname{tr}(\rho)^2 = 1$ только в частном случае, когда ρ является проектором. Позже в этом курсе мы найдем более хорошие меры точности воспроизведения.

2.3. Разложение Шмидта

2.3.1. Частичные следы. Решение этой части главным образом получается путем чисто механического применения определений. Начальным состоянием системы является:

$$|\Phi\rangle = \frac{1}{\sqrt{2}}|\uparrow\rangle_A\left(\frac{1}{2}|\uparrow\rangle_B + \frac{\sqrt{3}}{2}|\downarrow\rangle_B\right) + \frac{1}{\sqrt{2}}|\downarrow\rangle_A\left(\frac{\sqrt{3}}{2}|\uparrow\rangle_B + \frac{1}{2}|\downarrow\rangle_B\right) =$$
$$= \frac{1}{\sqrt{8}}\Big(|\uparrow\uparrow\rangle + \sqrt{3}|\uparrow\downarrow\rangle + \sqrt{3}|\downarrow\uparrow\rangle + |\downarrow\downarrow\rangle\Big),$$

что, будучи записанным как оператор плотности, представляет собой:

$$|\Phi\rangle\langle\Phi| = \frac{1}{8}\Big(|\uparrow\uparrow\rangle + \sqrt{3}|\uparrow\downarrow\rangle + \sqrt{3}|\downarrow\uparrow\rangle + |\downarrow\downarrow\rangle\Big) \times$$
$$\times\Big(\langle\uparrow\uparrow| + \sqrt{3}\langle\uparrow\downarrow| + \sqrt{3}\langle\downarrow\uparrow| + \langle\downarrow\downarrow|\Big) =$$
$$= \Big(|\uparrow\uparrow\rangle, |\uparrow\downarrow\rangle, |\downarrow\uparrow\rangle, |\downarrow\downarrow\rangle\Big)\frac{1}{8}\begin{pmatrix} 1 & \sqrt{3} & \sqrt{3} & 1 \\ \sqrt{3} & 3 & 3 & \sqrt{3} \\ \sqrt{3} & 3 & 3 & \sqrt{3} \\ 1 & \sqrt{3} & \sqrt{3} & 1 \end{pmatrix}\begin{pmatrix} \langle\uparrow\uparrow| \\ \langle\uparrow\downarrow| \\ \langle\downarrow\uparrow| \\ \langle\downarrow\downarrow| \end{pmatrix}.$$

Частичный след по системе B дает:

$$\begin{aligned}\rho_A &= \mathrm{tr}_B\,|\Phi\rangle\langle\Phi| = \\ &= \langle\uparrow_B|\Phi\rangle\langle\Phi|\uparrow_B\rangle + \langle\downarrow_B|\Phi\rangle\langle\Phi|\downarrow_B\rangle = \\ &= \frac{1}{8}\begin{bmatrix} |\uparrow\rangle\langle\uparrow| + \sqrt{3}|\uparrow\rangle\langle\downarrow| + \sqrt{3}|\downarrow\rangle\langle\uparrow| + 3|\downarrow\rangle\langle\downarrow| + \\ +3|\uparrow\rangle\langle\uparrow| + \sqrt{3}|\uparrow\rangle\langle\downarrow| + \sqrt{3}|\downarrow\rangle\langle\uparrow| + |\downarrow\rangle\langle\downarrow| \end{bmatrix} = \\ &= \frac{1}{8}\Big(4|\uparrow\rangle\langle\uparrow| + 2\sqrt{3}|\uparrow\rangle\langle\downarrow| + 2\sqrt{3}|\downarrow\rangle\langle\uparrow| + 4|\downarrow\rangle\langle\downarrow|\Big) = \\ &= \big(|\uparrow\rangle, |\downarrow\rangle\big)\begin{pmatrix} 1/2 & \sqrt{3}/4 \\ \sqrt{3}/4 & 1/2 \end{pmatrix}\begin{pmatrix} \langle\uparrow| \\ \langle\downarrow| \end{pmatrix}.\end{aligned}$$

Поскольку состояние $|\Phi\rangle$ симметрично относительно обмена системами A и B, то оказывается, что частичный след по системе A дает тот же самый вид приведенной матрицы плотности ρ_B:

$$\begin{aligned}\rho_B &= \mathrm{tr}_A\,|\Phi\rangle\langle\Phi| = \\ &= \langle\uparrow_A|\Phi\rangle\langle\Phi|\uparrow_A\rangle + \langle\downarrow_A|\Phi\rangle\langle\Phi|\downarrow_A\rangle = \\ &= \frac{1}{8}\begin{bmatrix} |\uparrow\rangle\langle\uparrow| + \sqrt{3}|\uparrow\rangle\langle\downarrow| + \sqrt{3}|\downarrow\rangle\langle\uparrow| + 3|\downarrow\rangle\langle\downarrow| + \\ +3|\uparrow\rangle\langle\uparrow| + \sqrt{3}|\uparrow\rangle\langle\downarrow| + \sqrt{3}|\downarrow\rangle\langle\uparrow| + |\downarrow\rangle\langle\downarrow| \end{bmatrix} = \\ &= \frac{1}{8}\Big(4|\uparrow\rangle\langle\uparrow| + 2\sqrt{3}|\uparrow\rangle\langle\downarrow| + 2\sqrt{3}|\downarrow\rangle\langle\uparrow| + 4|\downarrow\rangle\langle\downarrow|\Big) = \\ &= \big(|\uparrow\rangle, |\downarrow\rangle\big)\begin{pmatrix} 1/2 & \sqrt{3}/4 \\ \sqrt{3}/4 & 1/2 \end{pmatrix}\begin{pmatrix} \langle\uparrow| \\ \langle\downarrow| \end{pmatrix}.\end{aligned}$$

2.3.2 Разложение Шмидта. Решение этой части задачи тоже получается в результате простых манипуляций определениями, но с дополнительным преобразованием, с помощью которого мы предварительно поворачиваем базис системы A так, чтобы диагонализовать приведенную матрицу ρ_A.

Чтобы выполнить это, найдем сначала собственные состояния, диагонализующие ρ_A:

$$\begin{vmatrix} 1/2-\lambda & \sqrt{3}/4 \\ \sqrt{3}/4 & 1/2-\lambda \end{vmatrix} = 0,$$

$$1/4 - \lambda + \lambda^2 - 3/16 = 0,$$

$$\lambda^2 - \lambda + 1/16 = 0,$$

$$\lambda_\pm = 1/2 \pm \sqrt{3}/4,$$

$$|\psi^\pm\rangle_A = \frac{1}{\sqrt{2}}(|\uparrow\rangle_A \pm |\downarrow\rangle_A).$$

Чтобы выполнить (локальную) замену базиса, которая реализует эти собственные векторы в качестве базисных, используем обычную формулу перехода от одного представления к другому, основанную на очевидной тождественной вставке:

$$|\Phi\rangle = \sum_{i=\pm} |\psi^i\rangle\langle\psi^i|\Phi\rangle.$$

Коэффициентами этого разложения фактически являются состояния системы B, так как внутреннее произведение здесь вычисляется только по состояниям системы A. Действительно,

$$\begin{aligned}
\langle\psi^+|\Phi\rangle &= \frac{1}{2}({}_A\langle\uparrow| + {}_A\langle\downarrow|) \times \\
&\quad \times \left[|\uparrow\rangle_A \left(\frac{1}{2}|\uparrow\rangle_B + \frac{\sqrt{3}}{2}|\downarrow\rangle_B\right) + |\downarrow\rangle_A \left(\frac{\sqrt{3}}{2}|\uparrow\rangle_B + \frac{1}{2}|\downarrow\rangle_B\right)\right] = \\
&= \frac{1}{4}\left(|\uparrow\rangle_B + \sqrt{3}|\downarrow\rangle_B + \sqrt{3}|\uparrow\rangle_B + |\downarrow\rangle_B\right) = \\
&= \frac{1+\sqrt{3}}{4}\left(|\uparrow\rangle_B + |\downarrow\rangle_B\right) \equiv |\tilde{\varphi}_1\rangle_B,
\end{aligned}$$

$$\begin{aligned}
\langle\psi^-|\Phi\rangle &= \frac{1}{2}({}_A\langle\uparrow| - {}_A\langle\downarrow|) \times \\
&\quad \times \left[|\uparrow\rangle_A \left(\frac{1}{2}|\uparrow\rangle_B + \frac{\sqrt{3}}{2}|\downarrow\rangle_B\right) + |\downarrow\rangle_A \left(\frac{\sqrt{3}}{2}|\uparrow\rangle_B + \frac{1}{2}|\downarrow\rangle_B\right)\right] = \\
&= \frac{1}{4}\left(|\uparrow\rangle_B + \sqrt{3}|\downarrow\rangle_B - \sqrt{3}|\uparrow\rangle_B - |\downarrow\rangle_B\right) = \\
&= \frac{1-\sqrt{3}}{4}\left(|\uparrow\rangle_B - |\downarrow\rangle_B\right) \equiv |\tilde{\varphi}_2\rangle_B.
\end{aligned}$$

Мы почти у цели. Все, что нам осталось сделать — это нормировать полученные состояния:

$$\langle\tilde{\varphi}_1|\tilde{\varphi}_1\rangle = \frac{4+2\sqrt{3}}{16}({}_B\langle\uparrow| + {}_B\langle\downarrow|)(|\uparrow\rangle_B + |\downarrow\rangle_B) =$$

$$= \frac{1}{2}\left(1+\frac{\sqrt{3}}{2}\right) \equiv p_1,$$

$$\langle\tilde{\varphi}_2|\tilde{\varphi}_2\rangle = \frac{4-2\sqrt{3}}{16}({}_B\langle\uparrow| - {}_B\langle\downarrow|)(|\uparrow\rangle_B - |\downarrow\rangle_B) =$$

$$= \frac{1}{2}\left(1-\frac{\sqrt{3}}{2}\right) \equiv p_2.$$

Используя нормированные состояния $|\varphi_i\rangle_B \equiv \frac{1}{\sqrt{p_i}}|\tilde{\varphi}_i\rangle_B$, мы можем записать разложение Шмидта этого чистого состояния по ортонормированным состояниям систем A и B:

$$|\Phi\rangle = \sum_i \sqrt{p_i}|\psi_i\rangle_A|\varphi_i\rangle_B =$$

$$|\Phi\rangle = \sqrt{1+\frac{\sqrt{3}}{2}}\left[\frac{1}{\sqrt{2}}(|\uparrow\rangle_A+|\downarrow\rangle_A)\right]\left[\frac{1}{\sqrt{1+\frac{\sqrt{3}}{2}}}\frac{1+\sqrt{3}}{4}(|\uparrow\rangle_B+|\downarrow\rangle_B)\right] +$$

$$+\sqrt{1-\frac{\sqrt{3}}{2}}\left[\frac{1}{\sqrt{2}}(|\uparrow\rangle_A-|\downarrow\rangle_A)\right]\left[\frac{1}{\sqrt{1-\frac{\sqrt{3}}{2}}}\frac{1-\sqrt{3}}{4}(|\uparrow\rangle_B-|\downarrow\rangle_B)\right] =$$

$$= \left(\frac{1+\sqrt{3}}{2\sqrt{2}}\right)\left[\frac{1}{\sqrt{2}}(|\uparrow\rangle_A+|\downarrow\rangle_A)\right]\left[\frac{1}{\sqrt{2}}(|\uparrow\rangle_B+|\downarrow\rangle_B)\right] +$$

$$+\left(\frac{1-\sqrt{3}}{2\sqrt{2}}\right)\left[\frac{1}{\sqrt{2}}(|\uparrow\rangle_A-|\downarrow\rangle_A)\right]\left[\frac{1}{\sqrt{2}}(|\uparrow\rangle_B-|\downarrow\rangle_B)\right].$$

2.4. Трехкубитовое чистое состояние

Нет. Прежде чем объяснять, почему, я хотел бы отметить, что на самом деле неверно в этой задаче. Разложение Шмидта для трехкомпонентной системы должно выглядеть следующим образом:

$$\sum_i \sqrt{p_i}|i\rangle_A \otimes |i\rangle_B \otimes |i\rangle_C.$$

Надеюсь, это ни у кого не вызывает недоумения, так как множители $\sqrt{p_i}$, очевидно, должны присутствовать, чтобы нормировать состояние. В общем случае разложение Шмидта n-компонентной системы имело бы вид

$$\sum_i \sqrt{p_i} \bigotimes_j |i\rangle_j,$$

где каждый базис Шмидта $\{|i\rangle_j\}$ является ортонормированным в j-ой системе.

Теперь обратимся к «объяснению», которое я употребляю как эвфемизм «доказательства»[1].

Пусть $|\psi\rangle_{ABC}$ — чистое состояние трехкомпонентной системы; предположим, что $|\psi\rangle_{ABC}$ имеет разложение Шмидта. Коль скоро это так, то вычисление парциального следа по любым двум подсистемам даст диагональную в базисе Шмидта приведенную матрицу плотности оставшейся подсистемы. Более того, вычисляемые этом базисе приведенные матрицы плотности подсистем должны иметь *один и тот же* спектр значений p_i[2]. Любые локальные (действующие внутри одной подсистемы) унитарные преобразования базисов сохраняют собственные значения приведенных матриц плотности. Следовательно, спектры (ненулевые) приведенных матриц плотности всех этих подсистем должны быть идентичны независимо от того, в каком базисе они выражаются.

Это требование строгого «совпадения спектров» несправедливо для произвольных $|\psi\rangle_{ABC}$, и примеров этому множество. Я думаю, что простейшим контрпримером является:

$$|\psi\rangle_{ABC} = |0\rangle_A \left(\frac{1}{\sqrt{2}} \left(|00\rangle_{BC} + |11\rangle_{BC} \right) \right),$$

[1] Эвфемизм от греческого *euphemia* — воздержание от резких слов, смягченное выражение (перев.)

[2] Точнее, приведенные матрицы плотности должны иметь совпадающие спектры *ненулевых* собственных значений p_i (см. раздел 2.4). — *Прим. ред.*

$$\rho_{ABC} = |\psi\rangle_{ABC\,ABC}\langle\psi| =$$
$$= \frac{1}{2}\big(|000\rangle\langle 000| + |000\rangle\langle 011| + |011\rangle\langle 000| + |011\rangle\langle 011|\big),$$

$$\rho_A = \mathrm{tr}_B\,\mathrm{tr}_C\,\rho_{ABC}$$
$$= |0\rangle_{A\,A}\langle 0|$$
$$= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},$$
$$\rho_B = \mathrm{tr}_A\,\mathrm{tr}_C\,\rho_{ABC}$$
$$= \frac{1}{2}\big(|0\rangle_{B\,B}\langle 0| + |1\rangle_{B\,B}\langle 1|\big)$$
$$= \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix},$$

$$\{1,0\} \neq \left\{\frac{1}{2},\frac{1}{2}\right\}. \qquad \square$$

2.5. Квантовые корреляции в смешанном состоянии

Как мы видели в задаче 2.2, вероятность измерения собственного значения $\mathbf{P}_n$ равна $p_n = \mathrm{tr}\,\mathbf{P}_n\rho$. Взаимно однозначное соответствие между проекторами на кубиты и точками на поверхности сферы Блоха говорит о том, что вероятность результатов двух последовательных измерений — «спин вверх» вдоль оси $\hat{n}$ у первого кубита и «спин вверх» вдоль оси $\hat{m}$ у второго кубита — равна

$$p = \mathrm{tr}_B\left\{\mathbf{P}_{\hat{m}}\,\mathrm{tr}_A\left[\big(\mathbf{P}_{\hat{n}}\otimes\mathbf{1}_B\big)\rho\right]\right\},$$
$$p = \mathrm{tr}_B\left\{\frac{1}{2}\big(\mathbf{1}+\hat{m}\cdot\vec{\boldsymbol{\sigma}}_B\big)\,\mathrm{tr}_A\left[\frac{1}{2}\big(\mathbf{1}+\hat{n}\cdot\vec{\boldsymbol{\sigma}}_A\big)\otimes\mathbf{1}_B\big)\rho\right]\right\}.$$

По отношению к следу по системе A проектор $\mathbf{P}_{\hat{m}}$ является мультипликативной константой, поскольку его действие на систему A тривиально. В силу линейности следа такую константу можно внести под его знак:

$$p = \mathrm{tr}_B\,\mathrm{tr}_A\left[\left(\mathbf{1}_A\otimes\frac{1}{2}\big(\mathbf{1}+\hat{m}\cdot\vec{\boldsymbol{\sigma}}_B\big)\right)\left(\frac{1}{2}\big(\mathbf{1}+\hat{n}\cdot\vec{\boldsymbol{\sigma}}_A\big)\otimes\mathbf{1}_B\right)\rho\right] =$$
$$= \mathrm{tr}_B\,\mathrm{tr}_A\left[\left(\frac{1}{2}\big(\mathbf{1}+\hat{n}\cdot\vec{\boldsymbol{\sigma}}_A\big)\otimes\frac{1}{2}\big(\mathbf{1}+\hat{m}\cdot\vec{\boldsymbol{\sigma}}_B\big)\right)\rho\right].$$

С помощью данной в задаче ρ, эти следы можно вычислить явно, учитывая линейность следа и равенство нулю следов матриц Паули:

$$= \mathrm{tr}_B\,\mathrm{tr}_A\left[\left(\frac{1}{2}(1+\hat{n}\cdot\vec{\sigma}_A)\right)\otimes\left(\frac{1}{2}(1+\hat{m}\cdot\vec{\sigma}_B)\right)\left(\frac{1}{8}\mathbf{1}_{AB}+\frac{1}{2}|\psi^-\rangle\langle\psi^-|\right)\right] =$$

$$= \frac{1}{32}\,\mathrm{tr}_B\,\mathrm{tr}_A\left[(1+\hat{n}\cdot\vec{\sigma}_A)\otimes(1+\hat{m}\cdot\vec{\sigma}_B)\right] +$$

$$+\frac{1}{8}\,\mathrm{tr}_B\,\mathrm{tr}_A\left[\Big((1+\hat{n}\cdot\vec{\sigma}_A)\otimes(1+\hat{m}\cdot\vec{\sigma}_B)\Big)|\psi^-\rangle\langle\psi^-|\right] =$$

$$= \frac{1}{32}\,\mathrm{tr}_B\,\mathrm{tr}_A\left[1\otimes 1\right] + \frac{1}{8}\langle\psi^-|(1+\hat{n}\cdot\vec{\sigma}_A)\otimes(1+\hat{m}\cdot\vec{\sigma}_B)|\psi^-\rangle =$$

$$= \frac{1}{8} + \frac{1}{8}\langle\psi^-|1+\hat{n}\cdot\vec{\sigma}_A+\hat{m}\cdot\vec{\sigma}_B+\hat{n}\cdot\vec{\sigma}_A\otimes\hat{m}\cdot\vec{\sigma}_B|\psi^-\rangle =$$

$$= \frac{1}{4}+\frac{1}{8}\Big[\hat{n}\cdot\langle\psi^-|\vec{\sigma}_A|\psi^-\rangle+\hat{m}\cdot\langle\psi^-|\vec{\sigma}_B|\psi^-\rangle+\langle\psi^-|\hat{n}\cdot\vec{\sigma}_A\otimes\hat{m}\cdot\vec{\sigma}_B|\psi^-\rangle\Big].$$

В синглетном состоянии $|\psi^-\rangle$ математические ожидания σ_A и σ_B равны нулю, в чем можно убедиться или с помощью явных вычислений или заметив, что *синглет является скалярным* (спин-0) состоянием. Остается вычислить только одно слагаемое, самое правое из приведенных выше. Для этого имеется несколько способов. Возможно, проще всего показать, что благодаря спин-0 симметрии синглетное состояние имеет один и тот же вид в любом базисе, следовательно, мы можем выбрать систему координат, в которой $\hat{n}=\hat{z}$. Более того, симметрия состояния позволяет положить $\hat{m}=\hat{z}\cos\theta+\hat{x}\sin\theta$, так что мы находим

$$\langle\psi^-|\hat{n}\cdot\vec{\sigma}_A)\otimes\hat{m}\cdot\vec{\sigma}_B|\psi^-\rangle = \langle\psi^-|\sigma_z\otimes\sigma_z|\psi^-\rangle\cos\theta + \\ +\langle\psi^-|\sigma_z\otimes\sigma_x|\psi^-\rangle\sin\theta = -\cos\theta,$$

что дает ответ

$$p=\frac{1}{4}-\frac{1}{8}\cos\theta.$$

Этот результат интуитивно понятен. С большей вероятностью мы обнаруживаем спины антипараллельными, так как матрица плотности имеет большую синглетную компоненту. По этой же причине менее вероятно обнаружить спины параллельными. Вариация между двумя возможностями, естественно, синусоидальная.

Решения упражнений к главе 3

3.1. Реализация ПОЗМ

Поскольку мы имеем $n = 4$ положительных оператора, действующих в $N = 2$-мерном гильбертовом пространстве $\mathcal{H}$, то согласно теореме Наймарка эту ПОЗМ можно расширить до «ортогонального измерения фон Неймана»[1] в $n = 4$-мерном гильбертовом пространстве $\mathcal{H} \oplus \mathcal{H}^{\perp}$. Сделаем это путем расширения $N = 2$ проекторов до четырех, требуя ортонормированность состояний, из которых формируются эти проекторы. На лекциях было показано, что с помощью следующего отображения

$$|\varphi_a\rangle \oplus |\varphi_a^{\perp}\rangle \rightarrow |\varphi_a\rangle_A|0\rangle_B + |0\rangle_A|\varphi_a^{\perp}\rangle_B, \qquad a = 1, \ldots, n,$$

вариант «прямой суммы» теоремы Наймарка можно преобразовать в вариант «тензорного произведения».

Если вспомогательная система приготовлена в состоянии $|0\rangle_B$, то это отображение гарантирует, что дальнейшая эволюция системы A будет ограничена подпространством $\mathcal{H}$. Размерность расширенного тензорным произведением пространства равна $N(n - N + 1)$, что в нашем случае равно шести. Однако это не самое эффективное из возможных отображений. Мы можем использовать следующее, более рациональное, отображение той же самой размерности:

$$|\varphi_a\rangle \oplus |\varphi_a^{\perp}\rangle \rightarrow |\varphi_a\rangle_A|0\rangle_B + |\varphi_a^{\perp}\rangle_A|1\rangle_B, \qquad a = 1, \ldots, n.$$

Очевидно, это отображение также ограничивает систему A подпространством $\mathcal{H}$, если вспомогательная система приготовлена в состоянии $|0\rangle_B$, но размерность тензорного произведения гильбертовых пространств теперь только $2N = 4$.

Чтобы найти ПЗИ, сначала найдем расширение в прямую сумму пространств, а затем применим приведенное выше отображение. Состояниями, включающими ПОЗМ, которую мы хотели бы расширить, являются

$$|\tilde{\psi}_1\rangle = \frac{1}{\sqrt{2}}|\uparrow_z\rangle, \qquad |\tilde{\psi}_3\rangle = \frac{1}{\sqrt{2}}|\uparrow_x\rangle,$$

$$|\tilde{\psi}_2\rangle = \frac{1}{\sqrt{2}}|\downarrow_z\rangle, \qquad |\tilde{\psi}_4\rangle = \frac{1}{\sqrt{2}}|\downarrow_x\rangle.$$

[1] Некоторые авторы называют этот тип измерения ПЗИ (проекторно-значное измерение). К их числу принадлежит и автор. ПЗИ гораздо более ясно, чем «ортогональное измерение фон Неймана».

Чтобы расширить базис, удобнее и понятнее переписать их в спинорной форме в $\hat{z}$-базисе, в котором два последних состояния записываются с помощью соотношений[1]

$$|\uparrow_x\rangle = \frac{1}{\sqrt{2}}(|\uparrow_z\rangle + |\downarrow_z\rangle),$$

$$|\downarrow_x\rangle = \frac{1}{\sqrt{2}}(|\uparrow_z\rangle - |\downarrow_z\rangle),$$

$$|\tilde{\psi}_1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\end{pmatrix}, \qquad |\tilde{\psi}_3\rangle = \frac{1}{2}\begin{pmatrix}1\\1\end{pmatrix},$$

$$|\tilde{\psi}_2\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\end{pmatrix}, \qquad |\tilde{\psi}_4\rangle = \frac{1}{2}\begin{pmatrix}1\\-1\end{pmatrix}.$$

Первым состоянием, которое будет расширено, является $|\tilde{\psi}_1\rangle$. Единственным ограничением является нормировка, поэтому мы можем расширить его с помощью любого 2-спинора в $\mathcal{H}^-$, имеющего норму 1/2. Существует множество выборов, но реально разумны только те из них, у которых или равна нулю одна компонента, или обе компоненты имеют одинаковые значения. Я продемонстрирую, что получится, если выбрать расширение спинора первого типа:

$$|u_1\rangle = \begin{pmatrix}1/\sqrt{2}\\0\\1/\sqrt{2}\\0\end{pmatrix}.$$

Следующий вектор должен быть ортогонален предыдущему и также нормирован. С точностью до произвольной фазы это фиксирует его расширение, которое мы можем применить. Вновь имеется только один разумный выбор, дающий тривиальную фазу:

$$|u_2\rangle = \begin{pmatrix}0\\1/\sqrt{2}\\0\\1/\sqrt{2}\end{pmatrix}.$$

[1] Записывая состояния таким образом, я явно использую соглашение о фазе спинора $|\psi(\theta,\varphi)\rangle = \begin{pmatrix}\cos\theta/2\\ e^{i\varphi}\sin\theta/2\end{pmatrix}$, как это обычно делается. Хотя соглашение о «распределенной фазе» $|\psi(\theta,\varphi)\rangle = \begin{pmatrix}e^{-i\varphi/2}\cos\theta/2\\ e^{i\varphi/2}\sin\theta/2\end{pmatrix}$ выглядит более симметрично, оно ведет к общим фазам в $|\uparrow_x\rangle$ и $|\downarrow_x\rangle$, которые труднее запомнить и уж во всяком случае нефизичны.

Два последних выбора полностью фиксируются требованиями ортогональности и нормировки и имеют вид

$$|u_3\rangle = \begin{pmatrix} 1/2 \\ 1/2 \\ -1/2 \\ -1/2 \end{pmatrix}, \qquad |u_4\rangle = \begin{pmatrix} 1/2 \\ -1/2 \\ -1/2 \\ 1/2 \end{pmatrix}.$$

Теперь нужно применить наше отображение, чтобы преобразовать эти «прямые суммы» состояний в тензорные произведения состояний. То есть взять нашу исходную систему A и ввести вспомогательную систему B таким образом, чтобы базисные состояния в $\mathcal{H}^A \oplus \mathcal{H}^{A\perp}$ отобразились на базисные состояния в $\mathcal{H}^A \otimes \mathcal{H}^B$. Непосредственная проверка показывает, что это получается, если выполнить следующее отображение базисных векторов

$$\begin{pmatrix} q_1 \\ q_2 \\ q_3 \\ q_4 \end{pmatrix} \to \begin{pmatrix} |\uparrow_z\rangle_A |\uparrow_z\rangle_B \\ |\downarrow_z\rangle_A |\uparrow_z\rangle_B \\ |\uparrow_z\rangle_A |\downarrow_z\rangle_B \\ |\downarrow_z\rangle_A |\downarrow_z\rangle_B \end{pmatrix},$$

где введены обозначения $|0\rangle_B = |\uparrow_z\rangle_B$, $|1\rangle_B = |\downarrow_z\rangle_B$. Это позволяет записать проекторы в виде

$$\begin{aligned}
\Pi_1 &= |u_1\rangle\langle u_1| \\
&= \frac{1}{2}\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = |\uparrow_z\uparrow_x\rangle\langle\uparrow_z\uparrow_x|, \\
\Pi_2 &= |u_2\rangle\langle u_2| \\
&= \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} = |\downarrow_z\uparrow_x\rangle\langle\downarrow_z\uparrow_x|, \\
\Pi_3 &= |u_3\rangle\langle u_3| \\
&= \frac{1}{4}\begin{pmatrix} 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 \\ -1 & -1 & 1 & 1 \end{pmatrix} = |\uparrow_x\downarrow_x\rangle\langle\uparrow_x\downarrow_x|,
\end{aligned}$$

$$\Pi_4 = |u_4\rangle\langle u_4|$$
$$= \frac{1}{4}\begin{pmatrix} 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 \\ -1 & 1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} = |\downarrow_x\downarrow_x\rangle\langle\downarrow_x\downarrow_x|.$$

Для того, чтобы в исходной системе была реализована ПОЗМ, вспомогательная система должна быть приготовлена в состоянии $|\uparrow_z\rangle_B$.

Как упоминалось в ходе вывода, существует свобода в выборе путей, следовательно, возможны другие решения.

3.2. Обратимость супероператоров

а) Предположим, что супероператор $\mathcal{M}$ имеет левый обратный супероператор $\mathcal{N}$ такой, что $\mathcal{N}\circ\mathcal{M} = \mathcal{I}$. Согласно теореме о представлении Крауса $\mathcal{M}$ и $\mathcal{N}$ имеют представления операторных сумм:

$$\mathcal{M}(\rho) = \sum_\mu \mathbf{M}_\mu \rho \mathbf{M}_\mu^\dagger,$$
$$\mathcal{N}(\rho) = \sum_a \mathbf{N}_a \rho \mathbf{N}_a^\dagger,$$
$$\sum_\mu \mathbf{M}_\mu^\dagger \mathbf{M}_\mu = \sum_a \mathbf{N}_a^\dagger \mathbf{N}_a = \mathbf{1}.$$

Более того, представление операторной суммы их композиции выражается на языке операторов $\mathbf{R}_{\{a\mu\}} = \mathbf{N}_a\mathbf{M}_\mu$:

$$\sum_{a\mu} \mathbf{R}_{\{a\mu\}}\rho\mathbf{R}_{\{a\mu\}}^\dagger = \sum_{a\mu} \mathbf{N}_a\mathbf{M}_\mu\rho(\mathbf{N}_a\mathbf{M}_\mu)^\dagger =$$
$$= \sum_{a\mu} \mathbf{N}_a\mathbf{M}_\mu\rho\mathbf{M}_\mu^\dagger\mathbf{N}_a^\dagger = \mathcal{N}\circ\mathcal{M}(\rho),$$

$$\sum_{a\mu} \mathbf{R}_{\{a\mu\}}^\dagger\mathbf{R}_{\{a\mu\}} = \sum_{a\mu} (\mathbf{N}_a\mathbf{M}_\mu)^\dagger\mathbf{N}_a\mathbf{M}_\mu =$$
$$= \sum_{a\mu} \mathbf{M}_\mu^\dagger\mathbf{N}_a^\dagger\mathbf{N}_a\mathbf{M}_\mu =$$
$$= \sum_\mu \mathbf{M}_\mu^\dagger \left(\sum_a \mathbf{N}_a^\dagger\mathbf{N}_a\right)\mathbf{M}_\mu = \mathbf{1}.$$

Но поскольку $\mathcal{N} \circ \mathcal{M} = \mathcal{I}$, то операторы $\mathbf{R}_{\{a\mu\}}$ одновременно должны быть операторами Крауса для тождественного супероператора, имеющего тривиальное представление $\mathcal{I}(\rho) = \mathbf{1}\rho\mathbf{1}^\dagger$. В наиболее общем случае операторы Крауса определены с точностью до унитарного поворота; отсюда следует, что $\mathbf{N}_a\mathbf{M}_\mu = \lambda_{a\mu}\mathbf{1}$, где $\lambda_{a\mu}$ — элемент унитарной матрицы, а $\sum\limits_{a\mu} |\lambda_{a\mu}|^2 = \mathbf{1}$ согласно нормировке столбцов унитарной матрицы[1].

b) Используя тождественную вставку $\sum\limits_a \mathbf{N}_a^\dagger \mathbf{N}_a = 1$ и соотношение $\mathbf{N}_a\mathbf{M}_\mu = \lambda_{a\mu}\mathbf{1}$ из части (a), получим требуемый результат:

$$\mathbf{M}_\nu^\dagger \mathbf{M}_\mu = \sum_a \mathbf{M}_\nu^\dagger \mathbf{N}_a^\dagger \mathbf{N}_a \mathbf{M}_\mu = \tag{6.281}$$

$$= \sum_a \left(\mathbf{N}_a\mathbf{M}_\nu\right)^\dagger \mathbf{N}_a\mathbf{M}_\mu = \tag{6.282}$$

$$= \left(\sum_a \lambda_{a\nu}^* \lambda_{a\mu}\right) \mathbf{1} = \gamma_{\nu\mu}\mathbf{1}. \tag{6.283}$$

c) Из части (b) мы знаем, что $\mathbf{M}_\nu^\dagger \mathbf{M}_\mu = \gamma_{\nu\mu}\mathbf{1}$. Этого достаточно, чтобы показать пропорциональность друг другу всех операторов $\mathbf{M}$, поскольку в этом случае разложение Крауса имеет всего одно слагаемое, которое в соответствии с нормировкой должно быть унитарным.

Так как мы рассматриваем только ненулевые операторы, нам известно, что $\gamma_{\nu\mu} \neq 0$. Таким образом[2],

$$\det \mathbf{M}_\mu^\dagger \mathbf{M}_\mu = \det \gamma_{\mu\mu}\mathbf{1},$$

$$\det \mathbf{M}_\mu^\dagger \det \mathbf{M}_\mu = \left(\gamma_{\mu\mu}\right)^n,$$

$$\left(\det \mathbf{M}_\mu\right)^* \det \mathbf{M}_\mu \neq 0,$$

$$\det \mathbf{M}_\mu \neq 0.$$

---

[1] На самом деле требование унитарности матрицы $\lambda_{a\mu}$ здесь излишне. Справедливость равенства $\mathcal{N} \circ \mathcal{M}(\rho) = \mathcal{I}(\rho) = \rho$ для любого оператора плотности ρ требует выполнения $\mathbf{N}_a\mathbf{M}_\mu = \lambda_{a\mu}\mathbf{1}$, где $\lambda_{a\mu}$ — элемент *произвольной* матрицы с единичной нормой Гильберта–Шмидта, определяемой уравнениями (6.104), (6.105). Впрочем уже в следующем пункте решения данной задачи унитарность матрицы $\lambda_{a\mu}$ не предполагается, в противном случае матрица $\gamma_{\nu\mu}$, определяемая как $\sum\limits_a \lambda_{a\nu}^* \lambda_{a\mu} = \gamma_{\nu\mu}$ была бы равна единичной матрице $\gamma_{\nu\mu} = \delta_{\nu\mu}$. — *Прим. ред.*

[2] Здесь во втором равенстве n — размерность гильбертова пространства состояний рассматриваемой квантовой системы. — *Прим. ред.*

Следовательно, каждый из операторов $\mathbf{M}_\mu$ должен быть обратим и, в частности,

$$\mathbf{M}_\mu^\dagger \mathbf{M}_\mu = \gamma_{\mu\mu}\mathbf{1},$$
$$\mathbf{M}_\mu^\dagger = \gamma_{\mu\mu}\mathbf{M}_\mu^{-1}.$$

Отсюда следует, что все операторы $\mathbf{M}$ пропорциональны друг другу:

$$\mathbf{M}_\nu^\dagger \mathbf{M}_\mu = \gamma_{\nu\mu}\mathbf{1},$$
$$\mathbf{M}_\nu \mathbf{M}_\nu^\dagger \mathbf{M}_\mu = \gamma_{\nu\mu}\mathbf{M}_\nu,$$
$$\mathbf{M}_\nu(\gamma_{\nu\nu}\mathbf{M}_\nu^{-1})\mathbf{M}_\mu = \gamma_{\nu\mu}\mathbf{M}_\nu,$$
$$\mathbf{M}_\mu = \frac{\gamma_{\nu\mu}}{\gamma_{\nu\nu}}\mathbf{M}_\nu.$$

3.3. Как много супероператоров?

На лекции мы видели, что существует три эквивалентных способа установить, что $ является супероператором:

1. $ преобразует матрицы плотности в матрицы плотности.

2. $ является вполне положительным линейным отображением, сохраняющим эрмитовость и след своего аргумента.

3. $ имеет представление операторной суммы.

Необходимо найти количество степеней свободы $, используя любой из этих критериев. Здесь я опишу подходы, использующие только критерии (1) и (3). В каждом из этих подходов ρ рассматривается как $N \times N$ оператор плотности, который полностью описывает смешанное состояние (то есть ансамбль чистых состояний) в N-мерном гильбертовом пространстве.

Матрица плотности ρ является эрмитовой матрицей с единичным следом и, следовательно, зависит от $N^2 - 1$ свободных параметров. Однако было бы ошибкой думать, что действие $ сводится всего лишь к случайному перемешиванию этих параметров. Базис для ρ фактически является N^2-мерным, а ρ может быть записана как $\rho = \frac{1}{2}(\mathbf{1} + \vec{\alpha}\cdot\vec{\boldsymbol{\lambda}})$, где $\boldsymbol{\lambda}_i$ представляет собой $N^2 - 1$ линейно независимых базисных матриц. Как видно из этой записи, $ способен не только случайно перемешивать матрицы $\boldsymbol{\lambda}_i$, изменяя $\vec{\alpha}$, но также может отображать единицу на линейную комбинацию 1 и $\vec{\boldsymbol{\lambda}}$:

$$\$\left(\frac{1}{2}\mathbf{1}\right) = \frac{1}{2}(\mathbf{1} + \vec{\beta}\cdot\vec{\boldsymbol{\lambda}}) \quad \text{для некоторого } \vec{\beta}.$$

При таком подсчете количество свободных параметров равно $(N^2-1)^2$ для отображения $\vec{\lambda}$ и N^2-1 для аффинного сдвига $\mathbf{1}$, что в сумме дает $(N^2-1)^2+N^2-1=N^4-N^2$ вещественных параметров.

Если вы не убеждены в существовании аффинного сдвига, то посмотрите, как сдвигается центр сферы Блоха под действием канала затухания амплитуды в задаче 3.6 b.

Поскольку $ имеет представление операторной суммы, мы можем записать

$$\$(\rho)=\sum_{\mu}\mathbf{M}_{\mu}\rho\mathbf{M}_{\mu}^{\dagger},$$

где каждый оператор $\mathbf{M}_{\mu}\in \mathrm{GL}(N,C)$[1] зависит от $2N^2$ вещественных параметров. В $\mathrm{GL}(N,C)$ существует N^2 линейно независимых матриц, что означает, что *prima facie*[2] $ зависит самое большее от $2N^2(N^2)=2N^4$ вещественных параметров.

Матрицы $\mathbf{M}_{\mu}$ должны также удовлетворять условию нормировки

$$\sum_{\mu}\mathbf{M}_{\mu}^{\dagger}\mathbf{M}_{\mu}=\mathbf{1}.$$

Это дает только N^2 дополнительных связей, так как эрмитово сопряженное уравнение идентично записанному выше. Наконец, мы видели на лекции, что наиболее общей неоднозначностью в определении матриц $\mathbf{M}_{\mu}$ является унитарная перестановка операторов:

$$\mathbf{M}_{\mu}\rightarrow U_{\mu\nu}\mathbf{M}_{\nu}.$$

Так как существует самое большее N^2 матриц $\mathbf{M}_{\mu}$, то $U_{\mu\nu}\in \mathrm{U}(N^2)$ зависит от N^4 вещественных параметров. Таким образом, мы находим, что $ зависит самое большее от $2N^4-N^2-N^4=N^4-N^2$ вещественных параметров.

В обоих подсчетах мы нашли, что $ зависит самое большее от N^4-N^2 вещественных параметров.

3.4. Насколько быстра декогерентизация?

a) Уравнение движения простого затухающего гармонического осциллятора имеет вид

$$m\ddot{x}+b\dot{x}+m\omega^2x=0.$$

[1] $\mathrm{GL}(N,C)$ группа невырожденных матриц размерности N над полем комплексных чисел C. — *Прим. ред.*

[2] *Prima facie* (лат) — по первому виду, на первый взгляд. — *Прим. перев.*

Мы ожидаем, что при слабом затухании средняя энергия осциллятора убывает экспоненциально:

$$\langle E(t)\rangle = E_0 e^{-bt/m}.$$

Таким образом, *амплитуда* осцилляций должна затухать как $e^{-bt/2m}$. Из классической механики или откуда-нибудь еще мы помним, что при слабом затухании добротность определяется как

$$Q = 2\pi \left(\frac{\text{Полная энергия}}{\text{Потеря энергии за период}}\right) = \frac{\omega}{b/m}.$$

На лекции мы нашли, что декогерентизация хорошо моделируется каналом затухания фазы. Из основного уравнения для этого канала следует, что недиагональные в базисе когерентных состояний элементы матрицы плотности затухают как

$$\boldsymbol{\rho}_{nm}(t) = \boldsymbol{\rho}_{nm}(0) e^{-\Gamma |n-m|^2 t/2},$$

где Γ — темп рассеяния одного кванта осциллятора его окружением. Такой вид затухания наводит на мысль интерпретировать Γ как коэффициент эффективной радиационной силы затухания с добротностью

$$Q = \frac{\omega}{\Gamma}.$$

Время декогерентизации системы по порядку величины представляет собой время, за которое недиагональные элементы уменьшаются в e раз по сравнению с их начальными значениями:

$$t_{\text{decoh}} = \frac{2}{\Gamma |n-m|^2}.$$

Данное в задаче кот-состояние не выражается в базисе когерентных состояний. Однако для сильно локализованных гауссовских волновых пакетов мы ожидаем, что собственное состояние оператора уничтожения будет примерно пропорционально собственному состоянию $\hat{\mathbf{x}}$-оператора:

$$\hat{\mathbf{a}} = \sqrt{\frac{m\omega}{2\hbar}} \left(\hat{\mathbf{x}} + \frac{i}{m\omega}\hat{\mathbf{p}}\right),$$

$$\langle \hat{\mathbf{a}} \rangle = \sqrt{\frac{m\omega}{2\hbar}} \left(\langle \hat{\mathbf{x}} \rangle + \frac{i}{m\omega}\langle \hat{\mathbf{p}} \rangle\right) = \sqrt{\frac{m\omega}{2\hbar}} \langle \hat{\mathbf{x}} \rangle.$$

Следовательно, мы ожидаем, что показатель экспоненты недиагональных элементов матрицы плотности будет иметь порядок

$$|n-m|^2 = \frac{m\omega}{2\hbar}|x-(-x)|^2 = \frac{2m\omega x^2}{\hbar}.$$

Теперь у нас есть все необходимое, чтобы вычислить время декогерентизации маятника:

$$\begin{aligned} t_{\mathrm{decoh}} &= \frac{2}{\Gamma|n-m|^2} = \\ &= \frac{2Q\hbar}{\omega(2m\omega x^2)} = \\ &= \frac{Q\hbar}{m\omega^2 x^2} = \\ &= \frac{10^9 \cdot 10^{-34}\mathrm{J}\cdot\mathrm{s}}{10^{-3}\mathrm{kg}\cdot 1\,\mathrm{s}^{-2}\cdot 10^{-4}\mathrm{m}^2} = 10^{-18}\mathrm{s}. \end{aligned}$$

b) При нулевой температуре все уровни энергии осциллятора были связаны с основным состоянием окружения. При конечной температуре $n = \frac{kT}{\hbar\omega}$ состояний окружения доступны для взаимодействия[1]. Таким образом, по порядку величины темп затухания становится в n раз быстрее. Соответственно время декогерентизации должно уменьшиться на этот фактор:

$$\begin{aligned} t_{\mathrm{decoh}}(T) &= \frac{\hbar\omega}{kT} t_{\mathrm{decoh}}(0) = \\ &= \frac{10^{-34}\mathrm{J}\cdot\mathrm{s}\cdot 1\,\mathrm{s}^{-1}}{10^{-23}\mathrm{J}\cdot\mathrm{K}^{-1}\cdot 10^2\mathrm{K}} \cdot 10^{-18}\mathrm{s} = 10^{-31}\mathrm{s}. \end{aligned}$$

Мораль: декогерентизация — очень быстра. Это один из самых быстрых известных в настоящее время физических процессов.

3.5. Затухание фазы

a) Непосредственно видно, что $\mathbf{M}_0$, $\mathbf{M}_1$ и $\mathbf{M}_2$ выражаются только через две линейно независимые матрицы ($\mathbf{1}$ и σ_3). Это наводит на мысль, что возможно представление операторной суммы, использующее *только два*

[1] Это справедливо при $kT \gg \hbar\omega$. — *Прим. ред.*

оператора Крауса. (Фактически всегда, когда набор операторов Крауса зависит от n линейно независимых матриц, можно найти представление операторной суммы, использующее эти n операторов.)

Посмотрим явно, как операторы $\mathbf{M}$ действуют на матрицу плотности ρ общего вида

$$\begin{aligned}\rho &\rightarrow \mathbf{M}_0\rho\mathbf{M}_0^\dagger + \mathbf{M}_1\rho\mathbf{M}_1^\dagger + \mathbf{M}_2\rho\mathbf{M}_2^\dagger = \\ &= (1-p)\rho + \frac{p}{4}(\mathbf{1}+\sigma_3)\rho(\mathbf{1}+\sigma_3) + \frac{p}{4}(\mathbf{1}-\sigma_3)\rho(\mathbf{1}-\sigma_3) = \\ &= \left(1-\frac{p}{2}\right)\rho + \frac{p}{2}\sigma_3\rho\sigma_3.\end{aligned}$$

Эта форма подсказывает выбор

$$\mathbf{N}_0 = \sqrt{1-\frac{p}{2}}\mathbf{1},$$

$$\mathbf{N}_1 = \sqrt{\frac{p}{2}}\sigma_3$$

в качестве операторов Крауса канала затухания фазы. Действительно, $\mathbf{N}_0$ и $\mathbf{N}_1$ удовлетворяют условию $\mathbf{N}_0^\dagger\mathbf{N}_0 + \mathbf{N}_1^\dagger\mathbf{N}_1 = \mathbf{1}$ и, следовательно, должным образом нормированы.

b) Соотношение $\mathbf{M}_\mu = U_{\mu a}\mathbf{N}_a$ дает следующую систему уравнений для компонент $U_{\mu a}$:

$$\sqrt{1-p}\mathbf{1} = U_{00}\sqrt{1-\frac{p}{2}}\,\mathbf{1} + U_{01}\sqrt{\frac{p}{2}}\,\sigma_3,$$

$$\sqrt{\frac{p}{4}}(\mathbf{1}+\sigma_3) = U_{10}\sqrt{1-\frac{p}{2}}\,\mathbf{1} + U_{11}\sqrt{\frac{p}{2}}\,\sigma_3,$$

$$\sqrt{\frac{p}{4}}(\mathbf{1}-\sigma_3) = U_{20}\sqrt{1-\frac{p}{2}}\,\mathbf{1} + U_{21}\sqrt{\frac{p}{2}}\,\sigma_3.$$

Сравнение коэффициентов при линейно независимых $\mathbf{1}$ и σ_3 дает

$$U_{00} = \sqrt{\frac{2-2p}{2-p}}, \qquad U_{01} = 0,$$

$$U_{10} = \sqrt{\frac{p}{4-2p}}, \qquad U_{11} = \sqrt{\frac{1}{2}},$$

$$U_{20} = \sqrt{\frac{p}{4-2p}}, \qquad U_{21} = -\sqrt{\frac{1}{2}}.$$

Осталось лишь дополнить матрицу U до унитарной, потребовав, чтобы все ее строки и столбцы были взаимно ортогональны и нормированы:

$$|U_{00}|^2 + |U_{01}|^2 + |U_{02}|^2 = 1 \Rightarrow U_{02} = e^{i\theta}\sqrt{\frac{p}{2-p}},$$

$$|U_{10}|^2 + |U_{11}|^2 + |U_{12}|^2 = 1 \Rightarrow U_{12} = e^{i\varphi}\sqrt{\frac{1-p}{2-p}},$$

$$|U_{20}|^2 + |U_{21}|^2 + |U_{22}|^2 = 1 \Rightarrow U_{22} = e^{i\psi}\sqrt{\frac{1-p}{2-p}},$$

$$U_{01}^* U_{02} + U_{11}^* U_{12} + U_{21}^* U_{22} = 0 \Rightarrow e^{i(\varphi-\psi)} = 1 \Rightarrow \varphi = \psi,$$

$$U_{00}^* U_{02} + U_{10}^* U_{12} + U_{20}^* U_{22} = 0 \Rightarrow e^{i(\theta-\varphi)} = -1 \Rightarrow \theta = \varphi + \pi.$$

Больше связей нет, следовательно, с точностью до неопределенной общей фазы ($\mathbf{N}_2 = 0$ не может иметь хорошо определенной фазы)

$$U = \begin{pmatrix} \sqrt{\dfrac{2-2p}{2-p}} & 0 & -e^{i\varphi}\sqrt{\dfrac{p}{2-p}} \\ \sqrt{\dfrac{p}{4-2p}} & \sqrt{\dfrac{1}{2}} & e^{i\varphi}\sqrt{\dfrac{1-p}{2-p}} \\ \sqrt{\dfrac{p}{4-2p}} & -\sqrt{\dfrac{1}{2}} & e^{i\varphi}\sqrt{\dfrac{1-p}{2-p}} \end{pmatrix}.$$

c) Операторы Крауса для канала, имеющего унитарное представление U_{AE}, определяются как

$$\mathbf{M}_\mu \equiv \langle \mu_E | U_{AE} | 0_E \rangle,$$

где $|\mu\rangle_E$ — *ортогональные* состояния окружения. Мы можем обычным способом сформировать ортогональный базис окружения из $\{|0\rangle_E, |\gamma_0\rangle_E, |\gamma_1\rangle_E\}$. Одним из методов является применение процесса Грама — Шмидта, но вместо этого я выберу базис, отражающий симметрию между $|\gamma_0\rangle_E$ и $|\gamma_1\rangle_E$:

$$|\pm\rangle_E = \frac{\alpha_\pm}{\sqrt{2}}\left(|\gamma_0\rangle_E \pm |\gamma_1\rangle_E\right),$$

$$\langle \pm | \pm \rangle = 1,$$

$$\Rightarrow |\alpha_\pm|^2\left(1 \pm \langle \gamma_0 | \gamma_1 \rangle\right) = 1,$$

$$\Rightarrow \alpha_\pm = \sqrt{\frac{1}{1 \pm (1-\varepsilon)}}.$$

В этом базисе операторы Крауса имеют вид

$$\begin{aligned}
\mathbf{M}_0 &= \langle 0_E|U_{AE}|0_E\rangle = \sqrt{1-p}\,\mathbf{1},\\
\mathbf{M}_\pm &= \langle \pm_E|U_{AE}|0_E\rangle =\\
&= \sqrt{\frac{p}{2[1\pm(1-\varepsilon)]}}\begin{pmatrix} 1\pm(1-\varepsilon) & 0\\ 0 & \pm[1\pm(1-\varepsilon)]\end{pmatrix} =\\
&= \sqrt{\frac{p[1\pm(1-\varepsilon)]}{2}}\begin{pmatrix} 1 & 0\\ 0 & \pm 1\end{pmatrix}.
\end{aligned}$$

Они не похожи на операторы канала затухания фазы, но их можно преобразовать в три таких оператора. И даже более того, их можно преобразовать в *два* оператора, которые выглядят как операторы канала затухания фазы. Чтобы найти их, рассмотрим, как и в части (a), действие операторов $\mathbf{M}_{0,\pm}$ на произвольную матрицу плотности

$$\begin{aligned}
\boldsymbol{\rho} &\to \mathbf{M}_0\boldsymbol{\rho}\mathbf{M}_0^\dagger + \mathbf{M}_+\boldsymbol{\rho}\mathbf{M}_+^\dagger + \mathbf{M}_-\boldsymbol{\rho}\mathbf{M}_-^\dagger\\
&= (1-p)\boldsymbol{\rho} + \frac{p(2-\varepsilon)}{2}\boldsymbol{\rho} + \frac{p\varepsilon}{2}\boldsymbol{\sigma}_3\boldsymbol{\rho}\boldsymbol{\sigma}_3\\
&= \left(1-\frac{p\varepsilon}{2}\right)\boldsymbol{\rho} + \frac{p\varepsilon}{2}\boldsymbol{\sigma}_3\boldsymbol{\rho}\boldsymbol{\sigma}_3,
\end{aligned}$$

$$\begin{aligned}
\mathbf{N}_0 &= \sqrt{1-\frac{p\varepsilon}{2}}\,\mathbf{1},\\
\mathbf{N}_1 &= \sqrt{\frac{p\varepsilon}{2}}\,\boldsymbol{\sigma}_3.
\end{aligned}$$

В такой форме очевидно, что это операторы Крауса для канала затухания фазы, имеющего вероятность декогерентизации с его окружением, равную εp. Обратим внимание на то, что при $\varepsilon \to 1$ мы воспроизводим канал затухания фазы из части (a), а при $\varepsilon \to 0$ затухание фазы исчезает.

d) Если канал из (c) описывает рассеяние отдельного фотона, то мы имеем $\Gamma_{\text{scatt}} = p\Delta t$. Но декогерентизация возникает только тогда, когда окружение может различить результаты рассеяния, то есть $\Gamma_{\text{decoh}} = \varepsilon p\Delta t$. Следовательно,

$$\Gamma_{\text{decoh}} = \varepsilon\Gamma_{\text{scatt}}.$$

3.6. Декогерентизация на сфере Блоха

a) Под действием канала затухания фазы матрица плотности $\rho = \frac{1}{2}(\mathbf{1} + \vec{P}\cdot\vec{\sigma})$ эволюционирует как (используя операторы M_μ из задачи 3.5)

$$\begin{aligned}
\rho \to\ & \mathrm{M}_0\rho\mathrm{M}_0^\dagger + \mathrm{M}_1\rho\mathrm{M}_1^\dagger + \mathrm{M}_2\rho\mathrm{M}_2^\dagger = \\
=\ & (1-p)\rho + \frac{p}{4}(\mathbf{1}+\sigma_3)\rho(\mathbf{1}+\sigma_3) + \frac{p}{4}(\mathbf{1}-\sigma_3)\rho(\mathbf{1}-\sigma_3) = \\
=\ & \left(1-\frac{p}{2}\right)\rho + \frac{p}{2}\sigma_3\rho\sigma_3 = \\
=\ & \left(1-\frac{p}{2}\right)\rho + \frac{p}{2}\left[\frac{1}{2}\Big(\mathbf{1}+\sigma_3(\vec{P}\cdot\vec{\sigma})\sigma_3\Big)\right] = \\
=\ & \left(1-\frac{p}{2}\right)\rho + \frac{p}{2}\left[\frac{1}{2}\Big(\mathbf{1}-\vec{P}\cdot\vec{\sigma}+2P_3\sigma_3\Big)\right] = \\
=\ & \frac{1}{2}\left[\left(1-\frac{p}{2}+\frac{p}{2}\right)\mathbf{1} + \left(1-\frac{p}{2}-\frac{p}{2}\right)\vec{P}\cdot\vec{\sigma} + pP_3\sigma_3\right] = \\
=\ & \frac{1}{2}\Big[\mathbf{1} + (1-p)\vec{P}\cdot\vec{\sigma} + pP_3\sigma_3\Big] = \\
=\ & \frac{1}{2}\Big[\mathbf{1} + \Big((1-p)P_1, (1-p)P_2, P_3\Big)\cdot\vec{\sigma}\Big].
\end{aligned}$$

Таким образом, мы видим, что действие канала затухания фазы сжимает сферу Блоха, превращая ее в вытянутый вдоль оси z сфероид (эллипсоид вращения). Выделенное положение оси z означает, что канал затухания фазы действует в некотором предпочтительном базисе.

b) Под действием канала затухания амплитуды матрица плотности ρ эволюционирует как

$$\begin{aligned}
\rho \to\ & \mathrm{M}_0\rho\mathrm{M}_0^\dagger + \mathrm{M}_1\rho\mathrm{M}_1^\dagger \\
=\ & \frac{1}{2}\left[\begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-p} \end{pmatrix}(\mathbf{1}+\vec{P}\cdot\vec{\sigma})\begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-p} \end{pmatrix}\right] + \\
& + \frac{1}{2}\left[\begin{pmatrix} 0 & \sqrt{p} \\ 0 & 0 \end{pmatrix}(\mathbf{1}+\vec{P}\cdot\vec{\sigma})\begin{pmatrix} 0 & 0 \\ \sqrt{p} & 0 \end{pmatrix}\right] = \\
=\ & \frac{1}{2}\left[\begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-p} \end{pmatrix}\begin{pmatrix} 1+P_3 & P_1-iP_2 \\ P_1+iP_2 & 1-P_3 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-p} \end{pmatrix}\right] +
\end{aligned}$$

$$+\frac{1}{2}\left[\begin{pmatrix} 0 & \sqrt{p} \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1+P_3 & P_1-iP_2 \\ P_1+iP_2 & 1-P_3 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ \sqrt{p} & 0 \end{pmatrix}\right] =$$

$$= \frac{1}{2}\begin{pmatrix} 1+P_3+p-pP_3 & (P_1-iP_2)\sqrt{1-p} \\ (P_1+iP_2)\sqrt{1-p} & 1-P_3-p+pP_3 \end{pmatrix} =$$

$$= \frac{1}{2}\left[\mathbf{1} + \left(\sqrt{1-p}\,P_1, \sqrt{1-p}\,P_2, P_3 + p(1-P_3)\right)\cdot\vec{\boldsymbol{\sigma}}\right].$$

Таким образом, мы видим, что действие канала затухания амплитуды сжимает сферу Блоха в сплюснутый вдоль оси z эллипсоид вращения и сдвигает ее вверх.

c) Под действием «двойного канала Паули» матрица плотности $\boldsymbol{\rho}$ эволюционирует как

$$\boldsymbol{\rho} \to \mathbf{M}_0\boldsymbol{\rho}\mathbf{M}_0^\dagger + \mathbf{M}_1\boldsymbol{\rho}\mathbf{M}_1^\dagger + \mathbf{M}_2\boldsymbol{\rho}\mathbf{M}_2^\dagger =$$

$$= (1-p)\boldsymbol{\rho} + \frac{p}{2}\boldsymbol{\sigma}_1\boldsymbol{\rho}\boldsymbol{\sigma}_1 + \frac{p}{2}\boldsymbol{\sigma}_3\boldsymbol{\rho}\boldsymbol{\sigma}_3 =$$

$$= (1-p)\boldsymbol{\rho} + \frac{p}{2}\left[\frac{1}{2}\left(\mathbf{1}+\boldsymbol{\sigma}_1(\vec{P}\cdot\vec{\boldsymbol{\sigma}})\boldsymbol{\sigma}_1\right) + \frac{1}{2}\left(\mathbf{1}+\boldsymbol{\sigma}_3(\vec{P}\cdot\vec{\boldsymbol{\sigma}})\boldsymbol{\sigma}_3\right)\right] =$$

$$= (1-p)\boldsymbol{\rho} + \frac{p}{2}\left[\mathbf{1} - \frac{1}{2}\vec{P}\cdot\vec{\boldsymbol{\sigma}} + P_1\boldsymbol{\sigma}_1 - \frac{1}{2}\vec{P}\cdot\vec{\boldsymbol{\sigma}} + P_3\boldsymbol{\sigma}_3\right] =$$

$$= \frac{1}{2}\left[(1-p+p)\mathbf{1} + (1-p-p)\vec{P}\cdot\vec{\boldsymbol{\sigma}} + p\vec{P}\cdot\vec{\boldsymbol{\sigma}} - pP_2\boldsymbol{\sigma}_2\right] =$$

$$= \frac{1}{2}\left[\mathbf{1} + \left((1-p)P_1, (1-2p)P_2, (1-p)P_3\right)\cdot\vec{\boldsymbol{\sigma}}\right].$$

Таким образом, действие двойного канала Паули при $p < \frac{1}{2}$ сжимает сферу Блоха в сплюснутый вдоль оси y эллипсоид вращения, а при $p > \frac{1}{2}$ — в вытянутый вдоль оси y инвертированный сфероид (однополостной гиперболоид вращения).

3.7. Декогерентизация затухающего осциллятора

a) Рассмотрим производную X по времени:

$$\dot{X} = \mathrm{tr}\left[\dot{\boldsymbol{\rho}}_I(t)e^{\lambda\mathbf{a}^\dagger}e^{-\lambda^*\mathbf{a}}\right] =$$

$$= \Gamma\,\mathrm{tr}\left[\left(\mathbf{a}\boldsymbol{\rho}_I\mathbf{a}^\dagger - \frac{1}{2}\mathbf{a}^\dagger\mathbf{a}\boldsymbol{\rho}_I - \frac{1}{2}\boldsymbol{\rho}_I\mathbf{a}^\dagger\mathbf{a}\right)e^{\lambda\mathbf{a}^\dagger}e^{-\lambda^*\mathbf{a}}\right].$$

Чтобы упростить это выражение, мы хотим преобразовать два вторых слагаемых под знаком следа к такому же виду, что и первое (с целью по возможности сократить их друг с другом). Это можно сделать, используя свойство инвариантности следа относительно циклических перестановок и коммутационные соотношения между операторами уничтожения и рождения:

$$[\mathbf{a}, \mathbf{a}^\dagger] = \mathbf{1},$$

$$[\mathbf{a}, e^{\lambda \mathbf{a}^\dagger}] = [\mathbf{a}, \mathbf{a}^\dagger] \frac{\partial}{\partial \mathbf{a}^\dagger} \left(e^{\lambda \mathbf{a}^\dagger} \right) = \lambda e^{\lambda \mathbf{a}^\dagger},$$

$$[e^{-\lambda^* \mathbf{a}}, \mathbf{a}^\dagger] = \frac{\partial}{\partial \mathbf{a}} \left(e^{-\lambda^* \mathbf{a}} \right) [\mathbf{a}, \mathbf{a}^\dagger] = -\lambda^* e^{-\lambda^* \mathbf{a}}.$$

Применяя эти манипуляции к $\dot{X}$, найдем

$$\dot{X} = \Gamma \operatorname{tr} \left[\left(\mathbf{a} \boldsymbol{\rho}_I \mathbf{a}^\dagger - \frac{1}{2} \mathbf{a} \boldsymbol{\rho}_I (\mathbf{a}^\dagger - \lambda^*) - \frac{1}{2} (\mathbf{a} + \lambda) \boldsymbol{\rho}_I \mathbf{a}^\dagger \right) e^{\lambda \mathbf{a}^\dagger} e^{-\lambda^* \mathbf{a}} \right] =$$

$$= \frac{\Gamma}{2} \operatorname{tr} \left[\lambda^* \boldsymbol{\rho}_I e^{\lambda \mathbf{a}^\dagger} \mathbf{a} e^{-\lambda^* \mathbf{a}} - \lambda \boldsymbol{\rho}_I \mathbf{a}^\dagger e^{\lambda \mathbf{a}^\dagger} e^{-\lambda^* \mathbf{a}} \right].$$

От лишних операторов рождения и уничтожения можно избавиться, используя правила дифференцирования экспонент:

$$\frac{\partial}{\partial \lambda^*} e^{-\lambda^* \mathbf{a}} = -\mathbf{a} e^{-\lambda^* \mathbf{a}},$$

$$\frac{\partial}{\partial \lambda} e^{\lambda \mathbf{a}^\dagger} = \mathbf{a}^\dagger e^{\lambda \mathbf{a}^\dagger};$$

таким образом, мы получаем для $\dot{X}$ дифференциальное уравнение в частных производных:

$$\dot{X} = -\frac{\Gamma}{2} \operatorname{tr} \left[\lambda^* \boldsymbol{\rho}_I e^{\lambda \mathbf{a}^\dagger} \frac{\partial}{\partial \lambda^*} \left(e^{-\lambda^* \mathbf{a}} \right) + \lambda \boldsymbol{\rho}_I \frac{\partial}{\partial \lambda} \left(e^{\lambda \mathbf{a}^\dagger} \right) e^{-\lambda^* \mathbf{a}} \right] =$$

$$= -\frac{\Gamma}{2} \lambda^* \frac{\partial}{\partial \lambda^*} \operatorname{tr} \left[\boldsymbol{\rho}_I e^{\lambda \mathbf{a}^\dagger} e^{-\lambda^* \mathbf{a}} \right] - \frac{\Gamma}{2} \lambda \frac{\partial}{\partial \lambda} \operatorname{tr} \left[\boldsymbol{\rho}_I e^{\lambda \mathbf{a}^\dagger} e^{-\lambda^* \mathbf{a}} \right] =$$

$$= -\frac{\Gamma}{2} \left(\lambda^* \frac{\partial X}{\partial \lambda^*} + \lambda \frac{\partial X}{\partial \lambda} \right).$$

Здесь я довольно бесцеремонно переставил порядок операций дифференцирования и вычисления следа. Для данных целей я буду предполагать, что

здесь все относящиеся к делу функции равномерно непрерывны, так что эта коммутация разрешена.

Используя правило дифференцирования сложных функций (цепное правило), мы можем записать для X линейное уравнение в частных производных с постоянными коэффициентами:

$$\dot{X} = -\frac{\Gamma}{2}\left(\frac{\partial X}{\partial \ln \lambda^*} + \frac{\partial X}{\partial \ln \lambda}\right).$$

Естественно предположить, что решение этого равнения является функцией от линейной комбинации его аргументов:

$$X = X(\alpha \ln \lambda^* + \beta \ln \lambda + \gamma t).$$

Подставляя этот *анзац* в уравнение, мы находим соотношение между коэффициентами

$$\gamma = -\frac{\Gamma}{2}(\alpha + \beta),$$

что дает искомый скейлинговый закон:

$$\begin{aligned} X(\vec{\lambda}, t) &= X\left(\alpha \ln \lambda^* + \beta \ln \lambda - \frac{\Gamma}{2}(\alpha + \beta)t\right) \\ &= X\left(\alpha \ln\left(\lambda^* e^{-\Gamma t/2}\right) + \beta \ln\left(\lambda e^{-\Gamma t/2}\right)\right) \\ &= X(\vec{\lambda}', 0), \end{aligned}$$

$$\vec{\lambda}' = \vec{\lambda} e^{-\Gamma t/2}.$$

b) Прежде чем начинать решение, следует заметить, что этот кот ненормален не только в житейском смысле, но и в смысле борновской интерпретации. Чтобы должным образом нормировать этого кота, нам нужно положить равным единице «бра-кот кет-кот»:

$$|\mathrm{cat}\rangle = \frac{N}{\sqrt{2}}\left(|\alpha_1\rangle + |\alpha_2\rangle\right),$$

$$\langle \mathrm{cat}|\mathrm{cat}\rangle = \frac{|N|^2}{2}\left(\langle\alpha_1|\alpha_1\rangle + \langle\alpha_1|\alpha_2\rangle + \langle\alpha_2|\alpha_1\rangle + \langle\alpha_2|\alpha_2\rangle\right) = 1.$$

Но вместо того чтобы отвлекаться на дальнейшие детали нормировки этого кота, я просто замечу, что перед ним должен быть нормирующий множитель.

Результаты части (а) показывают, как связаны между собой след кота и оператора в момент времени t с их следом в момент $t = 0$. Однако оператором под знаком следа является оператор «смещения» $\mathbf{D}_\lambda = e^{\lambda \mathbf{a}^\dagger} e^{-\lambda^* \mathbf{a}}$, который переводит одно когерентное состояние в другое. Поскольку оператор любой наблюдаемой осциллятора можно разложить по этим операторам сдвига[1], то временная эволюция кота полностью определяется тем, как изменяется во времени действие на него этих операторов сдвига.

Конкретнее, согласно части (а):

$$\mathrm{tr}\left[|\mathrm{cat}(0)\rangle\langle\mathrm{cat}(0)|e^{\lambda'\mathbf{a}^\dagger}e^{-\lambda'^*\mathbf{a}}\right] = \mathrm{tr}\left[\boldsymbol{\rho}_{\mathrm{cat}}(t)e^{\lambda\mathbf{a}^\dagger}e^{-\lambda^*\mathbf{a}}\right].$$

В общем случае $\boldsymbol{\rho}_{\mathrm{cat}}(t)$ не обязано быть чистым состоянием (фактически мы увидим, что оно им не является), но до поры до времени будем предполагать его чистым. Это даст возможность преобразовать следы в математические ожидания. С помощью внутреннего произведения когерентных состояний

$$\begin{aligned}\langle\alpha|\beta\rangle &= e^{\alpha^*\beta - \left(|\alpha|^2+|\beta|^2\right)/2} = \\ &= e^{-\frac{1}{2}\left(|\alpha|^2+|\beta|^2-2\mathrm{Re}(\alpha^*\beta)\right)} e^{i\mathrm{Im}(\alpha^*\beta)} = \\ &= e^{-\frac{1}{2}|\alpha-\beta|^2} e^{i\mathrm{Im}(\alpha^*\beta)}\end{aligned}$$

мы находим, что

$$\langle\mathrm{cat}(t)|e^{\lambda\mathbf{a}^\dagger}e^{-\lambda^*\mathbf{a}}|\mathrm{cat}(t)\rangle = \langle\mathrm{cat}(0)|e^{\lambda'\mathbf{a}^\dagger}e^{-\lambda'^*\mathbf{a}}|\mathrm{cat}(0)\rangle,$$

$$\begin{pmatrix} e^{\lambda\alpha_1^*(t)-\lambda^*\alpha_1(t)} + \\ e^{\lambda\alpha_2^*(t)-\lambda^*\alpha_2(t)} + \\ \langle\alpha_1(t)|\alpha_2(t)\rangle e^{\lambda\alpha_1^*(t)-\lambda^*\alpha_2(t)} + \\ \langle\alpha_2(t)|\alpha_1(t)\rangle e^{\lambda\alpha_2^*(t)-\lambda^*\alpha_1(t)} \end{pmatrix} \cdot \begin{pmatrix} e^{(\lambda\alpha_1^*-\lambda^*\alpha_1)e^{-\Gamma t/2}} + \\ e^{(\lambda\alpha_2^*-\lambda^*\alpha_2)e^{-\Gamma t/2}} + \\ \langle\alpha_1|\alpha_2\rangle e^{(\lambda\alpha_1^*-\lambda^*\alpha_2)e^{-\Gamma t/2}} + \\ \langle\alpha_2|\alpha_1\rangle e^{(\lambda\alpha_2^*-\lambda^*\alpha_1)e^{-\Gamma t/2}} \end{pmatrix}.$$

[1] См., например, A. Peres, *Quantum Theory: Concepts and Methods*, Kluwer Academic Publishers, New York et al, 2002. [Оператор сдвига $\mathbf{D}(\lambda)$, действуя на $|0\rangle$ — основное состояние гармонического осциллятора, преобразует в $|\lambda\rangle = \mathbf{D}(\lambda)|0\rangle$ — собственное состояние оператора уничтожения $\mathbf{a}|\lambda\rangle = \lambda|\lambda\rangle$ (когерентное состояние). Преобразование одного когерентного состояния в другое обеспечивает закон умножения операторов сдвига $\mathbf{D}(\lambda)\mathbf{D}(\mu) = \mathbf{D}(\lambda + \mu)\exp[(\lambda\mu^* - \lambda^*\mu)/2]$. На русском языке с теорией когерентных состояний можно познакомиться по книгам И. А. Малкин, В. И. Манько, *Динамические симметрии и когерентные состояния квантовых систем*, М.: Наука (1979); А. М. Переломов, *Обобщенные когерентные состояния и их применения*, (1987). — *Прим. ред.*]

Эти слагаемые можно было бы почти согласовать друг с другом, предполагая, что эволюция во времени преобразует чистое состояние в другое чистое, но это ведет к тому, что недиагональные элементы не подходят друг к другу:

$$
\begin{aligned}
|\alpha_{1,2}\rangle &\to \left|\alpha_{1,2}e^{-\Gamma t/2}\right\rangle,\\
e^{\lambda \mathbf{a}^\dagger} e^{-\lambda^* \mathbf{a}} \left|\alpha_{1,2}e^{-\Gamma t/2}\right\rangle &= e^{(\lambda\alpha_{1,2}^* - \lambda^*\alpha_{1,2})e^{-\Gamma t/2}} \left|\alpha_{1,2}e^{-\Gamma t/2}\right\rangle,\\
\left\langle \alpha_{1,2}e^{-\Gamma t/2}\right| \left.\alpha_{2,1}e^{-\Gamma t/2}\right\rangle &= \langle\alpha_2|\alpha_1\rangle^{e^{-\Gamma t}} \neq \langle\alpha_2|\alpha_1\rangle.
\end{aligned}
$$

Чтобы исправить это несоответствие недиагональных элементов, мы должны потребовать, чтобы недиагональные компоненты кота затухали быстрее диагональных, как раз базис для когерентных состояний является затухающим. Это ведет к полностью перемешивающей состояния эволюции:

$$
\begin{aligned}
|\alpha_1\rangle\langle\alpha_1| &\to \left|\alpha_1 e^{-\Gamma t/2}\right\rangle \left\langle \alpha_1 e^{-\Gamma t/2}\right|,\\
|\alpha_2\rangle\langle\alpha_2| &\to \left|\alpha_2 e^{-\Gamma t/2}\right\rangle \left\langle \alpha_2 e^{-\Gamma t/2}\right|,\\
|\alpha_1\rangle\langle\alpha_2| &\to \langle\alpha_1|\alpha_2\rangle^{(1-e^{-\Gamma t})} \left|\alpha_1 e^{-\Gamma t/2}\right\rangle \left\langle \alpha_2 e^{-\Gamma t/2}\right|,\\
|\alpha_2\rangle\langle\alpha_1| &\to \langle\alpha_2|\alpha_1\rangle^{(1-e^{-\Gamma t})} \left|\alpha_2 e^{-\Gamma t/2}\right\rangle \left\langle \alpha_1 e^{-\Gamma t/2}\right|.
\end{aligned}
$$

Таким образом, наш кот эволюционирует в нечто более диагональное:

$$
\begin{aligned}
|\mathrm{cat}(0)\rangle\langle\mathrm{cat}(0)| \to \frac{|N|^2}{2} &\begin{pmatrix} 1 & \langle\alpha_1|\alpha_2\rangle^{(1-e^{-\Gamma t})} \\ \langle\alpha_2|\alpha_1\rangle^{(1-e^{-\Gamma t})} & 1 \end{pmatrix} =\\
= \frac{|N|^2}{2} &\Big[\mathbf{1} + e^{-\frac{1}{2}|\alpha_1-\alpha_2|^2(1-e^{-\Gamma t})}\big(\boldsymbol{\sigma}_x \cos\theta_{21}(t) +\\
&+ \boldsymbol{\sigma}_y \sin\theta_{21}(t)\big)\Big],
\end{aligned}
$$

где матрица плотности выше выражается в зависящем от времени базисе $\begin{pmatrix} |\alpha_1 e^{-\Gamma t/2}\rangle \\ |\alpha_2 e^{-\Gamma t/2}\rangle \end{pmatrix}$, а углы поворота $\theta_{21}(t)$ определяются как $\theta_{21}(t) = \mathrm{Im}\,(\alpha_2^*\alpha_1)(1-e^{-\Gamma t})$.

Если мы рассматриваем затухание только недиагональных элементов, то можно игнорировать фазу $\theta_{21}(t)$. Для времен $t \ll 1/\Gamma$ базисные состоя-

ния остаются приблизительно такими же:

$$|\alpha_1(t)\rangle \simeq \left|\alpha_1\left(1-\frac{\Gamma t}{2}\right)\right\rangle \simeq |\alpha_1\rangle,$$

а амплитуды недиагональных элементов экспоненциально затухают со временем:

$$e^{-\frac{1}{2}|\alpha_1-\alpha_2|^2(1-e^{-\Gamma t})} \simeq e^{-\frac{1}{2}|\alpha_1-\alpha_2|^2(1-(1-\Gamma t))} \simeq e^{-\frac{\Gamma t}{2}|\alpha_1-\alpha_2|^2}.$$

Решения упражнений к главе 4

4.1. Теорема Харди

Боб и Клер делят множество идентично приготовленных копий состояния

$$|\psi\rangle_{BC} = \sqrt{1-2x}|0\rangle_B \otimes |0\rangle_C + \sqrt{x}|0\rangle_B \otimes |1\rangle_C + \sqrt{x}|1\rangle_B \otimes |0\rangle_C,$$

где x — вещественное число из интервала $[0, 1/2]$.

а) Если Боб выполняет измерение в базисе $\{|0\rangle, |1\rangle\}$, а Клер — в базисе $\{|\varphi\rangle, |\varphi^\perp\rangle\}$, то всякий раз, когда результатом Боба является $|0\rangle$, Клер получает $|\varphi\rangle$. Вследствие симметрии подсистем в $|\psi\rangle_{BC}$, такая же картина будет наблюдаться, если Боб и Клер обменяются базисами.

Тогда мы можем спроецировать разделенное состояние на $|0\rangle$ в одной подсистеме, чтобы найти $|\varphi\rangle$ в другой подсистеме:

$$\begin{aligned}(|0\rangle_B\,{}_B\langle 0| \otimes \mathbf{1}_C)\,|\psi\rangle_{BC} &= \sqrt{1-2x}|0\rangle_B \otimes |0\rangle_C + \sqrt{x}|0\rangle_B \otimes |1\rangle_C = \\ &= |0\rangle_B \otimes \left(\sqrt{1-2x}|0\rangle_C + \sqrt{x}|1\rangle_C\right) \\ (|0\rangle_B\,{}_B\langle 0| \otimes \mathbf{1}_C)\,|\psi\rangle_{BC} &= |0\rangle_B \otimes (\mathcal{N}|\varphi\rangle_C).\end{aligned}$$

Нормируя проекцию, мы находим

$$|\varphi\rangle = \sqrt{\frac{1-2x}{1-x}}|0\rangle + \sqrt{\frac{x}{1-x}}|1\rangle.$$

Рассмотрим некоторое нормированное состояние $|\chi\rangle = a|0\rangle + b|1\rangle$, где $a, b \in \mathbb{C}$. Поскольку

$$\langle\chi^\perp|\chi\rangle = (b\langle 0| - a\langle 1|)\,(a|0\rangle + b|1\rangle) = 0,$$

то ортогональное ему нормированное состояние равно $|\chi^{\perp}\rangle = b^*|0\rangle - a^*|1\rangle$. Следовательно, учитывая, что при $x \in [0, 1/2]$ коэффициенты вещественны, мы можем определить

$$|\varphi^{\perp}\rangle = \sqrt{\frac{x}{1-x}}|0\rangle - \sqrt{\frac{1-2x}{1-x}}|1\rangle,$$

b) Боб и Клер оба выбрали $\{|\varphi\rangle, |\varphi^{\perp}\rangle\}$ в качестве базиса измерения. Вероятность $P(x)$ того, что результатом обоих измерений является $|\varphi^{\perp}\rangle$, вычисляется как квадрат соответствующей амплитуды состояния $|\psi\rangle_{BC}$:

$$P(x) = \left|\left({}_B\langle\varphi^{\perp}| \otimes {}_C\langle\varphi^{\perp}|\right)|\psi\rangle_{BC}\right|^2.$$

Мы можем вычислить

$$\begin{aligned}
{}_B\langle\varphi^{\perp}| \otimes {}_C\langle\varphi^{\perp}| &= \left(\sqrt{\frac{x}{1-x}}\,{}_B\langle 0| - \sqrt{\frac{1-2x}{1-x}}\,{}_B\langle 1|\right) \otimes \\
&\quad \left(\sqrt{\frac{x}{1-x}}\,{}_C\langle 0| - \sqrt{\frac{1-2x}{1-x}}\,{}_C\langle 1|\right), \\
{}_B\langle\varphi^{\perp}| \otimes {}_C\langle\varphi^{\perp}| &= \frac{x}{1-x}\,{}_B\langle 0| \otimes {}_C\langle 0| + \frac{1-2x}{1-x}\,{}_B\langle 1| \otimes {}_C\langle 1| - \\
&\quad - \frac{\sqrt{x(1-2x)}}{1-x}\left({}_B\langle 0| \otimes {}_C\langle 1| + {}_B\langle 1| \otimes {}_C\langle 0|\right).
\end{aligned}$$

Подстановка разложений ${}_B\langle\varphi^{\perp}| \otimes {}_C\langle\varphi^{\perp}|$ и $|\psi\rangle_{BC}$ в базисе $\{|0\rangle, |1\rangle\}$ в определение $P(x)$ дает следующий результат:

$$\begin{aligned}
P(x) &= \left|\frac{x}{1-x}\sqrt{1-2x} + \frac{1-2x}{1-x}\cdot(0) - \frac{\sqrt{x(1-2x)}}{1-x}(\sqrt{x}+\sqrt{x})\right|^2 = \\
&= \left|\frac{x\sqrt{1-2x}}{1-x} - \frac{2x\sqrt{1-2x}}{1-x}\right|^2 = \\
&= \left|-\frac{x\sqrt{1-2x}}{1-x}\right|^2, \\
P(x) &= \frac{x^2(1-2x)}{(1-x)^2}.
\end{aligned}$$

c) Заметим, что $P(x) \geqslant 0$ при $x \in [0, 1/2]$ и $P(0) = P(1/2) = 0$. Так как $P(x)$ непрерывна в этом интервале, ее максимум достигается в некоторой внутренней критической точке, удовлетворяющей условию $\dfrac{dP(x)}{dx} = 0$ (или ∞):

$$\frac{dP(x)}{dx} = \frac{d}{dx}\left[\frac{x^2(1-2x}{(1-x)^2}\right] = \frac{2x}{(1-x)^3}\Big[1 - 4x + 3x^2 + x - 2x^2\Big],$$

$$\frac{dP(x)}{dx} = \frac{2x}{(1-x)^3}\big(x^2 - 3x + 1\big).$$

Корнями приведенного выше квадратного трехчлена являются $x = \frac{1}{2}(3 \pm \sqrt{5})$. Внутри $0 < x < 1/2$ лежит только одна критическая точка $P(x)$: $x = \frac{1}{2}(3 - \sqrt{5})$. Подставляя ее значение в выражение для $P(x)$, находим $P_{\max} = \frac{1}{2}(5\sqrt{5} - 11)$.

d) Если $P(x)$ не равна нулю (что соответствует $0 < x < 1/2$), то существует измеримое нарушение предсказания Альберта (и теоремы Харди). Рассуждения Альберта некорректны на этапе комбинирования результатов двух взаимно исключающих экспериментов. Наблюдаемые, соответствующие измерениям в различных базисах, не коммутируют между собой, то есть не имеет смысла рассматривать систему общих собственных состояний обеих наблюдаемых. Коль скоро Боб (или Клер) выбирает измерение в базисе $\{|0\rangle, |1\rangle\}$, мы никогда не сможем (с определенностью) узнать, каким был бы результат измерения в базисе $\{|\varphi\rangle, |\varphi^{\perp}\rangle\}$.

Заметим, что одного запутывания недостаточно, чтобы опровергнуть рассуждения Альберта. До тех пор, пока Альберт рассматривает только коммутирующие наблюдаемые, он может построить теорию скрытых переменных, чтобы объяснить корреляции результатов измерений. Например, в случаях $x = 0$ и $x = 1/2$ оба базиса становятся идентичными и, как предсказывал Альберт, $P(x) = 0$.[1]

4.2. Закрытие лазейки детектирования

a) Выберем переменные $x, x', y, y' \in \{0, 1\}$. Мы хотим показать, что

$$xy + xy' + x'y - x'y' \leqslant x + y, \quad \forall\, x, x', y, y'.$$

[1] Заметим, что состояние $|\psi\rangle_{BC}$, факторизуемое при $x = 0$, остается запутанным при $x = 1/2$. – *Прим. ред.*

Конечно, можно перебрать все 16 возможностей. С другой стороны, мы могли бы воспользоваться неравенством КГШХ (доказанным на лекциях), определив переменные $\alpha = 2x - 1$, $\alpha' = 2x' - 1$, $\beta = 2y - 1$, $\beta' = 2y' - 1$. Заметим, что $\alpha, \alpha', \beta, \beta' \in \{-1, 1\}$. Применим неравенство КГШХ:

$$
\begin{aligned}
2 &\geqslant \alpha\beta + \alpha\beta' + \alpha'\beta - \alpha'\beta', \\
2 &\geqslant (2x-1)(2y-1) + (2x-1)(2y'-1) + \\
&\quad + (2x'-1)(2y-1) - (2x'-1)(2y'-1), \\
2 &\geqslant 4xy - 2x - 2y + 1 + 4xy' - 2x - 2y' + 1 + \\
&\quad + 4x'y - 2x' - 2y + 1 - 4x'y' + 2x' + 2y' - 1, \\
2 &\geqslant 4xy + 4xy' + 4x'y - 4x'y' - 4x - 4y + 2, \\
2 &\geqslant 4\Big[(xy + xy' + x'y - x'y') - (x + y)\Big] + 2, \\
0 &\geqslant (xy + xy' + x'y - x'y') - (x + y).
\end{aligned}
$$

Следовательно, $xy + xy' + x'y - x'y' \leqslant x + y \ \ \forall x, x', y, y' \in \{0, 1\}$.

b) Предположим, что существует локальная теория скрытых переменных, описывающая результаты выполняемых Алисой и Бобом измерений N фотонных пар. Пусть переменные $x_i, x_i', y_i, y_i' \in \{0, 1\}$ обозначают результаты регистрации фотонов i-й пары. А именно, $x_i, x_i' \in \{0, 1\}$ обозначают, сработал или нет детектор Алисы, ориентированный вдоль оси $\hat{a}$ или $\hat{a}'$ соответственно. Аналогично переменные $y_i, y_i' \in \{0, 1\}$ обозначают, сработал или нет детектор Боба, ориентированный вдоль оси $\hat{b}$ или $\hat{b}'$ соответственно. Каждый набор переменных x, x', y, y' должен удовлетворять доказанному в части (a) соотношению

$$x_i y_i + x_i y_i' + x_i' y_i - x_i' y_i' \leqslant x_i + y_i.$$

Сложим N неравенств, чтобы получить

$$
\begin{aligned}
\sum_{i=1}^{N} (x_i y_i + x_i y_i' + x_i' y_i - x_i' y_i') &\leqslant \sum_{i=1}^{N} (x_i + y_i), \\
\sum_{i=1}^{N} x_i y_i + \sum_{i=1}^{N} x_i y_i' + \sum_{i=1}^{N} x_i' y_i - \sum_{i=1}^{N} x_i' y_i' &\leqslant \sum_{i=1}^{N} x_i + \sum_{i=1}^{N} y_i.
\end{aligned}
$$

Деление обеих частей на положительное целое число не меняет неравенство, поэтому

$$\frac{1}{N}\sum_{i=1}^{N} x_i y_i + \frac{1}{N}\sum_{i=1}^{N} x_i y_i' + \frac{1}{N}\sum_{i=1}^{N} x_i' y_i - \frac{1}{N}\sum_{i=1}^{N} x_i' y_i' \leqslant \frac{1}{N}\sum_{i=1}^{N} x_i + \frac{1}{N}\sum_{i=1}^{N} y_i.$$

Выражения в левой части этого неравенства дают оценки вероятностей того, что Алиса и Боб одновременно детектируют отдельную фотонную пару (при определенном расположении их детекторов). Выражения в правой части дают оценки вероятностей того, что Алиса или Боб независимо детектируют фотон детекторами, ориентированными вдоль осей $\hat{a}$ и $\hat{b}$ соответственно. Пусть N настолько велико, что эти оценки достаточно близки к соответствующим вероятностям скрытых переменных. Тогда мы приходим к выводу, что

$$P_{++}(ab) + P_{++}(ab') + P_{++}(a'b) - P_{++}(a'b') \leqslant P_{+\cdot}(a) + P_{\cdot+}(b).$$

c) Заметим, что базис состояний Белла $\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$ удовлетворяет

$$\begin{aligned}
\boldsymbol{\sigma}_X \otimes \mathbf{1}|\Phi^+\rangle &= |\Psi^+\rangle = \mathbf{1} \otimes \boldsymbol{\sigma}_X|\Phi^+\rangle, \\
\boldsymbol{\sigma}_Y \otimes \mathbf{1}|\Phi^+\rangle &= i|\Psi^-\rangle = -\mathbf{1} \otimes \boldsymbol{\sigma}_Y|\Phi^+\rangle, \\
\boldsymbol{\sigma}_Z \otimes \mathbf{1}|\Phi^+\rangle &= |\Phi^-\rangle = \mathbf{1} \otimes \boldsymbol{\sigma}_Z|\Phi^+\rangle.
\end{aligned}$$

Таким образом, $\langle\Phi^+|\hat{a}\cdot\vec{\boldsymbol{\sigma}} \otimes \mathbf{1}|\Phi^+\rangle = 0 = \langle\Phi^+|\mathbf{1} \otimes \hat{b}\cdot\vec{\boldsymbol{\sigma}}|\Phi^+\rangle$ при любых $\hat{a}$, $\hat{b}$.

При данном единичном 3-векторе $\hat{a}$ оператор $\hat{a}\cdot\vec{\boldsymbol{\sigma}}$ имеет собственные значения $\{-1, +1\}$, соответствующие собственным состояниям кубита, ориентированным или антипараллельно, или параллельно оси $\hat{a}$. Оператор $\frac{1}{2}(\mathbf{1} + \hat{a}\cdot\vec{\boldsymbol{\sigma}})$ имеет те же собственные состояния, но с собственными значениями $\{0, +1\}$. Математическое ожидание этого последнего оператора в точности совпадает с вероятностью срабатывания ориентированного вдоль оси $\hat{a}$ детектора при условии его идеальной эффективности.

Тогда мы можем выразить вероятность одновременного детектирования Алисой и Бобом фотонов из разделенного состояния $|\Phi^+\rangle$ при эффективностях детекторов η_A, η_B:

$$\begin{aligned}
P_{++}(ab) &= \left\langle \Phi^+ \left| \frac{\eta_A}{2}\left(\mathbf{1} + \hat{a}\cdot\vec{\boldsymbol{\sigma}}\right) \otimes \frac{\eta_B}{2}\left(\mathbf{1} + \hat{b}\cdot\vec{\boldsymbol{\sigma}}\right) \right| \Phi^+ \right\rangle = \\
&= \frac{\eta_A\eta_B}{4}\left\langle \Phi^+ \left| \mathbf{1}\otimes\mathbf{1} + \hat{a}\cdot\vec{\boldsymbol{\sigma}}\otimes\mathbf{1} + \mathbf{1}\otimes\hat{b}\cdot\vec{\boldsymbol{\sigma}} + (\hat{a}\cdot\vec{\boldsymbol{\sigma}})\otimes(\hat{b}\cdot\vec{\boldsymbol{\sigma}}) \right| \Phi^+ \right\rangle = \\
&= \frac{\eta_A\eta_B}{4}\left[1 + 0 + 0 + \hat{a}\cdot\hat{b}\right], \\
P_{++}(ab) &= \frac{1}{4}\eta_A\eta_B(1 + \hat{a}\cdot\hat{b}).
\end{aligned}$$

Аналогичным образом находим

$$P_{++}(ab') = \frac{1}{4}\eta_A\eta_B(1 + \hat{a}\cdot\hat{b}'),$$

$$P_{++}(a'b) = \frac{1}{4}\eta_A\eta_B(1 + \hat{a}'\cdot\hat{b}),$$

$$P_{++}(a'b') = \frac{1}{4}\eta_A\eta_B(1 + \hat{a}'\cdot\hat{b}').$$

Также можно вычислить вероятности независимого детектирования:

$$P_{+\cdot}(a) = \left\langle \Phi^+ \left| \frac{\eta_A}{2}\left(\mathbf{1} + \hat{a}\cdot\vec{\boldsymbol{\sigma}}\right)\otimes\mathbf{1} \right| \Phi^+ \right\rangle = \frac{\eta_A}{2},$$

$$P_{\cdot+}(b) = \left\langle \Phi^+ \left| \mathbf{1}\otimes\frac{\eta_B}{2}\left(\mathbf{1} + \hat{b}\cdot\vec{\boldsymbol{\sigma}}\right) \right| \Phi^+ \right\rangle = \frac{\eta_B}{2}.$$

Чтобы максимально нарушить неравенство КГШХ, следует выбрать $\hat{a} = \hat{x}$, $\hat{a}' = \hat{z}$, $\hat{b} = \frac{1}{\sqrt{2}}(\hat{x} + \hat{z})$ и $\hat{b}' = \frac{1}{\sqrt{2}}(\hat{x} - \hat{z})$. Подставим их в найденные выше выражения:

$$P_{++}(ab) = \frac{1}{4}\eta_A\eta_B\left(1 + \hat{x}\cdot\frac{1}{\sqrt{2}}(\hat{x} + \hat{z})\right) = \frac{1}{4}\eta_A\eta_B\left(1 + \frac{1}{\sqrt{2}}\right),$$

$$P_{++}(ab') = \frac{1}{4}\eta_A\eta_B\left(1 + \hat{x}\cdot\frac{1}{\sqrt{2}}(\hat{x} - \hat{z})\right) = \frac{1}{4}\eta_A\eta_B\left(1 + \frac{1}{\sqrt{2}}\right),$$

$$P_{++}(a'b) = \frac{1}{4}\eta_A\eta_B\left(1 + \hat{z}\cdot\frac{1}{\sqrt{2}}(\hat{x} + \hat{z})\right) = \frac{1}{4}\eta_A\eta_B\left(1 + \frac{1}{\sqrt{2}}\right),$$

$$P_{++}(a'b') = \frac{1}{4}\eta_A\eta_B\left(1 + \hat{z}\cdot\frac{1}{\sqrt{2}}(\hat{x} - \hat{z})\right) = \frac{1}{4}\eta_A\eta_B\left(1 - \frac{1}{\sqrt{2}}\right).$$

Комбинируя эти вероятности, получим

$$P_{++}(ab) + P_{++}(ab') + P_{++}(a'b) - P_{++}(a'b') = \frac{1}{4}\eta_A\eta_B\left(2 + \frac{4}{\sqrt{2}}\right),$$

$$P_{++}(ab) + P_{++}(ab') + P_{++}(a'b) - P_{++}(a'b') = \frac{1}{2}\eta_A\eta_B(1 + \sqrt{2}).$$

Максимально запутанное состояние $|\Phi^+\rangle$ может нарушить выведенное в части (b) неравенство для локальных скрытых переменных, если

$$P_{++}(ab) + P_{++}(ab') + P_{++}(a'b) - P_{++}(a'b') \geqslant P_{+\cdot}(a) + P_{\cdot+}(b),$$

$$\frac{1}{2}\eta_A\eta_B(1+\sqrt{2}) > \frac{\eta_A}{2}+\frac{\eta_B}{2},$$

$$\frac{\eta_A\eta_B}{\eta_A+\eta_B} > \frac{1}{1+\sqrt{2}}.$$

4.3. Телепортация с помощью непрерывных переменных

a) Проверим сформулированное утверждение, выражая запутанные состояния в базисе $\{|q_1\rangle \otimes |q_2\rangle\}$:

$$\begin{aligned}\langle Q', P'|Q, P\rangle &= \frac{1}{2\pi}\int dq\, dq' e^{i(Pq-P'q')}\langle q'|q\rangle\langle q'+Q'|q+Q\rangle = \\ &= \frac{1}{2\pi}\int dq e^{i(P-P')q}\delta(Q-Q') = \\ &= \delta(Q-Q')\delta(P-P').\end{aligned}$$

b) Чтобы найти коэффициенты, вновь разложим в базисе $\{|q_1\rangle \otimes |q_2\rangle\}$:

$$\begin{aligned}\langle Q', P'|q_1, q_2\rangle &= \frac{1}{\sqrt{2\pi}}\int dq e^{-iPq}\langle q|q_1\rangle\langle q+Q|q_2\rangle = \\ &= \frac{1}{\sqrt{2\pi}}\int dq e^{-iPq}\delta(q-q_1)\delta(q+Q-q_2) = \\ &= \frac{1}{\sqrt{2\pi}}e^{-iPq_1}\,\delta[Q-(q_2-q_1)].\end{aligned}$$

c) В этой части нам нужно оставить неизменными переменные p и q. Как и в уравнении (4.84) в лекциях, мы хотим выразить состояние системы AC в запутанном базисе. В этом базисе Алиса будет выполнять измерения, посылая их результаты Бобу. Тогда, используя эти результаты, Боб сможет реконструировать в своей лаборатории исходное состояние системы C. Это — грубое описание того, как должна работать телепортация; после выполнения некоторых предварительных вычислений я представлю полную процедуру, которой должны следовать Алиса и Боб.

В качестве первого шага представим систему AC в запутанном базисе. Предварительно записав $|\psi\rangle_{ABC}$ в базисе

$$\{|q_1\rangle_A \otimes |q_2\rangle_B \otimes |q_3\rangle_C\},$$

сделаем это, используя тождественную вставку

$$1 = \int dQ'\, dP' |Q', P'\rangle_{CA\,CA}\langle Q', P'|.$$

Получающиеся при этом коэффициенты ${}_{CA}\langle Q', P'|q_1, q_2\rangle_{CA}$, которые уже были вычислены в части (b), позволяют перевыразить состояние в запутанном базисе системы AC:

$$
\begin{aligned}
|\psi\rangle_C|Q,P\rangle_{AB} &= \int dq\, {}_C\langle q|\psi\rangle_C|q\rangle_C \times \frac{1}{\sqrt{2\pi}}\int dq'\, e^{iPq'}|q'\rangle_A|q'+Q\rangle_B = \\
&= \frac{1}{\sqrt{2\pi}}\int dq\, dq'\, dQ'\, dP'\, {}_C\langle q|\psi\rangle_C e^{iPq'}\times \\
&\quad \times|Q',P'\rangle_{CA}\,{}_{CA}\langle Q',P'|q,q'\rangle_{CA}\otimes|q'+Q\rangle_B = \\
&= \frac{1}{2\pi}\int dq\, dq'\, dQ'\, dP'\, {}_C\langle q|\psi\rangle_C e^{iPq'}\times \\
&\quad \times e^{-iP'q}\delta[Q'-(q'-q)]|Q',P'\rangle_{CA}\otimes|q'+Q\rangle_B = \\
&= \frac{1}{2\pi}\int dq\, dQ'\, dP'\, {}_C\langle q|\psi\rangle_C e^{iP(Q'+q)-iP'q}\times \\
&\quad \times|Q',P'\rangle_{CA}\otimes|q+Q'+Q\rangle_B.
\end{aligned}
$$

С этого момента Алиса выполняет измерение в запутанном базисе AC, получая некоторое состояние $|Q',P'\rangle_{CA}$. Результирующим состоянием Боба является

$$
|\mathrm{Bob}\rangle = \int dq\, {}_C\langle q|\psi\rangle_C e^{iPQ'-i(P-P')q}|q+Q'+Q\rangle_B.
$$

Боб имеет почти все, что ему необходимо. Если Алиса посылает ему результаты своего измерения (Q',P'), то он может применить параллельные переносы координаты и импульса:

$$
\begin{aligned}
\mathbf{D}(q) &= e^{iq\mathbf{P}} = \int dq'\,|q'+q\rangle\langle q'|, \\
\mathbf{D}(p) &= e^{-ip\mathbf{Q}} = \int dq'\, e^{-ipq'}|q'\rangle\langle q'|,
\end{aligned}
$$

чтобы преобразовать свое состояние $|\mathrm{Bob}\rangle$ в то, в какое ему нужно. Проверяя состояние Боба, мы видим, что он должен применить к нему $\mathbf{D}(-Q'-Q)$ и $\mathbf{D}(P-P')$. Однако выполнение этих сдвигов[1] оставляет состояние Боба с общей фазой $e^{iPQ'}$. Конечно, она не имеет физического значения,

[1] Именно в этом порядке, сначала $\mathbf{D}(-Q'-Q)$, а затем $\mathbf{D}(P-P')$. *Прим. ред.*

но если угодно, то можно избавиться и от нее, применяя операторы сдвига в специальном порядке. Сначала заметим, что

$$\begin{aligned}\mathbf{D}(p)\mathbf{D}(q) &= \int dq''\,dq'\,e^{-ipq''}|q''\rangle\langle q''|q'+q\rangle\langle q'| = \\ &= \int dq'\,e^{-ipq'}e^{-ipq}|q'+q\rangle\langle q'| = \\ &= e^{-ipq}\int dq'\,dq''\,e^{-ipq''}|q'+q\rangle\langle q'|q''\rangle\langle q''| = \\ &= e^{-ipq}\mathbf{D}(q)\mathbf{D}(p).\end{aligned}$$

Используя этот результат, мы видим, что применение к состоянию Боба $|\mathrm{Bob}\rangle$ оператора

$$\begin{aligned}U &= \mathbf{D}(-P')\mathbf{D}(-Q')\mathbf{D}(P)\mathbf{D}(-Q) = \\ &= e^{-iPQ'}\mathbf{D}(-P')\mathbf{D}(P)\mathbf{D}(-Q')\mathbf{D}(-Q) = \\ &= e^{-iPQ'}\mathbf{D}(P-P')\mathbf{D}(-Q'-Q)\end{aligned}$$

восстанавливает состояние $|\psi\rangle$:

$$\begin{aligned}U|\mathrm{Bob}\rangle &= \int dq\,{}_C\langle q|\psi\rangle_C\,e^{iPQ'+i(P-P')q}e^{-iPQ'}\times \\ &\quad\times\mathbf{D}(P-P')\mathbf{D}(-Q'-Q)|q+Q'+Q\rangle_B = \\ &= \int dq\,{}_C\langle q|\psi\rangle_C\,e^{i(P-P')q}\mathbf{D}(P-P')|q\rangle_B = \\ &= \int dq\,{}_C\langle q|\psi\rangle_C\,e^{i(P-P')q}e^{-i(P-P')q}|q\rangle_B = \\ &= \int dq\,{}_C\langle q|\psi\rangle_C|q\rangle_B = \\ &= |\psi\rangle_B.\end{aligned}$$

Итак, протокол, которому должны следовать Алиса и Боб для телепортации с помощью непрерывных переменных, выглядит следующим образом:

1) Готовится запутанное состояние $|Q,P\rangle_{AC}$.

2) Алиса измеряет (Q',P') в запутанном базисе системы AC.

3) Алиса посылает Бобу результаты своего измерения (Q', P').

4) Боб применяет оператор $\mathbf{D}(-P')\mathbf{D}(-Q')\mathbf{D}(P)\mathbf{D}(-Q)$ к своему состоянию. В итоге он имеет состояние $|\psi\rangle_B$.

4.4. Телепортация со смешанными состояниями

a) Мы знаем, что если Алиса и Боб поделили синглет, то они могут осуществить телепортацию с идеальной точностью воспроизведения. Если вместо этого Алиса и Боб нечаянно разделили смешанное состояние, то выполняемое Алисой измерение Белла ничего не говорит об ее состоянии (следовательно, у нее нет классической информации, которую необходимо послать Бобу), а состояние Боба никак не коррелирует с состоянием Алисы. В этом случае лучшая стратегиея Боба состоит в угадывании, которое, как мы показали, имеет точность воспроизведения $1/2$. Так как данная в задаче матрица плотности может рассматриваться как *ансамбль* этих альтернатив, имеющих вероятности $(1-\lambda)$ и λ соответственно, то полная точность воспроизведения телепортации с помощью этого состояния равна

$$F = 1 \cdot (1-\lambda) + \frac{1}{2} \cdot \lambda = 1 - \frac{\lambda}{2}.$$

b) Эта точность воспроизведения больше, чем $2/3$, при $\lambda < 2/3$.

c) Очень похожие спин-спиновые корреляции рассматривались в задаче 2.5. Вырезая и склеивая ее фрагменты, я воспроизведу здесь (с небольшим изменением) решение. (Более детальное изложение смотрите в решении задачи 2.5).

$$\begin{aligned} p &= \mathrm{tr}_B\,\mathrm{tr}_A\left[\left(\frac{1}{2}\left(\mathbf{1}_A + \hat{n}\cdot\vec{\boldsymbol{\sigma}}_A\right)\otimes\frac{1}{2}\left(\mathbf{1}_B + \hat{m}\cdot\vec{\boldsymbol{\sigma}}_B\right)\right)\times\right. \\ &\qquad \left.\times\left(\frac{\lambda}{4}\mathbf{1}_{AB} + (1-\lambda)|\psi^-\rangle\langle\psi^-|\right)\right] = \\ &= \frac{\lambda}{16}\,\mathrm{tr}_B\,\mathrm{tr}_A\left[(\mathbf{1}_A + \hat{n}\cdot\vec{\boldsymbol{\sigma}}_A)\otimes(\mathbf{1}_B + \hat{m}\cdot\vec{\boldsymbol{\sigma}}_B)\right] + \\ &\qquad + \frac{1-\lambda}{4}\,\mathrm{tr}_B\,\mathrm{tr}_A\left[(\mathbf{1}_A + \hat{n}\cdot\vec{\boldsymbol{\sigma}}_A)\otimes(\mathbf{1}_B + \hat{m}\cdot\vec{\boldsymbol{\sigma}}_B)|\psi^-\rangle\langle\psi^-|\right] = \\ &= \frac{\lambda}{16}\,\mathrm{tr}_B\,\mathrm{tr}_A\left[\mathbf{1}_A\otimes\mathbf{1}_B\right] + \frac{1-\lambda}{4}\langle\psi^-|(\mathbf{1}_A + \hat{n}\cdot\vec{\boldsymbol{\sigma}}_A)\otimes(\mathbf{1}_B + \hat{m}\cdot\vec{\boldsymbol{\sigma}}_B)|\psi^-\rangle = \end{aligned}$$

$$= \frac{\lambda}{4} + \frac{1-\lambda}{4} + \frac{1-\lambda}{4}\langle\psi^-|\hat{n}\cdot\vec{\sigma}_A + \hat{m}\cdot\vec{\sigma}_B + \hat{n}\cdot\vec{\sigma}_A \otimes \hat{m}\cdot\vec{\sigma}_B|\psi^-\rangle =$$

$$= \frac{1}{4} + \frac{1-\lambda}{4}\Big[\hat{n}\cdot\langle\psi^-|\vec{\sigma}_A|\psi^-\rangle + \hat{m}\cdot\langle\psi^-|\vec{\sigma}_B|\psi^-\rangle +$$

$$+\langle\psi^-|\hat{n}\cdot\vec{\sigma}_A \otimes \hat{m}\cdot\vec{\sigma}_B|\psi^-\rangle\Big] =$$

$$= \frac{1}{4} + \frac{1-\lambda}{4}\langle\psi^-|\hat{n}\cdot\vec{\sigma}_A \otimes \hat{m}\cdot\vec{\sigma}_B|\psi^-\rangle =$$

$$= \frac{1}{4} - \frac{1-\lambda}{4}\cos\theta.$$

d) При $\lambda = 1/2$ вероятность того, что спины Алисы и Боба коррелированы, равна $p = \frac{1}{4} - \frac{1}{8}\hat{n}\cdot\hat{m}$. Очень естественным предположением относительно порождающего эту корреляцию распределения вероятностей скрытых переменных выглядят

$$f_A(\hat{\alpha}\cdot\hat{n}) = \frac{1}{2} + a(\hat{\alpha}\cdot\hat{n}),$$

$$f_B(\hat{\alpha}\cdot\hat{m}) = \frac{1}{2} + b(\hat{\alpha}\cdot\hat{m}).$$

Этот вид подсказывается взаимно-однозначным соответствием между проекторами на сфере Блоха и единичными векторами на S^2. Он автоматически порождает индивидуальные распределения наблюдаемых Алисы и Боба. Для того чтобы воспроизводить квантово-механические спин-спиновые корреляции между Алисой и Бобом, a и b должны удовлетворять условию

$$\int\limits_{\hat{\alpha}} f_A(\hat{\alpha}\cdot\hat{n}) f_B(\hat{\alpha}\cdot\hat{m}) = \frac{1}{4} + \frac{ab}{4\pi}\int(\hat{\alpha}\cdot\hat{n})(\hat{\alpha}\cdot\hat{m})d\Omega =$$

$$= \frac{1}{4} + \frac{ab}{4\pi}\left(\frac{4\pi}{3}\right)\hat{n}\cdot\hat{m} =$$

$$= \frac{1}{4} + \frac{1}{3}ab\cos\theta \Rightarrow$$

$$\Rightarrow ab = -\frac{3}{8}.$$

Для того чтобы f_A и f_B действительно были распределениями вероятностей (то есть принимали значения в $[0, 1]$), должны выполняться неравенства $|a| \leqslant 1/2$ и $|b| \leqslant 1/2$. Но, согласно неравенству Шварца, это означает,

что $|ab| \leqslant |a| \cdot |b| \leqslant 1/4 < 3/8$ (!). Таким образом, этой простой модели не достаточно — квантовые корреляции слишком сильны, чтобы моделироваться наивной теорией скрытых переменных.

Чтобы добиться сильных корреляций, рассмотрим *разрывные* функции распределения вероятностей

$$f_A(\hat{\alpha}\cdot\hat{n}) = \frac{1}{2} + a\,\mathrm{sign}(\hat{\alpha}\cdot\hat{n}),$$

$$f_B(\hat{\alpha}\cdot\hat{m}) = \frac{1}{2} + b(\hat{\alpha}\cdot\hat{n}).$$

Очевидно, что эта новая теория по-прежнему воспроизводит индивидуальные распределения Алисы и Боба с $\langle f_A\rangle = \langle f_B\rangle = \frac{1}{2}$. Чтобы вычислить их интеграл спин-спиновых корреляций, запишем $\hat{\alpha}$, $\hat{n}$ и $\hat{m}$ в конкретном базисе:

$$\begin{aligned}
\hat{\alpha} &= \hat{x}\cos\varphi\sin\theta + \hat{y}\sin\varphi\sin\theta + \hat{z}\cos\theta,\\
\hat{n} &= \hat{z},\\
\hat{m} &= \hat{x}\sin\psi + \hat{z}\cos\psi.
\end{aligned}$$

В этом базисе корреляционный интеграл имеет вид

$$\int\limits_{\hat{\alpha}} f_A(\hat{\alpha}\cdot\hat{n})f_B(\hat{\alpha}\cdot\hat{m}) = \frac{1}{4} + \frac{ab}{4\pi}\int(\hat{\alpha}\cdot\hat{m})\,\mathrm{sign}(\hat{\alpha}\cdot\hat{n})d\Omega =$$

$$= \frac{1}{4} + \frac{ab}{4\pi}\int\limits_0^{2\pi} d\varphi \int\limits_1^1 d(\cos\theta)\big(\cos\varphi\sin\theta\sin\psi + \cos\theta\cos\psi\big)\mathrm{sign}(\cos\theta) =$$

$$= \frac{1}{4} + \frac{ab}{2}\cos\psi\left[\int\limits_0^1 d(\cos\theta)\cos\theta - \int\limits_{-1}^0 d(\cos\theta)\cos\theta\right] =$$

$$= \frac{1}{4} + \frac{ab}{2}\cos\psi\left[\frac{1}{2} + \frac{1}{2}\right] = \frac{1}{4} + \frac{ab}{2}\cos\psi.$$

Это соответствует предсказанию квантовой механики при $ab = -1/4$, что выполняется, например, при $a = 1/2$, $b = -1/2$:

$$f_A(\hat{\alpha}\cdot\hat{n}) = \begin{cases} 1, & \hat{\alpha}\cdot\hat{n} \geqslant 0,\\ 0, & \hat{\alpha}\cdot\hat{n} < 0,\end{cases}$$

$$f_B(\hat{\alpha}\cdot\hat{m}) = \frac{1}{2}(1 - \hat{\alpha}\cdot\hat{m}).$$

4.5. Распределение квантовых ключей

а) Решение первой части этой задачи в целом совпадает с решением задачи следующей главы 5.2(b). Как там показано, ограничение собственных чисел оператора $\mathbf{F}_{DK}$ неотрицательными значениями накладывает верхнюю границу на возможные значения A. Я приведу здесь доказательство:

$$\begin{aligned}\mathbf{F}_{DK} &= \begin{pmatrix} 1-2A & 0 \\ 0 & 1-2A \end{pmatrix} \\ &+ A\begin{pmatrix} \cos^2\alpha & \cos\alpha\sin\alpha + \\ \cos\alpha\sin\alpha & \sin^2\alpha \end{pmatrix} + \\ &+ A\begin{pmatrix} \sin^2\alpha & \cos\alpha\sin\alpha \\ \cos\alpha\sin\alpha & \cos^2\alpha \end{pmatrix} = \\ &= \begin{pmatrix} 1-A & 2A\cos\alpha\sin\alpha \\ 2A\cos\alpha\sin\alpha & 1-A \end{pmatrix}.\end{aligned}$$

Характеристическое уравнение имеет вид:

$$\begin{aligned}0 &= \lambda^2 - \lambda\,\mathrm{tr}\,\mathbf{F}_{DK} + \det\mathbf{F}_{DK} = \\ &= \lambda^2 - 2(1-A)\lambda + (1-A)^2 - 4A^2\cos^2\alpha\sin^2\alpha \\ \lambda &= 1 - A \pm \sqrt{(1-A)^2 - (1-A)^2 + A^2\sin^2 2\alpha} = \\ &= 1 - A \pm A\sin 2\alpha.\end{aligned}$$

Из условия неотрицательности собственных чисел $\lambda \geqslant 0$ следует неравенство:

$$A \leqslant \frac{1}{1 \pm \sin 2\alpha}.$$

Поскольку $0 < \alpha < \pi/4$, ограничение положительности может быть переписано как

$$0 \leqslant A \leqslant \frac{1}{1 + \sin 2\alpha}.$$

Если Алиса делает равновероятный выбор из $\{|u\rangle, |v\rangle\}$, то матрица плотности Боба выглядит как $\boldsymbol{\rho} = \frac{1}{2}(|u\rangle\langle u| + |v\rangle\langle v|)$. Следовательно, вероятность получения результата DK:

$$\begin{aligned}p_{DK} &= \mathrm{tr}(\boldsymbol{\rho}\mathbf{F}_{DK}) = \\ &= \mathrm{tr}\left[\frac{1}{2}\begin{pmatrix} 1 & \sin 2\alpha \\ \sin 2\alpha & 1 \end{pmatrix}\begin{pmatrix} 1-A & A\sin 2\alpha \\ A\sin 2\alpha & 1-A \end{pmatrix}\right] =\end{aligned}$$

$$= 1 - A + A\sin^2 2\alpha =$$
$$= 1 + A(\sin^2 2\alpha - 1).$$

Для того чтобы минимизировать p_{DK}, мы должны выбрать *максимально возможное* значение A, а именно: $A = 1/(1 + \sin 2\alpha)$. Тогда вероятность того, что Боб не знает, что послала Алиса:

$$p_{DK} = 1 + \frac{\sin^2 2\alpha - 1}{1 + \sin 2\alpha} = \sin 2\alpha.$$

b) Наиболее естественный способ построения распределения квантовых ключей вокруг источника Алисы и ПОЗМ Боба представляет собой небольшую модификацию схемы BB84 с целью адаптировать ее к ПОЗМ. (См. раздел 4.2.2 в лекциях.) Алиса случайным образом готовит состояния, а Боб измеряет их с помощью своей ПОЗМ. Затем он открыто объявляет, как только узнает, что послала Алиса. Конечно, он не распространяется о том, *что* он открыл, а только о том, что это ему известно. При идентификации $|u\rangle \equiv 0$, $|v\rangle \equiv 1$, Алиса и Боб теперь имеют безопасно разделенную строку случайных битов, с помощью которой они могут выполнять шифрование (используя одноразовый протокол). Конечно, прежде чем ее использовать, им также будет необходимо провести коррекцию ошибок и секретное увеличение их строки, чтобы свести вероятность подслушивания к тому уровню, при котором они будут чувствовать себя комфортно. Однако эта «пост-обработка» их строки представляет именно то, что они должны были бы сделать, осуществляя стандартный протокол ортогональных состояний BB84.

c) Вмешательство Евы вызовет лишь ошибку, когда Ева перехватывает посланное Алисой $|u\rangle$ ($|v\rangle$), Бобу передается неправильное состояние $|v\rangle$ ($|u\rangle$). Для любого посланного Алисой сигнала это происходит с вероятностью $\sin^2\alpha$. [Эта симметрия имеет место благодаря тому, что для выполнения своего измерения Ева выбрала в качестве базиса векторы $\binom{1}{0}, \binom{0}{1}$, относительно которых $|u\rangle$ и $|v\rangle$ повернуты на один и тот же угол α по и против часовой стрелки соответственно.]

Имеется два способа описания влияния Евы на скорость появления ошибки, которые лишь слегка различаются в семантике, но дают различные численные результаты. Первым способом описания ее воздействия является:

> *пусть Боб имеет «убедительный» результат, вероятность того, что он отличается от посланного Алисой, равна*
>
> $$\sin^2\alpha.$$

Но поскольку нам известно, что Боб получает «убедительный» результат только с вероятностью $1 - \sin 2\alpha$, можно также сказать:

отнесенная к измеряемому Бобом состоянию вероятность того, что оно не может быть использовано в качестве правильного ключевого бита, равна

$$(1 - \sin 2\alpha) \sin^2 \alpha.$$

Оба этих ответа могут быть полезными. Первый описывает, что Ева испортила часть ключа. Второй описывает, сколько еще необходимо Бобу выполнить измерений, чтобы получить ключ той же длины, что и раньше. Если Алиса и Боб готовы пожертвовать некоторой частью своего ключа, чтобы обнаруживать любые гнусные делишки Евы, им следует выбрать α, максимизирующее последнее выражение, чтобы было как можно легче обнаруживать ее вмешательство. А именно им следует выбрать $\alpha = \pi/8$. Всякий раз, когда частота скорость ошибки их протокола будет превышать $(1 - \sin 2\alpha) \sin^2 \alpha$, они будут подозревать неладное.

Точный смысл поставленного в этой задаче вопроса состоит в рассмотрении влияний на убедительные результаты Боба. Следовательно, фактически первое выражение из приведенных выше следует представить как влияние Евы на протокол.

4.6. Минимальное возмущение

Алиса случайным образом (с равной вероятностью) готовит одно из двух возможных состояний: или $|\psi\rangle = \cos\alpha|0\rangle + \sin\alpha|1\rangle$, или $|\tilde{\psi}\rangle = \sin\alpha|0\rangle + \cos\alpha|1\rangle$. В части (d) упражнения 2.1 мы нашли, что оптимальная ПОЗМ, различающая эти два состояния, состоит из проекторов $|0\rangle\langle 0|$ и $|1\rangle\langle 1|$.

Пусть $\mathbf{M}_0 = |\phi_0\rangle\langle 0|$, а $\mathbf{M}_1 = |\phi_1\rangle\langle 1|$ с произвольными нормированными векторами $|\phi_0\rangle$ и $|\phi_1\rangle$. Это операторы измерения для реализации оптимальной ПОЗМ, различающей приготовленные Алисой состояния:

$$\mathbf{M}_0^\dagger \mathbf{M}_0 = |0\rangle\langle\phi_0|\phi_0\rangle\langle 0| = |0\rangle\langle 0|,$$
$$\mathbf{M}_1^\dagger \mathbf{M}_1 = |1\rangle\langle\phi_1|\phi_1\rangle\langle 1| = |1\rangle\langle 1|.$$

Если Ева выполняет это измерение до того как состояние достигнет Боба, то, в зависимости от того, посылала Алиса $|\psi\rangle$ или $|\tilde{\psi}\rangle$, он получит одно из состояний:

$$\boldsymbol{\rho}' = \sum_i \mathbf{M}_i |\psi\rangle\langle\psi| \mathbf{M}_i^\dagger = \cos^2\alpha |\phi_0\rangle\langle\phi_0| + \sin^2\alpha |\phi_1\rangle\langle\phi_1|,$$

$$\tilde{\boldsymbol{\rho}}' = \sum_i \mathbf{M}_i |\tilde{\psi}\rangle\langle\tilde{\psi}| \mathbf{M}_i^\dagger = \sin^2\alpha |\phi_0\rangle\langle\phi_0| + \cos^2\alpha |\phi_1\rangle\langle\phi_1|.$$

Ева хочет минимизировать «возмущение» $D=1-\frac{1}{2}(F+\tilde{F})$, чтобы максимизировать среднюю точность воспроизведения получаемого Бобом состояния.

а) Мы можем вычислить эти точности воспроизведения:

$$
\begin{aligned}
F &= \langle\psi|\boldsymbol{\rho}'|\psi\rangle = \\
&= \cos^2\alpha\langle\psi|\phi_0\rangle\langle\phi_0|\psi\rangle + \sin^2\alpha\langle\psi|\phi_1\rangle\langle\phi_1|\psi\rangle, \\
F &= \cos^2\alpha\langle\phi_0|\psi\rangle\langle\psi|\phi_0\rangle + \sin^2\alpha\langle\phi_1|\psi\rangle\langle\psi|\phi_1\rangle, \\
\tilde{F} &= \langle\psi|\tilde{\boldsymbol{\rho}}'|\psi\rangle = \\
&= \sin^2\alpha\langle\tilde{\psi}|\phi_0\rangle\langle\phi_0|\tilde{\psi}\rangle + \cos^2\alpha\langle\tilde{\psi}|\phi_1\rangle\langle\phi_1|\tilde{\psi}\rangle, \\
\tilde{F} &= \sin^2\alpha\langle\phi_0|\tilde{\psi}\rangle\langle\tilde{\psi}|\phi_0\rangle + \cos^2\alpha\langle\phi_1|\tilde{\psi}\rangle\langle\tilde{\psi}|\phi_1\rangle.
\end{aligned}
$$

Тогда, складывая их, получим

$$
\begin{aligned}
F+\tilde{F} &= \cos^2\alpha\langle\phi_0|\psi\rangle\langle\psi|\phi_0\rangle + \sin^2\alpha\langle\phi_1|\psi\rangle\langle\psi|\phi_1\rangle + \\
&\quad + \sin^2\alpha\langle\phi_0|\tilde{\psi}\rangle\langle\tilde{\psi}|\phi_0\rangle + \cos^2\alpha\langle\phi_1|\tilde{\psi}\rangle\langle\tilde{\psi}|\phi_1\rangle = \\
&= \left\langle\phi_0\left|\left[\cos^2\alpha|\psi\rangle\langle\psi| + \sin^2\alpha|\tilde{\psi}\rangle\langle\tilde{\psi}|\right]\right|\phi_0\right\rangle + \\
&\quad + \left\langle\phi_1\left|\left[\sin^2\alpha|\psi\rangle\langle\psi| + \cos^2\alpha|\tilde{\psi}\rangle\langle\tilde{\psi}|\right]\right|\phi_1\right\rangle \\
F+\tilde{F} &= \langle\phi_0|A|\phi_0\rangle + \langle\phi_1|B|\phi_1\rangle,
\end{aligned}
$$

где

$$
\begin{aligned}
A &= \cos^2\alpha\begin{pmatrix}\cos^2\alpha & \sin\alpha\cos\alpha\\ \sin\alpha\cos\alpha & \sin^2\alpha\end{pmatrix} + \sin^2\alpha\begin{pmatrix}\sin^2\alpha & \sin\alpha\cos\alpha\\ \sin\alpha\cos\alpha & \cos^2\alpha\end{pmatrix} = \\
&= \begin{pmatrix}(1-\sin^2\alpha)\cos^2\alpha & (1-\sin^2\alpha)\sin\alpha\cos\alpha\\ (1-\sin^2\alpha)\sin\alpha\cos\alpha & \sin^2\alpha\cos^2\alpha\end{pmatrix} + \\
&\quad + \begin{pmatrix}(1-\cos^2\alpha)\sin^2\alpha & \sin^3\alpha\cos\alpha\\ \sin^3\alpha\cos\alpha & \sin^2\alpha\cos^2\alpha\end{pmatrix}, \\
A &= \begin{pmatrix}1-2\sin^2\alpha\cos^2\alpha & \sin\alpha\cos\alpha\\ \sin\alpha\cos\alpha & 2\sin^2\alpha\cos^2\alpha\end{pmatrix}, \\
B &= \sin^2\alpha\begin{pmatrix}\cos^2\alpha & \sin\alpha\cos\alpha\\ \sin\alpha\cos\alpha & \sin^2\alpha\end{pmatrix} + \cos^2\alpha\begin{pmatrix}\sin^2\alpha & \sin\alpha\cos\alpha\\ \sin\alpha\cos\alpha & \cos^2\alpha\end{pmatrix} =
\end{aligned}
$$

$$= \begin{pmatrix} \sin^2\alpha\cos^2\alpha & (1-\cos^2\alpha)\sin\alpha\cos\alpha \\ (1-\cos^2\alpha)\sin\alpha\cos\alpha & (1-\cos^2\alpha)\sin^2\alpha \end{pmatrix} +$$

$$+ \begin{pmatrix} \sin^2\alpha\cos^2\alpha & \sin\alpha\cos^3\alpha \\ \sin\alpha\cos^3\alpha & (1-\cos^2\alpha)\cos^2\alpha \end{pmatrix},$$

$$B = \begin{pmatrix} 2\sin^2\alpha\cos^2\alpha & \sin\alpha\cos\alpha \\ \sin\alpha\cos\alpha & 1-2\sin^2\alpha\cos^2\alpha \end{pmatrix}.$$

b) Заметим, что $A^\dagger = A$, а $B^\dagger = B$ – эрмитовы матрицы, следовательно они могут быть диагонализованы. В части (d) упражнения 2.3 мы нашли, что собственные числа 2×2-матрицы можно выразить через их след и детерминант:

$$\lambda_i = \frac{1}{2}\left(\operatorname{tr} M \pm \sqrt{(\operatorname{tr} M)^2 - 4\det M}\right).$$

Заметим также, что $\operatorname{tr} A = \operatorname{tr} B = 1$, а $\det A = \det B$, так что эти матрицы имеют одинаковые (вещественные) собственные значения.

Пусть $\{\lambda_i\}$ и $\{|a_i\rangle\}$ – собственные значения и соответствующие им собственные векторы матрицы A. До тех пор пока A несингулярна (то есть $\det A \neq 0$), мы можем разлагать $|\phi_0\rangle = c_0|a_0\rangle + c_1|a_1\rangle$ в собственном базисе. Тогда мы можем вычислить

$$\langle\phi_0|A|\phi_0\rangle = \left(c_0^*\langle a_0| + c_1^*\langle a_1|\right)\sum_i |a_i\rangle\lambda_i\langle a_i|\left(c_0|a_0\rangle + c_1|a_1\rangle\right),$$

$$\langle\phi_0|A|\phi_0\rangle = \lambda_0|c_0|^2 + \lambda_1|c_1|^2.$$

Это просто взвешенная сумма собственных значений матрицы A. Без потери общности можно предположить, что $\lambda_0 > \lambda_1$. Тогда мы максимизируем выражение $\langle\phi_0|A|\phi_0\rangle$, выбирая $|\phi_0\rangle$ так, чтобы $|c_0| = 1$, а $|c_1| = 0$. Максимальное значение $\langle\phi_0|A|\phi_0\rangle$ просто равно максимальному собственному значению A.

Аналогично оптимальный выбор $|\phi_1\rangle$ сделает выражение $\langle\phi_1|B|\phi_1\rangle$ равным максимальному собственному значению B (которое совпадает с максимальным собственным значением A).

Из предыдущего следует, что $\lambda_{\max} = \frac{1}{2}\left(1 + \sqrt{1 - 4\det A}\right)$. Минимально возможное возмущение равно:

$$D_{\min} = 1 - \frac{1}{2}\left({}_{\text{opt}}\langle\phi_0|A|\phi_0\rangle_{\text{opt}} + {}_{\text{opt}}\langle\phi_1|B|\phi_1\rangle_{\text{opt}}\right) =$$

$$= 1 - \frac{1}{2}\left(\lambda_{\max} + \lambda_{\max}\right) = 1 - \lambda_{\max}$$

$$D_{\min} = \frac{1}{2}\left(1 - \sqrt{1 - 4\det A}\right).$$

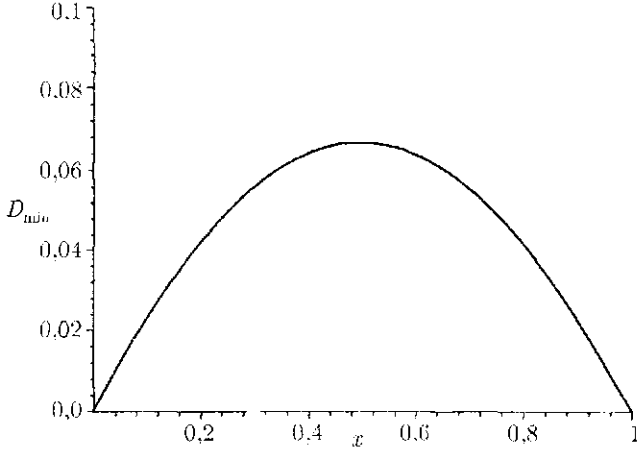
Мы можем переписать A через θ, определяемое соотношением $\cos\theta = \sin 2\alpha$:

$$A = \begin{pmatrix} 1 - \frac{1}{2}\sin^2 2\alpha & \frac{1}{2}\sin 2\alpha \\ \frac{1}{2}\sin 2\alpha & \frac{1}{2}\sin^2 2\alpha \end{pmatrix} = \begin{pmatrix} 1 - \frac{1}{2}\cos^2\theta & \frac{1}{2}\cos\theta \\ \frac{1}{2}\cos\theta & \frac{1}{2}\cos^2\theta \end{pmatrix}.$$

Тогда $\det A = \frac{1}{2}\cos^2\theta - \frac{1}{4}\cos^4\theta = \frac{1}{4}\cos^2\theta = \frac{1}{4}\left(\cos^2\theta - \cos^4\theta\right)$ и, следовательно,

$$D_{min} = \frac{1}{2}\left(1 - \sqrt{1 - \cos^2\theta + \cos^4\theta}\right).$$

c) Построим график функции $D_{\min}(x) = \frac{1}{2}\left(1 - \sqrt{1 - x + x^2}\right)$, где $x = \cos^2\theta$.



Если $\cos\theta = 1$, то начальные состояния $|\psi\rangle$ и $|\tilde{\psi}\rangle$ неразличимы. Тогда, независимо от того, выполняла Ева измерение или нет, Боб не может получить никакой информации о том, какое состояние приготовлено Алисой. Это означает, что он не может обнаружить вмешательство Евы, то есть вносимое ей возмущение неизмеримо.

Когда $\cos\theta = 0$, начальные состояния ортогональны, следовательно, Ева может выполнить оптимальную ПОЗМ в базисе $\{|0\rangle, |1\rangle\}$ и, не возмущая состояние, узнать, что приготовила Алиса. Если она пересылает его Бобу, то в этом случае измеримое возмущение отсутствует. Именно это препятствует использованию классических (ортогональных) состояний для безопасной связи — как Алисе и Бобу узнать, что их подслушивают?

Наибольшее значение $D_{\min}$ достигается при $x = \frac{1}{2}$, что соответствует $\theta = \arccos\frac{1}{\sqrt{2}} = \frac{\pi}{4}$. Это является фактическим выбором состояний схемы распределения квантовых ключей (такой как BB84), в которой Алиса и Боб хотят создать разделенную секретную строку битов, одновременно максимизируя величину возмущения, которое в среднем будет вносить подслушивающий, пытаясь узнать значения передаваемых битов. Позднее в этом курсе мы еще больше узнаем о квантовой криптографии.

Для этого выбора приготовлений мы можем вычислить

$$
\begin{aligned}
D_{\min}(x) &= \frac{1}{2} - \left(1 - \sqrt{1 - x + x^2}\right), \\
D_{\min}\left(x = \frac{1}{2}\right) &= \frac{1}{2} - \left(1 - \sqrt{1 - \frac{1}{2} + \frac{1}{4}}\right), \\
D_{\min}\left(x = \frac{1}{2}\right) &= \frac{1}{2} - \left(1 - \sqrt{\frac{3}{4}}\right), \\
D_{\min}\left(x = \frac{1}{2}\right) &\approx 0{,}067, \\
(p_{\text{error}})_{\text{optimal}} &= \frac{1}{2}(1 - \sin\theta), \\
(p_{\text{error}})_{\text{optimal}} &= \frac{1}{2}\left(1 - \frac{1}{\sqrt{2}}\right), \\
(p_{\text{error}})_{\text{optimal}} &\approx 0{,}146.
\end{aligned}
$$

4.7. Приближенное клонирование

а) Эта машина физически реализуема в том и только в том случае, когда она корректно сохраняет вероятности. Это требует, чтобы отображение было унитарным или антиунитарным, а из теоремы Вигнера следует, что на са-

мом деле оно должно быть унитарным. Унитарные отображения сохраняют не только вероятности, но и внутренние произведения. Следовательно, достаточно показать, что машина сохраняет внутреннее произведение, чтобы показать, что она физически реализуема.
До:

$$\begin{aligned}\langle 100|000\rangle &= 0,\\ \langle 000|000\rangle &= 1,\\ \langle 100|100\rangle &= 1.\end{aligned}$$

После:

$$\begin{aligned}\langle 100|\boldsymbol{U}^\dagger\boldsymbol{U}|000\rangle &= \left(\sqrt{\frac{2}{3}}\langle 111| + \sqrt{\frac{1}{3}}\langle\psi^+|\langle 0|\right)\\ &\quad\times\left(\sqrt{\frac{2}{3}}|000\rangle + \sqrt{\frac{1}{3}}|\psi^+\rangle|1\rangle\right)\\ &= 0,\\ \langle 000|\boldsymbol{U}^\dagger\boldsymbol{U}|000\rangle &= \frac{2}{3} + \frac{1}{3} = 1,\\ \langle 100|\boldsymbol{U}^\dagger\boldsymbol{U}|100\rangle &= \frac{2}{3} + \frac{1}{3} = 1.\end{aligned}$$

b) Переход от унитарного представления к представлению операторной суммы $ выполняется путем отождествления

$$\mathbf{M}_\mu = {}_{BC}\langle\mu|\boldsymbol{U}|\bar{0}\rangle_{BC},$$

где $|0\rangle_{BC}$ — некоторое фиксированное состояние. К данному в условии задачи описанию отображения естественно подходит выбор $|\bar{0}\rangle_{BC} = |00\rangle_{BC}$. В этом базисе необходимые нам существенные слагаемые $\boldsymbol{U}$ имеют вид

$$\begin{aligned}\boldsymbol{U} = &\sqrt{\frac{2}{3}}|000\rangle\langle 000| + \sqrt{\frac{1}{6}}|011\rangle\langle 000| + \sqrt{\frac{1}{6}}|101\rangle\langle 000| +\\ &+ \sqrt{\frac{2}{3}}|111\rangle\langle 100| + \sqrt{\frac{1}{6}}|010\rangle\langle 100| + \sqrt{\frac{1}{6}}|100\rangle\langle 100|.\end{aligned}$$

Следовательно, операторами представления операторной суммы являются:

$$\mathbf{M}_{00} = {}_{BC}\langle 00|\boldsymbol{U}|00\rangle_{BC} = \sqrt{\frac{2}{3}}|0\rangle\langle 0| + \sqrt{\frac{1}{6}}|1\rangle\langle 1|,$$

$$\mathbf{M}_{01} = {}_{BC}\langle 01|\boldsymbol{U}|00\rangle_{BC} = \sqrt{\frac{1}{6}}|1\rangle\langle 0|,$$

$$\mathbf{M}_{10} = {}_{BC}\langle 10|\boldsymbol{U}|00\rangle_{BC} = \sqrt{\frac{1}{6}}|0\rangle\langle 1|,$$

$$\mathbf{M}_{11} = {}_{BC}\langle 11|\boldsymbol{U}|00\rangle_{BC} = \sqrt{\frac{1}{6}}|0\rangle\langle 0| + \sqrt{\frac{2}{3}}|1\rangle\langle 1|.$$

c) Запись в виде суммы проекторов для матриц операторной суммы $\mathbf{M}_\mu$ позволяет быстро вычислить точность воспроизведения F даже без явного вычисления $\boldsymbol{\rho}'_A$:

$$F = \langle\psi|\boldsymbol{\rho}'_A|\psi\rangle = \left\langle \psi \left| \left(\sum_\mu \mathbf{M}_\mu|\psi\rangle\langle\psi|\mathbf{M}_\mu^\dagger \right) \right| \psi \right\rangle =$$

$$= \sum_\mu \langle\psi|\mathbf{M}_\mu|\psi\rangle\langle\psi|\mathbf{M}_\mu^\dagger|\psi\rangle = \sum_\mu \left|\langle\psi|\mathbf{M}_\mu|\psi\rangle\right|^2 =$$

$$= \left|\sqrt{\frac{2}{3}}|a|^2 + \sqrt{\frac{1}{6}}|b|^2\right|^2 + \frac{1}{3}|a|^2|b|^2 + \left|\sqrt{\frac{1}{6}}|a|^2 + \sqrt{\frac{2}{3}}|b|^2\right|^2 =$$

$$= \frac{5}{6}|a|^4 + \frac{5}{6}|b|^4 + \frac{5}{3}|a|^2|b|^2 = \frac{5}{6}\left(|a|^2 + |b|^2\right)^2 = \frac{5}{6}.$$

Этот результат означает, что, имея ресурс двух дополнительных вспомогательных кубитов, мы можем копировать неизвестный кубит с точностью воспроизведения $5/6$.

Действие этого «квантового ксерокса» на входящее состояние отображает его на состояние

$$\boldsymbol{\rho}'_A = \sum_\mu \mathbf{M}_\mu|\psi\rangle\langle\psi|\mathbf{M}_\mu^\dagger =$$

$$= \frac{1}{6}\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} |a|^2 & ab^* \\ a^*b & |b|^2 \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} +$$

$$+\frac{1}{6}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} |a|^2 & ab^* \\ a^*b & |b|^2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} +$$

$$
\begin{aligned}
&+\frac{1}{6}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} |a|^2 & ab^* \\ a^*b & |b|^2 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}+ \\
&+\frac{1}{6}\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} |a|^2 & ab^* \\ a^*b & |b|^2 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}= \\
&=\frac{1}{6}\begin{pmatrix} 4|a|^2 & 2ab^* \\ 2a^*b & |b|^2 \end{pmatrix}+\frac{1}{6}\begin{pmatrix} 0 & 0 \\ 0 & |a|^2 \end{pmatrix}= \\
&=\frac{1}{6}\begin{pmatrix} |b|^2 & 0 \\ 0 & 0 \end{pmatrix}+\frac{1}{6}\begin{pmatrix} |a|^2 & 2ab^* \\ 2a^*b & 4|b|^2 \end{pmatrix}= \\
&=\frac{1}{6}\begin{pmatrix} 5|a|^2+|b|^2 & 4ab^* \\ 4a^*b & |a|^2+5|b|^2 \end{pmatrix}= \\
&=\frac{1}{6}\begin{pmatrix} 4|a|^2 & 4ab^* \\ 4a^*b & 4|b|^2 \end{pmatrix}+\frac{1}{6}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}=\frac{2}{3}|\psi\rangle\langle\psi|+\frac{1}{6}\mathbf{1}.
\end{aligned}
$$

Этот квантовый ксерокс действует так же, как и деполяризующий канал с $p = 1/4$. Следовательно, в части (b) мы с полным основанием могли использовать операторы из раздела 3.4.1.

4.8. Прости нас, дядюшка Альберт

a) Пусть Σ_n обозначает оператор $(\boldsymbol{\sigma}_1 + i\boldsymbol{\sigma}_2)^{\otimes n} + (\boldsymbol{\sigma}_1 - i\boldsymbol{\sigma}_2)^{\otimes n}$. Из элементарной квантовой механики известно, что

$$\boldsymbol{\sigma}_\pm \equiv \frac{1}{2}(\boldsymbol{\sigma}_1 \pm i\boldsymbol{\sigma}_2)$$

являются повышающими и понижающими операторами для спина. Следовательно, действие $\boldsymbol{\Sigma}_n$ на $|\psi\rangle_n$ имеет вид:

$$
\begin{aligned}
\boldsymbol{\Sigma}_n|\psi\rangle_n &= \boldsymbol{\Sigma}_n\sqrt{\frac{1}{2}}\big(|000\ldots0\rangle + |111\ldots1\rangle\big) = \\
&= \sqrt{\frac{1}{2}}\Big[\big(2\boldsymbol{\sigma}_+\big)^{\otimes n}|000\ldots0\rangle + \big(2\boldsymbol{\sigma}_-\big)^{\otimes n}|111\ldots1\rangle\big)\Big] = \\
&= 2^n\cdot\sqrt{\frac{1}{2}}\big(|111\ldots1\rangle + |000\ldots0\rangle\big) = 2^n|\psi\rangle_n.
\end{aligned}
$$

b) Теория скрытых переменных утверждает, что $\boldsymbol{\sigma}_1$ и $\boldsymbol{\sigma}_2$ в любой момент времени являются функциями набора недоступных для нас «скрытых переменных». Она утверждает, что наша неспособность узнать эти переменные

заставляет все измерения σ_1 и σ_2 давать только *усредненные по ансамблю* этих скрытых переменных результаты.

Заметим, однако, что *модуль* оператора $(\sigma_1 \pm i\sigma_2)^{\otimes n}$ имеет только одно значение для любого возможного распределения значений наблюдаемых σ_1 и σ_2:

$$\left|(\sigma_1 \pm i\sigma_2)^{\otimes n}\right| = |(\pm 1) \pm i(\pm 1)|^n = 2^{n/2}.$$

c) Оператор $(\sigma_1 + i\sigma_2)^{\otimes n} + (\sigma_1 - i\sigma_2)^{\otimes n}$ эрмитов и, следовательно, его модуль является наблюдаемой величиной. Теория скрытых переменных предсказывает, что ее измеряемое значение дается усредненным по ансамблю определенных значений, принимаемых σ_1 и σ_2. Используя неравенство треугольника для нормы, мы можем ограничить этот модуль суммой выражений, вычисленных в части (b). Важность этого ограничения в том, что вычисленные в части (b) слагаемые *независимы* от любого такого распределения:

$$\begin{aligned} |\Sigma_n| &= \left|(\sigma_1 + i\sigma_2)^{\otimes n} + (\sigma_1 - i\sigma_2)^{\otimes n}\right| \leqslant \\ &\leqslant \left|(\sigma_1 + i\sigma_2)^{\otimes n}\right| + \left|(\sigma_1 - i\sigma_2)^{\otimes n}\right| = \\ &= |\sigma_1 + i\sigma_2|^n + |\sigma_1 - i\sigma_2|^n = |\sqrt{2}|^n + |\sqrt{2}|^n = 2^{n/2+1}. \end{aligned}$$

d) Эйнштейн сказал бы:

> *Sie haben demonstriert (wie auf der Hand gelegen haben sollte), daß mein Argument gegen Quanten Mechanik wissenschaftlich stichhaltig ist, weil es durch Experiment falsifizierbar ist. Für die Systeme, die $n > 2$ haben, sind die Voraussagungen der lokalen versteckten variablen Theorie und Quanten Mechanik offenbar inkompatibel. Lassen Sie uns ein Experiment machen, um zu überprüfen, daß ich Recht habe*[1]...

Под впечатлением экспериментального свидетельства, которое поддерживает квантовую механику и опровергает теорию скрытых переменных, Эйнштейн бы сказал:

> *Ach! Dieses ist wirklich mein größter Fehlgriff. Es scheint, daß Gott tatsächlich Würfel spielt*[2].

[1] Вы продемонстрировали (как это и должно было быть очевидно), что мои аргументы против квантовой механики научно обоснованы, пока они не опровергнуты экспериментально. Для системы из $n > 2$ частей предсказания локальной теории скрытых переменных и квантовой механики, очевидно, несовместимы. Давайте поставим эксперимент, чтобы убедиться в том, что я прав... .

[2] Ах! Это поистине моя самая большая ошибка. Похоже, что Бог действительно играет в кости.

4.9. Манипуляция запутыванием

а) Алиса может связать команды с помощью обмена запутыванием. Я опишу этот процесс на языке состояний и языке стабилизатора. Судите сами, какой язык покажется вам наиболее подходящим для этой задачи.

Язык состояний. Начальным состоянием системы является

$$
\begin{aligned}
|A_1Y, A_2P\rangle = \frac{1}{2}\big(&|00\rangle_A|\bar{0}\rangle_Y|\bar{0}\rangle_P + |11\rangle_A|\bar{1}\rangle_Y|1\rangle_P + \\
&+|01\rangle_A|\bar{0}\rangle_Y|\bar{1}\rangle_P + |10\rangle_A|\bar{1}\rangle_Y|\bar{0}\rangle_P\big) = \\
= \frac{1}{2\sqrt{2}}\Big[&|\Phi^+\rangle_A\big(|\bar{0}\rangle_Y|\bar{0}\rangle_P + |\bar{1}\rangle_Y|\bar{1}\rangle_P\big) + \\
&+|\Phi^-\rangle_A\big(|\bar{0}\rangle_Y|\bar{0}\rangle_P - |\bar{1}\rangle_Y|1\rangle_P\big) + \\
&+|\Psi^+\rangle_A\big(|\bar{0}\rangle_Y|1\rangle_P + |\bar{1}\rangle_Y|\bar{0}\rangle_P\big) + \\
&+|\Psi^-\rangle_A\big(|\bar{0}\rangle_Y|\bar{1}\rangle_P - |\bar{1}\rangle_Y|\bar{0}\rangle_P\big)\Big].
\end{aligned}
$$

Алиса измеряет два ее состояния в базисе Белла. Затем она посылает одной из команд два полученных ей классических бита. Тогда эта команда выполняет одну из следующих операций, гарантирующих, что получающееся в результате 50-кубитовое состояние является кот-состоянием

Состояние		Действие
$\|\Phi^+\rangle_A$	$\longrightarrow$	Ничего не делает.
$\|\Phi^-\rangle_A$	$\longrightarrow$	Один участник применяет σ_z.
$\|\Psi^+\rangle_A$	$\longrightarrow$	Все участники применяют σ_x.
$\|\Psi^-\rangle_A$	$\longrightarrow$	Все участники применяют σ_x Один участник применяет σ_z

Язык стабилизатора. Исходным стабилизатором системы является[1]

[1] Стабилизаторы — симплектические коды, корректирующие ошибки, рассматриваются в седьмой главе лекций, вошедшей во вторую часть этой книги. — *Прим. ред.*

Янки (25 кубитов)	Алиса	Святые отцы (25 кубитов)	Собственное значение
Z Z 1 ⋯ 1	1 1		+1
1 Z Z ⋯ 1	1 1		+1
⋮ ⋮ ⋮ ⋮	⋮ ⋮	1	⋮
1 1 1 ⋯ Z	Z 1		+1
X X X ⋯ X	X 1		+1
	1 Z	Z 1 1 ⋯ 1	+1
	1 1	Z Z 1 ⋯ 1	+1
1	⋮ ⋮	⋮ ⋮ ⋮ ⋮	⋮
	1 1	1 1 1 ⋯ Z	+1
	1 X	X X X ⋯ X	+1

Алиса измеряет **ZZ**, затем **XX**, получая собственные значения α_{par} и α_{ph}. После каждого измерения генераторы стабилизатора заменяются только на те генераторы, которые коммутируют с измерением. (Заметим, что произведение двух антикоммутирующих с измерением генераторов коммутирует с этим измерением.) Результирующим стабилизатором является (для ясности две колонки Алисы сдвинуты влево)

Алиса	Янки — Святые отцы	Собственное значение
Z Z	1	α_{par}
X X		α_{ph}
	Z Z 1 ⋯ ⋯ 1	+1
	1 Z Z ⋯ ⋯ 1	+1
	⋮ ⋮	⋮
1	1 ⋯ Z Z ⋯ 1	α_{par}
	⋮ ⋮	⋮
	1 1 1 ⋯ ⋯ Z	+1
	X X X ⋯ ⋯ X	α_{ph}

Для того чтобы команды разделили кот-состояние, Алиса должна сообщить одной из них собственные значения α_{par} и α_{ph}. После чего эта команда выполняет одну из следующих операций, гарантирующих, что получающийся в результате стабилизатор Янки и Святых Отцов имеет все собственные значения равные $+1$ (вспомним, что операция A переводит генератор стабилизатора $\mathbf{M}$ в $A\mathbf{M}A^{\dagger}$):

$(\alpha_{\text{par}}, \alpha_{\text{ph}})$		Действие
$(+1,+1)$	$\longrightarrow$	Ничего не делает.
$(+1,-1)$	$\longrightarrow$	Один участник применяет $\mathbf{Z}$.
$(-1,+1)$	$\longrightarrow$	Все участники применяют $\mathbf{X}$.
$(-1,-1)$	$\longrightarrow$	Все участники применяют $\mathbf{X}$ Один участник применяет $\mathbf{Z}$

b) (I) Если Алиса имеет вспомогательный кубит...

Имея вспомогательный кубит, Алиса может оставить команду в некотором смысле в том же положении, что и в части (a). Снова я опишу ее действия на языке состояний и языке стабилизатора.

Язык состояний. Алиса готовит свой вспомогательный кубит в состоянии

$$|A_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle).$$

Следовательно, начальным состоянием системы является

$$\begin{aligned}|A_1A_2Y\rangle = \frac{1}{2}\big(&|00\rangle_A|\bar{0}\rangle_Y + |11\rangle_A|\bar{1}\rangle_Y + \\ &+|01\rangle_A|\bar{0}\rangle_Y + |10\rangle_A|\bar{1}\rangle_Y\big) = \\ = \frac{1}{2\sqrt{2}}\Big[&|\Phi^+\rangle_A\big(|\bar{0}\rangle_Y + |\bar{1}\rangle_Y\big) + \\ &+|\Phi^-\rangle_A\big(|\bar{0}\rangle_Y - |\bar{1}\rangle_Y\big) + \\ &+|\Psi^+\rangle_A\big(|\bar{0}\rangle_Y + |\bar{1}\rangle_Y\big) - \\ &-|\Psi^-\rangle_A\big(|\bar{0}\rangle_Y - |\bar{1}\rangle_Y\big)\Big].\end{aligned}$$

Алиса измеряет два ее состояния в базисе Белла. (На самом деле ей нужно измерить только бит фазы.) Затем она посылает результат измерения оставшейся команде. Тогда эта команда выполняет одну из следующих

операций, гарантирующих, что получающееся в результате 24-кубитовое состояние является кот-состоянием:

Состояние		Действие
$\|\Phi^+\rangle_A, \|\Psi^+\rangle_A$	$\longrightarrow$	Ничего не делает.
$\|\Phi^-\rangle_A, \|\Psi^-\rangle_A$	$\longrightarrow$	Один участник применяет σ_z

Язык стабилизатора. Алиса готовит свой вспомогательный кубит в собственном состоянии $\mathbf{X} = +1$.[1] Начальным стабилизатором системы является

Алиса		Янки (24 кубита)			Собственное значение
X	**1**	**1**	$\cdots$	**1**	+1
1	**X**	**X**	$\cdots$	**X**	+1
1	**Z**	**Z**	$\cdots$	**1**	+1
1	**1**	**Z**	$\cdots$	1	+1
$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$
1	**1**	**1**	$\cdots$	**Z**	+1

Алиса измеряет **XX** на ее двух кубитах, получая собственное значение α. Новым стабилизатором является

Алиса		Янки (24)					Собственное значение
X	**X**						α
X	**1**			**1**			+1
		Z	**Z**	**1**	$\cdots$	**1**	+1
		1	**Z**	**Z**	$\cdots$	**1**	+1
1		$\vdots$	$\cdots$	$\vdots$		$\vdots$	−1
		1	**1**	**1**	$\cdots$	**Z**	+1
		X	**X**	**X**	$\cdots$	**X**	α

Алиса сообщает свое собственное значение α оставшейся команде, которая выполняет одну из следующих операций, гарантирующих, что полу-

[1] То есть в собственном состоянии оператора **X** с собственным значением +1. — *Прим. ред.*

чающийся в результате их стабилизатор имеет все собственные значения, равные $+1$:

α		Действие
$+1$	$\longrightarrow$	Ничего не делает.
-1	$\longrightarrow$	Один участник применяет $\mathbf{Z}$

(II) ..., а если она не имеет вспомогательного кубита.

Даже если Алиса не имеет вспомогательного кубита, прицеплявшегося выше, она по-прежнему может покинуть команду. Снова я опишу ее действия (на обоих языках).

Язык состояний. Начальным состоянием системы является

$$|AY\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|\bar{0}\rangle_Y + |1\rangle_A|\bar{1}\rangle_Y =$$

$$= \frac{1}{2}\Big[(|0\rangle_A + |1\rangle_A)(|\bar{0}\rangle_Y + |\bar{1}\rangle_Y) + (|0\rangle_A - |1\rangle_A)(|\bar{0}\rangle_Y - |\bar{1}\rangle_Y)\Big].$$

Алиса измеряет σ_x на своем спине и посылает результат оставшейся команде. Эта команда выполняет одну из следующих операций, гарантирующих, что получающееся в результате 24-кубитовое состояние является кот-состоянием:

Состояние		Действие
$\lvert\uparrow_x\rangle_A$	$\longrightarrow$	Ничего не делает.
$\lvert\downarrow_x\rangle_A$	$\longrightarrow$	Один участник применяет σ_z

Язык стабилизатора. Начальным стабилизатором системы является

Алиса	Янки (24 кубита)				Собственное значение
$\mathbf{X}$	$\mathbf{X}$	$\mathbf{X}$	$\cdots$	$\mathbf{X}$	$+1$
$\mathbf{Z}$	$\mathbf{Z}$	$\mathbf{1}$	$\cdots$	$\mathbf{1}$	$+1$
$\mathbf{1}$	$\mathbf{Z}$	$\mathbf{Z}$	$\cdots$	$\mathbf{1}$	$+1$
$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$
$\mathbf{1}$	$\mathbf{1}$	$\mathbf{1}$	$\cdots$	$\mathbf{Z}$	$+1$

Алиса измеряет $\mathbf{X}$ на своем кубите, получая собственное значение α. Новым стабилизатором является

Алиса	Янки (24)					Собственное значение
$\mathbf{X}$			$\mathbf{1}$			α
	$\mathbf{Z}$	$\mathbf{Z}$	$\mathbf{1}$	$\cdots$	$\mathbf{1}$	$+1$
	$\mathbf{1}$	$\mathbf{Z}$	$\mathbf{Z}$	$\cdots$	$\mathbf{1}$	$+1$
$\mathbf{1}$	$\vdots$	$\cdots$	$\vdots$		$\vdots$	$\vdots$
	$\mathbf{1}$	$\mathbf{1}$	$\mathbf{1}$	$\cdots$	$\mathbf{Z}$	$+1$
	$\mathbf{X}$	$\mathbf{X}$	$\mathbf{X}$	$\cdots$	$\mathbf{X}$	α

Алиса сообщает свое собственное значение α оставшейся команде, которая выполняет одну из следующих операций, гарантирующих, что получающийся в результате их стабилизатор имеет все собственные значения, равные $+1$:

α		Действие
$+1$	$\longrightarrow$	Ничего не делает
-1	$\longrightarrow$	Один участник применяет $\mathbf{Z}$

Решения упражнений к главе 5

5.1. Различимость неортогональных состояний

В отсутствие какой-либо предварительной информации, мы (как правоверные бейесиане) должны предположить, что с равной вероятностью Алиса готовит одно из состояний $|u\rangle$ и $|v\rangle$.

Пусть во всех частях этой задачи определены следующие случайные переменные:

$$A = \text{состояние, которое готовит Алиса,}$$

$$B = \text{результат, который получает Боб.}$$

Пусть для краткости B принимает значения $1, 2$ или 3, соответствующие применяемому Бобом имерительному оператору, а A принимает значения u и v, соответствующие приготавливаемым Алисой состояниям. В каждой части этой задачи мы должны вычислить следующие величины[1].

$$p(i|w) = \begin{cases} |\langle w|\mathbf{E}_i|w\rangle|^2 & \text{(ортогональное измерение)} \\ |\langle w|\mathbf{F}_i|w\rangle|^2 & \text{(ПОЗМ)} \end{cases},$$

[1] Конечно, учитывая связь $I(B;A) = I(A;B) = H(A) - H(A|B)$, вместо этого для вычислений можно выбрать $H(A|B)$ и $H(A)$.

$$H(B|A) = -\sum_{a,b} p(a,b)\log p(b|a) =$$

$$= -\sum_{a,b} p(b|a)p(a)\log p(b|a),$$

$$H(B) = -\sum_{a,b} p(a,b)\log p(b) =$$

$$= -\sum_{a,b} p(b|a)p(a)\log\left(\sum_{c} p(b|c)p(c)\right),$$

$$I(B;A) = H(B) - H(B|A).$$

а) Результатом исходной «фон неймановской» стратегии Боба является приобретение следующей информации.

Вероятности:

$$p(1|u) = 1, \quad p(2|u) = 0, \quad p(u) = \frac{1}{2},$$

$$p(1|v) = \cos^2\frac{\theta}{2}, \quad p(2|v) = \sin^2\frac{\theta}{2}, \quad p(v) = \frac{1}{2}.$$

Условная энтропия:

$$H(B|A) = -\frac{1}{2}\cos^2\frac{\theta}{2}\log\left(\cos^2\frac{\theta}{2}\right) - \frac{1}{2}\sin^2\frac{\theta}{2}\log\left(\sin^2\frac{\theta}{2}\right).$$

Энтропия Шеннона:

$$H(B) = -\frac{1}{2}\left(1+\cos^2\frac{\theta}{2}\right)\log\left[\frac{1}{2}\left(1+\cos^2\frac{\theta}{2}\right)\right] - \frac{1}{2}\sin^2\frac{\theta}{2}\log\left(\frac{1}{2}\sin^2\frac{\theta}{2}\right).$$

Взаимная информация:

$$I(B;A) = 1 - \frac{1}{2}\left(1+\cos^2\frac{\theta}{2}\right)\log\left(1+\cos^2\frac{\theta}{2}\right) + \frac{1}{2}\cos^2\frac{\theta}{2}\log\left(\cos^2\frac{\theta}{2}\right) =$$

$$= 1 - \frac{1}{2}\left(1+\cos^2\frac{\theta}{2}\right) H_2\left(\frac{1}{1+\cos^2\frac{\theta}{2}}\right),$$

где $H_2(x) = -x\log x - (1-x)\log(1-x)$ — бинарная функция энтропии.

b) Осуществляя более симметричное измерение ПОЗМ, Боб рассчитывает увеличить приобретение информации. Фактически мы находим, что, поступая так, он на самом деле *уменьшает* приобретение информации.

Вероятности:

$$p(1|u) = 0, \qquad p(2|v) = 0,$$
$$p(2|u) = A\sin^2\frac{\theta}{2}, \qquad p(1|v) = A\sin^2\frac{\theta}{2},$$
$$p(3|u) = 1 - A + A\cos^2\frac{\theta}{2}, \qquad p(3|v) = 1 - A + A\cos^2\frac{\theta}{2},$$
$$p(u) = \frac{1}{2}, \qquad p(v) = \frac{1}{2}.$$

Условная энтропия:

$$H(B|A) = -\left[A\sin^2\frac{\theta}{2}\log\left(A\sin^2\frac{\theta}{2}\right) + \right.$$
$$\left. + \left(1 - A + A\cos^2\frac{\theta}{2}\right)\log\left(1 - A + A\cos^2\frac{\theta}{2}\right)\right].$$

Энтропия Шеннона:

$$H(B) = -\left[A\sin^2\frac{\theta}{2}\log\left(\frac{1}{2}A\sin^2\frac{\theta}{2}\right) + \right.$$
$$\left. + \left(1 - A + A\cos^2\frac{\theta}{2}\right)\log\left(1 - A + A\cos^2\frac{\theta}{2}\right)\right].$$

Взаимная информация:

$$I(B;A) = -\left[A\sin^2\frac{\theta}{2}\log\frac{1}{2} + \left(1 - A + A\cos^2\frac{\theta}{2}\right)\log 1\right] =$$
$$= A\sin^2\frac{\theta}{2}.$$

Чтобы найти A, мы используем требование положительности $\mathbf{F}_3$, а именно $\mathbf{F}_3$ имеет положительные собственные значения:

$$\lambda^2 - \lambda\,\mathrm{tr}\,\mathbf{F}_3 + \det\mathbf{F}_3 = 0, \implies \lambda = 1 - A \pm A\cos\frac{\theta}{2},$$
$$\lambda \geqslant 0, \implies A \leqslant \frac{1}{1 \pm \cos\theta/2}.$$

При $\theta \in [0, \pi]$ таким наибольшим A, при котором оба собственных значения остаются положительными, является $A = \frac{1}{1+\cos\theta/2}$. Следовательно, максимальное приобретение информации равно

$$I(B;A) = 2\sin^2\frac{\theta}{4} = 1 - \cos\frac{\theta}{2}.$$

c) В последней отчаянной попытке Боб возвращается к измерению фон Неймана, которое «выявляет различие» между $|u\rangle$ и $|v\rangle$. Эта схема действительно оказывается наилучшей.

Вероятности:

$$p(1|u) = \cos^2\left(\frac{\theta+\pi}{4}\right), \qquad p(1|v) = \sin^2\left(\frac{\theta+\pi}{4}\right),$$

$$p(2|u) = \sin^2\left(\frac{\theta+\pi}{4}\right), \qquad p(2|v) = \cos^2\left(\frac{\theta+\pi}{4}\right),$$

$$p(u) = \frac{1}{2}, \qquad p(v) = \frac{1}{2}.$$

Условная энтропия:

$$H(B|A) = -\left[\sin^2\left(\frac{\theta+\pi}{4}\right)\log\left(\sin^2\left(\frac{\theta+\pi}{4}\right)\right) + \right.$$
$$\left. + \cos^2\left(\frac{\theta+\pi}{4}\right)\log\left(\cos^2\left(\frac{\theta+\pi}{4}\right)\right)\right].$$

Энтропия Шеннона:

$$H(B) = -\left[\frac{1}{2}\log\frac{1}{2} + \frac{1}{2}\log\frac{1}{2}\right] = 1.$$

Взаимная информация:

$$I(B;A) = 1 + \sin^2\left(\frac{\theta+\pi}{4}\right)\log\left(\sin^2\left(\frac{\theta+\pi}{4}\right)\right) +$$
$$+ \cos^2\left(\frac{\theta+\pi}{4}\right)\log\left(\cos^2\left(\frac{\theta+\pi}{4}\right)\right) =$$
$$= 1 - H_2\left(\cos^2\left(\frac{\theta+\pi}{4}\right)\right).$$

d) Несмотря на то что в условии задачи не было раздела **(d)**, в ее контексте полезно рассмотреть границу Холево, если, конечно, мы уверены в разумности результатов, полученных в предыдущих частях этой задачи.

Граница Холево утверждает, что приобретаемая Бобом информация ограничена сверху доступной информацией источника Алисы $\mathrm{Acc}(\mathcal{E}) = S(\rho) - \sum_x p_x S(\rho_x)$. Поскольку оба сигнальных состояния Алисы являются чистыми состояниями, доступная информация сводится к энтропии фон Неймана, которую мы можем вычислить путем диагонализации:

$$\rho = \begin{pmatrix} \frac{1}{2}\left(1+\cos^2\frac{\theta}{2}\right) & \frac{1}{2}\cos\frac{\theta}{2}\sin\frac{\theta}{2} \\ \frac{1}{2}\cos\frac{\theta}{2}\sin\frac{\theta}{2} & \frac{1}{2}\sin^2\frac{\theta}{2} \end{pmatrix},$$

$$\lambda^2 - \lambda + \frac{1}{4}\left[\left(1+\cos^2\frac{\theta}{2}\right)\sin^2\frac{\theta}{2} - \cos^2\frac{\theta}{2}\sin^2\frac{\theta}{2}\right] = 0,$$

$$\lambda = \frac{1}{2} \pm \frac{1}{2}\sqrt{1-\sin^2\frac{\theta}{2}} = \frac{1}{2} \pm \frac{1}{2}\cos\frac{\theta}{2} = \cos^2\frac{\theta}{4} \quad \text{или} \quad \sin^2\frac{\theta}{4}.$$

Таким образом, приобретаемая Бобом информация ограничена условием

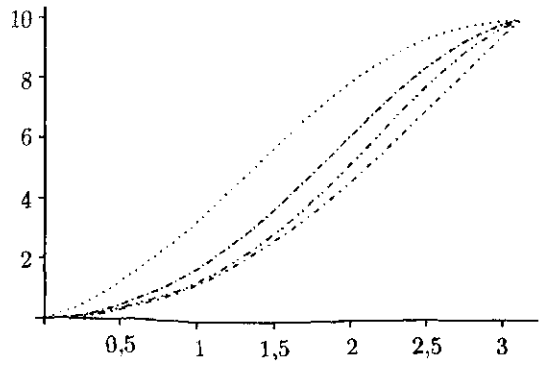
$$I(B;A) \leqslant \sin^2\frac{\theta}{4}\log\left(\sin^2\frac{\theta}{4}\right) - \cos^2\frac{\theta}{4}\log\left(\cos^2\frac{\theta}{4}\right) = H_2\left(\cos^2\frac{\theta}{4}\right).$$

Построив график приобретаемой Бобом информации, как функции для каждой из трех схем вместе с границей Холево, мы видим, что наилучшим выбором Боба является сратегия (c), несмотря на то, что граница Холево не насыщается. На диаграмме ниже стратегии a, b, c и h (для Холево) помечены соответствующими кодами азбуки Морзе[1]

5.2. Относительная энтропия

a) Эта задача содежит небольшую трудность, поскольку A и B не обязательно коммутируют между собой. Однако, работая с некоммутирующими объектами, мы можем применить обычный трюк и разлагать все выражения по компонентам обычных коммутирующих чисел. Пусть $\{|i\rangle\}$ является базисом, диагонализующим A, и пусть $\{|j\rangle\}$ – базис, диагонализующий B.

[1] Коды азбуки Морзе: a ↔ ·−; b ↔ −···; c ↔ −·−·; h ↔ ···· . – *Прим. перев.*



Разлагая по этим базисам, мы имеем

$$\begin{aligned}
\operatorname{tr}\left[f(\mathbf{B})-f(\mathbf{A})\right] &= \sum_i \langle i|f(\mathbf{B})-f(a_i)|i\rangle = \\
&= \sum_{i,j} \langle i|f(\mathbf{B})-f(a_i)|j\rangle\langle j|i\rangle = \\
&= \sum_{i,j} \langle i|f(b_j)-f(a_i)|j\rangle\langle j|i\rangle \leqslant \sum_{i,j} \langle i|(b_j-a_i)f'(a_i)|j\rangle\langle j|i\rangle = \\
&= \sum_i \langle i|(\mathbf{B}-a_i)f'(a_i)|i\rangle = \operatorname{tr}\left[(\mathbf{B}-\mathbf{A})f'(\mathbf{A})\right].
\end{aligned}$$

b) Этот результат, подобно многим неравенствам в теории информации, следует из неравенства $\ln x \leqslant x-1$. Достаточно показать, что $g(x) = -x\ln x$ является вогнутой функцией, следовательно, вогнутой является и функция $f(x) = g(x)/\ln 2$. Доказательство для $g(x)$:

$$\begin{aligned}
g(y)-g(x) &= -y\ln y + x\ln x = \\
&= y(\ln x - \ln y) + (x-y)\ln x = \\
&= y\ln\frac{x}{y} - (y-x)\ln x \leqslant \\
&\leqslant y\left(\frac{x}{y}-1\right) - (y-x)\ln x = \\
&= (y-x)(-1-\ln x) = \\
&= (y-x)g'(x);
\end{aligned}$$

$g(x)$ – вогнутая функция $\Longrightarrow$ $f(x)$ – вогнутая функция.

c) Применяя результаты **(a)** и **(b)**, находим, что относительная энтропия неотрицательна[1]:

$$\mathrm{tr}[-\rho\log\rho+\sigma\log\sigma]\leqslant \mathrm{tr}\left[(\rho-\sigma)\left(-\log\sigma-\frac{1}{\ln 2}\right)\right],$$

согласно частям **(a)** и **(b)**. Далее,

$$\begin{aligned}-\mathrm{tr}\,\rho\log\rho+\mathrm{tr}\,\sigma\log\sigma &\leqslant -\mathrm{tr}\,\rho\log\sigma+\mathrm{tr}\,\sigma\log\sigma,\\ -\mathrm{tr}\,\rho\log\rho &\leqslant -\mathrm{tr}\,\rho\log\sigma,\\ 0 &\leqslant \mathrm{tr}\,\rho\log\rho-\mathrm{tr}\,\rho\log\sigma,\\ 0 &\leqslant S(\rho|\sigma).\end{aligned}$$

d) Пусть σ — матрица плотности, совпадающая с единицей в подпространстве, являющемся носителем ρ. К искомому результату ведет выражение неотрицательности относительной энтропии между ρ и σ в базисе, в котором они обе диагональны:

$$\begin{aligned}0 &\leqslant S(\rho|\sigma)-S(\rho)-\mathrm{tr}\,\rho\log\sigma,\\ S(\rho) &\leqslant -\mathrm{tr}\left[\rho_1\log\sigma_1+\ldots+\rho_D\log\sigma_D\right]=\\ &= -\left(\log\frac{1}{D}\right)\mathrm{tr}(\rho_1+\ldots+\rho_D)=\log D.\end{aligned}$$

e) Используя неотрицательность относительной энтропии между ρ_{AB} и $\rho_A\otimes\rho_B$, находим

$$\begin{aligned}S(\rho_{AB}|\rho_A\otimes\rho_B) &= -S(\rho_{AB})-\mathrm{tr}\left[\rho_{AB}\log(\rho_A\otimes\rho_B)\right]\geqslant 0,\\ S(\rho_{AB}) &\leqslant -\mathrm{tr}\left[\rho_{AB}\left(\log\rho_A\otimes\mathbf{1}_B+\mathbf{1}_A\otimes\log\rho_B\right)\right]=\\ &= -\mathrm{tr}\,\rho_A\log\rho_A-\mathrm{tr}\,\rho_B\log\rho_B=S(\rho_A)+S(\rho_B).\end{aligned}$$

f) Рассмотрим матрицу плотности ρ_{AB} и ее частичные следы, данные соотношениями

$$\begin{aligned}\rho_{AB} &= \sum_i \lambda_i(\rho_i)_A\otimes(|e_i\rangle\langle e_i|)_B,\\ \rho_A &= \sum_i \lambda_i\rho_i,\\ \rho_B &= \sum_i \lambda_i|e_i\rangle\langle e_i|.\end{aligned}$$

[1]Формально, для того чтобы это доказательство было верным, нам нужно показать, что $f(x)$ является вогнутой при $x=0$. (ρ и σ могут иметь некоторые обращающиеся в нуль собственные значения.) Вы можете проверить самостоятельно, что при этом $f(x)$ остается вогнутой функцией.

Субаддитивность энтропии этой системы доказывает общую вогнутость $S(\boldsymbol{\rho})$:

$$S(\boldsymbol{\rho}_{AB}) \leqslant S(\boldsymbol{\rho}_A) + S(\boldsymbol{\rho}_B),$$

$$-\operatorname{tr}\left[\left(\sum_i \lambda_i (\boldsymbol{\rho}_i)_A \otimes (|e_i\rangle\langle e_i|)_B\right) \log\left(\sum_j \lambda_j (\boldsymbol{\rho}_j)_A \otimes (|e_j\rangle\langle e_j|)_B\right)\right] \leqslant$$

$$\leqslant S\left(\sum_i \lambda_i \boldsymbol{\rho}_i\right) - \operatorname{tr}\left[\sum_i \lambda_i |e_i\rangle\langle e_i| \log \sum_i \lambda_i |e_i\rangle\langle e_i|\right].$$

Если мы берем след по системе B в базисе $|e_i\rangle$, то сумма по j сводится к одному ее слагаемому с $i = j$. Упростим левую часть (LHS) этого неравенства:[1]

$$\begin{aligned}
\text{LHS} &= -\operatorname{tr}\left[\left(\sum_i \lambda_i \boldsymbol{\rho}_i \otimes |c_i\rangle\langle e_i|\right) \log\left(\lambda_i \boldsymbol{\rho}_i \otimes |e_i\rangle\langle e_i|\right)\right] = \\
&= -\operatorname{tr}\left[\left(\sum_i \lambda_i \boldsymbol{\rho}_i \otimes |e_i\rangle\langle e_i|\right)\left(\log \boldsymbol{\rho}_i \otimes \mathbf{1} + \mathbf{1} \otimes \log \lambda_i |e_i\rangle\langle e_i|\right)\right] = \\
&= -\operatorname{tr}\left[\sum_i \lambda_i \boldsymbol{\rho}_i \log \boldsymbol{\rho}_i \otimes |e_i\rangle\langle e_i|\right] - \\
&\quad -\operatorname{tr}\left[\sum_i \lambda_i \boldsymbol{\rho}_i \otimes |e_i\rangle\langle e_i| \log\left(\lambda_i |e_i\rangle\langle e_i|\right)\right] = \\
&= \sum_i \lambda_i S(\boldsymbol{\rho}_i) - \operatorname{tr} \boldsymbol{\rho}_i \left[\sum_i \lambda_i |e_i\rangle\langle e_i| \log\left(\lambda_i |e_i\rangle\langle e_i|\right)\right] = \\
&= \sum_i \lambda_i S(\boldsymbol{\rho}_i) - \sum_i \lambda_i \log \lambda_i.
\end{aligned}$$

[1] Здесь в ходе преобразований используется равенство

$$\begin{aligned}
\mathbf{P} \log \mathbf{P} &= \mathbf{P} \log(\mathbf{1} - \mathbf{Q}) = -\mathbf{P}\left(\mathbf{Q} + \tfrac{1}{2}\mathbf{Q}^2 + \tfrac{1}{3}\mathbf{Q}^3 + \ldots\right) \\
&= -\mathbf{P}\mathbf{Q}\left(1 + \tfrac{1}{2} + \tfrac{1}{3} + \ldots\right) = 0,
\end{aligned}$$

где $\mathbf{P} = |e\rangle\langle e|$, $\mathbf{Q} = \mathbf{1} - \mathbf{P}$ – проекторы на взаимно ортогональные подпространства. – *Прим. ред.*

Подставляя этот результат обратно в неравенство субаддитивности, мы получим условие вогнутости:

$$\sum_i \lambda_i S(\rho_i) - \sum_i \lambda_i \log \lambda_i \leqslant S\left(\sum_i \lambda_i \rho_i\right) - \sum_i \lambda_i \log \lambda_i,$$

$$\sum_i \lambda_i S(\rho_i) \leqslant S\left(\sum_i \lambda_i \rho_i\right).$$

5.3. Монотонность Линдблада — Ульмана

Используя некоторые разработанные в задаче 5.2 приемы, мы находим, что свойство монотонности позволяет вывести некоторые очень полезные результаты.

a) Применяя свойство монотонности к состоящей из трех частей системе, получим свойство строгой субаддитивности:

$$\begin{aligned}
S(\rho_{AB}|\rho_A \otimes \rho_B) &\leqslant S(\rho_{ABC}|\rho_A \otimes \rho_{BC}),\\
-S(\rho_{AB}) - \operatorname{tr}\left[\rho_{AB}\log(\rho_A \otimes \rho_B)\right] &\leqslant -S(\rho_{ABC})\\
&\quad - \operatorname{tr}\left[\rho_{ABC}\log(\rho_A \otimes \rho_{BC})\right],\\
-S(\rho_{AB}) + S(\rho_A) + S(\rho_B) &\leqslant -S(\rho_{ABC}) + S(\rho_A) + S(\rho_{BC}),\\
-S(\rho_{AB}) + S(\rho_B) &\leqslant -S(\rho_{ABC}) + S(\rho_{BC}),\\
S(\rho_{ABC}) + S(\rho_B) &\leqslant S(\rho_{AB}) + S(\rho_{BC}).
\end{aligned}$$

b) Действие супероператора \$ на матрицу плотности ρ_A (σ_A) можно представить, как вычисление следа по окружению после приведения его в контакт с системой A и совместной с ρ_A (σ_A) унитарной эволюции:

$$\begin{aligned}
\rho_{AB} &= U\left(\rho_A \otimes (|e\rangle\langle e|)_B\right)U^{-1},\\
\sigma_{AB} &= U\left(\sigma_A \otimes (|e\rangle\langle e|)_B\right)U^{-1},\\
\$\rho_A &= \operatorname{tr}_B \rho_{AB},\\
\$\sigma_A &= \operatorname{tr}_B \sigma_{AB}.
\end{aligned}$$

Энтропия фон Неймана матрицы плотности инвариантна относительно унитарной эволюции или присоединения чистого состояния. Опуская для простоты индексы чистого состояния $|e\rangle$ и унитарной матрицы U, мы видим:

$$\begin{aligned}
S(\boldsymbol{\rho}_{AB}|\boldsymbol{\sigma}_{AB}) &= \operatorname{tr}\left[U(\boldsymbol{\rho}_A \otimes |e\rangle\langle e|)U^{-1} \log\left(U(\boldsymbol{\rho}_A \otimes |e\rangle\langle e|)U^{-1}\right)\right] - \\
&- \operatorname{tr}\left[U(\boldsymbol{\rho}_A \otimes |e\rangle\langle e|)U^{-1} \log\left(U(\boldsymbol{\sigma}_A \otimes |e\rangle\langle e|)U^{-1}\right)\right] = \\
&= \operatorname{tr}\left[U(\boldsymbol{\rho}_A \otimes |e\rangle\langle e|)U^{-1} U \log(\boldsymbol{\rho}_A \otimes |e\rangle\langle e|)U^{-1}\right] - \\
&- \operatorname{tr}\left[U(\boldsymbol{\rho}_A \otimes |e\rangle\langle e|)U^{-1} U \log(\boldsymbol{\sigma}_A \otimes |e\rangle\langle e|)U^{-1}\right] = \\
&= \operatorname{tr}\left[(\boldsymbol{\rho}_A \otimes |e\rangle\langle e|) \log(\boldsymbol{\rho}_A \otimes |e\rangle\langle e|)\right] - \\
&- \operatorname{tr}\left[(\boldsymbol{\rho}_A \otimes |e\rangle\langle e|) \log(\boldsymbol{\sigma}_A \otimes |e\rangle\langle e|)\right] = \\
&= \operatorname{tr}(\boldsymbol{\rho}_A \log \boldsymbol{\rho}_A) - \operatorname{tr}(\boldsymbol{\rho}_A \log \boldsymbol{\sigma}_A) = \\
&= S(\boldsymbol{\rho}_A|\boldsymbol{\sigma}_A).
\end{aligned}$$

Вместе с монотонностью Линдблада–Ульмана это дает искомый результат

$$S(\$\boldsymbol{\rho}_A|\$\boldsymbol{\sigma}_A \leqslant S(\boldsymbol{\rho}_{AB}|\boldsymbol{\sigma}_{AB}) \leqslant S(\boldsymbol{\rho}_A|\boldsymbol{\sigma}_A).$$

c) Рассмотрим матрицы плотности, определенные соотношениями

$$\begin{aligned}
\boldsymbol{\rho}_{AB} &= \sum_x p_x(\boldsymbol{\rho}_x)_A \otimes (|e_x\rangle\langle e_x|)_B, \\
\boldsymbol{\rho}_A &= \sum_x p_x \boldsymbol{\rho}_x, \\
\boldsymbol{\rho}_B &= \sum_x p_x |e_x\rangle\langle e_x|.
\end{aligned}$$

Относительная энтропия $S(\boldsymbol{\rho}_{AB}|\boldsymbol{\rho}_A \otimes \boldsymbol{\rho}_B)$ в точности совпадает с информацией Холево $\chi(\mathcal{E})$ (для краткости опущены индексы подсистем A и B):

$$\begin{aligned}
S(\boldsymbol{\rho}_{AB}|\boldsymbol{\rho}_A \otimes \boldsymbol{\rho}_B) = \operatorname{tr}&\left[\left(\sum_x p_x \boldsymbol{\rho}_x \otimes |e_x\rangle\langle e_x|\right) \log\left(\sum_y p_y \boldsymbol{\rho}_y \otimes |e_y\rangle\langle e_y|\right)\right] - \\
&- \operatorname{tr}\left[\left(\sum_x p_x \boldsymbol{\rho}_x \otimes |e_x\rangle\langle e_x|\right) \log\left(\sum_w p_w \boldsymbol{\rho}_w \otimes \sum_z p_z |e_z\rangle\langle e_z|\right)\right].
\end{aligned}$$

Так же как и в задаче 5.2 **(f)**, мы можем взять след по состояниям системы B в базисе $|e_x\rangle$, сводя суммы по y и z к одному слагаемому каждую:

$$\begin{aligned}
S(\boldsymbol{\rho}_{AB}|\boldsymbol{\rho}_A \otimes \boldsymbol{\rho}_B) = &- \operatorname{tr}\left[\sum_x p_x \boldsymbol{\rho}_x \log \boldsymbol{\rho}_x \otimes |e_x\rangle\langle e_x|\right] + \\
&+ \operatorname{tr}\left[\sum_x p_x \boldsymbol{\rho}_x \otimes |e_x\rangle\langle e_x| \log(p_x|e_x\rangle\langle e_x|)\right] - \\
&- \operatorname{tr}\left[\sum_x p_x \boldsymbol{\rho}_x \log\left(\sum_w p_w \boldsymbol{\rho}_w \otimes |e_x\rangle\langle e_x|\right)\right] - \\
&- \operatorname{tr}\left[\sum_x p_x \boldsymbol{\rho}_x \otimes \log\left(p_x|e_x\rangle\langle e_x|\right)\right] = \\
= &- \sum_x p_x S(\boldsymbol{\rho}_x) - \sum_x p_x \log p_x + \\
&+ S\left(\sum_x p_x \boldsymbol{\rho}_x\right) + \sum_x p_x \log p_x = \\
= &- \sum_x p_x S(\boldsymbol{\rho}_x) + S\left(\sum_x p_x \boldsymbol{\rho}_x\right) = \\
= &\, \chi(\mathcal{E}).
\end{aligned}$$

5.4. ПОЗМ Переса — Вутерса

a) Записанные в обозначениях Дирака сигнальные состояния Алисы имеют вид

$$\begin{aligned}
|\varphi_1\rangle &= |\uparrow\rangle, \\
|\varphi_2\rangle &= -\frac{1}{2}\left(|\uparrow\rangle - \sqrt{3}|\downarrow\rangle\right), \\
|\varphi_3\rangle &= -\frac{1}{2}\left(|\uparrow\rangle + \sqrt{3}|\downarrow\rangle\right).
\end{aligned}$$

Дираковские обозначения позволяют очень быстро выразить состояния $|\Phi_i\rangle = |\varphi_i\rangle|\varphi_i\rangle$ $(i = 1, 2, 3)$ в базисе Белла:

$$
\begin{aligned}
|\Phi_1\rangle &= |\uparrow\uparrow\rangle = \\
&= \frac{1}{\sqrt{2}}\Big(|\Phi^+\rangle + |\Phi^-\rangle\Big), \\
|\Phi_2\rangle &= \frac{1}{4}\Big(|\uparrow\rangle - \sqrt{3}|\downarrow\rangle\Big)\Big(|\uparrow\rangle - \sqrt{3}|\downarrow\rangle\Big) = \\
&= \frac{1}{4}\Big(|\uparrow\uparrow\rangle + 3|\downarrow\downarrow\rangle - \sqrt{3}(|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle)\Big) = \\
&= \frac{1}{4}\Big(2(|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle) - (|\uparrow\uparrow\rangle - |\downarrow\downarrow\rangle) - \sqrt{3}(|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle)\Big) = \\
&= \frac{1}{2\sqrt{2}}\Big(2|\Phi^+\rangle - |\Phi^-\rangle - \sqrt{3}|\Psi^+\rangle\Big), \\
|\Phi_3\rangle &= \frac{1}{4}\Big(|\uparrow\rangle + \sqrt{3}|\downarrow\rangle\Big)\Big(|\uparrow\rangle + \sqrt{3}|\downarrow\rangle\Big) = \\
&- \frac{1}{4}\Big(|\uparrow\uparrow\rangle + 3|\downarrow\downarrow\rangle + \sqrt{3}(|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle)\Big) = \\
&= \frac{1}{2\sqrt{2}}\Big(2|\Phi^+\rangle - |\Phi^-\rangle + \sqrt{3}|\Psi^+\rangle\Big),
\end{aligned}
$$

Матрица плотности, соответствующая приготовлению Алисы, представляет собой одну треть суммы проекторов

$$
|\Phi_1\rangle\langle\Phi_1| = \frac{1}{8}\begin{pmatrix} 4 & 4 & 0 & 0 \\ 4 & 4 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},
$$

$$
|\Phi_2\rangle\langle\Phi_2| = \frac{1}{8}\begin{pmatrix} 4 & -2 & -2\sqrt{3} & 0 \\ -2 & 1 & \sqrt{3} & 0 \\ -2\sqrt{3} & \sqrt{3} & 3 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},
$$

$$
|\Phi_3\rangle\langle\Phi_3| = \frac{1}{8}\begin{pmatrix} 4 & -2 & 2\sqrt{3} & 0 \\ -2 & 1 & -\sqrt{3} & 0 \\ 2\sqrt{3} & -\sqrt{3} & 3 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},
$$

$$
\boldsymbol{\rho} = \operatorname{diag}\Big(1/2, 1/4, 1/4, 0\Big).
$$

Возможно это удивительно, что матрица плотности диагональна в базисе Белла. Следовательно, энтропией фон Неймана этого источника является

$$S(\boldsymbol{\rho}) = -\frac{1}{2}\log\frac{1}{2} - 2\left(\frac{1}{4}\log\frac{1}{4}\right) = \frac{3}{2}.$$

b) «Достаточно хорошее измерение» (ДХИ), которым следует пользоваться Бобу, чтобы декодировать сигнал Алисы, представляет собой ПОЗМ, определяемую операторами $\mathbf{F}_i = \mathbf{G}^{-1/2}|\Phi_i\rangle\langle\Phi_i|\mathbf{G}^{-1/2}$, где $\mathbf{G} = 3\boldsymbol{\rho}$:

$$\mathbf{F}_1 = \frac{1}{3}\begin{pmatrix} 1 & \sqrt{2} & 0 & 0 \\ \sqrt{2} & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

$$\mathbf{F}_2 = \frac{1}{6}\begin{pmatrix} 2 & -\sqrt{2} & -\sqrt{6} & 0 \\ -\sqrt{2} & 1 & \sqrt{3} & 0 \\ -\sqrt{6} & \sqrt{3} & 3 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

$$\mathbf{F}_3 = \frac{1}{6}\begin{pmatrix} 2 & -\sqrt{2} & \sqrt{6} & 0 \\ -\sqrt{2} & 1 & -\sqrt{3} & 0 \\ \sqrt{6} & -\sqrt{3} & 3 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Оказывается, что эта ПОЗМ в действительности является *ортогональным* измерением, определяющими состояниями которого служат

$$|\Psi_1\rangle = \frac{1}{\sqrt{3}}\Big(|\Phi^+\rangle + \sqrt{2}|\Phi^-\rangle\Big),$$

$$|\Psi_2\rangle = \frac{1}{\sqrt{6}}\Big(\sqrt{2}|\Phi^+\rangle - |\Phi^-\rangle - \sqrt{3}|\Psi^+\rangle\Big),$$

$$|\Psi_3\rangle = \frac{1}{\sqrt{6}}\Big(\sqrt{2}|\Phi^+\rangle - |\Phi^-\rangle + \sqrt{3}|\Psi^+\rangle\Big),$$

$$|\Psi_4\rangle = |\Psi^-\rangle, \quad \text{(для полноты базиса)}.$$

c) Как и в задаче 5.1, чтобы вычислить взаимную информацию между приготовлением Алисы и измерением Боба, мы должны начать с вычисления

вероятностей. В общем случае они представляют собой

$$\begin{aligned} p\,(\text{Боб измеряет } |\Psi_b\rangle|, \text{Алиса готовит } |\Phi_a\rangle) &= \langle\Phi_a|\mathbf{F}_b|\Phi_a\rangle \\ &= \langle\Phi_a|\Psi_b\rangle\langle\Psi_b|\Phi_a\rangle \\ &= |\langle\Psi_b|\Phi_a\rangle|^2. \end{aligned}$$

Последовательно вычисляя их для каждых a и b, мы действительно найдем цитированный в лекциях результат:

$$\begin{aligned} p(a|a) &= \frac{1}{3}\left(1+\frac{1}{\sqrt{2}}\right)^2, \\ p(b|a) &= \frac{1}{6}\left(1-\frac{1}{\sqrt{2}}\right)^2, \qquad b \neq a. \end{aligned}$$

Поскольку каждая вероятность здесь сводится к одному из двух значений, то нетрудно вычислить приобретаемую Бобом информацию:

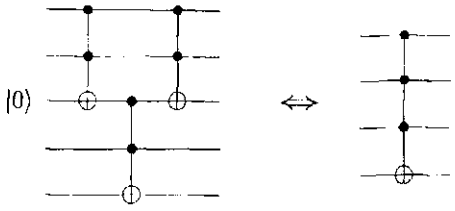
$$\begin{aligned} H(B) &= -[p(1|1)+2p(1|2)]\log\left[\frac{1}{3}\big(p(1|1)+2p(1|2)\big)\right] \\ &= -1\log\frac{1}{3} \approx 1{,}585 \\ H(B|A) &= -p(1|1)\log p(1|1) - 2p(1|2)\log p(1|2) \\ &= -\frac{1}{3}\left(1+\frac{1}{\sqrt{2}}\right)^2 \log\left[\frac{1}{3}\left(1+\frac{1}{\sqrt{2}}\right)^2\right] - \\ &\quad -\frac{1}{3}\left(1-\frac{1}{\sqrt{2}}\right)^2 \log\left[\frac{1}{3}\left(1-\frac{1}{\sqrt{2}}\right)^2\right] \\ &\approx 0{,}215893, \\ I(B;A) &\approx 1{,}36907. \end{aligned}$$

Решения упражнений к главе 6

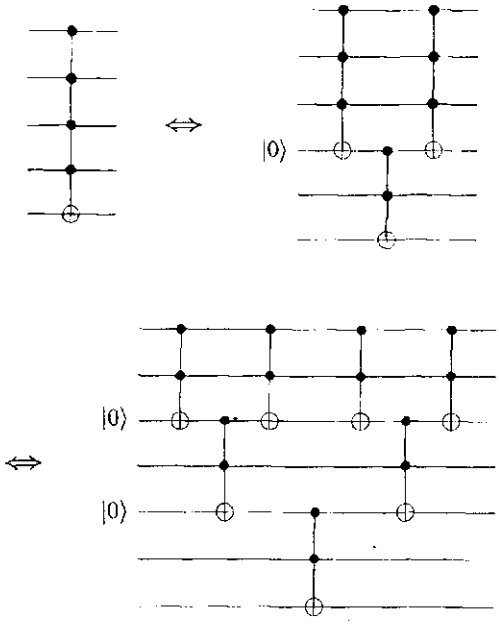
6.1. Линейное моделирование вентиля Тоффоли

а) Рассмотрим описанную в лекциях схему, которая выполняет $\theta^{(4)}$, используя только компоненты $\theta^{(3)}$ и один бит вспомогательного пространства,

первоначально полагаемый равным нулю

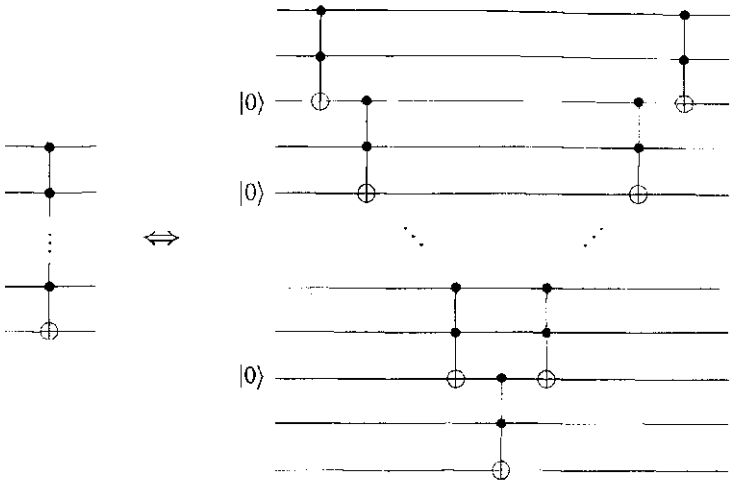


Используя конструкцию для вентиля $\theta^{(4)}$, мы можем рекурсивно построить вентиль $\theta^{(5)}$:



Заметим, что, благодаря тождеству $\left(\theta^{(3)}\right)^2 = \mathbf{1}$, два вентиля во внутренней части последней диаграммы необязательны. Продолжая рекурсивным образом эту процедуру, мы, очевидно, подобным образом можем исключить все внутренние вентили Тоффоли, получая в результате

конструкцию:



Поскольку каждой контрольной линии вентиля $\theta^{(n)}$, исключая линии 1, 2 и $2n-3$, сопоставлен вспомогательный бит, то для реализации этой схемы необходимо $n-3$ вспомогательных бита. Далее, поскольку каждый вспомогательный бит является целью двух вентилей $\theta^{(3)}$ (после вычисления необходимо восстановить исходное значение вспомогательного бита) и так как целевой бит вентиля $\theta^{(n)}$ в свою очередь также является целью вентиля $\theta^{(3)}$, то всего для этой конструкции необходимо $2(n-3)+1 = 2n-5$ вентилей $\theta^{(3)}$.

b) Описанный в **(a)** каскад вентилей Тоффоли отображает целевой бит y на

$$\begin{aligned} y \;\to\; & ((((s_1 \oplus x_1x_2)x_3 \oplus s_2)x_4 \oplus s_3 \ldots)x_{n-2} \oplus s_{n-3})x_{n-1} \oplus y \\ = \; & [s_1x_3x_4 \ldots x_{n-1} \oplus s_2x_4x_5 \ldots x_{n-1} \oplus \ldots \oplus s_{n-3}x_{n-1}] \\ & \oplus x_1 \ldots x_{n-1} \oplus y \\ = \; & [((((s_2 \oplus s_1x_3)x_4 \oplus s_3)x_5 \oplus s_4 \ldots)x_{n-2} \oplus s_{n-3})x_{n-1}] \\ & \oplus x_1 \ldots x_{n-1} \oplus y, \end{aligned}$$

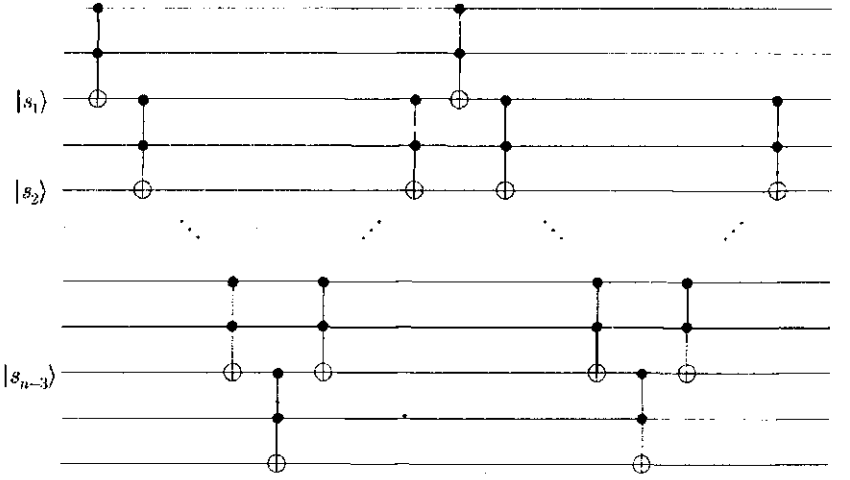
где s_i помечают вспомогательные биты, а x_i — контрольные линии.

Если все вспомогательные биты первоначально равны нулю, то заключенное в квадратные скобки слагаемое тождественно обращается в нуль.

Чтобы нейтрализовать влияние некоторых вспомогательных битов, не равных нулю в начальном состоянии, мы можем вычислить слагаемое в квадратных скобках $[\cdot]$ отдельно и подставить его XOR (то есть $[\cdot] \Rightarrow [\cdot] \oplus [\cdot]$) в окончательный результат

$$\begin{aligned} y \;&\to\; [\cdot] \oplus [\cdot] \oplus x_1 \ldots x_{n-1} \oplus y = \\ &= x_1 \ldots x_{n-1} \oplus y = \\ &= \theta^{(n)}(y, x_1 \ldots x_{n-1}). \end{aligned}$$

Конечно, мы должны быть внимательны к XOR в этом новом слагаемом *после* того, как восстановили значения вспомогательных битов. Наконец, как и в конструкции части **(а)**, нам нужно восстановить вспомогательные биты, на которые повлияла эта новая схема. Таким образом, модифицированный массив вентилей напоминает башни Бробдингнега[1]



Следовательно, количество вентилей в этом семействе схем равно $2n - 5 + 2(n-1) - 5 = 4n - 12$.

6.2. Набор универсальных квантовых вентилей

а) Используя указание, мы можем записать каждое из преобразований **A**, **B**, **C**, и **U** в виде произведений трех поворотов. Более того, нам известно,

[1]Бробдингнег – придуманная Джонатаном Свифтом фантастическая страна великанов, в которую попал Гулливер во время своего второго путешествия. – *Прим. перев.*

что сопряжение матрицей σ_x меняет знак угла матрицы поворота. Чтобы не переписывать всякий раз букву $\mathbf{R}$, я буду обозначать $\mathbf{R}_z(\psi)$ символом $\mathbf{Z}_\psi$, $\mathbf{R}_y(\theta)$ — символом $\mathbf{Y}_\theta$, а σ_x — символом $\mathbf{X}$. Принимая эти обозначения, можно записать

$$\begin{aligned}\mathbf{A} &= \mathbf{Z}_\alpha\mathbf{Y}_\beta\mathbf{Z}_\gamma,\\ \mathbf{B} &= \mathbf{Z}_\delta\mathbf{Y}_\varepsilon\mathbf{Z}_\varphi,\\ \mathbf{C} &= \mathbf{Z}_\lambda\mathbf{Y}_\mu\mathbf{Z}_\nu,\\ \mathbf{U} &= \mathbf{Z}_\psi\mathbf{Y}_\theta\mathbf{Z}_\phi.\end{aligned}$$

Подобно этому уравнения связи представляются в виде

$$\begin{aligned}\mathbf{1} &= \mathbf{Z}_\alpha\mathbf{Y}_\beta\mathbf{Z}_\gamma\mathbf{Z}_\delta\mathbf{Y}_\varepsilon\mathbf{Z}_\varphi\mathbf{Z}_\lambda\mathbf{Y}_\mu\mathbf{Z}_\nu =\\ &= \mathbf{Z}_\alpha\mathbf{Y}_\beta\mathbf{Z}_{\gamma+\delta}\mathbf{Y}_\varepsilon\mathbf{Z}_{\varphi+\lambda}\mathbf{Y}_\mu\mathbf{Z}_\nu,\\ \mathbf{Z}_\psi\mathbf{Y}_\theta\mathbf{Z}_\phi &= (\mathbf{Z}_\alpha\mathbf{Y}_\beta\mathbf{Z}_\gamma)\mathbf{X}(\mathbf{Z}_\delta\mathbf{X}\mathbf{X}\mathbf{Y}_\varepsilon\mathbf{X}\mathbf{X}\mathbf{Z}_\varphi)\mathbf{X}(\mathbf{Z}_\lambda\mathbf{Y}_\mu\mathbf{Z}_\nu) =\\ &= \mathbf{Z}_\alpha\mathbf{Y}_\beta\mathbf{Z}_{\gamma-\delta}\mathbf{Y}_{-\varepsilon}\mathbf{Z}_{-\varphi+\lambda}\mathbf{Y}_\mu\mathbf{Z}_\nu.\end{aligned}$$

С этого момента у нас два уравнения с девятью неизвестными. Найти решение будет большой удачей, не правда ли? Конечно, на самом деле это *матричные* уравнения, следовательно, имеется самое большее восемь уравнений, связывающих эти переменные, при условии, что ни одно из них не эквивалентно другому.

Тем не менее посмотрим, сможем ли мы найти решение для углов, не копаясь в матричных элементах. Непосредственно проверяется, что одно из решений первого уравнения связи возникает, если соседние матрицы определяют повороты на равные углы в противоположных друг другу направлениях, то есть когда углы удовлетворяют условиям

$$\begin{aligned}\varphi &= -\lambda, \qquad \varepsilon + \mu = -\beta,\\ \gamma &= -\delta, \qquad \alpha = -\nu.\end{aligned}$$

Этот выбор позволяет записать второе уравнение связи в виде

$$\mathbf{Z}_\alpha\mathbf{Y}_{-(\varepsilon+\mu)}\mathbf{Z}_{2\gamma}\mathbf{Y}_{-\varepsilon}\mathbf{Z}_{2\lambda}\mathbf{Y}_\mu\mathbf{Z}_{-\alpha} = \mathbf{Z}_\psi\mathbf{Y}_\theta\mathbf{Z}_\phi.$$

Выбор $\alpha = \psi$ согласует друг с другом последние повороты вокруг оси z в обеих частях этого равенства. Тогда $\mathbf{Z}_\phi$ согласуется при дополнительном выборе $\gamma = \mu = 0$:

$$\mathbf{Z}_\alpha\mathbf{Y}_{-2\varepsilon}\mathbf{Z}_{2\lambda-\alpha} = \mathbf{Z}_\psi\mathbf{Y}_\theta\mathbf{Z}_\phi.$$

Теперь мы имеем три уравнения с тремя неизвестными (прогресс!), которые имеют решение

$$\alpha = \psi,$$
$$\lambda - \frac{1}{2}(\phi + \psi),$$
$$\varepsilon = -\frac{\theta}{2}.$$

Подставляя их все вместе в матрицы $\mathbf{A}$, $\mathbf{B}$ и $\mathbf{C}$, мы находим, что они удовлетворяют условиям

$$\mathbf{A} = \mathbf{Z}_{\psi}\mathbf{Y}_{\theta/2},$$
$$\mathbf{B} = \mathbf{Y}_{-\theta/2}\mathbf{Z}_{-(\phi+\psi)/2},$$
$$\mathbf{C} = \mathbf{Z}_{(\phi-\psi)/2}$$

или в более общепринятых обозначениях:

$$\mathbf{A} = \mathbf{R}_z(\psi)\mathbf{R}_y(\theta/2),$$
$$\mathbf{B} = \mathbf{R}_y(-\theta/2)\mathbf{R}_z(-(\phi+\psi)/2),$$
$$\mathbf{C} = \mathbf{R}_z((\phi-\psi)/2).$$

b) Чтобы показать, что вентиль контролируемой фазы $\mathbf{P} = \operatorname{diag}(1, 1, e^{i\alpha}, e^{i\alpha})$ является однокубитовым вентилем, мы должны показать, что $\mathbf{P} = \mathbf{V} \otimes \mathbf{W}$ для унитарных матриц $\mathbf{V}$ и $\mathbf{W}$. Непосредственной проверкой можно убедиться в том, что $\mathbf{P}$ разлагается как $\mathbf{P} = \mathbf{Z}(\alpha) \otimes \mathbf{1}$, где $\mathbf{Z}(\alpha) \equiv \operatorname{diag}(1, e^{i\alpha})$.

Однако при более строгом подходе мы должны доказать следующее. Матрица $\mathbf{P}$ диагональна, и если она разлагается, то тоже на диагональные матрицы. Более того, поскольку $\{\{\mathbf{R}_z(\theta), \mathbf{1}\} | \theta \in [0, 2\pi]\}$ образует базис для диагональных матриц в $\mathrm{SU}(2)$, то в самом общем виде разложимая матрица $\mathbf{P}$ может быть записана в виде суммы четырех слагаемых:

$$\mathbf{P} = \lambda_1 \mathbf{1} \otimes \mathbf{1} + \lambda_2 \mathbf{1} \otimes \mathbf{R}_z(\theta) + \lambda_3 \mathbf{R}_z(\varphi) \otimes \mathbf{1} + \lambda_4 \mathbf{R}_z(\psi) \otimes \mathbf{R}_z(\chi),$$

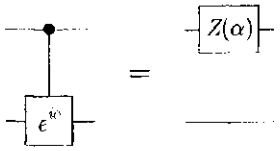
где $\lambda_i \in \mathbb{C}$ удовлетворяют условию $|\sum_i \lambda_i|^2 = 1$.

Так как $\mathbf{P}$ одинаково действует на состояния $|00\rangle$ и $|11\rangle$, то $\lambda_2 = \lambda_4 = 0$. Аналогично, так как $\mathbf{P}$ по разному действует на состояния $|00\rangle$ и $|01\rangle$, то $\lambda_1 = 0$. Следовательно, оставшийся коэффициент в наиболее общем случае представляет собой фазовый множитель $e^{i\eta}$. Таким образом,

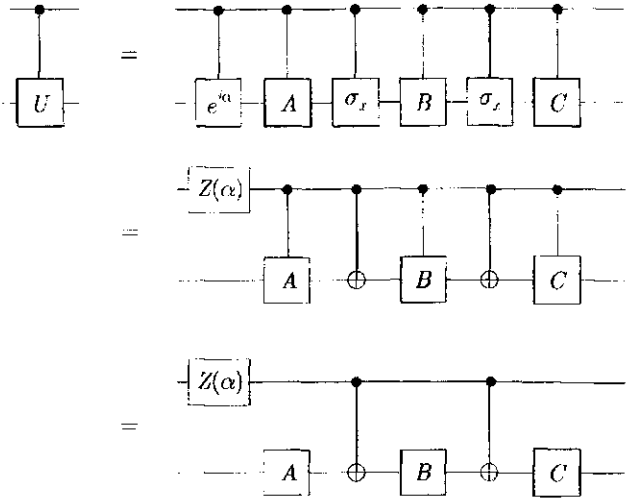
$$\mathbf{P} = e^{i\eta}\mathbf{R}_z(\varphi) \otimes \mathbf{1},$$
$$\operatorname{diag}(1, 1, e^{i\alpha}, e^{i\alpha}) = e^{i\eta}\operatorname{diag}(e^{i\varphi/2}, e^{i\varphi/2}, e^{-i\varphi/2}, e^{-i\varphi/2}),$$

что имеет решение $2\eta = -\varphi = \alpha$.

Следовательно, мы видим, что $\mathbf{P}$ действительно разложима, причем $\mathbf{P} = e^{i\alpha/2}\mathbf{R}_z(-\alpha) \otimes \mathbf{1}$. Общую фазу можно включить в состав другого сомножителя тензорного произведения, но, вероятно, самым естественным является упомянутый выше способ $\mathbf{P} = \mathbf{Z}(\alpha) \otimes 1$:



c) Произвольный элемент $SU(2)$ может быть записан как $\mathbf{A}\sigma_x\mathbf{B}\sigma_x\mathbf{C}$, где $\mathbf{A}$, $\mathbf{B}$ и $\mathbf{C}$ определены в части **(a)**. Следовательно, *произвольное* унитарное 2×2-преобразование $\mathbf{U} \in U(2)$ может быть записано как $\mathbf{U} = e^{i\alpha/2}\mathbf{A}\sigma_x\mathbf{B}\sigma_x\mathbf{C}$. Используя полученные в части **(a)** тождества, мы можем записать контролируемое $\mathbf{U}$ как последовательность однокубитовых вентилей и вентилей контролируемое NOT:



6.3. Точность

a) В этой задаче имеются некоторые трудности, поскольку на операторы не наложено никаких ограничений[1]. В частности, соотношения из условия

[1]Формально, для того чтобы нормы были определены, мы должны потребовать, чтобы $\mathbf{A}$ был компактным, а $\mathbf{B}$ – ограниченным. [Фактически приводимое ниже решение требует компактности обоих операторов, $\mathbf{A}$ и $\mathbf{B}$. – *Прим. ред.*]

задачи справедливы и для *недиагонализуемых* матриц, для которых мы не можем рассматривать $\|\mathbf{A}\|_{\mathrm{tr}}$ как сумму модулей собственных значений $\mathbf{A}$. Например, матрица

$$\mathbf{A} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

имеет $\|\mathbf{A}\|_{\mathrm{tr}} = 1$.

Тем не менее мы можем добиться успеха, покопавшись поглубже в закоулках нашей памяти и вспомнив *теорему о полярном разложении* из линейной алгебры, которая утверждает, что для любой матрицы $\mathbf{A}$ существует единственная унитарная матрица $\boldsymbol{U}$ такая, что

$$\begin{aligned} \mathbf{A} &= \mathbf{U}\sqrt{\mathbf{A}^\dagger\mathbf{A}}, \\ &= \mathbf{U}|\mathbf{A}|, \end{aligned}$$

где введено краткое обозначение $|\mathbf{A}|$ для $\sqrt{\mathbf{A}^\dagger\mathbf{A}}$. Это разложение полезно, поскольку по построению $|\mathbf{A}|$ является самосопряженной и, следовательно, диагонализуемой ортогональным базисом $\{|i\rangle\}$ с соответствующими собственными значениями (так называемые сингулярные числа матрицы $\mathbf{A}$) $|a_i|$. Используя это разложение, мы найдем:

$$\begin{aligned} |\operatorname{tr}\mathbf{A}| = |\operatorname{tr}\mathbf{U}|\mathbf{A}|| &= \left|\sum_i \langle i|\mathbf{U}|a_i||i\rangle\right| \leqslant \\ &\leqslant \sum_i \left|\langle i|\mathbf{U}|a_i||i\rangle\right| = \sum_i |a_i|\cdot|\langle i|\mathbf{U}|i\rangle| \leqslant \\ &\leqslant \sum_i |a_i| = \sum_i \langle i||\mathbf{A}||i\rangle = \operatorname{tr}|\mathbf{A}| = \|\mathbf{A}\|_{\mathrm{tr}}, \end{aligned}$$

где мы использовали тот факт, что унитарная матрица преобразует один ортогональный базис в другой, так что $|\langle i|\mathbf{U}|i\rangle| \leqslant 1$.

Другую часть этой задачи сложно проверить из-за порядка матриц $\mathbf{A}$ и $\mathbf{B}$ под знаком следовой нормы. Проще сначала показать, что $\|\mathbf{AB}\|_{\mathrm{tr}} \leqslant \|\mathbf{A}\|\cdot\|\mathbf{B}\|_{\mathrm{tr}}$, а затем обратиться к полярному разложению, чтобы получить искомое ограничение.

Вычисляя след в базисе, диагонализующем $\mathbf{B}^\dagger\mathbf{B}$ (то есть $\mathbf{B}^\dagger\mathbf{B} = \sum_i \lambda_i|i\rangle\langle i|$), мы находим

$$\begin{aligned} \|\mathbf{AB}\|_{\mathrm{tr}} &= \sum_i \langle i||\mathbf{AB}||i\rangle = \sum_i |\langle i||\mathbf{AB}||i\rangle| = \\ &= \sum_i \sqrt{|\langle i||\mathbf{AB}||i\rangle|^2} \leqslant \end{aligned}$$

$$\leqslant \sum_i \sqrt{\sum_j |\langle j||\mathbf{AB}||i\rangle|^2} = \sum_i \sqrt{\sum_j \langle i||\mathbf{AB}||j\rangle\langle j||\mathbf{AB}||i\rangle} =$$

$$= \sum_i \sqrt{\langle i||\mathbf{AB}|^2|i\rangle} = \sum_i \sqrt{\langle i|\mathbf{B}^\dagger\mathbf{A}^\dagger\mathbf{AB}|i\rangle} =$$

$$= \sum_i \sqrt{\frac{\langle i|\mathbf{B}^\dagger\mathbf{A}^\dagger\mathbf{AB}|i\rangle}{\langle i|\mathbf{B}^\dagger\mathbf{B}|i\rangle}\langle i|\mathbf{B}^\dagger\mathbf{B}|i\rangle} = \sum_i \frac{\|\mathbf{AB}|i\rangle\|}{\|\mathbf{B}|i\rangle\|}\sqrt{\langle i|\mathbf{B}^\dagger\mathbf{B}|i\rangle} \leqslant$$

$$\leqslant \sum_i \sup_{\mathbf{B}|i\rangle} \frac{\|\mathbf{AB}|i\rangle\|}{\|\mathbf{B}|i\rangle\|}\sqrt{\langle i|\mathbf{B}^\dagger\mathbf{B}|i\rangle} = \|\mathbf{A}\| \sum_i \sqrt{\langle i|\mathbf{B}^\dagger\mathbf{B}|i\rangle} =$$

$$= \|\mathbf{A}\| \sum_i \sqrt{\lambda_i} = \|\mathbf{A}\| \sum_i \langle i|\sqrt{\lambda_i}|i\rangle =$$

$$= \|\mathbf{A}\| \sum_i \langle i|\sqrt{\mathbf{B}^\dagger\mathbf{B}}|i\rangle = \|\mathbf{A}\| \cdot \|\mathbf{B}\|_{\mathrm{tr}}.$$

Как уже говорилось, это почти то, что требуется получить, но в неправильном порядке! Но мы можем привлечь полярное разложение, чтобы получить правильный порядок. Если положить $\mathbf{AB} = \mathbf{U}|\mathbf{AB}|$, то

$$\begin{aligned}\|\mathbf{AB}\|_{\mathrm{tr}} &= \mathrm{tr}\,|\mathbf{AB}| = \\ &= \mathrm{tr}(\mathbf{ABU}^{-1}) = \\ &= \mathrm{tr}(\mathbf{BU}^{-1}\mathbf{A}) = \\ &= \left|\mathrm{tr}(\mathbf{ABU}^{-1})\right|.\end{aligned}$$

Но согласно нашему первому результату

$$\left|\mathrm{tr}(\mathbf{ABU}^{-1})\right| \leqslant \|\mathbf{BU}^{-1}\mathbf{A}\|_{\mathrm{tr}},$$

а согласно второму —

$$\begin{aligned}\|\mathbf{BU}^{-1}\mathbf{A}\|_{\mathrm{tr}} &\leqslant \|\mathbf{BU}^{-1}\| \cdot \|\mathbf{A}\|_{\mathrm{tr}} = \\ &= \|\mathbf{B}\| \cdot \|\mathbf{A}\|_{\mathrm{tr}},\end{aligned}$$

то есть

$$\|\mathbf{AB}\|_{\mathrm{tr}} \leqslant \|\mathbf{B}\| \cdot \|\mathbf{A}\|_{\mathrm{tr}},$$

что и требовалось показать.

b) Этот результат вытекает из совершенных в части **(a)** подвигов Геракла

$$\begin{aligned}
\sum_a |P_a - \tilde{P}_a| &= \sum_a |\langle a|\boldsymbol{\rho}|a\rangle - \langle a|\tilde{\boldsymbol{\rho}}|a\rangle| = \sum_a |\langle a|\boldsymbol{\rho} - \tilde{\boldsymbol{\rho}}|a\rangle| - \\
&= \sum_a \langle a|\boldsymbol{\rho} - \tilde{\boldsymbol{\rho}}|a\rangle \operatorname{sign}\big[\langle a|\boldsymbol{\rho} - \tilde{\boldsymbol{\rho}}|a\rangle\big] = \\
&= \sum_a \operatorname{tr}\left[(\boldsymbol{\rho} - \tilde{\boldsymbol{\rho}})|a\rangle\langle a|\right] \operatorname{sign}\big[\langle a|\boldsymbol{\rho} - \tilde{\boldsymbol{\rho}}|a\rangle\big] = \\
&= \left|\sum_a \operatorname{tr}\left[(\boldsymbol{\rho} - \tilde{\boldsymbol{\rho}})|a\rangle\langle a|\right] \operatorname{sign}\big[\langle a|\boldsymbol{\rho} - \tilde{\boldsymbol{\rho}}|a\rangle\big]\right| = \\
&= \left|\operatorname{tr}\left[\sum_a (\boldsymbol{\rho} - \tilde{\boldsymbol{\rho}})|a\rangle\langle a| \operatorname{sign}\big[\langle a|\boldsymbol{\rho} - \tilde{\boldsymbol{\rho}}|a\rangle\big]\right]\right| \leqslant \\
&\leqslant \left\|\sum_a (\boldsymbol{\rho} - \tilde{\boldsymbol{\rho}}) \operatorname{sign}\big[\langle a|\boldsymbol{\rho} - \tilde{\boldsymbol{\rho}}|a\rangle\big] |a\rangle\langle a|\right\|_{\mathrm{tr}} = \\
&= \left\|(\boldsymbol{\rho} - \tilde{\boldsymbol{\rho}}) \sum_a \operatorname{sign}\big[\langle a|\boldsymbol{\rho} - \tilde{\boldsymbol{\rho}}|a\rangle\big] |a\rangle\langle a|\right\|_{\mathrm{tr}} \leqslant \\
&\leqslant \|\boldsymbol{\rho} - \tilde{\boldsymbol{\rho}}\|_{\mathrm{tr}} \cdot \left\|\sum_a \operatorname{sign}\big[\langle a|\boldsymbol{\rho} - \tilde{\boldsymbol{\rho}}|a\rangle\big] |a\rangle\langle a|\right\| \leqslant \\
&\leqslant \|\boldsymbol{\rho} - \tilde{\boldsymbol{\rho}}\|_{\mathrm{tr}}.
\end{aligned}$$

Здесь при переходе к последней строке мы воспользовались тем, что норма оператора, собственные значения которого равны ± 1, ограничена сверху единицей.

c) Без потери общности можно записать $|\tilde{\psi}\rangle = \alpha|\psi\rangle + \beta|\psi^{\perp}\rangle$, где $\alpha, \beta \in \mathbb{C}$ и удовлетворяют условию $|\alpha|^2 + |\beta|^2 = 1$. Выражая $\boldsymbol{\rho}$ и $\tilde{\boldsymbol{\rho}}$ в базисе $\{|\psi\rangle, |\psi^{\perp}\rangle\}$, получим

$$\begin{aligned}
\|\boldsymbol{\rho} - \tilde{\boldsymbol{\rho}}\|_{\mathrm{tr}} &= \operatorname{tr}\sqrt{(\boldsymbol{\rho} - \tilde{\boldsymbol{\rho}})^{\dagger}(\boldsymbol{\rho} - \tilde{\boldsymbol{\rho}})} = \\
&= \operatorname{tr}\sqrt{(\boldsymbol{\rho} - \tilde{\boldsymbol{\rho}})^2} = \\
&= \operatorname{tr}\sqrt{\begin{bmatrix} 1 - |\alpha|^2 & -\alpha\beta^* \\ -\alpha^*\beta & -|\beta|^2 \end{bmatrix}^2} =
\end{aligned}$$

$$= \operatorname{tr}\sqrt{\begin{bmatrix} |\beta|^2 & -\alpha\beta^* \\ -\alpha^*\beta & -|\beta|^2 \end{bmatrix}^2} =$$

$$= \operatorname{tr}\sqrt{\begin{bmatrix} |\beta|^4 + |\alpha|^2|\beta|^2 & 0 \\ 0 & |\beta|^4 + |\alpha|^2|\beta|^2 \end{bmatrix}} =$$

$$= \operatorname{tr}\sqrt{\begin{bmatrix} |\beta|^2 & 0 \\ 0 & |\beta|^2 \end{bmatrix}} =$$

$$= 2|\beta|.$$

Однако при $\beta \neq 0$ расстояние между состояниями $|\psi\rangle$ и $|\tilde{\psi}\rangle$

$$\begin{aligned} \| \, |\psi\rangle - |\tilde{\psi}\rangle \| &= \|(1-\alpha)|\psi\rangle - \beta|\psi^{\perp}\rangle\| = \\ &= \sqrt{|1-\alpha|^2 + |\beta|^2} = \\ &= |\beta|\sqrt{1 + \frac{|1-\alpha|^2}{|\beta|^2}} \geqslant |\beta|, \end{aligned}$$

Таким образом, если $\beta \neq 0$, то

$$\|\boldsymbol{\rho} - \tilde{\boldsymbol{\rho}}\|_{\mathrm{tr}} \leqslant 2\| \, |\psi\rangle - |\tilde{\psi}\rangle\|.$$

А поскольку при $\beta = 0$

$$\|\boldsymbol{\rho} - \tilde{\boldsymbol{\rho}}\|_{\mathrm{tr}} = 0 \leqslant 2\| \, |\psi\rangle - |\tilde{\psi}\rangle\|,$$

то, используя результат части **(b)**, мы находим, что

$$\sum_a |P_a - \tilde{P}_a| \leqslant \|\boldsymbol{\rho} - \tilde{\boldsymbol{\rho}}\|_{\mathrm{tr}} \leqslant 2\| \, |\psi\rangle - |\tilde{\psi}\rangle\|.$$

6.4. Поиск в базе данных в непрерывном времени

a) Поскольку гамильтониан $\mathbf{H}$ не зависит от времени, формальное интегрирование нестационарного уравнения Шредингера дает

$$|\psi(T)\rangle = e^{-i\mathbf{H}T}|\psi_0\rangle.$$

В рассматриваемом случае $|\psi_0\rangle = |s\rangle$.

Гамильтониан $\mathbf{H}$ ограничивает эволюцию подпространством $\{|\omega\rangle, |s\rangle\}$ с (ненормированным) базисом собственных состояний $\{|s\rangle + |\omega\rangle, |s\rangle - |\omega\rangle\}$

(Представьте, например, сферу Блоха, чтобы убедиться в этом.) Вычисляя собственные значения $\mathbf{H}$, находим

$$\begin{aligned}\mathbf{H}(|s\rangle \pm |\omega\rangle) &= E(|\omega\rangle\langle\omega| + |s\rangle\langle s|)(|s\rangle \pm |\omega\rangle) = \\ &= E\big[|\omega\rangle\langle\omega|(|s\rangle \pm |\omega\rangle) + |s\rangle\langle s|(|s\rangle \pm |\omega\rangle)\big] = \\ &= E\big[(|s\rangle \pm |\omega\rangle) \pm 2^{-n/2}(|s\rangle \pm |\omega\rangle)\big] = \\ &= E(1 \pm 2^{-n/2})(|s\rangle \pm |\omega\rangle),\end{aligned}$$

где мы подставили перекрытие $\langle s|\omega\rangle = 2^{-n/2}$.

Записывая $|s\rangle = \frac{1}{2}(|s\rangle + |\omega\rangle) + \frac{1}{2}(|s\rangle - |\omega\rangle)$, представим состояние системы в момент времени T в виде

$$\begin{aligned}|\psi(T)\rangle &= e^{-i\mathbf{H}T}|s\rangle = \\ &= \frac{1}{2}e^{-iET(1+2^{-n/2})}(|s\rangle + |\omega\rangle) + \frac{1}{2}e^{-iET(1-2^{-n/2})}(|s\rangle - |\omega\rangle) = \\ &= e^{-iET}\left[\cos\left(\frac{ET}{2^{n/2}}\right)|s\rangle - i\sin\left(\frac{ET}{2^{n/2}}\right)|\omega\rangle\right].\end{aligned}$$

Чтобы оптимизировать вероятность успешного определения $|\omega\rangle$, необходимо максимизировать вероятность $p = |\langle\omega|\psi(T)\rangle|^2$. Непосредственная проверка показывает, что значение $p = 1$ достигается, если фазы собственных векторов различаются на 180°:

$$\begin{aligned}e^{-iET(1+2^{-n/2})} &= -e^{-iET(1-2^{-n/2})}, \\ ET \cdot 2^{-n/2} &= -ET \cdot 2^{-n/2} + (2k+1)\pi, \\ T &= \frac{(2k+1)\pi}{2E}2^{n/2}.\end{aligned}$$

Очевидно, нам хотелось бы определить $|\omega\rangle$ как можно быстрее, поэтому выбирем $k = 0$ и получим границу Гровера:

$$T = \frac{\pi}{2E}2^{n/2}.$$

b) Можно получить весьма общую границу квадратичного ускорения поиска в базе данных в непрерывном времени, подобно тому, как это было сделано для поиска в базе данных в дискретном времени. Фактически мы увидим, что это, по существу, та же самая граница.

Допустим, что мы имеем алгоритм $\mathcal{A}$, который применяет гамильтониан $\mathbf{H} = \mathbf{H}_\omega + \mathbf{H}'(t)$ к состоянию $|\psi_0\rangle$ и спустя время T со стопроцентной надежностью определяет состояние $|\omega\rangle$. Так как $|\omega\rangle$ может принять любое из 2^n различных значений, гильбертово пространство, содержащее результат вычисления $|\psi_T\rangle$, должно иметь размерность как минимум 2^n. Более того, так как $\mathcal{A}$ должен быть способным *идеально* различать все альтернативы, множество

$$\{|\psi_T^a\rangle \mid |\psi_T^a\rangle \text{ представляет ответ } \mathcal{A}(|\psi_0\rangle) = a\}$$

должно образовывать ортогональный базис.

Теперь рассмотрим (скорее «плохой») алгоритм $\mathcal{D}$, который пытается определить $|\omega\rangle$, путем применения лишь гамильтониана $\mathbf{H} = \mathbf{H}'(t)$ к состоянию $|\psi_0\rangle$ в течение времени T. Так как мы неявно предполагаем, что $\mathbf{H}'(t)$ не имеет определенной зависимости от ω, кажется невероятным, что алгоритм $\mathcal{D}$ будет успешным. Но в то же самое время похоже, что в среднем[1] результат $|\psi_T^\omega\rangle$ алгоритма $\mathcal{A}$ должен отличаться от результата $|\varphi_T\rangle$ алгоритма $\mathcal{D}$ на величину, ограниченную некоторой функцией от T. («В течение ограниченного интервала времени оракул [гамильтониан] может только увести нас от нашей плохой догадки».)

Мы можем усилить наше подозрение, выполнив такой же анализ, что и в дискретном случае: разобьем $\mathcal{A}$ на отдельные шаги и определим границу того, как далеко от $|\varphi_t\rangle$ берется $|\psi_t^\omega\rangle$ на каждом шаге. (Но теперь шаги инфинитезимальны!)

Унитарные операторы, которые применяются алгоритмами $\mathcal{A}$ и $\mathcal{D}$ на каждом «шаге времени», представляют собой

$$\mathcal{A} : |\psi_t^\omega\rangle \to d\mathbf{U}_t|\psi_t^\omega\rangle,$$
$$\mathcal{D} : |\varphi_t\rangle \to d\mathbf{U}_t'|\varphi_t\rangle.$$

Действие $\mathcal{A}$ на «плохое» состояние $|\varphi_t\rangle$ в момент времени t имеет вид

$$d\mathbf{U}_t|\varphi_t\rangle = |\varphi_t\rangle + |E_t\rangle,$$

где

$$\begin{aligned}|E_t\rangle &= (d\mathbf{U}_t - d\mathbf{U}_t')|\varphi_t\rangle = \\ &= \big((\mathbf{1} - i\mathbf{H}dt) - (\mathbf{1} - i\mathbf{H}'dt)\big)|\varphi_t\rangle = \\ &= -i(\mathbf{H} - \mathbf{H}')|\varphi_t\rangle dt = \\ &= -iE|\omega\rangle\langle\omega|\varphi_t\rangle dt.\end{aligned}$$

[1] Среднее здесь представляет собой среднее *по ансамблю* всех возможных значений $|\omega\rangle$.

Как и в дискретном случае, спустя время T мы получаем непрерывный аналог уравнения (6.65) из лекций:

$$
\begin{aligned}
|\psi_T^\omega\rangle &= |\varphi_T\rangle + |E_T\rangle + d\mathbf{U}_T|E_{T-dt}\rangle + \ldots + d\mathbf{U}_T \ldots d\mathbf{U}_0|E_0\rangle = \\
&= |\varphi_T\rangle + e^{-i\mathbf{H}\cdot 0}|E_T\rangle + e^{-i\mathbf{H}dt}|E_{T-dt}\rangle + \ldots + e^{-i\mathbf{H}T}|E_0\rangle = \\
&= |\varphi_T\rangle + \int_0^T e^{-i\mathbf{H}t}|E_{T-t}\rangle dt = \\
&= |\varphi_T\rangle - iE\int_0^T e^{-i\mathbf{H}t}|\omega\rangle\langle\omega|\psi_{T-t}\rangle dt = \\
&= |\varphi_T\rangle - iE\int_0^T e^{-i\mathbf{H}(T-t)}|\omega\rangle\langle\omega|\psi_t\rangle dt = \\
&= |\varphi_T\rangle - iE\int_0^T e^{-i\mathbf{H}(T-t)}|\omega\rangle\langle\omega|e^{-i\mathbf{H}'t}|\psi_0\rangle dt.
\end{aligned}
$$

Вооруженные этим выражением, мы можем вывести границу для расстояния между $|\psi_T^\omega\rangle$ и $|\varphi_T\rangle$. (Аналог «зловещего» уравнения за номером (6.66) в лекциях[1].)

$$
\begin{aligned}
\| |\psi_T^\omega\rangle - |\varphi_T\rangle \| &= \left\| -iE\int_0^T e^{-i\mathbf{H}(T-t)}|\omega\rangle\langle\omega|\psi_t\rangle dt \right\| \leqslant \\
&\leqslant E\int_0^T \left\| e^{-i\mathbf{H}(T-t)}|\omega\rangle\langle\omega|\psi_t\rangle \right\| dt = \\
&= E\int_0^T \| |\omega\rangle\langle\omega|\psi_t\rangle \| dt = \\
&= E\int_0^T |\langle\omega|\psi_t\rangle| dt.
\end{aligned}
$$

[1] Подходящее для задания на пятницу 13-го, не правда ли?

Возводя это соотношение в квадрат, находим

$$\| |\psi_T^\omega\rangle - |\varphi_T\rangle\|^2 \leqslant E^2 \left(\int_0^T |\langle\omega|\psi_t\rangle| dt \right)^2 \leqslant$$

$$\leqslant E^2 T \int_0^T |\langle\omega|\psi_t\rangle|^2 dt.$$

Усредняя этот результат по всем возможным оракулам, мы находим, что, в подтверждение наших ранних подозрений, среднеквадратичное расстояние между конечными состояниями алгоритмов $\mathcal{A}$ и $\mathcal{D}$ ограничено сверху:

$$\left\langle (d(\mathcal{A}, \mathcal{D}))^2 \right\rangle = \frac{1}{2^n} \sum_\omega \| |\psi_T^\omega\rangle - |\varphi_T\rangle\|^2 \leqslant$$

$$\leqslant \frac{1}{2^n} E^2 T \sum_\omega \int_0^T \langle\psi_t|\omega\rangle\langle\omega|\psi_t\rangle dt =$$

$$= \frac{1}{2^n} E^2 T^2.$$

К счастью для нас, это среднеквадратичное расстояние также ограничено и снизу. Так как состояния $\{|\psi_T^\omega\rangle\}$ образуют ортогональный базис, они не могут все сколь угодно близко сконцентрироваться вокруг некоторого определенного фиксированного состояния. В частности, они не могут все сконцентрироваться вокруг $|\varphi_T\rangle$ и, следовательно, среднеквадратичное расстояние между конечными состояниями алгоритмов $\mathcal{A}$ и $\mathcal{D}$ ограничено снизу уравнением (6.159) из лекций:

$$\left\langle (d(\mathcal{A}, \mathcal{D}))^2 \right\rangle \geqslant \frac{1}{2^n} \left(2 \cdot 2^n - 2\sqrt{2^n}\right).$$

Сравнивая эти верхнюю и нижнюю границы, мы, как и было обещано, получаем квадратичную по времени границу гроверовского типа:

$$E^2 T^2 \geqslant 2 \cdot 2^n - 2\sqrt{2^n},$$

$$T \geqslant \frac{\sqrt{2}}{E} 2^{n/2} \sqrt{1 - 2^{-n/2}},$$

$$T \geqslant \frac{\sqrt{2}}{E} 2^{n/2}.$$

Поскольку $\sqrt{2} \approx 1{,}41$, а $\frac{\pi}{2} \approx 1{,}57$, эта общая граница сильнее текущего времени явного алгоритма из части **(а)** на

$$\frac{\pi/2 - \sqrt{2}}{\sqrt{2}} \approx 11\%.$$

Это то же различие, что и найденное нами в исходном (то есть дискретном) алгоритме Гровера. Поскольку в дискретном случае более тонкие границы демонстрировали насыщение алгоритма, у нас есть все основания ожидать, что и для непрерывного алгоритма подобное улучшение границы также будет демонстрировать оптимальность.

Прескилл Джон

Квантовая информация и квантовые вычисления

Том 1

Дизайнер М. Баженова
Технический редактор А. В. Широбоков
Компьютерная верстка Д. П. Вакуленко, А. В. Моторин
Корректор Г. Г. Тетерина

Подписано в печать 21.02.2008. Формат 60 × 84 1/16.
Печать офсетная. Усл. неч. л. 26,97. Уч. изд. л. 25,21.
Гарнитура Таймс. Бумага офсетная №1. Заказ №10.

Научно-издательский центр «Регулярная и хаотическая динамика»
426034, г. Ижевск, ул. Университетская, 1.
http://shop.rcd.ru E-mail: mail@rcd.ru Тел./факс: (+73412) 500–295

Переплет выполнен в ГУП УР «Ижевский полиграфический комбинат»
426039, г. Ижевск, Воткинское шоссе, 180.

Уважаемые читатели!

Интересующие Вас книги нашего издательства можно заказать через наш Интернет-магазин **http://shop.rcd.ru** или по электронной почте **subscribe@rcd.ru**

Книги можно приобрести в наших представительствах:

МОСКВА
Институт машиноведения им. А. А. Благонравова РАН
ул. Бардина, д. 4, корп. 3, к. 414, тел.: 135–54–37

ИЖЕВСК
Удмуртский государственный университет
ул. Университетская, д. 1, корп. 4, 2 эт., к. 211, тел./факс: (3412) 500 295

Также книги можно приобрести:

МОСКВА
Московский государственный университет им. М.В. Ломоносова
ГЗ (1 эт.), Физический ф-т (1 эт.), Гуманитарный ф-т (0 и 1 эт.),
Биологический ф-т (1 эт.).

Российский государственный университет нефти и газа им. И. М. Губкина
ГЗ (3–4 эт.), книжные киоски фирмы «Аргумент».

Магазины:

МОСКВА:	«Дом научно-технической книги» Ленинский пр., 40. тел.: 137-06-33
	«Московский дом книги» ул. Новый Арбат, 8. тел.: 290-45-07
	«Библиоглобус» м. «Лубянка», ул. Мясницкая, 6. тел.: 928–87 -44
ДОЛГОПРУДНЫЙ:	Книжный магазин «Физматкнига» новый корп. МФТИ, 1 эт. тел.: 409-93-28
САНКТ-ПЕТЕРБУРГ:	«Санкт-Петербургский дом книги» Невский проспект, 28
	Издательство СПбГУ, Магазин №1 Университетская набережная, 7/9

Дж. Прескилл — известный физик-теоретик, профессор теоретической физики Отделения Физики, Математики и Астрономии Калифорнийского Технологического Института (КАЛТЕХ). Область научных интересов — физика элементарных частиц и космология, топологические дефекты, непертурбативные методы квантовой теории поля, квантовые аспекты ранней Вселенной и черных дыр. В середине 90-х годов увлекся теорией квантовой информации, квантовых вычислений и кодирования. В настоящее время — один из ведущих специалистов в этой области. Руководитель Института Квантовых Вычислений, а также Центра Физики Информации при КАЛТЕХе.

ISBN 978-5-93972-651-1