Д.Баумеистер, А.Экерт, А.Цайлингер

ФИЗИКА КВАНТОВОЙ ИНФОРМАЦИИ

Москва: Постмаркет, 2002. - 376с.

Материал книги отражает новейшие достижения на новом, чрезвычайно актуальном направлении исследований, возникшем на стыке передовых областей науки - квантовой механики, оптики, лазерной физики, теории информации и программирования, дискретной математики.

Оглавление

Предметный указатель

Предисловие к русскому изданию

Предлагаемая русскоязычному читателю книга написана большим коллективом (44 человека) активных исследователей из европейских стран, работающих по программе Европейской Комиссии «Физика квантовой информации». Она посвящена новому и чрезвычайно актуальному направлению – исследованию фундаментальных квантовых свойств информации, возникшему на стыке едва ли не всех передовых областей современной физики – квантовой механики, квантовой оптики и оптики атомных пучков, взаимодействия излучения с веществом, а также теории информации и программирования, дискретной математики.

Значительный рост интереса ко всем этим вопросам в наше время вполне естественен и определяется внутренней логикой развития фундаментальной науки, как правило, опережающей прикладные исследования, но и особо стимулируемой нуждами тех из них, которые вышли на реальные применения, в большой мере определяющие развитие цивилизационных процессов в обществе, к которым, несомненно, относятся информатика, компьютеризация и коммуникация.

В книге рассматриваются как с теоретической, так и с экспериментальной точек зрения весь комплекс вопросов, связанных с этими проблемами – квантовые вычисления, квантовая криптография, перепутанные состояния и т.п. Изложенный материал отражает современный мировой уровень исследований в названной области. В ней реализована традиционная структура изданий, носящих обзорный характер по наиболее современным и актуальным темам. По существу, это набор лекций, связанных общей темой или проблемой и имеющих смешанный обзорно-оригинальный характер. Книги такого типа выпускались раньше целыми сериями и принесли очень большую пользу для ознакомления ученых с актуальными проблемами тех или иных областей знания. Как правило, уровень этих книг определяется высокой квалификацией авторов и в то же время является доступным не только специалистам, но и аспирантам и даже студентам старших курсов. Все сказанное в полной мере относится и к предлагаемой книге. Ее могут читать те, кто освоил базовые курсы физики, особенно квантовой механики.

Пониманию материала книги, изложенному с азов, способствует стройное логическое построение содержания, начинающегося с определения основных понятий – квантовой суперпозиции, кубитов и их преобразований, перепутывания и квантовой неразличимости, парадокса Эйнштейна-Подольского-Розена (ЭПР) и неравенств Белла. Далее с

теоретической и, что особенно важно, с экспериментальной точек зрения излагаются те проблемы, которые могут быть кардинальным образом развиты на принципиально новой – квантовой основе. Это – квантовая криптография, квантовое кодирование и квантовая телепортация. Особое значение может иметь применение результатов, полученных в соответствующих областях знания, при построении квантового компьютера и квантовых систем коммуникаций (в том числе и защищенных) на основе новых квантовых схем. На их основе, возможно, будут созданы новые методы обработки таких огромных объемов информации, которые принципиально недоступны существующим классическим методам.

Коллектив, подготовивший к изданию русскоязычный вариант книги, надеется, что ее появление закроет существенный пробел в отечественной научной литературе и позволит всем интересующимся этой захватывающей воображение областью получить стартовые знания.

На русском языке в последнее время стали появляться обзорные публикации, рассматривающие отдельные аспекты упомянутых проблем. Список некоторых из них приводится в конце предисловия. Недавно стало выходить в свет и периодическое издание «Квантовый компьютер» под редакцией академика В.А.Садовничего.

Особенно хотелось бы отметить содействие появлению русского издания со стороны издательства Шпрингер в лице г-жи Каролины Дэвис, редактора литературы по физике д-ра Келиха, а также редактора и одного из авторов английского издания проф. А.Цайлингера.

С.П.Кулик
Е.А.Шапиро
Т.А.Шмаонов

Дополнительная литература

1. Квантовый компьютер и квантовые вычисления. Ред. Журнала «Регулярная и хаотическая динамика», Ижевск 1999.

2. Ю.И.Ожигов. Квантовый компьютер и его возможности. М., МГТУ «Станкин». 1999.

3. К.А.Валиев и А.А.Кокин. Квантовые компьютеры: надежды и реальность. Редакция журнала «Регулярная и хаотическая динамика», Ижевск 2001, 352 с.

4. Б.Б.Кадомцев. Динамика и информация. М., Изд-во УФН, 2 изд.1999г., 400 с.

5. С.Я.Килин. Квантовая информация. УФН 168, 507 (1999).

6. М.Б.Менский. Квантовая механика: новые эксперименты, новые приложения и новые формулировки старых вопросов. УФН 170, №6, 631 (2000).

Предисловие к изданию на английском языке

Информация хранится, передаётся и обрабатывается с помощью физических средств. Значит, концепцию информации и вычисления можно сформулировать в контексте физической теории, а изучение информации, в конечном счете, требует проведения экспериментов. Это, безобидное на первый взгляд, предложение ведет к нетривиальным следствиям.

Согласно закону Мура, скорость микропроцессоров увеличивается вдвое примерно каждые 18 месяцев. Похоже, что единственный способ делать их существенно более быстрыми – это делать их меньше размером. В не слишком удаленном будущем они достигнут той отметки, когда логические элементы будут столь малы, что каждый из них будет состоять всего лишь из нескольких атомов. В этот момент станут важными квантовомеханические эффекты. Таким образом, если компьютеры должны становиться быстрее (а значит, меньше размером), то новая, квантовая технология должна заменить или дополнить то, что существует сейчас. Но оказывается, что такая технология может дать нам гораздо больше, чем просто более маленькие и быстрые микропроцессоры. Недавние теоретические результаты показали, что можно использовать квантовые эффекты, чтобы создать качественно новые пути вычислений и связи – в некоторых случаях гораздо более мощные, чем их классические аналоги.

Эта новая квантовая технология рождается сейчас во многих лабораториях. В последние два десятилетия были проведены эксперименты, в которых с небывалой точностью управляли и манипулировали единичными квантовыми частицами различных типов. Были реально проведены многие «мысленные» эксперименты, столь знаменитые в первые дни квантовой механики. Новые экспериментальные методики позволяют сейчас хранить и обрабатывать информацию, закодированную в индивидуальных квантовых системах. В результате у нас появилась новая область знаний - обработка квантовой информации, – которая представляет собой насыщенный сплав кванто-

вой физики с наукой об информации и компьютерах. Её охват простирается от установления новых взглядов на природу физических законов до изучения возможного коммерческого применения результатов в компьютерной и коммуникационной индустрии.

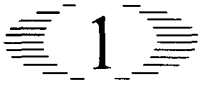
Часть этой работы, ведущейся по всему миру, поддерживается Европейской комиссией, в рамках программы TMR (Training and Mobility of Researchers), через поддержку исследовательской сети «Физика квантовой информации». Главы этой книги написаны, в основном, участниками этой сети в различных формах сотрудничества. Все они направлены на то, чтобы дать дидактическое введение в важные, новые области знания. Кроме того, в нескольких разделах представлены важные результаты, полученные исследователями, находящимися вне рамок программы TMR. Однако, мы не стремились написать монографию, дающую полный обзор науки о квантовой информации. Исследования в этой области ведутся очень активно, и любой всесторонний обзор очень быстро бы устарел. Эта книга охватывает такие вопросы, как теоретические и экспериментальные аспекты квантового перепутывания, квантовой криптографии, квантовой телепортации, квантовых вычислений, декогеренции квантовых состояний, исправления квантовых ошибок и квантовой коммуникации.

Мы надеемся, что наша книга станет полезным пособием для всех читателей, обладающих некоторыми познаниями в квантовой механике и испытывающих неподдельный интерес к удивительным возможностям, которые она нам предлагает.

Мы очень благодарны Томасу Дженневейну за многочисленные рисунки, нарисованные им для этой книги.

Оксфорд, Вена. Март 2000г.

Дик Боумейстер
Артур Экерт
Антон Цайлингер



Физика квантовой информации: основные понятия

Д. Боумейстер, А. Цайлингер

1.1 Квантовая суперпозиция

Принцип суперпозиции играет центральную роль во всех рассмотрениях квантовой информации, как и в большинстве мысленных экспериментов и парадоксов квантовой механики. Вместо того, чтобы изучать его теоретически или определять его абстрактно, мы обсудим здесь эксперимент, являющийся квинтэссенцией принципа квантовой суперпозиции – эксперимент с двумя щелями (Рис. 1.1). Согласно Фейнману [1], он «заключает в себе сердце квантовой механики». Необходимые составляющие этого эксперимента – это источник, диафрагма из двух щелей, и экран, на котором мы наблюдаем интерференционную картину. Природу этой интерференционной картины можно легко понять, если исходить из волновых свойств частиц, вылетающих из источника. Здесь можно заметить, что эксперимент с двумя щелями проводился с частицами различных типов, от фотонов [2] и электронов [3] до нейтронов [4] и атомов [5]. С точки зрения квантовой механики, состояние на экране – это когерентная суперпозиция

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|\Psi_a\rangle + |\Psi_b\rangle\right) , \qquad (1.1)$$

где $|\Psi_a\rangle$ и $|\Psi_b\rangle$ описывают квантовое состояние в том случае, если открыта только щель a или щель b.

Интересное свойство эксперимента с двумя щелями, подтвержденное во всех экспериментах, состоит в том, что, интерференционную картину можно собрать по одной частице – то есть, установив настолько низкую интенсивность источника, что каждая частица будет интерферировать только сама с собой. В этом случае у нас появляется соблазн спросить себя, через какую из двух щелей частица пролетает «на самом деле». Стандартная квантовая механика отвечает на это, что невозможно дать какой-либо разумный ответ на вопрос «через какую щель пролетает частица?» не используя соответствующие экспериментальные методы, способные дать ответ на этот вопрос. На са-

мом деле, если бы нам надо было поставить эксперимент, определяющий, через какую щель пролетает частица, нам бы пришлось тем или иным образом взаимодействовать с частицей, что привело бы к декогерентности – то есть, к потере интерференции. Мы можем наблюдать интерференцию только тогда, когда даже в принципе нет возможности узнать, через какую из щелей пролетает частица. В качестве небольшого предостережения, отметим, что также неверно и говорить, что частица пролетает через обе щели одновременно, хотя такое утверждение можно нередко услышать. Проблема здесь в том, что, с одной стороны, это предложение противоречиво, поскольку частица – это локализованный объект, и, с другой стороны, такое утверждение не несет смысла с точки зрения рассматриваемой операции. Отметим также, что можно получить частичное знание о том, через какую из щелей пролетает частица, за счет частичной потери когерентности.

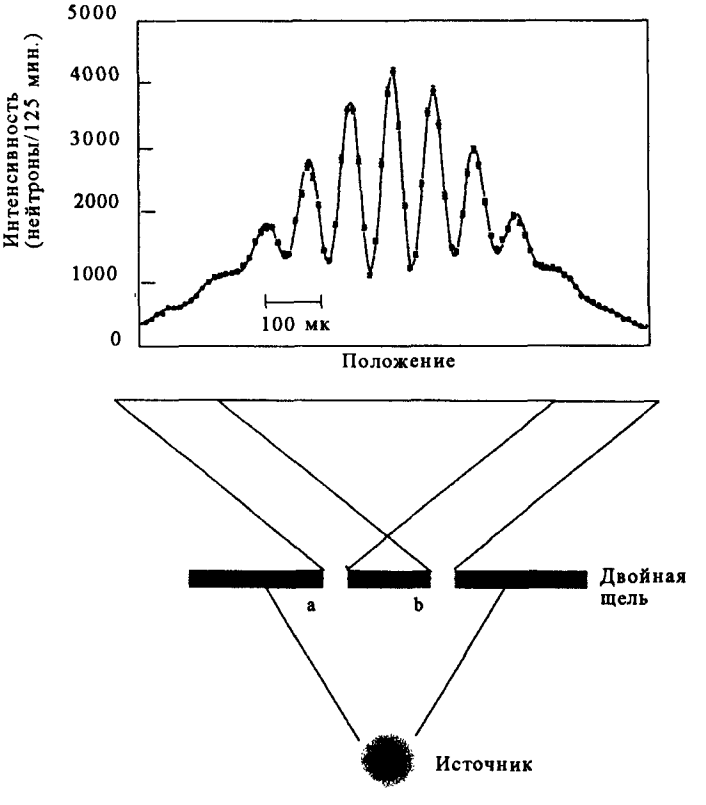


Рис. 1.1. Принцип эксперимента с двумя щелями. Интерференционная картина возникает в плоскости наблюдения за двухщелевой диафрагмой, даже если интенсивность источника столь мала, что в аппарате одномоментно находится только одна частица. Показанная здесь интерференционная картина была получена в реальных экспериментах на двух щелях с нейтронами [4].

1.2 Кубиты

Наиболее фундаментальная величина в науке об информации – это бит. Это система, которая может принимать два значения, «0» и «1». В классической реализации, бит, который можно себе представить, например, просто механическим переключателем, есть система, имеющая два четко различимых состояния. Между ними должен быть достаточно большой энергетический барьер, чтобы система не могла спонтанно переходить из одного состояния в другое, что было бы, очевидно, пагубным эффектом.

Кубит [6], квантовый аналог бита, должен, следовательно, также быть системой из двух состояний: $|0\rangle$ и $|1\rangle$. Кубитом может служить практически любая квантовая система, имеющая, по меньшей мере, два состояния. Можно придумать множество вариантов таких систем, и многие из них уже были реализованы экспериментально. Наиболее необходимая черта квантовых состояний, используемых в качестве битов, – это свойства когерентности и суперпозиции. При этом произвольное состояние выражается как

$$|Q\rangle = \alpha|0\rangle + \beta|1\rangle \ , \tag{1.2}$$

где $|\alpha|^2 + |\beta|^2 = 1$. Это означает не то, что значение кубита лежит где-то посередине между «0» и «1», но то, что кубит находится в когерентной суперпозиции двух состояний, и, если мы его измерим, то найдем, что кубит с вероятностью $|\alpha|^2$ несет значение «0», и с вероятностью $|\beta|^2$ – значение «1»:

$$p("0") = |\alpha|^2 \ , \quad p("1") = |\beta|^2 \ . \tag{1.3}$$

Несмотря на то, что, по определению кубита, его свойства кажутся неопределенными, важно понимать, что (1.2) описывает *когерентную* суперпозицию, а не некогерентную смесь «0» и «1». Важное отличие между ними состоит в том, что для когерентной суперпозиции всегда существует базис, в котором значение кубита строго определено, тогда как некогерентная смесь – это смесь, каким бы образом мы ее ни описывали. Для простоты, рассмотрим конкретное состояние

$$|Q'\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \ . \tag{1.4}$$

Это, очевидно, означает, что с 50% вероятностью кубит будет найден в состоянии либо «0», либо «1». Интересно что в базисе, повернутом в гильбертовом пространстве на 45%, значение кубита строго определено. Этот факт можно увидеть, применив к кубиту соответствующее преобразование. Одно из основных преобразований в науке

о квантовой информации – это так называемое преобразование Адамара, которое действует на кубит следующим образом:

$$H|0\rangle \to \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) , \quad H|1\rangle \to \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) . \tag{1.5}$$

Применив его к кубиту $|Q'\rangle$, получим

$$H|Q'\rangle = |0\rangle , \tag{1.6}$$

то есть, строго определенное значение кубита. Это было бы невозможно сделать с некогерентной смесью.

1.3 Преобразования одного кубита

Можно понять одну из наиболее базовых экспериментальных операций в физике квантовой информации, рассмотрев действие простого делителя, который делит луч в отношении 50/50. Такие делители были реализованы для частиц различных типов, не только для фотонов. Для произвольного делителя, исследуем случай двух входящих мод и двух выходящих – так, как это показано на Рис. 1.2.

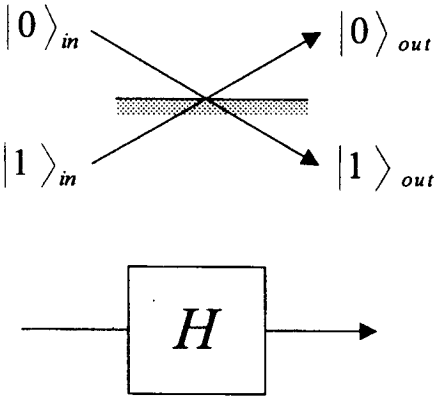


Рис. 1.2. Делитель 50/50 (вверху) и соответствующая диаграмма, обозначающая преобразование Адамара (внизу)

Частица, падающая сверху или снизу на делитель 50/50, появится либо в верхнем, либо в нижнем выходящем луче с одной и той же 50% вероятностью. Тогда из условия квантовой унитарности – то есть, из условия, что частицы не теряются, если делитель их не поглощает, – следуют определенные фазовые условия на действие делителя [7], с одной свободной фазой. Можно очень просто описать фазовое действие делителя, зафиксировав фазовые соотношения так, что оно будет описываться преобразованием Адамара (1.5).

Снова предположим, что состояние на вход – это произвольный кубит:

$$|Q\rangle_{in} = \alpha|0\rangle_{in} + \beta|1\rangle_{in} \ . \qquad (1.7)$$

Для случая одной частицы это означает, что α – это амплитуда вероятности обнаружить частицу, падающую на делитель сверху, а β – амплитуда вероятности обнаружить частицу, падающую снизу. Тогда в результате действия делителя получается конечное состояние

$$|Q\rangle_{out} = H|Q\rangle_{in} = \frac{1}{\sqrt{2}}\left((\alpha+\beta)|0\rangle_{out} + (\alpha-\beta)|1\rangle_{out}\right) \ , \qquad (1.8)$$

так что амплитуда вероятности найти частицу в верхнем выходящем пучке равна теперь $(\alpha + \beta)$, а амплитуда вероятности найти ее в нижнем пучке равна $(\alpha - \beta)$. В частности, если $\alpha = 0$ или $\beta = 0$, то видно, что частицу можно с равной вероятностью обнаружить в любом из выходящих пучков. В другом частном случае, $\alpha = \beta$, частица будет обязательно обнаружена в верхнем пучке, и никогда не будет обнаружена в нижнем.

Интересно и полезно рассмотреть последовательности таких делителей, поскольку они осуществляют последовательности преобразований Адамара. Для двух последовательных преобразований используется интерферометр Маха-Цандера (Рис. 1.3) с двумя одинаковыми делителями.

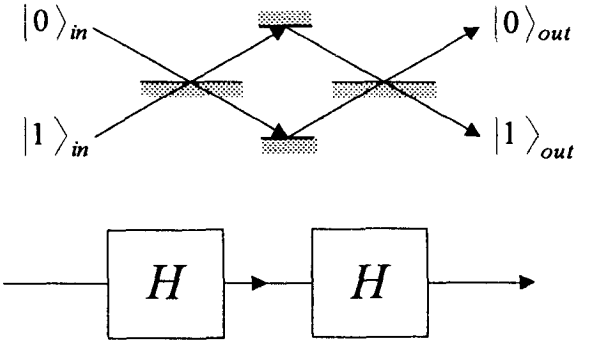


Рис. 1.3. Интерферометр Маха-Цандера (вверху) и последовательность из двух преобразований Адамара (внизу)

Показанные на рисунке зеркала нужны только для того, чтобы перенаправить пучки. Предполагается, что они одинаково действуют на два пучка, и, следовательно, при анализе их можно не учитывать. Тогда полное действие интерферометра можно описать просто как два последовательных преобразования Адамара, действующих на произвольное состояние на входе (1.7):

$$|Q\rangle_{out} = HH|Q\rangle_{in} = |Q\rangle_{in} \ . \tag{1.9}$$

Ответ следует из того простого факта, что двойное применение преобразования Адамара (1.5) есть тождественная операция. Это означает, что показанный на Рис. 1.3 интерферометр Маха-Цандера, делители в котором осуществляют преобразование Адамара, на выходе воспроизводит то состояние, которое он получает на входе. Рассмотрим еще раз крайний частный случай, когда вход состоит только из одного пучка – то есть, предположим, без потери общности, что $\alpha = 1$, а нижний пучок – пустой. Тогда, согласно (1.9), на выходе частица будет обязательно обнаружена наверху. И, что интересно, это произойдет именно потому, что между делителями частица была бы с одинаковой вероятностью (с определенной относительной фазой) обнаружена в каждом из пучков. Именно интерференция между двумя амплитудами, падающими на последний делитель, приводит к тому, что частица всегда оказывается в одном из выходящих пучков, и никогда – в другом.

На языке квантовой информации, кубит на выходе интерферометра Маха-Цандера будет иметь определенное значение, если кубит на входе будет также иметь определенное значение – и это только потому, что в промежутке между двумя преобразованиями Адамара значение кубита было максимально неопределенно.

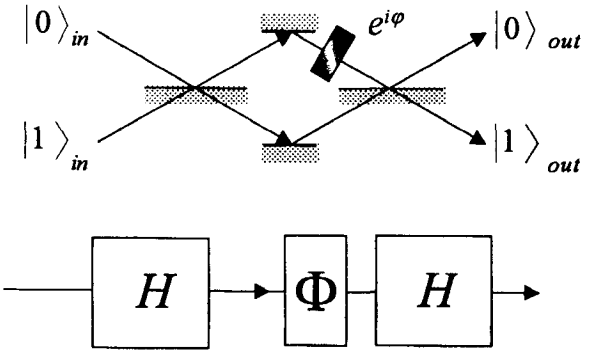


Рис. 1.4. Вверху: интерферометр Маха-Цандера с фазовращателем φ в одном из двух пучков. Это полностью меняет результат. Внизу: эквивалентное представление с преобразованиями Адамара и логическим элементом сдвига фазы.

Еще одним важным квантовым логическим элементом, помимо элемента Адамара, является фазовращатель. На Рис. 1.4 он дополнительно введен в интерферометр Маха-Цандера. Его функция состоит в том, чтобы просто совершить сдвиг фазы φ у одного из двух пучков (без потери общности, предполагаем, что это верхний пучок, поскольк-

ку важна только относительная фаза). В наших обозначениях, действие фазовращателя можно описать унитарным преобразованием

$$\Phi|0\rangle = e^{i\varphi}|0\rangle \ , \ \Phi|1\rangle = |1\rangle \ . \tag{1.10}$$

Следовательно, кубит на выходе можно вычислить, последовательно применяя все соответствующие преобразования к кубиту, который был на входе:

$$|Q\rangle_{out} = H\Phi H|Q\rangle_{in} \ . \tag{1.11}$$

Оставим читателю вычисление общего выражения для произвольного состояния кубита на входе. Мы же снова ограничим обсуждение случаем, когда есть только один пучок на входе, а именно $\alpha = 1$ и $\beta = 0$, то есть, $|Q\rangle_{in} = 0$. Тогда конечное состояние становится

$$H\Phi H|0\rangle = \frac{1}{2}\left(\left(e^{i\varphi}+1\right)|0\rangle + \left(e^{i\varphi}-1\right)|1\rangle\right) . \tag{1.12}$$

У этого выражения есть очень простая интерпретация. Сначала мы замечаем, пользуясь (1.12), что для $\varphi = 0$ значение кубита определенно и равно «0». С другой стороны, для $\varphi = \pi$, значение кубита строго равно «1». Это показывает, что фазовый сдвиг φ может переключать состояние выходного кубита между «0» и «1». В целом, вероятность, что кубит имеет значение «0» есть $P_0 = \cos^2(\varphi/2)$, а вероятность, что он несет значение «1» равна $P_1 = \sin^2(\varphi/2)$.

В этом разделе мы обсудили некоторые основные идеи, касающиеся линейных преобразований квантовых битов. Обратимся теперь к перепутанным кубитам.

1.4 Перепутывание

Рассмотрим источник, который испускает пару частиц так, что одна из них летит налево, а другая – направо (источник S на Рис. 1.5). Источник таков, что частицы испускаются с противоположными импульсами. Если частица, летящая налево (назовем ее частицей 1), обнаружена в верхнем пучке, то частица 2, летящая направо, будет обязательно обнаружена в нижнем. И наоборот, если частица 1 найдена в нижнем пучке, то частица 2 будет обязательно найдена в верхнем. На нашем языке кубитов мы бы сказали, что две частицы несут противоположные значения битов. Если частица 1 несет «0», то частица 2 несет «1», и наоборот. На языке квантовой механики, это двухчастичное состояние вида

$$\frac{1}{\sqrt{2}}\left(|0\rangle_1|1\rangle_2 + e^{i\chi}|1\rangle_1|0\rangle_2\right) . \tag{1.13}$$

Фаза χ определяется внутренними свойствами источника, и мы предположим для простоты, что $\chi = 0$. Уравнение (1.13) описывает то,

что называют перепутанным состоянием [8][1,2]. Оно интересно тем, что ни один из двух кубитов не несет определенного значения, но, как следует из вида квантового состояния, как только один из двух кубитов будет подвергнут измерению (результат которого будет совершенно случайным), то сразу окажется, что другой несет определенное значение. Говорят, что в этом проявляется загадка квантовой нелокальности, так как во время измерения два кубита могут быть удалены друг от друга на произвольно большое расстояние.

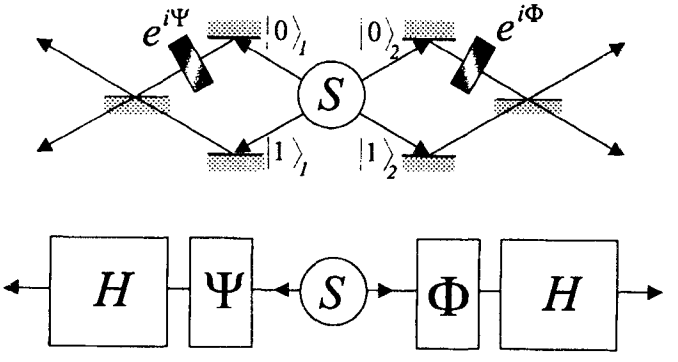


Рис.1.5. Источник испускает два кубита в перепутанном состоянии. Вверху: проверка с помощью двухчастичного интерферометра. Внизу: тот же принцип в терминах однофотонных логических элементов.

Самая интересная ситуация возникает тогда, когда оба кубита подвергнуты фазовому сдвигу и преобразованию Адамара, как показано на Рис. 1.5. Тогда, для детектирования после обоих преобразований Адамара – то есть, в случае проверки с помощью двухчастичного интерферометра [10] для детектирования за делителями, – появляются интересные нелокальные корреляции, нарушающие неравенства Белла [11]. Не углубляясь в теоретические и формальные детали (больше информации будет дано в разделе 1.7), можно сказать, что суть такого нарушения состоит в том, что невозможно объяснить корреляции между явлениями наблюдаемыми на двух сторонах прибора на основе одних лишь локальных свойств кубитов. Нельзя понять квантовые корреляции между ними, если считать, что на детектор, регистрирующий частицу на одной заданной стороне, не влияет величина фазы для другой частицы, заданной как параметр. Есть много возмож-

[1] От английского слова *Entanglement* – (свободного) перевода слова *Verschrankung*, введенного Шредингером в 1935 г., чтобы охарактеризовать эту специфическую черту составных квантовых систем.

[2] Мы используем термин «*перепутывание*» квантовых состояний, поскольку он на сегодняшний день устоялся в русскоязычной литературе. (*Прим. переводчика*).

ностей точно выразить смысл неравенств Белла, и можно их формально представить многими способами. Некоторые из них будут представлены в разделе 1.7, а оставшаяся часть может быть найдена в соответствующей литературе (см., например, работу [12] и ссылки в ней).

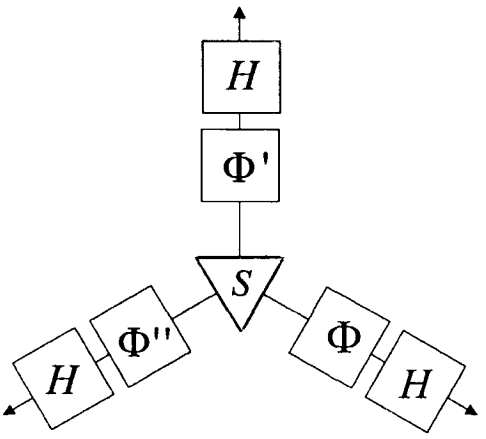


Рис. 1.6. Трехчастичное перепутывание в так называемом состоянии ГХЦ. Здесь мы показываем только представление в терминах элементарных логических элементов. Читатель легко может себе представить физическую реализацию трехчастичного интерферометра.

Очень интересное и очень уместное с точки зрения квантовой механики обобщение – это исследовать перепутывание для более чем двух кубитов. Например, рассмотрим простой случай перепутывания между тремя кубитами, как показано на Рис. 1.6. Предположим, что источник испускает три частицы, по одной в каждый из показанных на рисунке приборов, в специфической суперпозиции – в так называемом состоянии Гринбергера-Хорна-Цайлингера (ГХЦ) [13] (см. также раздел 6.3)

$$\frac{1}{\sqrt{2}}\left(|0\rangle_1|0\rangle_2|0\rangle_3+|1\rangle_1|1\rangle_2|1\rangle_3\right). \qquad (1.14)$$

Это квантовое состояние обладает очень специфическими свойствами. Также как и в перепутывании для двух частиц, ни один из трех кубитов не несет сам по себе информации, ни один из них не имеет строго определенного значения бита. Но как только один из них будет измерен, два других приобретут строго определенное значение, если только измерение производится в базисе 0–1. И этот вывод не зависит от пространственного размещения трех измерений.

Самое интересное то, что, если посмотреть на предсказываемые состоянием ГХЦ (1.14) соотношения между тремя измерениями после прохождения элементов сдвига фазы и преобразований Адамара,

то можно найти большое количество полных корреляций для определенных совместных наборов параметров [14] с тем интересным свойством, что невозможно понять даже абсолютно точные корреляции в рамках локальной модели. Это показывает, что квантовая механика расходится с локальным классическим взглядом на мир не только в области статистических предсказаний теории, но также и для предсказаний, которые можно сделать со всей определенностью.

1.5 Перепутывание и квантовая неразличимость

Чтобы понять как природу перепутывания так и способы его создания, надо осознать, что состояния общего вида (1.13) и (1.14) – это суперпозиции произведений независимых состояний. Вспомним обсуждение явления дифракции на двух щелях (раздел 1.1), где суперпозиция означала, что не существует способа сказать, какая из двух возможностей, формирующих эту суперпозицию, имеет место на самом деле. Это же правило надо применить, чтобы понять квантовое перепутывание. Например, для состояния

$$\Psi_{12} = \frac{1}{\sqrt{2}}\left(|0\rangle_1|1\rangle_2 + |1\rangle_1|0\rangle_2\right) . \tag{1.15}$$

нет способа сказать, несет ли кубит 1 значение «0» или «1», и, аналогично, несет ли кубит 2 значение «0» или «1». Но, если измерить один кубит, второй немедленно примет четко определенное квантовое состояние. Эти наблюдения приводят нас прямо к условиям того, как создавать и наблюдать перепутанные квантовые состояния.

Есть много способов создать перепутанные состояния. Во-первых, можно создать такой источник, что, в силу его физического устройства, появляющиеся квантовые состояния уже будут иметь свойство неразличимости, которое обсуждалось выше. Это реализуется, например, распадом частицы со спином 0 на две частицы со спином 1/2 с сохранением внутреннего момента импульса [15]. В этом случае спины возникающих частиц должны быть противоположными, и, если нет дальнейших механизмов, позволяющих различить возможности прямо у источника, появляющееся квантовое состояние есть

$$\Psi_{12} = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle_1|\downarrow\rangle_2 - |\downarrow\rangle_1|\uparrow\rangle_2\right) . \tag{1.16}$$

где, например, $|\uparrow\rangle_1$ обозначает частицу 1 со спином вверх. Состояние (1.16) обладает замечательным свойством вращательной инвариантности – то есть, два спина антипараллельны, относительно какого бы направления мы их ни измеряли.

Вторая возможность состоит в том, что источник может на са-

мом деле создавать состояния в виде индивидуальных компонент в суперпозиции (1.15), но состояния могут быть все равно каким-то образом различимы. Это происходит, например, при параметрическом рассеянии типа-II [16] (раздел 3.4.4), где состояния фотонов вдоль определенного выбранного направления равны

$$|H\rangle_1|V\rangle_2 \quad \text{и} \quad |V\rangle_1|H\rangle_2 \ . \tag{1.17}$$

Это означает, что либо фотон 1 поляризован горизонтально, а фотон 2 – вертикально, либо фотон 1 поляризован вертикально, а фотон 2 – горизонтально. Тем не менее, из-за разной скорости света внутри параметрического кристалла-преобразователя для горизонтально и вертикально поляризованных фотонов, временная корреляция между двумя фотонами в этих двух случаях разная. Следовательно, с помощью измерений во времени можно различить два члена в (1.17), и, из-за потенциальной возможности различить эти два случая, не возникает перепутанного состояния. Однако, даже и в такой ситуации можно создать перепутывание, смещая два созданных фотонных волновых пакета друг относительно друга таким образом, чтобы они перестали быть различимыми благодаря своему положению во времени. Фактически это означает применение техники квантового стирания [17], в которой маркер – в данном случае, относительный порядок во времени – стирается, так что получается состояние с квантовой неразличимостью

$$\Psi_{12} = \frac{1}{\sqrt{2}}\left(|H\rangle_1|V\rangle_2 + e^{i\chi}|V\rangle_1|H\rangle_2\right) , \tag{1.18}$$

которое является перепутанным.

Третье средство получить перепутанные состояния – это спроектировать неперепутанное состояние на перепутанное. Отметим, что перепутанное состояние никогда не ортогонально ни одной из своих компонент. Например, рассмотрим источник, создающий неперепутанное состояние

$$|0\rangle_1|1\rangle_2 \ . \tag{1.19}$$

Предположим, что это состояние теперь проходит через на фильтр, описываемый оператором проицирования

$$P = |\Psi\rangle_{12}\langle\Psi|_{12} \ , \tag{1.20}$$

где $|\Psi\rangle_{12}$ – это состояние (1.15). Тогда появляется следующее состояние:

$$\frac{1}{2}\left(|0\rangle_1|1\rangle_2 + |1\rangle_1|0\rangle_2\right)\left(\langle 0|_1\langle 1|_2 + \langle 1|_1\langle 0|_2\right)|0\rangle_1|1\rangle_2 =$$

$$= \frac{1}{2}\left(|0\rangle_1|1\rangle_2 + |1\rangle_1|0\rangle_2\right) \ ; \tag{1.21}$$

оно более не нормировано на единицу, так как действие оператора проицирования приводит к потере кубитов.

Тогда как каждый из обсуждаемых выше методов может быть, в принципе, использован для создания перепутанных состояний, возможно также и создавать перепутывание путем наблюдения состояния. Это, в целом, означает, что у нас есть неперепутанное или частично перепутанное состояние в том или ином виде, а также процедура самого измерения, которая проектирует квантовые состояния на перепутанные во многом таким же образом, как это только что обсуждалось. Эта процедура использовалась, например, при первой экспериментальной демонстрации перепутывания трех фотонов в ГХЦ (см. раздел 6.3) [18].

1.6 Логический элемент «управляемое НЕ».

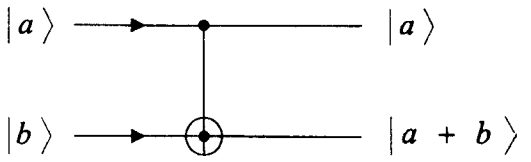


Рис. 1.7. Элемент «управляемое НЕТ» – это преобразование, связанное с двумя кубитами. Значение контрольного кубита (на рисунке вверху) влияет на нижний, чье значение «переключается» на обратное, если верхний кубит несет «1», и не меняется, если верхний кубит несет «0». Эта операция эквивалентна сложению по модулю 2.

До сих пор мы обсуждали только одно-кубитные логические элементы – то есть, элементы, которые оперируют только одним кубитом. Для квантовых вычислений наиболее важны двух-кубитные элементы, в которых эволюция одного кубита зависит от состояния второго. Самый простой из них – это элемент «управляемое НЕ», показанный на Рис. 1.7. Суть его работы в том, что значение так называемого целевого кубита (кубит-мишень) меняется на обратное в том и только том случае, если контрольный кубит имеет логическое значение «1». Логическое значение контрольного кубита не меняется. Можно описать действие квантового логического элемента «управляемое НЕ» следующими преобразованиями

$$|0\rangle_c|0\rangle_t \to |0\rangle_c|0\rangle_t \quad |0\rangle_c|1\rangle_t \to |0\rangle_c|1\rangle_t$$

$$|1\rangle_c|0\rangle_t \to |1\rangle_c|1\rangle_t \quad |1\rangle_c|1\rangle_t \to |1\rangle_c|0\rangle_t \qquad (1.22)$$

где $|0\rangle_c$ и $|1\rangle_c$ относятся к контрольному кубиту, а $|0\rangle_t$ и $|1\rangle_t$ – к целевому. Вместе с одно-кубитными преобразованиями, описанными в разделе

1.3, квантовый логический элемент «управляемое НЕ» может быть использован для построения квантовых вычислительных сетей. Одно из интересных явных приложений этих элементов состоит в создании с их помощью двух-кубитных и много-кубитных перепутанных состояний [19].

1.7 Аргумент ЭПР и неравенство Белла.

Сразу после открытия современной квантовой механики стало ясно, что она содержит новые, противоречащие интуиции черты. Самое примечательное тому свидетельство – знаменитый диалог между Нильсом Бором и Альбертом Эйнштейном [20]. Тогда как вначале Эйнштейн утверждал, что квантовая механика несостоятельна, позже он переформулировал свои доводы, доказывая, что она неполна. В своей ключевой статье [21] Эйнштейн, Подольский и Розен (ЭПР) рассматривают квантовые системы, состоящие из таких двух частиц, что ни координата, ни импульс каждой из частиц не определены, но сумма их координат (то есть, их центр масс) и разность их импульсов (то есть, импульс центра масс системы) определены абсолютно точно. Тогда получается, что измерение координаты или импульса, скажем, частицы 1 немедленно придает частице 2 точное значение координаты или импульса без взаимодействия с этой частицей. Исходя из того, что частицы 1 и 2 могут быть разнесены на произвольные расстояния, ЭПР предполагают, что измерение частицы 1 не может на самом деле повлиять на частицу 2 (условие локальности); и, следовательно, свойства частицы 2 не должны зависеть от измерения, проведенного над частицей 1. Они считают, что отсюда следует, что координата и импульс могут одновременно являться хорошо определенными свойствами квантовой системы.

В своем знаменитом ответе [22] Нильс Бор утверждает, что две частицы в случае ЭПР всегда являются частями одной квантовой системы. И это значит, что измерение над одной из частиц меняет возможные предсказания, которые можно сделать для всей системы, а значит и для второй частицы.

Дискуссию ЭПР-Бора долгое время считали чисто философской, пока в 1951 году Давид Бом [15] не ввел системы, перепутанные по спину, и в 1964 году Джон Белл [23] не показал, что, для таких перепутанных систем, измерения коррелирующих величин должны в случае квантовой механики приводить к результатам, отличным от того, что выйдет, если предположить, что свойства системы существуют до измерения и независимо от него. Даже несмотря на то, что квантовые

предсказания подтверждены теперь во многих экспериментах [24-26], со строго логической точки зрения вопрос до сих пор не закрыт, поскольку, из-за некоторых «лазеек» в экспериментах, до сих пор, в принципе, возможно логически защищать точку зрения локального реализма [27].

Покажем кратко ход рассуждений, приводящих к неравенству, эквивалентному первоначальному неравенству Белла. Рассмотрим источник, испускающий два кубита (Рис. 1.8) в перепутанном состоянии

$$\left|\Phi^{+}\right\rangle_{12} = \frac{1}{\sqrt{2}}\left(\left|H\right\rangle_1\left|H\right\rangle_2 + \left|V\right\rangle_1\left|V\right\rangle_2\right) \tag{1.23}$$

Рис. 1.8. Корреляционные измерения между детектируемыми событиями Алисы и Боба при различных выборах базисов детектирования (обозначенных углами α и β ориентаций поляризационных светоделителей PBS) приводят к нарушению неравенств Белла.

Один кубит посылается Алисе (налево на Рис. 1.8), а другой – Бобу (направо на Рис. 1.8). Алиса и Боб произведут измерение поляризации, используя поляризационные делители с двумя однофотонными счетчиками на выходе. Алиса с одинаковой вероятностью получит результат измерения «0» или «1», соответствующий детектирования кубита счетчиком 1 или 2 соответственно. Это утверждение останется верным, в каком бы поляризационном базисе она ни делала измерение, и результат измерения будет абсолютно случайным. Но если Боб выберет для измерения тот же базис, он всегда получит тот же результат. Таким образом, следуя первому шагу в рассуждении ЭПР, Алиса всегда сможет точно предсказать, какой результат будет у Боба. На втором шаге применяется гипотеза локальности, то есть, предположение, что никакое физическое воздействие не может моментально пробежать от прибора Алисы до прибора Боба, и значит, результат, измеренный Бобом должен зависеть только от свойств его кубита и прибора. Соединяя эти два шага, Джон Белл исследовал возможные корреляции для случая, когда Алиса и Боб выбирают базисы измерения под углом друг к другу. Можно увидеть, что для трех про-

извольных углов ориентации α, β, γ, должно [28] выполняться следующее соотношение:

$$N(1_\alpha, 1_\beta) \le N(1_\alpha, 1_\gamma) + N(1_\beta, 0_\gamma) \tag{1.24}$$

где

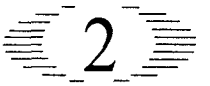
$$N(1_\alpha, 1_\beta) = \frac{N_0}{2} \cos^2(\alpha - \beta) \tag{1.25}$$

есть квантовомеханическое предсказание для числа случаев, в которых Алиса получит «1» в своем приборе, ориентированном под углом α, а Боб получит «1» в своем приборе, ориентированном под углом β, и N_0 – число пар, испущенных источником. Это неравенство нарушается предсказаниями квантовой механики, например, для таких углов, что $(\alpha - \beta) = (\beta - \gamma) = 30^0$. Нарушение неравенства означает, что, по крайней мере, одно из предположений, на которых основано неравенство Белла, не согласуется с квантовой механикой. Этот факт обычно считают доказательством нелокальности, хотя, конечно, это не единственно возможное объяснение[3].

1.8 Комментарии

Всего десять лет назад обсуждаемые здесь вопросы считались, в основном, философскими, хоть и имеющими большое отношение к нашим попыткам понять мир вокруг и нашу роль в нем. За последние несколько лет, к удивлению многих опытных исследователей, базовые понятия суперпозиции и квантового перепутывания оказались ключевыми составляющими в новых схемах квантовой коммуникации и квантовых вычислений. Здесь мы представили только сжатое введение в тему. Многие детали даны в различных главах этой книги. Дальнейшую информацию можно найти в Интернете, например, на сайте www.qubit.org или www.quantum.at со многими ссылками на другие адреса.

[3] Методическая сторона этого вопроса изложена в работе Н.В.Евдокимова, Д.Н.Клышко, В.П.Комолова, В.А.Ярочкина. «Неравенства Белла и корреляции ЭПР-Бома: действующая классическая радиочастотная модель». УФН, 166, 91-107 (1997). (*Прим. переводчика*).



Квантовая криптография

А.Экерт, Н.Жизан, Б. Хаттнер, Х.Инамори, Х.Вайнфуртер

2.1 Что не так в классической криптографии?

2.1.1 От СКИТАЛА к ЭНИГМЕ

Желание людей секретно переписываться является, по крайней мере, настолько же древним, как и само письмо, и восходит к зарождению нашей цивилизации. Методы секретной коммуникации были развиты во многих цивилизациях, включая Месопотамию, Египет, Индию и Китай, но детали, относящиеся к происхождению криптологии[1], остаются неизвестными [29].

Мы знаем, что в Европе первыми применили криптографию в военных целях спартанцы, самые воинственные из греков. Около 400 г. до н.э. они использовали устройство, называемое СКИТАЛ. Устройство, которое использовалось для сообщения между военачальниками, состояло из конусообразной дубинки, вокруг которой по спирали наматывалась полоска из пергамента или кожи, несущая сообщение. Слова писались вдоль дубинки, по одной букве на каждом витке полоски. Получатель сообщения наматывал пергамент на другую дубинку такой же формы, и посланное сообщение снова можно было прочесть, как показано на Рис. 2.1.

Есть свидетельства, что Юлий Цезарь в своей корреспонденции использовал простой метод подстановки букв. Каждая буква в письме Цезаря заменялась на другую букву, следующую за ней по алфавиту через три. Латинская буква A заменялась на D, B на E, и так далее. Например, английское слово COLD после подстановки Цезаря выглядит как FROG. Этот метод до сих пор называют шифром Цезаря, независимо от размера смещения, которое используется для подстановки.

[1] Наука о защищенном сообщении называется криптологией от греческого *криптос* – спрятанный – и *логос* слово. Криптология включает в себя криптографию, искусство создания кодов, и криптоанализ, искусство взламывания кодов.

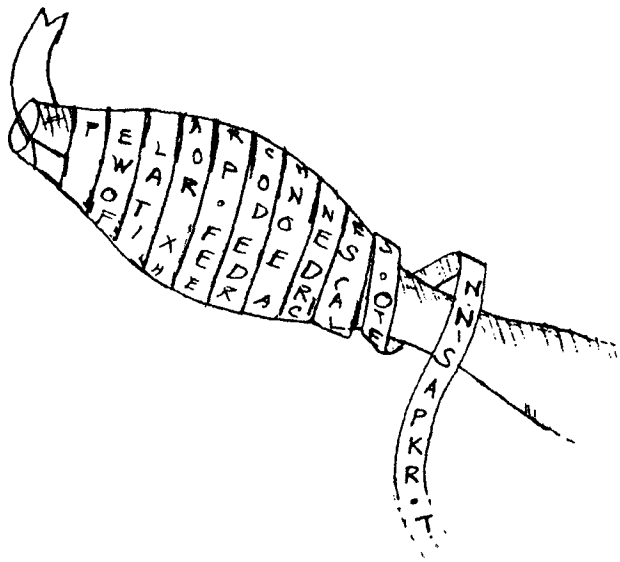


Рис. 2.1. Первая криптографическая машина — Скитал.

Эти два простых примера уже содержат два базовых метода шифрования, которые до сих пор используются шифровальщиками, а именно *перестановку* и *подстановку*. При перестановке (например, в СКИТАЛЕ), буквы *открытого текста* (научный термин, обозначающий передаваемое сообщение) специальным образом переставляются по отношению друг к другу. При подстановке (например, в шифре Цезаря) буквы открытого текста меняются на другие буквы, числа или произвольные символы. Эти два метода можно, в общем случае, комбинировать.

Вплоть до недавнего времени сложная криптография применялась почти исключительно в военных целях. Только у военных было достаточно средств, чтобы производить сложные механические приборы – такие, как прибор ЭНИГМА, который использовался немцами во время второй мировой войны, или его американский аналог М-209. Шифры ЭНИГМЫ были взломаны перед войной в Польше, а во время войны – в Блетчли Парке в Англии. Чтобы вскрыть эти шифры, команде из Блетчли Парка, в которую входил Алан Тьюринг, пришлось создать специальные электромеханические устройства. Позже это привело к созданию первого цифрового компьютера, который назывался КОЛОСС. Современная криптология (введение в нее см., например, в [30]-[32]) родилась одновременно с вычислительной техникой. По выражению Р. Л. Ривеста (одного из изобретателей популярной системы кодирования с открытым ключом RSA) криптоанализ был «повивальной бабкой вычислительной техники».

2.1.2 Ключи и их распределение

Первоначально защита криптотекста зависела от секретности обеих процедур шифрования и расшифровки. Однако, сегодня мы используем шифры, в которых можно открыть алгоритм шифрования и расшифровки кому угодно, без угрозы для сохранения секретности конкретной криптограммы. В таких шифрах, набор специальных параметров, называемый ключом, подается, вместе с открытым текстом, на вход в алгоритме зашифровки и, вместе с криптограммой, на вход алгоритма расшифровки. Это можно записать в виде

$$\hat{E}_k(P) = C \text{ , и, наоборот, } \hat{D}_k(C) = P, \tag{2.1}$$

где P обозначает открытый текст, C обозначает криптотекст или криптограмму, индекс k — криптографический ключ, и E и D — операции шифрования и расшифровки, соответственно.

Алгоритмы шифрования и расшифровки известны и открыты; секретность криптограммы полностью зависит от секретности ключа, и этот ключ должен состоять из *случайно выбранной*, достаточно длинной строки битов. Пожалуй, будет легче всего объяснить эту процедуру, если взглянуть на код Вернама, известный также как одноразовый блокнот.

Если мы выберем простой цифровой алфавит, в котором используются только заглавные буквы и некоторые знаки препинания, то есть

A	B	C	D	E	...	...	X	Y	Z		?	,	.
00	01	02	04	03	...	...	23	24	25	26	27	28	29

то мы сможем проиллюстрировать процедуру шифрования с секретным ключом на следующем простом примере (имеется ввиду меню агента 007): Чтобы получить криптограмму

S	**H**	**A**	**K**	**E**	**N**		**N**	**O**	**T**		**S**	**T**	**I**	**R**	**R**	**E**	**D**
18	07	00	10	04	13	26	13	14	19	26	18	19	08	17	17	04	03
15	04	28	13	14	06	21	11	23	18	09	11	14	01	19	05	22	07
03	11	28	23	18	19	17	24	07	07	05	29	03	09	06	22	26	10

(последовательность цифр в последней строке), добавим к числам открытого текста (верхний ряд цифр) числа из ключа (средний ряд), которые выбраны случайно в области от 0 до 29, и возьмем остаток от деления суммы на 30, так что мы выполняем сложение по модулю 30. Например, первая буква сообщения «S» записывается в от-

крытом тексте как «18», затем мы прибавляем 18+15 = 33; 33 = 1×30+3, следовательно, мы получаем в криптограмме 03. Шифрование и расшифровку можно записать, соответственно, как $P + k(\text{mod } 30) = C$ и $C - k(\text{mod } 30) = P$.

Описанный шифр был изобретен в 1917 году инженером компании AT&T Жильбером Вернамом. Позже Клод Шеннон показал [33], что, если ключ действительно случайный, если он такой же длины, что и само сообщение, и если он никогда не используется повторно, то одноразовая передача сообщения абсолютно защищена. Так что, если у нас есть действительно невзламываемая система, то что же не так в классической криптографии?

Существует одна проблема. Она называется *распределением ключа*. Как только ключ установлен, последующее сообщение предполагает пересылку криптограмм по некоему каналу, возможно даже по каналу, подверженному полному пассивному прослушиванию (например, публичные объявления через средства массовой информации). Этот этап действительно защищен. Однако чтобы определить ключ, два пользователя, у которых исходно нет никакой общей секретной информации, должны на какой-то стадии своего общения использовать некий очень надежный и секретный канал. Поскольку перехват есть серия измерений, проводимых подслушивающим агентом (какими бы сложными они не были с технической точки зрения), то любое классическое распределение можно в принципе подслушать, причем его «законные» пользователи не узнают, что имел место перехват. Это не было бы большой проблемой, если бы ключ был установлен раз и навсегда. В этом случае пользователи могли бы задействовать достаточно ресурсов (таких, как хранение в сейфе и охрана), чтобы гарантировать, что ключ прибудет к адресату в сохранности. Однако, поскольку ключ необходимо обновлять с каждым новым сообщением, такое распределение ключа стало бы недопустимо дорогим. По этой причине, в большинстве приложений, не требуют абсолютной секретности, но вместо этого используют менее дорогие и менее защищенные системы.

Для пересылки информации с более приземленными целями, обычно применяют стандарт DES (Data Encription Standart), который был принят в 1977 году, и который до сих пор используется для важной, но несекретной информации, особенно для коммерческих трансакций. Эта система использует короткий ключ, состоящий из 64 битов, 56 из которых используются напрямую в алгоритме, а последние 8 битов используются для детектирования ошибок. Она зашифровывает блоки из 64 битов открытого текста. В самом простом варианте, длинный открытый текст разрезается на блоки, и затем ключ использует-

ся при шифровании каждого из них. В более сложных (и безопасных) системах каждый зашифрованный блок зависит от предыдущих, что дополнительно защищает сообщение. Часто возникающие слухи о том, что стандарт DES взломан, до сих пор не подтвердились. Похоже, что DES был разработан на основе отличных критериев; при его коротком ключе, это очень хороший алгоритм. Дальнейшее обсуждение его многочисленных возможностей выходит за рамки нашего обзора, и может быть найдено в литературе или в Интернете. Как уже объяснялось выше, ни одна из них не является абсолютно защищенной: так как один и тот же ключ используется много раз, то в криптограмме присутствует информация об открытом тексте. Цель методик шифрования состоит в том, чтобы спрятать ее как можно лучше. Преданный делу криптоаналитик сможет сломать шифр и прочесть сообщение, но, если взлом займет слишком много времени, то информация устареет. В большинстве приложений рекомендуется пользоваться ключом в течение нескольких дней, после чего заменять его на новый. Конечно, проблема передачи ключа получателю остается, но с любой практической точки зрения она уже не так критична, поскольку сам ключ теперь гораздо меньших размеров.

Таким образом, возможна довольно хорошая защищенность, но как насчет полной секретности? Из краткого обсуждения, приведенного выше, следует, что в принципе мы можем достичь полной секретности при коммуникации путем одноразовых блокнотов, если решим проблему распределения ключа. Вопрос: можем ли мы решить проблему распределения ключа? В целом, ответ на этот вопрос — «да». Существуют два очень интересных решения, одно математическое и одно физическое. Математическое решение называется *криптографией с открытым ключом*, а физическое известно как *квантовая криптография*.

2.1.3 Открытые ключи и квантовая криптография

Прежде чем продолжать дальше, позвольте представить трех наших основных персонажей. Это Алиса и Боб – два лица, которые хотят секретно общаться, – и Ева, которая их подслушивает. Сценарий таков: Алиса и Боб хотят установить секретный ключ, а Ева хочет получить хотя бы частичную информацию о ключе.

Криптологи очень старались, чтобы дать Алисе и Бобу преимущество и решить проблему распределения ключа. Например, в 1970-х появилось хитрое математическое открытие – системы с «открытым ключом». Сегодня используются две основных криптографические системы с открытым ключом – протокол обмена ключом Диффи-Хел-

лмэна [34] и система шифрования RSA. Они были открыты в академическом сообществе, соответственно, в 1976 и 1978 годах. Однако эти методики были известны британским правительственным агентствам и до того, хотя этот факт вплоть до недавнего времени не был официально подтвержден. На самом деле, эти методы были впервые открыты в CESG в начале 1970-х Джоном Эллисом, который назвал их «несекретным шифрованием». В 1973 на основе идеи Эллиса К. Кокс разработал то, что мы сейчас называем RSA, а в 1974 М. Вильямсон предложил то, что по существу сейчас известно как протокол обмена ключом Диффи-Хеллмэна.

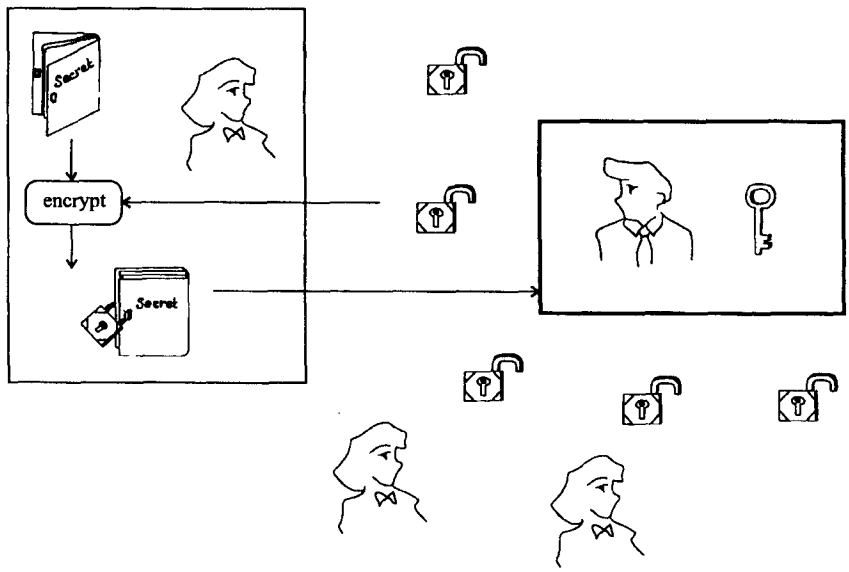


Рис. 2.2. Криптосистему с открытым ключом можно объяснить с помощью следующей механической аналогии. Представим, что Боб может изготовить много висячих замков, и любой желающий послать Бобу секретное сообщение может получить открытый замок, который сделал Боб. Открытый висячий замок можно рассматривать как открытый ключ. В частности, один берет себе Алиса. Как только Алиса закрыла замок, только Боб может его открыть, потому что только у Боба есть ключ — секретный ключ. Таким образом, Ализа может запереть любые данные по своему усмотрению и послать их Бобу с этим замком. Когда данные заперты, только Боб имеет к ним доступ благодаря своему секретному ключу.

В системах с открытым ключом пользователям не нужно договариваться о секретном ключе перед тем, как послать сообщение. Они работают по принципу сейфа с двумя ключами, так что есть один общий открытый ключ, чтобы его запереть, и еще один секретный ключ, чтобы его отпереть. У всех есть ключ, запирающий сейф, но только у кого-то одного есть ключ, который снова его откроет, так что кто угод-

но может положить в сейф сообщение, но только один человек может его оттуда забрать. Еще одной аналогией является пример с висячими замками, показанный на Рис. 2.2. Эти системы основаны на том факте, что некоторые математические операции гораздо легче провести в одном направлении, чем в другом. Поэтому в таких системах нет проблемы распределения ключей, но, к сожалению, их надежность основана на недоказанных математических фактах, таких, как сложность разложения больших целых чисел на простые множители (факторизации). То есть, всегда возможно найти секретный ключ по открытому ключу, но просто это трудно сделать. Например, безопасность RSA – очень популярной системы с открытым ключом, названной в честь трех ее изобретателей, Рона Ривеста, Ади Шамира и Леонарда Адлемана (Ron Rivest, Adi Shamir, Leonard Adleman) [35], – основана на трудности факторизации больших чисел. Математики уверены (твердо, хоть они этого и не доказали), что для того, чтобы факторизовать число из N десятичных цифр, классическому компьютеру требуется число шагов, которое растет экспоненциально в зависимости от N: то есть, прибавление еще одной цифры к числу, которое надо факторизовать, умножает требуемое время на фиксированный множитель. Таким образом, при увеличении числа цифр, задача быстро становится нерешаемой.

Это означает, что если и как только математики и компьютерщики придумают быстрые и хитрые процедуры для факторизации больших целых чисел, вся секретность и надежность криптосистем с открытым ключом исчезнут в одну ночь. Между тем, недавние исследования по квантовым вычислениям показывают, что квантовые компьютеры способны, по крайней мере, в принципе, факторизовать гораздо быстрее, чем классические компьютеры [36]! Это значит, что в некотором смысле криптосистемы с открытым ключом уже незащищены: любое сообщение, зашифрованное с помощью RSA, можно будет прочесть через несколько мгновений после того, как будет включен первый квантовый компьютер, и, следовательно, нельзя использовать RSA для шифрования информации, которая в тот счастливый день должна будет все еще оставаться секретной. Возможно, тот день наступит через десятилетия, но разве может кто-нибудь доказать или дать надежные гарантии, что так оно и будет? Все, на чем сейчас основывается надежность системы RSA – это уверенность в медленности технического прогресса.

Квантовая криптография предлагает совершенно новый способ решения проблемы распределения ключа. То, что квантовое вычисление отнимает одной рукой, оно возвращает, по крайней мере, частично, другой. Одним из простейших видов квантового вычисления –

видом, который теперь рутинно выполняется в лабораториях и может скоро стать коммерческим проектом – является квантовая криптография. Она обеспечивает абсолютно защищенное распределение ключа, поскольку, в отличие от классической криптографии, она основана на законах физики, а не на том факте, что для успешного подслушивания потребовались бы огромные вычислительные мощности.

Перед тем, как обсуждать квантовую криптографию (КК) в деталях, нам следует кратко упомянуть еще одну трудность в деле защищенной коммуникации, а именно *идентификацию*.

2.1.4 Идентификация: как узнать Золушку?

До сих пор, мы верили в чистоту канала связи: мы позволяли Еве подслушивать сообщения, которыми обменивались Алиса и Боб, но мы были уверены, что Ева не может их подделывать или изменять. То есть, мы предполагали, что у Алисы и Боба есть доступ к совершенному открытому каналу, то есть, каналу, который может просматривать кто угодно, однако, должно быть невозможно изменить информацию, посланную по нему – например, каналом может быть радиовещание. Во многих реалистичных сценариях это предположение может оказаться рискованным. В некоторых случаях хитрая Ева может мешать связи Алисы и Боба, разрезав канал пополам и выдавая себя за Алису для Боба и наоборот.

При этом условии она может, например, сделать две пары открыто-секретных ключей и дать один открытый ключ Алисе и один Бобу, сообщив Алисе, что дает ей открытый ключ Боба, и сообщив Бобу, что у него теперь есть открытый ключ Алисы. У Евы остаются соответствующие секретные ключи, и с этих пор все последующее сообщение между Алисой и Бобом происходит под ее полным контролем.

Точно также и криптосистема с секретным ключом, такая как одноразовый блокнот, допускает подделку, если враг знает посланное сообщение. Предположим, что посольство использует описанный выше шифр Вернама для связи со своей страной. Если Ева точно знает посланное сообщение, например, некоторые имена, то она может перехватить зашифрованное сообщение на пути к его месту назначения. Тем временем, она получает соответствующий ключ Вернама, выполняя для шифрованного текста сообщения вычитание по модулю 30. После этого она может использовать ключ по своему усмотрению, в интересующих ее целях, например дезинформации. Этот пример показывает, что даже совершенно защищенные криптосистемы не следует использовать вслепую.

«Сертификация» открытого ключа или «идентификация» сообще-

ния – это криптографический метод сосчитать атаки вышеописанного типа, называемые атаками с человеком посередине или атаками раздельных миров.

Если у Алисы и Боба и в самом деле есть общий секретный ключ, то для них существуют эффективные и удобные методы идентификации. Однако удобного способа сертифицировать открытый ключ до сих пор не существует. Единственный надежный способ проверить идентичность ключа состоит в том, чтобы встретиться лицом к лицу с его владельцем. К сожалению, квантовое распределение ключа не дает никаких более удобных способов идентификации, или борьбы с атаками человека в середине канала. Алиса и Боб должны по крайней мере один раз встретиться, чтобы обменяться идентификационным ключом[2].

В дальнейшем мы будем предполагать, что у Алисы и Боба есть доступ к совершенному открытому каналу, но все-таки вернемся, хоть и очень кратко, к проблеме идентификации.

2.2 Квантовое распределение ключа

Мы начнем обсуждение квантового распределения ключа с обзора некоторых общих принципов. За ним последуют более детальное рассмотрение и описания экспериментов в разделе 2.6.

2.2.1 Предварительные замечания

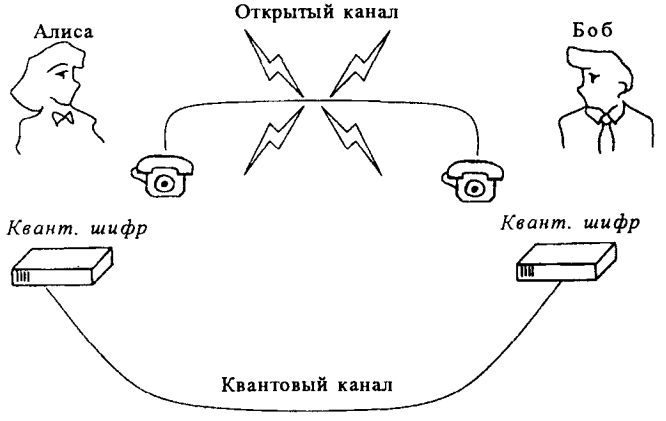


Рис. 2.3. Сценарий распределения квантового ключа. Алиса и Боб связаны двумя каналами, квантовым каналом и классическим открытым каналом.

[2] В обеих ситуациях Алиса и Боб могут довериться третьему лицу, третейскому судье, который обязан сертифицировать цифровые ключи.

Квантовое распределение ключа начинается с пересылки одиночного или перепутанных квантов между Алисой и Бобом. Подслушивание, с физической точки зрения, основано на серии экспериментов, которые подслушивающий агент выполняет на носителях информации, в данном случае на пересылаемых квантах. Согласно правилам квантовой механики, в общем случае любое измерение, выполняемое Евой, неизбежно меняет состояние передаваемых квантов, и Алиса и Боб могут это выяснить в последующей открытой связи[3]. Таким образом, основные составляющие квантового распределения ключа таковы: квантовый канал для обмена квантами и так называемый открытый канал, который используется, чтобы проверить, искажено ли сообщение через квантовый канал (см. Рис. 2.3). Еще раз повторим, что любой открытый канал можно просматривать кому угодно; однако, не должно быть возможно изменять информацию, посылаемую через такой канал.

Во время квантовой пересылки ключ либо закодирован с использованием заданного набора неортогональных квантовых состояний одиночной частицы, либо он получается из заданного набора измерений, выполняемых на перепутанных частицах после пересылки (в этом случае во время пересылки ключ еще даже не существует).

2.2.2 *Защита посредством неортогональных состояний: теорема о запрете клонирования*

Идея использовать неортогональные квантовые состояния для кодирования секретной информации принадлежит Стефану Визнеру, предложившему «квантовые деньги» [37], которые невозможно подделать путем копирования. Это так, потому что невозможно клонировать неортогональные квантовые состояния (или любое неизвестное квантовое состояние). Чтобы это увидеть, рассмотрим два нормированных состояния $|0\rangle$ и $|1\rangle$, таких, что $\langle 0|1\rangle \neq 0$. Предположим, что существует клонирующая машина, которая действует следующим образом:

[3] Здесь возникает законный вопрос: как мы можем быть уверены, что правила квантовой механики верны? Ответ на него состоит в том, что квантовая механика проверялась много раз с очень высокой степенью точности, и на данный момент это самая лучшая теория, которая у нас есть. Не очень разумно просить физиков доказать законы физики в целом и квантовой механики в частности. Конечно, ни одно из экспериментальных подтверждений квантовой механики не делает ее более «верной», но один единственный эксперимент может опровергнуть всю теорию. Рост нашего научного знания основывается на предположениях и опровержениях, и наиболее вероятно, что однажды квантовая механика будет вытеснена новой теорией, однако вряд ли эта новая теория даст новые результаты в современной области приложения квантовой механики. Скорее, новые эффекты будут обнаружены в экстремальных ситуациях, какие встречаются, например, в сильных гравитационных полях.

$$|0\rangle|\textit{бланк}\rangle|\textit{машина}\rangle \rightarrow |0\rangle|0\rangle|\textit{машина}_0\rangle \tag{2.2}$$

$$|1\rangle|\textit{бланк}\rangle|\textit{машина}\rangle \rightarrow |1\rangle|1\rangle|\textit{машина}_1\rangle \ , \tag{2.3}$$

где «бланк» обозначает исходное состояние частицы, которое после действия машины становится клоном, и где все состояния соответствующим образом нормированы. Операция клонирования должна быть унитарной и сохранять внутреннее произведение, так что мы требуем

$$\langle 0|1\rangle = \langle 0|1\rangle\langle 0|1\rangle\langle \textit{машина}_0|\textit{машина}_1\rangle \ , \tag{2.4}$$

что возможно только при $\langle 0|1\rangle = 0$ (два состояния взаимно ортогональны) или при $\langle 0|1\rangle = 1$ (два состояния неразличимы и, следовательно, не могут быть использованы для кодирования двух различных состояний бита), что противоречит нашему исходному предположению. Таким образом, если кто-то секретно приготавливает случайную последовательность состояний типа $|1\rangle|0\rangle|1\rangle|1\rangle\ldots$, где $|0\rangle$ и $|1\rangle$ выбраны случайно, то эту последовательность невозможно достоверно воспроизвести. Деньги Визнера с такими неклонируемыми квантовыми подписями потребовали бы хранения неортогональных квантовых состояний на банкнотах, что гораздо труднее, чем пересылка неортогональнах квантовых состояний из одного места в другое. Вот почему идея Визнера была адаптирована к распределению ключа. Чарльз Беннетт и Жиль Брассар предложили использовать неортогональные состояния фотонов, чтобы распределять криптографические ключи [38]. У любого, кто подслушивает и пытается различить неортогональные состояния $|0\rangle$ и $|1\rangle$, появляется проблема. Предположим, что Ева приготавливает свой измеряющий прибор в исходном состоянии $|\mathrm{m}\rangle$ и хочет отличить $|0\rangle$ от $|1\rangle$, не возмущая эти два состояния, то есть, она хочет выполнить следующую унитарную операцию

$$|0\rangle|\mathrm{m}\rangle \rightarrow |0\rangle|\mathrm{m}_0\rangle \tag{2.5}$$

$$|1\rangle|\mathrm{m}\rangle \rightarrow |1\rangle|\mathrm{m}_1\rangle \ . \tag{2.6}$$

Условие унитарности означает, что $\langle 0|1\rangle\langle \mathrm{m}|\mathrm{m}\rangle = \langle 0|1\rangle\langle \mathrm{m}_0|\mathrm{m}_1\rangle$, то есть, $\langle \mathrm{m}_0|\mathrm{m}_1\rangle = 1$, конечное состояние измеряющего прибора одно и тоже в обоих случаях. Два состояния не возмущены, но Ева не получила никакой информации о закодированном значении бита. Более общее измерение (но все еще не самого общего вида), возмущающее исходные состояния, так что $|0\rangle\rightarrow|0'\rangle$ и $|1\rangle\rightarrow|1'\rangle$, имеет вид

$$|0\rangle|\mathrm{m}\rangle \rightarrow |0'\rangle|\mathrm{m}_0\rangle \tag{2.7}$$

$$|1\rangle|\mathrm{m}\rangle \rightarrow |1'\rangle|\mathrm{m}_1\rangle \ . \tag{2.8}$$

Условие унитарности дает $\langle 0|1\rangle=\langle 0'|1'\rangle\langle \mathrm{m}_0|\mathrm{m}_1\rangle$. Минимум

$\langle m_0|m_1\rangle$, который соответствует ситуации, когда у Евы появляется самый лучший шанс различить два состояния своего прибора, получается при $\langle 0'|1'\rangle=1$, т.е., когда два состояния $|0\rangle$ и $|1\rangle$ после взаимодействия становятся неразличимыми. Хотя только что описанное измерение и не имеет наиболее общего вида, оно представляет собой хорошую иллюстрацию противоречивой связи между информацией, полученной при измерении, и возмущением исходных состояний. Протокол распределения ключа, который использует ее, будет в деталях описан позже.

2.2.3 Защита посредством перепутывания

Концептуальное основание для квантовой криптографии, основанной на перепутывании, обладает совсем другой природой, и включает в себя парадокс Эйнштейна-Подольского-Розена. В 1935 году Эйнштейн, вместе с Борисом Подольским и Натаном Розеном (ЭПР), опубликовали статью, в которой они сделали набросок того, как должна выглядеть «правильная» фундаментальная теория природы [21]. Программа ЭПР включала в себя полноту («в полной теории присутствует элемент, соответствующий каждому элементу реальности»), локальность («реальная фактическая ситуация в системе А не зависит от того, что происходит с системой В, пространственно отделенной от первой»), и определяла элемент физической реальности так: «если, никак не возмущая систему, мы можем с определенностью предсказать значение физической величины, то существует элемент физической реальности, соответствующий этой физической величине». Затем ЭПР рассмотрели мысленный эксперимент на двух перепутанных частицах, который показал, что квантовые состояния не могут во всех ситуациях быть полным описанием физической реальности. Аргумент ЭПР, впоследствии видоизмененный Дэвидом Бомом [15], формируется следующим образом. Представим себе синглетное по спину состояние двух частиц со спином 1/2

$$|\Psi\rangle=\frac{1}{\sqrt{2}}\left(|\uparrow\rangle|\downarrow\rangle-|\downarrow\rangle|\uparrow\rangle\right) , \tag{2.9}$$

где кет-векторы одиночных частиц $|\uparrow\rangle$ и $|\downarrow\rangle$ обозначают спин вверх и спин вниз по отношению к некоторому выбранному направлению. Это состояние сферически симметрично, и выбор направления не имеет значения. Две частицы, которые мы обозначим А и В, испускаются одним источником и разлетаются в разные стороны. После того, как они разлетятся достаточно далеко, так что они уже не будут друг с другом взаимодействовать, мы можем достоверно предсказать значение x-компоненты спина частицы А путем измерения x-компоненты

спина частицы B. Действительно, суммарный спин двух частиц равен нулю, и компоненты спина двух частиц должны обладать противоположными значениями. Измерение, выполненное на частице B не возмущает частицу A (ввиду локальности), следовательно, x-компонента спина есть элемент реальности согласно критерию ЭПР. Точно так же, благодаря сферической симметрии, y, z и любые другие компоненты спина также являются элементами реальности. Однако, поскольку не существует квантового состояния частицы со спином 1/2, в котором все компоненты спина имели бы определенные значения, то квантовое описание реальности неполно.

Программа ЭПР требовала другого описания квантовой реальности, однако, вплоть до установления теоремы Джона Белла (1964) не было ясно, возможно ли такое описание, и, если да, то приведет ли оно к другим предсказаниям результатов экспериментов. Белл показал, что предположения ЭПР о локальности, реальности и полноте несовместимы с некоторыми предсказаниями квантовой механики, касающимися перепутанных частиц [23]. Противоречие выявляется путем вывода из программы ЭПР экспериментально проверяемого неравенства, которое нарушается в некоторых предсказаниях квантовой механики. В разделе 1.7 приведен краткий вывод этого неравенства. Расширение оригинальной теоремы Белла Джоном Клаузером и Майклом Хорном (1974) сделало возможными экспериментальные тесты программы ЭПР [39], и некоторые из них были выполнены. Эксперименты подтвердили предсказания квантовой механики.

Какое это все имеет отношение к защите данных? Как ни удивительно, большое! Оказывается, что тот самый трюк, который был использован Беллом для проверки оснований квантовой теории, может защитить передачу данных от подслушивания! Возможно, это будет звучать не так удивительно, если еще раз вспомнить определение элемента реальности согласно ЭПР: «если, никак не возмущая систему, мы можем с определенностью предсказать значение физической величины, то существует элемент физической реальности, соответствующий этой физической величине». Если эта конкретная физическая реальность используется для кодирования двоичных значений криптографического ключа, то все, чего хочет подслушивающий агент – это элемент физической реальности, соответствующий кодирующей переменной. Таким образом, квантовая криптография на основе перепутывания практически использует квантовое перепутывание и теорему Белла, показывая, что граница между возвышенным и приземленным исследованием весьма размыта. Протокол описан ниже в деталях.

2.2.4 Как насчет зашумленных квантовых каналов?

Безотносительно к типу квантовой связи, вывод таков: совершенный квантовый канал (т.е. квантовый канал без шума) защищен. Любое возмущение в канале есть знак того, что кто-то пытался туда проникнуть. Таким образом, зашумленные сеансы связи надо отбрасывать. К сожалению, квантовые каналы связи очень хрупки, и на практике невозможно избежать некоторого количества вполне невинного шума из-за взаимодействия с окружением. Поэтому, вместо того, чтобы отбрасывать любую зашумленную передачу, «законные» пользователи должны найти процедуру для извлечения секретного ключа, даже в присутствии некоторого количества шума. Для начала, Алиса и Боб должны оценить, сколько информации могло утечь к подслушивающей Еве, как функцию параметров, которые они могут измерить. Это количество информации может быть приемлемым, допустимым, или недопустимым. Под допустимым мы имеем ввиду, что с помощью некоторых последовательных процедур, таких, как усиление секретности или квантовое усиление секретности (см. раздел 8.4), его можно уменьшить до любого желаемого приемлемого уровня, за счет более короткого ключа. Существует, однако, порог, и если слишком много информации утекло к Еве, то никакое последующее усиление секретности невозможно, и сеанс связи следует отбросить. Необходимость в более точном критерии была впервые выдвинута Хаттнером и Экертом [40]; с тех пор квантовое подслушивание развилось в самостоятельную научную область.

Если квантовая передача по зашумленным каналам основана на распределении перепутанных частиц, то усиление квантовой секретности определяет критерии защиты, с учетом самой общей атаки, которую может провестои подслушивающий агент. Усиление квантовой секретности преобразует частично перепутанные частицы (из-за подслушивания или любого внешнего возмущения) в полностью перепутанные, и известно, когда такое очищение квантового перепутывания возможно. Однако, с точки зрения практики, технология, необходимая для выполнения квантового очищения, аналогична той, что требуется для квантового компьютера, и, следовательно, пока недостижима.

Литература о защите информации секретности при передаче одиночных частиц довольно обширна. В начале, обсуждалась только защита от так называемых «некогерентных атак», при которых Ева имеет дело с каждой частицей по отдельности. Но квантовая механика допускает более общий и более мощный тип атак, известный как «когерентные атаки», при которых Еве разрешается использовать кванто-

вый компьютер. Недавно были предложены средства защиты от таких атак. Однако, чем более мощными являются рассматриваемые атаки, тем более жестокими должны быть условия защиты. То же самое относится к оптимизации всего протокола, которая критически важна для практических приложений.

2.2.5 Практические замечания

Квантовой криптографии (КК) препятствуют еще несколько проблем. Первая, общая для большинства приложений, кроме тех, в которых применяются перепутанные пары фотонов (раздел 2.4), состоит в том, что мы до сих пор не умеем создавать чистые однофотонные импульсы. Обычно источником света для КК является просто ослабленный луч лазера. Для такого типа света число фотонов в импульсе есть случайная величина с пуассоновским распределением. Это значит, что некоторые импульсы могут вообще не содержать фотонов, тогда как в других может быть 1, 2, и даже больше фотонов. Импульсов с более чем одним фотоном на импульс следует избегать, так как из них информация может утекать подслушивающему агенту. Чтобы сделать вероятность более чем одного фотона на импульс достаточно низкой, приходится использовать очень слабые импульсы, что, в свою очередь, уменьшает отношение сигнала к шуму. Общепринятая величина равна 0.1 фотона на импульс (это на самом деле означает, что только один импульс из 10 содержит фотон), что дает вероятность получить более, чем один фотон в импульсе, порядка 5×10^{-3}. Это все еще значит, что из 5% пригодных импульсов (тех, в которых есть, по крайней мере, один фотон) информация может утекать к подслушивающему агенту. Разработка хорошего однофотонного источника представляется делом технически возможным, но пока что эта цель не достигнута.

Вторая, более серьезная проблема для практического применения КК состоит в том, что квантовый канал нельзя усилить без потери его квантовых свойств. Следовательно, из-за потерь при передаче, КК может оперировать только на ограниченных расстояниях. Для всех существующих систем, основанных на инфракрасных фотонах в кварцевых световодах, минимальный уровень потерь составляет порядка 0.2 дБ/км. Так что, похоже, что системы КК на расстояниях, превышающих 100 км (с потерями в 20 дБ, и уровнем пропускания 0.01) в обозримом будущем невозможны. Следовательно, трансатлантический кабель с системой секретности на основе КК пока остается полной утопией.

Третья проблема состоит в том, что КК хорошо приложима к свя-

зи между двумя точками, но гораздо хуже применима для других типов сетей. Недавно были предложены некоторые улучшения в этом направлении [41], но они все еще ограничены связью одного пользователя с несколькими другими. Использование КК для связи от дома к дому все еще невыполнимо. Однако, своего рода локальную сеть, с центральной вещательной станцией (например, основное отделение банка) и некоторым числом приемников (например, филиалы банка) вполне можно себе представить.

2.3 Квантовое распределение ключа с одиночными частицами

2.3.1 Поляризованные фотоны

В квантовом распределении ключа с поляризованными фотонами, первоначально предложенном Ч. Х. Беннетом и Г. Брассаром [38, 42], использовались импульсы зеленого света, на расстоянии в 40 см. Здесь мы обсудим эту схему в некоторых деталях. Очевидно, что этот эксперимент был бесполезен с точки зрения практической передачи ключа, но представлял собой первые экспериментальные шаги в КК. Первое практическое воплощение этого конкретного протокола с оптическими световодами (на расстоянии около 1 км) было осуществлено в университете Женевы [43]. В наши дни расстояния достигают величины десятков километров. В этом разделе мы обсудим принципы КК с поляризованными фотонами, оставив экспериментальные реализации для раздела 2.6.

Рассмотрим импульсы поляризованного света, причем в каждом импульсе содержится по одному фотону. Мы начнем с горизонтальной либо вертикальной поляризации, которые будем обозначать квантово-механическим символами Дирака $\langle\leftrightarrow\rangle$ и $\langle\updownarrow\rangle$, соответственно. Чтобы передавать информацию, нам нужна кодирующая система, скажем, $\langle\updownarrow\rangle$ кодирует 0, и $\langle\leftrightarrow\rangle$ кодирует 1. С помощью этой системы отправитель, известный как Алиса, может послать любое сообщение получателю, известному как Боб. Например, если Алиса посылает серию импульсов $\langle\leftrightarrow\rangle$, $\langle\updownarrow\rangle$, $\langle\leftrightarrow\rangle$, $\langle\leftrightarrow\rangle$, $\langle\updownarrow\rangle$; то соответствующее двоичное число равно 10110. Когда она посылает только $\langle\leftrightarrow\rangle$ либо $\langle\updownarrow\rangle$, мы говорим, что Алиса шлет свои фотоны в $\oplus$-базисе. Как и требуется, ключ должен быть случайным. Алиса будет посылать 0 и 1 с равной вероятностью. Чтобы прочитать сообщение, Боб будет использовать поляризационный светоделитель (ПСД), пропускающий вертикальную поляризацию и отражающий горизонтальную. За ним следуют однофотонные детекторы, как показано на Рис. 2.4. Отсчет на детекто-

ре Д0 (Д1) означает, что Алиса послала 0 (1). В этом случае, мы будем говорить, что Боб производит детектирование также и в ⊕-базисе. Поскольку детекторы несовершенны, а также из-за потерь при передаче, часто оба детектора не регистрируют фотон. В этом случае Боб будет сообщать Алисе, что он не смог ничего зарегистрировать, и что соответствующий бит должен быть отброшен. Следовательно, только часть исходных битов будет реально использована, но те, что останутся, должны быть общими у Алисы и Боба. Таким образом, эта система бесполезна для пересылки сообщения, но она может быть использована для пересылки криптографического ключа, для которого единственные требования – это случайность и конфиденциальность.

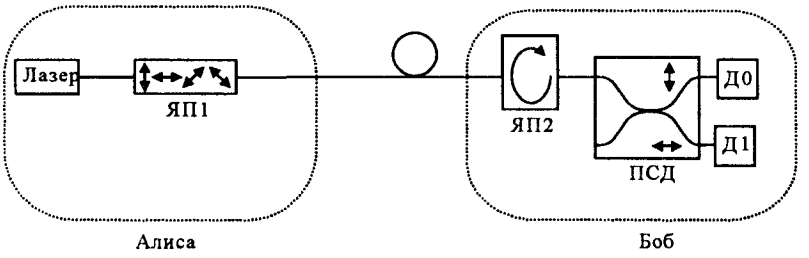


Рис. 2.4. Поляризационная схема: отправитель, Алиса, послает Бобу очень слабые импульсы поляризованного света. Поляризация управляется ячейкой Поккельса (ЯП), которая дает Алисе возможность выбирать между четырьмя возможными поляризациями: $|\updownarrow\rangle$, $|\leftrightarrow\rangle$, $|\nearrow\rangle$, $|\nwarrow\rangle$. На стороне Боба еще одна ячейка Поккельса контролирует поворот схемы: 0° соответствует измерению в ⊕-базисе, 45° соответствует измерению в ⊗ базисе. Поляризационный светоделитель (ПСД) разделяет луч на две ортогональные компоненты, которые детектируются либо Д0, либо Д1 (выбранная схема соответствует измерению в ⊕).

Вплоть до этого места, наша схема остается совершенно незащищенной. Подслушивающая сторона, известная как Ева, могла бы так же измерять импульсы с помощью такой же схемы, как у Боба, и перепосылать такие же импульсы Бобу. Тогда Ева бы узнавала все биты, которые разделяют Алиса и Боб. Чтобы добиться конфиденциальности, Алиса добавляет еще один случайный выбор: она теперь будет посылать либо предыдущие горизонтально-вертикальные поляризации (⊕-базис), либо одну из двух диагональных линейных поляризаций, причем $|\nearrow\rangle$ будет обозначать 0, а $|\nwarrow\rangle$ будет обозначать 1. Как и прежде, Алиса также будет посылать 0 и 1 с одинаковой вероятностью. Эти поляризации соответствуют ⊗-базису. Поворачивая свою схему на 45°, Боб также может решить провести свое измерение в ⊗-базисе. Секретность возникает благодаря фундаментальному свойству квантовой механики: индетерминизму. Одиночный фотонный импульс, приготовлен-

ный в ⊗-базисе и измеренный в ⊕-базисе, может с одинаковой вероятностью попасть на любой из детекторов, Д0 или Д1. И этот выбор совершенно случаен: ничто в фотоне не показывает, по какому пути он пойдет. Поэтому, если Алиса приготавливает фотон, скажем, в состоянии $|\nearrow\rangle$, и Боб (или кто-либо другой) пытается измерить его в ⊕-базисе, то он может с равной вероятностью получить отсчет на любом из детекторов, Д0 или Д1. Подчеркнем, что это вовсе не означает, что в луче $|\nearrow\rangle$ половина фотонов поляризована горизонтально, а другая половина – вертикально. Это было бы несовместимо с тем фактом, что, когда Боб использует ⊗-базис, он всегда получает 0. Фактически, система ведет себя так, как если бы в момент измерения она случайным образом выбирала, по какому пути ей пойти.

Очевидно, что все вышесказанное так же применимо и к Еве. Поскольку Алиса случайным образом выбирает тот или иной базис, для Евы не существует способа определить, в каком базисе проводить измерение. Когда она выбирает неверный базис, она получает случайный результат, который не коррелирует с выбором Алисы. Еще один важный момент состоит в том, что Ева не может узнать, что получила неверный результат: отсчет в Д0 может означать, что фотон был приготовлен в состоянии $|\updownarrow\rangle$, но может также и означать, что фотон был в состоянии $|\nearrow\rangle$ или $|\nwarrow\rangle$ и просто «выбрал» попасть на Д0. Вот почему нам нужны однофотонные импульсы: импульс с более, чем одним фотоном, посланный в неверном базисе, может дать отсчет на обоих детекторах Д0 и Д1, таким образом сообщая Еве, что она использовала не тот базис. Тогда она сможет просто отбросить эту передачу, и таким образом избежать ошибки. Однако когда она получает всего один фотон, то у нее нет другого выбора, кроме как переслать его Бобу в том состоянии, которое она измерила. Это неизбежно создаст ошибки в строке, которую получает Боб. Вышеописанная стратегия подслушивания, известная как стратегия перехвата и повторного отправления, является только одним из вариантов, которые есть у Евы.

Теперь у нас есть основные блоки для протокола поляризационной криптографии, пример которого приведен в таблице 2.1. Весь протокол проиллюстрирован на Рис. 2.5. Его можно резюмировать следующим образом:

1. Алиса случайным образом выбирает базис и поляризацию своих однофотонных импульсов и посылает их Бобу.

2. Для каждого импульса, Боб также случайным образом выбирает базис, который он будет использовать, и измеряет импульс. Он либо регистрирует отсчет на Д0 или на Д1, либо ничего не регистрирует, из-за потерь при связи или при детектировании. Ансамбль всех полученных битов называется сырым ключом.

3. Боб использует открытый канал, чтобы сообщить Алисе, какие фотоны он зарегистрировал, и какой базис при этом использовал. Разумеется, Боб не сообщает результат измерения (отсчет на Д0 или Д1). Алиса отвечает, сообщая, какой базис использовала она. В тех случаях, когда Алиса и Боб использовали один и тот же базис, $\oplus$ или $\otimes$, они должны получить абсолютно коррелированные биты. Однако, из-за несовершенства установки и из-за потенциального подслушивания, возникнет некоторое количество ошибок. Ансамбль этих битов называется просеянным ключом.

4. Чтобы преобразовать свои частично испорченные и, возможно, не вполне секретные строки в пригодный к использованию ключ, Алисе и Бобу теперь нужна некоторая обработка. Фактически, стадия обработки одинакова во всех версиях КК с одиночными частицами. Основные шаги таковы: оценить уровень ошибок при передаче; сделать предположение о максимальном количестве информации, которая могла утечь из-за подслушивания; и затем скорректировать все ошибки, в то же время уменьшая количество информации, потенциально доступное Еве, до любого требуемого уровня. Оставшаяся строка битов и есть секретный ключ.

Таблица 2.1. Пример поляризационного протокола. Алиса случайным образом выбирает базис ($\oplus$ или $\otimes$) и значение бита (0 или 1) и шлет соответствующее поляризационное состояние Бобу. Боб также случайно выбирает базис измерения и получает данный бит. Ансамбль этих битов есть сырой ключ. Затем Алиса и Боб по открытому каналу сообщают друг другу, какой базис они использовали, и оставляют только биты, соответствующие одному и тому же базису. Это – просеянный ключ. Они случайным образом выбирают несколько битов, чтобы проверить, нет ли Евы, и отбрасывают их. В нашем случае ошибок нет, что показывает, что связь была секретной. Оставшиеся биты образуют общий ключ.

Базис А	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$
Значение бита А	0	1	0	1	1	0	1	0	0	0	0
А посылает	$\lvert\nearrow\rangle$	$\lvert\leftrightarrow\rangle$	$\lvert\updownarrow\rangle$	$\lvert\nwarrow\rangle$	$\lvert\leftrightarrow\rangle$	$\lvert\nearrow\rangle$	$\lvert\nwarrow\rangle$	$\lvert\updownarrow\rangle$	$\lvert\nearrow\rangle$	$\lvert\nearrow\rangle$	$\lvert\updownarrow\rangle$
Базис В	$\otimes$	$\oplus$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\oplus$
Бит В	0	1	0	0	1	0	1	1	0	1	0
Тот же базис?	да	да	нет	нет	да	да	да	нет	нет	нет	да
У А остается	0	1			1	0	1				0
У В остается	0	1			1	0	1				0
Проверка Евы	да	нет			да	нет	нет				нет
Ключ		1				0	1				0

Рис.2.5. Диаграмма протокола распределения квантового ключа, основанного на одиночных фотонах.

Поляризационные схемы очень привлекательны в свободном пространстве, где сохраняется поляризация, но их труднее осуществить в оптических волноводах, из-за деполяризации и случайно флуктуирующего двулучепреломления. Деполяризация не является основной проблемой: ее действие можно подавить посредством достаточно когерентного источника. Временная шкала флуктуаций двулучепреломления при стационарных условиях является довольно медленной (1 час). Однако, во время эксперимента на установленном оптическом кабеле, мы наблюдали и гораздо более короткие временные шкалы, которые делали передачу ключа невозможной. Электронная система компенсации, осуществляющая непрерывное отслеживание и исправление поляризации, наверняка возможна, но она требует процедуры со-

гласования между Алисой и Бобом. Это может сделать схему чересчур громоздкой для потенциальных пользователей.

2.3.2 Системы, кодированные по фазе

Вместо того, чтобы полагаться на поляризацию, которую нелегко контролировать в оптических волноводах, можно базировать систему КК на кодировании по фазе. Первоначально фазовое кодирование с оптическими волноводами и интерферометрами Маха-Цандера было введено в контексте квантовой криптографии на основе перепутывания [44], но его также можно использовать и в системах с одиночными частицами [45]. Теоретическая схема показана на Рис. 2.6. Она представляет собой раздвинутый интерферометр Маха-Цандера, с Алисой с левой стороны и Бобом с правой и с двумя связывающими их волноводами. И у Алисы, и у Боба, есть по одному фазовому модулятору (ФМ), которые позволяют им осуществлять кодирование и декодирование. Предположим, что Боб не использует свой ФМ, и что схема настроена так, чтобы создавать конструктивную интерференцию на Д0 и деструктивную на Д1. Если Алиса использует свой ФМ, чтобы создавать сдвиг фазы в 0 или π (соответствующий значению бита 0 или 1), то Боб получит отсчет либо на Д0, либо на Д1. Это эквивалентно предыдущей схеме, в которой используются всего две поляризации. Чтобы достичь конфиденциальности, мы добавляем случайный выбор базиса. Алиса должна выбрать один из четырех сдвигов фазы: 0, π, (что соответствует $\oplus$-базису), или $\pi/2$, $3\pi/2$ (соответствующие $\otimes$-базису). Со своей стороны, Боб также выберет между нулевым сдвигом фазы, т.е., измерением в $\oplus$-базисе, и сдвигом фазы в $\pi/2$, т.е., измерением в $\otimes$-базисе. Это будет эквивалентно предыдущей поляризационной схеме.

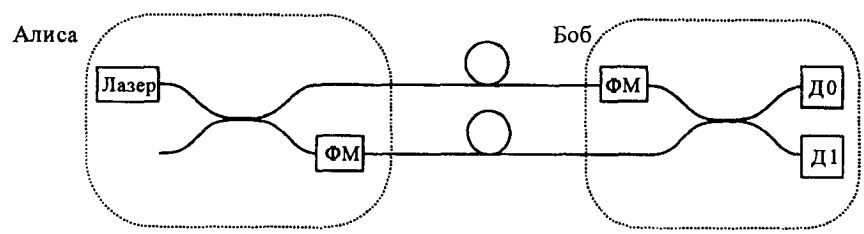


Рис.2.6. Фазовая схема с раздвинутым интерферометром Маха-Цандера. Относительный выбор фазы в двух фазовых модуляторах (ФМ) создает интерференционную картину. Алиса выбирает одну из четырех фаз: 0 или π, что соответствует $\oplus$-базису, либо $\pi/2$ или $3\pi/2$, что соответствует $\otimes$-базису. Боб выбирает либо 0 (соответствует $\oplus$-базису), либо $\pi/2$ (соответствует $\otimes$-базису). Когда Алиса и Боб используют один и тот же базис, отсчет на Д0 обозначает 0, а отсчет на Д1 обозначает 1. В тех же случаях, когда базисы различны, нет никаких корреляций между битом, посланным Алисой и тем, который получил Боб.

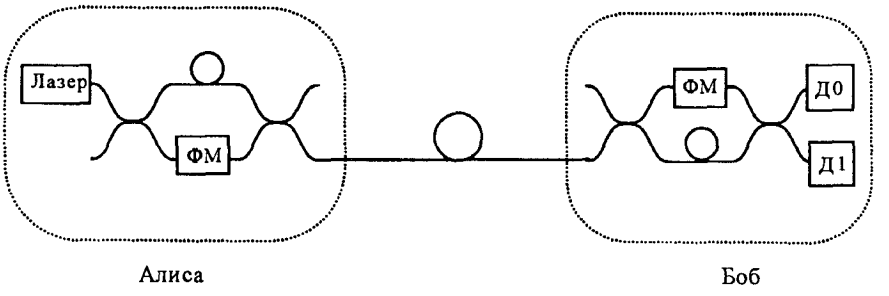


Рис. 2.7. Фазовая схема с переделанным интерферометром Маха-Цандера: Вместо того, чтобы проходить по двум различным путям, два импульса теперь распространяются по одному и тому же световоду, хоть и с задержкой по времени. Такая схема увеличивает стабильность интерферометра, но прибавляет 3 дБ потерь в установке Боба.

К сожалению, сохранить разность фаз в таком раздвинутом интерферометре (длиной более 20 км) очень трудно. Следовательно, с практической точки зрения, лучше переделать интерферометр, как показано на Рис. 2.7. Один импульс, входящий в МЦ со стороны Алисы, делится на два. Получившиеся два импульса распространяющиеся один за другим, от Алисы к Бобу, вдоль одного передающего световода, обозначаются как К (для короткого пути) и Д (для длинного пути). После прохождения через часть МЦ, находящуюся у Боба, из них получаются три импульса. Два из них, обозначаемые как КК (коротко-короткий) и ДД (длинно-длинный) не важны, так как они не приводят к интерференции. В то же время, центральный импульс соответствует двум возможным путям: КД или ДК, которые неразличимы и, следовательно, интерферируют. Как и в предыдущем параграфе, выбор фазовых сдвигов, создаваемых Алисой и Бобом, дает кодирование и декодирование. Такая схема более стабильна, чем предыдущая, поскольку оба импульса фактически идут по одному и тому же пути в большей части интерферометра. Недостаток ее состоит в том, что мы теряем половину сигнала в импульсах ДД и КК.

В схеме, предложенной Ч. Беннетом [45], использовались только две фазы у Алисы. За детальным объяснением мы отсылаем читателя к оригинальной статье. Основное преимущество систем этого типа состоит в том, что для них, в принципе, не требуется контроль поляризации. Однако на практике, из-за некоторой зависимости поляризации от условий в компонентах системы, предпочтительнее ее контролировать. Более того, в этих схемах все еще необходимы тщательная настройка и контроль длины пути между двумя сторонами интерферометра.

2.4 Квантовое распределение ключа с помощью перепутанных состояний

2.4.1 Передача сырого ключа

Распределение ключа выполняется через квантовый канал, который состоит из источника, испускающего пару фотонов в синглетном поляризационном состоянии:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|\updownarrow\rangle|\leftrightarrow\rangle - |\leftrightarrow\rangle|\updownarrow\rangle\right) \tag{2.10}$$

Фотоны разлетаются в разные стороны вдоль оси z по направлению к двум законным пользователям канала, Алисе и Бобу, которые, после того, как фотоны разлетелись, выполняют измерения и регистрируют результат этих измерений в одном из трех базисов, получаемых вращением $\oplus$-базиса вокруг оси z на углы $\phi_1^a = 0$, $\phi_2^a = 1/4\pi$, $\phi_3^a = 1/8\pi$ для Алисы и $\phi_1^b = 0$, $\phi_2^b = -1/8\,\pi$, $\phi_3^b = 1/8\,\pi$ для Боба.

Индексы «*a*» и «*b*» относятся к анализаторам Алисы и Боба, соответственно. Пользователи выбирают свои базисы независимо и случайно для каждой пары приходящих частиц. Каждое измерение дает два возможных результата, +1 (фотон измерен в первом поляризационном состоянии в выбранном базисе) и −1 (он измерен во втором поляризационном состоянии в выбранном базисе), и потенциально может открыть один бит информации.

Величина

$$E\left(\phi_i^a, \phi_j^b\right) = P_{++}\left(\phi_i^a, \phi_j^b\right) + P_{--}\left(\phi_i^a, \phi_j^b\right) -$$

$$-P_{+-}\left(\phi_i^a, \phi_j^b\right) - P_{-+}\left(\phi_i^a, \phi_j^b\right) \tag{2.11}$$

есть коэффициент корреляции измерений, выполненных Алисой в базисе, повернутом на ϕ_i^a и Бобом в базисе, повернутом на ϕ_j^b. Здесь $P_{\pm\pm}(\phi_i^a, \phi_j^b)$ обозначает вероятность, что в базисе, определенном ϕ_i^a, был получен результат ±1, и в базисе, определенном ϕ_j^b, был получен результат ±1. Согласно правилам квантовой механики,

$$E\left(\phi_i^a, \phi_j^b\right) = -\cos\left[2(\phi_i^a - \phi_j^b)\right]. \tag{2.12}$$

Для двух пар базисов одной и той же ориентации (ϕ_1^a, ϕ_1^b и ϕ_3^a, ϕ_3^b) квантовая механика предсказывает полную антикорреляцию результатов, полученных Алисой и Бобом: $E(\phi_1^a, \phi_1^b) = E(\phi_3^a, \phi_3^b) = -1$.

Можно определить величину S, составленную из коэффициентов корреляции, для которых Алиса и Боб использовали анализаторы различной ориентации

$$S = E\left(\phi_1^a, \phi_3^b\right) + E\left(\phi_1^a, \phi_2^b\right) + E\left(\phi_2^a, \phi_3^b\right) - E\left(\phi_2^a, \phi_2^b\right). \tag{2.13}$$

Это та же самая величина S, что и в обобщенной теореме Белла, выдвинутой Клаузером, Хорном, Шимони и Хольтом и известной как неравенство КХШХ [12]. Квантовая механика требует чтобы

$$S = -2\sqrt{2} \,. \tag{2.14}$$

После того, как произошла передача, Алиса и Боб могут публично объявить, какие ориентации анализаторов они выбирали в каждом конкретном эксперименте, и разделить эксперименты на две различные группы: в первой группе будут эксперименты, в которых они использовали отличающиеся ориентации анализаторов, а во второй – те, в которых ориентации анализаторов совпадали. Они также отбрасывают все эксперименты, в которых один из них или они оба вообще не смогли зарегистрировать ни одной частицы. После этого Алиса и Боб могут открыто показать результаты, которые они получили в рамках одной только первой группы экспериментов. Это позволяет им установить значение S, которое, если частицы не были прямо или косвенно «возмущены», должно совпасть со значением (2.14). Такое совпадение дает законным пользователям гарантию, что результаты, полученные ими во второй группе измерений, антикоррелируют и могут быть преобразованы в секретную строку битов – ключ.

Подслушивающий агент, Ева, не может извлечь из частиц никакой информации на их пути от источника к законным пользователям, просто потому, что там никакой информации не закодировано! Информация «рождается» только после того, как законные пользователи выполняют измерения и после этого открыто общаются. Ева может попытаться подставить свои собственные приготовленные данные Алисе и Бобу, чтобы их обмануть, но так как она не знает, какая ориентация анализаторов будет выбрана для данной пары частиц, у нее нет хорошей стратегии, которая позволила бы ей остаться незамеченной. В этом случае ее вмешательство будет эквивалентно введению элементов *физической реальности* в направления поляризации и понизит величину S ниже ее «квантового» значения. Таким образом, теорема Белла может выявить факт подслушивания.

2.4.2 Критерии защиты

Мы лучше всего проанализируем подслушивание в системе, если примем самый удобный для подслушивания сценарий, а именно, что Еве разрешено приготовить все пары, которые Алиса и Боб будут в последствии использовать для установления ключа. Таким образом, мы принимаем наиболее консервативную точку зрения, которая приписывает все возмущение в канале подслушиванию, даже если на самом

деле большая его часть (если не всё возмущение) может происходить от невинного шума, относящегося к окружающей среде.

Начнем наш анализ подслушивания в духе теоремы Белла и рассмотрим простой случай, в котором Ева точно знает, в каком состоянии находится каждая частица. Вслед за работой [46] предположим, что Ева приготавливает каждое состояние в ЭПР парах раздельно, так что каждая отдельная частица в каждой паре обладает четко определенной поляризацией в некотором направлении. Эти направления могут меняться от пары к паре, и можно сказать, что Ева с вероятностью $p(\theta_a, \theta_b)$ приготавливает частицу Алисы в состоянии $|\theta_a\rangle$ и частицу Боба в состоянии $|\theta_b\rangle$, где θ_a и θ_b – это два угла, описывающие поляризации, отложенные от вертикальной оси. Такой тип приготовления дает Еве полный контроль над состояниями *индивидуальных* частиц. Именно в этом случае у Евы всегда есть преимущество, и Алиса и Боб должны избегать установления ключа; они узнают об этом, оценив величину $|S|$, которая в данном случае будет меньше $\sqrt{2}$. Чтобы это увидеть, запишем оператор плотности для каждой пары в виде

$$\rho = \int_{-\pi/2}^{\pi/2} p(\theta_a,\theta_b)|\theta_a\rangle\langle\theta_a|\otimes|\theta_b\rangle\langle\theta_b|d\theta_a d\theta_b \ . \tag{2.15}$$

Уравнение (2.13) с соответствующим образом видоизмененными коэффициентами корреляции выглядит так

$$\begin{aligned} S = \int_{-\pi/2}^{\pi/2} p(\theta_a,\theta_b)d\theta_a d\theta_b \Big\{ &\cos\left[2(\phi_1^a-\theta_a)\right]\cos\left[2(\phi_3^b-\theta_b)\right] \\ &+\cos\left[2(\phi_1^a-\theta_a)\right]\cos\left[2(\phi_2^b-\theta_b)\right] \\ &+\cos\left[2(\phi_2^a-\theta_a)\right]\cos\left[2(\phi_3^b-\theta_b)\right] \\ &-\cos\left[2(\phi_2^a-\theta_a)\right]\cos\left[2(\phi_2^b-\theta_b)\right]\Big\} \ , \end{aligned} \tag{2.16}$$

и приводит к

$$S = \int_{-\pi/2}^{\pi/2} p(\theta_a,\theta_b)d\theta_a d\theta_b \sqrt{2}\cos\left[2(\theta_a-\theta_b)\right] \ , \tag{2.17}$$

что означает

$$-\sqrt{2} \le S \le \sqrt{2} \tag{2.18}$$

для каждого состояния, описываемого распределением вероятности $p(\theta_a, \theta_b)$.

Ясно, что Ева может отказаться от полного контроля квантовых состояний индивидуальных частиц в парах и перепутать по крайней мере некоторые из них. Если бы она собиралась приготовить все пары

в полностью перепутанных синглетных состояниях, то она бы потеряла весь контроль и все знание о данных Алисы и Боба, которые легко смогли бы теперь установить секретный ключ. Этот случай не реалистичен, потому что на практике Алиса и Боб никогда не зарегистрируют $|S|=2\sqrt{2}$. Однако, если Ева приготавливает только частично перепутанные пары, то тогда Алиса и Боб все еще могут установить абсолютно защищенный ключ, при условии, что они используют алгоритм *квантового усиления секретности* (КУС) [47]. Случай частично перепутанных пар, $\sqrt{2} \leq |S| \leq 2\sqrt{2}$, является наиболее важным, и, чтобы утверждать, что у нас есть действующая схема распределения ключа, мы должны доказать, что и в этом конкретном случае можно установить ключ. Опуская технические детали, мы представим только основную идею КУС; детали можно найти в работе [47] и в разделе 8.4.

Во-первых, заметим, что никакие две частицы, находящиеся совместно в чистом состоянии, не могут быть перепутаны ни с каким третьим физическим объектом. Следовательно, любая физическая процедура, которая предоставляет нам ЭПР пары в чистых состояниях, должна была также устранить перепутывание между любой из этих пар и любой другой системой. Схема КУС основана на итерационном квантовом алгоритме, который, если его выполнять с абсолютной точностью, начав с набора ЭПР пар в смешанных состояниях, отбросил бы некоторые из них и приготовил бы оставшиеся в состояниях, сходящихся к чистому синглетному состоянию. Если же (как должно быть в реальности) алгоритм выполняется не вполне совершенно, то оператор плотности для пар, остающихся после каждой итерации, будет сходиться не к синглетному состоянию, но к некоторому близкому к нему состоянию; однако степень перепутывания с любым подслушивающим агентом будет, тем не менее, продолжать падать, и ее можно довести до произвольно малой величины. Алиса и Боб могут выполнять КУС, находясь в удалении друг от друга, путем последовательности локальных унитарных операций и измерений, согласовывая их через открытый канал. КУС можно осуществить с помощью методик, которые в настоящее время разрабатываются (см. [48]).

Существенным элементом процедуры КУС является схема «очищения перепутывания» [49] (см. главу 8). Недавно было показано, что можно очистить любые частично перепутанные состояния частиц с двумя состояниями [50]. Таким образом, если только оператор плотности не может быть записан как смесь произведений чистых состояний, т.е., он не имеет форму (2.15), Алиса и Боб могут перехитрить Еву!

2.5 Квантовое подслушивание

Процедура КУС требует технологии, которая на сегодняшний день еще не вполне развита. Поэтому давайте обсудим другие методы, гораздо более близкие к экспериментальному осуществлению. Эти методы важны, так как мы хотим построить прототипы распределения ключа на основе имеющейся сейчас технологии, и нам надо определить условия, при которых они будут действительно защищенными. Приведенное ниже рассуждение является общим, и его можно применить как к одночастичному, так и к основанному на перепутывании распределению ключей. Однако, в чисто педагогических целях, наше описание будет предполагать одночастичную схему, в которой Алиса посылает Бобу фотоны.

2.5.1 Исправление ошибок

Поскольку важно, чтобы у Алисы и Боба были идентичные строки битов, они должны исправлять расхождения в своих просеянных ключах. Этот шаг, называемый согласованием или исправлением ошибок, может использовать открытый канал, но он должен предоставить Еве настолько мало информации о согласованном ключе, насколько возможно (или использовать настолько мало секретных битов, насколько возможно, если Алиса и Боб решат зашифровать наиболее важную часть своего открытого общения с помощью ранее установленного секретного ключа). Минимальное число r битов, которыми Алиса и Боб должны открыто обменяться, чтобы исправить свои данные, определяется теоремой Шеннона о кодировании [32]: в нашем случае, когда каждый бит передается некорректно с вероятностью ошибки ε, независимо для каждого передаваемого бита, теорема утверждает, что

$$r = n\left(-\varepsilon \log_2 \varepsilon - (1-\varepsilon)\log_2(1-\varepsilon)\right) \tag{2.19}$$

где n обозначает длину просеянного ключа.

У теоремы Шеннона есть неконструктивное доказательство, которое означает, что мы знаем, что существует схема исправления, открывающая всего r битов секретных данных, но теорема не дает нам явной процедуры. Обычные линейные коды, исправляющие ошибки, оказываются в этом отношении довольно неэффективными. Однако, Брассар и Сэлвэйл [51] придумали практическую интерактивную схемы коррекции, которая близко подходит к пределу Шеннона. Эта схема работает следующим образом:

Алиса и Боб группируют свои биты в блоки определенного размера, который должен быть оптимизирован как функция уровня ошибок.

Они обмениваются информацией о четности каждого блока по открытому каналу. Если их четности согласуются, то они переходят к следующему блоку. Если четности не согласуются, то они заключают, что в соответствующем блоке было сделано нечетное количество ошибок, и ищут одну из них рекурсивно, разрезав блок на два подблока и сравнивая четности в первом подблоке: если четности совпадают, то второй подблок содержит нечетное число ошибок, а если различаются, то нечетное число ошибок содержится в первом блоке. Эта процедура рекурсивно продолжается в подблоке с нечетным числом ошибок.

После этого первого шага каждый рассматриваемый блок содержит либо четное число ошибок, либо ни одной. Затем Алиса и Боб перетасовывают положения своих битов и повторяют ту же процедуру с блоками большего размера (этот размер также оптимизируется). Однако если исправляется ошибка, то Алиса и Боб могут заключить, что в некоторых ранее рассмотренных блоках теперь содержится нечетное число ошибок. Они выбирают наименьший из этих блоков и рекурсивно, как и раньше, исправляют одну ошибку. Так они поступают до тех пор, пока в каждом ранее рассмотренном блоке не окажется либо четное число ошибок, либо ни одной.

Далее продолжаются аналогичные шаги, и интерактивное исправление ошибок останавливается после определенного числа шагов. Это число шагов должно быть оптимизировано, чтобы максимизировать вероятность, что не осталось никаких расхождений, и, в то же время, минимизировать утечку секретных данных. В отличие от схемы исправления, использованной в оригинальной работе [42], эта схема исправления не отбрасывает ни одного бита из просеянного ключа.

2.5.2 Усиление секретности

К этому моменту у Алисы и Боба есть, с высокой вероятностью, идентичный согласованный ключ. Они также точно знают уровень ошибок $\bar{\varepsilon}$, который дает очень хорошую оценку для вероятности ошибки ε. Алиса и Боб предполагают, что все ошибки были вызваны потенциальным подслушивающим агентом, Евой. Кроме того, они учитывают утечку во время шага исправления ошибок, если они есть. Отсюда они выводят τ, число битов, на которое надо сократить согласованный ключ, чтобы уменьшить информацию Евы о конечном ключе ниже заданного значения. Точнее говоря, в большинстве протоколов квантового распределения ключа, для данного целого τ Алиса случайно выбирает матрицу K размера $(n - \tau)\times n$ (со значениями 0 или 1) и открыто передает K Бобу (не зашифровывая ее). Конечный секретный ключ тогда равен

$$\mathbf{k}_{\text{конечный}} = K \cdot \mathbf{k}_{\text{согласованный}} (\text{mod } 2) \qquad (2.20)$$

где $\mathbf{k}_{\text{согласованный}} = (k_1, k_2, \ldots k_n), k_i \in \{0,1\}$ обозначает согласованный ключ.

Осуществить усиление секретности легко, но доказательство защищенности всего протокола квантового распределения ключа является трудной теоретической задачей квантовой криптографии. Поэтому доказательства защищенности предлагались по нарастающей против все более и более мощных атак. Обычно мы делим эти атаки на две категории:

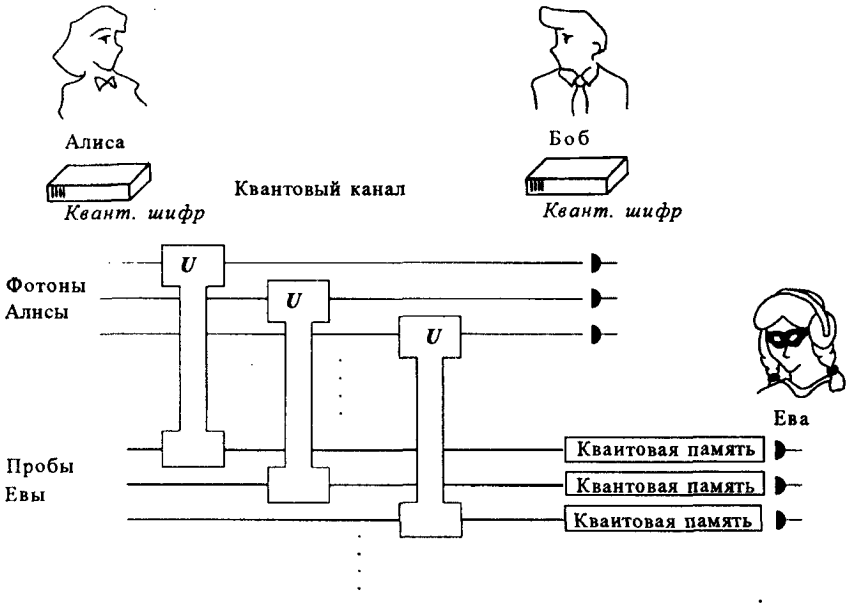


Рис. 2.8. Некогерентные атаки: каждый фотон независимо перепутывается с 2-кубитной пробой. Пробы хранятся в квантовой памяти вплоть до объявления базисов измерений. Тогда каждая проба измеряется независимо от других.

1. Некогерентные атаки (Рис 2.8). В некогерентных атаках, или одночастичных атаках, Ева ограничена перепутыванием квантовой пробы $\mathcal{P}_i$ с одним фотоном за один раз. Она может сохранять $\mathcal{P}_i$ до тех пор, пока Боб не измерит перепутанный фотон и не завершатся все открытые сообщения между Алисой и Бобом. Разумеется, Алиса и Боб не могут сказать, когда Ева измеряет свои пробы – до или после того, как Боб измеряет свои фотоны. Следовательно, наилучшей стратегией для Евы будет подождать, пока Алиса и Боб открыто объявят базисы измерения, и тогда по-умному измерить свои пробы, чтобы извлечь как можно больше информации. Однако в некогерентных атаках Ева ограничена тем, что должна измерять все $\mathcal{P}_i$ индивидуально.

Более детально, принимая в расчет сценарий, представленный в разделе 2.3.1 и обозначая начальное состояние пробы у Евы через $|E\rangle_i$, наиболее общее унитарное преобразование $\mathcal{U}$, перепутывающее $\mathcal{P}_i$ с фотоном Алисы выглядит (в $\oplus$-базисе) как

$$|E\rangle_i|\updownarrow\rangle \xrightarrow{\mathcal{U}} |E_{00}^{\oplus}\rangle|\updownarrow\rangle + |E_{01}^{\oplus}\rangle|\leftrightarrow\rangle \tag{2.21}$$

$$|E\rangle_i|\leftrightarrow\rangle \xrightarrow{\mathcal{U}} |E_{10}^{\oplus}\rangle|\updownarrow\rangle + |E_{11}^{\oplus}\rangle|\leftrightarrow\rangle \ , \tag{2.22}$$

где символы $|E_{ij}^{\oplus}\rangle$ обозначают ненормализованные состояния $\mathcal{P}_i$. Поскольку можно выбрать $|E\rangle_i$ из покрытия $\{|E_{ij}^{\oplus}\rangle\}_{i,j}$, мы можем предположить, что $\mathcal{P}_i$ описываются 4-мерным гильбертовым пространством, т.е., каждая проба описывается двумя кубитами.

Если Алиса шлет свой фотон в $\otimes$-базисе, то действие $\mathcal{U}$ выводится из (2.21, 2.22) с помощью линейности:

$$|E\rangle_i|\nearrow\rangle \xrightarrow{\mathcal{U}} |E_{00}^{\otimes}\rangle|\nearrow\rangle + |E_{01}^{\otimes}\rangle|\nwarrow\rangle \tag{2.23}$$

$$|E\rangle_i|\nwarrow\rangle \xrightarrow{\mathcal{U}} |E_{10}^{\otimes}\rangle|\nearrow\rangle + |E_{11}^{\otimes}\rangle|\nwarrow\rangle \ , \tag{2.24}$$

где

$$|E_{00}^{\otimes}\rangle = \frac{|E_{00}^{\oplus}\rangle + |E_{10}^{\oplus}\rangle + |E_{01}^{\oplus}\rangle + |E_{11}^{\oplus}\rangle}{2} \tag{2.25}$$

$$|E_{01}^{\otimes}\rangle = \frac{|E_{00}^{\oplus}\rangle + |E_{10}^{\oplus}\rangle - |E_{01}^{\oplus}\rangle - |E_{11}^{\oplus}\rangle}{2} \tag{2.26}$$

$$|E_{10}^{\otimes}\rangle = \frac{|E_{00}^{\oplus}\rangle - |E_{10}^{\oplus}\rangle + |E_{01}^{\oplus}\rangle - |E_{11}^{\oplus}\rangle}{2} \tag{2.27}$$

$$|E_{11}^{\otimes}\rangle = \frac{|E_{00}^{\oplus}\rangle - |E_{10}^{\oplus}\rangle - |E_{01}^{\oplus}\rangle + |E_{11}^{\oplus}\rangle}{2} \tag{2.28}$$

Ева должна выбрать такое преобразование $\mathcal{U}$, что

1. подслушивание остается осторожным, т.е., например, вероятность, что Боб измеряет $|\updownarrow\rangle$, тогда как Алиса отправила $|\leftrightarrow\rangle$, не должна превышать допустимого уровня ошибки. Можно увидеть, что это требование эквивалентно тому, что нормы $\langle E_{ij}^{\oplus}|E_{ij}^{\oplus}\rangle$ и $\langle E_{ij}^{\otimes}|E_{ij}^{\otimes}\rangle$, $i \neq j$, должны быть малы (эти вероятности обычно называют помехами).

2. подслушивание эффективно, т.е. Ева должна максимизировать вероятность угадать правильное значение бита, зная использованный базис (она узнала его из открытого канала) и, соответственно, измеряя свою пробу. Например, предположим, что Ева узнает, что i-ый фотон был послан в $\oplus$-базисе. Тогда она знает, что если значение со-

ответствующего бита у Алисы равно 0, то у Евы проба $\mathcal{P}_i$ должна быть в смешенном состоянии:

$$\rho_0 = \mathrm{Tr}_{\text{фотон}}\left[\left(\mathcal{U}|E\rangle_i|\updownarrow\rangle\right)\left(\mathcal{U}|E\rangle_i|\updownarrow\rangle\right)^{\dagger}\right] \tag{2.29}$$

$$= \left|E_{00}^{\oplus}\right\rangle\left\langle E_{00}^{\oplus}\right| + \left|E_{01}^{\oplus}\right\rangle\left\langle E_{01}^{\oplus}\right| \ . \tag{2.30}$$

Аналогично, если Алиса отправила свой фотон в состоянии $\leftrightarrow$ (соответствующем значению бита 1), то у Евы проба должна быть в смешанном состоянии:

$$\rho_1 = \mathrm{Tr}_{\text{фотон}}\left[\left(\mathcal{U}|E\rangle_i|\leftrightarrow\rangle\right)\left(\mathcal{U}|E\rangle_i|\leftrightarrow\rangle\right)^{\dagger}\right] \tag{2.31}$$

$$= \left|E_{10}^{\oplus}\right\rangle\left\langle E_{10}^{\oplus}\right| + \left|E_{11}^{\oplus}\right\rangle\left\langle E_{11}^{\oplus}\right| \ . \tag{2.32}$$

Следовательно, Ева должна решить, настолько верно насколько это возможно, находится ли ее проба $\mathcal{P}_i$ в состоянии ρ_0 или ρ_1. Известно [52, 53] что это решение достигается с помощью измерения на пробе $\mathcal{P}_i$. Измеренная переменная определяется ее собственными векторами, которые, в данном случае, совпадают с собственными векторами $\rho_0 - \rho_1$.

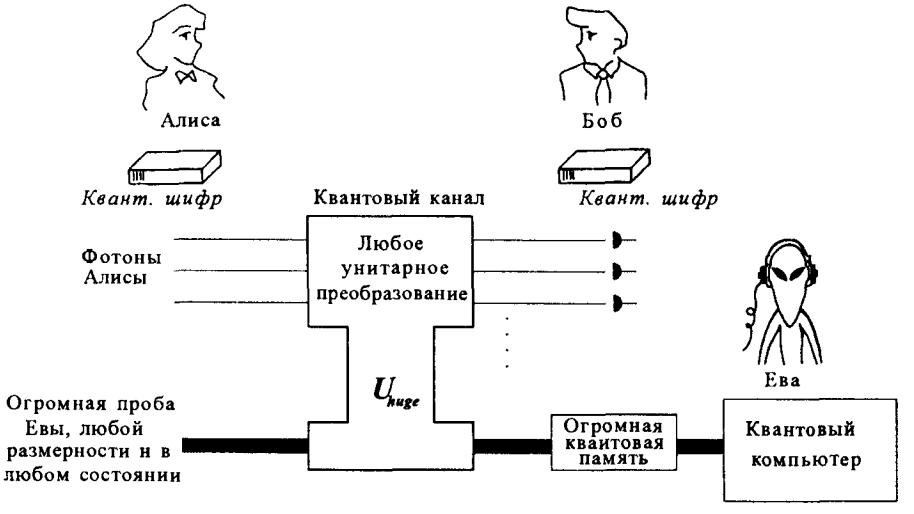


Рис.2.9. Когерентные атаки: Еве разрешено использовать пробу любой размерности в любом начальном состоянии и перепутывать ее с фотоном, посланным Алисой, любым унитарным образом. Эта проба хранится вплоть до объявления базисов.

Оптимизация этого перепутывания тщательно обсуждалась в работах [52]-[56] для различных протоколов однофотонного квантового

распределения ключа. Результаты этих работ связывают вероятность ошибки в квантовом канале (или помех) с максимальной информацией, которую могла получить Ева. Зная эту величину (точнее говоря, связанную с ней величину, называемую информацией Реньи) можно использовать обобщенную теорему об усилении секретности [57], чтобы вычислить параметр сжатия τ, гарантирующий ожидаемую степень конфиденциальности. Утечка информации считается допустимой, если τ достаточно мало по сравнению с размером согласованного ключа.

2. Когерентные атаки (Рис. 2.9): при когерентных или совместных атаках Ева может любым унитарным образом перепутывать пробу любой размерности и в любом состоянии со *всей последовательностью* передаваемых фотонов. Она удерживает эту большую пробу до тех пор, пока не закончатся открытые обсуждения, и затем производит наиболее общее измерение по своему выбору. Самый общий класс измерений называется положительно определенными операторными мерами (ПООМ), их более подробное описание можно найти, например, в работе [58].

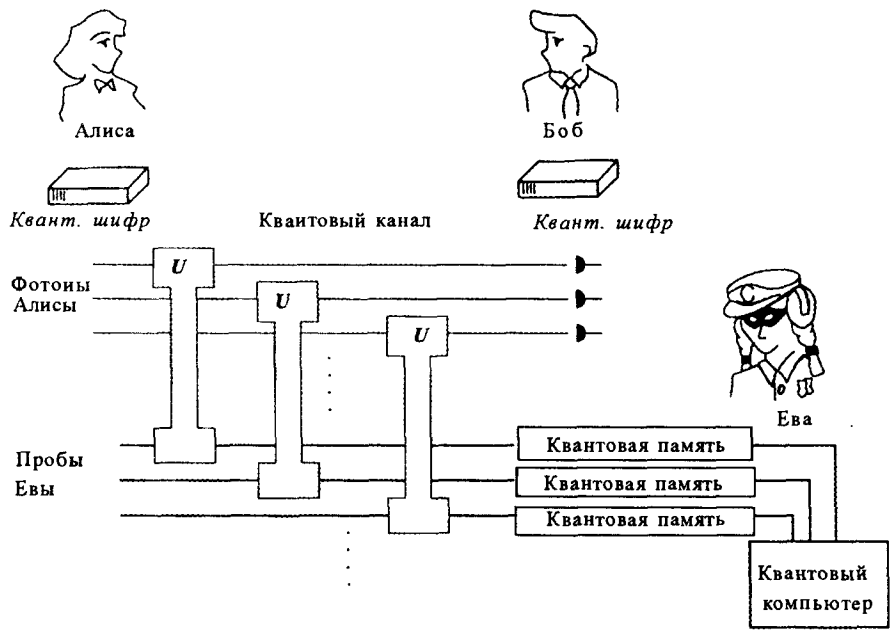


Рис. 2.10. Коллективные атаки: аналогично когерентным атакам, но теперь Еве разрешено сделать глобальное обобщенное измерение на всех пробах, рассматриваемых как единая квантовая система.

Коллективные атаки (Рис. 2.10) образуют подкласс когерентных атак, в котором каждый фотон Алисы *i* индивидуально перепутывает-

ся с отдельной пробой $\mathcal{P}_i$. Следовательно, Ева получает пробы в таких же состояниях, как и при некогерентных атаках. Однако после того, как завершены все открытые обсуждения, Еве разрешается провести любое ПООМ на всех пробах, рассматриваемых как большая единая квантовая система. Заметим, что при коллективной атаке перед этим ПООМ, индивидуальные пробы $\mathcal{P}_i$ неперепутаны и независимы друг от друга. Трудно доказать утверждения о защите от когерентных атак. На сегодняшний день рассмотрены только линейные протоколы исправления ошибок, а не интерактивное исправление ошибок. Доказательство надежности таких протоколов при защите от коллективных атак можно найти в работе [59], а против общих когерентных атак – в работе [60].

Идентификация: Как мы уже говорили, Алиса и Боб должны идентифицировать свою связь, чтобы сосчитать возможные атаки со стороны человека между ними. Они должны также убедиться, что они эффективно владеют новым секретным ключом. К счастью, существуют классические криптографические методики, решающие эти задачи с произвольно высокой вероятностью. Здесь мы даем сжатое описание алгоритма идентификации. За дальнейшими деталями отсылаем читателя к работе [61]. Общее обсуждение идентификации можно найти в работе [30].

Мы предполагали, что у Алисы и Боба есть общий идентификационный ключ **A**, который является секретной строкой двоичных чисел. Этот ключ короче, чем новый секретный ключ, созданный с помощью квантового распределения ключа, но мы предполагаем, что его длины достаточно для целей идентификации.

Выбрано целое число t: это параметр защиты. Предположим, что Алиса хочет идентифицировать для Боба данные $\mathbf{M}_0$. Например, двоичная строка $\mathbf{M}_0$ содержит заранее определенные куски их открытых сообщений. Строка $\mathbf{M}_0$ длины m делится на подблоки P_i длины $2s$, где $s = t + \log_2\log_2 m$ (последний подблок при необходимости заполняется нулями). Алиса и Боб берут первые $2s$ битов из **A**, которые определяют число a. Следующие $2s$ битов из **A** определяют число b. Эти $4s$ битов отбрасываются из **A**. Затем Алиса и Боб для каждого подблока P_i вычисляют

$$p_i' = ap_i + b \pmod{2^s}\ , \tag{2.33}$$

где p_i обозначает число, представленное двоичной строкой P_i.

Получившиеся числа p_i' преобразуются в потоки битов длины s и состыковываются, вместе образуя $\mathbf{M}_1$. Эта операция повторяется (с неизменным s) r раз, пока $\mathbf{M}_r$ не станет длины s. t битов низшего порядка из $\mathbf{M}_r$ образуют ярлык T. Оставшаяся часть **A** отбрасывается и никогда больше не используется.

Наконец, ярлык T посылается Бобу, который проверяет идентичность $\mathbf{M}_0$, проделав те же вычисления и сравнив результаты.

Можно осуществить идентификацию в протоколе квантового распределения ключа следующим образом. Алиса идентифицирует заранее определенные куски открытых сообщений. Боб делает то же самое, с другими заранее определенными кусками. Если эта идентификация проходит успешно, то квантовое распределение ключа считается успешным, и можно использовать небольшую часть нового ключа в качестве идентификационного ключа для следующего сеанса распределения. Таким образом, Алисе и Бобу не надо еще раз встречаться, чтобы установить новый идентификационный ключ. Предположим, что Ева предприняла атаку как человек, находящийся между ними. У Евы есть общий секретный ключ с Алисой, и еще один общий секретный ключ с Бобом. Она знает набор данных $\mathbf{M}_0$, идентифицированный Алисой, так как она изображала перед Алисой Боба в течение всего протокола. Однако, можно показать, что, получив T и зная $\mathbf{M}_0$, Ева может угадать идентификационный ключ с ничтожной вероятностью. Следовательно, Ева не сможет пройти тест на идентификацию.

2.6 Экспериментальные реализации

После того как группами из Монреаля – IBM [42] (распределение ключа с использованием поляризованных фотонов и распространения света в свободном пространстве) и Оксфорда – DERA [44] (перепутанные фотоны, распространение по оптическим волокнам, фазовая кодировка) были выполнены пионерские эксперименты, развитие квантовой криптографии продолжалось по двум направлениям. С одной стороны, ставилась задача оптимизации систем, относительно расстояния связи, скорости генерации ключа и возникновения ошибки в квантовом бите (QBER). С другой стороны, одновременно с этим предпринимались попытки построения стабильных систем, более простых с точки зрения потенциальных пользователей, больше интересующихся защищенностью связи, нежели квантовой механикой и проблемами оптического согласования. Как было показано в предыдущих разделах, общие идеи, стоящие в основе различных реализаций, очень похожи, за исключением ЭПР-схем, отличающихся, главным образом, типом модуляции или используемым анализом. Далее мы рассмотрим некоторые усовершенствования ключей, на которых основана современная квантовая криптография.

Кроме достижения максимальной надежности передающих и принимающих модулей главной целью является увеличение расстояния связи. Вообще говоря, здесь имеется две возможности. Первая со-

стоит в установлении прямого оптического канала между Алисой и Бобом и передачи сигнала в свободном пространстве путем использования телескопов. Во второй – применяются оптические волокна, по которым свет передается из одной точки в другую. Выбор метода передачи в той или иной степени диктуется используемой длиной волны. Оптические волокна имеют весьма малое поглощение в так называемых телекоммуникационных окнах в диапазоне около 1300нм (0.35*дБ/км*). Однако, необходимые для этого режима фотонные детекторы, пока недостаточно эффективны [62]. Криптография, использующая передачу через свободное пространство посредством спутников, находящихся на близлежащих околоземных орбитах, может охватывать любые расстояния. Первичные тесты, выполненные на земле, показывают, что такого рода квантово-криптографическая передача в принципе, возможна, по крайней мере, для невысоких значениях чисел передаваемых битов.

2.6.1 Кодирование поляризации

В первой установке по квантовой криптографии в протоколе распределения ключа использовались различные поляризационные состояния. На стандартной оптической скамье длиной 1м Алиса генерировала слабые световые импульсы при помощи обыкновенного светодиода (СД) и пропускала коллимированный свет через интерференционный фильтр (550±20нм) и поляризатор. Используя две ячейки Поккельса, она могла выбрать одно из четырех состояний поляризации (горизонтальное, вертикальное, лево- и право-циркулярное). В ячейке Поккельса величина двулучепреломления определенного кристалла зависит от приложенного электрического поля. Как правило, необходимы достаточно высокие напряжения порядка 2-4кВ для поворота поляризации на 90^0, скажем от горизонтальной поляризации к вертикальной (что на практике ограничивает скорость переключения). На выходе квантового канала длиной 32см Боб мог анализировать состояние поляризации, используя свои ячейки Поккельса и детектируя фотоны при помощи фотоумножителей, расположенных после призмы Волластона.

По мнению авторов этой работы, даже если подслушивающее устройство могло разрушить систему при подслушивании шума, создаваемого ячейками Поккельса, все равно в этом первом демонстрационном эксперименте уже проявляется множество привлекательных особенностей квантовой криптографии. С самого начала было показано, какой может быть и должна быть простая экспериментальная реализация квантовой криптографии для того чтобы любой пользователь квантовой коммуникационной системы смог более эффективно ее применять.

Более того, была достигнута относительная ошибка на уровне 4.4%, что позволило распределять, после коррекции ошибки, ключ по 219 надежным битам за время 85 секунд.

Для того чтобы обеспечить большее расстояние связи между Алисой и Бобом, в эксперименте Мюллера и др. [43] было использовано оптическое волокно длиной 1км. Однако, при работе с поляризационной кодирующей системой, основанной на оптическом волокне, необходимо преодолеть ряд препятствий. С одной стороны, анализатор Боба должен оставаться согласованным с поляризацией света, посылаемого Алисой; с другой стороны, поляризация света будет изменяться при прохождении по оптоволоконному кабелю. Топологические эффекты, вызванные геометрией светового пути, будут влиять на конечное состояние поляризации света, выходящего из оптоволокна со стороны Боба [63]. К тому же, двулучепреломление, наведенное механическими напряжениями, вызывает и флуктуации конечной поляризации, и уменьшение степени поляризации из-за дисперсии поляризационной моды. Это приводит к необходимости использования одномодовых лазеров для получения достаточно большого времени когерентности и активной стабилизации поляризации между Алисой и Бобом. И наконец, необходим тщательный отбор различных компонентов передающих и приемных модулей для минимизации любой внутренней поляризационной зависимости.

Недавно в системах с распространением света в свободном пространстве началось использование высокой стабильности поляризационных кодирующих модулей. Поскольку в атмосфере отсутствует двулучепреломление, не нужно заботиться о флуктуациях в согласовании между модулями Алисы и Боба. Квантовая криптография, основанная на открытых оптических путях [64], в основном, сталкивается с проблемой прохождения света через турбулентную атмосферу и детектирования единичных фотонов на фоне сильного шума. Сочетание узкополосной частотной и пространственной фильтрации с наносекундной техникой должно позволить осуществить генерацию ключа с приемлемыми величинами относительной ошибки. В проведенном недавно группой из Лос-Аламоса эксперименте была достигнута 14%-ая эффективность связи на расстоянии 950м в свободном пространстве; в итоге получена скорость передачи битов в 50Гц (частота повторения импульсов передатчика Алисы составляла 20кГц) с ошибкой порядка 1.5 [65]. Этот эксперимент демонстрирует осуществимость создания секретного ключа с помощью спутника, находящегося на низкой околоземной орбите, по крайней мере в ночное время и с приемлемой скоростью передачи битов.

2.6.2 Кодирование фазы

Как уже отмечалось в разд.2.3.2 фазовая кодировка может быть реализована аналогично поляризационной. Крайне высокая чувствительность к любым внешним воздействиям установки на основе интерферометра Маха-Цандера, показанной на рис. 2.6, может быть преодолена при использовании разбалансированной конфигурации интерферометра Маха-Цандера, предложенной Беннетом [45]. Поскольку два когерентных вклада впоследствии разделяются лишь на несколько фемтосекунд, распространяясь при этом по одному волокну, то они не подвергнуты никаким температурным или механическим флуктуациям. Разность оптических путей в разбалансированном интерферометре Боба должна быть такой же, как и в интерферометре Алисы и оставаться постоянной с точностью до долей длины волны. Это, однако, требует, лишь тщательной локальной температурной стабилизации двух интерферометров.

В настоящее время коммерчески выпускаются фазовые модуляторы для двух телекоммуникационных длин волн, что по-видимому, делает выбор в пользу стандартных фазовых кодирующих систем при реализации каналов на основе оптоволокна. Однако, в таких схемах также необходимо тщательное поляризационное согласование. Разумеется, в двух разбалансированных интерферометрах Маха-Цандера поляризация должна устанавливаться так, чтобы интерферирующие компоненты имели одинаковую поляризацию на выходном светоделителе Боба. После исходного согласования блоков Алисы и Боба все должно быть стабильно и не вызывать никаких проблем. Более серьезная трудность обусловлена тем фактом, что фазовые модуляторы сделаны из электрооптических кристаллов, которые обеспечивают лишь одно из двух направлений поляризации. Для того, чтобы избежать флуктуаций интенсивности на выходе у Боба, через модулятор можно пропускать лишь одну строго определенную поляризацию. Это возвращает нас к необходимости управления прошедшей поляризацией.

В своих экспериментах Таунсэнд и др. [66] впервые расщепили входной лазерный импульс (1.3 μ, 80 пс) на два, распространяющихся по двум плечам разбалансированного интерферометра Маха-Цандера Алисы. В соответствии с протоколом BB84, фазовый модулятор, находящийся в одном из плеч, вызывает один из четырех возможных фазовых сдвигов. Поляризация в другом плече поворачивается так, чтобы на выходном светоделителе Алисы два вклада имели *ортогональные* поляризации. Входной светоделитель Боба заменен на поляризационный светоделитель, чтобы обеспечить правильную поляризацию в плече, содержащем фазовый модулятор Боба. Контроллер

поляризации в конце линии передачи устанавливается так, чтобы эти два направления поляризации были согласованы с осями выходного светоделителя Боба. Не смотря на то, что стабилизация поляризации по-прежнему необходима, согласование не является таким строгим, поскольку малые отклонения вызывают лишь небольшие флуктуации в конечной интенсивности. Достигнутые уровни ошибок составили менее 4% при частоте повторения импульсов 1МГц. Всевозможные усовершенствования схемы при передаче на расстояние более 48км с помощью подземного кабеля, выполненные группой из Лос-Аламоса, позволили достигнуть уровня ошибок около 1% при частоте импульсов 30КГц.

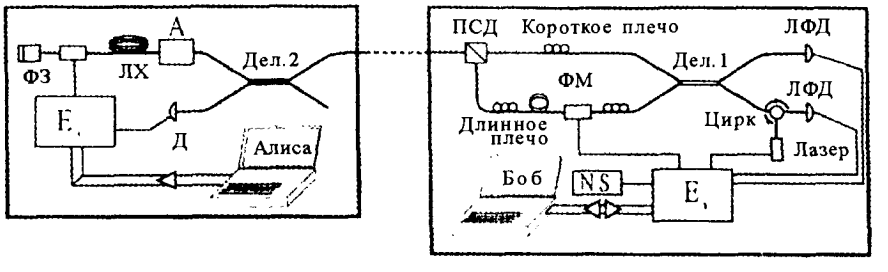


Рис.2.11. Принцип квантовой криптографии plug & play. Боб посылает световой импульс через циркулятор. Этот импульс расщепляется на делителе Дел.1. Первая половина направляется по короткому пути. Контроллер поляризации устанавливается так, чтобы этот импульс полностью проходил через поляризационный светоделитель ПСД. Затем, он распространяется к Алисе, где расщепляется снова на делителе Дел.2 для обеспечения сигнала синхронизации. Далее, он проходит через аппаратуру Алисы и отражается обратно к Бобу. Благодаря действию фарадеевского зеркала, компенсируется двулучепреломление оптического звена и импульс возвращается назад ортогонально поляризованным. Затем он отражается поляризационным светоделителем ПСД и идет в длинное плечо, где Боб вводит фазовый сдвиг с помощью модулятора ФМ. Второй импульс распространяется по двум плечам в обратной последовательности. Алиса вводит фазовый сдвиг. Поскольку оба импульса распространяются вдоль одних и тех же оптических путей, они оказываются у делителя Дел.1 одновременно с идентичными поляризациями, что приводит к интерференции. Линия хранения ЛХ введена в систему Алисы, чтобы избежать проблем, связанных с рэлеевским рассеянием назад.

В так называемой системе «plug & play» нет необходимости постоянного согласования поляризации в волоконной передающей линии. Идея, лежащая в основе, состоит в том, что световой импульс излучается не Алисой, а Бобом; импульс сначала распространяется к Алисе, где он модулируется, а затем отражается назад к Бобу. Если отражатели выполнены на основе *фарадеевских зеркал*, то поляризации интерферирующих компонент на выходе Боба всегда согласованы между собой.

Фарадеевское зеркало, т.е. 45^0-ый ротатор Фарадея и отражающее назад зеркало, формирует отраженную поляризацию ортогональную поляризации света, направляемого в волокно; таким образом любые изменения поляризации вдоль линии передачи или внутри интерферометра эффективно подавляются.

Система, реализующая на основе этой идеи протокол BB84 с четырьмя состояниями, показана на рис.2.11 и рассматривается в [68]. В этом эксперименте Алиса и Боб были разнесены на расстояние 23км при использовании стандартного телекоммуникационного оптоволоконного кабеля, игравшего роль линии передачи. Без какой бы то ни было активной стабилизации был достигнут уровень ошибки менее 1% при уровне формирования сетевого ключа в 210Гц. Во всех этих экспериментах на длинах телекоммуникационных волн порядка 1300нм, основная часть шума была вызвана высоким фоном темновых отсчетов в однофотонных детекторах (InGaAs/InP лавинные фотодиоды, охлаждаемые до 173К, т.е. в пределах возможностей охлаждения элементами Пельте). Использование синхронизации и стробируемой электронной приемной системы позволяет уменьшить уровень шумов, однако на последующее практическое использование квантовой криптографии огромное влияние окажет совершенствование детекторов.

2.6.3 Квантовая криптография, основанная на перепутывании

При использовании неклассических свойств перепутанных пар частиц становится (см. разд.2.4) возможной реализация ряда новых особенностей криптографии. Однако, на основе существующей технологии построить такие схемы оказывается значительно труднее, чем рассмотренные выше, одночастичные, в основном, из-за необходимости генерировать состояния с высокой степенью перепутывания. Неполное перепутывание между фотонами, поступающими к Алисе и Бобу, может быть улучшено только при использовании техники очищения перепутывания, которая, при современном уровне развития технологии, не может быть реализована. Таким образом, любой шум, сопровождающий перепутывание, непосредственно влияет на характеристики системы. С момента первой демонстрации [44] основной целью было усовершенствование источника перепутанных фотонных пар. В настоящее время таким источником пар фотонов служит процесс параметрического рассеяния света. Из-за низкой эффективности этого процесса для получения достаточного уровня битов приходится использовать широкополосное излучение. Отсюда, необходим поиск компромисса, позволившего бы избежать проблем, возникающих при передаче фотонных пар через диспергирующее оптическое волокно.

В большинстве подходов используется перепутывание между энергией и временем (детали см. в [69, 70]). Если пара фотонов рождается в процессе параметрического рассеяния, то может возникнуть нелокальная интерференция между выходами двух разбалансированных, но при этом идентичных, интерферометров Маха-Цандера или Майкельсона. При этом разность оптических путей в каждом интерферометре должна быть меньше, чем длина когерентности лазера накачки. Для разделения вкладов интерферирующих и неинтерферирующих компонент требуется временная селекция. Минимальное время разрешения существующих счетчиков фотонов составляет порядка 300пс; соответствующая разность оптических путей оказывается около 30см. Эксперименты по проблеме ЭПР-Белла, выполненные в Женеве, показывают, что возможно распределить перепутанные пары по стандартным телекоммуникационным линиям и наблюдать высокую степень перепутывания на физических расстояниях между детекторами около 10км (действительная длина оптических волокон между источником и детекторами составляла 8км и 9км [71])

В процессе параметрического рассеяния света может быть получено и поляризационное перепутывание (тип II, [16][4]). Недавно, в эксперименте наблюдалось нарушение неравенства Белла также и для независимых наблюдателей [72]. В этом эксперименте два наблюдателя – Алиса и Боб – разнесены на расстояние около 400м (и соединены оптическим волокном длиной 1км). Но в этом эксперименте все измерения, от генерации случайных ориентаций для анализа до детектирования фотона, выполнялись за времена (~80нс) гораздо более короткие, нежели время, необходимое для передачи сообщения между ними (~1300нс). Быстрая электро-модуляционная система и регистрирующая аппаратура, разработанная для этого эксперимента, может быть непосредственно использована для реализации квантовой криптографии на основе состояний единичных фотонов и при нарушении неравенства Белла, что служит гарантией защищенной связи.

[4] Недавно, в работе [*] было показано, как генерировать максимально перепутанные поляризационные состояния в самом общем случае – при любом типе синхронизма (I или II), в поле импульсной накачки и произвольной длине кристаллов. В работе [**] такие состояния были приготовлены и в невырожденном по частоте случае.

[*]Y.H.Kim, M.V.Chekhova, S.P.Kulik, M.Rubin, and Y.H.Shih. Interferometric Bell state preparation using femtosecond pulse pumped spontaneous parametric down-conversion. Phys.Rev.A 63, 062301 (2001).

[**]Y.Kim, S.P.Kulik, Y.Shih. «Bell state preparation using pulsed nondegenerate two-photon entanglement» Phys.Rev.A 63, 060301 (2001).

2.7 Заключительные замечания

Исследования по квантовой криптографии во всех ее возможных проявлениях становятся все более активными и любой самый полный обзор в этой области будет быстро отставать от реального состояния дел. Поэтому, мы решили дать здесь лишь некоторые основные положения, в надежде на то, что они послужат отправной точкой для введения в этот раздел знаний. Мы исходили из того, что квантовая криптография сегодня представляет реальную альтернативу традиционным криптографическим методам и в недалеком будущем, быть может, мы будем вынуждены доверять квантовой механике больше, чем теории чисел при нашем конфиденциальном общении.

Читатель должен быть предупрежден, что мы лишь очертили круг деятельности, ведущейся в настоящее время, пренебрегая такими разделами, как надежное двух-групповое вычисление, деталями квантовой идентификации, детальным анализом техники подслушивания и критериев надежности, а также некоторыми альтернативными методиками распределения ключа (например, схемой Вайдмана и Голденберга, основанной на посылке ортогональных состояний в двух направлениях). Много интересных статей об этих и о других аналогичных разделах можно найти в e-print архиве Лос-Аламосской национальной лаборатории (http://xxx.lanl.gov/archive/quant-ph) и других www-серверах, например, http:/www.qubit.org.

3

Квантовая плотная кодировка и квантовая телепортация

3.1 Введение

Д. Боумейстер, Х. Вайнфуртер, А. Цайлингер

В главе 2 было показано, как можно использовать квантовое перепутывание для распределения секретных ключей. В этой главе мы обратимся к другим основам квантовой передачи информации, которые используют перепутывание. В разделе 3.2 описывается «квантовая плотная кодировка», которая представляет собой способ передать два бита информации при манипуляции только одной из двух перепутанных частиц, каждая из которых индивидуально может нести 1 бит информации [73]. Схема «квантовой телепортации», изначально предложенная Беннетом, Брассардом, Крэпо, Джозсой, Пересом и Вуттерсом [74] излагается в разд. 3.3. Основная идея квантовой телепортации – передача состояния некоторой квантовой системы на другую удаленную квантовую систему.

Квантовая плотная кодировка и квантовая телепортация были успешно продемонстрированы в квантовой оптике. При оптической реализации двумя существенными компонентами являются источник перепутанных фотонов, описываемый в разд.3.4, и анализатор белловских состояний, рассматриваемый в разд.3.5. В разд. 3.6. представлена экспериментальная демонстрация квантовой плотной кодировки [75]. В разд. 3.7. рассказывается об эксперименте по квантовой телепортации, выполненном в Инсбруке [76], в котором поляризационное состояние единичного фотона телепортируется при помощи вспомогательной пары перепутанных фотонов. В разд. 3.8 описывается эксперимент, предложенный Попеску [77] и выполненный в Риме, в котором поляризационное состояние, приготовленное на одном фотоне из перепутанной по импульсу пары фотонов, передается удаленному партнеру. В разд.3.9 объясняется телепортация непрерывных квантовых переменных, первоначально предложенная Вайдманом [79], в дальнейшем усовершенствованная Брауншгейном и Кимблом [80] и экспериментально продемонстрированная в Калтехе (Caltech) [81]. Каж-

дый эксперимент имеет свои преимущества и недостатки, и для сравнения разных методов мы отсылаем читателя к литературе [82-84].

Если начальное квантовое состояние протокола телепортации это часть перепутанного состояния, то результат процесса телепортации состоит в том что, две системы, которые не взаимодействуя друг с другом непосредственно, становятся перепутанными. Такой процесс, известный как «обмен перепутыванием», будет рассмотрен в разд. 3.10, а различные применения – в разд.3.11.

3.2 Протокол квантовой плотной кодировки

В схеме для плотной квантовой кодировки, теоретически предложенной Беннетом и Виснером [73], используется перепутывание между двумя кубитами, каждый из которых по отдельности имеет два ортогональных состояния |0> и |1>. С классических позиций можно сказать что существует четыре возможных поляризационных комбинации для пары таких частиц: 00, 01, 10 и 11. Присваивая каждой комбинации различные информационные сообщения оказывается, что манипулируя *обеими* частицами, можно закодировать два бита информации.

Квантовая механика позволяет также закодировать информацию в суперпозициях классических комбинаций. Такие суперпозиции состояний двух (или более) частиц называются перепутанными состояниями (см. разд.1.4), а удобный базис, в котором представляются такие состояния двух частиц (с индексами 1 и 2), образован максимально перепутанными состояниями Белла

$$\left|\Psi^{+}\right\rangle_{12}=\frac{1}{\sqrt{2}}\left(\left|0\right\rangle_{1}\left|1\right\rangle_{2}+\left|1\right\rangle_{1}\left|0\right\rangle_{2}\right) \tag{3.1}$$

$$\left|\Psi^{-}\right\rangle_{12}=\frac{1}{\sqrt{2}}\left(\left|0\right\rangle_{1}\left|1\right\rangle_{2}-\left|1\right\rangle_{1}\left|0\right\rangle_{2}\right) \tag{3.2}$$

$$\left|\Phi^{+}\right\rangle_{12}=\frac{1}{\sqrt{2}}\left(\left|0\right\rangle_{1}\left|0\right\rangle_{2}+\left|1\right\rangle_{1}\left|1\right\rangle_{2}\right) \tag{3.3}$$

$$\left|\Phi^{-}\right\rangle_{12}=\frac{1}{\sqrt{2}}\left(\left|0\right\rangle_{1}\left|0\right\rangle_{2}-\left|1\right\rangle_{1}\left|1\right\rangle_{2}\right) \tag{3.4}$$

Присваивая каждому белловскому состоянию разные информационные сообщения, опять же можно закодировать два бита информации, теперь при манипуляции только *одной* из двух частиц.

Это достигается в следующей квантовой коммуникационной схеме. В начале, Алиса и Боб получают по одной частице из перепутанной

пары, скажем, в состоянии $|\Psi^+\rangle_{12}$, определенном в (3.1). Затем, Боб выполняет одно из четырех возможных унитарных преобразований над своей частицей (частица 2). Эти четыре преобразования таковы:

1. Тождественная операция (не изменяющая начального двухчастичного состояния $|\Psi^+\rangle_{12}$).

2. Обмен состояниями ($|0\rangle_2 \rightarrow |1\rangle_2$ и $|1\rangle_2 \rightarrow |0\rangle_2$, изменяющий двухчастичное состояние к виду $|\Phi\rangle_{12}$).

3. Зависимый от состояния фазовый сдвиг (отличающийся на π для $|0\rangle_2$ и $|1\rangle_2$ и преобразующий состояние к виду $|\Psi^-\rangle_{12}$).

4. Обмен состояниями и фазовый сдвиг одновременно (дающие состояние $|\Phi^+\rangle_{12}$.

Поскольку четыре операции производятся над четырьмя белловскими состояниями, то четыре различных сообщения, т.е. 2 бита информации, могут быть переданы посредством частицы Боба (имеющей два состояния) к Алисе. Алиса, в итоге, читает закодированную информацию, путем определения состояния Бэлла двухчастичной системы. Такая схема увеличивает информационную плотность канала передачи до двух битов, по сравнению с классическим максимумом в один бит.[1]

3.3 Протокол квантовой телепортации

В этом разделе мы рассмотрим схему по квантовой телепортации, предложенную Беннетом, Брассардом, Крепэ, Джозсой, Пересом и Вуттерсом [74]. Схема показана на рисунке 3.1.

Идея состоит в том, что у Алисы имеется частица в определенном квантовом состоянии – кубит $|\Psi\rangle_1 = \alpha|0\rangle_1 + \beta|1\rangle$, где $|0\rangle$ и $|1\rangle$ представляют два ортогональных состояния с комплексными амплитудами α и β, удовлетворяющими условию $|\alpha|^2 + |\beta|^2 = 1$. Алиса хочет передать это квантовое состояние Бобу, но считается, что она не может доставить ему частицу непосредственно. В соответствии с проекционным постулатом квантовой механики мы знаем, что любое квантовое измерение, выполненное Алисой над ее частицей, неминуемо разрушит квантовое состояние без получения полной информации, необходимой Бобу для воссоздания исходного состояния. Как же она может передать Бобу это квантовое состояние? Ответ состоит в использовании вспомогательной пары перепутанных частиц 2 и 3 (ЭПР пара), когда частица 2 вручается Алисе, а частица 3 посылается Бобу.

[1] В то время как совершенно понятно, что эта схема увеличивает плотность информации канала передачи, доступного Бобу, до двух битов, мы должны заметить, что канал, передающий другой фотон, пропускает 0 бит информации и, таким образом, переданная информация не превышает 2 бит.

Рассмотрим случай при котором перепутанная пара частиц 2 и 3, распределенная между Алисой и Бобом, находится в состоянии

$$\left|\Psi^{-}\right\rangle_{23} = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle_2\left|1\right\rangle_3 - \left|1\right\rangle_2\left|0\right\rangle_3\right) . \qquad (3.5)$$

Важное свойство этого перепутанного состояния состоит в том, что как только измерение одной из частиц проектирует ее в определенное состояние, которое может быть любой нормированной линейной суперпозицией |0> и |1>, другая частица должна оказаться в ортогональном состоянии. Специфическое фазовое соотношение между двумя членами в правой части (3.5) (здесь разность фаз равна π, что проявляется в знаке «минус») подразумевает, что утверждение об ортогональности не зависит от базиса, выбранного для поляризационного измерения.

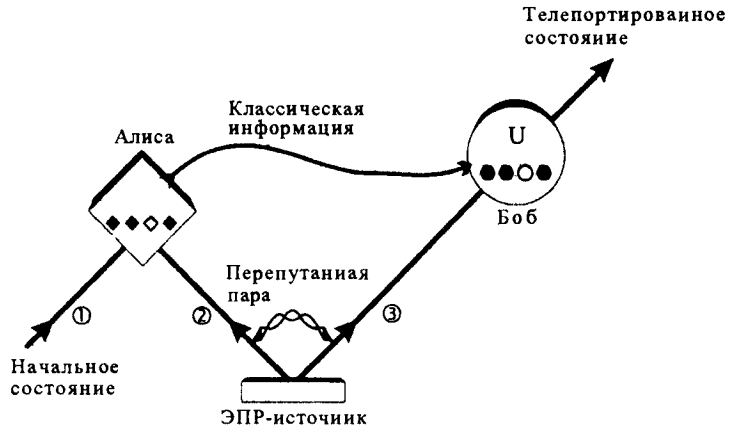


Рис. 3.1. Принцип квантовой телепортации. У Алисы находится квантовая система – частица 1 в начальном состоянии, которую она хочет передать Бобу. Алиса и Боб также имеют по одной частице из вспомогательной пары частиц 2 и 3, испущенной источником состояний Эйнштейна – Подольского – Розена (ЭПР). Затем, Алиса выполняет совместное измерение состояния Белла над начальной частицей и имеющейся у нее частицей из вспомогательной пары. Результатом измерения является проектирование обеих частиц в перепутанное состояние[2]. После этого Алиса посылает Бобу по классическому каналу связи результат своего измерения, и он выполняет унитарное преобразование (U) над другой (своей) частицей вспомогательной пары; эта частица теперь имеет в точности такое же состояние как и у начальной частицы. В случае квантовой телепортации кубита, Алиса выполняет проекционное измерение в четыре ортогональных состояния (белловские состояния), которые образуют полный базис. Сообщение Бобу результата измерения Алисы, т.е. два бита классической информации, дает ему возможность воссоздать начальный кубит.

[2] Здесь под измерением (ИБС) понимается не столько акт физической регистрации частиц, сколько некая операция, в результате которой приготавливается перепутанное состояние двух частиц, т.е. одно из четырех состояний Белла (3.1 – 3.4) (*Прим. переводчика*).

Хотя первоначально частицы 1 и 2 не являются перепутанными, их совместное поляризационное состояние может всегда быть представлено в виде суперпозиции четырех максимально перепутанных состояний Бэлла (3.1) – (3.4), поскольку эти состояния образуют полный ортонормированный базис. Общее состояние частицы 3 записывается в виде:

$$|\Psi\rangle_{123} = |\Psi\rangle_1 \otimes |\Psi\rangle_{23} = \frac{1}{2}[|\Psi^-\rangle_{12}(-\alpha|0\rangle_3 - \beta|1\rangle_3)$$
$$+|\Psi^+\rangle_{12}(-\alpha|0\rangle_3 + \beta|1\rangle_3)$$
$$+|\Phi^-\rangle_{12}(\alpha|1\rangle_3 + \beta|0\rangle_3)$$
$$+|\Phi^+\rangle_{12}(\alpha|1\rangle_3 - \beta|0\rangle_3)] . \qquad (3.6)$$

Теперь Алиса выполняет измерение белловских состояний (ИБС) частиц 1 и 2, т.е. проектирует две находящиеся у нее частицы в одно из четырех состояний Белла. В результате этого измерения оказывается, что частица Боба будет обнаружена в состоянии, которое в точности соответствует начальному состоянию. Например, если измеренное Алисой состояние Белла совпадает с $|\Phi^-\rangle_{12}$, то частица 3, находящаяся у Боба, находится в состоянии $\alpha|1\rangle_3 + \beta|0\rangle_3$. Все, что должна сделать Алиса – это проинформировать Боба через классический канал связи о результате ее измерения, а Боб должен выполнить соответствующее унитарное преобразование (U) над частицей 3, чтобы получить начальное состояние частицы 1. Этим завершается телепортационный протокол.

Заметим, что во время процедуры телепортации значения α и β остаются неизвестными. Из своих измерений состояний Белла Алиса не получает никакой информации о телепортируемом состоянии. Единственное, что достигается при ИБС – это передача квантового состояния. Заметим также, что во время ИБС частица 1 теряет свое начальное квантовое состояние, т.к. она перепутывается с частицей 2. Поэтому состояние $|\Psi\rangle_1$ разрушается Алисой при телепортации, что удовлетворяет требованию теоремы о запрете клонирования в квантовой механике [88]. Более того, начальное состояние частицы 1 может быть совершенно неизвестно не только Алисе, но и вообще, кому бы то ни было. Состояние могло бы быть квантово-механически полностью не определено в то время, когда происходит измерение состояние Белла. Это случай, когда, как было отмечено Беннетом и др. [74], частица 1 является частью перепутанной пары и поэтому сама по себе не имеет определенных свойств. Это неизбежно приводит к обмену перепутыванием, которое будет обсуждаться в разд.3.10 [85, 87].

Экспериментальная реализация квантовой телепортации или квантовой плотной кодировки и обмена перепутыванием подразумевает наличие перепутанных частиц и построения анализатора состояний Белла. В следующих двух разделах будут описаны экспериментальные квантово-оптические методы, позволяющие готовить перепутанные фотоны и анализировать (частично) состояния Белла.

3.4 Источники перепутанных фотонов

Н.Жизан, Дж.Рэрити, Г.Вейхс

Существует несколько источников перепутанных квантовых систем. Источник перепутанных атомов, основанный на квантовой электродинамике резонаторов (КЭР), будет обсуждаться в разд. 5.2.3. Перепутанные ионы приготавливаются в электромагнитных ловушках Пауля, см. разд. 5.2.11. Управляемое перепутывание между ядерными спинами в единичной молекуле реализуется в методе ядерного магнитного резонанса, представленного в разд. 5.3. Изучаются также источники перепутывания и в физике твердого тела; однако сегодня еще слишком рано говорить об управляемом перепутывании в этом случае. В настоящем разделе мы расскажем об источниках перепутывания в квантовой оптике, которые оказались, на сегодняшний день, наиболее удачными для создания эффективного перепутывания.

В квантовой оптике существует два класса систем, в которых может быть осуществлено перепутывание (общие вопросы создания перепутывания обсуждаются в разд. 1.5). Первый класс характеризуется перепутыванием между отдельными фотонами и будет описан в настоящем разделе. Другой путь состоит в установлении перепутывания между квадратурными компонентами (т.е. во входных и выходных фазах компонент электромагнитного поля по сравнению с фазой опорного генератора) световых пучков или между двумя ортогональными поляризационными компонентами световых пучков (см. разд. 3.9.2).

3.4.1 Параметрическое преобразование частоты вниз

Нелинейные оптические процессы используются во многих экспериментах квантовой оптики. Нелинейная оптика является частью классической электродинамики, объектом которой служат сильные поля, неупруго рассеивающиеся в различных средах. Неупругое рассеяние в оптическом диапазоне означает, что не только направление, но и частота света изменяется при взаимодействии с веществом, которое описывается электромагнитной восприимчивостью. Во время таких

взаимодействий, как правило, рождаются новые поля. Разложение по порядкам восприимчивости дает различные оптические нелинейные процессы: трех-волновое (параметрические взаимодействия) и четырех-волновое смешение. Отдельные компоненты P_i электромагнитной поляризации **P** внутри вещества определяются из соотношения

$$P_i = \chi_{ij}^{(1)} E_j + \chi_{ijk}^{(2)} E_j E_k + \chi_{ijkl}^{(3)} E_j E_k E_l + \dots \,, \tag{3.7}$$

где E_i –компоненты электрического поля.

Для того чтобы иметь возможность наблюдать нелинейные процессы в объеме взаимодействия, размеры которого сильно превышают длины волн участвующих в процессе полей, мы должны рассматривать вклады от всего объема как целого. Интерференция между этими вкладами приводит к так называемым условиям фазового синхронизма, которые представляют собой определенные соотношения между волновыми векторами соответствующих электромагнитных полей.

Если взглянуть на эти процессы с точки зрения квантовой электродинамики, мы обнаружим, что существуют не только вынужденные, но и спонтанные эффекты, похожие на взаимодействия электромагнитного поля с атомом. Спонтанный распад фотонов при нелинейных взаимодействиях впервые был исследован теоретически Д.Н.Клышко [89] и экспериментально Бурнхэмом и Вайнбергом [90]. Особым примером таких процессов является процесс спонтанного параметрического преобразования (частоты) вниз[3]. Это нелинейный процесс, вызванный наличием $\chi^{(2)}$, в котором на входе в среде изначально присутствует лишь одно поле с частотой ω_p. Из-за нелинейного взаимодействия и присутствия поля накачки ω_p, происходит спонтанное рождение фотонов в двух других модах с частотами ω_1 и ω_2. В результате закона сохранения энергии оказывается, что

$$\omega_1 + \omega_2 = \omega_p \,. \tag{3.8}$$

Вместе с условием фазового синхронизма[4]

$$\boldsymbol{k}_1 + \boldsymbol{k}_2 = \boldsymbol{k}_p \,, \tag{3.9}$$

это приводит к различным решениям в динамике взаимодействия, зависящим от вещества среды и от наблюдаемых частот. Эффектив-

[3] В русскоязычной литературе этот процесс известен под названием спонтанное параметрическое рассеяние (СПР) света [Д.Н. Клышко. Фотоны и нелинейная оптика. М.«Наука» 1980г. 256с.]. В дальнейшем мы будем придерживаться именно этого термина (*Прим. переводчика*).

[4] Здесь и везде далее предполагается точное выполнение условий синхронизма, которое строго говоря, имеет вид $k_p - k - k_2 = \Delta$, где волновая расстройка Δ – определяется в стационарном случае пространственными размерами области нелинейного взаимодействия трех волн (*Прим. переводчика*).

ность преобразования зависит от модуля соответствующих компонент $\chi^{(2)}$ и, как правило, очень низка. Если, например, излучение накачки попадает в вещество с высокой нелинейностью (дигидрофосфат калия, β-борат бария), в преобразованном свете можно наблюдать порядка 10^{10} фотонов в секунду выходящих из небольшого (несколько миллиметров в длину) образца. Из соображений симметрии следует, что восприимчивость второго порядка $\chi^{(2)}$ отлична от нуля только в нецентросимметричных веществах – свойство, присущее только некоторым кристаллам.

При параметрическом преобразовании частоты в видимом диапазоне мы различаем две возможные схемы фазового синхронизма. Синхронизм «типа I» возникает, когда два рождающихся фотона имеют одинаковые поляризации, в то время как при синхронизме «типа II» их поляризации ортогональны в базисе, который определяется ориентацией кристалла. Возможность приготовления и наблюдения перепутывания заложена в одновременности рождения двух фотонов в процессе преобразования, удовлетворении фазовых соотношений, а также надлежащей пространственной и временной селекции излучаемого света.

3.4.2 Перепутывание во времени

Рис. 3.2. Схема эксперимента типа Фрэнсона, по проверке интерференции перепутанных во времени фотонных пар. Измерения проводятся с помощью двух удаленных разбалансированных интерферометров Маха-Цандера. Фаза каждого интерферометра изменяется фазовращателем, расположенным в длинном (L) плече.

Коррелированные пары фотонов, рождающиеся в процессе спонтанного параметрического рассеяния (СПР), обладают несколькими свойствами. При СПР с синхронизмом типа I и типа II можно наблюдать то, что иногда называют перепутыванием во времени. Это свойство отражает факт одновременного рождения фотонов пары, и, что они удовлетворяют закону сохранения энергии, который приводился выше. Последнее означает, что время излучения любой пары не определено в пределах времени когерентности лазера накачки. Критерий одновременности возникает из-за того, что отдельные фотоны па-

ры имеют широкий спектр (порядка нескольких нанометров) и временем когерентности около 100 фсек. Такой вид перепутывания был использован в так называемой двухфотонной интерферометрии Фрэнсона (см.рис.3.2), где оба фотона проходят через раздельные разбалансированные интерферометры Маха-Цандера [91]. Два одинаковых интерферометра построены так, что длина когерентности отдельных фотонов меньше, чем разность оптических путей в каждом интерферометре. Как следствие – невозможность наблюдения интерференции при наблюдении излучения одним детектором, расположенным на выходе того или другого интерферометра. Однако, если интересоваться совпадениями фотоотсчетов двух детекторов, стоящих после интерферометров, наблюдаются осцилляции в скорости счета совпадений при внесении сдвига фаз между плечами интерферометров. Состояние внутри интерферометров может быть представлено в виде

$$|\Psi\rangle = \frac{1}{2}[|S\rangle_1|S\rangle_2 + e^{i(\phi_1+\phi_2)}|L\rangle_1|L\rangle_2 +$$

$$+e^{i\phi_2}|S\rangle_1|L\rangle_2 + e^{i\phi_1}|L\rangle_1|S\rangle_2] \ , \qquad (3.10)$$

где индексы 1 и 2 относятся к фотонам, движущимся, соответственно, влево и вправо, как показано на рис.3.2. Состояние (3.10), в действительности, представляет собой факторизованное состояние. Однако, регистрация только событий, отвечающих тому, что оба фотона прошли длинными путями (L – L) или короткими путями (S – S), дает истинные совпадения фотоотсчетов. Другие события могут быть исключены при правильном выборе окна схемы совпадений. В первых экспериментах [91] возможность варьирования размеров окна не использовалась и поэтому максимальная видность, которая была зарегистрирована, оказалась ограничена уровнем 50%. В более поздних экспериментах с использованием узкого окна схемы совпадений для пост-селекции только перепутанного состояния, видность оказалась выше 90% [92].

Здесь необходимо упомянуть об одном интересном развитии идеи о перепутывании по времени. Можно заменить непрерывный лазер накачки на импульсный и направить пучок в интерферометр так, что разница длин плеч интерферометра окажется больше чем длительность импульса [93], см. рис. 3.3. Таким образом, если фотон накачки распадается на пары фотонов в кристалле после прохождения через интерферометр, стоящий в пучке накачки, то время распада приобретает неопределенность. Действительно, несбалансированный интерферометр преобразует состояние фотона накачки в суперпозицию $\alpha|\text{short}\rangle_{pump} + \beta|\text{long}\rangle_{pump}$ и процесс СПР в кристалле преобразует это состояние в

$$\alpha|\text{short}\rangle_s \otimes |\text{short}\rangle_i + \beta|\text{long}\rangle_s \otimes |\text{long}\rangle_i \qquad (3.11)$$

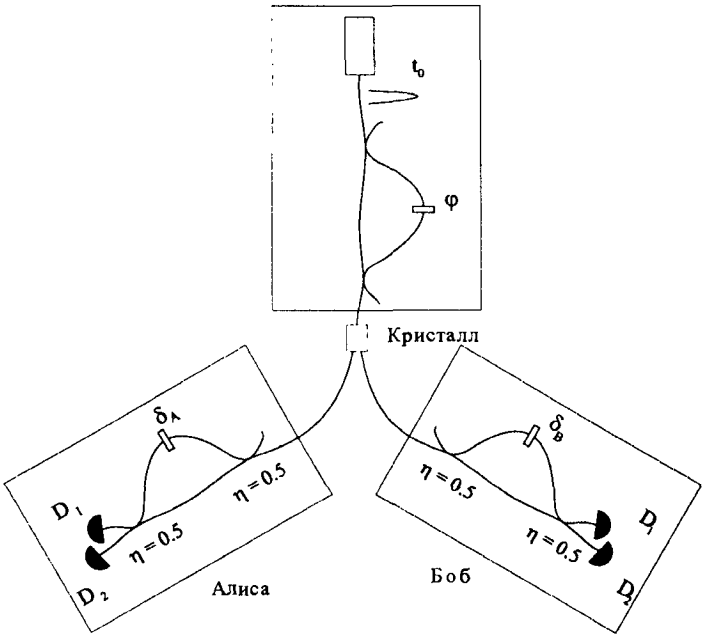


Рис. 3.3. Схема импульсного двухфотонного источника, дающего состояния, перепутанные по времени и его возможного применения в квантовой криптографии. Парные фотоны, образованные из фотона накачки, прошедшего через длинное или короткое плечо интерферометра, когерентны. Алиса и Боб регистрируют фотоны через три разные интервала времени (относительно момента времени излучения): короткого, промежуточного и длинного. Фотоотсчеты, соответствующие регистрации после короткого и длинного интервалов проявляют 100%-ую корреляцию. После промежуточного интервала фотоотсчеты отвечают дополнительному базису $|\text{short}\rangle \pm |\text{long}\rangle$, и также полностью коррелированы (в предположении, что $\varphi + \delta_A + \delta_B = 0$). Заметим, что в схеме не используется ни генератор случайных чисел, ни активный оптический элемент.

В отличие от перепутанных во времени фотонов, получаемых от непрерывного лазера накачки длина когерентности импульсного лазера не имеет значения, т.к. необходимая когерентность создается разбалансированным интерферометром. Другими словами, неопределенность во времени прибытия фотона накачки (в пределах длины когерентности лазера) заменяется на два острых временных пика, отвечающих прохождению фотона накачки по короткому $|\text{short}\rangle$ или длинному $|\text{long}\rangle$ пути; образуется базис нашего кубитового пространства. Отсюда следует, что в качестве накачки может быть использован, к примеру, любой стандартный лазерный диод. Более того, базисные состояния можно различать по их времени прибытия, без использования каких-либо дополнительных оптических схем. Изменяя соотношение между пропусканием и отражением интерферометра, а также

фазу разбалансированного интерферометра, можно приготавливать все 2-кубитовые перепутанные состояния. Это означает, что можно реализовать все 2-кубитовые квантовые коммуникационные протоколы.

3.4.3 Перепутывание по импульсу

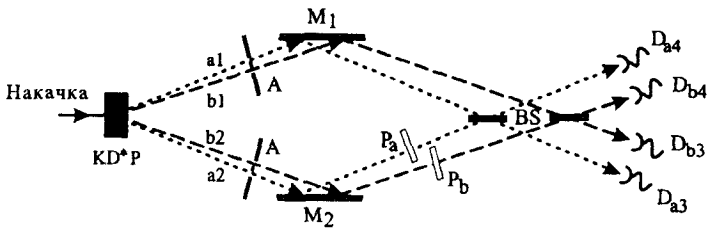


Рис. 3.4. Схема эксперимента Рэрити-Тапстера по импульсному перепутыванию при СПР с синхронизмом типа I. Две коррелированные пары мод вырезаются из пространственного спектра излучения СПР при помощи двух двойных диафрагм *A*. Излучение с разными длинами волн перемешивается на светоделителе *BS*. Детекторы D_{a3}, D_{b3}, D_{a4} и D_{b4} используются для измерения в выходных модах светоделителя.

Другой вид перепутывания – перепутывание по импульсу – происходит при неколлинеарном СПР. Условия фазового синхронизма допускают излучение полей с разными частотами в разных направлениях. Используя диафрагмы A (см. Рис. 3.4), можно вырезать две отдельные моды (направления) в излучении источника СПР [94]. Селекция происходит таким образом, что каждая пара состоит из фотона цвета *a* (частота немного выше половины частоты накачки) и фотона цвета *b* (с частотой ниже половины частоты накачки). Пары излучаются либо в моды *a1*, *b1* либо в моды *a2*, *b2*, как показано на Рис.3.4. До светоделителя BS мы получаем состояние

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left[e^{i\phi_b}|a\rangle_1|b\rangle_2 + e^{i\phi_a}|a\rangle_2|b\rangle_1\right] , \qquad (3.12)$$

которое является перепутанным, хотя моды, на этой стадии, полностью различимы. Перепутывание проявляется, когда *a*-моды и *b*-моды перемешиваются на светоделителе. По правую сторону от делителя, верхние и нижние пути прихода фотонов неразличимы, что ведет к интерференции. 50%-ый светоделитель преобразует падающие на него поля к виду

$$|in\rangle_1 \to \frac{1}{\sqrt{2}}\left[|out\rangle_3 + i|out\rangle_4\right] ,$$

$$|in\rangle_2 \to \frac{1}{\sqrt{2}}\left[|out\rangle_4 + i|out\rangle_3\right] . \qquad (3.13)$$

Состояние перед детекторами, таким образом имеет вид

$$|\Psi\rangle = \frac{1}{2}[\left(e^{i\phi_a} - e^{i\phi_b}\right)|a\rangle_4|b\rangle_3 + \left(e^{i\phi_b} - e^{i\phi_a}\right)|a\rangle_3|b\rangle_4 +$$

$$+i\left(e^{i\phi_a} + e^{i\phi_b}\right)|a\rangle_4|b\rangle_4 + i\left(e^{i\phi_a} + e^{i\phi_b}\right)|a\rangle_3|b\rangle_3 \ . \qquad (3.14)$$

Четыре слагаемых дают амплитуды вероятностей регистрации совпадений в каждой из четырех возможных комбинаций пар детекторов. Чтобы получить вероятность регистрации совпадений между детекторами, стоящими в a-модах и b-модах, нужно найти квадрат модуля от этих амплитуд. Вероятность будет изменяться гармоническим образом при изменении разности фаз интерферометра $\phi = \phi_a - \phi_b$. Интерференционные эффекты первого порядка между перемешанными a- и b-модами не возникают, потому что фазы отдельных фотонов в разных парах случайны. Сохранение фазы при параметрических процессах возникает как следствие закона сохранения энергии, о чем шла речь выше; сумма фаз полей в a- и b-модах в точности равна фазе поля накачки.

Интерферометр с модой a (b) позволяет измерить «фазу» между двумя возможными актами излучения в базисе, задаваемом фазой ϕ_a (ϕ_b). 100%-ая корреляция (антикорреляция) при парном измерении этой фазы всякий раз, когда $\phi = \phi_a - \phi_b = 0$ ($\pi/2$), подтверждает нелокальную природу этого эффекта[5]. Этот результат не может быть воспроизведен при наличии реальной локальной фазы (удовлетворяющей приведенному выше условию на сумму фаз), связанной с каждым из фотонов в паре на выходе из кристалла. В эксперименте [94] была измерена видность интерференции 82%, что превышает результат, предсказываемый любой локальной моделью эксперимента. Однако, из-за трудностей в юстировке четырех пучков, видность интерференции низка по сравнению с наблюдаемой в поляризационных экспериментах.

3.4.4 Перепутывание по поляризации

Недавно был найден новый тип источника СПР, в котором осуществляется неколлинеарный синхронизм типа II [16]. При определенных углах между пучком накачки и оптической осью кристалла-преобразователя условия фазового синхронизма таковы, что фотоны излуча-

[5] Использование авторами термина «нелокальность» не имеет четкого физического обоснования, т.к. может быть связано с наличием неких сверхсветовых взаимодействий. Для прояснения этого вопроса отсылаем читателя к работе [Д.Н. Клышко. Квантовая оптика: квантовые классические и метафизические аспекты. УФН, 164, № 11, 1187 – 1214 (1994)] *Прим. переводчика*.

ются вдоль конусов, не имеющих общей оси, как показано на Рис.3.5 и Рис.3.6. Вдоль одного из конусов излучение поляризовано как обыкновенные волны, вдоль другого – как необыкновенные. Эти конусы, в общем случае, пересекаются вдоль двух направлений. Если теперь вспомнить, что при синхронизме типа II, два фотона в паре всегда поляризованы ортогонально, то окажется, что в этих двух направлениях пересечения излучаемый свет не поляризован. Это происходит потому, что мы не можем определить какому из конусов принадлежит данный фотон. На самом деле это не совсем так, поскольку в двулучепреломляющем кристалле обыкновенные и необыкновенные фотоны распространяются с разными скоростями, и мы могли бы, по крайней мере, в принципе, различить эти два случая по времени прибытия соответствующего фотона. Возможно, однако, скомпенсировать этот «снос», помещая в каждый из пучков точно такой же кристалл половинной толщины и повернутый на 90^0. Такая процедура полностью стирает любую подобную информацию и мы получаем следующее настоящее перепутанное по поляризации состояние

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left[|V\rangle_1|H\rangle_2 + e^{i\varphi}|H\rangle_1|V\rangle_2\right] . \qquad (3.15)$$

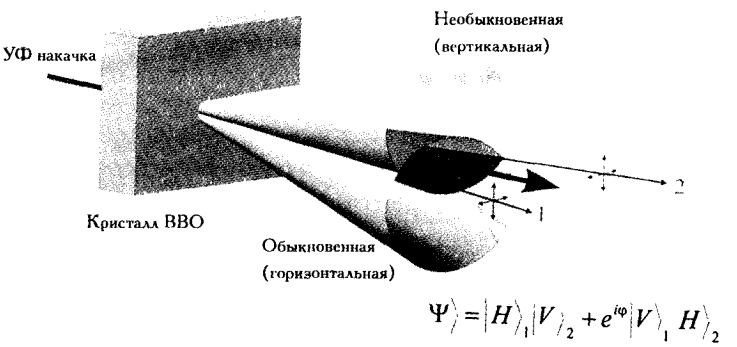


Рис. 3.5. Неколлинеарное СПР с синхронизмом типа II может дать два наклоненных конуса света с определенной длиной волны. В то же время излучаются и другие длины волн, но для наблюдения поляризационного перепутывания необходимо вырезать центральную длины волны, используя узкополосные оптические фильтры.

Более того, мы можем использовать эти компенсационные кристаллы для изменения фазы φ между двумя компонентами перепутанного состояния. При использовании дополнительной полуволновой пластинки в одном из двух пучков можно получить два других состояния Белла

$$\left|\Phi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}\left[|V\rangle_1|V\rangle_2 \pm |H\rangle_1|H\rangle_2\right] . \qquad (3.16)$$

И снова, чтобы увидеть интерференционные эффекты, состояние исследуется в том базисе, где вертикальные и горизонтальные поляризации не различаются. Это можно сделать очень просто, перемешав состояния поляризатором, ориентированным под углом 45^0

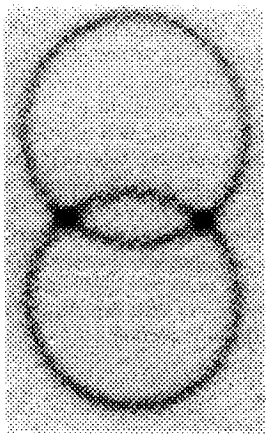


Рис. 3.6. Спонтанное параметрическое рассеяние с синхронизмом типа II, как его видно через узкополосный фильтр. Два кольца - это сечения обыкновенного и необыкновенного конусов световых лучей. Вдоль направлений пересечения наблюдается неполяризованный свет.

3.5 Анализатор состояний Белла

Д. Боумейстер, Х. Вайнфуртер, А. Цайлингер

Формально говоря, анализ белловских состояний, необходимый при квантовой плотной кодировке и квантовой телепортации (см. разд. 3.2 и 3.3) не является проблемой. Все, что нужно сделать – это спроектировать входное состояние на базис белловских состояний (3.1 –3.4) и при многократном повторении этого эксперимента определить вероятности, с которыми начальное состояние может быть найдено в одном из состояний Белла. Состояния Белла, конечно, зависят от типа перепутывания, которым характеризуется начальное состояние. В случае перепутывания между поляризационными и импульсными степенями свободы, проицирование на полный базис белловских состояний возможно при помощи простых линейных оптических элементов. В случае перепутывания по поляризации между фотонами ситуация выглядит гораздо сложнее и до сих пор проицирование было реализовано только на два состояния Белла. Другие два состояния оставались вырожденными при их детек-

тировании[6]. Такой частичный анализ состояний Белла объясняется в следующем разделе.

3.5.1 Статистика фотонов при прохождении через светоделитель

Частичный анализ состояний Белла при поляризационном перепутывании использует статистику двух кубитов при прохождении их через светоделитель. Основной принцип анализатора опирается на то, что из четырех белловских состояний (3.1 – 3.4) только одно является антисимметричным при перестановке двух частиц. Это состояние $|\Psi^-\rangle_{12}$ (3.2), которое, очевидно, изменяет знак при смене индексов 1 и 2. Оставшиеся три состояния симметричны. Таим образом, видно, что находясь в состоянии $|\Psi^-\rangle_{12}$, кубит подчиняется фермионной симметрии, а во всех остальных трех состояниях – бозонной. До сих пор мы не уточняли являются ли частицы, переносящие кубиты, фермионами или бозонами. Это происходило потому, что состояния, записанные в виде (3.1 – 3.4) не являются полными состояниями частиц, а описывают только внутреннее (двух-уровневое) состояние частиц. Общее же состояние можно получить, добавляя к нему пространственное состояние частиц, которое также может быть симметричным или антисимметричным. В случае бозонов, пространственная часть волновой функции должна быть антисимметричной для состояния $|\Psi^-\rangle_{12}$ и симметричной для трех других, в то время как для фермионов, все должно быть наоборот.

Рассмотрим для начала два фотона, которые являются бозонами, и предположим, что состояния Белла описывают поляризацию фотонов, т.е. внутреннюю степень свободы. Далее, очевидно, что общее состояние двух фотонов должно быть симметричным. В случае, когда две частицы падают симметрично на входы светоделителя, т.е. каждая частица приходится на одну из входных мод $|a\rangle$ и $|b\rangle$, внешние (пространственные) состояния принимают вид

$$|\Psi_A\rangle_{12} = \frac{1}{\sqrt{2}}\left(|a\rangle_1|b\rangle_2 - |b\rangle_1|a\rangle_2\right) \tag{3.17}$$

$$|\Psi_S\rangle_{12} = \frac{1}{\sqrt{2}}\left(|a\rangle_1|b\rangle_2 + |b\rangle_1|a\rangle_2\right), \tag{3.18}$$

[6] Уже после выхода настоящего издания в свет было осуществлено проектирование в полный базис поляризационных состояний Белла. Для этого использовался процесс параметрического преобразования частоты вверх [Y. H. Kim, S.P.Kulik, Y. Shih, Quantum Teleportation with a Complete Bell State Measurement. Phys. Rev. Lett. 86, № 7, 1370 – 1373 (2001)] (*Прим. переводчика*).

где $|\Psi_A\rangle_{12}$ и $|\Psi_S\rangle_{12}$ – антисимметричное и симметричное состояния, соответственно. Из-за требований, накладываемых симметрией, общие двухфотонные состояния в итоге имеют вид:

$$|\Psi^+\rangle|\Psi_S\rangle\,,\ |\Psi^-\rangle|\Psi_A\rangle\,,\ |\Phi^+\rangle|\Psi_S\rangle \quad \text{и} \quad |\Phi^-\rangle|\Psi_S\rangle\,. \tag{3.19}$$

Заметим, что только состояние, антисимметричное во внешних переменных, является также антисимметричным во внутренних переменных. Именно это состояние выходит из светоделителя во внешнем антисимметричном состоянии. Это можно просто показать, если предположить, что делитель не влияет на внутреннее состояние и применяя оператор, описывающий светоделитель (преобразование Адамара) к внешнему состоянию. Используя

$$H|a\rangle = \frac{1}{\sqrt{2}}\left(|c\rangle + |d\rangle\right) \tag{3.20}$$

$$H|b\rangle = \frac{1}{\sqrt{2}}\left(|c\rangle - |d\rangle\right) \tag{3.21}$$

получаем, что

$$H|\Psi_A\rangle_{12} = \frac{1}{\sqrt{2}}\left(|c\rangle_1|d\rangle_2 - |d\rangle_1|c\rangle_2\right) = |\Psi_A\rangle_{12}\,. \tag{3.22}$$

Поэтому пространственно антисимметричное состояние является собственным для оператора, описывающего светоделитель [95, 96]. Наоборот, во всех других трех случаях симметричного внешнего состояния $|\Psi_S\rangle$, два фотона оказываются в одном из двух выходов светоделителя. Именно поэтому, очевидно, что состояние $|\Psi^-\rangle$ можно однозначно отделить от всех других. Это единственное из четырех белловских состояний, которое приводит к совпадениям фотоотсчетов детекторов, помещенных в каждую выходную моду делителя [97-99]. Как же можно идентифицировать три других состояния? Этот вопрос возвращает нас к тому, что различие, с одной стороны, между $|\Psi^+\rangle$ и $|\Phi^+\rangle$ и, с другой стороны, между $|\Psi^+\rangle$ и $|\Phi^-\rangle$ основано на том, что только в $|\Psi^+\rangle$ два фотона имеют действительно различные поляризации, в то время как в двух других состояниях они имеют одинаковые поляризации. Таким образом, выполнение поляризационных измерений и наблюдение за фотонами по одну сторону от светоделителя позволяет различить состояние $|\Psi^+\rangle$ от состояний $|\Phi^+\rangle$ и $|\Phi^-\rangle$. Необходимо отметить, что простое обобщение этой процедуры ведет к тому, что любые два ортогональные максимально перепутанные состояния можно различить друг от друга тем же способом, поскольку при локальных унитарных преобразованиях нужно производить операции поворота в двумерном гильбертовом пространстве.

Рассмотрим теперь такой же эксперимент с фермионами [100], где снова белловские состояния описывают внутренние состояния. Например, если два кубита перепутаны по спинам, находим, что четыре возможных состояния имеют вид

$$|\Psi^+\rangle|\Psi_A\rangle\ ,\ |\Psi^-\rangle|\Psi_S\rangle\ ,\ |\Phi^+\rangle|\Psi_A\rangle \quad \text{и} \quad |\Phi^-\rangle|\Psi_A\rangle\ , \tag{3.23}$$

поскольку требуется антисимметричность общего состояния. Поэтому для фермионов только одно из состояний пространственно симметрично, три других являются пространственно антисимметричными. Таким образом, только в одном случае, а именно для $|\Psi^-\rangle$ два фермиона будут покидать светоделитель, находясь в одной моде. В остальных трех случаях они будут выходить в разные выходные пространственные моды. Примечательно, что такое состояние опять же может быть отделено от других из-за определенных свойств симметрии.

3.6 Экспериментальная плотная кодировка кубитов

Квантово-оптическая демонстрация схемы квантовой плотной кодировки [75], обсуждаемой в разд.3.2, требует присутствия трех отдельных элементов (Рис.3.7): источника ЭПР состояний, генерирующего перепутанные фотоны, станции Боба для кодирования сообщений с помощью унитарного преобразования над его частицей и анализатора белловских состояний, находящегося у Алисы, чтобы распознать сигнал, посылаемый Бобом. Перепутанные по поляризации фотоны готовятся в процессе СПР с синхронизмом типа II (разд.3.4.). Ультрафиолетовый пучок (λ = 351 нм) аргонового лазера преобразуется в пары фотонов (λ = 702 нм) с ортогональными поляризациями.

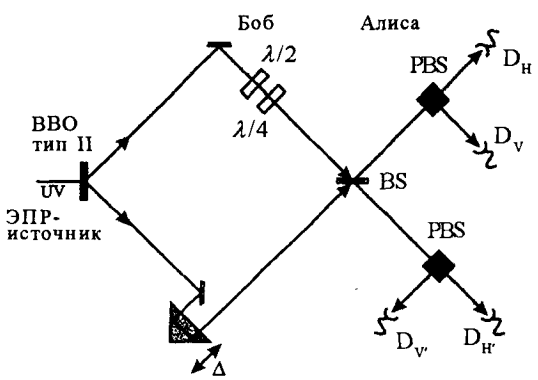


Рис. 3.7. Экспериментальная установка для квантовой плотной кодировки [75].

Перепутанное состояние $|\Psi^+\rangle$ получается после компенсации двулучепреломления в кристалле BBO вдоль определенных направлений излучения (тщательно выделенных при помощи 2-мм ирисовых диафрагм, расположенных на расстоянии 1.5 метра от кристалла). Один пучок направлялся к кодирующей станции Боба, другой – непосредственно к анализатору белловских состояний, находящемуся у Алисы. При юстировке схемы был использован «оптический тромбон». Оптический тромбон представляет собой устройство, возвращающее излучение назад в том же направлении, но по другому пути. Это дает возможность плавно менять задержку в пределах длины когерентности сигнальных и холостых фотонов ($l_c \approx 100\mu$)

При кодировании поляризации частицы, имеющейся у Боба, были выполнены необходимые преобразования. Это осуществлялось с помощью полуволновой пластинки, изменяющей поляризацию, и четвертьволновой пластинки для внесения фазового сдвига, зависящего от поляризации[7]. Управляемый таким образом пучок в станции Боба, затем перемешивался с другим пучком у Алисы на анализаторе белловских состояний. Анализатор состоял из светоделителя, и помещенных за ним двухканальных поляризационных устройств, в каждой из двух его выходных мод. В эксперименте производился анализ совпадений фотоотсчетов между четырьмя счетчиками фотонов.

Поскольку только состояние $|\Psi^-\rangle$ имеет антисимметричную пространственную часть, именно это состояние и регистрировалось при измерении числа совпадений между различными выходами светоделителя (т.е. совпадения фотоотсчетов между детекторами D_H и $D_{V'}$ или между $D_{H'}$ и D_V). Для оставшихся трех состояний оба фотона выходят в одну и ту же выходную моду светоделителя. Состояние $|\Psi^+\rangle$ можно просто отличить от двух других благодаря различным поляризациям двух фотонов, дающим после двухканального поляризационного устройства совпадения между отсчетами детекторов D_H и D_V или между $D_{H'}$ и $D_{V'}$. Два состояния $|\Phi^+\rangle$ и $|\Phi^-\rangle$ преобразуются в такое двухфотонное состояние, которое поглощается отдельным детектором и, таким образом, их не удается различить.

В таблице 3.1 приведена сводка различных манипуляций кодировщика Боба и вероятностей исходов, регистрируемых Алисой.

[7] Компонента, поляризованная вдоль оси четвертволновой пластинки, приобретает сдвиг фазы на $\pi/2$ относительно другой. Переориентация оптической оси с вертикального положения на горизонтальное вызывает точное изменение фазы между $|H\rangle$ и $|V\rangle$ на π.

Таблица 3.1. Сводка возможных манипуляций и регистрируемых событий в эксперименте по квантовой плотной кодировке с коррелированными фотонами.

Установки Боба:		Посылаемое состояние	События, регистрируемые Алисой
λ/2	λ/4		
0°	0°	$\|\Psi^+\rangle$	совпадения между D_H и D_V или $D_{H'}$ и $D_{V'}$
0°	90°	$\|\Psi^-\rangle$	совпадения между D_H и $D_{V'}$ или $D_{H'}$ и D_V
45°	0°	$\|\Phi^+\rangle$	2 фотона либо в D_H, D_V, $D_{H'}$ либо в $D_{V'}$
45°	90°	$\|\Phi^-\rangle$	2 фотона либо в D_H, D_V, $D_{H'}$ либо в $D_{V'}$

Сначала эксперименты выполнялись при следующей установке параметров станции Боба: состояние ЭПР источника выбиралось так, что из станции Боба выходило состояние $|\Psi^+\rangle$, т.е. когда оси обеих фазовых пластинок установлены вертикально; другие состояния Белла могли генерироваться при соответствующих установках пластинок, показанных в табл. 3.1. Для того, чтобы наблюдать интерференцию на анализаторе Алисы, мы изменяли разность плеч Δ между двумя пучками с помощью оптического тромбона. Когда $\Delta >> l_c$ интерференция отсутствовала и наблюдалась классическая статистика в совпадениях фотоотсчетов детекторов. При оптимальной настройке разности плеч ($\Delta = 0$) интерференция возникала, что давало возможность распознать закодированную информацию.

На Рис. 3.8 и 3.9 показаны зависимости скоростей счета совпадений $C_{HV}(\cdot)$ и $C_{HV'}(\circ)$ от разности длин в случае $|\Psi^+\rangle$ и $|\Psi^-\rangle$, соответственно (скорости счета совпадений $C_{HV'}$ и C_{HV} ведут себя аналогичным образом; мы используем обозначение C_{AB} для совпадений между детекторами D_A и D_B). При $\Delta = 0$, C_{HV} достигает максимума для состояния $|\Psi^+\rangle$ (Рис.3.8) и уменьшается (вплоть до уровня случайных совпадений[8]) для $|\Psi^-\rangle$ (Рис.3.10). $C_{HV'}$ проявляет противоположную зависимость и соответствует состоянию $|\Psi^-\rangle$. Результаты этих измерений означают, что если регистрируются оба фотона, то идентифицируется состояние $|\Psi^+\rangle$ с достоверностью 95%, а состояние $|\Psi^-\rangle$ – с 93%.

[8] Если W_1 и W_2 – скорости счета некоррелированных световых сигналов, регистрируемых детекторами 1 и 2, то скорость счета случайных совпадений между этими детекторами оказывается $W_{\text{случ. совп}} = W_1 W_2 T$, где T – временное окно схемы совпадений. (*Прим. переводчика.*)

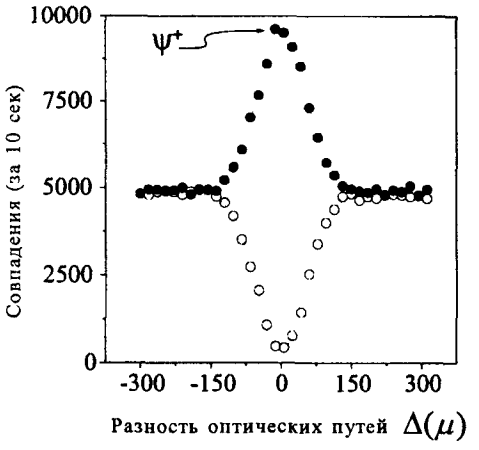


Рис. 3.8. Скорость счета совпадений C_{HV}(•)и $C_{HV'}$(○) как функции разности плеч Δ, при передаче состояния $|\Psi^+\rangle$. При идеальной настройке (Δ = 0) происходит конструктивная интерференция для C_{HV}, позволяющая идентифицировать это состояние.

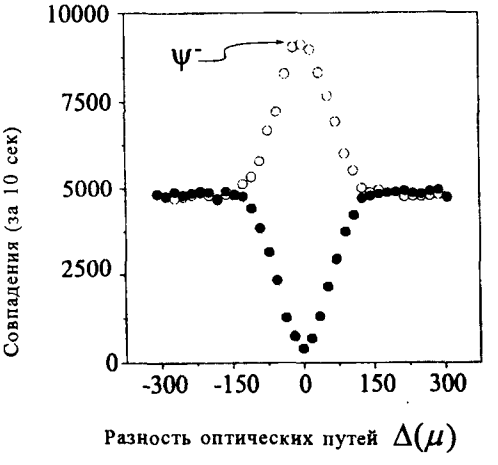


Рис. 3.9. Скорость счета совпадений C_{HV}(•)и $C_{HV'}$(○) как функции разности плеч Δ, при передаче состояния $|\Psi^-\rangle$. Конструктивная интерференция для $C_{HV'}$ дает возможность прочитать информацию, связанную с этим состоянием.

При использовании кремниевых лавинных фотодиодов, работающих в гейгеровской моде в режиме счета фотонов, необходимо модифицировать анализатор белловских состояний, поскольку нужно суметь зарегистрировать два фотона, появляющихся в одной

выходной моде анализатора и соответствующих состояниям $|\Phi^+\rangle$ и $|\Phi^-\rangle$[9].

Одна из возможностей полностью избежать интерференции таких состояний состоит во введении перед светоделителем Алисы зависящей от поляризации задержки, превышающей время когерентности. Например, это достигается с помощью толстых пластин из кристаллического кварца, задерживающих $|H\rangle$ в одном пучке и $|V\rangle$ в другом. Другой метод состоит в расщеплении получившегося двухфотонного состояния при помощи дополнительного светоделителя с последующей регистрацией (с 50%-ой вероятностью) совпадений отсчетов детекторов, помещенных в каждую выходную моду этого светоделителя. Чтобы продемонстрировать принципиальную возможность такого метода, мы разместили такое устройство вместо детектора D_H. На Рис. 3.10 показано, как увеличивается скорость счета совпадений $C_{H\bar{H}}$(□) при разности плеч $\Delta = 0$, по сравнению с сигналами C_{HV} и $C_{HV'}$, соответствующими фоновому уровню, когда Боб посылает состояние $|\Phi^-\rangle$.

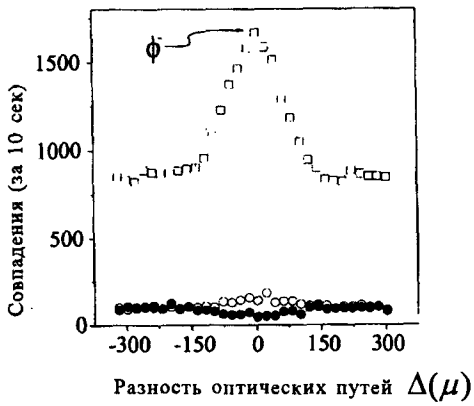


Рис. 3.10. Скорость счета совпадений C_{HV}(•), $C_{H\bar{H}}$(□) и $C_{HV'}$(○) как функции разности плеч Δ. Максимум в сигнале $C_{H\bar{H}}$ означает передачу третьего состояния $|\Phi^-\rangle$, закодированного в двухуровневой частице. Сигнал $C_{H\bar{H}}$ в четыре раза меньше сигналов, показанных на Рис. 3.8 и 3.9, из-за уменьшения вероятности регистрации $|\Phi^-\rangle$, см текст.

Заметим, однако, что для обоих методов в половине всех исходов оба фотона все же поглощаются одним детектором; поэтому, поскольку

[9] Необходима специальная идентификация двухфотонного состояния: кремниевые фотодиоды дают одинаковые импульсы фототока для одного и более фотонов, если они попадают в диод одновременно; таким образом только регистрация совпадений позволяет обнаружить двухфотонное состояние. В определенных типах фотоумножителей одно- и двухфотонное поглощение фотокатода дают различные выходные сигналы. Однако в настоящее время эффективность таких детекторов крайне низка.

мы использовали только одну подобную конфигурацию, максимальная скорость счета для $C_{H\bar{H}}$ составляет лишь около четверти от максимума величины C_{HV} или $C_{HV'}$ (Рис. 3.8 и 3.9).

Поскольку теперь мы можем различить три разных состояния, то можно считать, что имеются условия для передачи сообщений, передаваемых методом квантовой плотной кодировки. На Рис. 3.11 показаны различные скорости счета совпадений (нормированные к соответствующей максимальной скорости передаваемого состояния) при передаче ASCII кодов «KM°» (т.е. кодов 75, 77, 179) с помощью лишь 15 тритов вместо 24 классических битов. Из этих измерений можно получить отношение сигнал-шум, сравнивая уровни полезного сигнала с суммой двух других регистрируемых сигналов. Эти отношения при передаче трех состояний отличались из-за различия в видности соответствующих интерференционных компонент и составляли

$S/N_{|\Psi^+\rangle}$=14.8, $S/N_{|\Psi^-\rangle}$=13.0 и $S/N_{|\Phi^-\rangle}$=8.5.

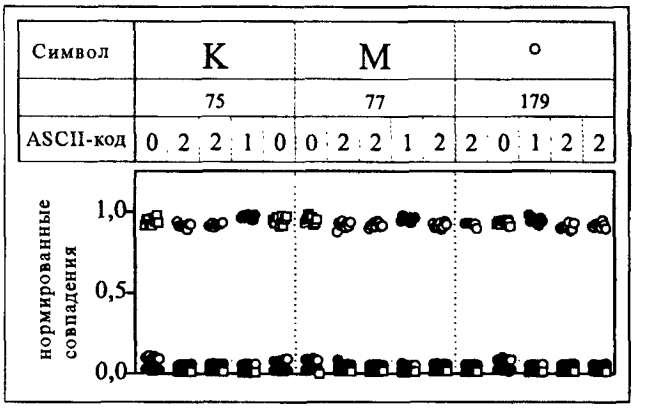


Рис.3.11. Квантовая плотная кодировка «1.58 бит на фотон»: ASCII-коды для символов «KM°» (т.е. 75, 77, 179), закодированных в 15 тритах (когда «0» ≡ $|\Phi^-\rangle \triangleq$ □, «1» ≡ $|\Psi^+\rangle \triangleq$ •, «2» ≡$|\Psi^-\rangle \triangleq$), вместо 24 битов, обычно используемых. Данные для каждого типа закодированного состояния нормированы на максимум скорости совпадений для этого состояния.

3.7 Эксперименты по квантовой телепортации кубитов.

Д.Боумейстер, Дж.-В.Пэн, Х.Вайнфуртер, А.Цайлингер

В этом разделе будет рассмотрена экспериментальная демонстрация квантовой телепортации кубитов, закодированных в поляризационном состоянии единичных фотонов [76]. При телепортации входной фотон, который находится в определенном поляризационном состоянии (имен-

но это поляризационное состояние и «копируется» при телепортации), и пара перепутанных фотонов являются объектами измерения, так что один из фотонов перепутанной пары приобретает поляризацию исходного фотона. На Рис. 3.12 схематично изображена экспериментальная установка. Как объяснялось в разд. 3.3, при экспериментальной реализации квантовой телепортации требуется как приготовление, так и измерение перепутанных состояний; приготовление заключается в создании источника состояний Эйнштейна–Подольского–Розена (ЭПР), а измерение – в идентификации белловских состояний. ЭПР – источник перепутанных поляризационных состояний был рассмотрен в разд. 3.4, а анализатор белловских состояний $|\Psi^-\rangle_{12}$ – в разд.3.5.

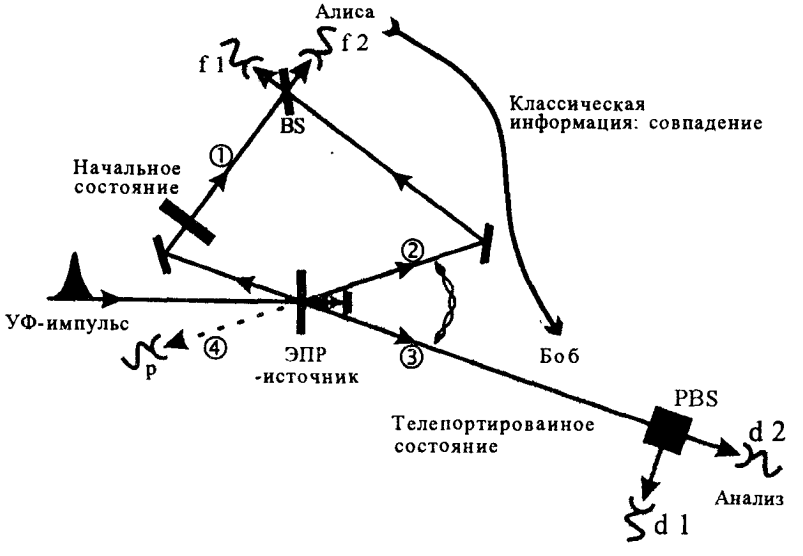


Рис. 3.12. Схематичное изображение экспериментальной установки по квантовой телепортации кубита. Импульс ультрафиолетового лазера, проходящий через кристалл, образует пару перепутанных фотонов 2 и 3. После отражения, во время повторного прохода через тот же кристалл, импульс дает другую пару фотонов, один из которых будет использован для приготовления начального состояния фотона 1 (поляризационное состояние которого предназначено для телепортации). Другой служит в качестве индикатора, сигнализирующего о том, что телепортируемый фотон (точнее его состояние), присутствует в схеме. Алиса наблюдает за совпадениями после светоделителя (BS), где перемешиваются начальный фотон 1 и один из вспомогательных. Боб, после получения классической информации о том, что Алиса зарегистрировала совпадение отсчетов детекторов f 1 и f 2 , что идентифицирует белловское состояние $|\Psi^-\rangle_{12}$, знает, что его фотон 3 имеет точно такое же состояние, как и исходный фотон 1. Он может проверить это, используя поляризационный анализ, проводимый при помощи поляризационного делителя (PBS) и детекторов d 1 и d 2 . Детектор P обеспечивает информацию о том, что фотон 1 действительно присутствует в схеме.

Экспериментальная демонстрация квантовой телепортации кубитов, представленная в этом разделе, ограничивается использованием проектирования только в белловское состояние $|\Psi^-\rangle_{12}$. Унитарное преобразование, которое должен выполнить Боб после измерения Алисой фотонов 1 и 2 (единственное измерение, доступное Алисе в этой схеме – это измерение состояния $|\Psi^-\rangle_{12}$) – это просто тождественное преобразование, т.е. Боб должен зарегистрировать фотон в том же состоянии, что и фотон 1[10].

Чтобы не допустить генерации независимых фотонов 1 и 2, отличающихся по времени регистрации детекторами, что не дало бы возможности измерить состояние Белла, использовалась следующая методика. Фотон 2, совместно с его перепутанным партнером – фотоном 3, генерировались в процессе СПР света. Импульсы накачки, получаемые после удвоения частоты титан-сапфирового лазера с модуляцией добротности, имели длительность 200 фс. Импульсы накачки после отражения от зеркала повторно проходили через кристалл и вызывали рождение второй пары фотонов 1 и 4. Фотон 4 использовался как сигнал, подтверждающий наличие фотона 1. Таким образом фотоны 1 и 2 оказывались локализованными в пределах длительности импульса 200 фс. Их, возможно более полное, перекрытие во времени на детекторах достигалось с помощью регулируемой задержки. Это, однако, еще не гарантировало неразличимости при регистрации, т.к. перепутанные фотоны при СПР, обычно имеют длину когерентности, характерную для волнового пакета длиной 50 фс, что меньше длительности импульсов накачки. Поэтому, регистрация совпадений фотоотсчетов от фотонов 1 и 2 с их партнерами 3 и 4 с временным разрешением лучше, чем 50 фс, могло бы, в принципе, показать, какие фотоны составляли пару. Для достижения неразличимости при регистрации волновые пакеты должны были быть растянуты до длительности, превосходящей длительность импульса накачки. В эксперименте это достигалось с помощью узкополосных интерференционных фильтров (4 нм) помещенных перед детекторами. Такая фильтрация давала волновые пакеты с длительностью около 500 фс, что приводило к степени неразличимости фотонов порядка 85% [101].

[10] В эксперименте, который рассматривается в настоящем разделе, Боб действительно выполняет тождественное преобразование, т.е. ничего не делает с фотоном 3. В оригинальной версии [74] Боб не измеряет поляризационное состояние фотона 3, а выполняет одно из четырех унитарных преобразований, изменяя поляризацию проходящего фотона. Только при идентификации одного из четырех белловских состояний, а именно $|\Psi^-\rangle$, что происходит в 25 % случаев, Бобу нужно сохранить поляризацию фотона 3 без изменения (см также [Д.Н.Клышко. К теории интерпретации эффекта «квантовой телепортации», ЖЭТФ, вып. 4 (10), 1171 – 1187 (1998)]). (*Прим. переводчика.*)

Все существенные компоненты экспериментальной установки по *квантовой телепортации были обсуждены выше. Таким образом, мы* подошли к вопросу о том, как с помощью такой установки экспериментально подтверждается утверждение о том, что неизвестное квантовое состояние может быть телепортировано. Для этого, нужно доказать, что телепортация работает для набора неизвестных неортогональных состояний. Проверка с помощью неортогональных состояний необходима для демонстрации решающей роли квантового перепутывания в схеме телепортации[11].

3.7.1 Экспериментальные результаты

В первом эксперименте фотон 1, в котором был закодирован начальный кубит, приготавливался в состоянии с линейной поляризацией под углом 45°. Телепортация должна происходить, как только фотоны 1 и 2 детектируются в состоянии $|\Psi^-\rangle_{12}$. Это означает, что если регистрируется совпадение отсчетов между детекторами f1 и f2 (Рис. 3.12), т.е. фотоны 1 и 2 проектируются в состояние $|\Psi^-\rangle_{12}$, то фотон 3 должен оказаться поляризованным под углом 45° (с точностью до несущественного знака, см. (3.6)). Поляризация фотона 3 анализируется при его прохождении через поляризационный светоделитель, выделяющий поляризации + 45° и – 45°. Для демонстрации телепортации необходимо, чтобы только детектор d2, находящийся в выходной моде поляризационного светоделителя «+ 45°», зарегистрировал фотон, как только произойдет совпадение отсчетов между f1 и f2. Детектор d1, расположенный в моде «– 45°», при этом не должен регистрировать фотон. Поэтому, запись тройного совпадения d2-f1- f2 (+ 45°- анализ) вместе с отсутствием тройного совпадения d1-f1-f2 (– 45°-анализ) служит доказательством того, что поляризация фотона 1, представляющего начальный кубит, была передана фотону 3.

Чтобы удовлетворить условию неразличимости между фотонами 1 и 2 (см. предыдущий раздел), время прихода фотона 2 варьировалось путем внесения задержки между первым и вторым актами спонтанного излучения пар фотонов. Это достигалось с помощью перемещения отражающего зеркала (см. Рис.3.12). Телепортация должна происходить внутри области временного перекрытия фотонов 1 и 2.

Вне этой области фотоны 1 и 2 независимо попадают либо в детектор f1, либо в f2. Вероятность получения совпадения между де-

[11] Эта причина аналогична той, которая возникает при мотивации использования неортогональных состояний для построения неравенств Белла (см. разд.1.7 и приводимые там ссылки).

текторами f1 и f2, поэтому оказывается 50%. Это значение вдвое превышает вероятность внутри области телепортации, т.к. только компонента $|\Psi^-\rangle$ двухфотонного состояния, попадающего на светоделитель, будет приводить к совпадениям. Поскольку фотон 2 является частью перепутанного состояния, он сам по себе не имеет поляризации, и совместное состояние фотонов 1 и 2 составляет равновесовую суперпозицию всех четырех состояний Белла, независимо от состояния фотона 1. Фотон 3 также не должен проявлять поляризационных свойств, т.к. он является перепутанным с фотоном 2. Поэтому, оба детектора d1 и d2 имеют 50%-ую вероятность регистрации фотона 3. Этот простой аргумент приводит к 25%-ой вероятности событий, как для –45°-анализа (совпадения d1-f1-f2), так и для +45°-анализа (d2-f1-f2) вне области телепортации.

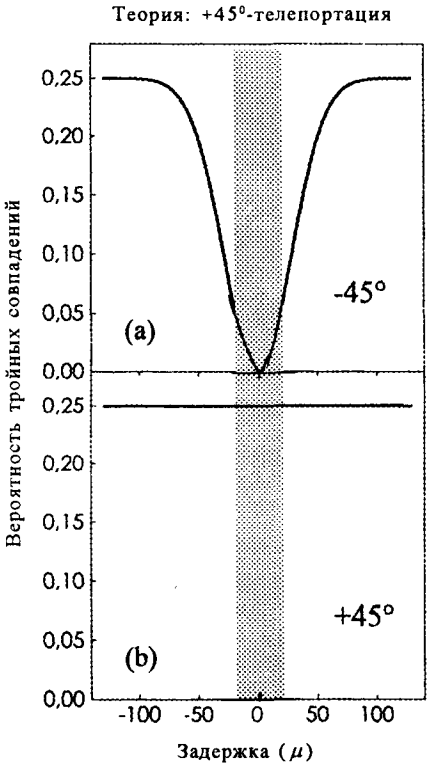


Рис. 3.13. Теоретическое предсказание поведения вероятности тройных совпадений между двумя детекторами в анализаторе состояний Белла (f1 и f2) и одним из детекторов, анализирующим телепортируемое состояние. Признак телепортации поляризационного состояния фотона (+45°) – провал до нуля скорости счета тройных совпадений при нулевой задержке в –45°-анализе (d1-f1-f2) (*a*) и постоянный уровень сигнала при +45°-анализе (d2-f1-f2) (*b*). Затененная область обозначает область телепортации.

На Рис.3.13 показаны вероятности тройных совпадений как функции задержки. Успешная телепортация +45°-го поляризационного состояния характеризуется уменьшением вероятности до нуля при –45°-анализе, см. Рис. 3.13a и постоянной вероятностью при выполнении –45°-анализа, см. Рис. 3.13b. Заметим, что приведенные выше аргументы относятся к вероятности наблюдения события d1-f1-f2 (d2-f1-f2) при условии срабатывания контрольного детектора p (см. рис.3.12).

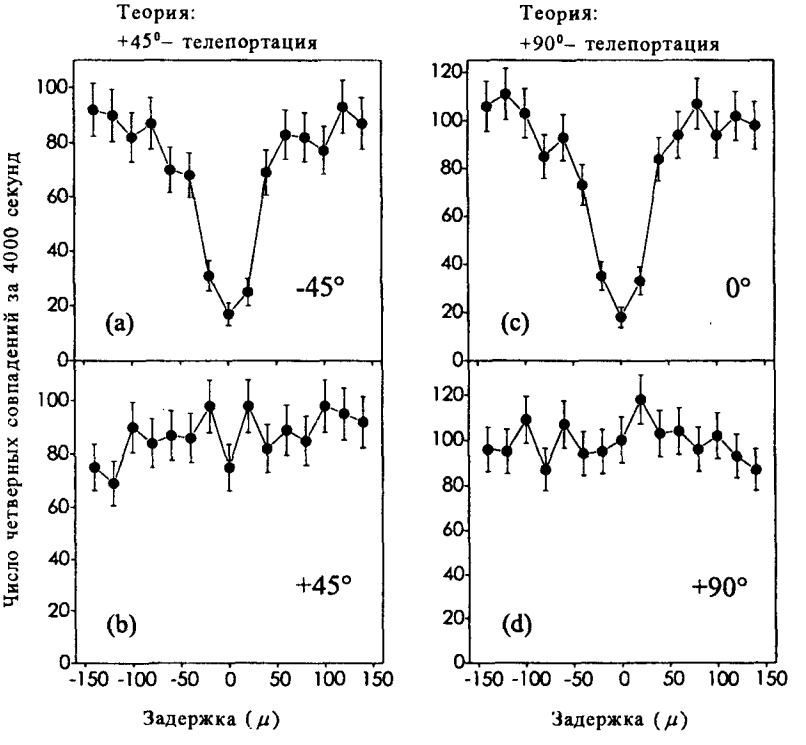


Рис. 3.14. Экспериментальная демонстрация телепортации кубитов. Измеренные скорости счета совпадений d1-f1-f2 (–45°) d2-f1-f2 (+45°) в случае, когда состояние телепортированного фотона составляет +45° (*a*) и (*b*) или +90° (*c*) и (*d*) при условии детектирования вспомогательного фотона детектором p. Скорости счета четверных совпадений нанесены как функции задержки (в мкм) между прибытием фотонов 1 и 2 на светоделитель Алисы (см. рис.3.12). Эти данные в совокупности с рис. 3.13, подтверждают факт телепортации произвольного состояния кубита.

Экспериментальные результаты по телепортации фотонов, поляризованных под углом +45°, представлены в первой колонке Рис. 3.14. Рисунки 4.14a и 3.14b надо сравнивать с теоретическими предсказаниями, показанными на Рис. 3.13.

Резкое уменьшение числа совпадений при –45°-анализе и посто-

янный уровень сигнала при +45°-анализе подтверждает, что фотоны 3 поляризованы вдоль направления поляризации фотонов 1, в соответствии с протоколом квантовой телепортации. Отметим еще раз, что в этих экспериментах использовались четверные совпадения, где четвертый фотон являлся вспомогательным, подтверждающим наличие фотона 1.

Чтобы предотвратить любые попытки объяснения экспериментальных результатов с классической точки зрения, были проведены измерения четверных совпадений в случае телепортации +90°-ых поляризационных состояний, т.е. для состояний не являющихся ортогональными к +45°-го состояния. Экспериментальные результаты показаны на Рис. 3.14c и 3.14d. Была зарегистрирована видность около 70%±3% при измерении «провалов» в случае ортогонально поляризованных состояний.

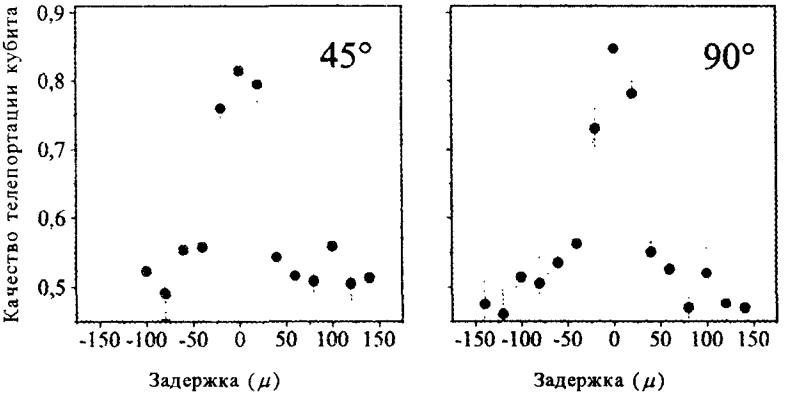


Рис. 3.15. Качество телепортации кубита, закодированного в поляризации однофотонного состояния. Степень наложения начального кубита с телепортированным, определенная при помощи техники четверных совпадений, составила 80%.

Из результатов, показанных на Рис. 3.14, можно непосредственно получить «качество» телепортации кубита, закодированного в поляризации однофотонного состояния. «Качество» (fideliti) определяется как мера совпадения начального кубита с телепортированным, и показано на Рис.3.15. В эксперименте регистрация телепортированных фотонов играла двойную роль: с одной стороны это использовалось в качестве фильтрации только тех событий, в которых был задействован начальный кубит, а с другой – для измерения качества процедуры телепортации. По поводу фильтрации заметим, что анализатор белловских состояний Алисы мог зарегистрировать два события, вызванных генерацией двух пар коррелированных фотонов при повторном прохождении (отраженного) импульса накачки через нелинейный кристалл. В этом случае

Боб вообще не будет наблюдать фотонов [83], а у детектора **p** окажутся два фотона. Такие исходы могут быть идентифицированы, и следовательно, исключены из рассмотрения с помощью детектора **p**, который позволяет различить одно- и двух-фотонные состояния [102].

Независимо от того, используется такая модифицированная схема регистрации или нет, измеренное качество будет одним и тем же [84]. Главным образом оно определяется степенью неразличимостью фотонов, регистрируемых Алисой в анализаторе состояний Белла. Мера неразличимости непосредственно связана с соотношением между спектральной шириной импульса накачки и интерференционных фильтров. Чем больше это отношение, тем выше качество, но меньше полезные сигналы.

3.7.2 Телепортация перепутывания

В рассмотренном эксперименте, вместо использования четвертого фотона, как вспомогательного, показывающего, что фотон 1 имеется в наличии, можно попытаться исследовать тот факт, что фотоны 1 и 4 также могут быть приготовлены в перепутанном состоянии, скажем, в состоянии, как показано на Рис.3.16.

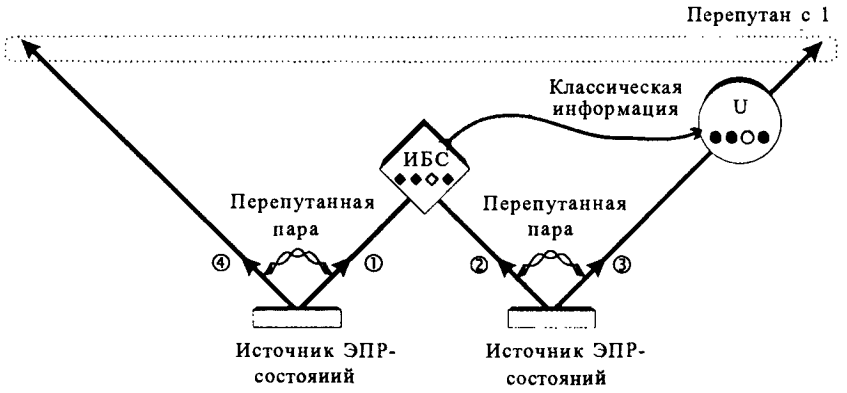


Рис. 3.16. Принцип обмена перепутыванием. Два источника ЭПР-состояний дают две пары перепутанных фотонов – пару 1–4 и пару 2–3. Два фотона, по одному из каждой пары (фотоны 1 и 2), измеряются в анализаторе белловского состояния. В результате другие два фотона 3 и 4 проектируются в перепутанное состояние.

Состояние фотона 1, поэтому, полностью не определено и вся информация заключена в совместных свойствах фотонов 1 и 4. Если фотон 1 подвергается квантовой телепортации, как рассматривалось в предыдущем разделе, фотон 3 приобретает свойства фотона 1 и поэтому становится перепутанным с фотоном 4 (см. Рис. 3.16). Интересно,

что фотоны 4 и 3 получены от разных источников и никогда не взаимодействовали непосредственно друг с другом; тем не менее, в результате процедуры квантовой телепортации, они образуют перепутанную пару. Экспериментальная проверка такого эффекта передачи перепутывания [86], известного как обмен перепутыванием, и несколько его возможных применений [85, 87], будут рассмотрены в разд.3.10 и 3.11.

3.7.3 Заключительные замечания и перспективы

При переносе кубита, закодированного в поляризационном состоянии одного фотона на другой кубит, использовались пары фотонов, перепутанных по поляризациям, и методы двухфотонной интерферометрии. Телепортация также была реализована в других оптических системах, которые будут обсуждаться в двух следующих разделах. Однако эффект квантовой телепортации не ограничивается только оптическими экспериментами. Наряду с парами перепутанных фотонов можно приготавливать перепутанные атомы [103], а также, в принципе, перепутывать фотоны с атомами или фононы с ионами и т.д. Тогда телепортация позволила бы перенести, например, состояние коротко-живущей, быстро распадающейся частицы на какие-нибудь более стабильные системы. Это открыло бы новые возможности для квантовой памяти, где информация входящих фотонов регистрировалась бы на ионах (атомах) в ловушках, тщательно изолированных от окружения.

Более того, при наличии механизмов «очищения» перепутывания [49] (см.гл. 8), т.е. схемы по улучшению степени перепутывания, когда она уменьшается из-за декогерентности при удержании или пропускании частиц через зашумленный канал, становится возможным передавать квантовое состояние частицы в определенное место. Этого можно добиться, даже если доступные квантовые каналы имеют ограниченное качество, т.е. посылка частицы как целого, могла бы разрушить хрупкое квантовое состояние. Если квантовое состояние передается через зашумленный квантовый канал на слишком большое расстояние, то качество передачи становится слишком низким и использование стандартных методов выделения сигнала затруднительно. В такой ситуации метод квантового повторителя позволяет разделить квантовый канал на короткие участки, которые очищаются по отдельности, а затем, объединяются методом обмена перепутыванием [104] (разд.8.7). Способность сохранить квантовые состояния в условиях неблагоприятного окружения даст огромные преимущества в области квантовой коммуникации и квантовых вычислений.

3.8 Схема квантовой телепортации двух частиц

Д. Боумейстер

Схема телепортации, рассмотренная в разд. 3.3, содержит две новые концепции. Во-первых, показано, как можно использовать перепутывание в качестве составного элемента канала квантовой передачи информации. Во-вторых, продемонстрировано, что информация, связанная с состоянием квантовой частицы, физически может быть разложена на классическую компоненту и чисто квантовую, а затем восстановлена из них обратно. Ни одна из этих компонент не содержит никакой информации о начальном квантовом состоянии, но будучи соединены вместе, они определяют это состояние полностью.

В предыдущем разделе эти концепции демонстрировались в трех- и четырехфотонных экспериментах. Недостаток этих экспериментов состоял в том, что Алиса не могла выполнить полное измерение белловских состояний, что уменьшало эффективность телепортации квантового состояния. Полное измерение состояний Белла подразумевало бы управляемое взаимодействие между двумя фотонами, что чрезвычайно трудно осуществить на практике[12]. В этом разделе рассматривается схема, предложенная С.Попеску [77] и экспериментально реализованная в Риме, лишена этого недостатка, но накладывает некоторые ограничения на передаваемые квантовые состояния.

В оригинальном варианте схемы телепортации задействованы три частицы. Две из них находятся в перепутанном (синглетном) состоянии, причем первая посылается Алисе, а вторая – Бобу; они образуют «нелокальный канал связи». Третья частица изначально находится в состоянии Ψ, именно это состояние и должна передать Алиса. Можно предположить, что частица была приготовлена в этом состоянии третьим участником – «Ассистентом», или, что Алиса получила его непосредственно извне. Схема, рассматриваемая здесь, содержит только две частицы, причем одна из них приходит по нелокальному каналу. «Ассистент» должен помочь Алисе закодировать Ψ прямо в ее компоненте синглетной пары, вместо того, чтобы кодировать Ψ в третьей частице. Для этого «Ассистент» использует какую-то степень свободы частицы Алисы, отличающуюся от той степени свободы, по которой частица перепутана с другой, находящейся у Боба. Это отнюдь не облегчает задачу Алисы. Алиса по прежнему не может распознать,

[12] Такое взаимодействие, основанное на нелинейно-оптическом процессе генерации суммарной частоты, было недавно осуществлено в работе [Y. H. Kim, S.P.Kulik, Y. Shih, Quantum Teleportation with a Complete Bell State Measurement. Phys. Rev. Lett. 86, № 7, 1370 – 1373 (2001) (*Прим. переводчика*).

что из себя представляет Ψ. Поэтому, если бы она не смогла воспользоваться классическим каналом, она и не смогла бы помочь Бобу приготовить его частицу в состоянии Ψ. Однако, используя нелокальный квантовый канал, Алиса в состоянии выполнить свою задачу, передавая квантовое состояние Бобу.

В такой двухчастичной схеме действия Алисы проще, чем в трехчастичной схеме. Это связано с тем, что заставить взаимодействовать разные степени свободы одной частицы проще, чем заставить взаимодействовать две разные частицы.

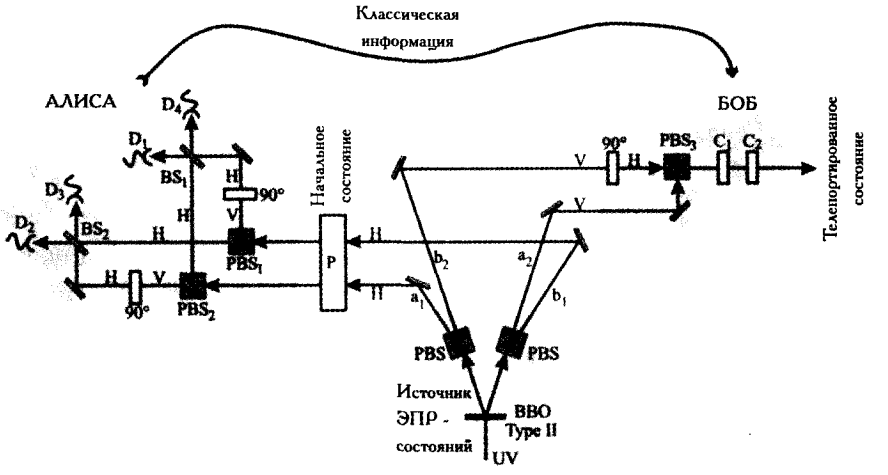


Рис. 3.17. Экспериментальная схема двухчастичного протокола квантовой телепортации. Установка состоит из источника СПР с синхронизмом типа II (кристалл BBO) для генерации перепутанных по поляризации фотонов; поляризационного светоделителя (PBS); 50/50 светоделителей (***PB***); однофотонных детекторов (D); пластинок, поворачивающих поляризацию на 90^0; «Ассистента» (P) исходного квантового состояния и преобразователей поляризации (C).

Мы будем рассматривать протокол двухчастичной квантовой телепортации двигаясь шаг за шагом по оптической экспериментальной установке, предложенной в работе [77]. Первый шаг состоит в приготовлении двух фотонов, перепутанных в направлении их распространения, т.е. по импульсам. Поляризация каждого фотона имеет определенное значение. В прямоугольнике, заключающем в себе источник ЭПР-состояний (Рис. 3.17), показано, как это можно сделать [78]. Используя СПР с синхронизмом типа II, сначала приготавливается поляризационное перепутанное состояние

$$\left|\Psi^{+}\right\rangle=\frac{1}{\sqrt{2}}\left(\left|H\right\rangle_1\left|V\right\rangle_2+\left|V\right\rangle_1\left|H\right\rangle_2\right)\ , \tag{3.24}$$

где индексы 1 и 2 обозначают направления распространения коррелированных фотонов. Фотоны проходят через поляризационные светоделители, которые отражают (пропускают) горизонтальную (вертикальную) поляризацию. Этот процесс преобразует поляризационное перепутывание в перепутывание по импульсам, и состояние фотонов приобретает вид

$$\frac{1}{\sqrt{2}}\left(|a_1\rangle|a_2\rangle+|b_1\rangle|b_2\rangle\right)|H\rangle_1|V\rangle_2 . \qquad (3.25)$$

Теперь индексы 1 и 2 обозначают спаренные каналы, ведущие к Алисе и Бобу, соответственно. Фотоны с индексом 1 обязательно имеют H-поляризацию, а фотоны с индексом 2 – V-поляризацию. Перепутывание фотонов по импульсу и образует нелокальный канал передачи.

На пути к Алисе фотон 1 перехватывается «Ассистентом» P, который изменяет его поляризацию с H на произвольную квантовую суперпозицию

$$|\Psi\rangle_1=\alpha|H\rangle_1+\beta|V\rangle_2 \qquad (3.26)$$

«Ассистент» воздействует на поляризацию обеих частей канала a_1 и b_1 совершенно одинаково. Состояние $|\Psi\rangle$ – это квантовое состояние, которое Алиса хочет передать Бобу. Заметим, что использование двух степеней свободы –поляризационной и импульсной – принципиально[13]. Полное состояние $|\Phi\rangle$ двух фотонов после приготовления имеет вид

$$|\Phi\rangle=\frac{1}{\sqrt{2}}\left(|a_1\rangle|a_2\rangle+|b_1\rangle|b_2\rangle\right)|\Psi\rangle_1|V\rangle_2 , \qquad (3.27)$$

что является формальным аналогом состояния в (3.6).

Следующий шаг протокола состоит в том, что Алиса выполняет совместное измерение (состояния Белла) начального состояния $|\Psi\rangle$ и ее (Алисы) части перепутанного по импульсу состояния. Предполагая, что существует способ спроицировать фотон 1 на четыре белловские состояния для его импульса и поляризации, мы получаем эквивалент соотношения (3.6):

$$\begin{aligned}|\Phi\rangle=\frac{1}{\sqrt{2}}[&\left(|a_1\rangle|V\rangle_1+|b_1\rangle|H\rangle_1\right)\left(\beta|a_2\rangle+\alpha|b_2\rangle\right)|V\rangle_2+\\&+\left(|a_1\rangle|V\rangle_1-|b_1\rangle|H\rangle_1\right)\left(\beta|a_2\rangle-\alpha|b_2\rangle\right)|V\rangle_2+\\&+\left(|a_1\rangle|H\rangle_1+|b_1\rangle|V\rangle_1\right)\left(\alpha|a_2\rangle+\beta|b_2\rangle\right)|V\rangle_2+\\&\left(|a_1\rangle|H\rangle_1-|b_1\rangle|V\rangle_1\right)\left(\alpha|a_2\rangle-\beta|b_2\rangle\right)|V\rangle_2] . \qquad (3.28)\end{aligned}$$

[13] М.Жуковский предложил задействовать пространственные и поляризационные степени свободы частиц при генерации «трехчастичного» ГХЦ-перепутывания, используя только две частицы [105]

Первый сомножитель в каждом слагаемом соответствует состоянию Белла фотона 1, а второй сомножитель – соответствующее состояние фотона 2. В отличие от случая трехчастичного протокола, проектирование частицы 1 в базис состояний Белла не представляет серьезной проблемы и может быть выполнено со 100%-ой эффективностью. Для выполнения операции проицирования необходимо перепутать поляризационные и импульсные свойства фотона 1. Это делается с использованием поляризационных светоделителей в плечах a_1 и b_1 и перемешивая V- компоненты, поступающие из a_1 ($|a_1\rangle|V_1\rangle$) с H-компонентами, поступающими из b_1 ($|b_1\rangle|H_1\rangle$) и наоборот. Конфигурация, чувствительная к относительной фазе, получается, если направить фотоны с одинаковой поляризацией на неполяризационный светоделитель и дать им проинтерферировать. Регистрация фотонов детекторами D_1, D_2, D_3, или D_4 непосредственно отвечает проицированию в одно из четырех белловских состояний.

Последний шаг протокола состоит в том, что Алиса информирует Боба, какой из детекторов зарегистрировал фотон. Обладая такой информацией, Боб может воспроизвести начальное поляризационное состояние следующим образом. Сначала он преобразует импульсную суперпозицию фотона 2 (см. (3.28)) в такую же поляризационную суперпозицию, просто повернув поляризацию в плечах b_2 (или a_2) на 90° с помощью фазовой пластинки и совместив оба пучка поляризационным делителем. После этого, он просто переключает два оптических элемента, в зависимости от той информации, которую ему передает Алиса. Переключения состоят в смене поляризаций H на V и во внесении относительного сдвига фаз на π между H и V. Эти манипуляции преобразуют поляризационное состояние фотона 2 в поляризационное состояние, приготовленное на фотоне 1, и, таким образом, завершают копирование.

Преимущество представленной схемы состоит в том, что выполняется полное измерение состояний Белла и задействовано только две частицы. При этом демонстрируются две основные концепции телепортации: доказывается, что квантовая информация расщепляется на классическую и чисто квантовую части и, что происходит нелокальная передача. Более того, такая схема имеет гораздо более высокую эффективность по сравнению с трех-частичной, рассмотренной в предыдущем разделе.

Недостатком предлагаемого метода является то, что Алиса не может телепортировать состояние частицы, приходящей извне. Поэтому и требуется помощь «Ассистента»: начальное поляризационное состояние данное Алисе, должно быть приготовлено на частице, перепутанной по импульсу с той, которая имеется у Боба. Кроме того, состояние Ψ должно быть чистым, т.е. оно не может быть частью перепутанного состояния.

Мы отсылаем читателя к работе [78], в которой приводятся детали экспериментальной реализации установки, рассмотренной выше. Там же обсуждаются экспериментальные результаты, подтверждающие передачу квантового состояния от Алисы к Бобу.

Мы крайне признательны С.Попеску за помощь при подготовке этого раздела.

3.9 Телепортация непрерывных квантовых переменных

Д.Боумейстер

3.9.1 Применение перепутывания координаты и импульса

В этом разделе мы рассмотрим основную идею другой схемы квантовой телепортации, предложенной Л.Вайдманом [79], разработанной, впоследствии, Браунстайтом и Кимблом [80] и реализованной экспериментально в Калтеке [81]. В этой схеме используется перепутывание между координатой и импульсом. В результате, в этом варианте квантовой телепортации координата и импульс (определяющие внешнее состояние) квантовой системы передаются к другой – удаленной квантовой системе, в отличие от схем, обсуждаемых в разд.3.7 и 3.8, где передавалось внутреннее состояние (поляризация). Важное отличие между координатой и импульсом, с одной стороны и поляризации – с другой, заключается в том, что они по-разному представляются в терминах суперпозиции определенных базисных состояний. Для описания координаты и импульса требуется бесконечное число базисных состояний, т.к. любым двум различным координатам и импульсам отвечают два разных ортогональных собственных состояния (собственные состояния координаты и собственные состояния импульса образуют бесконечномерное гильбертово пространство).

Рассмотрим случай, когда у Алисы имеется квантовая частица с определенными координатой x_1 и импульсом p_1 (см. Рис. 3.18) и Алиса хочет отправить эту квантовую информацию Бобу, который находится на некоторм расстоянии от нее. В следствие принципа неопределенности Гейзенберга в отношении к x и p, (т.е. из-за того, что операторы координаты и импульса не коммутируют $[\hat{x}, \hat{p}] = i\hbar$), Алиса не может измерить одновременно x_1 и p_1 с произвольной точностью. Поэтому квантовая механика запрещает Алисе узнать ту информацию, которую она передает. Способ преодоления этой проблемы концептульно такой же, как и в протоколе, рассмотренном в разд.3.3. Точно так же вспомогательная пара перепутанных частиц, полученная из ЭПР-источника (Рис.3.18) должна быть распределена между Алисой и Бобом.

Однако, вспомогательные частицы должны быть перепутаны по их координате и импульсу. Рассмотрим случай, в котором перепутывание частиц 2 и 3 определяется условиями:

$$x_2 + x_3 = 0\,, \text{ и } \; p_2 - p_3 = 0 \tag{3.29}$$

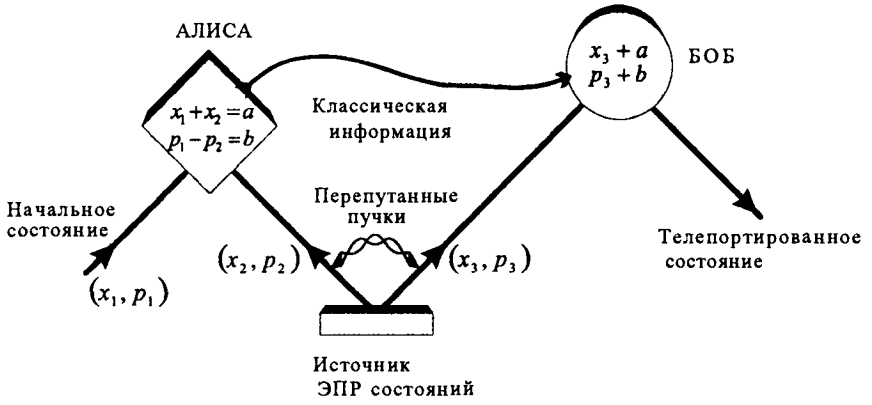


Рис. 3.18. Схематичное изображение квантовой телепортации непрерывных переменных.

Из (3.29) следует, что свойства x_2, x_3, p_2 и p_3 отдельных частиц совершенно неопределены. Вместо этого определены их совместные свойства. Заметим, что хотя для каждой частицы операторы $\hat{x}$ и $\hat{p}$ не коммутируют, операторы $(x_2 + x_3)$ и $(p_2 - p_3)$ коммутируют, из-за знака минус в сумме импульсов по сравнению с суммой координат. Поэтому для перепутанного состояния совместные свойства и $(x_2 + x_3)$ и $(p_2 - p_3)$ могут быть одновременно измерены с произвольной точностью.

Следующий шаг протокола состоит в том, что Алиса выполняет действие, эквивалентное измерению состояний Белла частиц 1 и 2. Т.е. состояние частиц 1 и 2 проектируется на перепутанное состояние. При телепортации внутреннего состояния частицы (поляризации) существует только 4 возможных исхода при измерении белловских состояний. Действительно, перепутывание по поляризации между двумя частицами, каждая из которых находится в двумерном гильбертовом пространстве, представимо в виде суперпозиции 4 базисных состояний. В нашем случае измерение Алисы дает

$$(x_2 + x_3) = a\,, \text{ и } \; (p_2 - p_3) = b\,, \tag{3.30}$$

где a и b – два действительных числа, принимающие непрерывный ряд возможных значений. Отсюда следует, что измерение суммы

координат и разности импульсов двух частиц требует проицирования в ∞-мерное гильбертово пространство.

В результате исходного перепутывания (3.29) и измерения Алисы (3.30), информация, полученная о квантовом состоянии и находящаяся в руках Боба, представляется в виде

$$x_3 = x_1 - a \quad \text{и} \quad p_3 = p_1 - b. \tag{3.31}$$

Для завершения протокола квантовой телепортации, единственное, что остается сделать Алисе – это послать Бобу по классическому каналу результат ее измерений, т.е. измеренные значения a и b, и тогда Боб просто обнаружит значение координаты и импульса своей частицы, соответственно, равными a и b. В итоге частица 3, находящаяся у Боба, оказывается в том же квантовом состоянии, что и исходная частица 1.

3.9.2 Квантово-оптическая реализация

Экспериментальная реализация квантовой телепортации непрерывных квантовых переменных была осуществлена в Калтеке (Калифорния, США) [81]. В этом эксперименте были задействованы не координата x и импульс p частиц, а пучки света, которые характеризовались параметрами, удовлетворяющими таким же коммутационным соотношениям, как между $\hat{x}$ и $\hat{p}$. Аналогия основана на том факте, что одна (поперечная) мода квантованного поля излучения описывается так же, как и гармонический осциллятор [106-109].

Классический гармонический осциллятор с массой m, частотой ω, координатой x и импульсом p описывается гамильтонианом

$$H = \frac{p^2}{2m} + \frac{m}{2}\omega^2 x^2 . \tag{3.32}$$

Для получения квантово-механического гамильтониана, x и p нужно интерпретировать как операторы ($x \to \hat{p}$, и $x \to \hat{p} = i\hbar\partial/\partial x$), удовлетворяющие коммутационному соотношению $[\hat{x}, \hat{p}] = i\hbar$

$$\hat{x} = \sqrt{\frac{\hbar}{2m\omega}}\left(\hat{a}^\dagger + \hat{a}\right) , \tag{3.33}$$

$$\hat{p} = \sqrt{\frac{\hbar}{2m\omega}}\left(\hat{a}^\dagger - \hat{a}\right) . \tag{3.34}$$

Тогда гамильтониан квантованного гармонического осциллятора принимает привычный вид

$$\hat{H} = \hbar\omega\left(\hat{a}^\dagger\hat{a} + \frac{1}{2}\right). \tag{3.35}$$

Наиболее важные соотношения между a и $a^\dagger$ таковы:

$$\hat{a}|n\rangle = \sqrt{n}|n-1\rangle \ , \quad \hat{a}|0\rangle = 0 \ , \tag{3.36}$$

$$\hat{a}^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle \ , \tag{3.37}$$

$$\left[\hat{a},\hat{a}^\dagger\right] = 1 \ , \quad \left[\hat{a},\hat{a}\right] = \left[\hat{a}^\dagger,\hat{a}^\dagger\right] = 0 \tag{3.38}$$

$$\hat{a}^\dagger\hat{a} = \hat{N} \ , \tag{3.39}$$

где $|n\rangle$ обозначает n-ое возбужденное состояние гармонического осциллятора и $\hat{N}$ – оператор числа частиц. Согласно (3.36) и (3.37) $\hat{a}$ и $\hat{a}^\dagger$ могут интерпретироваться как операторы уничтожения (понижающий оператор) и рождения (повышающий оператор) для гармонического осциллятора.

Одна поперечная мода (с частотой ω) квантованного поля излучения может быть представлена в терминах операторов a и $a^\dagger$. В наиболее общем виде, включая все несущественные множители в один коэффициент E_0 и учитывая только одну поляризацию, оператор электрического поля в фиксированной точке принимает вид

$$\hat{E}(t) = E_0\left(\hat{a}e^{-i\omega t} - \hat{a}^\dagger e^{+i\omega t}\right) \ , \tag{3.40}$$

где $\hat{a}$ и $\hat{a}^\dagger$ теперь интерпретируются как операторы уничтожения и рождения фотонов. По аналогии с гармоническим осциллятором, можно определить операторы X и P:

$$\hat{X} = \left(\hat{a}^\dagger + \hat{a}\right) \ , \tag{3.41}$$

$$\hat{P} = i\left(\hat{a}^\dagger - \hat{a}\right) \ . \tag{3.42}$$

Оператор электрического поля можно переписать в терминах $\hat{X}$ и $\hat{P}$:

$$\hat{E}(t) = E_0\left(\hat{X}\cos(\omega t) + \hat{P}\sin(\omega t)\right) \ . \tag{3.43}$$

Собственные значения $\hat{X}$ и $\hat{P}$, называемые квадратурными амплитудами поля, интерпретируются как амплитуды синфазной и противофазной компонент электрического поля (по отношению к локальному осциллятору). Из коммутационного соотношения $[\hat{X},\hat{P}]=2i$ следует, что $\Delta X\Delta P = 1$ ($\langle\Delta A\rangle^2 = \langle A^2\rangle - \langle A\rangle^2$); это означает, что синфазная и противофазная амплитуды не могут быть измерены одновременно с произвольной точностью, аналогично тому, как это имеет место для координаты x и импульса p квантовой частицы. Следовательно, мы установили соответствие между x и p частицы и X и P одномодового светового поля.

Следующий шаг в реализации схемы квантовой телепортации непрерывных квантовых переменных состоит в построении перепутан-

ных световых полей. Для этого нам нужно ввести понятие сжатого света [108]. Это полезно для визуализации квантового состояния одномодового светового поля на фазовой плоскости XY. Вакуумное состояние представляется кружком 1 в начале координат (Рис.3.19). Кружок 2 на Рис.3.19 представляет «когерентное поле», которое определяется как смещенное вакуумное поле. Эти кружки характеризуют минимальную неопределенность величин X и P. Неопределенность симметрична по X и P, однако такая симметрия необязательна при выполнении условия $\Delta X \Delta P = 1$. Эллипс на Рис.3.19 представляет сжатое состояние, для которого $(\Delta Y)^2 < 1$, следовательно $(\Delta X)^2 > 1$.

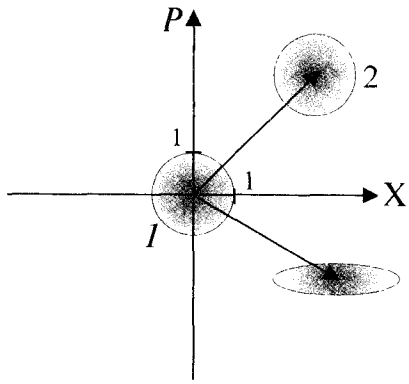


Рис. 3.19. Представление одномодовых световых полей в координатах X (синфазная амплитуда) и P (противофазная амплитуда) на фазовой плоскости. Диск 1 в начале координат изображает симметричное вакуумное состояние с минимальной неопределенностью. Диск 2 представляет когерентное состояние, которое определяется как смещенное вакуумное состояние. Эллипс изображает сжатое состояние (сжатое в P направлении).

Теперь рассмотрим случай, когда два световых поля $\mathcal{A}$ и $\mathcal{B}$ максимально сжаты в направлениях X и Y, соответственно, и направим эти пучки на два входа 50%-ого светоделителя, как показано на Рис.3.20. После светоделителя поля, помеченные индексами 2 и 3, удовлетворяют соотношениям

$$X_2 + X_3 = 0 \text{, и } \quad P_2 - P_3 = 0 , \tag{3.44}$$

что как раз свойственно необходимому перепутанному состоянию [81]. (Для световых полей, перепутанных по поляризации, см. [110-112].)

Приготовление сжатых состояний, так же как и генерация перепутанных состояний, основано на параметрическом усилении в нелинейном кристалле [107, 112, 113]. Входной сигнал – поле с частотой ω_1 взаимодействует в нелинейном кристалле с сильным полем накачки

на частоте ω_3 (см. Рис.3.21). В результате нелинейного взаимодействия возникает третье поле с частотой $\omega_2 = \omega_3 - \omega_1$, а сигнальное поле усиливается. Мы будем рассматривать простейший случай, в котором учитывается только одно направление поляризации и коллинеарный режим фазового синхронизма. Это предполагает, что все поля распространяются в одном направлении. Кроме того, будем рассматривать вырожденный случай, когда, $\omega_1 = \omega_2 \equiv \omega$ и $\omega_3 = 2\omega_2$.

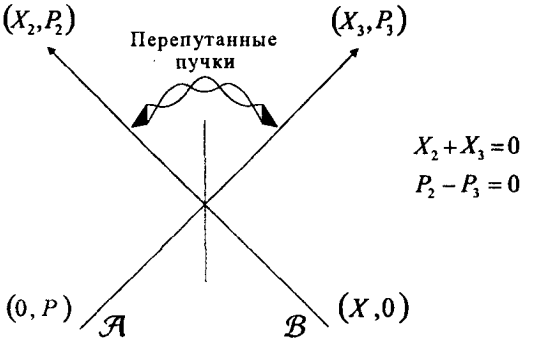


Рис. 3.20. Приготовление перепутанных световых полей. Два световых поля $\mathcal{A}$ и $\mathcal{B}$, максимально сжатые по X и Y, подаются на вход 50%-го светоделителя. На выходе светоделителя образуется пара перепутанных световых пучков.

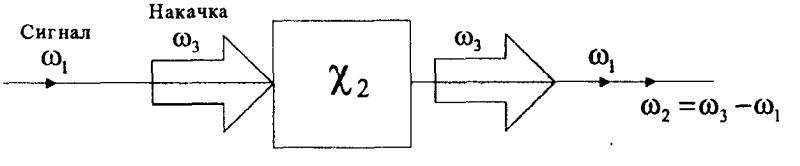


Рис. 3.21. Параметрическое усиление. Входное сигнальное поле с частотой ω_1 взаимодействует в нелинейном кристалле (вещество с $\chi^{(2)}$) с мощным полем накачки с частотой ω_3. В результате такого нелинейного взаимодействия рождается третье поле на частоте $\omega_2 = \omega_3 - \omega_1$, а сигнальное поле усиливаться.

Эволюция излученного на частоте ω поля, взаимодействующего в кристалле с сильным полем на частоте 2ω, описывается гамильтонианом

$$\hat{H} = \hbar\omega\left(\hat{a}^\dagger\hat{a} + \frac{1}{2}\right) + S\cos(2\omega t)\left(\hat{a}^\dagger - \hat{a}\right)^2. \qquad (3.45)$$

Второе слагаемое в правой части (3.45) учитывает взаимодействие между полем накачки, которое описывается классически, и двумя по-

лями с вырожденной частотой ω. S – это постоянная связи, зависящая от нелинейности кристалла и интенсивности накачки. Принимая во внимание закон сохранения энергии, это определяющее взаимодействие слагаемое в (3.45) можно свести к виду

$$S\left((\hat{a})^2 e^{i2\omega t} - (\hat{a}^\dagger)^2 e^{-i2\omega t}\right). \tag{3.46}$$

Зависимость от времени оператора поля (мы работаем в представлении Гейзенберга, где операторы являются функциями времени) учитывается через уравнения эволюции операторов $\hat{a}$ и $\hat{a}^\dagger$:

$$\frac{d\hat{a}}{dt} = -\frac{i}{\hbar}\left[\hat{a}, \hat{H}\right] = -i\omega\hat{a} - iS\hat{a}^\dagger e^{-i2\omega t}, \tag{3.47}$$

$$\frac{d\hat{a}^\dagger}{dt} = -\frac{i}{\hbar}\left[\hat{a}^\dagger, \hat{H}\right] = i\omega\hat{a}^\dagger + iS\hat{a}e^{+i2\omega t}. \tag{3.48}$$

Этот набор связанных уравнений расщепляется, если подставить операторы $\hat{X}$ и $\hat{P}$, которые были определены в (3.41) и (3.42). Уравнения эволюции для операторов квадратурных амплитуд поля имеют вид

$$\frac{d\hat{X}}{dt} = S\hat{X}, \qquad \frac{d\hat{P}}{dt} = -S\hat{P} \tag{3.49}$$

и имеют следующие решения

$$\hat{X}(t) = \hat{X}(0)e^{St}, \qquad \hat{P}(t) = \hat{P}(0)e^{-St}. \tag{3.50}$$

Являясь функциями времени взаимодействия, оператор синфазной амплитуды $\hat{X}$ экспоненциально растет, в то время как оператор $\hat{P}$ экспоненциально уменьшается. Таким образом, вырожденное параметрическое усиление работает как фазово-чувствительный усилитель, обеспечивающий усиление синфазных сигналов ($\varphi = 0 \bmod \pi$) и подавление противофазных ($\varphi = (\pi/2) \bmod \pi$). Другими словами, параметрическое усиление сигнала будет сжимать P-компоненту светового поля.

Для увеличения времени взаимодействия, а следовательно, и степени сжатия, нелинейные кристаллы обычно помещаются внутрь оптического резонатора, настроенного на частоту ω. Такое устройство называется параметрическим генератором света (ПГС). Для того, чтобы не перейти в режим (лазерной) генерации, потери в резонаторе должны слегка превышать усиление. В противном случае, возникают интенсивные световые поля, которые приводят к насыщению внутри кристалла (через нелинейности высших порядков). В эксперименте [81] внешнее поле, подаваемое на вход ПГС на частоте ω, не использовалось, т.е. усиливалась только вакуумная компонента.

Рассмотрев приготовление световых полей типа ЭПР, при использовании двух сжатых полей и светоделителя, вернемся теперь к пробле-

ме осуществления измерения состояний Белла. В то время как создание анализатора белловских поляризационных состояний сталкивается с определенными трудностями (см. разд.3.5), в нашем случае проицирование на перепутанное состояние выполняется очень просто. Смешивая на светоделителе исходный пучок, характеризующийся параметрами (X_1, P_1), с одним из пучков, приходящих из ЭПР-источника, с параметрами (X_2, P_2), мы получаем на выходе светоделителя два пучка, характеризуемыми соотношениями

$$\left(X_{\mathcal{C}}, P_{\mathcal{C}}\right) = \left(X_1 - X_2, P_1 - P_2\right) \text{ и } \left(X_{\mathcal{D}}, P_{\mathcal{D}}\right) = \left(X_1 + X_2, P_1 + P_2\right) \quad (3.51)$$

Используя метод балансного гомодинирования (см. [107]), Алиса измеряет X-компоненту пучка $\mathcal{D}$ и P-компоненту $\mathcal{C}$, и получает значения $a = X_1 + X_2$ и $b = P_1 - P_2$, соответственно, как и требуется протоколом квантовой телепортации. Метод балансного гомодинирования основан на смешении сигнального поля с полем опорного генератора на 50%-ом светоделителе и записи разностного фототока двух детекторов, помещенных в выходные моды светоделителя (фототок каждого детектора пропорционален интенсивности падающего на него света). Разность измерямых интенсивностей является функцией фазы опорного генератора φ [107]:

$$I(\varphi) = C\left(X \sin\varphi + P \cos\varphi\right), \quad (3.52)$$

где C – постоянная, зависящая от интенсивности опорного генератора и свойств детекторов. Перестраивая фазу опорного генератора, можно измерять любую суперпозицию квадратурных компонент.

Следуя протоколу квантовой телепортации, Алиса посылает Бобу измеренные значения a и b, а Боб должен изменить свое оптическое поле соответствующим образом. Это изменение экспериментально выполняется путем отражения светового поля (у Боба) от частично отражающих зеркал (скажем, при 99%-ом отражении и 1%-ом прохождении) и введения через зеркало дополнительного поля, промодулированного по фазе и амплитуде в соответствии со значениями a и b. В принципе, Боб завершает протокол, имея почти совершенную копию светового поля, изначально находившегося у Алисы.

В реальном эксперименте [81] требовалось использование некоторых сложных экспериментальных процедур, таких как генерация сжатых состояний с высокой степенью сжатия и точное выравнивание пространственных положений и фаз световых пучков. Несовершенство этих процедур ограничивало качество, определяемое как измеренное перекрытие входного состояния у Алисы и телепортированного состояния у Боба; оно составило 0.58 ± 0.02. Это качество, однако, превосходит предел 0.5, который может быть достигнут (в предположении, что выходное состояние попадает в класс когерентных состо-

яний) при использовании только классического обмена информацией между Алисой и Бобом.

Мы крайне признательны Г.Дж.Кимблу и Е.С.Полцику за полезные замечания.

3.10 Обмен перепутыванием: телепортация перепутывания

Д.Боумейстер, Дж-В. Пэн, Г.Вайнфуртер, А.Цайлингер

Перепутывание может быть реализовано, если имеются две частицы, испущенные из одного источника [94, 114] (разд.3.4), или если они взаимодействуют друг с другом [103,115]. (разд.4.3, 5.2.4 и 5.2.11). Другая возможность для получения перепутывания состоит в проицировании состояния двух частиц на перепутанное состояние. Такое проекционное измерение не обязательно предполагает прямого взаимодействия между двумя частицами. Когда каждая из частиц перепутана с какой-нибудь другой частицей, соответствующее измерение (например, измерение состояний Белла), выполненное над этими другими частицами, будет автоматически редуцировать состояние оставшихся двух частиц в перепутанное состояние. Это замечательное применение постулата редукции получило название обмена перепутыванием [74. 85, 87].

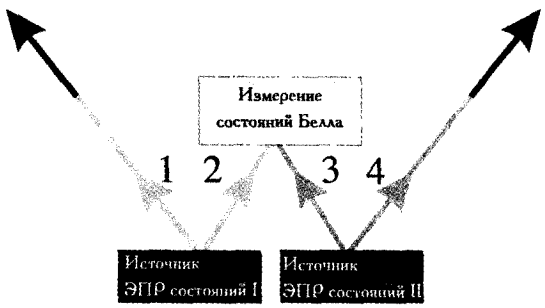


Рис. 3.22. Принцип обмена перепутыванием. Два ЭПР-источника излучают пары перепутанных фотонов 1-2 и 3-4. По одному фотону из каждой пары (фотоны 2 и 3) участвует в процессе измерения состояния Белла. Это приводит к проицированию двух других фотонов 1 и 4 на перепутанное состояние. Изменение насыщенности линий обозначает изменение в наборе возможных предсказаний, которые могут быть сделаны о состоянии частиц.

Рассмотрим два ЭПР-источника, каждый из которых спонтанно излучает пары перепутанных частиц (рис.3.22). Имея в виду экспери-

менты, рассматриваемые ниже, предположим, что состояния перепутанных по поляризации фотонов имеют вид:

$$|\Psi\rangle_{1234} = \frac{1}{2}\left(|H\rangle_1|V\rangle_2 - |V\rangle_1|H\rangle_2\right)\left(|H\rangle_3|V\rangle_4 - |V\rangle_3|H\rangle_4\right) . \qquad (3.53)$$

Общее состояние отражает тот факт, что фотоны 1 и 2 (3 и 4) находятся в перепутанном по поляризации антисимметричном состоянии. Кроме того, состояние пары 1-2 факторизуется с состоянием пары 3-4, т.е. перепутывания между фотонами 1 или 2 с фотонами 3 или 4 не происходит.

Выполним теперь совместное измерение состояний Белла фотонов 2 и 3, т.е. спроектируем фотоны 2 и 3 на одно из четырех белловских состояний (см. разд.3.5). Такое измерение будет также проицировать фотоны 1 и 4 на белловское состояние, такое, которое зависит от результата белловского измерения фотонов 2 и 3. Ясно, что при выборе начального состояния в виде (3.53), конечное состояние фотонов 1 и 4 будет идентично тому, на которое проектируются фотоны 2 и 3. Это следствие того факта, что состояние (3.53) можно переписать в форме

$$|\Psi\rangle_{1234} = \frac{1}{2}\left(|\Psi^+\rangle_{14}|\Psi^+\rangle_{23} - |\Psi^-\rangle_{14}|\Psi^-\rangle_{23} - \right.$$
$$\left. - |\Phi^+\rangle_{14}|\Phi^+\rangle_{23} + |\Phi^-\rangle_{14}|\Phi^-\rangle_{23}\right) . \qquad (3.54)$$

Во всех случаях фотоны 1 и 4 оказываются перепутаны, несмотря на то, что они никогда не взаимодействовали в прошлом. После проицирования частиц 2 и 3 становится известно о перепутывании между частицами 1 и 4.

Как уже отмечалось в разд.3.7.2, обмен перепутыванием можно рассматривать и как телепортацию перепутанного состояния. Этот факт был продемонстрирован с помощью экспериментальной установки (рис.3.23), похожей на установку для квантовой телепортации, показанной на рис. 3.12. Мы отсылаем читателя к разд.3.7, где приводится детальное описание этой установки. Существенное отличие между двумя экспериментами состоит в том, что в схеме телепортации отдельных кубитов (рис.3.12) фотон 4 играл роль индикатора, указывающего на наличие фотона 1, в то время как здесь (рис.3.23), полностью используется перепутывание между каждой парой фотонов.

Обмен перепутыванием можно рассматривать как телепортацию либо состояния фотона 2 на фотон 4, либо состояния фотона 3 на фотон 1. Эти точки зрения полностью эквивалентны. Замечательная особенность этой схемы состоит в том, что в действительности, телепортируемое состояние – это состояние фотона, которое не являет-

ся полностью определенным. Хорошо известно, что состояние частицы, максимально перепутанной с другой, должно описываться максимально смешанной матрицей плотности. Поэтому, то, что телепортируется при данной ситуации не является квантовым состоянием фотона, а просто способом перепутывания его с другим фотоном.

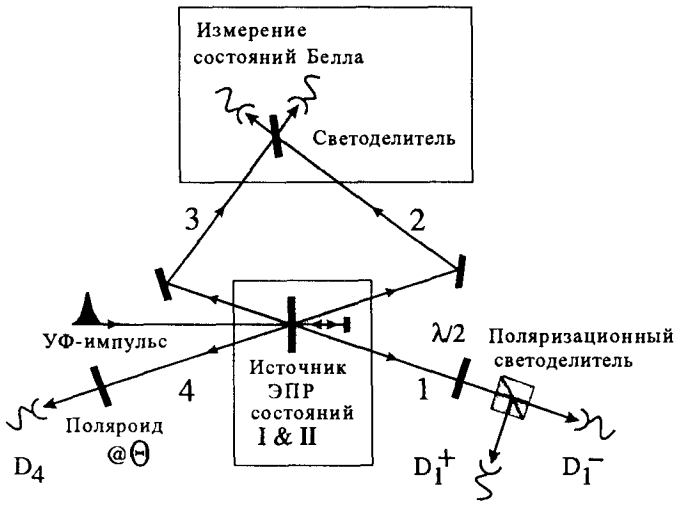


Рис. 3.23. Экспериментальная установка. Ультрафиолетовый импульс накачки, проходящий через нелинейный кристалл, вызывает рождение пары 1-2 перепутанных фотонов. Фотон 2 направляется на светоделитель. После отражения, во время повторного прохода через кристалл, импульс накачки дает вторую пару 3 – 4 перепутанных фотонов. Фотон 3 также направляется на светоделитель. Когда фотоны 2 и 3 вызывают импульс совпадения между отсчетами двух детекторов, помещенных позади светоделителя, фотоны проицируются в состояние $|\Psi^-\rangle_{23}$. Следствием такого измерения состояния Белла является то, что два оставшихся фотона 1 и 4 также оказываются спроицированными в перепутанное состояние. Для анализа их перепутывания можно наблюдать за совпадениями между отсчетами детекторов $D1^+$ и D4, и между декторами $D1^-$ и D4, при разных углах Θ направления поляризации. Поворотом полуволновой пластинки перед поляризационным светоделителем можно анализировать поляризацию фотона 1 в линейном поляризационном базисе. Заметим, что, т.к. регистрация совпадений между отсчетами детекторов $D1^+$ и D4 и $D1^-$ и D4 условная – в зависимости от регистрация состояния Ψ^-, необходимо следить за четверными совпадениями.

В соответствии со схемой обмена перепутыванием, при проектировании фотонов 2 и 3 в состояние $|\Psi^-\rangle_{23}$, фотоны 1 и 4 должны спроицироваться в состояние $|\Psi^-\rangle_{14}$. Для проверки того, что получается именно это перепутанное состояние, мы должны проанализировать поляризационные корреляции между фотонами 1 и 4 одновременно с совпадениями между отсчетами детекторов в анализаторе состояний

Белла. Если фотоны 1 и 4 находятся в состоянии $|\Psi^-\rangle_{14}$, их поляризации должны быть ортогональными при измерении в любом поляризационном базисе[14]. Используя полуволновую пластинку, ориентированную под углом 22.5° и два детектора ($D1^+$ и $D1^-$) позади поляризационного светоделителя, анализируется поляризация фотона 1 вдоль +45° оси ($D1^+$) и вдоль –45° оси ($D1^-$). Фотон 4 анализируется детектором D4 при любых направлениях поляризации Θ.

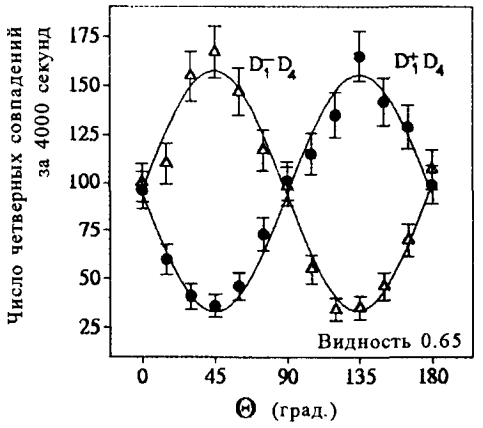


Рис. 3.24. Проверка перепутывания. Четверные совпадения, возникающие из двойных совпадений $D1^+$ D4 и $D1^-$ D4 при условии двойных совпадений при измерении состояния Белла – как функции угла поляризатора Θ. Две дополнительные друг к другу кривые с видностью 0.65 ± 0.02 демонстрируют, что фотоны 1 и 4 находятся в состоянии, перепутанном по поляризации.

Если обмен перепутыванием действительно происходит, то четверные совпадения между $D1^+$ и D4, а также между $D1^-$ и D4, при условии детектирования $|\Psi^-\rangle_{23}$, должны проявлять две синусоидальных кривых, как функций аргумента Θ, сдвинутых по фазе на 90°. Кривая $D1^+$ D4 должна, в принципе, падать до нуля при Θ = 45°, в то время как кривая $D1^-$ D4 – иметь при этом положении максимум. На рис.3.24 показаны экспериментальные результаты для совпадений между $D1^+$ и D4, и между $D1^-$ D4, при условии что фотоны 2 и 3 были зарегистрированы двумя детекторами в анализаторе белловских состояний.

Заметим, что такой метод подразумевает регистрацию четверных совпадений. Результаты четко демонстрируют ожидаемые сину-

[14] В действительности, в обсуждаемых экспериментах проводилась проверка инвариантности состояния $|\Psi^-\rangle_{14}$ только по отношению к повороту линейного ортогонального базиса (*Прим. переводчика*).

соидальные кривые, дополнительные для двух детекторов ($D1^+$ и $D1^-$) при регистрации фотона 1 в направлениях с ортогональными поляризациями. При проведении дополнительных измерений было показано, что эти кривые не зависят (с точностью до фазового сдвига в аргументе Θ) от базиса, в котором регистрируется фотон 1, т.е. независимо от угла поворота полуволновой пластинки. Наблюдаемая видность 0.65 заметно превосходит предел, получающийся из классической волновой теории, и составляющий 0.5. Заметим, что этот результат является реализацией квантовой телепортации в чисто квантовой ситуации, т.к. перепутывание между двумя частицами, не имеющими общего источника и не взаимодействовавшими друг с другом в прошлом, возникает только в результате рассматриваемой процедуры. В следующем разделе будут рассмотрены некоторые приложения эффекта обмена перепутыванием.

3.11 Применение обмена перепутыванием

С.Бозе, В.Ведрал, П.Л.Найт

Обмен перепутыванием может быть использован для целого ряда практических целей: построения квантового *телефонного коммутатора*, *ускорения* распределения перепутанных частиц между двумя частями, в разновидностях *последовательного очищения* и для *построения перепутанных состояний охватывающих большое количество частиц* [87]. Ниже мы детально рассмотрим эти приложения.

3.11.1 Квантовый телефонный коммутатор

Предположим, что имеется N пользователей в некоторой информационной сети. Для начала каждый пользователь сети должен объединиться перепутанными парами частиц с центральным коммутатором. Рассмотрим Рис.3.25: A, B, C и D – это пользователи, имеющие в своем распоряжении перепутанные частицы, находящиеся совместно с центральным коммутатором O в состояниях Белла (1, 2), (3, 4), (5,6) и (7,8) соответственно. Предположим теперь, что A, B и C хотят составить ГХЦ-триплет. Тогда коммутатор O должен суметь выполнить измерение, которое проектирует частицы 2, 3 и 5 на ГХЦ-состояния. Немедленно после этого произойдет редукция частиц 1, 4 и 6, принадлежащих, соответственно, A, B и C в ГХЦ-состояние. Подобным же образом можно перепутать частицы, принадлежащие любым N пользователям сети и создать N-частичное состояние типа ШК.

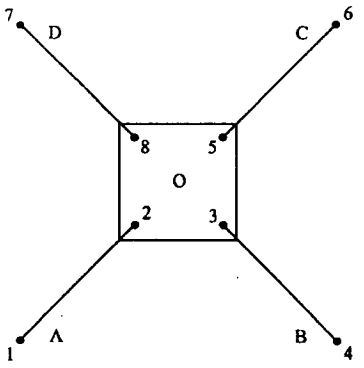


Рис.3.25. Конфигурация, используемая для распределения перепутывания. Изначально пользователи A, B, C и D объединены посредством белловских пар с центральным коммутатором O. Следовательно, локального измерения в т. O достаточно, для того чтобы перепутать частицы, принадлежащие любой выборке пользователей составленной из A, B, C и D.

Основное преимущество использования такой методики для установления перепутывания над генерацией N-частичных перепутанных состояний от одного источника с их последующим перераспределением состоит в следующем.

(А) Во-первых, каждый пользователь может сначала очистить большое количество частично декогерентных белловских пар, объединенных с центральным коммутатором, для того чтобы получить меньшее количество, но чистых белловских пар. Такая операция может использоваться как начальная при генерации любых типов многочастичных состояний типа шредингеровской кошки (ШК), имеющихся у пользователей. Представляется, что таким образом будут решены проблемы, связанные с возникновением декогерентности при распространении частиц (по крайней мере, в принципе). Так же, полностью удается избежать проблемы необходимости очищения N-частичных ШК-состояний. Очищение синглетных состояний, рассмотренных в нашей схеме, позволит генерировать N-частичные состояния в их наиболее чистом виде.

(Б) Во-вторых, при необходимости, наш метод дает определенную свободу в перепутывании частиц, принадлежащих любому набору пользователей. Возможно, что заранее не будет точно известен тот набор пользователей, которых нужно объединить N-частичным состоянием. Чтобы *a-priori* учесть все возможности, потребовалось бы выделить все мыслимые комбинации пользователей и распределяемых между ними частиц, находящихся в многочастичных состояниях. Это представляется очень невыгодным. С дру-

гой стороны, генерация перепутанных N-парных состояний в нужный момент времени и распределение их между пользователями, нуждающимися в общении – это процесс, требующий больших затрат времени.

Байхэм, Хаттер и Мор [116] разработали аналогичную схему криптографической сети с коммутатором, которая использует обращенную ЭПР-схему для установки соединений.

3.11.2 Ускорение распределения перепутывания

Теперь мы объясним, как стандартный обмен перепутыванием помогает сохранить значительное время, когда нужно обеспечить двух удаленных пользователей парой атомов или электронов (или любыми частицами, имеющими массу), находящимися в состоянии Белла и испущенными неким центральным источником. Метод состоит в помещении между ними нескольких, приготовляющих белловские состояния и измеряющих такие состояния, подстанций. Рассмотрим Рис.3.26a. A и B – это два пользователя, разделенные расстоянием L. В точке O, расположенной точно между ними находится источник белловских пар. Время, необходимое для того, чтобы частицы достигли точек A и B, по крайней мере, равно $t_1 = L/2\upsilon$, где скорость частиц $\upsilon < c$ (скорость света). Рассмотрим теперь Рис.3.26b, на котором две станции C и D, приготавливающие белловские пары, установлены посередине между AO и BO, соответственно, и O теперь является просто белловской измерительной станцией. При $t = 0$, обе станции C и D посылают белловские пары (1,2) и (3, 4), соответственно. Частицы 2 и 3 прибывают в т. O, 1 попадает в т. A, а 4 –в т. B. Все они прибывают к пунктам назначения точно за время $t = L/4\upsilon$. В этот момент в т. O выполняется измерение состояния Белла над частицами 2 и 3. Это измерение немедленно приводит к редукции частиц 1 и 4, попадающих в A и B, соответственно, в состояние Белла. Если обозначить время измерения через t_m, то время, необходимое для того, чтобы снабдить белловской парой точки A и B (когда имеются дополнительные подстанции C и D), равно $t_2 = L/4\upsilon + t_m$. Очевидно, что t_2 меньше, чем t_1, если $t_m < L/4\upsilon$. Конечно, к этому времени нужно добавить время, необходимое для классической связи между станцией O и пользователями A и B (у которых и происходит проицирование частиц 1 и 4 в какое-то белловское состояние). Так, что для фотонов, находящихся в состояниях Белла, такая процедура, в действительности, не экономит времени. Но для массивных частиц, это определенно, единственный путь уменьшения времени, необходимого для обеспечения двух удаленных пользователей беловской парой. Таким же об-

разом, можно уменьшать это время, помещая все большее количество дополнительных подстанций, где приготавливаются и измеряются состояния Белла.

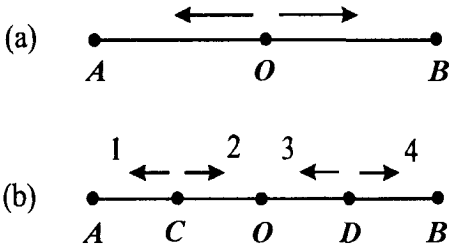


Рис. 3.26. Иллюстрация метода увеличения скорости распределения перепутанных пар частиц (с ненулевой массой) между двумя удаленными пользователями *A* и *B* (a). Добавлены дополнительные подстанции (b), осуществляющие генерацию белловских состояний. Эти подстанции *C* и *B* помещены между *A* и *B*. В т. *O* осуществляется дополнительное измерение состояний Белла.

3.11.3 Коррекция амплитудных ошибок, возникающих при распространении сигналов

Нам хотелось бы показать, как можно использовать обмен перепутыванием, с некоторой вероятностью, которую мы оценим, для коррекции амплитудных ошибок, которые могут накапливаться при распространении максимально перепутанных состояний. Предположим, что на Рис. 3.26b белловские пары, испущенные из *C* и *D*, приобретают амплитудные ошибки и становятся не максимально перепутанными:

$$|\Psi\rangle = \cos\theta|01\rangle + \sin\theta|10\rangle \ . \tag{3.55}$$

Тогда общее состояние двух перепутанных пар, когда частицы 2 и 3 попадают в т. *O*, имеет вид

$$|\Phi\rangle = \cos^2\theta|0101\rangle + \sin\theta\cos\theta\left(|1001\rangle + |0110\rangle\right) + \sin^2\theta|1010\rangle \ . \tag{3.56}$$

Если теперь выполнить измерение состояния Белла частиц 2 и 3, которые попали в т. *O*, то вероятность проицирования их в белловские состояния $|00\rangle+|11\rangle$ или $|00\rangle-|11\rangle$ оказывается $1/2\ \sin^2 2\theta$, тогда как вероятность найти их спроицированными в одно из двух оставшихся белловских состояний равна $1/2(1+\cos^2 2\theta)$. В первом случае (т.е. когда частицы 2 и 3 проицируются в $|00\rangle + |11\rangle$ или $|00\rangle - |11\rangle$) удаленные частицы 1 и 4 проицируются на белловские состояния $|00\rangle + |11\rangle$ или $|00\rangle-|11\rangle$. При этом, несмотря на амплитудные ошибки, вызванные распространением частиц, пользователи в *A* и *B* в итоге приобретают совместное состояние Белла. Конечно, в случае двух других исходов,

состояние частиц 2 и 3, частиц 1 и 4 переходит в состояния, имеющие меньшую степень перепутывания, чем (3.55). Именно поэтому мы и рассматриваем обмен перепутыванием в качестве метода, исправляющего амплитудные ошибки, лишь с вероятностной точки зрения. Вероятность успеха в этом случае в $1/2\ \sin^2 2\theta$ меньше, чем вероятность неудачного исхода $1/2(1+\cos^2 2\theta)$. Однако, из результатов измерения белловских состояний известно, в каких случаях коррекция оказалась успешной. Такой метод может рассматриваться как вид последовательного очищения, в отличие от стандартной методики очищения [47, 117] (см. разд.8.2), которое происходит параллельно. Можно показать, что существует такая степень перепутывания, которая сохраняется при этом типе процессов очищения [118] (см. также разд. 6.4, где определяется степень перепутывания).

3.11.4 Перепутанные состояния с большим числом частиц.

Используя нашу схему, можно генерировать перепутанные состояния с бóльшим количеством частиц из перепутанных состояний с меньшим числом частиц. Основные необходимые компоненты, это ГХЦ состояния (трех-частичные максимально перепутанные состояния) и устройство по измерению состояний Белла. Рассмотрим, каким образом можно приготовить (N+1)-частичное максимально перепутанное состояние из N-частичного максимального перепутанного состояния. Нужно взять одну частицу из N-частичного максимального перепутанного состояния, а другую – из ГХЦ состояния и выполнить измерение белловского состояния этих двух частиц. В результате, эти две частицы окажутся в состоянии Белла, а оставшиеся частиц N+1 – в максимально перепутанном состоянии. Такой способ приготовления дается схемой

$$|E(N)\rangle \otimes |E(3)\rangle \xrightarrow{\textit{измерение состояния Белла}} |E(N+1)\rangle \otimes |E(2)\rangle .$$

Пример приготовления 5-ти частичного максимально перепутанного состояния из 4-х частичного при помощи рассмотренной только что процедуры показан на рис.3.27.

Для рассмотрения вопроса о генерации ГХЦ-состояния, являющимся основным компонентом в рассмотренной схеме, можно использовать метод, предложенный Цайлингером и др. [119] (см. также разд.6.3.4, где рассмотрена генерация трех-фотонного перепутывания). Наоборот, можно приготовить ГХЦ-состояния используя наш метод, начиная с трех белловских пар и выполняя ГХЦ-измерение, выбирая по одной частице из каждой пары. Подробная схема для приготовления 3-частичных ГХЦ-состояний из трех перепутанных пар была предложна ранее Жуковским и др [101].

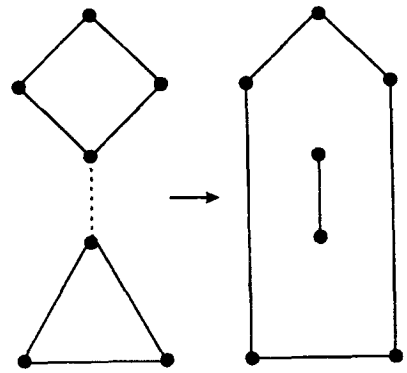


Рис. 3.27. Построение пятичастичного перепутанного состояния из четырехчастичного при использовании ГХЦ-состояния и измерения состояния Белла.

Концепция квантовых вычислений

Принципы квантовых вычислений можно объяснять многими способами и на различных уровнях. Этот факт нашел свое отражение в данной главе. Она состоит из трех самостоятельных частей. Первая представляет собой элементарное введение в предмет с акцентом на фундаментальные понятия; при этом избегается использование математического формализма. Для многих этот уровень объяснения будет соответствовать их целям. Те, кто хочет разобраться в деталях, могут переходить ко второй части. В ней читатель сначала познакомится с самыми первыми квантовыми алгоритмами. Затем обсуждается вычислительная сложность и более продвинутые темы, такие как квантовая факторизация. Наконец, в третьей части, последней по счету, но не последней по значимости, представлены проекты претворения сложных теоретических идей в реально работающие устройства. В главе 5 обсуждаются достигнутые на сегодняшний день экспериментальные результаты и продолжающиеся усилия по дальнейшему развитию квантовых вычислений.

4.1 Введение в квантовые вычисления.

Д. Дойч и А. Экерт

4.1.1 Новый способ использования природных ресурсов

Многие вехи в истории технологии были связаны с открытием новых путей освоения природы – то есть, с использованием различных физических ресурсов, таких, как материалы, силы, и источники энергии. В двадцатом веке, когда изобретение компьютеров позволило обрабатывать сложную информацию вне человеческого мозга, к этому списку добавилась *информация*. История компьютерной технологии, в свою очередь, состояла из последовательности переходов от одной физической реализации к другой – от шестеренок к реле, к электронным лампам, транзисторам, интегральным микросхемам и т.д. Сегодняшние литографические технологии позволяют вытравливать на поверх-

ностях кремниевых пластинок логические элементы и проводники менее чем микрон в сечении. Скоро использование этих технологий приведет к появлению еще меньших деталей, пока не наступит тот момент, когда логические элементы будут настолько маленькими, что каждый из них будет состоять всего из нескольких атомов.

В масштабе человеческого восприятия и в больших масштабах классические (не квантовые) законы физики являются хорошим феноменологическим приближением, но в атомных масштабах начинают доминировать законы квантовой механики. Чтобы компьютеры становились быстрее (а значит и меньше размером), новая *квантовая* технология должна заменить или дополнить существующую сейчас. Но оказывается, что такая технология может предложить гораздо больше, чем просто меньшие и более быстрые микропроцессоры. Она может обеспечить реализацию абсолютно новых вычислительных моделей, использующих новые квантовые алгоритмы, которые не имеют классических аналогов. Более того, квантовая теория вычислений играет даже более фундаментальную роль, чем ее классическая предшественница, поэтому тот, кто хочет получить фундаментальное понимание физики или процессов обработки информации, должен включить эти новые идеи в свое мировоззрение.

4.1.2 От битов к кубитам.

Что же так сильно отличает квантовые компьютеры от классических? Давайте внимательнее посмотрим на элементарную единицу информации: *бит*. Хотя понятия битов и кубитов уже объяснялись в Главе 1, мы решили для полноты и независимости изложения снова упомянуть их.

С физической точки зрения бит – это система с двумя состояниями: она может быть приготовлена в одном из двух различимых состояний, представляющих два логических значения – нет или да, неверно или верно, или просто 0 или 1. Например, в цифровых компьютерах напряжение между пластинками конденсатора может представлять бит информации: заряд на конденсаторе означает 1, а отсутствие заряда означает 0. Один бит информации может быть также закодирован, например, с использованием двух различных поляризаций света или двух различных электронных состояний атома. Кроме того, согласно квантовой механике, если бит может находиться в одном из двух различимых состояний, то он может также находиться и в их *когерентной суперпозиции*. Это новые состояния, которые в общем случае не имеют классических аналогов и в которых атом одновременно представляет *оба* значения 0 и 1. Чтобы привыкнуть к тому,

что физическая величина может одновременно принимать два значения, полезно рассмотреть эксперимент, показанный на Рис. 4.1.

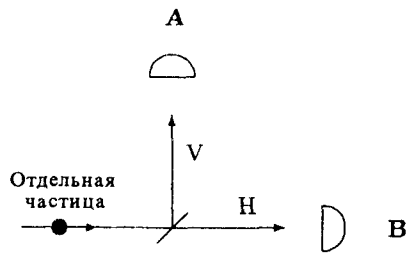


Рис. 4.1. Полупрозрачное зеркало отражает половину падающего на него света. Но отдельный фотон не расщепляется: когда мы посылаем фотон на такое зеркало, он с равной вероятностью регистрируется либо детектором A, либо детектором B. Это, тем не менее, не означает, что фотон покидает зеркало в горизонтальном (H) или вертикальном (V) направлении случайным образом. На самом деле, фотон одновременно летит по двум путям! Это может быть показано с помощью немного более сложного эксперимента, изображенного на Рис. 4.2.

Полупрозрачное зеркало отражает половину падающего на него света, при этом оставшаяся половина проходит сквозь него без изменений. Пусть один фотон налетает на такое зеркало, как показано на Рис. 4.1. Что при этом произойдет? Что мы точно знаем, это то что фотон не расщепляется на два: мы можем поместить фотодетекторы в любых точках установки, и запустив фотон, убедиться в том, что если один из фотодетекторов зарегистрирует попадание фотона, то ни один из остальных ничего не зарегистрирует. В частности, если поместить фотодетекторы за зеркалом в точках, через которые проходят два возможных выходящих пучка, то фотон будет зарегистрирован с равной вероятностью каждым из детекторов. Получается, что фотон пролетает зеркало в одном из двух направлений случайным образом? Нет, это не так! Может показаться очевидным, по крайней мере, то, что фотон в каждом конкретном эксперименте находится *или* в прошедшем пучке H, *или* в отраженном пучке V. Но это тоже не так. На самом деле, фотон одновременно движется по двум путям, как это может быть показано с помощью установки на Рис. 4.2. Два обычных зеркала расположены так, что оба пути пересекаются на втором полупрозрачном зеркале. С помощью этой установки можно наблюдать удивительный, чисто квантовый эффект *одночастичной интерференции*.

Предположим, что конкретный фотон двигался после прохождения зеркала вдоль пути, обозначенного H на Рис. 4.2. Тогда (из сравнения с Рис. 4.1) мы должны найти, что два детектора регистрируют фотоны с одинаковой вероятностью. В точности то же самое наблю-

далось бы, если бы фотоны двигались вдоль вертикального пути V. Следовательно, если бы фотон действительно двигался строго по одному пути внутри прибора – неважно какого – каждый из детекторов A и B в среднем срабатывал бы в половине проведенных экспериментов. Однако на самом деле происходит иначе. Оказывается, что в случае приведенной установки, фотон *всегда* попадает на детектор A и *никогда* на детектор B.

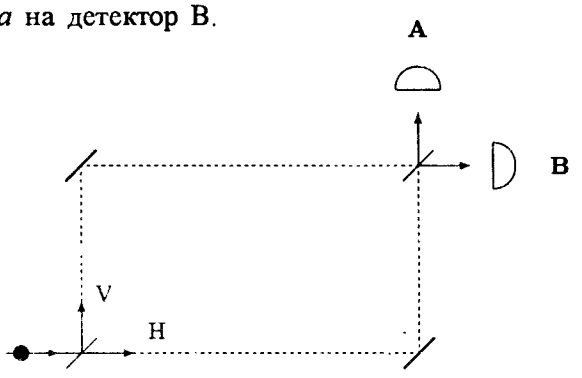


Рис. 4.2. Одночастичная интерференция. Влетающий в интерферометр фотон всегда достигает детектора A и никогда - детектора B. Любое объяснение, в котором предполагается, что фотон движется по определенной траектории внутри интерферометра – H или V – приводит к заключению, что детекторы A и B должны срабатывать в среднем в половине проведенных экспериментов. Но опыт показывает противоположное.

Неизбежным является вывод о том, что фотон должен был в некотором смысле двигаться вдоль обоих путей одновременно – поскольку, если один из путей перекрывается поглощающим экраном, то попадание фотона в детектор A и B немедленно становится равновероятным. Другими словами, блокирование любого из путей приводит к освещению B; когда же оба пути открыты, фотон каким-то способом получает информацию, которая не позволяет ему попасть в B, – информацию, которая распространяется вдоль другого пути со скоростью света, отражаясь от зеркал, в точности так же, как распространяется фотон. Это свойство квантовой интерференции – которое можно описать как существование невидимых двойников, оказывающих влияние на движение наблюдаемых частиц – относится не только к фотонам, но и ко всем частицам и физическим системам. Таким образом, квантовая теория описывает намного более богатую реальность, чем та вселенная, которую мы наблюдаем вокруг нас. Оказывается, что эта реальность имеет приближенно структуру сосуществующих и влияющих друг на друга только через явление интерференции различных вариантов этой вселенной – но все, что нам понадобится от философии существования параллельных

«вселенных» в этой статье – это факт, что то, что мы видим как отдельную частицу на самом деле является одним из аспектов невероятно сложной сущности, остальную часть которой мы не можем непосредственно наблюдать. Квантовые вычисления – это способ заставить невидимые аспекты частицы – ее двойники в других вселенных – работать на нас.

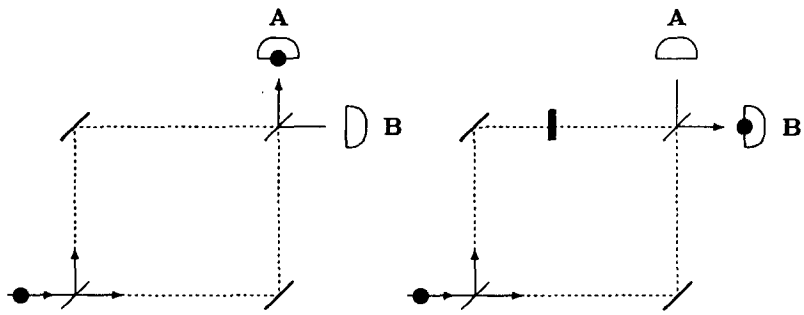


Рис. 4.3. Стеклянная пластинка, помещенная на пересечении с одним из путей в интерферометре, может перенаправить фотоны от одного детектора к другому. Все фотоны, входящие в левый интерферометр, попадают на детектор A. В правом интерферометре интерференция изменяется за счет присутствия стеклянной пластики на вертикальном пути. В результате фотоны оказываются на детекторе B. Следовательно, то, что произошло только на одном из путей, достоверно изменило конечный результат эксперимента. Этот эффект особенно полезен в квантовых вычислениях.

Один из особенно полезных для квантовых вычислений эффектов может быть продемонстрирован, если мы задержим фотон на одном из путей H или V. Этого можно добиться, поставив на пути стеклянную пластинку, как показано на Рис. 4.3. Так как интерференция между фотоном и его невидимым двойником зависит от точных времен их прибытия, мы можем выбирать толщину пластинки и, соответственно, время задержки так, чтобы фотон достоверно (то есть во всех «вселенных») оказывался на детекторе B вместо детектора A. Таким образом, то, что произошло только на одном из путей (и, как следствие, только в одной из «вселенных») оказало влияние на оба пути. Мы вернемся к этому вопросу позже.

Точно так же, как фотон может находиться в когерентной суперпозиции распространения вдоль пути H и вдоль пути V, так и любой квантовый бит, или *кубит*, может быть приготовлен в суперпозиции двух логических состояний 0 и 1. Именно в этом смысле кубит может хранить 0 и 1 одновременно, в произвольной пропорции. Но следует заметить, что, так же, как и фотон при измерении будет обнаружен только на одном из двух путей, при измерении кубита будет зарегистрировано случайным образом только одно из

двух хранящихся в нем чисел. Само по себе это свойство не очень полезно.

Но давайте разовьем идею суперпозиции чисел немного дальше. Рассмотрим регистр, построенный из трех физических битов. Классический 3-битный регистр может хранить в точности одно из восьми различных чисел, т.е. регистр может быть в одном из восьми возможных состояний 000, 001, 010, ..., 111, представляющих числа от 0 до 7. Но квантовый регистр, составленный из трех кубитов, может одновременно хранить до восьми чисел в квантовой суперпозиции. Замечательно, что восемь различных чисел могут физически присутствовать в одном регистре; но это не более удивительно, чем присутствие чисел 0 и 1 в одном кубите. При добавлении кубитов к регистру его емкость по отношению к хранению квантовой информации растет экспоненциально: четыре кубита могут хранить 16 различных чисел одновременно, и, в общем случае, L кубитов могут хранить до 2^L чисел одновременно. Регистр из 250 кубитов – по существу состоящий из 250 атомов – сможет хранить одновременно больше чисел, чем количество атомов в видимой вселенной. (В любом случае, это *заниженная* оценка количества квантовой информации, которую они могут хранить, так как в общем случае элементы суперпозиции присутствуют в непрерывно изменяемой пропорции, при этом каждый со своим фазовым углом.) Несмотря на это, если мы измерим содержимое регистра, то увидим только одно из этих чисел. Однако, мы можем начать производить нетривиальные квантовые вычисления, так как, если регистр приготовлен в суперпозиции большого числа различных чисел, мы можем выполнять математические операции одновременно над ними всеми.

Например, если кубиты – это атомы, то соответствующим образом подобранные лазерные импульсы влияют на их электронные состояния, и начальная суперпозиция закодированных чисел развивается в другую суперпозицию. В процессе такой эволюции каждое число в суперпозиции подвергается воздействию, так что мы производим большой объем параллельных вычислений. Следовательно, квантовый компьютер может за один шаг вычислений произвести одну операцию над, скажем, 2^L различными входными числами, и результат будет суперпозицией всех соответствующих чисел на выходе. Для того чтобы выполнить такую же задачу, любой классический компьютер должен повторить вычисления 2^L раз, или использовать 2^L различных параллельно работающих процессоров. Таким образом, квантовый компьютер предоставляет огромный выигрыш в использовании вычислительных ресурсов, таких как время и память – хотя бы только для определенных типов вычислений.

4.1.3 Квантовые алгоритмы

Какого типа? Как мы уже говорили, это не обычное хранение информации, поскольку, хотя компьютер теперь содержит все результаты 2^L вычислений, законы физики позволяют нам увидеть только один из них. Тем не менее, так же как один ответ «А» в эксперименте на Рис. 4.2. зависит от информации, распространявшейся вдоль каждого из двух путей, квантовая интерференция позволяет нам теперь получить один окончательный ответ, который логически зависит от всех 2^L промежуточных результатов.

Именно таким образом недавно открытый Ловом Гровером из AT&T Белл лаборатории в Нью-Джерси [120] замечательный алгоритм достигает поразительного результата, производя поиск в неупорядоченном списке из N элементов за время всего лишь порядка $\sqrt{N}$ шагов. Рассмотрим, например, поиск определенного телефонного номера в адресной книге, содержащей миллион записей, хранящихся в памяти компьютера в алфавитном порядке. Легко доказать (и это очевидно), что ни один классический алгоритм не может улучшить метод прямого перебора записей одна за одной, пока данный номер не будет найден, что в среднем потребует 500000 обращений в память. Квантовый компьютер может проверить все эти записи одновременно, путем одного обращения в память. Однако, если просто запрограммировать его выдать результат в этом месте, то никакого улучшения по сравнению с классическим алгоритмом не получится: только в одном из миллиона вычислительных путей (т.е. в одной из миллиона вселенных) была проверена запись, которую мы ищем, так что вероятность того, что мы получим эту информацию при измерении состояния компьютера есть всего лишь одна миллионная. Но если мы оставим эту квантовую информацию в компьютере не измеренной, последующая квантовая операция может привести к тому, что эта информация повлияет на другие пути – так же как в описанном выше простом интерференционном эксперименте. Таким образом информация об интересующей нас записи распространяется с помощью квантовой интерференции на другие «вселенные». Оказывается, что если повторить эту порождающую интерференцию процедуру около 1000 раз (в общем случае, $\sqrt{N}$ раз), то информация о том, какая запись содержит данный номер, будет доступна для измерения с вероятностью 0.5, – то есть она распространится на более чем половину «вселенных». Поэтому повторение всего алгоритма еще несколько раз позволит найти искомую запись с вероятностью, чрезвычайно близкой к 1.

В дополнение к нахождению записи с заданным свойством, вариации алгоритма поиска Гровера могут также находить наименьшее или

наибольшее число в списке, модальное значение и т.д., так что это очень гибкий инструмент. Тем не менее, на практике поиск в физической базе данных вряд ли будет основным применением алгоритма Гровера – по крайней мере до тех пор, пока классическая память будет оставаться дешевле квантовой памяти. Поскольку операция переноса базы данных из классической в квантовую память (биты в кубиты) сама потребует $O(N)$ шагов, алгоритм Гровера в лучшем случае ускорит время поиска на постоянный множитель, чего можно достигнуть с помощью использования классических параллельных процессоров. По-настоящему алгоритм Гровера найдет применение только в *алгоритмических* поисках, – то есть, поисках в списках, которые не хранятся в памяти, а сами на ходу генерируются компьютерной программой. Например, играющий в шахматы квантовый компьютер может использовать его для исследования триллионов возможных продолжений из текущей позиции за примерно то же число шагов, которое потребуется классическому компьютеру (использующему слепой поиск «в лоб») для исследования всего миллиона продолжений. Несмотря на большие возможности по «отсечению ветвей дерева» в классических шахматных алгоритмах, это должно привести к очень существенному улучшению.

Как недавно показал Жиль Брассар из университета Монреаля [121], другим важным применением алгоритма Гровера будет использование его в криптоанализе для атаки классических криптографических схем, таких как DES (the Data Encryption Standard, см. главу 2 по квантовой криптографии). Взлом DES по существу требует поиска среди $2^{56}=7\text{x}10^{16}$ возможных ключей. Если их перебирать со скоростью, скажем, в один миллион ключей в секунду, то классическому компьютеру потребуется около тысячи лет для отыскания правильного ключа, в то время как квантовый компьютер использующий алгоритм Гровера сделает это менее чем за 4 минуты!

По странному совпадению, несколько основных свойств квантовых компьютеров имеют приложения в криптографии. Одно из них - это алгоритм Гровера. Другое – это квантовый алгоритм для эффективной факторизации больших целых чисел, открытый в 1991 году Питером Шором, также из AT&T Белл лаборатории в Нью Джерси [36]. Здесь различие в производительности между квантовым и классическими алгоритмами еще более впечатляющее. Математики верят (твердо, хотя они на самом деле это не доказали), что для факторизации числа с N десятичными знаками любому классическому компьютеру требуется число шагов, которое растет экспоненциально с N. Иначе говоря, добавление одного десятичного знака к числу в общем случае *умножает* время, необходимое для его факторизации, на постоянный множитель (см. раздел 4.2). Таким образом, при уве-

личении числа знаков задача быстро становится нереальной. Наибольшее число, которое было разложено на простые множители в качестве математического соревнования, т.е. число, чьи простые множители были втайне выбраны математиками, чтобы составить задачу для других математиков, состояло из 129 знаков. Никто не может даже представить себе, как можно факторизовать с помощью классического алгоритма число, скажем, из тысячи знаков; вычисление займет время во много раз большее, чем возраст вселенной. Напротив, квантовые компьютеры могут факторизовать число с тысячью знаками за долю секунды – и время расчета будет расти только как куб числа знаков.

Кроме того, невыполнимость факторизации лежит в основе стойкости наиболее надежных на сегодняшний день методов шифрования, в частности системы RSA (Rivest, Shamir и Adleman), которая часто используется для защиты электронных банковских счетов [122] (детали см. в главе 2). Когда будет построена машина для квантовой факторизации (квантовый компьютер специального назначения для факторизации больших чисел), все такие криптографические системы станут ненадежными.

Потенциальная мощь использования квантовых явлений для выполнения вычислений была впервые предсказана в общих чертах Ричардом Фейнманом на Первой Конференции по Физике Вычислений, проведенной в MIT в 1981 году. Он заметил, что в общем случае оказывается невозможным эффективно смоделировать развитие квантовой системы на классическом компьютере [123]. Компьютерное моделирование квантовой эволюции обычно связано с экспоненциальным замедлением по сравнению с естественной эволюцией, по существу за счет того, что количество классической информации, необходимой для описания эволюции квантовой системы экспоненциально больше, чем количество информации, нужной для описания с той же точностью соответствующей классической системы. (Для предсказания эффектов интерференции нужно описать всё экспоненциально большое множество двойников системы в параллельных вселенных.) Тем не менее, Фейнман рассматривал это не как препятствие, а как потенциальную возможность. Он указал, что, если для выяснения того, что произойдет в эксперименте с многочастичной интерференцией, требуется так много вычислений, то сама постановка такого эксперимента и измерение результата эквивалентны проведению сложного вычисления.

Квантовые вычисления уже были использованы для предсказания поведения квантовых систем в простых случаях. В какой-то момент в обозримом будущем они будут играть новую и незаменимую роль в структуре науки, поскольку возможность науки делать предсказания будет основываться на квантовых вычислениях.

Основы квантовой теории вычислений (которая теперь должна рассматриваться как *общая* теория вычислений – классическая теория Тьюринга это только приближение) были заложены в 1985 году, когда Дэвид Дойч из Оксфордского университета опубликовал определяющую теоретическую статью, в которой он описал *универсальный квантовый компьютер* [124]. С тех пор началась охота за интересными вещами, которые могут делать квантовые компьютеры, и одновременно поиск научных и технологических решений, которые позволят нам построить квантовые компьютеры.

4.1.4 Построение квантовых компьютеров

В принципе, мы знаем, как построить квантовый компьютер; мы начинаем с простых квантовых логических элементов (см. главу 1) и затем соединяем их в квантовые сети.

Как и классический, квантовый логический элемент – это очень простое вычислительное устройство, которое за определенное время осуществляет одну элементарную квантовую операцию, обычно над двумя кубитами [125]. Конечно, квантовые логические элементы отличаются от их классических аналогов тем, что они могут создавать квантовые суперпозиции и производить операции над ними. Тем не менее, с увеличением числа квантовых элементов в сети мы быстро наталкиваемся на серьезные практические проблемы. Чем с большим количеством взаимодействующих кубитов мы имеем дело, тем труднее оказывается разработать взаимодействие, при котором проявляется квантовая интерференция. Помимо технических сложностей работы на масштабах одного атома и одного фотона, одной из наиболее серьезных проблем является предотвращение влияния взаимодействия, обеспечивающего квантовую интерференцию, на окружающую среду. Чем больше используется компонентов, тем с большей вероятностью квантовая информация распространится за пределы квантового компьютера и будет потеряна во внешней среде, таким образом, искажая вычисления. Этот процесс называется *декогерентностью* и детально обсуждается в главе 7. Следовательно, наша задача – разработать суб-микроскопические системы, в которых кубиты оказывают влияние друг на друга, но не на окружающую среду.

Некоторые физики с пессимизмом относятся к перспективам существенного прогресса в квантовой компьютерной технологии. Они считают, что декогерентность на практике никогда не будет уменьшена до такого уровня, что можно будет произвести более чем несколько последовательных шагов квантового вычисления. (Между прочим, уже это позволило бы создать несколько очень полезных устройств, см. ниже

таблицу 4.1). Другие исследователи с большим оптимизмом считают, что реальные квантовые компьютеры появятся через годы, а не через десятилетия. Мы склоняемся к оптимистической точке зрения - отчасти потому, что теория говорит нам, что не существует *фундаментальных* препятствий на этом пути и что возможны квантовая коррекция ошибок и отказоустойчивые вычисления (см. главу 7), отчасти, из-за удивительного таланта и способности решать проблемы работающих над этим проектом физиков-экспериментаторов, и, наконец, потому, что благодаря оптимизму, задуманное свершается.

Таблица 4.1. Вехи развития квантовой компьютерной технологии

Тип оборудования	Число требуемых кубитов	Число шагов до наступления декогерентности	Статус
Квантовая криптография	1	1	Реализовано
Квантовая криптография, основанная на перепутывании	2	1	Продемонстрирован
Квантовый логический элемент С–НЕ	2	1	Продемонстрирован
Комплекс логических элементов	2	2	Продемонстрирован
Алгоритм Дойча	2	3	Продемонстрирован
Удвоение емкости канала	2	2	Близко к реализации
Телепортация	3	2	Продемоистрирована
Обмен перепутыванием	4	1	Продемонстрирован
Станция повторения для квантовой криптографии	несколько	несколько	Теория еще неполна
Квантовое моделирование	несколько	несколько	Простые эксперименты
Алгоритм Гровера с игрушечными даниыми	3+	6+	Продемонстрированы с ЯМР
Сверхточные стандарты частоты	несколько	несколько	Обозримое будущее
Очищение перепутывания	несколько	несколько	Обозримое будущее
Алгоритм Шора с игрушечными даниыми	16+	тысячи+	
Квантовая машина для факторизации	сотни	сотни	
Универсальный кваитовый компьютер	тысячи+	тысячи+	

Тем не менее, одним рывком проблемы не будут решены. Текущая задача состоит не в том, чтобы построить полностью завершенный универсальный квантовый компьютер, а в том, чтобы перейти от экспериментов, в которых мы можем наблюдать квантовые явления к экспериментам, где мы можем их нужным образом контролировать. Простые квантовые логические элементы, состоящие из двух кубитов, уже реализованы в лабораториях в Европе и в США. Следующее десятилетие должно принести контроль над несколькими кубитами, и без сомнения, наш новый способ использования природы должен будет начать приносить плоды. Например, известно, что простые квантовые сети могут предоставить более стабильные стандарты частот [126] (см. раздел 7.6). Некоторые возможные вехи в развитии квантовой компьютерной технологии представлены в таблице 4.1.

4.1.5 Более глубокие приложения

Когда физика вычислений впервые систематически исследовалась в 1970-х, основным опасением было то, что квантово-механические эффекты могут привести к фундаментальным ограничениям на точность, с которой физические объекты могут реализовывать свойства битов, логических ячеек, композиций операций и т.д., которые появляются в абстрактной и математически сложной теории вычислений. Поэтому были опасения, что мощь и элегантность теории, ее основополагающие концепции – такие как вычислительная универсальность – ее важные результаты – такие, как теорема остановки Тьюринга и более современная теория вычислительной сложности – могут оказаться всего лишь плодами чистой математики, не имеющими в действительности отношения к чему-либо в природе.

Исследования, которые мы обсуждали, не только доказали, что эти опасения беспочвенны, но и в каждом случае блестяще обосновали лежащие в основе соображения, – так полно, как двадцать лет назад никто не мог и мечтать. Как уже объяснялось, квантовая механика не устанавливает ограничений на то, какие классические вычисления могут быть осуществлены в природе, а разрешает их все, и к тому же предоставляет новые режимы вычислений, в том числе алгоритмы, выполняющие задачи, которые не могут быть выполнены никаким классическим компьютером (такие как абсолютно надежная криптография с открытым ключом). Что касается стройности теории, то исследователи в этой области привыкли к тому факту, что реальная теория вычислений более самосогласованна и гораздо более естественна, чем можно было когда-либо ожидать от ее классического приближения, согласуется с фундаментальными теориями в других

областях. Даже на самом простом уровне, слово «квантовый» обозначает то же, что и слово «бит» – элементарная порция – и это отражает тот факт, что полностью классические системы, подверженные общей нестабильности, известной как «хаос», абсолютно не поддерживают цифровые вычисления (так что даже машины Тьюринга, теоретические прототипы всех классических компьютеров, втайне всегда были квантово-механическими!). Гипотеза Черча-Тьюринга в классической теории (о том, что все «естественные» модели вычислений по существу эквивалентны) никогда не была доказана. Ее аналог в квантовой теории вычислений (принцип Тьюринга, гласящий что универсальный квантовый компьютер может смоделировать поведение любой конечной физической системы) был напрямую доказан в статье Дойча в 1985 году [124]. В квантовом случае был доказан еще более сильный результат (также высказанный в качестве гипотезы, но никогда не доказанный в классическом случае), а именно что такое моделирование всегда может быть осуществлено за время, которое является, самое большое, полиномиальной функцией времени, требующегося для физической эволюции.

К числу многих ответвлений теории квантовых вычислений в очевидно далеких областях относится их связь с философией и практикой математических доказательств. Проведение вычисления, которое приводит к определенному результату, эквивалентно *доказательству* того, что наблюдаемый результат является одним из возможных результатов вычисления. Поскольку мы можем описывать операции компьютера математически, то такое доказательство всегда может быть переведено в доказательство некоторой математической теоремы. Это было верно и в классическом случае, но в отсутствие интерференционных эффектов всегда можно проследить шаги вычисления, и таким образом произвести доказательство, которое удовлетворяет классическому определению: последовательность предложений, каждое из которых есть либо аксиома, либо следует из предыдущих предложений в последовательности в соответствии со стандартными правилами логических умозаключений. Теперь мы должны оставить это определение. В дальнейшем доказательство должно рассматриваться как процесс – само вычисление, а не его запись – поскольку мы должны принять, что в будущем квантовые компьютеры будут доказывать теоремы методами, которые ни человеческий мозг, ни какой-либо другой арбитр не будет в состоянии проверить шаг за шагом, поскольку если бы «последовательность предложений», соответствующая такому доказательству была бы распечатана, то бумага много раз заполнила бы наблюдаемую вселенную. Более детальное обсуждение глубоких свойств квантовых вычислений может быть найдено в [127].

4.1.6 Заключительные замечания

Экспериментальные и теоретические исследования квантовых вычислений в настоящее время привлекают все возрастающее внимание, как со стороны академических исследователей, так и со стороны индустрии по всему миру. Идея о том, что природу можно контролировать и манипулировать ей на квантовом уровне является мощным стимулом для воображения физиков и инженеров. Почти ежедневно происходит прогресс в разработке все более обещающих технологий, реализующих квантовые вычисления, и новых квантовых алгоритмов, имеющих различные преимущества по сравнению со своими классическими аналогами. Здесь есть потенциал для действительно революционных инноваций.

Эта статья является переработанной версией вводной статьи по квантовым вычислениям, которая появилась в мартовском выпуске за 1998 год в журнале Physics World [128].

4.2 Квантовые алгоритмы

Р. Джозса

4.2.1 Введение

Квантовый алгоритм – это любой физический процесс, использующий характерные квантовые эффекты для выполнения полезных вычислительных задач. Удобно формализовать описание этих квантовых вычислительных процессов в терминах модели, выстраивающей параллель с формализмом классических вычислений. По сути, в квантовом случае элементы памяти в компьютере – это кубиты, а не биты, а логические операции – это унитарные преобразования, а не булевы операции классического вычисления. Можно утверждать [124], что модели такого рода достаточно, чтобы описать любой квантовый процесс. От любого компьютера требуется, чтобы он оперировал «конечными средствами», то есть, чтобы он имел возможность использовать только некоторый конечный набор базовых унитарных операций. Любая другая операция, которая может нам понадобиться в алгоритме, должна быть построена (или аппроксимирована с достаточной точностью) из этих базовых строительных блоков соединением их действия на выбранные кубиты. Можно показать [129, 130], что достаточно использовать различные маленькие наборы унитарных операций (так называемые «универсальные наборы») чтобы аппроксимировать любую унитарную операцию над любым числом кубитов с произвольной точностью.

Одно из наиболее полезных и важных следствий из этого форма-

лизма состоит в том, что он дает способ оценить сложность вычислительной задачи (опять-таки, выстраивая параллель понятиям классической теории сложности). Нас будет особенно интересовать временная сложность, то есть, оценка числа элементарных операций, необходимых для решения вычислительной задачи, как функция объема входных данных.

Если два компьютера A и B обладают разными (универсальными) наборами базовых операций, то временная сложность для произвольной вычислительной задачи будет, в общем случае, различной. Однако, можно сперва запрограммировать в B выполнение каждой из базовых операций A с помощью его собственного набора, а затем запустить любую программу, написанную на языке набора операций A. Пусть k обозначает максимальное число операций, необходимых B, чтобы воспроизвести любую из базовых операций A. Тогда временная сложность на B будет, самое большее, в k раз больше сложности на A, то есть смена набора базовых операций приводит, самое большее, к равномерному замедлению (независимо от размера входа) для любой вычислительной задачи. В теории сложности вычислений нас, в целом, интересует не точное число шагов в вычислении, а только характерный темп роста числа шагов при увеличении объема входных данных. В целом, мы интересуемся только тем, ограничено ли число шагов полиномиальной функцией от объема входных данных (приводя к так называемым полиномиальным по времени, или эффективным, алгоритмам) или же оно растет экспоненциально (или сверх-полиномиально) с их объемом. Согласно сделанным выше замечаниям, это различие не зависит от выбора компьютера, оно является внутренним свойством самой вычислительной задачи.

Наш основной интерес при изучении квантовых алгоритмов вызывает возможность найти полиномиальные по времени алгоритмы для таких задач, для которых не известно классических полиномиальных по времени алгоритмов. То есть, мы хотим продемонстрировать, что квантовые эффекты могут привести к экспоненциальному ускорению, по сравнению с классической обработкой информации. Мы опишем различные ситуации, в которых это происходит – алгоритмы Дойча, Саймона и Шора. Мы также опишем квантовый алгоритм поиска Гровера, который дает, по сравнению с любым классическим алгоритмом, ускорение в квадратный корень из числа шагов, а не экспоненциальное ускорение. Тем не менее, он представляет большой практический интерес. Алгоритм Гровера представляет также и большой теоретический интерес благодаря своей связи с классическим классом сложности, называемым NP [131,132].

Мы увидим в главе 5, что возможное применение любого доста-

точно большого квантового алгоритма в настоящее время представляет собой чрезвычайно сложную экспериментальную задачу. Тем не менее, существование интересных квантовых алгоритмов, хотя бы на уровне теоретических построений, очень важно само по себе, поскольку оно указывает на новые существенные отличия в коренной структуре между классической и квантовой физикой. С точки зрения переработки информации, временная эволюция в квантовой физике, похоже, сложнее, чем классическая эволюция во времени, причем это отличие можно описать в рамках теории сложности вычислений.

Можно увидеть, что корни ключевых квантово-механических эффектов, приводящих к экспоненциальному ускорению в перечисленных выше квантовых алгоритмах, лежат в различных свойствах квантового *перепутывания*. Мы начнем с обсуждения двух основных ускоряющих эффектов; мы будем их называть «квантовое параллельное вычисление» (раздел 4.2.2) и «принцип локальных операций» (раздел 4.2.3).

4.2.2 Квантовое параллельное вычисление

Рассмотрим функцию f: $A \to B$, где A и B - конечные множества. Обычно A и B – это наборы из всех 2^n строк из n битов (для некоторого n) – как, например, в алгоритмах Дойча и Саймона, – или $\mathbb{Z}_N$, множество целых чисел по модулю N (для некоторого N), – как в алгоритме Шора. В наших приложениях A и B будут также Абелевыми группами. Пусть $\mathcal{H}_A$ (соответственно, $\mathcal{H}_B$) будет гильбертовым пространством с ортонормальным базисом, состоящим из элементов A (соответственно, B). В контексте квантового вычисления, вычисление f соответствует унитарной эволюции U_f, которую обычно определяют как операцию на $\mathcal{H}_A \otimes \mathcal{H}_B$, переводящей $|a\rangle|b\rangle$ в $|a\rangle|b \oplus f(a)\rangle$ (см. Рис. 4.4). Здесь $\oplus$ обозначает абелеву групповую операцию на B.

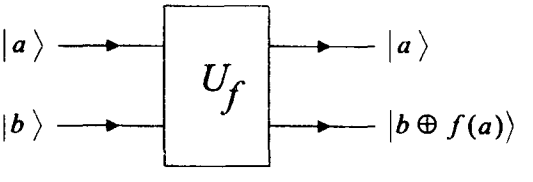


Рис. 4.4. Картина квантового логического элемента для унитарного преобразования U_f, соответствующего вычислению функции f. Верхняя и нижняя линии представляют, соответственно, верхний и нижний регистры.

$\mathcal{H}_A$ – это пространство состояний входного регистра, а $\mathcal{H}_B$ – пространство состояний выходного регистра. Состояние на входе $|a\rangle$ не меняется, чтобы U_f была гарантированно унитарной операцией для

любой возможной f. Если изначально b было равно 0, то $f(a)$ можно считать непосредственно с выходного регистра с помощью стандартного измерения в данном базисе.

Предположим теперь, что входной регистр установлен в виде суперпозиции значений, скажем, в виде равной суперпозиции $\Sigma_{a\in A}|a\rangle$ (где мы опустили нормировочный множитель). Тогда, применив U_f с b=0, мы получаем на выходе, благодаря линейности квантовой эволюции, суперпозицию $\Sigma|a\rangle|f(a)\rangle$ (см. Рис. 4.5).

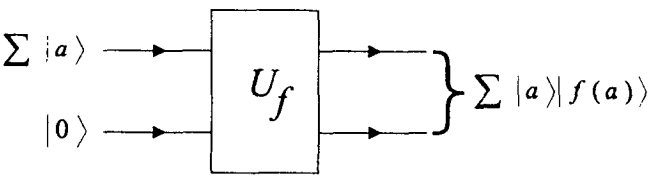


Рис. 4.5. Квантовое параллельное вычисление

Запустив U_f всего *один* раз, мы вычислили *все* значения f в суперпозиции. Это и есть процесс квантового параллельного вычисления, введенный Дойчем в [124]. Заметим, что состояние на выходе $\Sigma|a\rangle|f(a)\rangle$ – это, в общем случае, перепутанное состояние входного и выходного регистров. Разумеется, феномен суперпозиции – это свойство также и *классических* линейных систем, и любой эффект, зависящий только от суперпозиции, может быть легко применен и в классической системе. Однако, у феномена квантового перепутывания нет классического аналога, и его фундаментальная роль в квантовом вычислении была подчеркнута и исследована в [133, 134].

Пусть B={0,1} обозначает аддитивную группу целых по модулю 2, и $\mathcal{B}$ обозначает гильбертово пространство одного кубита, то есть, двумерное гильбертово пространство с заданным стандартным базисом обозначаемым $\{|0\rangle, |1\rangle\}$. $\mathcal{B}^n$ будет обозначать 2^n-мерное гильбертово пространство $\mathcal{B}\otimes\ldots\otimes\mathcal{B}$ n кубитов с базисом $\{|x\rangle:\in B^n\}$, задаваемым всеми n-битными строками. Пусть H обозначает фундаментальную одно-кубитную унитарную операцию

$$H=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}. \tag{4.1}$$

Тогда

$$H|0\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle) \text{ и } H|1\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle). \tag{4.2}$$

Рассмотрим функцию $f: B^n\to B$. В качестве примера вычисления с помощью квантового параллелизма, мы можем задать суперпози-

цию всех входных значений, а затем вычислить все значения f для этой суперпозиции следующим образом:

(i) Начнем со стандартного состояния n (входных) кубитов $|0\rangle...|0\rangle$, и применим H по отдельности к каждому кубиту. В результате получим во входном регистре состояние

$$\frac{1}{2^{n/2}}\left(|0\rangle+|1\rangle\right)...\left(|0\rangle+|1\rangle\right)=\frac{1}{2^{n/2}}\sum_{x\in B^n}|x\rangle \tag{4.3}$$

(ii) Добавим единственный (выходной) кубит в состоянии $|0\rangle$ и применим U_f. Получим состояние:

$$|f\rangle=\frac{1}{2^{n/2}}\sum_{x\in B^n}|x\rangle|f(x)\rangle \tag{4.4}$$

Заметим, что для (i) требуется только $O(n)$ операций, – то есть, полиномиальное число по n, – но этот шаг приводит к суперпозиции экспоненциально большого числа значений f в (4.4).

Квантовое перепутывание играет также и еще одну роль в представлении суперпозиций. Если бы мы хотели построить общую суперпозицию 2^n мод классически, нам бы понадобилось по *одной* системе для каждой моды, например, 2^n колебательных мод колеблющейся струны. Эти моды будут соответствовать все более и более высоким уровням некоторого физического ресурса, например, энергии колеблющейся струны, и, представление общей суперпозиции 2^n мод потребовало бы экспоненциального (по n) объема ресурса. В противоположность этому, в квантовой теории мы можем представить суперпозицию 2^n мод с помощью n двухуровневых систем – *благодаря эффекту перепутывания*. Для представления такой общей суперпозиции необходим всего лишь *линейный* объем физических ресурсов, поскольку необходимо возбудить независимо не более чем n систем. Следовательно, хотя суперпозиция и встречается в классических системах, феномен квантового перепутывания приводит к экспоненциальной экономии физических ресурсов, необходимых для работы с большими суперпозициями.

4.2.3 Принцип локальных операций

В любом вычислении, будь то классическое или квантовое, обрабатываемая информация воплощается в идентичности физического состояния компьютера (его части). Сравним описание идентичности состояния n классических битов с его квантовой аналогией, состоянием n кубитов. Хотя n битов могут находиться в любом из экспоненциально большого числа состояний, можно полностью описать каждое состояние, задав всего лишь n битов информации. Напротив, в

общее (перепутанное) состояние n кубитов может входить экспоненциально большое число частей суперпозиции. В этом смысле, квантовая система может содержать экспоненциально больше информации, чем классическая. Эта черта – не следствие того факта, что квантовые амплитуды могут принимать непрерывный набор значений, - она сохраняется, даже если мы ограничим амплитуды некоторым простым дискретным множеством значений. Например, состояние $(n+1)$ кубитов $|f\rangle$ в (4.4) содержит информацию обо всем экспоненциально большом наборе значений вида ноль/один для функции f. Заметим, что информация, необходимая для описания неперепутанного состояния (т.е. произведения независимых состояний) n кубитов, растет линейно с ростом n, и она в n раз больше информации, необходимой для описания одного единственного состояния.

Формализм квантовой механики позволяет эффективно обрабатывать обширную информацию, содержащуюся в квантовом состоянии, со скоростью, которую нельзя достичь никакими классическими средствами. Это замечательное свойство квантовой теории было впервые отмечено Фейнманом в работе [123]. Предположим, что у нас есть физическая система из n кубитов в некотором перепутанном состоянии $|\psi\rangle$, и мы действуем одно-кубитной операцией U на первый кубит. Это считалось бы в квантовом вычислении одним шагом (или, точнее, постоянным числом шагов, независимым от n – если U надо составлять из других базовых операций, заложенных в компьютере). Рассмотрим теперь классическое вычисление, соответствующее этому преобразованию информации в квантовом состоянии. Можно описать $|\psi\rangle$ покомпонентно (относительно базиса n битов) амплитудами, где каждый индекс равен 0 или 1, и U представляется унитарной матрицей 2×2 U_i^j. Применение U соответствует умножению на матрицу

$$a_{i_1\ldots i_n}^{(new)} = \sum_j U_{i_1}^j a_{j i_2\ldots i_n} \quad . \tag{4.5}$$

Таким образом, необходимо выполнить умножение на матрицу 2×2 2^{n-1} раз, по одному разу для каждой возможной строки $i_2\ldots i_n$, что потребует вычислительных ресурсов, которые будут *экспоненциально* расти с ростом n. На квантовом же компьютере, благодаря перепутыванию, эти 2^{n-1} повторений не нужны. В этом состоит наш «принцип локальных операций»: единственная локальная операция, действующая на подсистему большой перепутанной системы, перерабатывает информацию в таком объеме, который потребовал бы, в общем случае, экспоненциально больших ресурсов в классическом вычислении.

В вышеуказанном смысле, n кубитов обладают экспоненциально большей емкостью, чем n битов. Однако, у потенциально огромной информации, заключенной в квантовом состоянии, есть еще одно при-

мечательное свойство: бóльшая ее часть никоим образом *не доступна* для чтения! Теория квантового измерения накладывает строгие ограничения на количество информации, которое можно получить о неизвестном квантовом состоянии. Эту изначальную недоступность информации можно описать количественно [135, 136] в терминах теории информации Шеннона [137]. В случае общего состояния n кубитов, несущего объем информации порядка $O(2^n)$, оказывается, что из одной копии такого состояния с помощью каких бы то ни было физических средств может быть получено не более, чем n классических битов информации. Это совпадает с максимальной информационной емкостью n битов.

Полное (в основном, недоступное) информационное содержание данного неизвестного квантового состояния называется квантовой информацией. Естественную квантовую физическую эволюцию можно считать обработкой квантовой информации. Таким образом, взгляд на мир с точки зрения сложности вычислений открывает новое необычное различие между классической и квантовой физикой: чтобы осуществлять естественную квантовую эволюцию, Природа должна обрабатывать огромное количество информации со скоростью, которую нельзя достичь никакими классическими средствами, и, в то же время, бóльшая часть этой обрабатываемой информации держится скрытой от нас! Надо, однако, отметить, что внутренне ей присущая недоступность квантовой информации *не* отменяет возможности использовать эти огромные возможности по обработке информации для полезных вычислительных целей. Ибо, можно получать небольшие объемы информации о полном виде конечного состояния, для получения которого все равно потребовались бы экспоненциально большие классические ресурсы. Можно это проиллюстрировать примером из описанной выше техники параллельного вычисления: полная квантовая информация состояния $|f\rangle$ в (4.4) включает в себя информацию обо всех отдельных значениях функции $f(x)$, но ее нельзя выяснить никаким измерением. Однако, *можно* определить некоторые глобальные черты собрания всех значений функции с помощью соответствующих измерений над состоянием $|f\rangle$, недиагональных в стандартном базисе $\{|x\rangle|y\rangle\}$. Например, если f – периодическая функция, то мы можем определить значение периода, которое, конечно, есть далеко не полная характеристика всей функции, но для оценки которого с помощью классических средств все равно потребовалось бы экспоненциально большое количество раз вычислить значение функции. Этот факт будет ключевым в работе алгоритма Шора (раздел 4.2.6).

Обсудив некоторые основные вычислительные достоинства кван-

товой теории в общем виде, мы теперь опишем работу различных основных квантовых алгоритмов.

4.2.4 Оракулы и алгоритм Дойча

Алгоритм Дойча [124, 138] был первым явным примером вычислительной задачи, которую с помощью квантовых эффектов можно решить экспоненциально быстрее, чем с помощью любых классических средств. Затем он был улучшен в работе [139], и мы здесь опишем его самую новую форму.

Рассмотрим все четыре возможных однобитных функций $f: B \to B$. Среди них есть две постоянных функции:

$$\begin{matrix} f(0)=0 \\ f(1)=0 \end{matrix} \quad \text{или} \quad \begin{matrix} f(0)=1 \\ f(1)=1 \end{matrix} \tag{4.6}$$

и две «сбалансированных» функции (сбалансированных в том смысле, что выходные значения 0 и 1 появляются с одинаковой частотой):

$$\begin{matrix} f(0)=0 \\ f(1)=1 \end{matrix} \quad \text{или} \quad \begin{matrix} f(0)=1 \\ f(1)=0 \end{matrix} . \tag{4.7}$$

Предположим теперь, что у нас есть «черный ящик» или «оракул», который вычисляет одну (неизвестно, которую) из этих функций. Оракул можно изобразить как запечатанный ящик (см. Рис. 4.4), который выдает значение функции для любого значения, заданного на входе (или суперпозиции, заданной на входе, как на Рис. 4.5). Или же мы можем представить себе оракула в виде компьютерной подпрограммы, которую мы можем запускать, но чей текст или внутренний принцип работы мы узнать не можем. (Позже мы обсудим важность этого ограничения нашего доступа к оценке f). Наша задача – узнать, что вычисляет оракул, – сбалансированную функцию или константу.

В рамках классической механики нам, разумеется, необходимо запустить оракул дважды, чтобы наверняка решить задачу. Ведь если нам известно только одно значение функции (например, $f(0)$ или $f(1)$, то у нас совсем нет информации о том, сбалансирована ли функция или же она равна константе! Теперь мы покажем, что на квантовом компьютере проблему можно решить точно, обратившись к оракулу всего один раз.

Мы используем возможность квантового параллельного вычисления (как описано выше) с одним дополнительным трюком – в самом начале установим выходной регистр на $1/\sqrt{2}(|0\rangle - |1\rangle)$. Квантовое вычисление идет следующим образом. Начав со стандартного состояния $|0\rangle\,|0\rangle$ во входном и выходном регистре, мы применяем операцию НЕ к выходному регистру, и затем H к обоим, что дает

$$|0\rangle|0\rangle \to |0\rangle|1\rangle \to \left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

$$= \frac{1}{\sqrt{2}}\sum_{x\in B}|x\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right). \qquad (4.8)$$

Затем мы даем это состояние оракулу, то есть, применяем U_f. Вспоминая, что U_f преобразует $|x\rangle|y\rangle$ в $|x\rangle|y \oplus f(x)\rangle$, мы видим, что

$$U_f : |x\rangle(|0\rangle-|1\rangle) \longrightarrow \begin{cases} |x\rangle(|0\rangle-|1\rangle) \text{ если } f(x)=0 \\ -|x\rangle(|0\rangle-|1\rangle) \text{ если } f(x)=1. \end{cases}$$

Таким образом

$$U_f : \frac{1}{\sqrt{2}}\sum_{x\in B}|x\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \to \left(\frac{1}{\sqrt{2}}\sum_{x\in B}(-1)^{f(x)}|x\rangle\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right). \qquad (4.9)$$

В течение всего процесса выходной регистр оставался в состоянии $1/\sqrt{2}(|0\rangle-|1\rangle)$. Входной регистр оставлен в состоянии $1/\sqrt{2}\Sigma_{x\in B}(-1)^{f(x)}|x\rangle$. Если f – постоянная функция, то мы получаем $\pm 1/\sqrt{2}(|0\rangle+|1\rangle)$, а если f сбалансирована, то получаем $\pm 1/\sqrt{2}(|0\rangle-|1\rangle)$. Легко проверить, что операция H обратна самой себе, то есть, что $HH = I$. В заключение процедуры, применим H ко входному регистру, и получим (с учетом (4.2)) состояние $\pm|0\rangle$, если f – постоянная функция, и $\pm|1\rangle$ если f сбалансирована. Эти значения легко различить с помощью измерения в стандартном базисе, таким образом наверняка различив сбалансированную и постоянную функции после всего лишь одного обращения к оракулу. Полная последовательность операций приведена на сетевой диаграмме на Рис. 4.6.

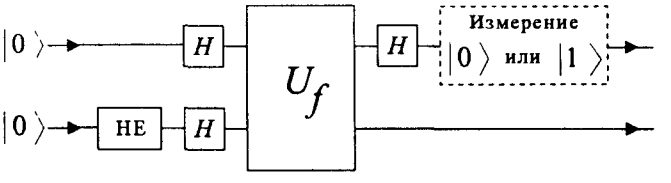


Рис. 4.6. Алгоритм Дойча для 1-битных функций. Измеренное значение 0 (соответственно, 1) означает, что функция f – постоянная (соответственно, сбалансированная).

Само по себе различие между одним и двумя обращениями к оракулу не имеет значения при рассмотрении формальной сложности. Однако идею описанного выше процесса можно легко обобщить на случай, когда действительно проявляется *экспоненциальное* различие между классическим и квантовым процессами.

Вместо рассмотрения функций, отображающих один бит на один бит, предположим, что у нас есть оракул, который вычисляет некоторую функцию от n битов на один бит:

$$f : B^n \to B$$

(и мы также знаем значение n). Пусть известно, что эта функция есть либо константа (т.е. все ее 2^n значений одновременно равны либо 0, либо 1), либо она сбалансирована, где под сбалансированностью понимается то, что ровно половина (т.е. 2^{n-1}) ее значений равна 0, а другая половина равна 1. Заметим, что для n > 1, в общем случае функция из n битов в 1 бит не является ни сбалансированной, ни постоянной, но, тем не менее, существует огромное количество сбалансированных функций. Наша задача снова состоит в том, чтобы определить (с полной определенностью), является ли f константой или сбалансированной функцией. Случай $n = 1$ – это, в точности, задача, рассмотренная выше.

В классическом сценарии, если мы обратимся к оракулу 2^{n-1} раз, чтобы получить 2^{n-1} значений f, то, каким бы образом последующие запросы ни зависели от ответа на предыдущие, мы все равно не сможем решить задачу в *каждом* случае. Действительно, предположим, что все 2^{n-1} ответов оказались равны между собой (что всегда возможно, хоть и маловероятно, в случае сбалансированной функции). Независимо от выбора аргументов на входе, всегда найдутся постоянная и сбалансированная функции, полностью согласующиеся с собранной информацией. Следовательно, любое классическое решение задачи должно содержать более, чем 2^{n-1} обращений к оракулу - то есть, по меньшей мере, экспоненциальное (по n) их число. На самом деле, легко видеть, что $2^{n-1}+1$ обращений будет всегда достаточно. В квантовом случае, проблему можно решить с определенностью с помощью всего лишь *одного* обращения к оракулу. Метод решения – это прямое обобщение случая одного бита.

Начнем с ряда из n (входных) кубитов и одного (выходного) кубита. Пусть вначале все кубиты в находятся стандартном состоянии $|0\rangle$. Применим H к каждому из входных кубитов. Согласно (4.3), это приведет к равной суперпозиции всех возможных значений на входе в первых n кубитах. Точно также как и в предыдущем случае, приготовим последний (выходиой) кубит в состоянии $1/\sqrt{2}(|0\rangle-|1\rangle)$. Затем предложим получившееся состояние $n+1$ кубитов оракулу. Это формально совпадает с (4.9) с той разницей, что теперь x пробегает все значения из B^n, а не из B. После работы оракула первые n кубитов будут в состоянии

$$|\xi_f\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in 2^n} (-1)^{f(x)} |x\rangle \quad . \tag{4.10}$$

(Попутно заметим, что в оригинальной версии алгоритма Дойча [138] 1992 года было необходимо обратиться к оракулу два раза, чтобы произвести состояние $|\xi_f\rangle$). Далее, если f была постоянной функцией, то $|\xi_f\rangle$ окажется в такой же равной суперпозиции всех возможных $|x\rangle$ с общим знаком плюс или минус. В то же время, если f была сбалансирована, то $|\xi_f\rangle$ окажется суперпозицией, в которую половина членов будет входить со знаком плюс, а другая – со знаком минус. Эти две суперпозиции взаимно ортогональны, и существует соответствующее измерение над $|\xi_f\rangle$, которое с определенностью отличит сбалансированную функцию от постоянной.

Мы должны описать в явном виде, как можно выполнить это измерение. Мы не можем предполагать, что можно выполнить произвольное измерение в произвольном квантовом алгоритме за один вычислительный шаг (точно так же, как нельзя предполагать, что за один шаг можно выполнить произвольную унитарную операцию). Чтобы оценить сложность произвольного вычисления, предположим, что мы можем только детектировать состояния $|0\rangle$ или $|1\rangle$ любого кубита в вычислительном базисе, и это считается одним вычислительным шагом. Любое общее измерение можно свести к последовательности таких стандартных измерений, если сначала унитарно перевести собственный базис измерения в вычислительный базис, а затем последовательно считать биты. Сложность измерения тогда определяется как число шагов, необходимых, чтобы выполнить унитарное преобразование, плюс число кубитов, которые надо считать.

В нашем случае измерение, которое отличает сбалансированные $|\xi_f\rangle$ от постоянных, можно осуществить следующим образом. Вспомним, что операция H обратна самой себе ($HH = I$), и что H, примененная к каждому кубиту состояния $|0\rangle|0\rangle...|0\rangle$ даёт равную суперпозицию всех $|x\rangle$ (см. 4.3). Следовательно, если H применить к этой суперпозиции еще раз, то получится состояние $|0\rangle|0\rangle...|0\rangle$. Поэтому мы применяем H к каждому кубиту состояния $|\xi_f\rangle$ (на это требуется n шагов). Если функция f была постоянной, то получится состояние $\pm|0\rangle|0\rangle...|0\rangle$. Если же f была сбалансирована, то получится какое-то ортогональное состояние, то есть, суперпозиция $|x\rangle$, включающая в себя какое-то $x \neq 00...0$. Таким образом, мы считываем каждый из n кубитов и смотрим, все ли они равны 0, или нет (еще n шагов), и на этом измерение завершается. В целом, квантовому алгоритму Дойча требуется $O(n)$ шагов (включая одно обращение к оракулу) для того, чтобы наверняка отличить сбалансированную функцию от постоянной, тогда как любому классическому алгоритму для достижения той же цели требуется $O(2^n)$ шагов.

Алгоритм Дойча является так называемым «результатом ора-

кула» или «относительным» результатом (по отношению к оракулу). Он не дает абсолютного экспоненциального разделения между классическим и квантовым вычислением, но дает такое разделение, только если сделать некоторые дальнейшие (правдоподобные, но недоказанные) вычислительные предположения относительно того факта, что у нас нет доступа к внутреннему устройству оракула. Вследствие этого предположения, если нам дана программа, вычисляющая f, то не существует механического способа использовать общий синтаксис такой программы, чтобы узнать, сбалансированна f или постоянна, быстрее, чем запустив эту программу достаточное число раз. Конечно, для вычисления постоянной функции требуется только очень короткая программа, которую легко распознать. Но можно столкнуться и с очень сложной и запутанной программой, которая также будет вычислять постоянную функцию – так, что этот факт будет очень трудно увидеть из ее синтаксиса. Хотя наше предположение весьма правдоподобно, оно остается недоказанным, поскольку очень трудно анализировать такие алгоритмы, которые в качестве входных данных рассматривают синтаксис программы! Заметим, что, если бы можно было доказать *абсолютное* экспоненциальное разделение между классическим и квантовым вычислениями, то это бы разрешило некоторые старые фундаментальные вопросы в классической теории вычислительной сложности (например, это бы означало, что $P \neq PSPACE$; см. определение этих терминов в [131]). Похоже, что очень трудно формально доказать экспоненциальное превосходство квантового вычисления над классическим.

Еще одна важная черта алгоритма Дойча состоит в следующем. Если не требуется, чтобы алгоритм работал совершенно, то есть, если мы допускаем некоторую (произвольно малую) ошибку, то показанное здесь экспоненциальное разделение между классическим и квантовым вычислениями исчезает. Дело в том, что для любого $\varepsilon > 0$ существует классический (вероятностный) алгоритм, который за фиксированное (не зависящее от n!) число шагов для любой заданной f отличит сбалансированную функцию от постоянно с вероятностью $(1 - \varepsilon)$. Этот алгоритм работает следующим образом. Мы оцениваем f для некоторых K *случайно* выбранных входных значений. Если все ответы одинаковы, то считаем, что f – «константа». В противном случае считаем, что она сбалансирована. Небольшое размышление показывает, что ответ «сбалансирована» будет верен всегда, а ответ «константа» будет верен с вероятностью ошибки, не превышающей $1/2^K$. Таким образом, для любого заданного $\varepsilon > 0$ выбираем K настолько большим, чтобы было $(1/2^K) < \varepsilon$. Заметим, что K не зависит от n, так что K запросов оракула приводят к постоянному числу шагов в алгоритме.

Экспоненциальное разделение между классическим и квантовым вычислением происходит только в предельном случае $\varepsilon = 0$. Можно возразить, что предельная ситуация не имеет физического смысла, так как любой компьютер, будучи физическим прибором, не может быть абсолютно изолирован от своего окружения. Следовательно, всегда есть (небольшая) вероятность того, что он сработает неправильно – например, в какой-то момент какой-нибудь бит может поменять значение под воздействием космического луча. Поэтому было бы очень интересно найти такую задачу, вычислительная сложность которой в квантовом и в классическом случае различалась бы экспоненциально, даже если допустима небольшая ошибка. Первый такой пример был дан Бернстайном и Вацирани [140]. С помощью рекурсивной конструкции они описали вычислительную задачу, которая могла бы быть решена на квантовом компьютере за полиномиальное время, но которой потребовалось бы $O(n^{\log n})$ шагов на классическом компьютере. Затем Саймон [141] описал более простую задачу, которую на квантовом компьютере можно было бы решить за время $O(n^2)$, но которой на классическом компьютере требовалось полное экспоненциальное время (т.е. $O(2^n)$). Апофеозом этой линии развития стал алгоритм Шора [36] для факторизации, который устранил также и зависимость от оракула. Алгоритм Шора дает метод факторизации целого числа N за число шагов, полиномиальное (с менее, чем кубической зависимостью) от числа цифр ($\log N$) в N, и дает правильный результат с вероятностью $(1 - \varepsilon)$ для любого заданного $\varepsilon > 0$. Несмотря на многочисленные попытки, которые делались в течение нескольких сотен лет (такими выдающимися математиками, как Гаусс, Лежандр, Ферма, и другими), мы не знаем классического полиномиального по времени вероятностного алгоритма для решения этой задачи. В отличие от алгоритмов Дойча и Саймона, алгоритм Шора не связан с оракулом. Однако это не доказывает абсолютного экспоненциального превосходства квантового вычисления над классическим, поскольку нет доказательства того, что не существует классического полиномиального по времени алгоритма для факторизации (а есть только огромное число неудавшихся попыток сконструировать такой алгоритм!)

4.2.5. Преобразование Фурье и периоды

Квантовый алгоритм факторизации Шора и алгоритм Саймона будут существенным образом зависеть от замечательной способности квантового компьютера определять период заданной периодической функции. Мы проиллюстрируем используемые при этом идеи в следующем базовом примере. Предположим, что у нас есть черный ящик,

который вычисляет заведомо периодическую функцию $f : Z_N \to Z$ периода r:

$$f(x+r) = f(x) \quad \text{для всех } x. \tag{4.11}$$

Вспомним, что Z_N обозначает группу целых чисел по модулю N, и сложение здесь делается по модулю N. Мы также предполагаем, что f не принимает дважды за период одного и того же значения. Заметим, что (4.11) может выполняться, только если N делится на r без остатка.

Наша цель – определить r. В классическом подходе (при отсутствии дальнейшей информации о f), мы можем только подставлять в черный ящик различные значения x в надежде получить два одинаковых ответа, и, через них – информацию о периоде функции. В общем случае, чтобы с высокой вероятностью получить два одинаковых значения, потребуется $O(N)$ случайных попыток. С помощью квантовых эффектов мы сможем найти r всего лишь за $O((\log N)^2)$ шагов, что представляет собой экспоненциальное ускорение по сравнению с классическим алгоритмом.

Для начала, используем квантовое параллельное вычисление, чтобы получить все значения f в равной суперпозиции. В результате получим состояние

$$|f\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle |f(x)\rangle \ . \tag{4.12}$$

Хотя это состояние содержит в себе все свойства периодичности функции f, пока неясно, как извлечь из него информацию об r! Если мы измерим состояние второго регистра и обнаружим, например, число y_0, то состояние в первом регистре сократится до равной суперпозиции всех таких $|x\rangle$, так что $f(x) = y_0$. Если x_0 – одно из таких x, и $N=Kr$, то мы получим в первом регистре периодическое состояние

$$|\psi\rangle = \frac{1}{\sqrt{K}} \sum_{k=0}^{K-1} |x_0 + kr\rangle \ . \tag{4.13}$$

Здесь важно отметить, что число $0 \le x_0 \le r-1$ было сгенерировано случайным образом, поскольку все значения y_0 функции f могли выпасть с равной вероятностью. Поэтому, если теперь измерить значение этого регистра, результатом будет случайно выпавшее число между 0 и N--1, и он не даст нам абсолютно никакой информации об r!

Разрешение этой трудности состоит в использовании преобразования Фурье, которое, как известно, даже в классическом случае способно выловить из набора данных периодические формы, не взирая на то, как эти формы сдвинуты. Дискретное преобразование Фурье $\mathcal{F}$ для целых чисел по модулю N – это унитарная матрица $N \times N$, элементы которой равны

$$\mathcal{F}_{ab} = \frac{1}{\sqrt{N}} e^{2\pi i \frac{ab}{N}} \tag{4.14}$$

Если мы применим это унитарное преобразование к состоянию $|\psi\rangle$, описанному выше, то получим [144]

$$\mathcal{F}|\psi\rangle = \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} e^{2\pi i \frac{x_0 j}{r}} \left| j \frac{N}{r} \right\rangle . \tag{4.15}$$

Важный момент, который здесь надо отметить – это то, что в метках кет-векторов больше не появляется случайный сдвиг x_0 (см. Рис. 4.7).

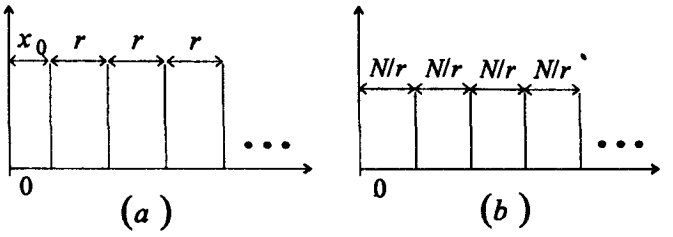


Рис. 4.7. Графическое представление периодических амплитуд (а) состояния $|\psi\rangle$, и его преобразования Фурье. После применения $\mathcal{F}$ к $|\psi\rangle$ период r превратился в N/r, а случайный сдвиг x_0 исчез.

Если мы теперь измерим квантовое состояние $|\psi\rangle$, то получим вектор под номером c, который обязательно будет кратен N/r, то есть, $c = \lambda N/r$. Тогда можно записать

$$\frac{c}{N} = \frac{\lambda}{r}, \tag{4.16}$$

где c и N – известные нам числа, а значения $0 \le \lambda \le r-1$ с равной вероятностью могли быть случайно выбраны в эксперименте (поскольку все амплитуды в состоянии $\mathcal{F}|\psi\rangle$ одинаковы по величине). Теперь, если случайно выбранное число λ оказалось взаимно простым с r, (то есть, у них нет общих множителей) то мы можем найти r, сократив дробь c/N до несократимой. Какова вероятность, что случайно выбранное λ *окажется* взаимно простым с r? Согласно теореме о простом числе (см. [142, 143] и Приложение А в [144]), количество простых чисел, не превышающих r, растет как $r/\log r$ при больших r. Таким образом, вероятность того, что наше случайно выбранное число λ окажется взаимно простым с r, равна, по меньшей мере, $1/\log r$, что больше, чем $1/\log N$. Следовательно, если мы повторим описанную выше процедуру $O(\log N)$ раз, то сможем определить r с любой наперед заданной точностью $(1-\varepsilon)$, насколько угодно близкой единице.

Как было отмечено выше, мы хотим, чтобы нашему квантовому алгоритму для определения r требовалось для работы poly $(\log N)$

шагов – то есть, число шагов, полиномиальное по $\log N$, а не по самому N. Тогда он будет экспоненциально быстрее, чем любой известный классический алгоритм для определения периодичности. Выше мы показали, что для определения r достаточно $O(\log N)$ повторений, но в наших доводах все еще остается большой пробел: преобразование Фурье $\mathcal{F}$, которое мы использовали, – это большая унитарная операция, размера $N \times N$, и мы не можем *изначально* предполагать, что ее можно осуществить всего лишь за poly $(\log N)$ базовых вычислительных шагов. Можно показать, что любую унитарную операцию размера $d \times d$ можно осуществить на квантовом компьютере за $O(d^2)$ шагов [124, 144]. Это также и число шагов, необходимое классическому компьютеру для умножения матрицы размера $d \times d$ на d-мерный вектор. В нашем случае вычисления $\mathcal{F}$, эта граница $O(N^2)$ неудовлетворительна. К счастью, у преобразования Фурье есть некоторые специфические дополнительные свойства, которые позволяют осуществить его за $O((\log N)^2)$ шагов. Эти свойства вытекают из классической теории быстрого преобразования Фурье (БПФ) [145], которая показывает, как уменьшить число в $O(N^2)$ шагов, нужных для матричного умножения, до $O(N \log N)$ шагов. Если применить те же самые идеи в квантовом случае, то можно увидеть [134,144], как принцип локальных операций позволяет свести число шагов к $O((\log N)^2)$, что нам и было необходимо. Отметив этот важный момент, мы опустим многочисленные технические детали конструкции БПФ и его применения в квантовом случае. Эти детали разработаны в работе [134], к которой мы отсылаем заинтересованного читателя. Отметим также, что, согласно (4.14),

$$\mathcal{F}|0\rangle = \frac{1}{\sqrt{n}} \sum_{x=0}^{N-1} |x\rangle \quad , \tag{4.17}$$

так что, имея эффективную реализацию $\mathcal{F}$, мы сможем эффективно создать большое равномерное распределение, чтобы получить $|f\rangle$ в (4.12).

Итак, квантовый алгоритм для определения периода функции f, с N кубитами на входе, начинается с применения квантового параллельного вычисления, чтобы вычислить все значения f в равной суперпозиции за $O(\log N)$ шагов. Затем применяется преобразование Фурье, чтобы в получившемся в результате состоянии проявилась периодическая структура. Принцип локальных операций, примененный к квантовой версии алгоритма БПФ, гарантирует, что можно проделать преобразование Фурье за poly$(\log N)$ шагов. Аналогичному классическому вычислению потребовалось бы $O(N)$ раз вызвать функцию f для вычисления таблицы ее значений, а затем еще $O(N \log N)$ шагов для

выполнения БПФ. Таким образом, квантовый алгоритм создает экспоненциальное ускорение.

Интересно отметить, что понятие периодичности и построение преобразования Фурье можно обобщить на случай *произвольной* конечной группы G. Наше предыдущее обсуждение относится к одному частному случаю аддитивной группы целых чисел по модулю N. Обобщенная точка зрения помогает лучше понять работу преобразования Фурье. Далее мы кратко опишем некоторые важные используемые при этом идеи, ограничив наше внимание случаем абелевых групп. (Оставшуюся часть этого раздела можно, при желании, пропустить. Связь с изложением последующих разделов при этом не будет потеряна.)

Пусть G – произвольная абелева группа. Пусть f: G $\to X$ – функция на группе (принимающая значения из некоторого множества X), и рассмотрим

$$K = \{k \in G : f(k+g) = f(g) \text{ для всех } g \in G\} . \tag{4.18}$$

(Отметим, что мы записали групповую операцию с помощью аддитивного обозначения). K – это подгруппа G, называемая стабилизатором, или группой симметрии f. Она характеризует симметрию f по отношению к групповой операции G. В нашем предыдущем примере группа G являлась Z_N, а K была циклической подгруппой всех чисел, кратных r. Пусть существует аппарат, вычисляющий f. Наша цель – найти K. Точнее, мы хотим вычислить K за время $O(\text{poly}(\log |G|))$, где $|G|$ – размер группы, и вычисление f на входе считается одним вычислительным шагом. (Заметим, что мы могли бы найти K за время $O(\text{poly}(|G|)$, просто вычислив и проверив все значения f). Начнем, как и в предыдущем примере, с создания состояния

$$|f\rangle = \frac{1}{\sqrt{G}} \sum_{g \in G} |g\rangle |f(g)\rangle , \tag{4.19}$$

и затем считаем второй регистр. Предположив, что f невырождена – в том смысле, что $f(g_1) = f(g_2)$ iff $g_1 - g_2 \in K$, получим в первом регистре

$$|\psi(g_0)\rangle = \frac{1}{\sqrt{|K|}} \sum_{k \in K} |g_0 + k\rangle , \tag{4.20}$$

что соответствует значению $f(g_0)$ во втором регистре при случайном выборе g_0. В (4.20) записана равная суперпозиция состояний из случайно выбранного подмножества K из G. При этом, G – это объединение непересекающихся подмножеств, так что, если мы считаем метку состояния в (4.20), то увидим случайный элемент случайно выбранного подмножества. То есть, с равной вероятностью будет выбра-

на произвольная случайная метка из G, которая не сообщит нам никакой информации о K.

Общая конструкция «преобразования Фурье G» даст нам способ устранить g_0 из меток состояний, точно так же, как и в вышеописанном примере. Получившееся в результате состояние даст непосредственную информацию о K. Пусть $\mathcal{H}$ обозначает гильбертово пространство с базисом $\{|g\rangle : g \in G\}$, помеченным элементами G. Каждый элемент группы $g_1 \in G$ создает унитарный оператор «сдвига» $U(g_1)$ на $\mathcal{H}$, определяемый как

$$U(g_1)|g\rangle = |g + g_1\rangle \quad \text{для всех } g. \tag{4.21}$$

Заметим, что состояние в (4.20) можно представить как сдвинутое на g_0:

$$\sum_{k \in K} |g_0 + k\rangle = U(g_0)\left(\sum_{k \in K} |k\rangle\right). \tag{4.22}$$

Наша основная идея состоит в том, чтобы ввести в $\mathcal{H}$ новый базис $\{|\chi_g\rangle : g \in G\}$ специальных состояний, *инвариантных относительно сдвига* в том смысле, что

$$U(g_1)|\chi_{g_2}\rangle = e^{i\phi(g_1, g_2)}|\chi_{g_2}\rangle \quad \text{для любых } g_1, g_2, \tag{4.23}$$

то есть, состояния $|\chi_g\rangle$ – это общие собственные состояния всех операторов сдвига $U(g)$. Заметим, что все $U(g)$ коммутируют между собой, так что такой базис общих собственных состояний гарантированно существует. Если мы теперь, согласно (4.22), запишем $|\psi(g_0)\rangle$ в новом базисе, то тогда суперпозиции $\Sigma_{k \in K}|k\rangle$ и $\Sigma_{k \in K}|g_0 + k\rangle$ будут содержать состояния с метками одного и того же типа, определенными только подгруппой K. Считывание метки в этом базисе даст теперь напрямую информацию о составляющих элементах K.

Преобразование Фурье $\mathcal{F}$ на G определяется просто как унитарное преобразование, которое приводит базис, инвариантный относительно сдвигов, обратно к стандартному базису:

$$\mathcal{F}|\chi_g\rangle = |g\rangle \quad \text{для всех } g. \tag{4.24}$$

Следовательно, чтобы считать $|\psi(g_0)\rangle$ в новом базисе, мы просто применяем $\mathcal{F}$ и производим считывание в стандартном базисе.

Чтобы в явном виде задать $\mathcal{F}$, достаточно выписать состояния $|\chi_g\rangle$ через компоненты стандартного базиса. Существует стандартный способ вычисления этих компонент, основанный на построениях из теории представлений групп. Мы здесь опустим детали; заинтересованный читатель найдет их в работах [134] и [146]. Для группы Z_N получаем

$$|\chi_k\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i \frac{jk}{N}} |j\rangle \ , \tag{4.25}$$

что приводит к формуле для преобразования Фурье, данной в (4.25).

Изложенная здесь теоретико-групповая схема служит для обобщения и расширения степени применимости квантового алгоритма для определения периодичности. Например, квантовый алгоритм Саймона [134, 141, 146, 147] оказывается просто нахождением периодичности на группе $(Z_2)^n$ – группе всех n-битных строк с покомпонентным сложением по модулю 2. Саймон рассматривал следующую проблему: предположим, что у нас есть черный ящик, вычисляющий функцию f, переводящую n-битные строки в n-битные строки. Также известно, что эта функция – вида «два к одному» в том смысле, что существует такая фиксированная n-битная строка, ξ что

$$f(x+\xi) = f(x) \quad \text{для всех } n\text{-битных строк } x. \tag{4.26}$$

Наша задача – определить ξ.

Чтобы увидеть, что это просто обобщение задачи о нахождении периодичности, заметим, что в группе $(Z_2)^n$ n-битных строк каждый элемент удовлетворяет соотношению $x+x=0$. Следовательно, утверждение (4.26) просто означает, что функция f периодична на группе, с подгруппой периодичности $K = \{ 0, \xi \}$. Таким образом, чтобы найти ξ, мы конструируем преобразование Фурье на группе n-битных строк и затем применяем стандартный алгоритм, описанный выше. Соответствующее гильбертово пространство $\mathcal{H}$ с базисом, помеченным n-битными строками – это просто последовательность из n кубитов. Используя общие конструкции из теории представлений групп [134], можно увидеть, что преобразование Фурье – это применение H (из (4.1)) к каждому из n кубитов. Квантовый алгоритм определяет ξ за $O(n^2)$ шагов, тогда как можно утверждать [141] что любому классическому алгоритму потребовалось бы для этого вычислить f как минимум $O(2^n)$ раз. Полное описание этого алгоритма можно найти в работах [141, 146, 147].

Формализм преобразования Фурье оказался самой важной составляющей частью открытых на сегодняшний день квантовых алгоритмов. Некоторое его дальнейшее развитие, включая обобщение на случай неабелевых групп, можно найти в работах [148, 149].

4.2.6 Квантовый алгоритм Шора для факторизации.

Самый знаменитый на сегодняшний день квантовый алгоритм - это алгоритм Шора для задачи факторизации (то есть, разложения на про-

стые множители) [36, 144, 146]. В ней надо для заданного числа N найти число k (не равное 1 и N), на которое N делится без остатка. В этом разделе мы кратко опишем, как можно свести эту задачу к задаче нахождения периода некоторой периодической функции f. Тогда квантовый алгоритм, описанный в предыдущем разделе, решит задачу факторизации числа N за poly(log N) шагов, то есть, за время, полиномиальное по числу цифр в числе N.

Для начала, отметим, что пока не найден такой классический алгоритм, который бы факторизовал N за время, полиномиальное по числу цифр в N. Например, самый наивный возможный алгоритм основан на пробном делении N по очереди на все числа между 1 и $\sqrt{N}$ (так как любое составное N должно разлагаться на множители из этого диапазона). На это требуется, по крайней мере, $\sqrt{N}$ шагов (по крайней мере, один шаг на каждое деление), а $\sqrt{N} = 2^{1/2\log N}$ экспоненциально велико по log N. При всех достижениях современной математики, самому быстрому известному нам алгоритму требуется время порядка $\exp((\log N)^{1/3} (\log \log N)^{2/3})$.

Чтобы свести задачу факторизации к задаче нахождения периода, нам понадобятся некоторые основные результаты из теории чисел. Более углубленно они описаны в приложении работы [144], а полное их объяснение можно найти в самых стандартных текстах по теории чисел [142, 143]. Мы начнем с того, что выберем случайным образом число $a < N$. С помощью алгоритма Евклида вычислим, за время poly(log N), наибольший общий делитель a и N. Если он оказался больше единицы, то, значит, мы нашли делитель N, и алгоритм завершен! Однако, с подавляющей вероятностью, выбранное наугад число a окажется взаимно простым с N. Из теоремы о простом числе (о ней упоминалось в предыдущем разделе) следует, что эта вероятность превышает $1/\log N$ при больших N. Если a взаимно просто с N, то, согласно теореме Эйлера из теории чисел, существует такая степень a, которая делится на N с остатком 1. Пусть r обозначает наименьшую такую степень:

$$a^r \equiv 1 \mod N \quad \text{и } r \text{ – наименьшая такая степень.} \tag{4.27}$$

(Если a не взаимно просто с N, то такой степени не существует). Число r называется *порядком* a по модулю N. Далее мы покажем, что информация об r может дать нам делитель N.

Предположим, что мы знаем, как определить r (см. ниже) и, кроме того, предположим, что число r оказалось *четным*. Тогда можно переписать (4.27) в виде $a^r - 1 \equiv 0 \mod N$, и разложить левую часть этого выражения как разность квадратов:

$$(a^{r/2} - 1)(a^{r/2} + 1) \equiv 0 \mod N \ . \tag{4.28}$$

Пусть $\alpha = a^{r/2} - 1$ и $\beta = a^{r/2} + 1$. Тогда произведение $\alpha\beta$ делится на N. Если ни α, ни β по отдельности не делятся на N, то у каждого из них есть с N общие множители. В этом случае, вычислив наибольший общий делитель N с α и β (снова с помощью алгоритма Евклида) мы найдем нетривиальный делитель числа N.

В качестве примера, возьмем $N = 15$, и выберем взаимно простое с ним число $a = 7$. Вычисляя степени 7 по модулю 15, найдем, что, $7^4 \equiv 1 \bmod 15$, то есть, что порядок 7 по модулю 15 равен 4. Значит, число 15 должно без остатка делить произведение $(7^{4/2} - 1)(7^{4/2} + 1) = (48)(50)$. Вычисляя наибольшие общие делители 15 и 50 и 48, находим, что они равны, соответственно, 5 и 3 – то есть, двум нетривиальным делителям числа 15.

Наш метод даст делитель N при условии, что r окажется простым числом, и что ни одно из чисел $(a^{r/2} \pm 1)$ не делится на N без остатка. Чтобы гарантировать, что эти два условия выполняются достаточно часто (для случайно выбранных чисел a), воспользуемся

Теоремой: Пусть N – нечетное число, и предположим, что $a < N$ взаимно просто с N выбрано случайным образом. Пусть r – порядок a по модулю N. Тогда вероятность того, что число r – четное, и что $(a^{r/2} \pm 1)$, не делятся на N без остатка, всегда $\geq 1/2$. □

Доказательство (довольно длинное) этой теоремы можно найти в приложении В к работе [144], к которой мы отсылаем читателя за деталями.

В целом, наш метод позволит найти делитель N с вероятностью, по крайней мере, 50% в каждом случае. Эту вероятность успешного вычисления можно сделать насколько угодно близкой к единице, поскольку после K повторений всей процедуры (с константой K не зависящей от N) число N окажется факторизовано с вероятностью, превышающей $1 - 1/2^K$.

Все шаги в этой процедуре – например, применение алгоритма Евклида или арифметические операции с числами, – можно проделать за время poly(log N). Единственный спорный элемент алгоритма – это способ найти r за время poly(log N). Рассмотрим экспоненциальную функцию

$$f(x) = a^x \bmod N \ . \tag{4.29}$$

Теперь (4.27) утверждает, в точности, что функция f – периодическая с периодом r, то есть, что $f(x+r) = f(x)$. Значит, можно использовать квантовый алгоритм для определения периода, описанный в предыдущем разделе, чтобы найти r. Чтобы применить этот алгоритм, нам надо ограничить диапазон значений x в (4.29) *конечной* областью $0 \leq x \leq q$ для некоторого q. Если q не делится на (неизвестное) число

r, то есть, $q = Ar+t$ для некоторого $0 < t < r$, то получившаяся функция не будет в точности периодической – один последний период, состоящий из t значений, будет неполным. Однако если будет выбрано достаточно большое q, содержащее большое количество периодов функции f, то влияние последнего неполного периода на преобразование Фурье размера $q \times q$ будет пренебрежимо мало. Это интуитивно ясно. На самом деле, можно показать, что, если выбрать q порядка $O(N^2)$, то можно определить r достаточно точно. Более подробный анализ этой неполной периодичности (включающий теорию непрерывных дробей) читатель сможет найти в [36, 144]. В качестве числа q обычно выбирается некоторая степень двойки, что особенно хорошо согласуется с формализмом быстрого преобразования Фурье (см. [134, 145]).

4.2.7 Квантовый поиск и NP

Предположим, что у нас есть база данных, представляющая собой неупорядоченный неструктурированный лист из N записей, по крайней мере, одна из которых удовлетворяет некоторому заданному интересующему нас свойству. Мы хотим найти эту особенную запись. Любому классическому методу, определяющему местонахождение этой записи с некоторой постоянной (не зависящей от N) вероятностью потребуется $O(N)$ шагов. Ибо, согласно элементарной теории вероятностей, если мы проверим k записей, то найдем нужную с вероятностью k/N. Эта вероятность стремится к 0 при увеличении N, если только само число k – не порядка N. Алгоритм квантового поиска Гровера [120, 150] решает задачу всего лишь за $0(\sqrt{N})$ шагов. В этой задаче квантовые эффекты ускоряют решение в корень из числа шагов, в отличие от намного более сильного экспоненциального ускорения в квантовых алгоритмах, которые мы обсуждали выше. В алгоритме Гровера нам потребуется возможность проверять суперпозиции записей, точно так же, как в предыдущих алгоритмах оценивались значения функций от суперпозиций входных данных.

Предположение о неструктурированности базы данных очень важно для нашего результата. Например, если бы база данных состояла из N случайных чисел, *отсортированных* в возрастающем порядке, то нам понадобилось бы всего $O(\log N)$ шагов, чтобы классически (с помощью стандартного метода деления пополам) отыскать любое из этих чисел. Аналогично, можно было бы использовать любую заранее известную структуру базы данных, чтобы уменьшить время поиска. Предположение о неструктурированности аналогично тому, как мы ранее использовали оракулы (или черные ящики), внутренняя структура которых была нам недоступна. На самом деле, можно следую-

щим образом более аккуратно переформулировать задачу поиска в базе данных на языке оракулов: нам дан черный ящик, который вычисляет функцию от N входных данных, со значениями на выходе 0 или 1. Кроме того, известно, что $f(x) = 1$ только для одного вводного значения x_0. Наша задача – найти x_0.

Сейчас мы кратко опишем алгоритм квантового поиска Гровера для нахождения x_0 за $O(\sqrt{N})$ шагов. (Дальнейшие технические детали можно при желании при первом чтении пропустить. Следует только запомнить черты этого алгоритма, описанные выше). Как и при обсуждении алгоритма Дойча и квантового параллельного вычисления, предположим, что оракул задан как унитарное преобразование U_f, которое преобразует $|x\rangle|j\rangle$ в $|x\rangle|j \oplus f(x)\rangle$. Здесь $1 \le x \le N$, $j = 0$ или 1, и $\oplus$ обозначает сложение по модулю 2. Будет также удобно ограничить наше внимание случаем, когда $N = 2^n$, то есть, когда N – степень двойки, так что f есть функция от n битов со значениями на одном бите. Пусть $\mathcal{B}^n$ есть гильбертово пространство n кубитов (т.е. входного регистра) со стандартным базисом $\{|x\rangle\}$, помеченным всеми n-битными строками x. В своей первоначальной форме алгоритм Гровера основан на двух унитарных операциях, I_{x_0} и D, каждая из которых действует на $\mathcal{B}^n$. I_{x_0} – это унитарная операция, которая просто инвертирует амплитуду $|x_0\rangle$:

$$I_{x_0}|x\rangle = \begin{cases} |x\rangle & \text{если } x \neq x_0 \\ -|x\rangle & \text{если } x = x_0 \end{cases} \qquad (4.30)$$

Ее легко сконструировать с помощью U_f, заранее установив ее выходной регистр (последние $n+1$ кубитов) в состояние $1/\sqrt{2}(|0\rangle - |1\rangle)$, как это мы делали в алгоритме Дойча. Тогда применение U_f будет эквивалентно действию на входном регистре, в то время как выходной регистр останется в состоянии $1/\sqrt{2}(|0\rangle - |1\rangle)$(см. Рис. 4.8).

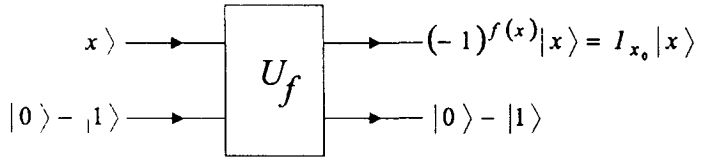


Рис. 4.8. Создание I_{x_0} с помощью U_f. Здесь f обозначает оракул, который помечает x_0.

Оператор D определяется следующим образом. Пусть H_n обозначает применение H (см. (4.1)) к каждому из n кубитов, и пусть I_0 будет оператором I_{x_0} с $x = 00\ldots0$. Тогда D определяется как

$$D = -H_n I_0 H_n \,. \qquad (4.31)$$

Прямое вычисление матричных элементов D [120, 150] показывает, что все недиагональные матричные элементы равны $2/N$, а все диагональные равны $-1+2/N$ (напомним, что здесь $N = 2^n$). Следовательно

$$D|x\rangle = -|x\rangle + \frac{2}{N}\sum_y |y\rangle \ . \tag{4.32}$$

У D есть простая геометрическая интерпретация: «инверсия относительно среднего». Для любого состояния $|\psi\rangle = \Sigma a_x|x\rangle$, положим $D|\psi\rangle = \Sigma a'_x|x\rangle$, и пусть $\bar{a}=(1/N)\Sigma a_x$ обозначает среднюю амплитуду для состояния $|\psi\rangle$. С помощью (4.32) получаем

$$a'_x = -a_x + \frac{2}{N}\sum_y a_y = \bar{a} - (a_x - \bar{a}) \ . \tag{4.33}$$

Обозначив $\Delta a_x = a_x - \bar{a}$, получим, что $a_x = \bar{a} + \Delta a_x$ и $a'_x = \bar{a} - \Delta a_x$, так что значения амплитуд просто отражены относительно среднего $\bar{a}$.

Чтобы выполнить алгоритм Гровера, начнем с равной суперпозиции $|\psi_0\rangle = (1/\sqrt{N})\Sigma|x\rangle$, которую можно приготовить, например, применив H_n к $|0...0\rangle$. Это состояние соответствует проверке всех элементов базы данных в равной суперпозиции. Наша цель – так изменить $|\psi_0\rangle$, чтобы сконцентрировать всю амплитуду на $x = x_0$. Алгоритм состоит из многократного применения оператора DI_{x_0}, что приводит к последовательности состояний $|\psi_k\rangle$:

$$|\psi_0\rangle = \frac{1}{\sqrt{N}}\sum|x\rangle$$
$$|\psi_{k+1}\rangle = DI_{x_0}|\psi_k\rangle \ . \tag{4.34}$$

С помощью выражений для D и I_{x_0}, легко видеть, что амплитуды всех $|x\rangle$ с $x \neq x_0$ остаются равными друг другу, так что каждое состояние $|\psi_k\rangle$ имеет вид

$$|\psi_k\rangle = \alpha_k \sum_{x\neq x_0}|x\rangle + \beta_k|x_0\rangle \ , \tag{4.35}$$

где, также, α_k и β_k – действительные числа. Используя выражения для матричных элементов D и I_{x_0}, можно вывести рекуррентные соотношения:

$$\alpha_0 = \beta_0 = \frac{1}{\sqrt{N}} \ ,$$
$$\alpha_{k+1} = (1-\frac{2}{N})\alpha_k - \frac{2}{N}\beta_k \ , \tag{4.36}$$
$$\beta_{k+1} = (1-\frac{2}{N})\beta_k + (N-1)\frac{2}{N}\alpha_k \ .$$

Нормировка дает

$$\beta_k^2 + (N-1)\alpha_k^2 = 1 \ , \tag{4.37}$$

из чего следует, что было бы удобно ввести обозначения

$$\alpha_k = \frac{1}{\sqrt{N-1}} \cos\theta_k$$

и $\beta_k = \sin\theta_k$.

Тогда можно убедиться [151], что рекуррентные соотношения (4.36) выполняются при

$$\alpha_k = \frac{1}{\sqrt{N-1}} \cos(2k+1)\theta \quad , \quad \beta_k = \sin(2k+1)\theta \quad , \tag{4.38}$$

где угол θ определен равенством $\sin\theta = 1/\sqrt{N}$.

Таким образом, при изменении k, β_k меняется по синусоидальному закону. У нас получится $\beta_k = 1$, например, если $(2k+1)\theta = \pi/2$ – то есть, при $k = (\pi - 2\theta)/4\theta$. Для больших N можно считать $\sin\theta = 1/\sqrt{N} \approx \theta$, и тогда $k = \pi/4\sqrt{N} - 1/2$, что порядка $\sqrt{N}$. Значит, если мы проделаем итерации такое число раз, которое будет равно целому числу, ближайшему к этому значению k, то сможем с высокой (и не зависящей от N) вероятностью найти x_0, произведя считывание конечного состояния в стандартном базисе (см. [151] для дальнейшего анализа рассматриваемых вероятностей). На этом алгоритм завершен.

Со времени появления первой работы Гровера основные идеи, использованные в описанном выше алгоритме, были далее развиты в большом количестве других приложений – таких, как оценка среднего и медианы в базе данных из N чисел [152], или анализ случая более чем одной помеченной записи в базе данных [151, 153]. Использовав оригинальную комбинацию алгоритмов Гровера и Шора, Брассар, Хойе и Тапп показали [153], что возможно также узнать *количество* помеченных записей (не определяя их положение). Не вдаваясь в детали, идея, лежащая в основе их подхода, состоит в том, что амплитуды α_k и β_k, описанные выше, изменяются периодически с периодом, зависящим от числа помеченных записей. Эта периодичность оценивается с помощью квантового преобразования Фурье, как это было отмечено в предыдущих разделах. Также было показано [151, 153, 154], что, хоть это и удивительно на первый взгляд, если заменить в определении D унитарную операцию H_n на почти унитарную операцию U, то алгоритм с измененным определением D все равно сможет находить x_0 за $O(\sqrt{N})$ шагов.

Алгоритм Гровера дает нам возможность проводить поиск в экспоненциально большом пространстве данных. Проблема экспоненциального поиска очень важна для многих областей математики и программирования. С практической точки зрения, интересна ситуация, когда можно проверить, выполняется ли для данной записи желаемое

свойство (то, по которому проводится поиск) за *полиномиальное* время – проще говоря, когда, «вычислительно легко» проверить, выполняется ли это свойство для одного кандидата, но поиск надо вести среди экспоненциально большого их числа. Например, предположим, что нам дан граф, который состоит из набора вершин, а также ребер, соединяющих между собой некоторые вершины. Граф с n вершинами можно записать в виде матрицы $n \times n$, состоящей из нулей и единиц, в которой элемент ij равен 1 тогда и только тогда, когда в графе есть ребро, соединяющее вершину i с вершиной j. Мы хотим узнать, существует ли замкнутый путь, по которому можно обойти все вершины, побывав на каждой ровно один раз. У этой, так называемой, задачи о гамильтоновой цепи, есть много важных приложений. В общем случае, если дан граф, то на нем существует экспоненциально много возможных цепей (то есть, экспоненциально много, как функция от размера матрицы, описывающей граф). Но если дана цепь, то легко за полиномиальное время проверить, удовлетворяет она требуемому условию, или нет (надо просто обойти эту цепь и посмотреть, побывает ли она на каждой вершине ровно один раз). В теории вычислительной сложности класс задач такого типа называется *NP* (см. более глубокое обсуждение в [131, 132]). С интуитивных позиций, в задачах класса *NP* «трудно» найти элемент, удовлетворяющий условиям, но «легко» проверить, удовлетворяется условие или нет.

Многие очень интересные с точки зрения как математики, так и практики вычислительные задачи принадлежат классу *NP* (см. длинный и разнообразный перечень примеров в [132]). Пожалуй, самая знаменитая нерешенная проблема в классической теории вычислительной сложности – это проблема $P \neq NP$, которая состоит в вопросе, возможно ли решить за полиномиальное время любую задачу из *NP*. Мотивирующая идея здесь состоит в том, что если выполнение свойства можно «вычислительно легко» проверить, то, может быть, на вопрос, содержится ли оно в данной структуре, также можно ответить за полиномиальное время. Заметим, что мы здесь думаем не о полном просмотре экспоненциально большого числа кандидатов (что гарантированно потребовало бы экспоненциального времени), но о некоем хитром анализе самой структуры, породившей экспоненциально большое число возможностей. Например, для задачи о гамильтоновой цепи – существует ли способ как-то проверить описание самого графа, чтобы увидеть, содержит ли он гамильтонову цепь, вместо того, чтобы примитивно проверять все цепи по очереди.

Учитывая сложность и масштаб некоторых задач из класса *NP* [132], маловероятно, что их можно решить за полиномиальное вре-

мя. Однако, несмотря на огромное внимание, этот факт до сих пор не доказан! Заметим, что в каждом случае приходится привлекать те или иные особенные математические свойства данной структуры – например, решение задачи о гамильтоновой цепи было бы равносильно доказательству некоей новой глубокой теоремы в теории графов.

Вернемся теперь к алгоритму поиска Гровера. Здесь требовалось, чтобы база данных была *неструктурированной* (в противоположность тому, что только что было описано), и, тем не менее, с помощью квантовых методов, мы достигли ускорения в квадратный корень числа шагов по сравнению с прямым полным классическим поиском. Это ускорение можно применить к поиску вслепую в любой задаче из класса *NP*. Критический вопрос здесь таков: можно ли ускорить поиск в *неструктурированном* пространстве с экспоненциально большим числом элементов *еще сильнее*, используя квантовые эффекты каким-то еще более хитрым образом? Например, мы видели, что можно создать экспоненциально большие суперпозиции за линейное время (4.3), и что можно использовать эти суперпозиции, чтобы за один запрос проверить экспоненциально большое число значений функции (см. (4.4)). В первые дни теории квантовых вычислений была надежда, что этот эффект может привести к методу просмотра за полиномиальное время экспоненциально большого пространства возможностей, что привело бы к квантовому методу решения любой задачи из *NP* за полиномиальное время. Например, если дан граф, то мы можем рассматривать суперпозиции любых возможных цепей – но можно ли использовать этот эффект, чтобы с высокой вероятностью определить, существует или нет гамильтонова цепь? Эта надежда была разбита в работе [155] Беннетом, Бернстайном, Брассаром и Вазирани, которые строго доказали, что никакой квантовый процесс не может ускорить неструктурированный поиск сильнее, чем ускорение в квадратный корень, которое достигается в алгоритме Гровера. Грубо говоря, их идея состоит в следующем. Хотя мы и можем проверить за один запрос экспоненциально большое число кандидатов, находящихся в суперпозиции, но, в общем случае, регистрация желаемого свойства произойдет с экспоненциально малой амплитудой из-за экспоненциально большого числа элементов в суперпозиции. Следовательно, чтобы зарегистрировать свойство с любым постоянным уровнем вероятности, придется повторить весь процесс экспоненциально большое число раз.

Таким образом, в контексте квантового вычисления, точно так же, как и в классическом вычислении, если мы хотим решить задачу из класса *NP* за полиномиальное время, то мы должны каким-то хитрым

образом использовать структуру задачи. Например, экспоненциальное ускорение в алгоритмах Саймона и Шора достигается с использованием специальных математических свойств теории периодичности через технику Фурье-анализа. К сожалению, оказывается, что решение важного вопроса о связи всего класса *NP* с вычислимостью за полиномиальное время выглядит в квантовом контексте ничуть не ближе, чем в контексте классической теории вычислительной сложности.

4.3 Квантовые ЛЭ и квантовое вычисление с захваченными ионами

Дж.И. Цирак, П.Цоллер, О.Ф.Поятос

4.3.1 Введение

Из того, что обсуждалось выше, ясно, что квантовое вычисление может быть удивительно мощным инструментом. Весь вопрос в том, можем ли мы воплотить в реальность основные элементы квантового вычисления – такие, как, например, квантовые логические элементы – и, если да, то в каких физических системах. Вместо общего обсуждение проблемы, мы сосредоточимся на одном конкретном примере. Мы опишем в некоторых деталях проекты, связанные с созданием квантового компьютера на основе системы захваченных ионов [156, 157]. В этой схеме каждый кубит – это суперпозиция основного электронного состояния ($|0\rangle$) и возбужденного (метастабильного) состояния ($|1\rangle$) иона в ловушке (см. Рис. 4.9). Будет показано, что набор ионов, двигающихся в линейной ловушке и взаимодействующих с лазерным светом – это реальная физическая система, на основе которой может быть создан квантовый компьютер.

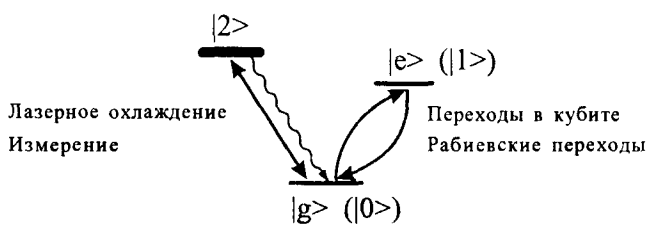


Рис. 4.9. Двойная резонансная структура внутренних уровней одного иона. Два из этих уровней, вместе со слабым переходом между ними, действуют как кубит ($|0\rangle$, $|1\rangle$), тогда как третий уровень, $|2\rangle$, связанный с состоянием $|0\rangle$ дипольно-разрешенным переходом, служит для охлаждения и измерения, с помощью метода квантового скачка.

4.3.2 Квантовые логические элементы с захваченными ионами

Мы рассмотрим ситуацию, когда N ионов содержатся в линейной ловушке Пауля (со скрещенными полями), которая может захватывать и держать ионы с помощью комбинации статического и переменного электрических полей (см. главу 5). Ионы, в основном, двигаются вдоль оси ловушки, так как в этом направлении захватывающий потенциал довольно слаб, и взаимодействуют с различными лазерными полями (Рис. 4.10).

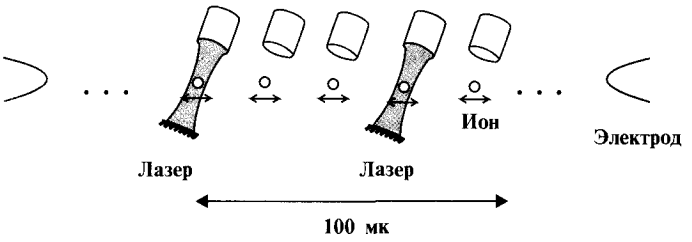


Рис. 4.10. N ионов в линейной ловушке, взаимодействующих с лазерным полем. Движение ионов используется в качестве шины данных между кубитами.

Взаимная связь в движении различных ионов создается кулоновским отталкиванием, которое сильнее всех остальных взаимодействий при типичных расстояниях между ионами в несколько оптических длин волн.

Одно из преимуществ систем захваченных ионов перед другими системами состоит в том, что многие необходимые методы управления квантовыми состояниями и их приготовления к настоящему моменту уже хорошо развиты в исследованиях по высокоточной спектроскопии и стандартам частоты. Например, переходы Раби и измерения электронных состояний ионов являются хорошо разработанными инструментами. Эти методы будут основными составляющими квантового вычисления. В то время как переходы Раби, то есть когерентные переходы между внутренними состояниями, осуществляются с помощью лазерного импульса фиксированной длительности (например, π-импульс полностью переводит атом с возбужденного состояния на основное и наоборот), измерения внутреннего состояния производятся с помощью так называемой техники квантового скачка. Рассмотрим ситуацию двойного резонанса, где один резонансный переход – очень сильный, а второй намного слабее. В этом случае, можно измерить состояние избранных уровней, реализующих кубиты. Это делается с помощью двух лазерных импульсов, настроенных в резонанс, соответственно, на каждый из двух переходов. Состояние кубита бу-

дет измерено по присутствию или отсутствию спонтанно испущенного фотона, соответствующего сильному (дипольно-разрешенному) переходу, см. Рис. 4.9. Оказалось, что эффективность этой схемы детектирования почти достигает единицы. С другой стороны, мы будем также использовать методы лазерного охлаждения, чтобы свести движение ионов к малым колебаниям около положения равновесия. Говоря вкратце, лазерное охлаждение основано на эффективном использовании давления излучения - импульса, которым обладает любой световой луч. Такой импульс, пренебрежимо малый на макроскопической шкале, может, тем не менее, действовать на атомы с силой достаточно большой для того, чтобы заметно уменьшить их скорости (эта сила может достигать $10^4 g$, где g – это ускорение свободного падения). Можно эффективно использовать такие силы с помощью эффекта Доплера: таким образом, ионы, двигающиеся в сторону, противоположную направлению распространения лазерного пучка, будут испытывать силу, способную существенно замедлить их движение.

Предположим, что ионы охлаждены лазером во всех трех измерениях, так что они могут совершать только малые колебания вокруг положения равновесия. В этом случае движение ионов описывается в терминах нормальных мод, что эквивалентно набору несвязанных осцилляторов, которые могут быть проквантованы обычным образом. Для этого для каждой моды должен быть достигнут так называемый предел Лэмба-Дике, который физически означает, что ион содержится в области, намного меньшей, чем длина волны используемого излучения.

Задача построения квантового компьютера будет эквивалентна вопросу о том, как создать одно- и двух-кубитные логические элементы. Создать одно-кубитные элементы будет просто, так как все, что для этого нужно – это применить переходы Раби между внутренними состояниями кубита. Как мы уже отмечали, эта техника для захваченных ионов хорошо известна. Основная трудность состоит в том, чтобы квантовомеханически связать два кубита – то есть, чтобы создать их когерентную суперпозицию. Чтобы это сделать, мы рассмотрим внешние степени свободы, связанные с движением всей цепочки ионов. В частности, мы используем самую низкую квантованную моду – движение центра масс (ЦМ), описывающую движение всех ионов так, как если бы они представляли собой одну объединенную массу. Задача здесь состоит в том, чтобы перенести информацию с одного внутреннего кубита на «*квантовый провод*» – движение ЦМ. Как только это будет выполнено, будет также возможно перенести информацию с «*квантового провода*» на другой выбранный кубит, осуществив таким образом когерентное взаимодействие между двумя кубитами.

4.3.3 N холодных ионов, взаимодействующих с лазерным светом.

Этот раздел будет содержать несколько более технический материал. Здесь будет более детально показано, как описать систему ионов и лазеров, а также ее способность выполнять квантовые вычисления. Рассмотрим взаимодействие данного иона *i* со стоячей лазерной волной (таким же образом можно описать и бегущую волну). Гамильтониан, которым описывается эта ситуация, в системе отсчета, вращающейся с лазерной частотой, записывается как $H = H_{ex} + H_{int} + H_{las}$, где ($\hbar = 1$)

$$H_{ex} = \sum_{k=1}^{N} \nu_k a_k^{\dagger} a_k \ ,$$

$$H_{\text{int}}^{i} = -\frac{\delta_i}{2}\sigma_z^i \ ,$$

$$H_{las}^{i} = \frac{\Omega_i}{2}\sin(k_L r_i + \phi_i)(\sigma_i^{+} + \sigma_i^{-}) \ . \qquad (4.39)$$

Здесь $\delta_i = \omega_L^i - \omega_0^i$ – это расстройка лазера (здесь $\omega^i{}_L$ обозначает частоту лазера, а $\omega^i{}_0$ – частоту, связанную с переходом в кубите), ν_k – частоты различных нормальных мод, Ω_i – частота Раби[1] (скорость когерентной эволюции, вызванной лазерным полем), k_L – волновой вектор лазерной волны (как правило, лазерный луч подает под углом к оси ловушки. В этом случае k_L будет равен $k_\theta = k_L \cos(\theta)$, см. Рис. 4.10), ϕ_i – фаза, описывающая положение иона относительно стоячей волны, и r – координата иона (в общем случае, выраженная через линейную комбинацию нормальных мод). Кроме того, мы использовали операторы Паули, относящиеся к двухуровневому атому со спином 1/2, а также операторы рождения (уничтожения), относящиеся к квантованному гармоническому осциллятору.

Когда лазерный луч действует на один из ионов, он вызывает переходы между (внутренними) основным и возбужденным состояниями, а также может изменить состояние коллективных нормальных мод. Однако, в пределе Лэмба-Дике, и с учетом достаточно слабой интенсивности излучения лазера, будет изменено только движение ЦМ. В этих пределах, взаимодействие с лазером можно представить в виде

$$H_{las}^{i} \approx H_a^i + H_b^i$$

[1] Этот термин связан с именем И. И. Раби, который разработал метод использования осциллирующго магнитного поля, чтобы вызвать переходы между внутренними уровнями в атомах и молекулах.

$$= \frac{\Omega_i^a}{2}(\sigma_i^+ + \sigma_i^-) + \frac{\Omega_i^b}{2}\frac{\eta_{\text{ЦМ}}}{\sqrt{N}}(a_{\text{ЦМ}}\sigma_i^+ + a_{\text{ЦМ}}^\dagger \sigma_i^-) \qquad (4.40)$$

где $\eta_{\text{цм}}$ – это параметр Лэмба-Дике, связанный с частотой захвата в аксиальном направлении ν_z, которая совпадает с частотой ЦМ моды. Можно использовать приведенный здесь гамильтониан, только если $\Omega_1{}^a \neq 0$ ($\delta_a = 0$) или $\Omega_1{}^b \neq 0$ ($\delta_b \approx -\nu_1$). Это значит, что мы найдем два возможных взаимодействия, либо изменяющих (*b*), либо не изменяющих (*a*) движение ионов.

Покажем теперь, как на основе этих взаимодействий можно реализовать квантовые логические элементы с одним и двумя кубитами. Можно легко создать одно-кубитные квантовые логические элементы, поскольку они связаны только с вращениями вектора состояния отдельного иона, без изменения состояния его перемещения. Их можно реализовать с помощью лазера, настроенного в резонанс по отношению к частоте внутреннего перехода ($\delta_i = 0$). При этом ион локализован в пучности стоячей лазерной волны. Мы видели, что в этом случае эволюция задана гамильтонианом $H_a{}'$, и включает в себя следующее вращение

$$|g\rangle_i \to \cos(k_L\pi/2)|g\rangle_i - ie^{i\phi}\sin(k_L\pi/2)|e\rangle_i,$$
$$|e\rangle_i \to \cos(k_L\pi/2)|e\rangle_i - ie^{-i\phi}\sin(k_L\pi/2)|g\rangle_i.$$

С другой стороны, реализовать двух-кубитные логические элементы будет труднее. Для начала, пусть лазерная частота выбрана так, что $\delta_i = -\nu_z$, то есть, она возбуждает только одну моду ЦМ, и ион локализован в узле стоячей волны лазерного луча. Взаимодействие с лазером задано теперь гамильтонианом $H_b{}^i$. После включения лазера на фиксированный отрезок времени $t = k\pi/(\Omega_i^b\ \eta_z/\sqrt{N})$ ($k\pi$-импульс), состояния изменятся следующим образом:

$$|g\rangle_i|1\rangle \to \cos(k_L\pi/2)|g\rangle_i|1\rangle - ie^{i\phi}\sin(k_L\pi/2)|e'\rangle_i|0\rangle,$$
$$|e'\rangle_i|0\rangle \to \cos(k_L\pi/2)|e'\rangle_i|0\rangle - ie^{-i\phi}\sin(k_L\pi/2)|g\rangle_i|1\rangle,$$
$$|g\rangle|0\rangle \to |g\rangle|0\rangle\ , \qquad (4.41)$$

где $|0\rangle$ ($|1\rangle$) обозначает моду ЦМ с нулем фононов (одним фононом), ϕ – это фаза лазера, и $|e'\rangle$ может быть либо состоянием $|1\rangle$ рассматриваемого кубита (обозначается как $|e\rangle$), либо селективно возбужденным вспомогательным электронным состоянием. (Это селективное возбуждение можно создать с помощью различных поляризаций или частот. С точки зрения эксперимента, похоже, что частотами удается лучше управлять, чем поляризациями). Двух-кубитный логический

квантовый элемент может быть создан следующим образом: (i) сфокусировав на первом ионе π-импульс, мы меняем внутреннее состояние первого иона на состояние движения в моде ЦМ, (ii) проводим условную перемену знака, сфокусировав 2π-импульс на втором ионе и использовав вспомогательный уровень $|e'\rangle_i$, и (iii) π-импульс поменяет состояние моды ЦМ обратно на внутреннее состояние первого иона. Полная эволюция будет выражаться как

$$\begin{array}{ccccccc} & (i) & & (ii) & & (iii) & \\ |g\rangle_1|g\rangle_2|0\rangle & \rightarrow & |g\rangle_1|g\rangle_2|0\rangle & \rightarrow & |g\rangle_1|g\rangle_2|0\rangle & \rightarrow & |g\rangle_1|g\rangle_2|0\rangle, \\ |g\rangle_1|e\rangle_2|0\rangle & \rightarrow & |g\rangle_1|e\rangle_2|0\rangle & \rightarrow & |g\rangle_1|e\rangle_2|0\rangle & \rightarrow & |g\rangle_1|e\rangle_2|0\rangle, \\ |e\rangle_1|g\rangle_2|0\rangle & \rightarrow & -i|g\rangle_1|g\rangle_2|1\rangle & \rightarrow & i|g\rangle_1|g\rangle_2|1\rangle & \rightarrow & |e\rangle_1|g\rangle_2|0\rangle, \\ |e\rangle_1|e\rangle_2|0\rangle & \rightarrow & -i|g\rangle_1|e\rangle_2|1\rangle & \rightarrow & -i|g\rangle_1|e\rangle_2|1\rangle & \rightarrow & -|e\rangle_1|e\rangle_2|0\rangle. \end{array} \tag{4.42}$$

Таким образом, конечным результатом эволюции будет перемена знака в только том случае, если оба иона находятся в возбужденном (внутреннем) состоянии. Заметим, что до и после логического элемента ЦМ мода находится в состоянии вакуума $|0\rangle$. Наконец, с помощью этих операций мы можем реализовать логические элементы с использованием *n-кубитов* в любом наборе ионов.

4.3.4 Квантовые логические элементы при ненулевой температуре

В предыдущем разделе мы видели, что система, состоящая из набора ионов в линейной ловушке, может оказаться многообещающим кандидатом для реального осуществления квантовых вычислений в эксперименте. Похоже, что основные требования для вычислений с лазерно-охлажденными ионами в ловушках – это точное управление операциями с гамильтонианом, высокая степень декогерентности, и охлаждение ионов до основного колебательного состояния, чтобы приготовить чистое начальное состояние коллективной фононной моды. Мы не будем углубляться в первые две проблемы, поскольку они больше относятся к таким темам, как исправление ошибок и декогерентность, которые будут обсуждаться в главе 7. Здесь мы покажем, как можно преодолеть ограничение, требующее в пределе охлаждения до нулевой температуры.

Рассмотрим случай двух ионов в линейной ловушке. Оригинальная идея здесь состоит в том, чтобы использовать движение пространственного волнового пакета одного иона направо либо налево, в зависимости от поглощения лазерного фотона или вынужденного испускания, после чего положение второго иона в ловушке будет за-

висеть от динамики первого. Таким образом, можно вызывать изменение состояния второго иона, в зависимости от координаты. В результате получается необходимый для вычисления квантовый логический элемент, в котором конечное внутреннее состояние второго иона зависит от начального внутреннего состояния первого иона.

В некотором смысле, мы использовали идеи из атомной интерферометрии, в которой атомные волновые пакеты обычно разделяются на несколько частей, каждая часть участвует в своем динамическом процессе и в конце их объединяют, чтобы изучить их предыдущую эволюцию путем своего рода анализа оптической интерференции.

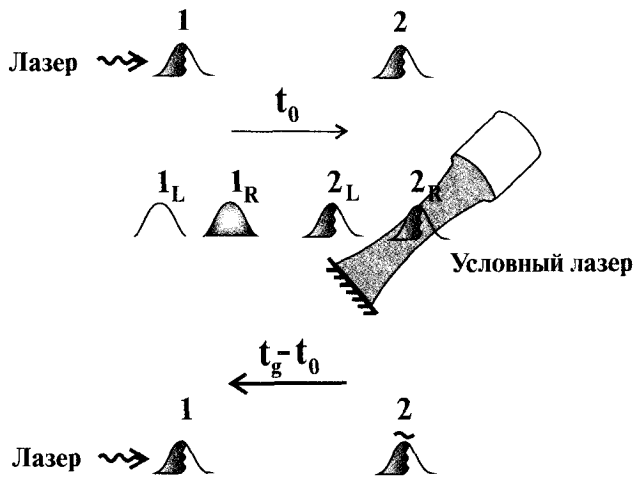
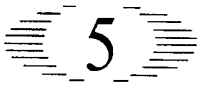


Рис. 4.11. Лазеры и конфигурация волновых пакетов для двух-кубитного логического элемента при ненулевой температуре. После прохождения логического элемента, внутреннее состояние кубита-мишени (ион 2) либо изменится, либо нет (обозначено тильдой), в зависимости от внутреннего состояния контрольного кубита (ион 1) – то есть, толчка направо или налево из-за поглощения или вынужденного излучения фотона. Здесь темный (светлый) цвет пакета обозначает возбужденное (основное) внутреннее состояние. См. более подробное изложение в тексте.

Покажем, в частности, как можно осуществить двух-кубитную логическую операцию. Сначала, с помощью лазерного луча, ион 1 толкается налево или направо, в зависимости от его внутреннего состояния, благодаря излучению (поглощению) фотона. Таким образом, второй ион получит толчок, через кулоновское отталкивание, зависящий от внутреннего состояния иона 1. Соответствующий волновой пакет превратится в два возможных волновых пакета, перепутанных с внутренним состоянием управляющего иона (обозначено 1_R, 1_L, ... для иона 1

двигающегося направо и налево, и т. д.). Если пространственное разделение этих волновых пакетов (в некоторый момент t_0) достаточно велико, то мы можем манипулировать ионом-мишенью, ионом 2, в зависимости от его положения в пространстве (то есть, в зависимости от состояния управляющего иона (иона 1)) и таким образом произвести логическую операцию на кубитах. В дальнейшем эти атомные волновые пакеты начнут осциллировать в ловушке, и, с помощью соответствующей последовательности лазерных импульсов, можно будет уничтожить этот импульс, переданный двум ионам, и восстановить (в момент времени t_g) начальное состояние пространственного движения, см. Рис. 4.11. Тогда состояние пространственного движения иона до и после действия логического элемента будет факторизовано по отношению к внутреннему атомному состоянию, независимо от того, смешанное это состояние или чистое – то есть, независимо от температуры.

В этой главе были рассмотрены перспективные системы для выполнения квантовых вычислений. Обсуждались следствия, вытекающие из условной динамики ионов, которые приводят к двум противоположным ситуациям, а именно, к режимам нулевой и ненулевой температур. Обоснование использования режима нулевой температуры было сделано группой Д. Вайнлэнда из NISTa [158]; показано, что построение квантовых компьютеров на мелкомасштабных ионных ловушках станет вполне реальным в ближайшем будущем. В следующей главе будут представлены некоторые аспекты экспериментальной реализации квантовых логических элементов.



На подступах к квантовым вычислениям: эксперимент

5.1 Введение

В предыдущей главе были изложены основные теоретические идеи квантовых вычислений. Но насколько вероятно на самом деле построить квантовый компьютер? Реализация даже одного квантового логического элемента требует, чтобы две сильно взаимодействующие квантовые системы были абсолютно изолированы от внешних возмущений, что сдерживает наш оптимизм. В этой главе представлены несколько экспериментальных процедур и результатов, которые показывают, что возможно создание небольшого количества в высокой степени управляемых, сильно взаимодействующих квантовых систем. Не будем, однако, загадывать ляжет ли это в основу практических квантовых вычислений.

Предложено три экспериментальных метода, в которых достигнуты подходящие условия для реализации мелкомасштабных квантово-логических операций. Это – квантовая электродинамика резонаторов (КЭР), эксперименты с ионами в ловушках и ядерный магнитный резонанс (ЯМР). Первые два метода используют простейшую связанную квантово-механическую систему: двухуровневую систему, взаимодействующую с квантовым осциллятором. Чтобы подчеркнуть эту общую особенность, в разделе 5.2 эксперименты по КЭР рассматриваются параллельно с соответствующими экспериментами по ионам в ловушках.

Эксперименты по КЭР были особенно успешными при демонстрации фундаментальных особенностей квантовой механики, таких как квантовые осцилляции Раби, представленные в разд. 5.2.3, состояния шредингеровского кота и квантовой декогерентности; они рассмотрены в разд. 5.2.4. Эти эксперименты демонстрируют прекрасный способ реализации основных квантовых логических операций; однако, представляется, что используя эти методы будет трудно осуществить большое количество таких операций.

Что касается проблемы увеличения масштабов, то эксперименты по ионам в ловушках выглядят более обещающими, т.к. возможно при-

готовить и охладить цепочку ионов в линейной ловушке. Эту цепочку можно рассматривать как регистр кубитов, в котором к каждому кубиту (выполненному на одном атоме) можно обеспечить доступ путем жесткой фокусировки лазерных пучков. В разделах 5.2.5 – 5.2.12 демонстрируется, как осуществляется квантовая логика на уровне единичных ионов, а в разд. 5.3 представлен общий обзор экспериментов по квантовым вычислениям с цепочкой ионов.

Третий метод квантовых вычислений основан на ядерном магнитном резонансе (ЯМР). Здесь уже были продемонстрированы результаты по выполнению небольшой последовательности простых квантово-логических операций. ЯМР подразумевает переходы между зеемановскими подуровнями атомных ядер в магнитном поле. Частоты ЯМР сигналов ядер внутри молекул зависят от детального химического состава окружения ядер. Это открывает доступ к различным ядерным спинам внутри отдельных молекул. Спины играют роль кубитов, которые связаны друг с другом посредством сильных спин-спиновых взаимодействий внутри молекул. Такая связь составляет основной элемент квантового вычисления. В разделе 5.4 описываются принципы квантовых вычислений на основе ЯМР.

Более изощренные пути подхода к построению квантовой логики основаны на твердотельных устройствах. Но хотя прорыв в построении таких устройств был бы чрезвычайно важен, область такого рода исследований не является достаточно развитой, чтобы обсуждать ее в этой книге.

5.2 Эксперименты по КЭР: атомы в резонаторах и ионы в ловушках

Х.С.Ногель, Д.Лейбфрид, Ф.Шмидт-Калер, Дж.Эшнер, Р.Блатт, М.Брунэ, Дж.М.Раймонд, С.Харош.

5.2.1 Двухуровневая система, взаимодействующая с квантовым осциллятором

Атом в оптическом резонаторе или ионы в ловушке могут рассматриваться в хорошем приближении, как двухуровневая система, взаимодействующая с квантовым гармоническим осциллятором. В одном случае двухуровневый атом связывается с модой резонатора. В другом – два внутренних состояния иона (сверхузкие или метастабильные уровни энергии) связываются с колебательными степенями свободы ионов в ловушке. Поэтому обе системы характеризуются одним и тем же взаимодействием. Гамильтониан взаимодействия (Джэйнса-Каммингса) может быть записан в виде:

$$H_{\text{int}} = -\hbar\frac{\Omega}{2}(a\sigma^{+} + a^{+}\sigma^{-}), \qquad (5.1)$$

где a^{+} и a – операторы рождения и уничтожения для квантового осциллятора, σ^{+} и σ^{-} повышающие и понижающие операторы для двухуровневой системы, Ω – постоянная связи. Такой гамильтониан описывает излучение и поглощение фотонов (в случае КЭР экспериментов) или фононов (в случае экспериментов с ионами в ловушках), сопровождаемые атомными или ионными переходами. Когда мода гармонического осциллятора находится точно в резонансе с частотой перехода двухуровневой системы, гамильтониан описывает реальный обмен энергией. Если же система выведена из резонанса, то процессы передачи энергии виртуальны и взаимодействие приводит к сдвигу фазы атомных уровней.

Ключевой момент заключается в реализации режима сильной связи, когда простое взаимодействие (5.1) доминирует над всеми процессами релаксации, такими как спонтанное излучение атомов, фотонное/фононное затухание и декогерентность, вызванная тепловым шумом. Убедительная экспериментальная реализация простейшей системы поле-вещество позволяет продемонстрировать элементарные операции квантовой логики. В то же время эти эксперименты призваны служить тестами в нашем понимании некоторых аспектов квантовой теории, наименее всего поддающихся интуиции, таких как нелокальное перепутывание и мезоскопические суперпозиции состояний.

КЭР развивалась как в оптическом, так и в микроволновом диапазонах – основные принципы проведения экспериментов очень близки. Обзор этих двух типов экспериментов можно найти в [160]. В оптической области атомные переходы требуют наличия высокодобротных резонаторов. Здесь режим сильной связи уже был исследован и реализован. В этом разделе мы уделим основное внимание микроволновому диапазону. Долгоживущие, легко регистрируемые циркулярные ридберговские атомы сильно связываются с излучением миллиметрового диапазона, находящимся в высокодобротном сверхпроводящем резонаторе. Атомы с тепловыми скоростями, проходя через резонатор, оказываются в перепутанном состоянии с модой поля. Времена жизни поля в резонаторе и в атомной двухуровневой системы намного превышают время взаимодействия. Поэтому, поле и атом остаются перепутанными даже после того, как атом покинет резонатор. Таким образом, общее квантовое состояние поля и атома, может быть исследовано или использовано уже после того, как атом покинет резонатор.

Во втором типе экспериментов, рассматриваемом в этом разделе, обсуждаются ионы, запертые в гармонической электромагнитной

ловушке. Квантовый осциллятор представляет собой специфическую колебательную моду ионов. Мода связана посредством лазерных импульсов с внутренним состоянием ионной двухуровневой системе. При точной настройке световых лазерных импульсов взаимодействие движения иона с внутренним состоянием с хорошей точностью описывается гамильтонианом типа Джейнса-Каммингса. Большие времена когерентности ионной двухуровневой системы и колебательной моды удается получить с использованием методов, применяемых при создании ионных стандартов частоты.

Несмотря на существенные различия в экспериментальных методах, атомно-резонаторные и ионно-ловушечные эксперименты описываются в рамках единой простой модели. Поэтому любой эксперимент, проектируемый для КЭР имеет аналог в технике ионных ловушек и наоборот. Более того, результаты, достигнутые в этих двух методах, также приблизительно сопоставимы. В последующих разделах описываются КЭР-эксперименты в резонаторах в СВЧ диапазоне, а так же эксперименты с ионами в ловушках при взаимодействии Джейнса-Каммингса. В заключение дается обзор перспектив использования этих методов в квантовых вычислениях.

5.2.2 КЭР с атомами и резонаторами

В этом разделе представлена общая схема экспериментов по КЭР с атомами в микроволновых резонаторах. Детальное рассмотрение, как в теоретическом, так и в экспериментальном плане содержится, например, в [160, 161].

Циркулярные ридберговские атомы служат исключительно ценным инструментом в экспериментах по КЭР. Такие атомы с их долгоживущими энергетическими уровнями [162, 163], имеющими главные квантовые числа n порядка 50 и максимальные орбитальные и магнитные квантовые числа, ведут себя как огромные антенны, сильно взаимодействующие с излучением миллиметрового диапазона. Матричный элемент дипольного момента перехода между циркулярными состояниями $n = 51$ ($|e\rangle$) и $n = 50$ ($|g\rangle$), что составляет 51.099 ГГц, оказывается порядка 1250 атомных единиц. При помещении в слабое направленное электрическое поле, которое не воздействует на другие уровни, они характеризуются большим временем жизни, достигающим 30 мс, и ведут себя как хорошие двухуровневые системы. К тому же эти уровни могут быть надежно и с большой чувствительностью зарегистрированы с помощью ионизационно-полевого метода.

В миллиметровом диапазоне можно построить качественные резонаторы на основе сверхпроводящих материалов. В экспериментах

используются резонаторы типа Фабри-Перо с ниобиевыми зеркалами и размерами порядка сантиметров. При низких температурах, таких как 0.6 К, добротность лежит в диапазоне от 10^8 до 10^9, что соответствует времени удержания фотона от нескольких сотен микросекунд до нескольких миллисекунд. Это время гораздо больше, чем время взаимодействия атома с полем, составляющее несколько десятков микросекунд для атомов, имеющих тепловые скорости. При таких низких температурах тепловое поле пренебрежимо мало и вероятность найти резонатор в его основном состоянии оказывается порядка 98%.

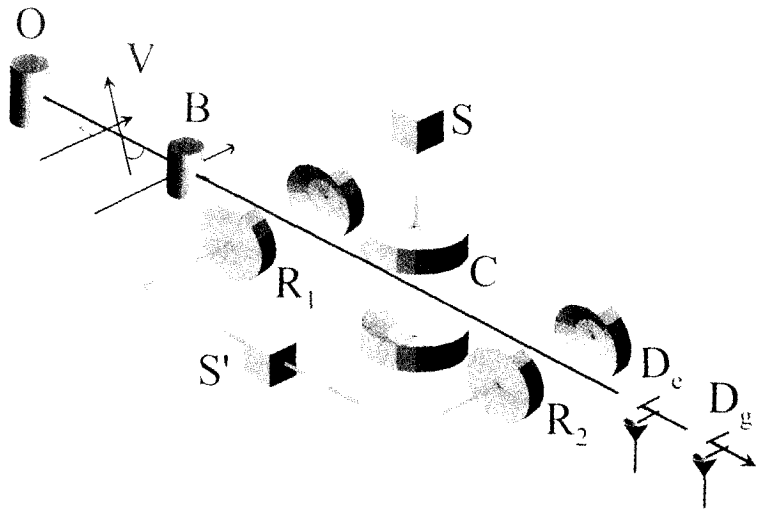


Рис. 5.1. Схема установки в эксперименте с атомом в резонаторе.

Схема экспериментальной установки, используемой в университете Эколь Нормаль (Париж) [164-168], изображена на Рис.5.1. Сердцевина охлаждена до температуры 0.6 К в гелиевом (^{3}He – ^{4}He) криостате. Атомы, испущенные печкой *O*, отбираются по скоростям в зоне *V* методом оптической накачки лазерным пучком, ориентированным под определенным углом к направлению распространения атомов. Отселектированные по скоростям атомы затем приготавливаются (в *B*) в одном из состояний $|e\rangle$ или $|g\rangle$ при помощи последовательности лазерных импульсов и адиабатических переходов в радиочастотном диапазоне [163]. Приготовление происходит в импульсном режиме, так что циркулярные атомы генерируются в определенные моменты времени и с определенными скоростями, распределенными в интервале между 200 и 400 м/с и с точностью ±2 м/с. Положение атомов известно в любое время с точностью ±1 мм. Таким образом, атомы, проходящие через систему, могут быть подвержены селективным преоб-

разованиям. Среднее число атомов, генерируемых за каждую вспышку, поддерживается меньше единицы, так что вероятность приготовления двух атомов одновременно очень мала.

Сверхпроводящий резонатор C изготовлен из двух сферических ниобиевых зеркал, размером 2.7 см каждое. В резонаторе поддерживается поперечная электромагнитная гауссова мода с диаметром перетяжки 6 мм. При необходимости резонатор заполняется полем либо от самих атомов – через процесс резонансной связи, либо от микроволнового источника S, излучающего когерентное поле. Резонатор может быть настроен в резонанс, либо выведен из резонанса с атомным переходом путем подбора расстояния между зеркалами или при изменении частоты перехода с помощью наложения электрического поля через зеркала.

До входа в резонатор C атомы проходят через низкодобротный вспомогательный резонатор R_1, в котором классический микроволновый импульс может перемешивать уровни $|e\rangle$ и $|g\rangle$. Каждый атом проходит C за время несколько десятков фемтосекунд, в течении которого происходит сильное взаимодействие между атомом и резонаторным полем. Постоянная связи атома с полем (Ω при взаимодействии Джейнса-Каммингса) составляет $\Omega/2\pi$ = 50 кГц для атома, находящегося в центре резонатора. Эта величина соответствует скорости обмена единичным фотоном между атомом и резонаторной модой. Когда атом двигается через резонатор, связь $\Omega(\boldsymbol{r})$ выражается через гауссову функцию от его положения. После резонатора C импульс классического микроволнового поля может снова перемешать состояния $|e\rangle$ и $|g\rangle$ во вспомогательном резонаторе R_2. Наконец, атомы достигают двух селективных по состояниям ионизационно-полевых детекторов D_e и D_g, с помощью которых подсчитывается число атомов в состояниях $|e\rangle$ и $|g\rangle$ с 40%-ой эффективностью.

Вся последовательность экспериментальных действий состоит в посылке одного или двух атомов, разделенных точно определенным интервалом, через систему и детектирование их в D_e и D_g. Эта последовательность повторяется много раз с периодом 1.5 мс, который намного превышает время затухания резонатора, так что при запуске каждой последовательности поле в C находится в одном и том же начальном состоянии. Результаты многократных испытаний подвергаются статистической обработке. Распределения совместных двухатомных вероятностей, как правило, составляются из 15000 испытаний, записываемых приблизительно в течение двух часов. Было выполнено два типа экспериментов. В первом, рассмотренном в разделе 5.2.3, атомы и резонаторная мода находятся точно в резонансе, что приводит, посредством обмена энергии, к перепутыванию энергети-

ческих состояний поля и атомов. Во втором, рассмотренном в разделе 5.2.4, атомы и поле не находятся в резонансе и поэтому взаимодействие приводит к сдвигу энергетических уровней атомов и резонатора, т.е. перепутыванию соответствующих фаз.

5.2.3 *Резонансная связь: осцилляции Раби и перепутанные атомы*

Рассмотрим случай, когда резонатор настроен в резонанс с атомным переходом $|e\rangle \rightarrow |g\rangle$. В непрерывном потоке атомов, отдельный атом может излучать или поглощать единичные фотоны в C [161-169]; такое же совокупное излучение происходит при работе микромазера [170]. Это взаимодействие в системе на уровне единичных атомов и фотонов было использовано при демонстрации квантовых осцилляций Раби [171], перепутывания между двумя атомами [168] и детектирования отдельных фотонов без поглощения [169].

Простейший эксперимент выполняется при помещении атома, находящегося на уровне $|e\rangle$, в резонатор и измерении вероятности того, что состояние атома изменится с $|e\rangle$ на $|g\rangle$ (зоны R_1 и R_2 не используются) [165]. Измерение повторяется для различных времен взаимодействия t между атомом и резонатором, которое варьируется в течение пролетного времени либо изменением скорости атомов, либо штарковской настройкой частоты атомного перехода в резонанс с модой поля за часть пролетного времени.

На Рис. 5.2(A) показан сигнал осцилляций Раби, как функция эффективного времени взаимодействия t в случае, когда резонаторное поле изначально находилось в вакуумном состоянии. Экспериментальные данные изображены точками, сплошная линия – теоретический расчет. Эффективное время взаимодействия t, рассчитанное исходя из параметров эксперимента, учитывает гауссово изменение связи внутри резонатора. Наблюдаются четыре полные осцилляции Раби с частотой близкой к $\Omega/2\pi = 50$ кГц. Они соответствуют основному процессу модели Джейнса-Каммингса: обратимая эволюция атома между $|e\rangle$ и $|g\rangle$, сопровождаемая испусканием и поглощением одного фотона. Затухание осцилляций вызвано несовершенством эксперимента. Во временной шкале этот сигнал вакуумных осцилляций Раби является двойником вакуумного расщепления Раби, наблюдаемого в спектре системы атом – пустой резонатор [172, 173].

На Рис. 5.2(B-D) изображен сигнал осцилляций, когда первоначально в резонаторе имеется когерентное поле со средним числом фотонов равным, соответственно на каждом из рисунков, $n = 0.40(\pm 0.02)$, $0.85(\pm 0.04)$ и $1.77(\pm 0.15)$. Осцилляции содержат несколько частотных компонент, отвечающих различным числам фотонов в поле. Биения

между ними вызывают исчезновение и появление осцилляций [171]. Фурье – образы сигналов Раби, показанные на Рис.5.2(a – d), содержат пики на частотах $\Omega\sqrt{n+1}$, соответствующих частоте Раби в n-фотонном поле ($n = 0 \div 3$). Частота Раби, пропорциональная амплитуде классического поля, является, таким образом, дискретной величиной. Этот факт служит *прямым доказательством квантования поля.* На Рис. 5.2($\alpha - \delta$) показаны Фурье компоненты амплитуд, которые непосредственно дают распределения чисел фотонов. Небольшой пик при $\Omega\sqrt{2}$ на Рис.5.2(a) возникает благодаря остаточному тепловому полю, которое имеет среднее число фотонов 0.06 при температуре 0.8K.

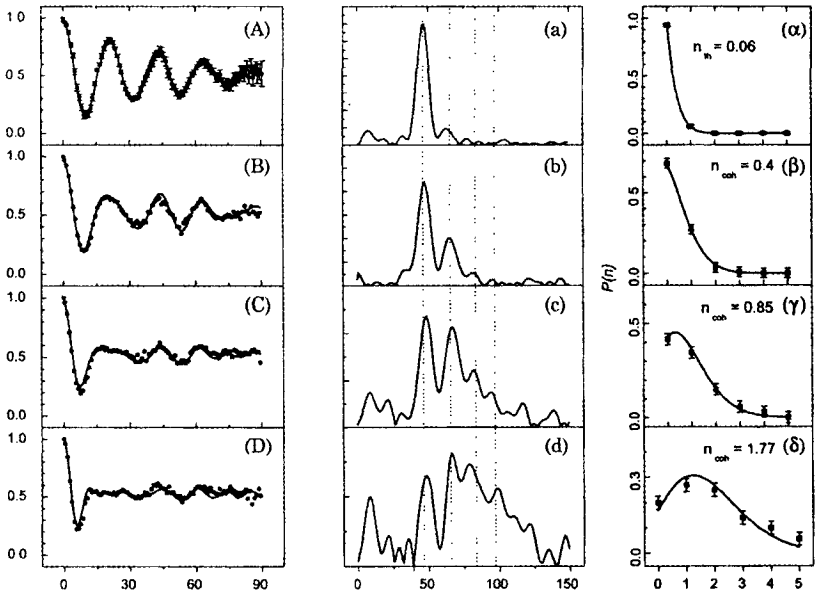


Рис. 5.2. Квантовые осцилляции Раби. (*A*), (*B*), (*C*) и (*D*): нутация сигнала Раби. (*A*): поле отсутствует и среднее число тепловых фотонов 0.06 (±0.01); (*B*), (*C*) и (*D*): когерентное поле со средним числом фотонов 0.40 (±0.02), 0.85 (±0.04) и 1.77 (±0.15). Точки – экспериментальные данные; сплошные линии– теория. (*a*), (*b*), (*c*), (*d*): соответствующие Фурье-образы. Частоты, пропорциональные квадратным корням из последовательных целых чисел, показаны вертикальными линиями. (α), (β), (γ), (δ) : распределения чисел фотонов, построенные на основе экспериментальных данных (точки). Сплошные линии: теоретические тепловое (α) или когерентное ((β), (γ), (δ)) распределения.

Кроме доказательства квантования энергии поля этот эксперимент демонстрирует, что резонансное взаимодействие атома с модой поля доминирует над процессами релаксации. Результирующее перепуты-

вание атом-поле может быть использовано для создания или манипулирования квантовым перепутыванием, обеспечивая, таким образом, основу для элементарных квантовых вычислительных операций.

Перепутывание между атомом и полем впервые использовалось при построении очень простого устройства: квантовая память, на основе одиночного кубита в резонаторе. Такая память реализуется записью первым атомом и чтением вторым. В простейшей ситуации первый атом попадает в пустой резонатор в состоянии $|e\rangle$. Эффективное время взаимодействия t таково, что $\Omega t = \pi$. Поэтому, атом покидает C в состоянии $|g\rangle$, оставляя однофотонное состояние в C. После задержки T второй атом, входящий в резонатор в состоянии $|g\rangle$, поглощает этот фотон, и при обеспечении отсутствия спонтанного распада, покидает резонатор в состоянии $|e\rangle$. Уменьшение вероятности найти второй атом в $|g\rangle$ при увеличении задержки T позволяет измерить время жизни единичного фотона в резонаторе. Неудивительно, что это время совпадает с классическим временем затухания энергии T_r [167].

Можно направить в пустой резонатор атом, приготовленный в суперпозиции состояний $|e\rangle$ и $|g\rangle$ с одинаковыми весами, путем приложения микроволнового импульса $\pi/2$ в зоне R_1 (с частотой ν). Компонента $|e\rangle$ атомного состояния испускает с единичной вероятностью фотон в зоне C, в то время как $|g\rangle$–компонента остается неизменной. Суперпозиционное состояние атома переходит, таким образом, в состояние суперпозиции поля, т.е. смесь 0- и 1-фотонных состояний; атом покидает C в состоянии $|g\rangle$. Среднее число фотонов в моде поля резонатора C равно 1/2, фаза поля задана и определяется микроволновым полем в R_1. Информация о фазе переносится атомом из R_1 в C.

Поле считывается вторым атомом, приготовленным в состоянии $|g\rangle$ после задержки T; атом вновь подвергается воздействию π-импульса в C. Квантовая когерентность при этом переносится на второй атом, оставляя резонатор пустым, в виде суперпозиции состояний $|e\rangle$ и $|g\rangle$. В зоне R_2 к атому прикладывается $\pi/2$-импульс микроволнового поля с той же фазой и частотой ν, которые воздействовали на первый атом в зоне R_1. Резонатор R_2, вместе с последующими за ним D_e и D_g, является, таким образом, детектором суперпозиции состояний, считывающим и информацию о фазе. Вероятность регистрации атома в $|e\rangle$ или $|g\rangle$ осциллирует с частотой ν, как при обычной интерференции Рамзея. В отличие от этого случая, два импульса воздействуют на разные атомы и когерентность перераспределяется между ними через резонаторное поле в C. Рисунки 5.3(a-c) демонстрируют интерференционные сигналы, показывающие перераспределение когерентности для трех различных временных интервалов между двумя атомами. При увеличении этого интервала период и амплитуда модуляции

уменьшаются. Уменьшение контраста модуляции отражает затухание поля в C. Время затухания в два раза превышает T_r, т.к. в этом эксперименте проявляется суперпозиция фоковских состояний с определенным числом фотонов $|1\rangle$ и $|0\rangle$; второе состояние затуханию не подвержено.

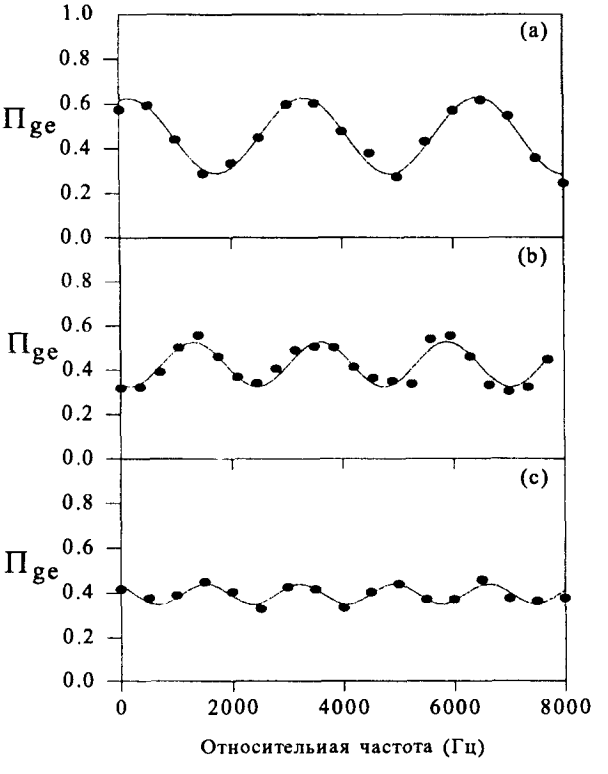


Рис. 5.3. Перераспределение когерентности меду двумя атомами: условная вероятность $\Pi_{ge}(\nu)$ детектирования второго атома в состоянии $|e\rangle$ при условии, что первый атом был зарегистрирован в состоянии $|g\rangle$, как функция частоты ν микроволнового импульса, приложенного к первому атому в зоне R_1 и ко второму в R_2. Задержки между двумя микроволновыми импульсами в R_1 и R_2 равны 301, 436, и 581 мкс, соответственно, от (*a*) до (*c*).

В этом эксперименте кубит распределяется между двумя атомами посредством однофотонного поля. В промежуточном состоянии резонаторное поле является существенно неклассической суперпозицией вакуумного и однофотонного состояний. Такой процесс, в котором проявляется совместное состояние поля и атома, является ключевым в реализации квантовых логических элементов КЭР [174].

Аналогичная схема, при незначительной модификации, может быть использована для приготовления и манипулирования нелокального пе-

репутывания типа атом – поле или атом – атом [175]. Первый атом, находящийся в состоянии $|e\rangle$, подвергается воздействию $\pi/2$-импульса ($\Omega t = \pi/2$) и направляется в пустой резонатор. Перепутывание атом – атом может быть достигнуто при прохождении второго атома, приготовленного в состоянии $|g\rangle$, через резонатор C, с характерным временем взаимодействия, соответствующим $\Omega t = \pi$. Фотон, испущенный первым атомом, поглощается вторым с единичной вероятностью; таким образом, резонатор оказывается пустым, а атом – в перепутанном состоянии:

$$|\Psi_{EPR}\rangle = \frac{1}{\sqrt{2}}\left(|e_1, g_2\rangle - |g_1, e_2\rangle\right), \tag{5.2}$$

где индексы относятся, соответственно, к первому и второму атому.

Уравнение (5.2) описывает ЭПР(Эйнштейн-Подольский-Розен)-пару перепутанных частиц [21]. Атомы могут быть представлены в виде частиц со спином 1/2 и состояниями $|e\rangle$ и $|g\rangle$, соответствующими +1/2 и – 1/2 состояниям, квантованными вдоль направления Oz. $|\Psi_{EPR}\rangle$ представляет собой состояние с нулевым спином и является инвариантом относительно вращений; это означает, что два спина должны быть антикоррелированы, т.е они всегда детектируются с противоположными значениями, относительно произвольного направления оси квантования. Чтобы проиллюстрировать этот факт, выберем ось в плоскости xOy в направлении под углом ϕ с осью Ox. Собственные векторы спина вдоль этой оси имеют вид $|e\rangle \pm e^{i\phi}|g\rangle$ и состояние $|\Psi_{EPR}\rangle$ может быть записано в форме (с обобщенной фазой), отражающей свойство антикорреляции:

$$\begin{aligned}|\Psi_{EPR}\rangle = &\left(|e_1\rangle + e^{i\phi}|g_1\rangle\right)\left(|e_2\rangle - e^{i\phi}|g_2\rangle\right)\\ &-\left(|e_1\rangle - e^{i\phi}|g_1\rangle\right)\left(|e_2\rangle + e^{i\phi}|g_2\rangle\right).\end{aligned} \tag{5.3}$$

Для того, чтобы проанализировать перепутывание в энергетическом базисе (вдоль оси Oz), определим состояние атомов после того, как они вышли из резонатора C. В идеальном случае совместная вероятность зарегистрировать атомы в различной комбинации $|e\rangle$ и $|g\rangle$ должна быть $P_{eg} = P_{ge} = 1/2$, $P_{ee} = P_{gg} = 1/2$. Вместо этого мы обнаруживаем, что $P_{eg} = 0.44$, $P_{ge} = 0.27$, $P_{ee} = 0.06$, $P_{gg} = 0.23$. Отличие возникает благодаря распаду фотонов, находящихся в C, за время между появлением двух атомов, а также из-за несовершенства эксперимента. Количественный анализ данных показывает, что ЭПР-пары возникают с 63%-ой вероятностью [168].

Антикорреляционные свойства, которые следуют из (5.3), анализируются при воздействии на оба атома $\pi/2$-импульсом зоне R_2. Переворот спина в R_2 при регистрации вдоль оси Oz, эквивалентен пере-

вороту при регистрации вдоль горизонтальной оси. Более того, регистрация в базисе $|e\rangle$ или $|g\rangle$ после R_2 соответствует атомной суперпозиции $|e\rangle \pm e^{i\phi}|g\rangle$ до R_2, где ϕ – это фаза импульса, приложенного в зоне R_2 (знак + выбирается для состояния $|e\rangle$). Антикорреляция приводит к тому, что состояние второго атома при этом измерении должно быть спроицировано на суперпозицию, в которой «направление спина» противоположно «направлению спина» первого атома. Если бы оба атома пересекли R_2 одновременно, то должна была бы наблюдаться полная антикорреляция между показаниями детекторов $|e\rangle$ и $|g\rangle$. На самом деле когерентность между вторым атомом, задержанным на время T, и полем в R_2, прецессирует в течение T. Конечная вероятность регистрации второго атома в $|e\rangle$ или $|g\rangle$ зависит от фазы, набежавшей между состояниями атома и микроволнового поля в R_2. Этот набег фазы пропорционален разности между пролетным временем T и рамзеевским частотным сдвигом «атом-поле». Здесь опять возникает аналогия с интерференцией Рамзея. Однако, здесь два микроволновых импульса прикладываются к разным атомам, а фаза перераспределяется между ними посредством нелокальных квантовых корреляций.

На Рис. 5.4 показаны условные вероятности $\Pi_{e1,e2}(\Pi_{g1,e2})$ детектирования второго атома в состоянии $|e\rangle$, если первый находится в состоянии $|e\rangle$ ($|g\rangle$), как функции частоты ν в зонах Рамзея. Модуляция свидетельствует о когерентности состояния второго атома. Вероятности, показанные на рисунке, находятся в противофазе, т.к. фаза второго атома изменяется на π, если первый атом зарегистрирован в состоянии $|g\rangle$, вместо $|e\rangle$.

Экспериментальные данные демонстрируют факт приготовления управляемого перепутывания между двумя кубитами (здесь два атома разнесены на расстояние порядка 1.5 см). При объединении резонансных и дисперсионных взаимодействий, эта схема может быть распространена для приготовления триплетов атомов ввиде $|e,e,e\rangle - |g,g,g\rangle$ [175-177].

Резонансное взаимодействие между атомом и полем может быть так же использовано при беспоглощательном детектировании фотона, находящегося в резонаторе [169]. Сущность этого метода состоит в том, что атом, находящийся на уровне $|g\rangle$ и пересекающий резонатор, приобретает условный фазовый сдвиг и испытывает 2π-переколебание Раби в однофотонном поле. Когда атом пролетает через пустой резонатор (начальное состояние $|g, 0\rangle$), он не подвержен взаимодействию. Если же в резонаторе находится один фотон, то система атом-поле испытывает преобразование $|g, 1\rangle \rightarrow -|g, 1\rangle$ Фазовый сдвиг общей волновой функции на π аналогичен повороту на 2π в реальном про-

странстве частицы со спином 1/2. Такой условный фазовый сдвиг может быть выявлен интерферометрией Рамзея при переходе, не связанным с резонаторным полем – с уровня g на опорный уровень i. Наблюдение фазового сдвига равнозначно детектированию фотона в резонаторе. В отличие от большинства фотодетекторов, фотон покидает резонатор после взаимодействия со «считывающим» атомом. Этот эксперимент, таким образом, эквивалентен квантовому неразрушающему измерению однофотонного поля, локализованного в подпространстве, состоящего из смеси вакуума и однофотонных состояний. Кроме того, условная динамика, лежащая в основе этого метода, может рассматриваться как предпосылка к созданию квантового логического элемента.

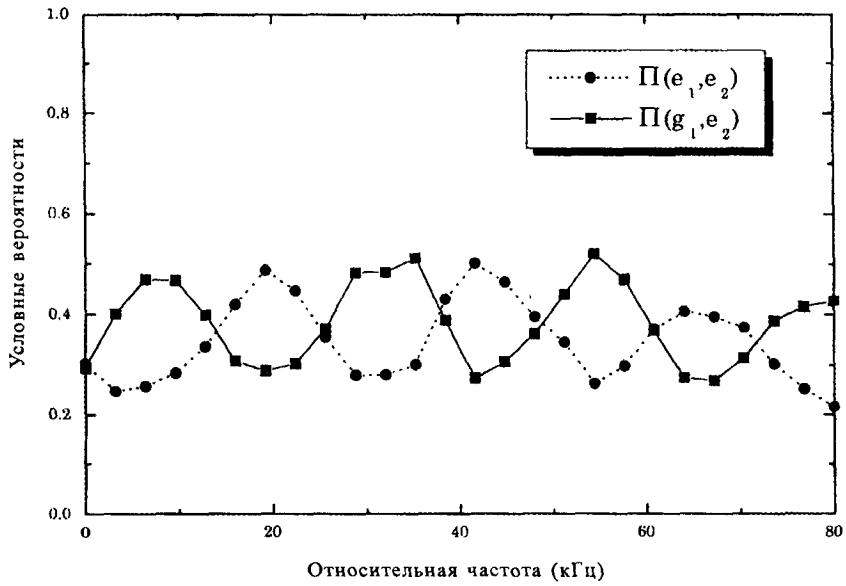


Рис. 5.4. Атомное ЭПР-перепутывание: условные вероятности $\Pi(e_1,e_2)$ (кружочки) и $\Pi(g_1,e_2)$ (квадратики) измерить второй атом в состоянии $|e\rangle$, если первый был зарегистрирован в $|e\rangle$ или $|g\rangle$, соответственно. Вероятности показаны как функции частоты ν импульсов, приложенных в R_2. Линии, соединяющие экспериментальные точки, нанесены для удобства визуального восприятия.

5.2.4 *Дисперсионная связь: шредингеровская кошка и декогерентность*

Рассмотрим теперь случай, при котором частота атомного перехода ω_0 и частота моды поля ω отличаются на величину δ, причем расстройка δ велика, по сравнению с Ω и шириной линии резонатора. При этих условиях, в силу закона сохранения энергии, процессы поглоще-

ния и излучения фотонов атомами запрещены и взаимодействие с резонатором является чисто дисперсионным. Энергетическое перепутывание атома и поля, рассмотренное в предыдущем разделе, заменяется на перепутывание атомного состояния с фазой поля излучения, которое может рассматриваться классически. Таким образом, микроскопическая степень свободы управляет «макроскопической» величиной. Это перепутывание служит прототипом квантового измерения и позволяет исследовать таинственный мир квантовой механики с необычной точки зрения.

Пусть циркулярный ридберговский атом взаимодействует со слабым когерентным полем в C; амплитуду резонаторного поля обозначим через α; среднее число фотонов $|\alpha|^2$ обычно распределено в интервале от 0 до 10. Так как вакуумная частота Раби представляется гауссовой функцией от положения атома внутри резонатора, то возмущение включается и выключается адиабатически. Следовательно обмен фотоном между атомом и резонаторным полем маловероятен даже при небольших расстройках ($\delta/2\pi = 100 \div 700$ кГц). Поэтому взаимодействие проявляется только в сдвиге частоты уровня. Резонаторная мода сдвигается на величину $\pm\Omega^2/4\delta$ для атома, находящегося в центре резонатора. Этот сдвиг, вызываемый эффектом «показателя преломления» единичного атома, имеет противоположные величины для атома в состояниях $|e\rangle$ и $|g\rangle$ [161]. Величина сдвига достигает значения ± 6 кГц при $\delta/2\pi$ = 100 кГц, отвечающему удельному (на один атом) показателю преломления на 15 порядков превышающему значение, характерное для «обычных атомов».

Частотный сдвиг, возникающий при прохождении единичного атома через резонатор, проявляется в сдвиге фазы когерентного резонаторного поля на $\pm\,\Phi = \pm\,\Omega^2 t/4\delta$, где t – эффективное время взаимодействия. Фазовый сдвиг обычно оказывается порядка одного радиана. Такое взаимодействие между атомом и полем может быть использовано для генерации неклассической суперпозиции состояний поля с различными фазами. Атом приготавливается в суперпозиции состояний $|e\rangle$ и $|g\rangle$ путем подачи импульса $\pi/2$ в зоне R_1. При пересечении атомом резонатора, полю одновременно придаются два противоположных фазовых сдвига $\pm\,\Phi$. Состояние комбинированной системы атом – поле, таким образом, принимает вид

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(\left|e,\alpha e^{i\Phi}\right\rangle + \left|g,\alpha e^{-i\Phi}\right\rangle\right). \tag{5.4}$$

Это состояние является перепутанным – энергия атома коррелирована с фазой резонаторного поля. Когерентное поле может быть представлено как вектор в фазовом пространстве, длина и направление которого связаны с амплитудой и фазой, как показано на Рис. 5.5(а).

Конец вектора лежит в круге единичного радиуса, описывающего квантовую неопределенность состояния поля. Из уравнения (5.4) видно, что этот вектор ведет себя как «стрелка прибора», принимающая два разных направления, отвечающих за состояния атома, как показано на Рис. 5.5(b). Взаимодействие осуществляет «измерение», в котором «вектор поля» используется для определения энергии атома. Здесь уместно напомнить метафору Шредингера [178]: компоненты поля $+\Phi$ и $-\Phi$ аналогичны состояниям знаменитой «живой» и «мертвой» кошки, перепутанными с атомом, находящимся в суперпозиции возбужденного и основного состояний.

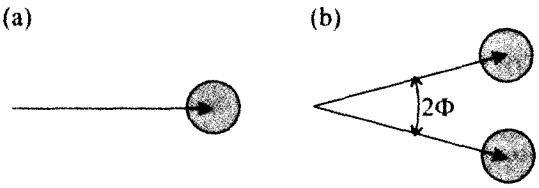


Рис. 5.5. (a): Наглядное представление в фазовом пространстве когерентного состояния поля. (b) Компоненты поля в (5.4), коррелированные с атомными состояниями $|e\rangle$ и $|g\rangle$.

После выхода из резонатора, но до детектирования, атом подвергается воздействию другого $\pi/2$-импульса в зоне R_2, когерентному с импульсом в зоне R_1. Вероятность детектирования P_g атома в состоянии $|g\rangle$ измеряется, как функция частоты ν поля, приложенного в R_1 и R_2. На Рис. 5.6(a) показан экспериментальный результат для случая, когда в резонаторе не было фотонов и при расстройке $\delta/2\pi$ = 712 кГц. Состояние атома может быть преобразовано из $|e\rangle$ в $|g\rangle$ либо в зоне R_1 (прохождение через C в состоянии $|g\rangle$), либо в R_2 (прохождение через C в состоянии $|e\rangle$).Так как атом не оставляет никаких следов своего присутствия внутри резонатора, эти два способа не могут быть идентифицированы и соответствующие амплитуды интерферируют, что и приводит к осцилляциям (интерференция Рамзея) в P_g.

На Рис. 5.6(b – d) показаны экспериментальные результаты для когерентного резонаторного поля со средним числом фотонов 9.5 и уменьшающихся расстроек. Чем меньше расстройка, тем больше разделение компонент поля в C. Врезки на Рис.5.6(b – d) иллюстрируют фазовую информацию о поле, которая записана в атомном состоянии. Такая «каким-путем» (which-way) информация, даже не будучи прочитанной, должна разрушать эффект интерференции, в соответствии с принципом дополнительности. Количественный анализ показывает, что интерференционный сигнал определяется интегралом перекрытия между двумя компонентами поля; его модуль отвечает за контраст

интерференции, а фаза – за рамзеевскую модуляцию. Для больших Φ перекрытие мало и модуляция исчезает. Результаты убедительно показывают, что резонатор действует как счетчик атомного состояния. Кроме того, фазовый сдвиг в модуляции при больших расстройках, обеспечивает точную информацию о числе фотонов.

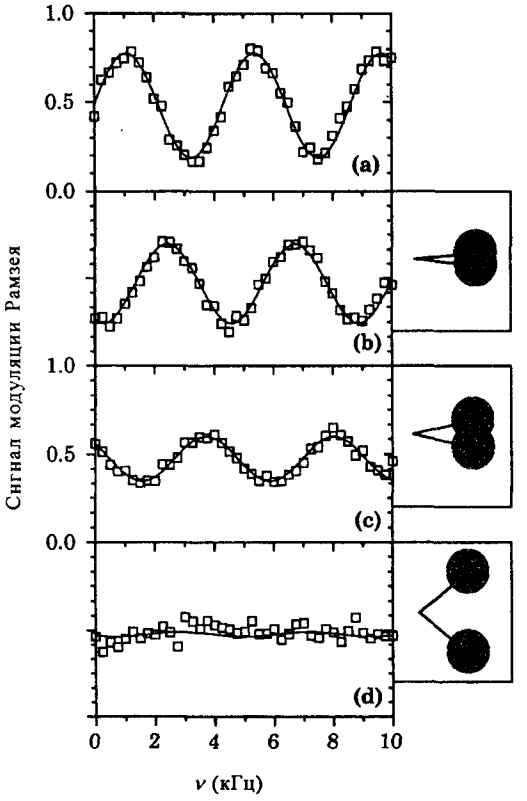


Рис. 5.6. Рамзеевская модуляция в вероятности регистрации атома на уровне $|g\rangle$ как функции ν : (*a*) резонатор C – пустой, $\delta/2\pi = 712$ кГц; от (b) до (d) в C имеется когерентное поле с $|\alpha| = \sqrt{9.5} = 3.1$, $\delta/2\pi = 712$, 347 и 104 кГц, соответственно. Точками отмечены экспериментальные данные, сплошные кривые – синусоидальная аппроксимация. На врезках показаны представления компонент поля, выходящих из C, в фазовом пространстве.

Квантовая суперпозиция мезоскопического поля, возникающая в процессе такого приготовления и детектирования атома, проходящего через резонатор, весьма чувствительна к внешним воздействиям и подвержена декогерентности; особенно когда $|\alpha|^2$ и/или Φ становятся большими [179-186]. Чтобы проследить за эволюцией от квантовой суперпозиции к классической смеси, «состояние кошки» для поля апробируется на втором атоме, проходящем через резонатор после за-

держки T [166, 188]. Пробный атом испытывает такой же фазовый сдвиг, как и первый. Каждая из двух компонент поля, вызванная первым атомом, расщепляется на две части. Это означает, что конечное состояние поля содержит четыре компоненты, две из которых совпадают при нулевой фазе. В каких бы комбинациях состояний два атома не пересекли C – либо в ($|e\rangle$, $|g\rangle$), либо в ($|g\rangle$, $|e\rangle$) фаза возвращается к исходному значению. После перемешивания атомных состояний в зоне R_2 информация о начальной комбинации исчезает ($|e\rangle$, $|g\rangle$ или $|g\rangle$, $|e\rangle$), поскольку второй атом частично «стер» [187] информацию о поле, оставшуюся от первого атома. Вклады этих двух комбинаций, таким образом, приводят через совместные вероятности P_{ee}, P_{eg}, P_{ge}, P_{gg} и корреляционные сигналы $\eta = P_{ee}/(P_{ee} + P_{eg}) - P_{ge}/(P_{ge} + P_{gg})$ к наличию интерференционных членов.

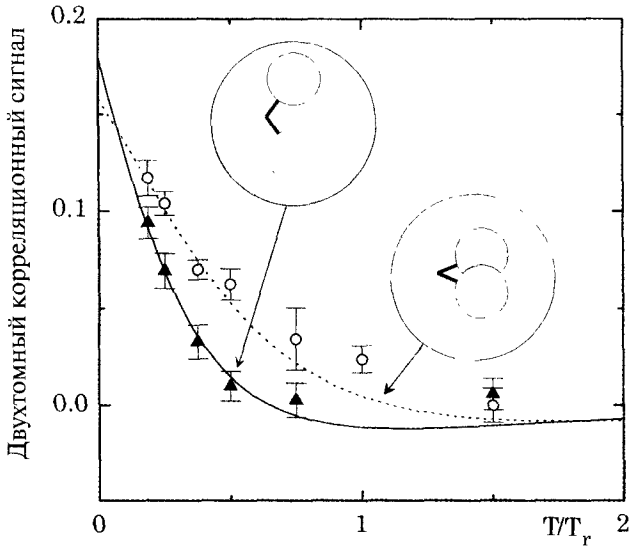


Рис. 5.7. Декогерентность шредингеровской кошки: сигнал двух-атомной корреляции как функция T/T_r для $\delta/2\pi$ = 170 кГц (кружки) и $\delta/2\pi$ = 70 кГц (треугольники). Пунктир и сплошная линия – теория. Врезки: наглядное представление, соответствующее компонентам поля, разделенным на 2Φ.

Если состояние суперпозиции выживает за время T, то η, в идеальном случае, принимает значение 1/2; если же состояние поля становится простой смесью, η оказывается равной нулю. Экспериментальные значения η, как функции T, показаны на Рис. 5.7 для двух различных состояний типа «кошки» (обозначенных на врезках). Точки представляют эксперимент, сплошная линия – теорию [188]. Максимальное значение 0.18 ограничено только невысоким контрастом использованного интерферометра Рамзея. Декогерентность возникает на временах, гораздо более коротких, чем время затухания резонатора, и

более заметна, когда расстояние между компонентами «кошки» увеличивается. Видно, что наблюдается нетривиальный механизм релаксации, постоянная времени которой очень сильно зависит от начального состояния.

Декогерентность вызвана потерей фотонов в резонаторе. Каждый потерянный фотон может быть описан как маленький «шредингеровский котенок», копирующий в окружающее пространство (термостат) информацию о фазе, запасенную в C. Простой факт того, что такая «утечка» информации могла бы быть прочитана, уничтожает интерференционные эффекты, вызванные квантовой когерентностью «кошки». В этом смысле, декогерентность является дополнительным явлением. Малое время декогерентности состояния шредингеровской кошки, рассмотренное выше, оказывается порядка T_{cav}/n, что объяснимо при таком подходе. Чем больше число фотонов, тем короче время, требуемое для утечки единичной «фотонной копии» в термостат. В этом эксперименте проверяются основные особенности декогерентности и ясно видна нестойкость квантовой когерентности в больших системах. Экстраполяция квантово-механической суперпозиции состояний к макроскопическому масштабу приводит к почти мгновенной декогерентности, что подтверждает копенгагенскую интерпретацию квантовых измерений для любых практических целей. Этот эксперимент также помогает понять и те трудности, которые возникают при создании и управлении крупномасштабным квантовым перепутыванием, а именно, что квантовая декогерентность является основной лимитирующей преградой при реализации процессов крупномасштабной обработки квантовой информации. Дальнейшая дискуссия об ограничениях, возникающих при квантовых вычислениях без рассмотрения схем квантовой коррекции ошибок, будет продолжена в разделе 7.3.

5.2.5 Эксперименты с ионами в ловушках

Один или несколько ионов, находящихся в радиочастотной ловушке Пауля, являются идеальным объектами для изучения динамики простых квантовых систем, и с помощью лазерных импульсов экспериментатор может осуществлять взаимодействие таких простых систем в большей степени по своему выбору. Особенно интересный случай состоит в представлении поля фотонов в КЭР, о чем говорилось в предыдущих разделах, моделью гармонического осциллятора, которая описывает движение иона (ионов) во внешнем потенциале ловушки. Подходящее световое поле может связывать внутренние электронные уровни иона $|g\rangle$ и $|e\rangle$ с внешним колебательным движением с час-

тотой ω. При этом гамильтониан взаимодействия имеет вид [189-192]:

$$H_{\text{int}} = -\hbar G(\sigma^{+} e^{i\eta(a^{+}+a)-i\delta t} + \sigma^{-} e^{-i\eta(a^{+}+a)+i\delta t}), \qquad (5.5)$$

где $\eta = \delta k\sqrt{\hbar/(2m\omega)}$ – параметр Лэмба-Дике с модулем δk волнового вектора (или разницей волновых векторов если система связана посредством рамановских переходов), $(a^{+} + a)$ – оператор координаты в терминах понижающих операторов гармонического осциллятора и G – константа связи, пропорциональная амплитуде связывающего светового поля. Такой гамильтониан взаимодействия является более общим, чем гамильтониан в модели Джейнса – Каммингса (5.1), но сводится к последнему выбором расстройки частоты светового поля и разности энергий двух внутренних состояний: с $\delta = -\omega$ и в пределе $\eta\sqrt{\langle(a^{+}+a)^2\rangle} << 1$. В общем, любая расстройка $\eta = (n' - n)\omega$, (n', n – целые числа) будет резонансно вызывать переходы между состояниями $|g,n\rangle$ и $|e,n'\rangle$ и, таким образом, осуществляется переход к другому эффективному гамильтониану взаимодействия. Вдобавок, константа связи G не задается матричными элементами дипольного момента и объемной модой резонатора, как в случае экспериментов, о которых шла речь в предыдущих разделах. Она может меняться при соответствующем выборе интенсивности света.

Способы лабораторной реализации этих идей возникли при попытках построения стандартов частоты на ионах в ловушках и охлажденных атомах [193-195]. Динамическое захватывание заряженных частиц в радиочастотных (ВЧ) ловушках было впервые предложено и экспериментально реализовано В.Паулем в 1958 году [196]. ВЧ электрическое поле, генерируемое электродами с подходящей конфигурацией, создает псевдо-потенциал, ограничивающий движение заряженной частицы [197]. Для удержания единичного иона электроды должны иметь характерные размеры от нескольких миллиметров до сотни микрон. Частоты ВЧ-полей лежат в диапазоне 10 – 300 МГц, а амплитуды составляют сотни вольт. Движение частицы, ограниченное таким полем, имеет в динамическом псевдо-потенциале быструю компоненту, синхронную с частотой приложенного возбуждающего поля (микродвижение), и медленную (секулярную). Для квадрупольной геометрии ВЧ-поля псевдо-потенциал является гармоническим и квантованное секулярное движение захваченных ионов с хорошей точностью описывается моделью квантового гармонического осциллятора. Более детальное описание различных типов ловушек Пауля и их специфических свойств будет рассмотрено в разделе 5.3.2.

Для стандартов частоты ионы в ловушках должны содержать по крайней мере один долгоживущий узкий уровень, который может лежать либо в микроволновом (например, основное состояние перехода

в сверхтонкой структуре) либо в оптическом диапазоне (например, переходы в метастабильное возбужденное состояние). Для уменьшения доплеровских сдвигов и других нежелательных эффектов, связанных с движением, используется лазерное охлаждение, являющееся очень удобным инструментом. Механизм такого охлаждения был предложен Винлэндом и Дэмелтом [198], а экспериментально эффект наблюдался в 1978 году [199]. Требования к условиям экспериментов с фундаментальными квантовыми системами и использованием квантовой логики почти идентичны. В настоящее время узкая линия перехода получается в хорошо изолированной двухуровневой системе, в то время как лазерное охлаждение служит ключевым инструментом по инициализации движения гармонического осциллятора в четко определенном состоянии.

5.2.6 Выбор ионов и доплеровское охлаждение

Хотя ионная ловушка является очень глубокой (высота стенки потенциала несколько эВ) и удерживает почти все ионы, только некоторые из ионов подходят для резонаторных КЭР-подобных экспериментов. Эти ионы должны иметь структуру энергетических уровней, пригодную для построения двухуровневой системы с пренебрежимо малой декогерентностью, вызванной спонтанным распадом; они также должны быть пригодными для оптического охлаждения и детектирования. Такие ионы должны иметь один электрон на внешней оболочке (водородоподобные ионы) и, соответственно, простую структуру электронных уровней. Двухуровневая система должна либо иметь два сверхузких основных состояния, либо долгоживущее метастабильное электронное состояния [200]. Большинство подобных экспериментов было выполнено с $^{9}Be^{+}$ в Национальном Институте Стандартов и Технологий (Боулдер (NIST)) в группе ионного удержания [201]; другие группы также ускоряют работы по квантовой логике и когерентному управлению, например, в Альмадене – IBM ($^{138}Ba^{+}$), в Лос-Анжелесе – JPL [202] ($^{199}Hg^{+}$), в Гарчинге – MPQ [203] ($^{25}Mg^{+}$), в Лос-Аламосской Национальной Лаборатории [204] и в университете Майнца [205] ($^{40}Ca^{+}$), в Гамбурге [206] ($^{138}Ba^{+}$, $^{171}Yb^{+}$) и Инсбруке [207] ($^{40}Ca^{+}$, $^{138}Ba^{+}$). Последующее обсуждение будет касаться $^{9}Be^{+}$, сверхтонкие основные состояния которого образуют двухуровневую систему и $^{40}Ca^{+}$, где используется оптически возбуждаемый метастабильный уровень. Схемы уровней $^{40}Ca^{+}$ и $^{9}Be^{+}$ показаны на Рис.5.8.

Охлаждение необходимо, чтобы реализовать четко определенное начальное колебательное состояние удерживаемых ионов. Наиболее очевидный выбор представляют основные состояния [208], однако

были предложены и ловушечные состояния [209]. Наибольшая часть кинетической энергии удаляется уже при доплеровском охлаждении. Метод основан на том факте, что атомы, двигающиеся навстречу лазерному источнику, могут возбуждаться, если частота лазера слегка отстроена в красную область (доплеровский сдвиг) по сравнению с частотой перехода. Движение атомов будет замедляться благодаря рассеянию фотонов. Передаваемый из-за поглощения импульс постоянно суммируется, в то время как для спонтанного излучения усредненный уносимый импульс стремится к нулю, из-за равномерной диаграммы направленности в телесном угле 4π стерадиан. Таким образом, энергия движения или, что эквивалентно, температура ионов уменьшается. Значение конечной энергии, достижимое при этой методике, определяется пределом доплеровского охлаждения $E_D = \hbar\Gamma/2$, где Γ обозначает естественную ширину возбужденного состояния охлаждаемого перехода. Такая же процедура применяется и к ионам в ловушкам, если колебательная частота (секулярная частота ω_i вдоль соответствующей оси) меньше, чем естественная ширина Γ. В этом случае требуемое движение по направлению к лазерному источнику обеспечивается периодическим колебанием ионов в ловушке, так как для свободных атомов конечная температура для такого процесса охлаждения равна $T_D = E_D / k_B$ [210] (обычно порядка нескольких мК).

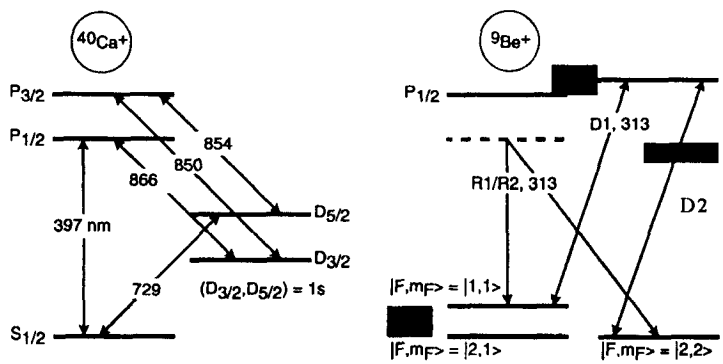


Рис. 5.8. Схема уровней $^{40}Ca^+$ и $^9Be^+$. Указаны длины волн различных переходов. Для $^{40}Ca^+$ также показаны времена жизни возбужденных состояний.

Для большинства ионов оптический переход, используемый при доплеровском охлаждении, лежит в УФ диапазоне. Для $^9Be^+$ используется переход между $^2S_{1/2}$ и $^2P_{3/2}$ с длиной волны 313 нм, тогда как для $^{40}Ca^+$ длина волны перехода составляет 397 нм. Соответственно, в обоих ионах Be^+ и Ca^+ ширина линии порядка 20 Мгц. Охлаждающий свет генерируется путем удвоения частоты титан-сапфирового лазе-

ра. В Ca^+ уровень $P_{1/2}$ может распадаться в метастабильное состояние $D_{3/2}$ и необходим дополнительный лазерный диод, излучающий на длине волны 866 нм, чтобы подкачивать ионы. В обоих случаях доплеровское охлаждение приводит к состоянию теплового движения с температурой порядка 1 *m*К, но значение числа колебательных квантов $\langle n_D \rangle$ гармонического осциллятора зависит от удерживающей способности ловушки. Для ловушки из Be^+, использованной в NISTe, $\omega/2\pi$ составляло 11.2 МГц, т.е. $\langle n_D \rangle \approx 1.3$ [211], в то время как для гораздо менее симметричной линейной ловушки с Ca^+ в Инсбруке, ($\omega/2\pi \approx 100$ – 180 кГц) $\langle n_D \rangle \approx 50$ [212]. Конструкция ловушек определяется, исходя из компромисса между расстоянием между ионами, которое желательно выбирать побольше, чтобы иметь доступ к каждому лазерным лучом, и типом охлаждающей схемы, которую предпочтительнее делать возможно проще. Ионная ловушка в Инсбруке дает возможность иметь расстояние между ионами порядка 15 мкм, а ловушка в NISTe – около 1 – 2 мкм.

Для единичного иона понятие температуры используется в эргодическом смысле, т.е. среднее по повторяющимся измерениям, в конечном счете, будет давать окончательную температуру. Для секулярных частот ω_i, больших чем Γ, лучше использовать спектральную структуру охлаждаемого перехода. Благодаря колебательному движению иона в ловушке спектр поглощения приобретает сателлиты ($\omega_0 \pm n\omega$), где ω_0 обозначает частоту перехода. Интенсивность таких сателлитов определяется колебательной энергией. Можно использовать эти сателлиты для получения оптического охлаждения ниже доплеровского предела. Этот метод будет изложен в следующем разделе.

5.2.7 Сателлитное охлаждение

В хорошем приближении ион в ловушке может рассматриваться как квантово-механический гармонический осциллятор. Как показано на Рис. 5.9, при движении вдоль одной оси внутренние состояния единичного двухуровневого атома имеют структуру уровней гармонического осциллятора, похожую на молекулярную структуру, где колебательные состояния определяются частотой ловушки вдоль этого направления. Эти уровни могут быть подходящим образом отнесены к внутренним степеням свободы $|e\rangle$, $|g\rangle$ (описывающими электронный переход) и внешними степенями свободы $|n\rangle$ (т.е. возбуждениями гармонического осциллятора). Спектральная структура цепочки ионов гораздо богаче, но методы, упомянутые в этом разделе, после соответствующих усовершенствований, по-прежнему пригодны и для работы с ней (см.разд.5.3.3).

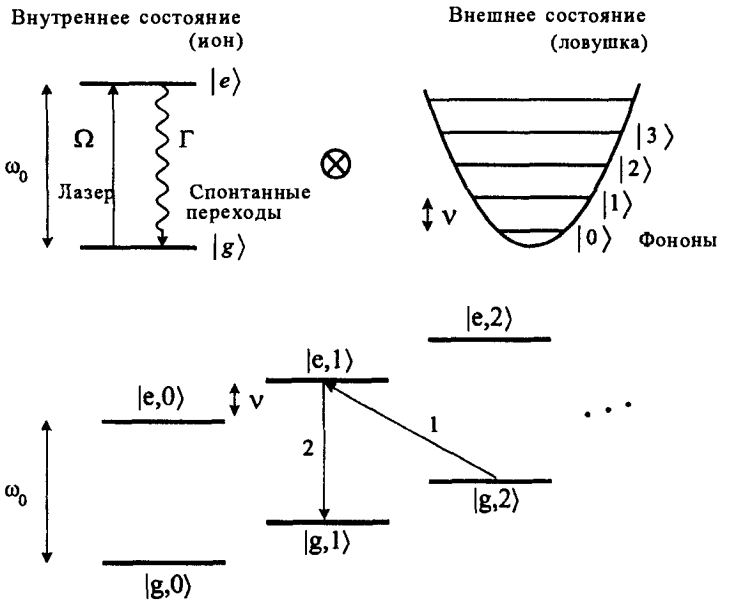


Рис.5.9. Схема уровней единичного двухуровневого иона, запертого в гармоническом потенциале. Сателлитное охлаждение достигается при поглощении фотона, вызывающего переход $|g,n\rangle \rightarrow |e,n-1\rangle$ обозначенный стрелкой 1, и последующим распадом (через спонтанное излучение или процесс с дополнительной оптической накачкой) в состояние $|g,n-1\rangle$ (стрелка 2).

Очень эффективное охлаждение получается при настройке частоты лазера так, что поглощение возникает на нижнем сателлите колебательного движения. Такое поглощение вызвано переходом $|g,n\rangle \rightarrow |e,n-1\rangle$ (стрелка 1 на рис.5.9). Последующее спонтанное испускание наиболее вероятно возникает на частоте перехода $|e,n-1\rangle \rightarrow |g,n-1\rangle$ (стрелка 2 на рис. 5.9) и, таким образом, среднее возбуждение механического колебания эффективно притушено колебательным квантом. Можно также активно подзаселить уровень $|g,n-1\rangle$ через быстрый распад с третьего уровня. Если фотон отдает энергию E_{rec} при распаде и эта энергия много меньше чем энергия осцилляторного кванта, то состояние изменяется только с вероятностью $E_{rec}/(\hbar\omega)$. В среднем отдача не передается движению иона, но переходит на ловушку как целое. Когда такие шаги повторяются в течение достаточного большого времени, ион, с высокой вероятностью, в конце концов, оказывается в основном состоянии; поскольку состояние $|g,0\rangle$ было достигнуто, оно перестает быть связанным с обоими лазерными полями (темное состояние).

В экспериментах, выполненными на рамановских переходах в Be^+, т.е. переходах вызываемых двумя лазерными пучками R1 и R2, обо-

значенными R1/R2 на Рис. 5.8, связываются два (сверхтонких основных) состояния с разностью частот $\omega_{HF}/(2\pi) \approx 1.25$ ГГц через виртуальный третий уровень. Рамановские пучки получаются при отстройке удвоенной частоты лазера на красителе от перехода $^2S_{1/2} - {}^2P_{3/2}$ (приблизительно 12 ГГц) и последующим расщеплением на две компоненты с разностью частот около 1.25 ГГц с помощью акустооптического модулятора (AOM). Таким образом, разность частот и относительная фаза двух компонент может управляться с ВЧ-точностью и при этом абсолютная стабильность лазера не должна быть слишком высока. В экспериментах, выполненных в NISTe, не предпринималось попыток сузить линию генерации лазера на красителе, которая составляла приблизительно 1 МГц. При сателлитном охлаждении разность частот подстраивается к величине $\omega_{HF} - \omega$ (красный сателлит). Цикл охлаждения затем продолжается по схеме, описанной выше, с дополнительной подкачкой, вызывающей возбуждение дипольного перехода с уровня $^2S_{1/2}$ на уровень $^2P_{3/2}$, который также используется при доплеровском охлаждении [211].

Для Ca^+ метастабильный уровень $D_{5/2}$, показанный на Рис. 5.8, с временем спонтанного перехода порядка одной секунды, может быть использован в методе сателлитного охлаждения вместе с основным состоянием. Как и в предыдущем случае, кванты движения удаляются при возбуждении переходов путем отстройки лазерной частоты ω в длинноволновую область от узкой резонансной линии. В противоположность рамановским переходам, лазер должен иметь высокую стабильность частоты для того, чтобы разрешить сателлиты движения, т.е. особое внимание следует уделять стабилизации. Установка, используемая в университете Инсбрука, состоит из титан-сапфирового лазера с длиной волны 729 нм, стабилизированного с помощью опорного резонатора, помещенного в вакуум и изолированного от температурных и вибрационных воздействий. Добротность резонатора составляет 250 000 и предварительные тесты показали, что ширина линии лазера оказывается уже чем 1 кГц. В принципе, возврат без отдачи в основное состояние мог бы служить подкачкой, но время жизни метастабильного состояния 1с делало бы процесс охлаждения очень медленным. Чтобы ускорить цикл охлаждения, основной уровень ионов подкачивается через короткоживущий уровень $P_{3/2}$. Таким методом в 1989 году в NISTe был охлажден единичный ион Hg^+ в основном состоянии при одномерной геометрии [214]. В Ca^+ подкачиваемый переход возбуждается лазерным диодом с длиной волны 814 нм. Охлаждение единичных ионов в основном состоянии и недавно реализованное охлаждение разных колебательных мод двух ионов, наблюдалось в сферической ловушке Пауля в университете

Инсбрука [215]. О первом опыте по охлаждению основного состояния коллективных мод движения двух ионов $^9Be^+$ в ловушке сообщалось в [216].

Очевидно, что охлаждение основного состояния реализовать проще, если доплеровское охлаждение происходит при низких колебательных квантовых числах. В этом случае, чтобы достигнуть основного колебательного состояния, необходимо выполнить только несколько циклов сателлитного охлаждения. Для жесткой ловушки в NISTe пяти рамановских циклов охлаждения оказалось достаточно чтобы система оставалась в основном состоянии 98% времени [211]. В случае Ca^+, в сферической ловушке, используемой в Инсбруке, была зарегистрирована относительная населенность в основном состоянии движения 99.9%, после охлаждения за 6.4 мс [215] (собственная частота ловушки 4.5 МГц). Здесь скорость переходов при охлаждении составляла несколько кГц. В случае линейной ловушки в Инсбруке, имеющей гораздо более низкую частоту и, следовательно, более высокие колебательные квантовые числа после доплеровского охлаждения, возникали трудности при охлаждении основного состояния. Однако, преимуществом линейной ловушки, как уже упоминалось выше, являются большие расстояния между ионами, что упрощает индивидуальную адресацию в квантовых операциях. Более того, наблюдался низкий уровень нагрева – порядка одного фонона за 190 мс, по сравнению с достаточно большими размерами ловушки – около 1.4 мм [215].

5.2.8 Размещение электронов и детектирование колебательного движения

Квантованное движение малого числа ионов очень слабо связано с термостатом и его трудно зарегистрировать непосредственно. Наоборот, внутреннее электронное состояние можно зарегистрировать очень удобным способом – в так называемом, методе «размещения электронов», предложенном Дэмелтом [217]. Эта ситуация очень похожа на «классические» эксперименты по КЭР, где фотонное поле локализовано внутри сверхпроводящего резонатора и труднодоступно, но косвенно может детектироваться при измерении ридберговских атомов после их взаимодействия с осцилляторной модой.

Основная идея метода «размещения электронов» очень проста. Необходима трехуровневая система, состоящая из основного состояния $|g\rangle$, метастабильного возбужденного состояния $|e\rangle$ и короткоживущего состояния $|p\rangle$. Основное состояние на некоторое время связывается с состоянием $|e\rangle$ – система оказывается в состоянии суперпозиции $\alpha|g\rangle + \beta|e\rangle$. Если теперь осуществить переход $|g\rangle \rightarrow |p\rangle$, короткожи-

вущее состояние $|p\rangle$ возбуждается и распадется, но только если система перейдет в состояние $|g\rangle$. Тот факт, что фотон излучается при распаде состояния $|p\rangle$, что можно было бы наблюдать в принципе, и составляет измерение суперпозиции. Такое измерение дает результат $|g\rangle$ с вероятностью $|\alpha|^2$, соответствующей возбуждению и распаду состояния $|p\rangle$, и результат $|e\rangle$ с вероятностью $|\beta|^2$, отвечающей отсутствию возбуждения и распада состояния $|p\rangle$. Даже если эффективность детектирования фотона при одном распаде $|p\rangle$ очень мала (обычно 10^{-3}), можно повторить возбуждение системы и рассеять миллионы фотонов, в конце концов зарегистрировать несколько из них и убедиться, что система перешла в состояние $|g\rangle$. Если состояние системы «размещено» в основном метастабильном состоянии $|e\rangle$ рассеяния больше происходить не будет. В каждом отдельном эксперименте ответ будет либо $|g\rangle$ (рассеянные фотоны зарегистрированы), либо $|e\rangle$ (рассеянные фотоны не регистрируются); таким образом измерение этих состояний почти со 100%-ой эффективностью полностью разрушает когерентность между $|g\rangle$ и $|e\rangle$.

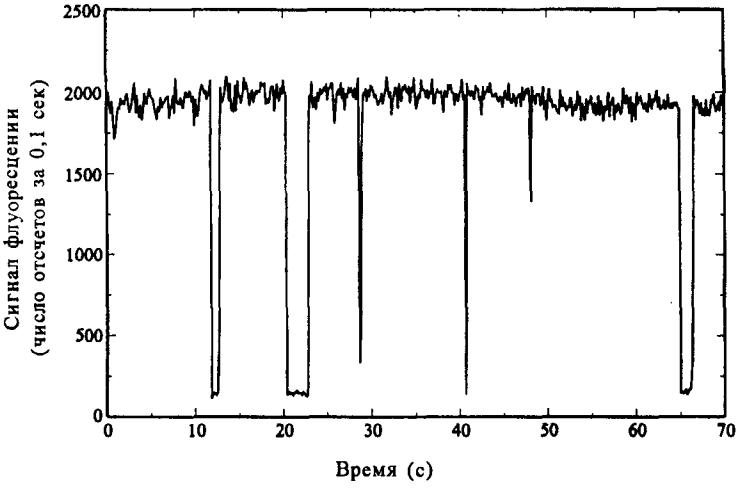


Рис. 5.10. Квантовые скачки единичного иона $^{40}Ca^{+}$. Если ион совершает переход в метастабильное состояние $D_{5/2}$, флуоресценция пропадает. После промежутка времени, совпадающего с временем жизни возбужденного состояния ($\tau \approx 1$ с), спонтанный переход сбрасывает ион в основное состояние и флуоресценция возвращается к первоначальному уровню.

После усреднения по многим экспериментам, количество испытаний, в которых наблюдаются рассеянные фотоны, будет пропорционально $|\alpha|^2$. В качестве примера, подтверждающего эффективность такого метода, на рис.5.10 показан сигнал фотоумножителя, регистрирующего свет, рассеянный на одиночном ионе Ca^{+} при непрерыв-

ном возбуждении перехода $S_{1/2} \rightarrow P_{1/2}$ с длиной волны 397 нм. Когда ион Ca^+ находится в $S_{1/2}$-состоянии, он рассеивает около 2000 фотонов за 100 мс и они регистрируются фотоумножителем. Через некоторое время, скажем, порядка t = 20 с, ион возбуждается в состояние $D_{5/2}$ слабым пучком света с длиной волны 729 нм и скорость отсчетов детектора падает до 150 событий за 100мс, что складывается из темновых отсчетов фотоумножителя и некоторого количества рассеянного возбуждающего излучения с длиной волны 397нм, попадающего на детектор. Очевидно, что два состояния могут быть различимы с хорошей точностью за 1мс и при среднем темновом времени порядка 1с, определяемым излучательным временем жизни состояния $D_{5/2}$.

С небольшими усовершенствованиями метод квантового размещения может также использоваться для разрешения сверхтонкой структуры основных состояний, как это необходимо в экспериментах с $^9Be^+$. Поскольку $|g\rangle$ выбирается в состоянии с максимальным m_F ($F = 2$, $m_F = 2$), можно возбуждать циклический переход в состояние $^2P_{3/2}$ ($F = 3$, $m_F = 3$) используя σ^+ циркулярно-поляризованный лазерный свет (D2 на Рис. 5.8); такой способ не оставляет иону других путей возвращения в основное состояние $|g\rangle$. Несовершенство экспериментальной процедуры приготовления поляризованного света σ^+ и неточность попадания в резонанс могут возбудить нерассеивающие состояния, что уменьшает эффективность регистрации [218].

5.2.9 Когерентные состояния движения

Приготовление когерентных состояний света с использованием КЭР обсуждалось в разд.5.2.3. В этом разделе мы будем рассматривать приготовление когерентных состояний движения иона (ионов) в ловушке. Начиная от основного состояния, когерентные состояния движения могут быть приготовлены при воздействии на ионы классической резонансной силы с осцилляторной частотой. Наиболее удобный способ состоит в воздействии на ионы электрической силы с частотой ω. В зависимости от амплитуды, фазы и длительности возмущения возникающие когерентные состояния описываются комплексным параметром α, причем $|\alpha|^2 = \bar{n}$, – значение квантового числа осциллятора.

В случае более одного иона, нормальные моды могут возбуждаться при настройке на их резонансные частоты. Необходимо заботиться о том, чтобы возбуждающее поле имело правильную геометрию. Мода центра масс будет возбуждаться однородным полем, для вытянутых мод необходима определенная кривизна поля, при возбуждении мод высших порядков нужны высшие моменты поля. Несколько фильмов, в которых показаны когерентные состояния с большими числа-

ми ($\bar{n}$ = 100000), в массиве до семи ионов, можно найти на web-страничке группы из Инсбрука [207]. Один из кадров показан также на рис. 5.11. Неоднородность поля в этом эксперименте была достаточно большой для возбуждения двух низших нормальных мод. На рис. 5.11(a) показаны вытянутые или дышащие моды, а на рис.5.11(b) показана мода ЦМ. Картинки были получены стробоскопическим методом CCD-камерой при медленном сканировании.

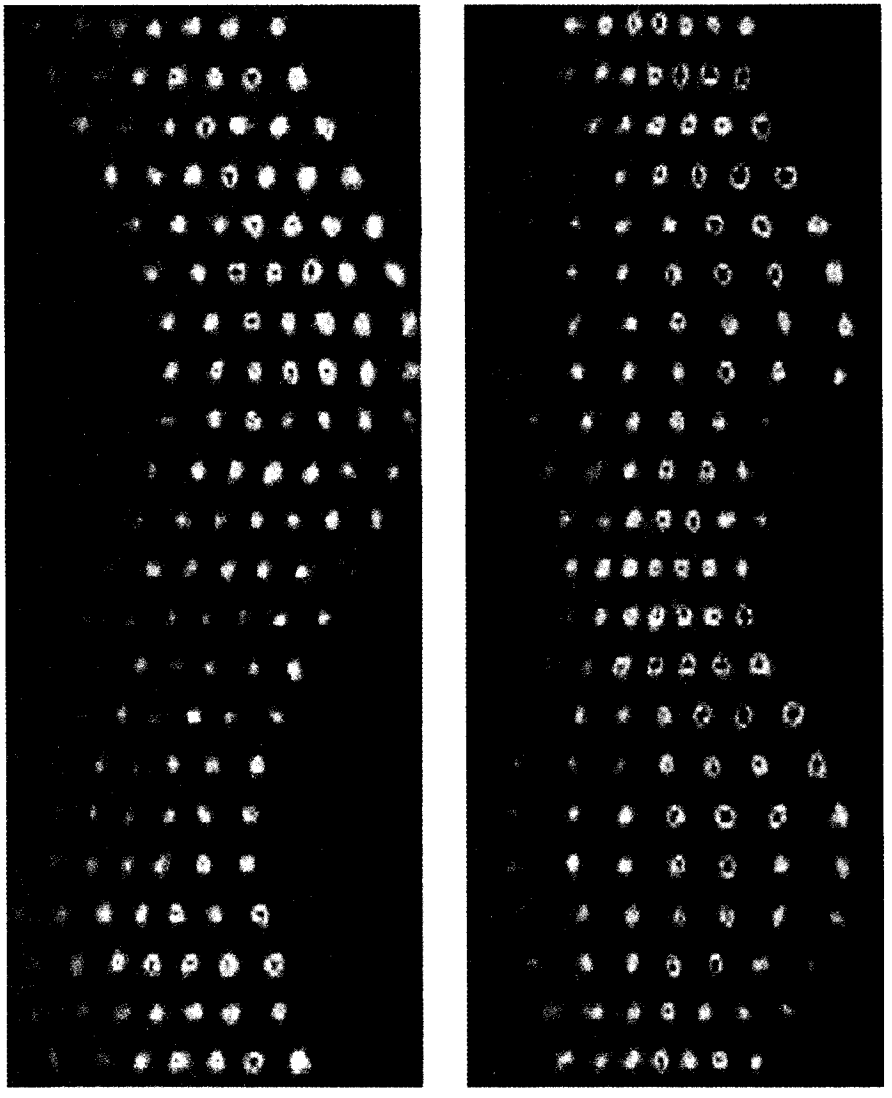


Рис. 5.11. Экспериментальная демонстрация дышащей моды (a) и движения центра масс (b) массива из 7 ионов. На рисунках приведены фотографии, сделанные для массива ионов за фиксированный интервал времени (короткий, по сравнению с временным масштабом колебательного движения).

Вместо использования электрического заряда ионов и внешних электрических сил для приготовления когерентных возбуждений колебательных мод, можно использовать внутреннее состояние ионов, взаимодействующих с лазерными световыми полями. Два лазерных (рамановских) пучка с разницей частот равной ω не будут индуцировать переходы между внутренними состояниями, зато будут когерентно возбуждать все более высокие колебательные моды. В результате ион(ы) будет (коллективно) осциллировать с частотой гармонического осциллятора ω, возбуждаемого двумя световыми полями. Поскольку частоты обоих пучков близки к частоте перехода между $^2S_{1/2}$ и $^2P_{1/2}$, на ион действует сила со стороны колеблющегося диполя. Придав рамановским пучкам σ^+-поляризацию, можно сделать эту силу зависящей от внутреннего состояния: для $|g\rangle$ связанного состояния внутри сверхтонкой структурой уровня $^2P_{1/2}$ не существует, поэтому только $|e\rangle$-состояние будет чувствовать воздействие со стороны диполя. Как говорилось в разд. 5.2.1, при синтезе состояний типа шредингеровской кошки этот момент является решающим. Обе методики генерации когерентных состояний уже были использованы группой из NISTa при работе с единичными ионами Be^+ в ловушке.

Для когерентных состояний с малыми значениями колебательных квантовых чисел амплитуда колебательного движения слишком мала для того, чтобы разрешить его с помощью камеры: движение ионов очень трудно зарегистрировать непосредственно. Вместо этого можно связать колебательное движение с внутренним двухуровневым состоянием системы.

Чтобы измерить колебательное движение, т.е. определить населенности состояний с определенным числом фотонов $|n\rangle$, мы сначала индуцируем «синие сателлитные» переходы лазерным светом, отстроенным по частоте в синюю область спектра на $\delta = +\omega$. Эти переходы между $|g, n\rangle$ и $|e, n + 1\rangle$ изображены на рис. 5.12. При использовании непрерывного режима генерации лазера, осцилляции Раби возбуждаются между уровнями, показанными стрелками на Рис.5.12.

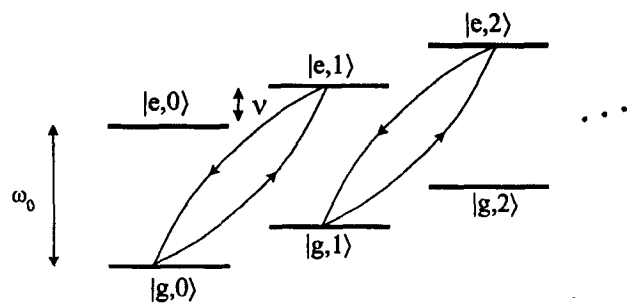


Рис. 5.12. Схема уровней одиночного двухуровневого иона в ловушке в виде гармонического потенциала. Стрелками показаны осцилляции Раби между уровнями $|g, n\rangle$ и $|e, n + 1\rangle$. Частота Раби зависит от n.

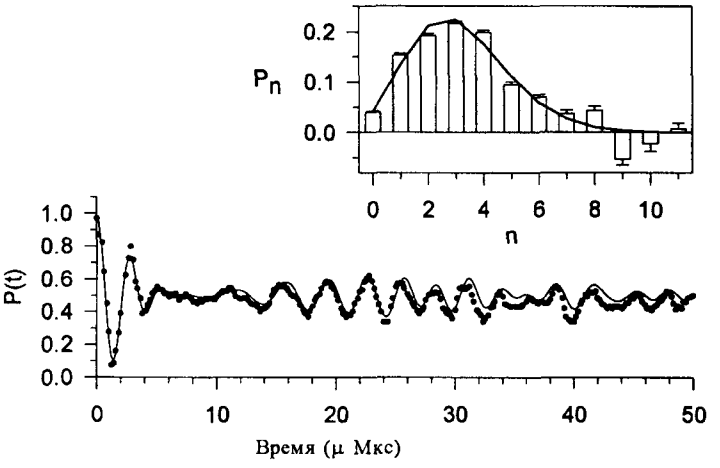


Рис. 5.13. P_g для когерентного состояния. Сплошная линия – аппроксимация данных (точки) суммой состояний, имеющих когерентное распределение. Параметр аппроксимации – значение квантового числа $\bar{n} = 3.1 \pm 0.1$. На врезке показаны амплитуды компонент состояний (столбики) и аппроксимация пуассоновским распределением с $\bar{n} = 2.9 \pm 0.1$. (Воспроизводится из [220]).

При включенном лазере с отстройкой в синюю область, вероятность $P_g(t)$ того, что ион изначально находившийся во внутреннем состоянии $|g\rangle$, спустя время t все еще находится в нем, дается формулой:

$$P_g(t) = \frac{1}{2}\left[1 + \sum_{n=0}^{\infty} P_n \cos(2\Omega_{n,n+1}t)e^{-\gamma_n t}\right], \qquad (5.6)$$

где P_n – вероятность найти атом в состоянии с числом n и $\Omega_{n,n+1}$ – частота перехода между уровнями $|g, n\rangle$ и $|e, n+1\rangle$. В пределе, обсуждавшемся в связи с формулой (5.5), $\Omega_{n,n+1} = \Omega_0 \eta \sqrt{n+1}$. Ключевой момент состоит в том, что частоты различаются для всех пар $(n, n+1)$ и, таким образом Фурье-преобразование от $P_g(t)$ дает вероятности P_n. Экспериментальные данные получены при освещении системы синим сателлитным излучением в течение времени t и затем – измерении внутреннего состояния иона при помощи техники «размещения», которая обсуждалась в предыдущем разделе. После многих повторений эксперимента для каждого момента времени t (1000 раз) можно определить $P_g(t)$. Временные сигналы можно затем подвергнуть Фурье-преобразованию, чтобы получить распределение уровней P_n. Экспериментально зарегистрированный сигнал $P_g(t)$ и его Фурье-преобразование для когерентного состояния единичного иона Be^+ с показаны на Рис. 5.13. Этот сигнал очень похож на результаты, полученные методом КЭР и показанные на Рис. 5.2. После быстрого спада за время

порядка 6 мкс, сигнал нарастает за $t \approx 12$ мкс. Другой спад и подъем заметен на временах от 32 мкс до 45 мкс перед тем, как когерентность полностью исчезает.

5.2.10 Функция Вигнера однофононного состояния

Функция P_n, определенная в предыдущем разделе, непосредственно соответствует диагональным элементам ρ_{nn} матрицы плотности ρ и на первый взгляд кажется, что это единственное, что можно определить. Но оказывается можно обойти эту проблему, вводя когерентный сдвиг в начальное состояние движения. Экспериментально это делается точно так же, как и при синтезе когерентных состояний. Вместо сдвига основного состояния $|\alpha\rangle = U(\alpha)|0\rangle$, теперь сдвигается начальное состояние движения: $|\psi_{mot},\alpha\rangle = U(\alpha)|\psi_{mot}\rangle$. Затем измеряются населенности различных состояний $|\langle n|U(\alpha)|\psi_{mot}\rangle|^2$, как рассматривалось в разд.5.2.9. Проделывая эту операцию с достаточным количеством различных параметров сдвига α, можно восстановить недиагональные элементы матрицы плотности в базисе определенного числа частиц, или вигнеровскую функцию начального состояния движения [219].

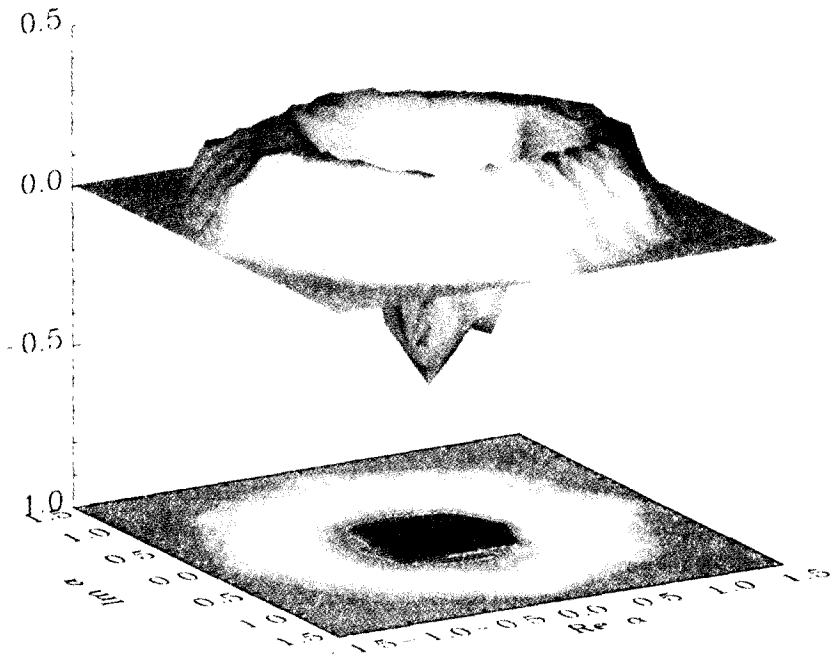


Рис. 5.14. Поверхность и контур воспроизведенной функции Вигнера W(α) в приближении состояния с $n = 1$. Отрицательные значения W(α) вблизи нуля выявляют неклассическую природу такого состояния. (Воспроизведено из [219])

Имея основное состояние движения и выполняя все необходимые операции, предопределенные видом гамильтониана (5.5), можно синтезировать почти любые состояния движения. Практически, группой из NIST уже были реализованы и проанализированы тепловые состояния, состояния с определенным числом частиц (фоковские), сжатые, типа шредингеровской кошки и другие суперпозиции n-частичных состояний единичных ионов [219-221].

Состояния с заданным числом частиц синтезируются из основных состояний с помощью воздействия последовательностью π-импульсов на синие и красные сателлиты. Такая последовательность заставляет ион двигаться по следующему пути: $|g,0\rangle \rightarrow |e,1\rangle \rightarrow |g,2\rangle \rightarrow ...$ и так далее. Таким образом были получены состояния с числами вплоть до $n = 16$. Сигнал от них представляется простой синусоидой, частота которой возрастает по закону $\sqrt{n+1}$ с некоторыми отклонениями, вызванными тем, что η не равно нулю ($\eta = 0.202$, см. рис. 1 в [220]). Более интересно, что вигнеровская функция принимает отрицательные значения для состояний с нечетными n. Экспериментально измеренная вигнеровская функция состояния с $|n\rangle = |1\rangle$, показана на Рис. 5.14. Она отрицательна вблизи нуля, что находится в хорошем согласии с теорией.

5.2.11 Сжатые состояния и состояния типа шредингеровской кошки для ионов

Состояния сжатого вакуума могут быть приготовлены по аналогии со случаем оптического параметрического генератора, когда ион возбуждается электрическим полем на частоте 2ω, либо двумя рамановскими пучками с соответствующей расстройкой частот. В эксперименте уже получены состояния сжатого вакуума с отношением квадратурных компонент 40 (уровень подавления шума в сжатой квадратуре 16 дБ) [220]. К сожалению, в противоположность сжатому свету, до сих пор не находится чувствительного измерительного приложения, в котором можно было бы использовать состояния, обладающие столь впечатляющей степенью сжатия.

Состояния типа ШК, имеющие вид (5.4), но включающие движение иона вместо фотонного поля, были получены в Be^+ [221]. После лазерного охлаждения в состояние $|g, n = 0\rangle$, показанное на Рис. 5.15(a), состояние ШК синтезируется при подаче нескольких последовательных импульсов рамановских пучков света.

$\pi/2$-импульс раскладывает волновую функцию в суперпозицию состояний $|g, 0\rangle$ и $|e, 0\rangle$ с одинаковыми амплитудами, как показано на Рис. 5.15(b). Затем, поляризованные рамановские пучки, отстроенные друг относительно друга на ω, возбуждают только движение в коге-

рентном состоянии $|\alpha\rangle$, коррелированном с $|e\rangle$ – компонентой, как объяснялось в разд. 5.2.9 и показанное на Рис. 5.15(c). На Рис.5.15(d) изображено, как π-импульс поля затем меняет местами внутренние состояния суперпозиции. Рис. 5.15(e) иллюстрирует как второй импульс поляризованных рамановских пучков возбуждает другое когерентное состояние движения $|\alpha e^{i\phi}\rangle$, коррелированное с новой $|e\rangle$ – компонентой. После этого шага состояние принимает вид

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|e\rangle|\alpha e^{i\phi}\rangle + |g\rangle|\alpha e^{-i\phi}\rangle\right). \tag{5.7}$$

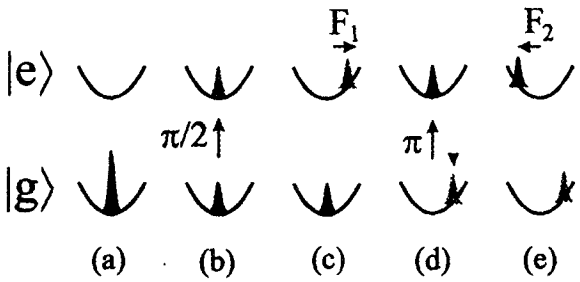


Рис. 5.15. приготовление состояний ШК на ионах. (a) начальное состояние $|g, n = 0\rangle$. (b) $\pi/2$-импульс готовит состояние $|g, 0\rangle$ и $|e, 0\rangle$. (c) Возбуждение когерентного состояния колебательного движения через оптическое взаимодействие между поляризованными рамановскими пучками и $|e\rangle$. (d) π-импульс инвертирует внутреннее состояние населенностей. (e) в итоге возбуждается другое когерентное состояние для новой $|e\rangle$-компоненты и приводящее к состоянию ШК.

Относительная фаза ϕ определяется фазой колебания на разностной частоте рамановских пучков, лежащей в ВЧ диапазоне; она просто управляется с помощью фазовой синхронизации ВЧ источников. При рассмотрении декогерентных свойств такого состояния нужно иметь в виду, что они не описываются и не моделируются также хорошо, как при распаде резонаторной моды. С другой стороны, обилие возможных взаимодействий позволяет экспериментатору конструировать «термостат» по своему усмотрению. Такой искусственный термостат будет в основном определять декогерентность при условии такой связи, чтобы характерные времена индуцированных потерь оказывались гораздо меньше, чем времена релаксации, наблюдаемые без термостата.

5.2.12 Квантовая логика на единичном ионе $^9Be^+$ в ловушке

Охлажденные ионы в ловушке, взаимодействующие с лазерными полями, являются достойными кандидатами для экспериментальной реализации квантовых логических устройств, рассмотренных в разд.4.3.

Впервые это было отмечено Цираком и Цоллером [156]. Квантовая информация содержится в кубитах, построенных на внутренних уровнях ионов, в то время как нормальные моды внешнего движения, общие для всех ионов в ловушке, могут служить «регистром данных» для того, чтобы перемешать внутренние состояния (см. разд. 5.3.7). К настоящему времени несколько групп произвели охлаждение ионов в линейных ловушках до состояния, когда они образуют кристаллические цепочки (см. Рис.5.11). Было достигнуто охлаждение в основное состояние движения. Эта деятельность находится в постоянном развитии, для того, чтобы продемонстрировать охлаждение основного состояния цепочек, содержащих большее количество ионов.

В эксперименте, выполненном в 1995 году группой из NISTa был реализован квантовый логический элемент «контроллируемое-НЕ» между внутренней двухуровневой системой иона ($|g\rangle$ и $|e\rangle$, бит-мишень) и его движением в ловушке ($|n = 0\rangle$ и $|n = 1\rangle$, управляющий бит); таким образом, было продемонстрировано, что возможно чтение из «регистра данных» гармонического движения [223]. Чтобы логический элемент функционировал, использовалась последовательность трех лазерных импульсов:

1. $\pi/2$-импульс, генерирующий линейную суперпозицию $|g\rangle$ и $|e\rangle$.

2. 2π-импульс для произвольного перехода синего сателлита, связывающего $|e\rangle$ и $|aux\rangle$ и вызывающий обусловленный фазовый сдвиг в $|e\rangle$-части суперпозиции. Такой сателлит связывает только $|e\rangle$ и $|aux\rangle$; если движение характеризуется $|n = 1\rangle$, то фаза $|e\rangle$-компоненты инвертируется.

3. В заключение, $-\pi/2$-импульс приводит к конструктивной или деструктивной интерференции одного из этих состояний, в зависимости от того, имел место обусловленный сдвиг фаз в $|e\rangle$-компоненте или нет.

Для получения более наглядной картины можно представить всю последовательность этих операций также, как и при рамзеевских резонансных экспериментах. Пусть $|g\rangle$ – это исходное состояние, тогда первый $\pi/2$-импульс создает суперпозицию $|g\rangle + |e\rangle$. Затем, в зависимости от того выполняется ли $n = 0$ или нет, суперпозиция оставляется неизменной либо вводится фазовый сдвиг для возбужденной части (т.е. $|g\rangle - |e\rangle$, только при $n = 1$). Последний шаг – воздействие $-\pi/2$-импульса. Таким образом, в отсутствие фазового сдвига внутреннее состояние возвращается в $|g\rangle$, но если есть сдвиг фаз ($n = 1$), то состояние переключается в $|e\rangle$. Управляющий кубит остается без изменения в течение этого процесса. По такой схеме группой из NISTa была измерена таблица истинности для операции «контролируемое-НЕ», а также продемонстрированы когерентные свойства этого логического элемента (см. Рис.2 и 3 в [223]).

5.2.13 Сопоставление результатов и дальнейшие перспективы

В предыдущих разделах обсуждались эксперименты по квантовой информации и квантовым вычислениям на примере КЭР и ионов в ловушках. Несмотря на то, что КЭР и ионно-ловушечные эксперименты в основном описываются гамильтонианом типа Джейнса-Каммингса, т.е. характеризуются похожей динамикой, каждая методика имеет свои преимущества и недостатки.

Приготовление начального состояния осуществляется по стандартной методике микроволновой КЭР, т.к. основное состояние резонатора может быть достигнуто при криогенном охлаждении до температур ^{3}He. Генерация пучков долгоживущих циркулярных ридберговских атомов, отобранных по скоростям, происходит при использовании стандартных инфракрасных лазеров и радиочастотных полей. При лазерном охлаждении ионов, в основном, используются источники света ультрафиолетового диапазона. В экспериментах по КЭР реализуется точное взаимодействие Джейнса-Каммингса, в то время как в экспериментах с ионными ловушками – лишь приближенное, т.е. в пределе малого значения параметра Лэмба-Дике. С другой стороны, связывание ионов в ловушках с осцилляторной модой дает больше свободы и может быть описано более широким классом функций, чем при точном взаимодействии Джейнса-Каммингса. Декогерентность атомов (ионов) практически пренебрежимо мала, как для ридберговских атомов, так и для сверхузких (метастабильных) состояний атомов. При рассмотрении моды гармонического осциллятора, источники потерь в сверхпроводящем резонаторе хорошо известны и поддаются моделированию. Единственный регулируемый параметр декогерентности – добротность резонатора – определяется независимо при помощи классических методов СВЧ-диапазона. Для ионов в ловушках источники колебательной декогернтности пока недостаточно изучены. Учет «фундаментальных» источников декогерентности, таких как затухание, индуцированное изображением заряда иона в структуре электродов или фоновые столкновения в газе, дает на порядок меньший нагрев, чем наблюдаемый в экспериментах [215, 218]. Такой «аномальный» нагрев будет исследоваться в дальнейшем и в конечном счете проблема будет решена, т.к. нет фундаментальных причин для ее существования.

Для выполнения операций, представляющих интерес для квантовых вычислений, необходимо манипулировать, по крайней мере, несколькими кубитами. При использовании существующих технологий КЭР-эксперименты с пучком циркулярных ридберговских атомов, пересекающих резонатор, оказываются весьма трудновыполнимыми для

последовательности из двух или трех атомов. Как уже обсуждалось выше, среднее число атомов за импульс должно быть существенно меньше единицы, чтобы избежать событий с участием двух атомов. Наложение во времени трех или четырех атомов происходит чрезвычайно редко и время накопления, таким образом, нарастает экспоненциально с ростом числа атомов. Этому ограничению не подвержены эксперименты с ионами в ловушках. Удержать несколько ионов в линейной ловушке сравнительно просто. Индивидуальная адресация к отдельным ионам при помощи жестко сфокусированных импульсных лазерных пучков вполне достижима. При сохранении охлажденным основного колебательного состояния, квантовые логические операции на нескольких кубитах представляются реализуемыми.

Другое немаловажное достоинство экспериментов с ионными ловушками состоит в почти 100%-ой квантовой эффективности детектирования состояний ионов при использовании методов квантового размещения. Например, эксперименты по проверке неравенств Бэлла или с перепутанными ионами могли бы очень просто решить проблему эффективности детектирования, остающуюся пока открытой в других экспериментах, где используются фотоны или даже атомы (представляется, что в КЭР-экспериментах не существует перспектив увеличения квантовой эффективности более 90%).

Таким образом, представляется, что «классические» КЭР-эксперименты более подходят для исследования декогерентности и перепутывания с ограниченным числом атомов (вплоть до четырех) в очень хорошо контролируемых системах. В настоящее время идут эксперименты по приготовлению перепутанных триплетов атомов ГХЦ-типа. Исследование процессов декогерентности будет продолжаться и дальше. В частности, можно непосредственно определить вигнеровскую функцию резонаторного поля [224]. Это позволило бы понять сущность процесса декогерентности состояния ШК. Наконец, в экспериментах с двумя отдельными сверхпроводящими резонаторами могли бы быть приготовлены нелокальные мезоскопические состояния, объединяющие две наиболее интригующие особенности квантового мира.

В ионных ловушках уже было продемонстрировано восстановление функции Вигнера, но отсутствие теоретических моделей и недостаточно понятая природа процесса декогерентности в ионных ловушках усложняет его понимание. Ловушки также являются многообещающими в качестве инструмента по исследованию квантовой логики в умеренных масштабах, т.е. при вовлечении до десятка кубитов и выполнении нескольких сотен операций. Однако, реализация алгоритма Шора по факторизации на простые множители для разрушения классических криптографических кодов требует, по крайней мере, 400 ку-

битов, что выходит, как представляется, за границы имеющихся знаний и существующих технологических возможностей.

Должны быть найдены новые пути преодоления фундаментальных пределов, таких как спонтанное излучение; в тоже время реализация алгоритмов коррекции ошибок и стабилизации кодов могла бы указать способы решения этих проблем. На пути их преодоления предвидится много интересных задач по обработке квантовой информации, которые уже решены в методиках, оперирующих с несколькими кубитами, например, в методе очищении перепутывания. Такие «информационно-обогащенные» состояния также могли бы быть использованы для улучшения существующих стандартов частоты на ионных ловушках (разд.7.6).

Помимо всех возможных применений, эксперименты на простых фундаментальных взаимодействиях в системах с хорошо контролируемым окружением дают возможность исследовать самые сокровенные особенности квантовой механики.

5.3. ЛИНЕЙНЫЕ ИОННЫЕ ЛОВУШКИ ДЛЯ КВАНТОВЫХ ВЫЧИСЛЕНИЙ

Х.С.Ногель, Ф.Шмидт-Келер, Дж.Эшнер, Р.Блатт, В.Ланге, Х.Бэлдауф, Х.Уолтер

5.3.1 Введение

После того, как был достигнут практически полный контроль над квантовым состоянием единичного иона, как было показано в разд.5.2., внимание было переключено на системы нескольких ионов с хорошо контролируемыми взаимодействиями между ними. Манипуляции с их совместным квантовым состоянием ставят целью приготовление перепутанных состояний, не имеющих классического аналога. Более того, возможность перепутывания массивных частиц открывает перспективы для новых экспериментов, включая измерение состояний Бэлла, и ГХЦ -состояний [176], которые позволили бы выполнить новые квантово-механические тесты. Перепутывание частиц дает возможность детального изучения процесса квантового измерения и исследования явления декогерентности.

Для реализации квантовых логических элементов [156] – основных блоков для построения квантового компьютера – была предложена, благодаря своим уникальным свойствам, цепочка ионов в линейной ловушке. Логические устройства оперируют с квантовыми регистрами, приготовленными из квантовых битов (кубитов), которыми можно манипулировать аналогично классическим битам, используя

реализуемые логическими элементами операции. Квантовые логические элементы на основе ионных ловушек основаны на перепутывании внутренних степеней свободы ионов (электронные возбуждения) и коллективного движения (колебательного возбуждения) запертых в ловушке цепочек. Квантово–механическим аналогом классического элемента XOR является так называемая операция «контролируемое-НЕ», которая может быть реализована с использованием строго заданной последовательности лазерных импульсов, направляемых к двум разным ионам в цепочке. Было показано, что элемент «контролируемое-НЕ» является универсальным логическим элементом, так что, в принципе, любое вычисление может быть выполнено, используя только такой двух-ионный квантовый элемент и операции однобитовых вращений [227]. Реализация таких операций с логическими элементами, основанными на цепочках ионов, представляет фундаментальный интерес, так как все основные алгоритмы могли бы быть проверены только на линейных ионных ловушках.

В этом разделе обсуждаются специфические свойства линейных ионных ловушек, а также их использование для квантовых вычислений. В разд.5.3.2 приводится обзор операций над ионными ловушками и рассмотрены всевозможные способы реализации линейных ловушек. В разд. 5.3.3 представлены методики, требуемые для охлаждения в основное состояние движения и возможные предпосылки для реализации квантовых логических элементов на цепочках ионов. Упорядоченные структуры ионов кратко обсуждаются в разд. 5.3.4. В 5.3.5 – 5.3.9 приводится обзор и обсуждение специфических приемов, необходимых при операциях над квантовыми логическими элементами, т.е. приготовление состояний и манипулирование ими, возбуждение общей моды и чтение внутреннего электронного состояния с единичной эффективностью.

5.3.2 Удержание ионов в линейной ловушке

Заряженные частицы, такие как ионы атомов, могут удерживаться электромагнитными полями либо при использовании комбинации статического электрического и магнитного полей (ловушка Пеннинга), либо зависящего от времени неоднородного электрического поля (ловушка Пауля) [197]. Ловушка Пауля и, особенно ее линейный вариант, представляется предпочтительной [228] для применения заряженных ионов в качестве квантовых битов и регистров.

Чтобы удержать частицу, требуется присутствие возвращающего поля $\boldsymbol{F}$, например, $\boldsymbol{F} \propto -\boldsymbol{r}$, где $\boldsymbol{r}$ – расстояние от начала координат ловушки. Такие силы могут быть получены в квадрупольном потенциале $\Phi = \Phi_0(\alpha x^2 + \beta y^2 + \gamma z^2)/r_0^2$, где Φ_0 обозначает напряжение, прило-

женное к квадрупольной конфигурации электродов, r_0 – характерный размер ловушки, а константы α, β, γ определяют форму потенциала. Например трехмерное удержание в ловушке Пауля описывается параметрами $\alpha = \beta = -2\gamma$, если же $\alpha = -\beta$, $\gamma = 0$, получается квадрупольный фильтр массы. Трехмерная ловушка Пауля обеспечивает удерживающую силу, приложенную к отдельной пространственной точке, и поэтому в основном используется в экспериментах с единичными ионами или для удержания больших центрально-симметричных ионных облаков. Для того, чтобы создать квантовый регистр на ионах в ловушке, требуются цепочки ионов. Поэтому, в большинстве случаев применяется линейный вариант ловушки Пауля, который основан на потенциале фильтра квадрупольной массы. Такой потенциал обеспечивает удерживающие силы в двух направлениях, перпендикулярных оси z, но не оказывает влияния на движение вдоль оси z. Для аксиального удержания нужно использовать дополнительные электроды. Радиальное удержание ионов требует постоянного напряжения U_{dc} и переменного $V_{ac}\cos(\Omega t)$, приложенного к электродам. Потенциал ловушки вблизи оси имеет вид

$$\Phi = \frac{U_{dc} + V_{ac}\cos(\Omega t)}{2r_0^2}(x^2 - y^2), \tag{5.8}$$

где за r_0 обозначено расстояние от оси ловушки до поверхности одного из электродов. Если приложено только постоянное напряжение, то (5.8) описывает седловой потенциал, который приводит к стабильному удержанию только в одном направлении, как показано на Рис. 5.16. Однако, при подаче переменного напряжение (*ac*) возникает ловушка. Как видно из Рис.5.16, изменение знака переменного напряжения ведет к удержанию частицы в направлении, вдоль которого ранее имелась нестабильность. Выбирая надлежащим образом частоту Ω, частицы можно удерживать в ловушке бесконечно долго. Как видно из (5.8), идеальный потенциал можно создать при использовании электродов гиперболической формы (см. Рис. 5.17a). Для упрощения они обычно изготавливаются приблизительно в виде цилиндрических стержней, как на Рис. 5.17b, или более совершенной формы (Рис.5.17c), которая зависит от требований, предъявляемых к конструкции для доступа лазерного пучка и диагностики. Аксиальное удержание обеспечивается дополнительным статическим потенциалом U_{cap}, приложенным вдоль оси z, используя дополнительные кольцевые электроды (Рис.5.17b) или сегментами стержневых электродов (Рис. 5.17c). Это создает статическую гармоническую стенку в направлении z, которая характеризуется продольной частотой ловушки

$$\omega_z = \sqrt{2kqU_{cap}/mz_0^2}. \tag{5.9}$$

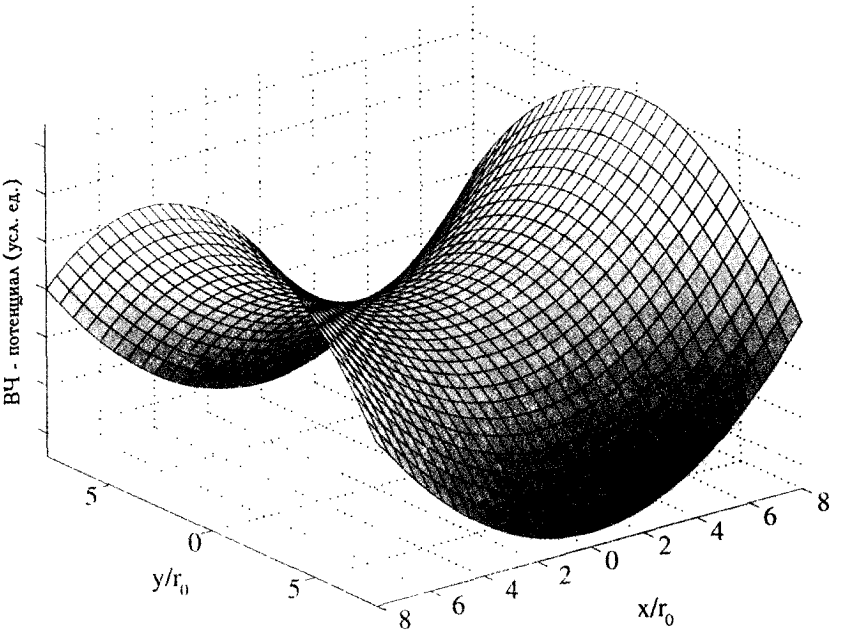


Рис. 5.16. Седловой потенциал ВЧ-ловушки Пауля. Удержание заряженной частицы около x = y = 0 достигается быстрым чередованием знака потенциала.

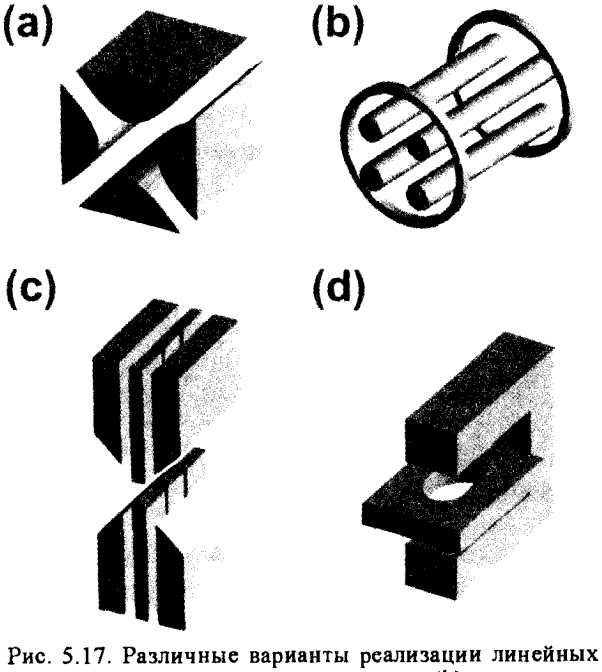


Рис. 5.17. Различные варианты реализации линейных ионных ловушек. (a) линейная квадрупольная ловушка; (b) четырех-стержневая ловушка; (c) остроконечная линейная ловушка; (d) ловушка Пауля с удлиненным кольцевым электродом.

Здесь, m и q обозначают массу и заряд иона, z_0 – половина расстояния между аксиальными электродами и k – эмпирически определяемый геометрический фактор порядка единицы, который учитывает особенности конфигурации электродов. В принципе, точное значение k может быть получено либо численно, либо, в некоторых случаях, аналитически. Однако, с практической точки зрения, использование измеренного значения k достаточно для описания экспериментальных данных. В направлениях x и y уравнения движения, получающиеся из (5.8), представляются в виде уравнений Матье [228]:

$$\frac{d^2u_x}{d\tau^2}+(a_x+2q_x\cos(2\tau))u_x=0 \tag{5.10}$$

$$\frac{d^2u_y}{d\tau^2}+(a_y+2q_y\cos(2\tau))u_y=0\ , \tag{5.11}$$

где

$$a_x=\frac{4q}{m\Omega^2}\left(\frac{U_{dc}}{r_0^2}-\frac{kU_{cap}}{z_0^2}\right) \tag{5.12}$$

$$a_y=-\frac{4q}{m\Omega^2}\left(\frac{U_{dc}}{r_0^2}+\frac{kU_{cap}}{z_0^2}\right) \tag{5.13}$$

$$q_x=-q_y=\frac{2qV_{ac}}{m\Omega^2r_0^2} \tag{5.14}$$

$$\tau=\frac{\Omega t}{2}. \tag{5.15}$$

Общее решение уравнений (5.10, 5.11) может быть найдено в виде бесконечного ряда гармоник частот ловушки Ω [197]. На самом деле условие что $a_i<q_i^2\ll 1$, $i = x, y, z$ обычно выполняется, что позволяет найти аналитическое приближение решений уравнений движения. Оно содержит гармоническое секулярное движение (макродвижение) с частотами ω_i и наложенным на него микродвижением с частотой возбуждения ловушки Ω,

$$u_i(t)=A_i\cos(\omega_i t+\varphi_i)\left[1+\frac{q_i}{2}\cos(\Omega t)\right],\qquad i = x, y. \tag{5.16}$$

Амплитуды A_i и фазы φ_i зависят от начальных условий, а секулярные частоты даются выражениями

$$\omega_i=\beta_i\frac{\Omega}{2}\ ,\quad \beta_i\approx\left[a_i+\frac{q_i^2}{2}\right]\ . \tag{5.17}$$

В этом пределе и при $U_{dc} = 0$ (что обычно выполняется), микро-

движение пренебрежимо мало и ион осциллирует так, как если бы он был заперт в гармоническом псевдопотенциале Ψ в радиальном направлении:

$$q\Psi = q\frac{|\nabla \Phi|^2}{4m\Omega^2} = \frac{1}{2}m\omega_r^2(x^2 + y^2) \tag{5.18}$$

с радиальной секулярной частотой $\omega \approx qV_{ac}/(\sqrt{2}m\Omega r_0^2)$.

Основное преимущество линейной ловушки Пауля (по сравнению с трехмерной ловушкой Пауля, используемой для хранения единичных ионов) состоит в том, что микродвижение захваченных в z-направлении ионов исчезает полностью. Таким образом, такое движение является гармоническим колебанием в статическом потенциале, обеспечивающем аксиальный захват.

Хотя применение линейных ловушек для квантовых регистров на ионах представляется предпочтительным, вариант вытянутой трехмерной ловушки Пауля может быть использован для создания цепочек из двух или трех ионов [216]. Такое устройство состоит из кольцевого электрода эллиптической формы и двух оконечных электродов (рис.5.17d); цепочка ионов ориентирована вдоль длинной оси кольцевого электрода. В этой геометрии возможно добиться более высоких частот ловушки, чем в линейном варианте, что предпочтительнее с точки зрения оптического охлаждения (см. разд. 5.2.7 и 5.3.3). С другой стороны, всегда существует остаточное микродвижение, которое может вызвать ВЧ-нагрев цепочки.

5.3.3 Лазерное охлаждение и квантовое движение

Для того, чтобы надлежащим образом сохранять квантовую информацию, квантовое состояние каждого отдельного иона в цепочке должно быть тщательно приготовлено. Это достигается при лазерном охлаждении с использованием метода, похожего на рассмотренный в разд.5.2.7 для единичного иона в ловушке. Последняя стадия охлаждения также будет сателлитным охлаждением, которое, в конечном счете, приготавливает цепочку ионов в основном состоянии движения. Однако, появление отдельных колебательных мод цепочки с различными частотами изменяет процесс охлаждения. В частности, картина сателлитного охлаждения, представленная в разд. 5.2.7, не относится, вообще говоря, к двум или более ионам. Важное отличие состоит в том, что несоизмеримые частоты колебательных мод приводят к квазиконтинуальному энергетическому спектру дискретных эквидистантных уровней, как для одной колебательной моды. Уровни энергии системы теперь относятся к внутреннему состоянию $|g\rangle$ или $|e\rangle$, а также двигательному состоянию $|\boldsymbol{n}\rangle$, где $\boldsymbol{n} = (n_1, n_2, \ldots)$ – вектор

чисел колебательных мод с частотами $\omega = (\omega_1, \omega_2, \ldots)$. Соответственно, в резонансном спектре для переходов из $|g, n\rangle$ в $|e, m\rangle$ проявляются сателлиты, которые расположены гораздо более тесно, чем у единичного иона, и при настройке лазера на одну выделенную частоту, одновременно возбуждаются все сателлитные переходы вокруг этой частоты в интервале, определяемом шириной линии γ перехода.

Говоря более конкретно, можно выделить два случая [229]. Если сателлитное охлаждение происходит в режиме Лэмба-Дике, т.е. если только два колебательных состояния n_j и $n_{j\pm1}$ оказываются заметно связанными посредством отдачи при световом взаимодействии, вклад дают сателлиты первого порядка, в то время как процесс обмена более чем одним колебательным квантом подавлен. Спектр сателлитов прост (см. Рис. 5.18a) и настройка на один из сателлитов приводит к охлаждению соответствующей моды, так же как и для единичного иона. Правда картина не совсем точно совпадает со случаем единичного иона, из-за наличия других мод, которые не взаимодействуют с лазером, а нагреваются благодаря спонтанному излучению. Поэтому для того, чтобы достигнуть основного состояния для всех мод требуются варьировать расстройки или использовать существенно более широкий спектр γ.

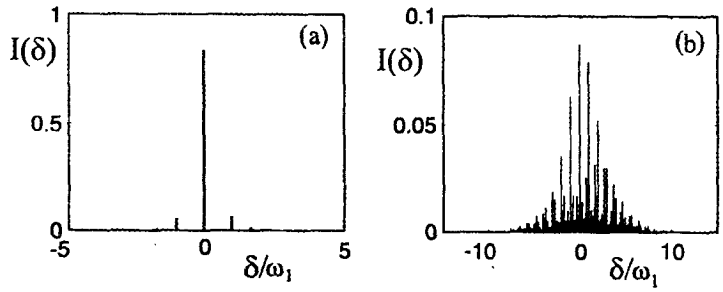


Рис. 5.18. Резонансный спектр двух ионов в ловушке внутри (a) и вне (b) режима Лэмба-Дике. Оптический переход без изменения состояния движения при нулевой расстройке показан вместе с его колебательными сателлитами при соответствующих расстройках. Внутри режима Лэмба=Дике (a) существенны только фундаментальные сателлиты при $\delta = \omega_{1,2}$, которые возникают при возбуждении лишь одного колебательного кванта. Вне режима Лэмба-Дике (b) появляется множество сателлитов, которые влекут за собой изменения в возбуждении обеих мод на один или более квант. Воспроизведено из [229].

Другой случай, т.е. сателлитное охлаждение вне режима Лэмба-Дике, применяется в настоящее время при построении большинства устройств квантовой логики на линейных ионных ловушках. Для этого случая пример сателлитного спектра цепочки из двух ионов показан на Рис. 5.18b. Очевидно, что если лазер настроен на определенную

частоту ниже резонанса, возбуждается ряд переходов, что приводит к изменению в возбуждении обеих мод, т.е. дополнительно требуется один или более квантов. В этом случае, в противоположность режиму Лэмба-Дике, обе моды охлаждаются одновременно. К тому же появляется другая зависимость скорости охлаждения от ширины линии перехода γ: скорость охлаждения увеличивается нелинейно с шириной линии, поскольку, во-первых, скорость цикла поглощения – испускания пропорциональна γ, и во-вторых, число уровней, с которыми связывается начальное состояние, а, следовательно, и число каналов по которым цепочка ионов может охлаждаться, также растет с γ. Учет скорости охлаждения, т.е. общего времени охлаждения важен, если при доплеровском охлаждении все еще оказываются возбужденными многие колебательные степени свободы. Это характерно для экспериментов с линейными ионными ловушками.

В результате численных расчетов было установлено, что в обоих случаях – внутри и вне режима Лэмба-Дике – сателлитное охлаждение можно использовать для перевода двух ионов в их основное состояние движения. Вне режима Лэмба-Дике сильная зависимость скорости охлаждения от ширины линии перехода γ может быть использована для оптимизации времени охлаждения подбором γ в ходе процесса охлаждения.

Типы ионов, использующихся для охлаждения, не обязательно должны совпадать с теми, которые пригодны для квантовых вычислений. В институте квантовой оптики им. М.Планка выполняется эксперимент, в котором задействованы линейные цепочки, содержащие ионы магния и индия. Индий можно очень эффективно подвергнуть сателлитному охлаждению в основное состояние [230], в то время как магний мог бы быть использован для переноса квантовой информации. Разделение процессов охлаждения и вычисления позволяет непрерывно охлаждать все нормальные моды без возмущения содержания квантового регистра.

В заключение разбора экспериментальных особенностей лазерного охлаждения в основное колебательное состояние в ловушках Пауля отметим, что любые случайно оставшиеся электрические поля, должны быть тщательно скомпенсированы. Такие поля могут быть вызваны неоднородностью полей на электродах и будут воздействовать на ионы, выталкивая их с оси ловушки. Следовательно, ионы будут испытывать остаточное микродвижение, которое препятствует надлежащему оптическому охлаждению. Случайные поля компенсируются приложением постоянных потенциалов к дополнительным электродам для того, чтобы втолкнуть ионы назад к оси ловушки. Это последовательно проделывается с единичным ионом, запертым в обычных

ловушках Пауля, причем во всех трех пространственных направлениях. Такая же техника может быть использована и в линейных ионных ловушках. В случае цепочки ионов, тщательное размещение всех электродов служит важной предпосылкой ликвидации микродвижения.

5.3.4 Ионные цепочки и нормальные моды

В линейной ионной ловушке ионы могут быть заперты и оптически охлаждены так, что они образуют упорядоченные структуры [212, 231]. Если радиальное удержание достаточно сильное, ионы размещаются сами собой в линейную цепочку вдоль оси ловушки на расстояниях, определяемых равновесием между кулоновским отталкиванием и потенциалом, обеспечивающим аксиальное удержание. На рисунке 5.19 показан пример цепочки ионов Ca^+ в ионной ловушке.

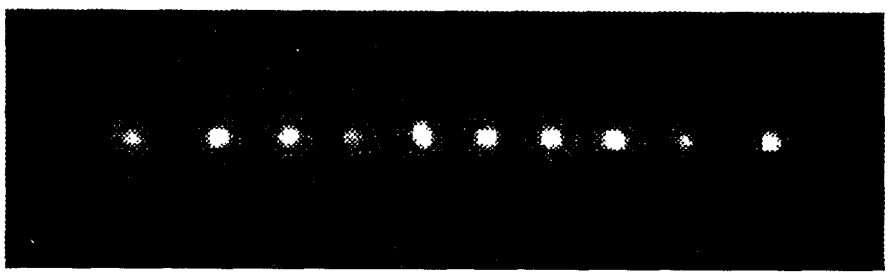


Рис. 5.19. Пример ионной цепочки в линейной ловушке Пауля. Среднее расстояние между двумя ионами приблизительно равно 10 мкм. Время экспозиции CCD-камеры – 1с. Измеренное разрешение системы изображения, состоящей из линзы и CCD-камеры лучше не хуже чем 4 мкм. Для сравнения, см. [231].

Положения равновесия ионов могут быть оценены численно. Если потенциал ловушки близок к гармоническому, эти положения могут быть описаны единственным параметром – аксиальной частотой ω_z (5.9) [212, 232]. Малые смещения ионов из положения равновесия не описываются в терминах движения отдельных ионов, т.к. кулоновское взаимодействие связывает заряженные частицы. Вместо этого движение ионной цепочки должно представляться в терминах нормальных мод цепочки частиц как целого, колеблющейся с определенными частотами. В качестве примера, рассмотрим два иона, запертых в линейной ионной ловушке. Первая нормальная мода соответствует колебанию целой цепочки ионов, двигающихся вперед и назад, как будто они жестко связаны. Такому колебанию отвечает т.н. *мода центра масс* (МЦМ) цепочки [232]. Вторая нормальная мода соответствует

такому колебанию, когда ионы двигаются в противоположных направлениях. В более общем случае эта т.н. *дышащая мода* описывает цепочку N ионов, двигающихся с амплитудой, пропорциональной их расстоянию до центра ловушки. На Рис. 5.11a и b в разд. 5.2.9 показана стробоскопическая картина дышащей моды и движения центра масс, сделанная в университете Инсбрука для цепочки из 7 ионов.

Прямой расчет нормальных мод (собственных мод) и соответствующих собственных частот ионной цепочки дает следующие простые результаты [200, 232]: (i) для одномерной цепочки, состоящей из N ионов существует точно N нормальных мод и нормальных частот; (ii) частота моды центра масс в точности совпадает с частотой единичного иона; (iii) частоты высших порядков слабо зависят от номера N, и представляются рядом (1, 1.732, 2.4, 3.05(2), 3.67(2), 4.28(2), 4.88(2), ...)ω_z, где числа в скобках обозначают максимальное отклонение частоты при увеличении N от 1 до 10 ионов, (iv) относительные амплитуды нормальных мод должны быть оценены численно (по крайней мере для цепочек, содержащих более чем 3 иона, см. уравнение (28) в [232]).

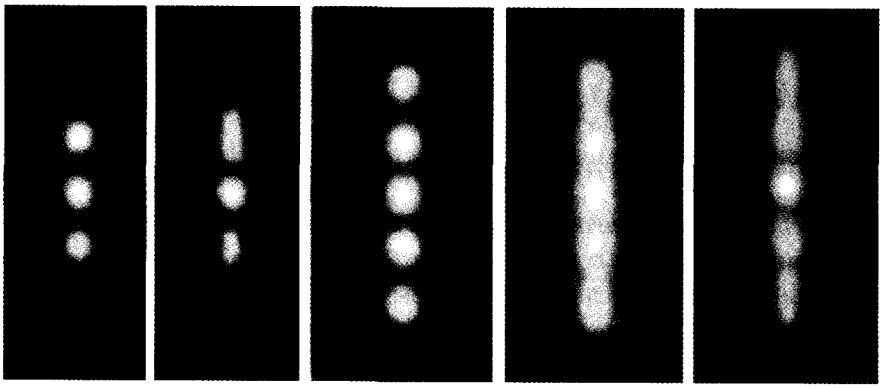


Рис. 5.20. Колебательное возбуждение цепочки из пяти ионов при наличии вешнего переменного напряжения. Слева направо: возбуждение отсутствует. Слабое и сильное возбуждение МЦМ (158.5 кГц), возбуждение дышащей моды (276.0 кГц).

После загрузки ловушки цепочкой ионов, нормальные моды могут быть возбуждены приложением дополнительного переменного напряжения либо к одному из кольцевых электродов, либо к компенсирующим электродам [212]. Возбуждение нормальной моды можно наблюдать как увеличение ширины пятна в CCD-камере задолго до появления провала в сигнале флуоресценции, регистрируемого фотоумножителем. Измерение частоты дышащей моды согласуется (с точностью не хуже 1%) с ожидаемым значением, отличающимся в $\sqrt{3}$ раз от частоты моды центра масс. На Рис. 5.20 представлено возбуждение

моды центра масс (158.5 кГц) для 5 ионов и двух величин амплитуд возбуждения. Для того чтобы возбудить дышащую моду необходимо приложить напряжение, обычно превышающее приблизительно в 300 раз то, которое нужно для возбуждения моды центра масс (3В по сравнению с 0.01В). Возбуждения мод высших порядков не наблюдались при уровнях напряжений, доступных в установке [212]. Это объясняется тем фактом, что возбуждающее поле практически однородно вдоль ионной цепочки, т.е. эффективность возбуждения высших мод, для которых необходимы градиенты поля, проходящего через ионы, была крайне низка.

Колебание МЦМ возбуждается при помощи однородного поля и поэтому очень чувствительно к флуктуациям поля, пространственное изменение которого обычно мало на масштабах, задаваемых расстоянием между ионами. Наоборот, возбуждение мод высших порядков требует больших градиентов поля. Поэтому нежелательное возбуждение происходило намного реже для мод высших порядков. Заметим, что во время квантового вычисления, кванты колебаний в ионной цепочке генерируются рамановскими сателлитными переходами, индуцированными лазерным взаимодействием с единичным ионом.

5.3.5 *Ионы как квантовый регистр*

Квантовая информация может храниться в ионе, если его приготовить либо в одном из двух различных электронных состояниях $|g\rangle$, $|e\rangle$, либо в виде любой суперпозиции этих двух состояний. Очевидное требование при выборе этих состояний состоит в том, что излучательное время жизни обоих состояний должно быть значительно больше, чем время, необходимое для выполнения вычисления, т.е. до того, как спонтанный распад разрушит когерентность. Одна из возможностей состоит в использовании основного состояния иона и метастабильного возбужденного состояния или даже двух метастабильных состояний. Времена жизни могут быть порядка секунд (например, при использовании уровней ^2D в $^{40}Ca^+$, Рис.5.21b), что должно быть достаточно для простых квантовых вычислений. Возможны даже более длительные времена жизни при использовании двух компонент сверхтонкой структуры основного состояния, которые стабильны по отношению к электродипольному распаду [216, 228]. Примеры включают ионы $^9Be^+$, $^{25}Mg^+$ и $^{43}Ca^+$; случай с бериллием показан на Рис.5.21c. Кроме того, в случае ионов, не обладающих сверхтонкой структурой, информация может храниться и в основном состоянии, если использовать зеемановскую структуру. Заметим, что поскольку ионы обычно имеют два зеемановских основных подуровня, этот подход запрещает те опера-

ции с кубитами, которые используют вспомогательные уровни, как в фазовых логических элементах, описываемых ниже. Все внутренние состояния N ионов в ловушке образуют $2N$-мерное гильбертово пространство, в котором происходит квантовое вычисление.

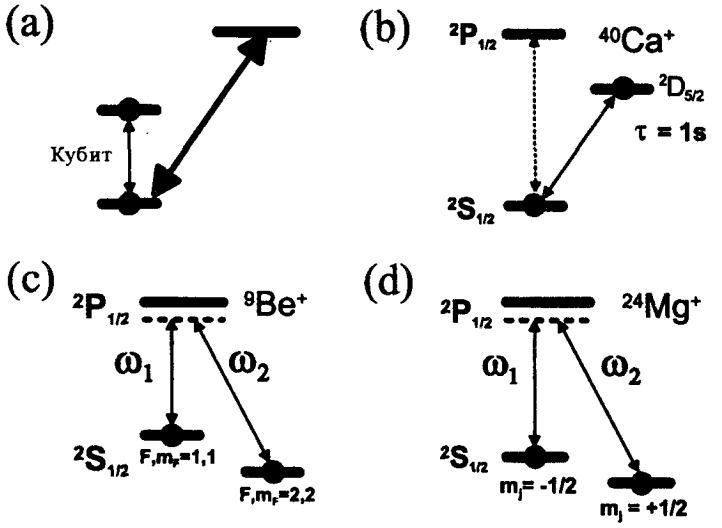


Рис. 5.21. Схема уровней ионов в ловушке используемых для квантовых вычислений. (a) трехуровневая схема с медленными переходами кубитов и быстрыми переходами для эффективного считывания; (b) кубит в основном состоянии и метастабильное состояние; (c) кубит в сверхузких основных состояниях; (d) кубит в зеемановских подуровнях.

5.3.6 Приготовление единичного кубита и манипуляции с ним

До выполнения квантового вычисления входные данные должны быть загружены в квантовый регистр. Этот процесс соответствует возбуждению каждого из N ионов в определенное квантовое состояние. Наиболее просто это достигается при воздействии лазерного излучения на внутренние состояния ионов. Предварительное требование состоит в том, что каждый лазерный луч должен иметь индивидуальный доступ к каждому иону. Расстояние между соседними ионами в ловушке составляет порядка 10мкм, значит лазерный пучок должен быть сфокусирован в пятно такого размера для предотвращения перекрестных возбуждений ионов. Подходящая схема для доступа к ионам состоит в отклонении лазерного пучка с помощью акустооптического или электрооптического эффекта, последовательно к каждому иону в цепочке. Этот метод был экспериментально продемонстрирован группой из Инсбрука [213].

Приготовление входного состояния данного кубита включает два

этапа. В первом – кубит стирается при помещении иона в одно из двух базисных состояний ($|g\rangle$ и $|e\rangle$), например, с помощью оптической накачки. Из этого хорошо определенного начального состояния произвольное суперпозиционное состояние ($\alpha|g\rangle + \beta|e\rangle$) кубита может быть получено с использованием резонансного лазерного импульса переменной длительности, путем возбуждения осцилляций Раби между двумя состояниями кубита. Если используется π-импульс, то кубит переключается в ортогональное состояние и в случае коротких импульсов таким образом можно приготовить суперпозиционное состояние кубита. Техника переключений Раби также используется, если требуются полные перевороты единичных кубитов во время квантового вычисления для обеспечения когерентной перестройки компонент квантового регистра.

Детали того, как происходит переключение Раби, зависят от используемой структуры. Если состояния кубита разделены оптическими частотами, используется однофотонный переход. В случае же сверхтонкой или зеемановской структуры электронных уровней применяются два рамановских пучка, объединяющие квантовые состояния через промежуточный виртуальный уровень близкий к возбужденному состоянию иона.

5.3.7 Колебательная мода в качестве квантовой шины данных

В операциях, рассматриваемых до сих пор, единичные кубиты были задействованы независимо друг от друга. Однако, при вычислениях (логических операциях) необходимо обеспечить сильную связь между кубитами, так что динамика любого иона в цепи может считаться обусловленной состоянием других ионов. Гораздо более сильное взаимодействие между ионами в ловушке происходит благодаря кулоновскому отталкиванию, которое в состоянии равновесия сбалансировано внешним запирающим потенциалом. Как было показано в разд.5.3.4, ионы совершают сильно коррелированные колебания вокруг положения равновесия. Особенный интерес при связывании ионов, находящихся в различных положениях в ионной ловушке, вызывает мода центра масс (МЦМ), когда все ионы осциллируют синфазно в направлении оси ловушки. Цирак и Цоллер [156] показали, как можно использовать МЦМ для передачи квантовой информации между ионами, которые могут находиться в далеко отстоящих положениях внутри цепочки.

Прежде всего, колебание МЦМ должно быть охлаждено в основное квантово-механическое состояние. Этого можно добиться при помощи техники сателлитного охлаждения, описанной в разд.5.3.3. Кван-

товая информация затем может быть передана от любого иона в цепочке к МЦМ с помощью следующей процедуры. Один ион селективно облучается сфокусированным лазерным пучком и после π-импульса, настроенного на резонанс первого длинноволнового колебательного сателлита, внутреннее состояние этого иона записывается на внешнее (колебательное) состояние ионной цепочки (см. Рис.5.22a). В результате основное и первое возбужденное состояния колебания МЦМ оказываются в суперпозиции нижнего и верхнего состояний кубита, который изначально представлял собой ион. Благодаря коррелированному движению в МЦМ все ионы цепочки совершают одинаковое колебательное движение и, следовательно, несут одинаковую квантовую информацию. Задача построения квантового логического элемента, т.е. изменения состояния иона в соответствии с состоянием другого иона, таким образом, сводится к задаче изменения ионного состояния, в соответствии с колебательным состоянием МЦМ (см. Рис.5.22b). Подробнее это будет объяснено в следующем разделе. Колебание ионов можно представить как квантовую шину, связывающую кубитовые регистры вдоль цепочки. После того, как завершена такая операция на втором ионе, этап (a) должен быть обращен, чтобы возвратить колебательную моду в ее основное состояние и в тоже время вернуть первый ион в его начальное состояние.

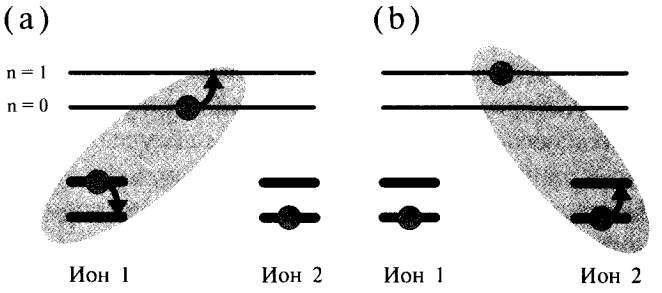


Рис. 5.22. Колебательная мода иона как квантовая шина данных. (a) с первым лазерным импульсом состояние иона 1 записывается в МЦМ; (b) состояние иона 2 изменяется в соответствии с состоянием МЦМ.

5.3.8 *Двух-битовые логические элементы и квантовый компьютер на ионных ловушках*

Существенный шаг предложения Цирака и Цоллера по построению ионно-ловушечного квантового компьютера состоит в реализации двухбитового квантового логического элемента (ЛЭ) на колебательном состоянии МЦМ и внутреннего состояния иона, как внутренних кубитов. В дальнейшем будут рассматриваться логические элементы, в

которых колебательная мода служит контрольным битом, обуславливающим изменение состояния иона – мишени.

Наиболее простыми считаются ЛЭ, у которых только одна комбинация базисных состояний приводит к изменению состояния выхода. Это случай так называемых фазовых ЛЭ, в которых волновая функция системы испытывает сдвиг фаз на π (изменение знака), если оба входных кубита находятся в верхнем состоянии и остается неизменной во всех других случаях. Чтобы осуществить изменение знака волновой функции, достаточно приложить к иону 2π-импульс. Для получения требуемой условной динамики импульс должен быть настроен в резонанс с переходом, связывающим только верхнее внутреннее состояние иона. Это требует наличия дополнительного электронного уровня, имеющего другую зеемановскую структуру. Условная зависимость от колебательного состояния достигается при настройке на первый коротковолновый МЦМ-сателлит, что вызывает переход, если имеется по крайней мере один колебательный квант. Заметим, что при построении таких схем может быть возбуждено не более одного колебательного кванта.

Возможны и другие ЛЭ при сочетании фазового ЛЭ с переворотом единичного кубита. В качестве примера приведем ЛЭ контролируемое-НЕ (CNOT) (см. разд.5.2.12), где бит-мишень обращает свое состояние, в зависимости от состояния управляющего бита. Это может быть достигнуто при воздействии $\pi/2$-импульса до и после фазового ЛЭ, что соответствует временному изменению вычислительного базиса на $|g\rangle \pm |e\rangle$. Логический элемент CNOT для единичного кубита, при использовании его колебательной моды в качестве управляющего бита, был экспериментально продемонстрирован в [211].

В некоторых случаях может быть полезным получение ЛЭ CNOT непосредственно, например, когда в наличии нет подходящих вспомогательных уровней в структуре электронных состояний. Для этого можно использовать тот факт, что связь внутренних и внешних степеней свободы нелинейно зависит от числа возбужденных колебательных квантов [233]. При подходящих параметрах резонансный импульс будет воздействовать либо как 2π-импульс, если система находится в нижнем колебательном состоянии, либо в качестве π-импульса, когда имеется один колебательный квант, причем только в последнем случае состояние иона будет обращено.

5.3.9 Чтение кубитов

При завершении квантового вычисления необходимо прочитать результат этого вычисления, т.е. определить состояние регистра кубитов. Очевидно, что этот шаг подразумевает проицирование состояния ионов в базисе состояний, используемом для детектирования.

Квантовый компьютер на ионных ловушках имеет то преимущество, что чтение происходит почти со 100%-ой вероятностью детектирования при использовании метода, который впервые применялся для детектирования квантовых скачков в единичных ионах [234] (см.разд. 5.2.8). Каждый ион последовательно освещается лазером, настроенным на быстрый переход, связанный только с одним состоянием кубита; при этом регистрируется возникающая флуоресценция (рис.5.23). Наличие рассеянного света свидетельствует о заселенности связанного состояния, отсутствие флуоресценции – о заселении ортогонального состояния. Суперпозиция состояний может быть исследована при перевороте кубита перед детектированием.

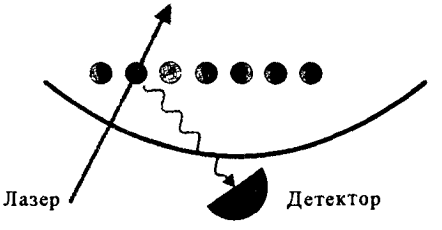


Рис. 5.23. Измерение состояний ионных кубитов. К каждому иону имеется доступ лазерного пучка, настроенного на переход чтения (см рис. 5.21а) и запись флуоресценции.

5.3.10 Заключение

В предыдущих разделах мы остановились на принципах действия ионных ловушек и их применениях в задачах выполнения квантовых вычислений.

В настоящее время цепочка ионов в линейной ловушке представляется наиболее обещающим кандидатом для демонстрации основной концепции квантового компьютера. Главные преимущества такой системы – большие времена декогерентности внутренних состояний ионов и возможность приготовления, когерентного контроля и чтения состояний кубитов с помощью лазерных импульсов. Среди квантовых вычислительных схем, недавно реализованных экспериментально, ионные ловушки имеют, по крайней мере теоретически, наибольший потенциал для выполнения масштабирования, чтобы создать достаточно длинные кубитовые регистры для запуска полезных квантовых алгоритмов.

В реально осуществимом ионно-ловушечном квантовом компьютере размер вычислений, которые могут быть выполнены, ограничивается чисто практическими проблемами. Флуктуации электромагнитного поля и столкновения с остаточным газом в вакуумной камере могут привести к скорости потери когерентности большей, чем

скорости радиоактивного распада внутренних состояний иона. Еще более разрушительным фактором является декогерентность колебательных состояний ионной цепочки. Для единичного иона $^{198}Hg^{+}$ переход с основного колебательного уровня происходит за 0.15с [214], в то время как в случае $^{9}Be^{+}$, измеренное время жизни составляет 1мс [211]. Экспериментальные результаты для ионов $^{40}Ca^{+}$ см. в [215]. Такие процессы устанавливают верхний предел на количество операций, выполняемых квантовым компьютером до потери когерентности. Однако, с точки зрения недавних экспериментальных результатов [212, 216], некоторые серьезные технические ограничения могут быть преодолены с использованием дышащих мод в качестве квантовой шины данных.

Существуют и другие проблемы при выполнение квантовых вычислений во время логических операций. Процессами, ухудшающими качество эволюции системы, являются неточность временных характеристик лазерных импульсов, погрешности в частотных расстройках а также интенсивностях и фазах лазерных пучков, отклонения от фокальной плоскости положений ионов. Однако, такие погрешности могут быть в конечном счете последовательно учтены с помощью методов коррекции ошибок и специальных протоколов.

Хотя количество ионов, которое может быть удержано в ловушке, должно быть ограничено размером ловушки и мощностью лазера, используемого для охлаждения, до сих пор цепочки только из двух ионов были успешно охлаждены в основное состояние движения [216]. В ближайшем будущем хотелось бы увеличить это число до нескольких десятков ионов, но необходимы тысячи кубитов и миллиарды лазерных импульсов для выполнения, к примеру, алгоритма Шора по факторизации больших чисел. Нам представляется, что в настоящее время это находится вне экспериментальных возможностей. Однако, ионные ловушки служат лучшими моделями для тестирования небольших сетей квантовых ЛЭ, также как и схем квантовой коррекции ошибок. В этом направлении ионные ловушки представляют собой идеальный объект для синтеза, манипуляций и апробирования перепутанных квантовых состояний цепочек ионов.

5.4. ЭКСПЕРИМЕНТЫ ПО ЯДЕРНОМУ МАГНИТНОМУ РЕЗОНАНСУ

Дж.А.Джонс

5.4.1 Введение

При ядерном магнитном резонансе (ЯМР) изучаются переходы между зеемановскими подуровнями атомных ядер в магнитном поле. На основе этого простого определения трудно представить себе, как ЯМР мо-

жет кого-либо заитересовать. Однако в действительности, ЯМР лежит в основе одного из наиболее важных спектроскопических методов, используемых в науках, занимающихся изучением молекул [235, 236]. Это происходит потому, что частоты сигналов ЯМР крайне чувствительны к детальному химическому окружению ядер, и таким образом, тщательное изучение ЯМР-спектра молекул позволяет определять их структуру.

ЯМР давно рассматривается как возможная технология для реализации квантовых компьютеров. На первый взгляд, эта идея представляется очень привлекательной, так как ядерные спины дают хороший источник кубитов, и казалось бы совершенно нетрудно построить квантовые логические элементы. В этом, однако, состоит основная проблема: очень сложно установить квантовый ЯМР-компьютер в фиксированное основное состояние, которое существенно необходимо для любых интересных вычислений. Эта проблема была недавно решена с использованием двух разных подходов [237-239], что способствовало быстрому прогрессу в этой области.

Из-за важности ЯМР для наук о молекулах, происходило интенсивное техническое развитие ЯМР спектрометров. Огромные суммы денег были затрачены на оптимизацию каждой их компоненты. В настоящее время коммерчески доступные спектрометры широко распространены и имеют параметры, близкие к теоретическим пределам. Современные спектрометры – это чрезвычайно сложные устройства, но управляются они крайне просто и при ничтожной помощи даже самые бестолковые теоретики должны быть в состоянии выполнить простые ЯМР-эксперименты.

5.4.2 Гамильтониан ЯМР

В наихудшем случае гамильтониан ЯМР имеет довольно сложный вид [236, 240, 241], но во многих случаях большинство сложностей могут быть проигнорированы. Во-первых, я буду рассматривать только ядра со спином 1/2 (такие, как ^{1}H, ^{13}C, ^{15}N, ^{19}F и ^{31}P), так как эти ядра не испытывают многих взаимодействий, которые происходят в ядрах с более высокими значениями спинов. Эти ядра также наиболее важны для реализации квантовых ЯМР компьютеров, так как двухспиновые состояния ядер со спином 1/2 представляют естественную двухуровневую систему для построения кубита. Во-вторых, я буду предполагать, что ЯМР-образец – это жидкость (обычно либо чистая жидкость, либо раствор). Быстрое молекулярное движение в жидкости сильно упрощает гамильтониан ЯМР, так как анизотропные взаимодействия могут быть заменены их изотропным средним значением,

которое часто обращается в нуль. ЯМР-сигналы от ядер со спином 1/2 в жидкостях обычно обладают довольно узким спектром, поэтому такие исследования часто называются методом ЯМР с высоким разрешением [242].

При ЯМР высокого разрешения особенно важны два типа взаимодействий. Первый из них – это, конечно, зеемановское взаимодействие. В присутствии магнитного поля B_z, направленного вдоль оси z, вырождение двух спиновых состояний ($I_z = \pm 1/2\hbar$) снимается из-за зеемановского взаимодействия

$$H = -\gamma I_z B_z \ , \tag{5.19}$$

где γ (гиромагнитное отношение) – постоянная, характеризующая ядро. Зеемановское расщепление соответствует частотам порядка 500 МГц для ядра ^{1}H в типичных для ЯМР магнитах; таким образом, ЯМР-эксперименты выполняются в радиочастотном диапазоне.

Использование традиционных методик пространственной локализации для разделения вкладов отдельных молекул практически неудобно, так как расстояние между молекулами (несколько ангстрем) мало по сравнению с длиной волны радиочастотного излучения; кроме того, отдельные молекулы совершают быстрое движение. Вместо этого детектируется общий сигнал от всех молекул сразу. Отсюда следует важное следствие для ЯМР-экспериментов – они выполняются не с отдельными спиновыми системами, а со статистическими ансамблями таких систем. Однако, можно различить вклады разных ядер в одной молекуле. Электроны, окружающие ядра, экранируют их от магнитного поля, изменяя гиромагнитное отношение[1]. Степень такой экранировки зависит от химического окружения ядра, следовательно, ядра в различном окружении имеют слегка отличающиеся частоты переходов.

Второй важный тип взаимодействия ЯМР высокого разрешения – скалярная связь (J-связь). Это не простое диполь-дипольное взаимодействие, которое усреднено по быстрому хаотическому движению молекул, а более тонкий эффект, связанный с контактным взаимодействием Ферми. Когда взаимодействие между двумя ядрами I и S мало по сравнению с разностью их ЯМР-частот, (слабая связь) гамильтониан взаимодействия принимает простой вид

$$\mathcal{H} = J_{IS} I_z S_z \ , \tag{5.20}$$

где J_{IS} – константа спин-спинового взаимодействия, зависящая от особенностей молекулярной структуры. Эта связь непосредственно на-

[1] Чаще говорят об изменении поля, действующего на ядра, которое в случае экранировки отличается от внешнего поля H (*Прим. переводчика*).

блюдается в ЯМР-спектрах в виде расщепления (величина расщепления J_{IS}) сигналов ЯМР, отвечающих каждому ядру.

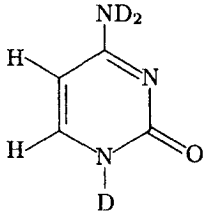


Рис. 5.24. Структура частично дейтерированного цитозина, полученного при растворении цитозина в D_2O; три протона, связанные с ядрами азота, заменяются на ионы дейтерия, оставляющие два ядра ^1H в качестве изолированной спиновой системы (все другие ядра игнорируются).

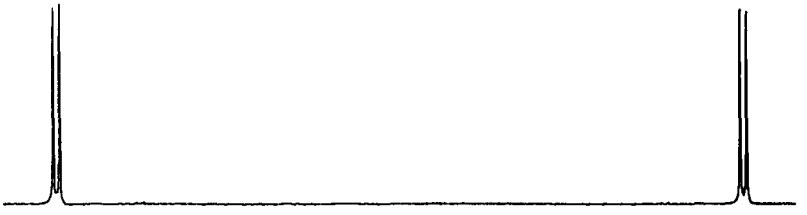


Рис. 5.25. ЯМР спектр ^1H в частично дейтерированном цитозине. Каждая пара линий это ЯМР-сигнал от двух ядер ^1H.

Простой пример: На Рис. 5.24 показана химическая структура дейтерированного цитозина. Цитозин это один из четырех «базисных» элементов, которые используются при кодировке информации в ДНК и недавно был использован для реализации квантового компьютера [243]. Для этого три ядра водорода в молекуле были замещены дейтерием, что просто достигается при растворении цитозина в D_2O. Спектр ^1H такой молекулы, полученный на 500-мегагерцовом ЯМР-спектрометре, показан на Рис. 5.25. Каждое из двух ^1H ядер дает пару сигналов, называемых дублетом. Два дублета находятся на частотах порядка 500 МГц, расстояние между ними равно 763 Гц; тонкое расщепление внутри каждого дублета (7.2 Гц) вызвано спиновым взаимодействием между ядрами.

5.4.3 Построение квантового компьютера на ЯМР

Наиболее общий подход к выполнению квантовых вычислений основан на квантовых логических схемах, хотя рассматривались и некоторые другие модели. Такой квантовый компьютер должен иметь четыре основных элемента. Первый из них – кубит – это просто два спино-

вых состояния ядра (со спином 1/2), представляющие идеальную двухуровневую систему. Оставшиеся элементы выглядят несколько сложнее.

Квантовые логические элементы. Квантовые логические схемы получаются при взаимодействии кубитов с квантовыми ЛЭ. Хотя существует множество различных ЛЭ, хорошо известно, что любой ЛЭ может быть построен с использованием соответствующей комбинации одно- и двух-кубитовых ЛЭ [224]. Одно-кубитовые ЛЭ соответствуют поворотам единичного спина в его гильбертовом пространстве, что просто осуществляется с помощью ВЧ полей. Двух-кубитовые ЛЭ, такие как ЛЭ «контролируемое-НЕ» – более сложные, так как предполагают наличие некой динамики и, следовательно, требуют определенного взаимодействия между двумя битами. Скалярное ЯМР-взаимодействие (J-связь) при ЯМР хорошо подходит для этой цели: поскольку оно не имеет точно того вида, который необходим для традиционных управляемых ЛЭ, оно может быть получено из одно-кубитовых ЛЭ [245]. Например, ЛЭ «контролируемое-НЕ» получается при помещении ЛЭ «управляемого фазового сдвига» (который осуществляет преобразование $|11\rangle \rightarrow -|11\rangle$, оставляя другие базовые состояния неизменными) между парой одно-кубитовых ЛЭ Адамара, действующих на кубит-мишень. Управляемый фазовый сдвиг, сам по себе, можно получить, совмещая свободную эволюцию при скалярном взаимодействии (которое осуществляет вращение фазы двух кубитов), с одно-кубитовым ЛЭ фазового сдвига [245].

Оператор сброса. Квантовые ЛЭ преобразуют кубиты из одного состояния в другое. Очевидно, что предпочтительнее, если кубиты начинают движение из некоторого чистого входного состояния. Практически, достаточно найти какой-нибудь метод, позволяющий достигнуть какое-нибудь одно чистое состояние, так как другие начальные состояния тогда можно получить с помощью одно-битовых ЛЭ. Очевидный выбор начального состояния состоит в установлении всех кубитов в $|0\rangle$, что и отвечает операции сброса.

В принципе, сброс должен осуществляться просто, потому что он переводит квантовый компьютер в его основное энергетическое состояние, чего можно добиться каким-нибудь процессом охлаждения. К сожалению этот подход не годится для ЯМР, так как энергетическое расщепление между зеемановскими подуровнями мало, по сравнению с больцмановской энергией, при любых разумных температурах. При комнатной температуре энергетическая щель так мала, по сравнению с kT, что населенности всех этих состояний почти одинаковы при небольшом отклонении от усредненной (порядка 10^4). От усредненной населенности сигнал ЯМР не на-

блюдается, т.к. сигналы от разных молекул компенсируются, но слабый сигнал, вызванный отклонениями от средней населенности, все-таки присутствует.

Для молекулы, содержащей единичное изолированное ядро, т.е. компьютера с единичным кубитом, эффективное состояние $|0\rangle$ достигается сравнительно просто. При термодинамическом равновесии отклонение от равных населенностей лишь слегка больше в (низкоэнергетичном) состоянии $|0\rangle$ по сравнению с (незначительно более высоким по энергии) состоянием $|1\rangle$. К сожалению, это простое приближение не работает для больших систем, т.к. в них картина изменения населенностей гораздо более сложная и не совпадает с желаемой. Такая очевидная неспособность выполнения операции сброса ставила ЯМР в ряд неосуществимых квантовых компьютерных технологий в течение многих лет.

К концу 1996 года было выработано два независимых подхода для решения этой проблемы. В первом подходе, исследованном Кори и соавторами [237, 238], используется сложная последовательность ЯМР-импульсов, чтобы изменить населенности различных спиновых состояний; в конечном счете реализуется нужная картина и, таким образом, состояние равновесия сводится к желаемому начальному состоянию. В альтернативном подходе разработанном Чуангом и Гершенфельдом, осуществляется разделение спиновой системы на много различных подсистем [239, 246]. В пределах этих подсистем картина равновесия населенностей имеет необходимый вид, т.е. достигается желаемое начальное состояние. Несмотря на то, что этот подход теоретически более элегантен, с практической точки зрения он трудно реализуем, поэтому широко не использовался. Другие подходы, например, временно́е усреднение [247], концептуально близки к подходу Кори и др. и не будут в дальнейшем здесь рассматриваться. Детальное сравнение различных методов было проведено Хэвелом и соавторами [248].

Выход. В итоге необходимо иметь какой-нибудь способ для чтения окончательного результата. Обычно это получается при чтении значений одного или нескольких кубитов, которые закончили процесс вычисления в основных состояниях. В квантовом компьютере на ЯМР это соответствует определению того, является ли населенность состояния $|0\rangle$ выше, чем в состоянии $|1\rangle$, или наоборот. На практике невозможно определить эти населенности непосредственно, но можно просто выполнить эквивалентное измерение, прикладывая $\pi/2$-импульс ВЧ поля. При этом создается когерентная суперпозиция состояний $|0\rangle$ и $|1\rangle$, которая затем осциллирует в магнитном поле. Относительные населенности могут быть определены при наблюдении ве-

личины и фазы такого осциллирующего сигнала. Абсолютная фаза его смысла не имеет, но можно добавить опорный сигнал, так что останется измерить лишь относительные фазы.

В некоторых квантовых алгоритмах используется два и более кубитов и в этом случае существует два разных подхода. Первый подход состоит в возбуждении только одного из соответствующих спинов; при этом состояния других спинов могут быть выявлены проверкой мультиплетной структуры наблюдаемого спина. В противоположность этому, можно возбудить все спины и наблюдать их одновременно; в таком случае состояние каждого спина определяется непосредственно из фазы ЯМР сигнала.

Квантовые компьютеры на ЯМР имеют потенциальное преимущество перед другими технологиями, которое состоит в том, что нет нужды работать с собственными состояниями. Вместо этого можно непосредственно наблюдать некоторые суперпозиционные состояния. Такая возможность возникает из-за полного ансамблевого усреднения в любом ЯМР-измерении. В то время как измерения системы единичных кубитов вызывает редукцию суперпозиционного состояния, такого не происходит при ансамблевом усреднении. Таким образом, например, можно наблюдать две дополнительные величины непрерывно и одновременно. Этот тип операций мог бы оказаться полезным в будущих экспериментах.

5.4.4 Проблема Дойча

Идеи, обсуждавшиеся выше, могут быть проиллюстрированы при использовании квантового компьютера на ЯМР, спроектированного для выполнения алгоритма, решающего проблему Дойча [138, 249]. Эта проблема подробно обсуждается в разд. 4.3.4 и здесь мы лишь напомним ее суть. Рассмотрим бинарную функцию

$$f(x): B \mapsto B \ , \tag{5.21}$$

и предположим, что существует соответствующий оператор U_f, такой, что

$$|x\rangle|y\rangle \xrightarrow{U_f} |x\rangle|y \oplus f(x)\rangle \ . \tag{5.22}$$

Очевидно, что возможно построить квантовые схемы по определению $f(0)$ и $f(1)$, как показано на Рис. 5.26a. Проблема Дойча состоит в определении $f(0) \oplus f(1)$ при однократном применении оператора U_f (соответствующим единственному акту определения f). Это невозможно сделать на классическом компьютере, но выполняется на квантовом при использовании схемы, показанной на Рис. 5.26b. Такая схема была реализована на нашем двух-кубитовом ЯМР-квантовом компьютере, основанном на частично дейтерированном цитозине [243]

(похожие результаты были также получены Чуангом и др. при использовании ЯМР-квантового компьютера, основанного на хлороформе [250]). В нашем компьютере каждый дублет отвечает сигналу от одного кубита. Значение кубита определяется из фазы соответствующего сигнала: положительный сигнал соответствует кубиту в состоянии $|0\rangle$, тогда как отрицательный сигнал – кубиту в состоянии $|1\rangle$.

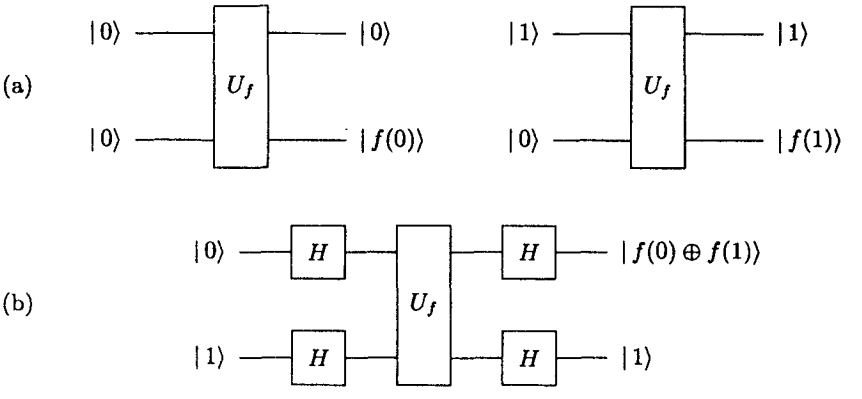


Рис. 5.26. (a) Квантовые схемы для определения $f(0)$ и $f(1)$ для бинарной функции. (b) квантовая схема для определения $f(0) \oplus f(1)$ при однократном воздействии оператора U_f (проблема Дойча). H представляет единичный кубит ЛЭ Адамара.

Как уже говорилось, абсолютная фаза ЯМР-сигнала смысла не имеет, так как зависит от множества экспериментальных факторов. Относительные фазы, однако, очень важны. Можно получить «абсолютные» фазы настройкой спектра таким образом, что фаза опорного сигнала станет правильной. Относительные фазы сигналов в двух разных экспериментах тоже могут иметь смысл, если эти эксперименты выполняются в идентичных условиях, так что можно использовать опорный сигнал из одного эксперимента для корректировки сигналов из другого. Именно такой подход используется при получении результатов, обсуждаемых ниже.

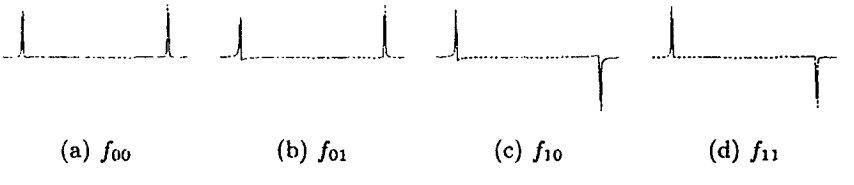


Рис. 5.27. Экспериментальные результаты, полученные на ЯМР-квантовом компьютере по определению $f(0)$; результат показан для каждой из четырех возможных бинарных функций f.

Экспериментальные результаты для классического алгоритма по определению $f(0)$ показаны на Рис. 5.27. В этом алгоритме левая пара линий (соответствующая первому кубиту) показывает входное состояние, а правая (соответствующая второму кубиту) показывает значение выхода. Результаты демонстрируются для четырех возможных бинарных функций, перечисленных в таблице 5.1. Как и ожидалось, сигналы, расположенные в парах слева, всегда положительны – они указывают на значение входной величины (0), в то же время сигналы, расположенные в парах по правую сторону, положительны, когда $f(0) = 0$ (для f_{00} и f_{01}) и отрицательны, когда $f(0) = 1$ (для f_{10} и f_{11}). Абсолютная фаза спектров неизвестна, но эта проблема решается при подстройке фазы спектра (а) таким образом, чтобы все левые сигналы в парах стали положительными, а затем используется точно такая же фазовая коррекция во всех остальных спектрах.

Таблица 5.1. Четыре возможные бинарные функции, отображающие один бит на другой.

x	$f_{00}(x)$	$f_{01}(x)$	$f_{10}(x)$	$f_{11}(x)$
0	0	0	1	1
1	0	1	0	1

На обсуждаемых рисунках не показана тонкая структура каждого дублета, но это не очень важно, так как при данной реализации квантового компьютера все линии мультиплета должны иметь один и тот же знак, что и наблюдается в действительности. В идеале этот знак был бы просто положительным или отрицательным, но на практике, наблюдаемые формы линий выглядят немного сложнее. Кроме того, все линии должны были бы иметь одну и ту же высоту, тогда как экспериментальные результаты показывают их существенные различия. Такие возмущения формы линий и высот возникают из-за ошибок в компьютере. Большинство этих ошибок – это систематические ошибки, которые появляются из-за неидеальности выполнения операций квантовыми логическими элементами. Влияние таких ошибок можно уменьшить путем тщательной оптимизации последовательности импульсов ЯМР, используемых при работе логических элементов.

Такой же алгоритм может быть использован для определения $f(1)$: все что нужно сделать – это изменить входную величину. Результаты такого подхода показаны на Рис. 5.28. В этом случае левые сигналы пар всегда отрицательны – они показывают новую входную величину

(1), правые же сигналы пар могут быть либо отрицательными, либо положительными. Как и ожидалось этот сигнал положителен, если $f(1) = 0$ (для f_{00} и f_{10}) и отрицателен, если $f(1) = 1$ (для f_{01} и f_{11}). Заметим, что была использована такая же фазовая коррекция, как и в примере, показанном на Рис. 5.27; это подтверждает, что относительные фазы могут быть определены для двух различных экспериментов, выполненных при идентичных условиях.

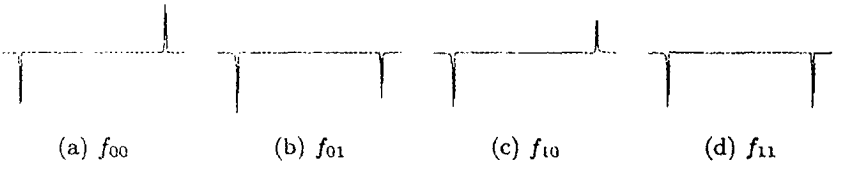


Рис. 5.28. Экспериментальные результаты, полученные на ЯМР-квантовом компьютере по определению $f(1)$; результат показан для каждой из четырех возможных бинарных функций f.

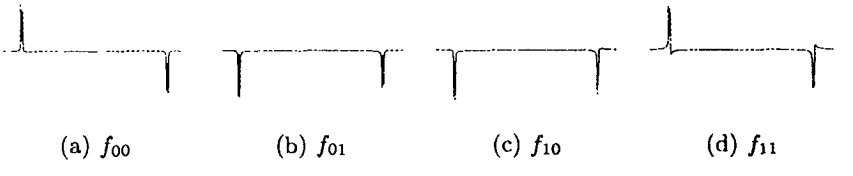


Рис. 5.29. Экспериментальные результаты, полученные на ЯМР-квантовом компьютере по определению $f(0) \oplus f(1)$ (проблема Дойча); результат показан для каждой из четырех возможных бинарных функций f.

И, наконец, такой квантовый компьютер можно использовать и при реализации алгоритма, решающего проблему Дойча (определение $f(0) \oplus f(1)$). Результаты показаны на Рис. 5.29. В этом случае входного бита нет, так как квантовый компьютер использует суперпозицию двух возможных входов, и ответ записывается в виде фазы левых и правых сигналов пар. Второй кубит является просто вспомогательным битом; оба начинают и заканчивают вычисление в состоянии $|1\rangle$. Как и ожидалось, правые сигналы всегда отрицательны. В то время как левые – положительные для f_{00} и f_{11} (для которых $f(0) \oplus f(1) = 0$), и отрицательные для f_{01} и f_{10} (для которых $f(0) \oplus f(1) = 1$).

5.4.5 Квантовый поиск и другие алгоритмы

После открытия возможности эффективной генерации начальных состояний, квантовые компьютеры, основанные на ЯМР, стали быстро развиваться. Двух-кубитовые компьютеры уже использовались при

реализации квантового алгоритма поиска Гровера в пространстве двух кубитов [251, 253]. Этот алгоритм позволяет обнаружить один объект при поиске среди четырех объектов после единственного запроса; квантовый компьютер начинает выполнение алгоритма в состоянии $|00\rangle$ и заканчивает в состоянии, соответствующем одному из возможных ($|00\rangle$, $|01\rangle$, $|10\rangle$ или $|11\rangle$). Такой алгоритм был реализован в нашем квантовом компьютере на цитозине [252]; результаты приведены на Рис. 5.30. Эти результаты немного лучше, чем опубликованные ранее [252]; они были получены при использовании модифицированной, по сравнению с [254], импульсной последовательности.

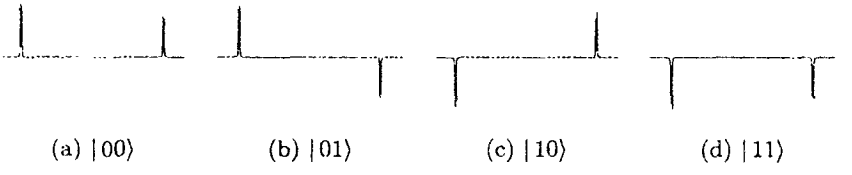


Рис. 5.30. Экспериментальные результаты, полученные на ЯМР-квантовом компьютере, выполняющего квантовый поиск Гровера в пространстве двух кубитов; результат показан для каждого из четырех возможных исходов.

Пока квантовые компьютеры на ЯМР способны выполнять простой поиск Гровера, при котором может быть найден только один объект. Трудности возникают в общем случае, когда критерию поиска должно удовлетворять более одного объекта. В этом случае обычный квантовый компьютер будет выбирать один из возможных вариантов случайным образом, тогда как компьютер на ЯМР – некоторый вид ансамблевого усреднения по всем вариантам; эту проблему будет трудно или даже невозможно преодолеть имея ансамблевый результат. Возможный путь ее решения лежит в использовании аналогичного подхода – приближенного квантового счета [254].

Были также исследованы и трех-кубитовые системы; они, в основном, использовались при демонстрации интересных квантовых явлений, таких как ГХЦ-состояний [255, 256], простых протоколов коррекции ошибок [257, 259] и телепортации [259]. Однако, они были использованы и при реализации трех-кубитового алгоритма Дойча – Джозса [260]. Частичная демонстрация этого алгоритма в пяти-кубитовой системе приводится в [261].

5.4.6 Перспективы

Существует несколько основных проблем, которые приводят к ограничению размеров реальных квантовых компьютеров на ЯМР, осно-

ванных на имеющихся подходах. Наиболее остро эти проблемы связаны с экспоненциальными потерями интенсивности сигнала при увеличении числа кубитов, сопровождаемыми эффектами декогерентности. В действительности эти эффекты вряд ли являются существенно важными так как имеются другие, выступающие, по всей видимости, на первый план. Полезно, тем не менее, обсудить и те и другие, а также пути их устранения.

Экспоненциальное уменьшение сигнала. Экспоненциальные потери сигнала с увеличением числа кубитов возникают в результате необходимости выделения эффективного чистого состояния из тепловой равновесной матрицы плотности. Добавление дополнительного кубита означает добавление дополнительного спина, удвоение числа спиновых состояний системы и, таким образом, удвоение числа путей, по которым может произойти переворот состояния любого спина. Выделение эффективного чистого состояния эквивалентно селекции только одного из этих возможных переходов с последующей потерей интенсивности сигнала [262]. Заметим, что эта проблема относится не только к методу ЯМР, а возникает и при любом ансамблевом квантовом вычислении, работающем при высоких температурах ($\Delta E \ll kT$).

Очевидно, что такое экспоненциальное падение сигнала является потенциальным пределом, но на практике его важность преувеличена. Спектры ЯМР могут быть получены при очень высоком отношении сигнл-шум (спектр, показанный на Рис. 5.24, характеризуется отношением сигнал-шум 800), и таким образом, потери сигнала становятся серьезной проблемой для ЯМР-компьютеров, содержащих десять или более кубитов. Можно увеличить отношение сигнал-шум очень простым способом – усреднением сигнала, увеличением размера образца или при использовании более тонких методов, таких как оптическая накачка [263]. Другой подход, предложенный Шульманом и Вацирани [264] состоит в применении вычислительных методов для очищения набора кубитов с низким качеством [264]. Практически нереально использовать этот подход непосредственно для тепловых ансамблей; но при комбинировании с другими методами по увеличению степени начальной поляризации, например, с методом оптической накачки, он может оказаться полезным.

Декогерентность. Декогерентность, (т.е. превращение когерентной суперпозиции в некогерентную смесь при случайных процессах) является другой потенциальной проблемой, которая представляется общей для всех реализаций квантовых компьютеров. Любая квантовая суперпозиция имеет характерное время декогерентности и надо быть уверенным, что любые вычисления выполняются за время, не слишком большое, по сравнению с временем декогерент-

ности (хотя техника коррекции ошибок позволяет расширить этот временной масштаб). В квантовых компьютерах на ЯМР это время, вообще говоря, связано с временем спин-спиновой релаксацией T_2, хотя это и является упрощением, так как T_2 – это время декогерентности единичного спина, а время декогерентности много-спиновой системы может сильно от него отличаться. Тем не менее T_2 действительно дает достаточное приближение для соответствующей временной шкалы, которая для современных ЯМР-компьютеров (основанных на небольших молекулах в растворе) составляет порядка нескольких секунд.

Полезным для квантового компьютера параметром служит не само по себе время декогерентности, а отношение между временем декогерентности и временем, требуемым для выполнения квантовой логической операции. Для простых двух-кубитовых ЛЭ, таких как контролируемое-НЕ, это время сравнимо с обратной константой связи скалярного спин-спинового взаимодействия (около 5 – 150 мс); ясно, что за это время можно выполнить тысячи логических операций. В действительности существуют системы с гораздо большими значениями T_2, но такие системы нельзя использовать для построения квантовых компьютеров на ЯМР, т.к. они не обладают спин-спиновыми взаимодействиями, необходимыми для реализации квантовых ЛЭ.

Другие проблемы. Гораздо более важными, чем любая из обсуждавшихся выше проблем, являются две другие проблемы – селективная адресация спинов и рост сложности ЛЭ с увеличением числа спинов.

Проблему селективной адресации различных спинов понять довольно просто. В традиционных квантовых компьютерах отдельные кубиты различаются по пространственным положениям в соответствующих физических системах, но такой подход не может быть использован в ЯМР. Вместо этого кубиты (соответствующие им спины) различаются по частотам ЯМР-переходов. К сожалению этот частотный диапазон довольно узок (обычно порядка нескольких кГц) и трудно осуществить абсолютно селективные возбуждения спинов с близкими частотами [265]. Это один из главных источников возмущений, четко наблюдающийся в экспериментальных спектрах (Рис.5.27 – 5.30). Очевидно, что эта проблема станет более серьезной в системах с большим числом спинов, т.к. труднее будет убедиться, что все спины отделены достаточными частотными интервалами.

Из-за этого большинство авторов предпочитает исследовать гетероядерные спиновые системы. Такие как ЯМР-компьютеры, осно-

ванные на спиновой паре ^{1}H – ^{13}C в хлороформе. Это гораздо проще, чем соответствующий гомоядерный вариант, т.к. частоты переходов двух спинов теперь отделены на сотни МГц, и селективное спиновое возбуждение становится тривиальным. Такой подход содействовал ускоренному прогрессу двух- и трех-спиновых систем, но не может быть автоматически расширен, т.к. существует только небольшое количество различных подходящих ядер. В любом случае ЯМР-спектрометры не могут работать более чем с двумя – тремя различными ядрами одновременно. Таким образом, любой квантовый компьютер на ЯМР, включающий большое количество кубитов, столкнется с проблемой селективной адресации спинов.

Вторая проблема – более тонкая; она касается увеличения сложности квантовых ЛЭ в многоспиновых системах. В идеале было бы возможно взять двух-кубитовый ЛЭ, разработанный для двух-кубитового компьютера и использовать его в трех- или четырех-кубитовом компьютере без серьезных усовершенствований. Для квантовых компьютеров на ЯМР это можно строго доказать. Взаимодействия, образующие базис ЛЭ, в основном спин-спиновая связь, являются частью полного гамильтониана ЯМР, под воздействием которой спиновая система эволюционирует при отсутствии специфического возбуждения. Квантовые ЛЭ образуются при модуляции вклада различных компонент полного гамильтониана, что дает эффективный гамильтониан, который имеет желаемый вид. Этот процесс, однако, становится более сложным при наличии дополнительных кубитов, т.к. необходимо модулировать не только взаимодействия между спинами, включенными в этот ЛЭ, но и любые взаимодействия с дополнительными спинами, чтобы эффективно их исключать [266]. В наименее благоприятном случае система из N спинов содержит $1/2\ N(N+1)$ одно- и двух-спиновых взаимодействий в гамильтониане, из которых только три отвечают за образование любого отдельного двух-кубитового ЛЭ. Хотя эта проблема не является столь серьезной, как это могло показаться сначала [267-269], все же исключение этих нежелательных взаимодействий может оказаться самой трудной задачей при построении квантовых компьютеров на ЯМР, работающих на заметном числе кубитов.

Альтернативные подходы. Имея в виду те потенциальные проблемы, которые были перечислены выше, некоторые исследователи начали думать о принципиально новых подходах при построении квантовых компьютеров на системах с ЯМР. До сих пор ни одна из таких идей не была продемонстрирована; все они имеют мало общего с «традиционными» квантовыми компьютерами.

Одна общая особенность большинства таких умозрительных схем

состоит в использовании твердых тел вместо жидкостей. Это имеет много существенных следствий, важных при исследовании ЯМР, причем как полезных, так и не очень. Индивидуальные молекулы в твердых образцах будут оставаться приблизительно в стационарных состояниях и поэтому для селективного возбуждения отдельных спинов, в принципе, могла бы использоваться техника пространственной локализации. Большая длина волны ВЧ излучения препятствует прямому доступу, но методы, развитые для получения ЯМР-изображений[2] [270], действительно позволяют проводить пространственную дискриминацию спинов. При таком подходе, однако, будет трудно достигнуть атомного разрешения, отчасти из-за трудностей при получении достаточно сильных градиентов поля, а также из-за низкой чувствительности ЯМР, непозволяющей непосредственно детектировать отдельные спины [270]. Расчеты показывают, что предельное разрешение должно составлять 1 мкм, поэтому придется использовать кластеры спинов, а не отдельные ядра.

Второе следствие продвижения в сторону твердотельных структур состоит в значительном изменении вида гамильтониана ЯМР, так как анизотропные взаимодействия здесь больше не усредняются. В частности, прямые диполь-дипольные связи между спинами дают наибольший вклад в спин-спиновое взаимодействие. Такие связи гораздо сильнее, чем скалярное взаимодействие и позволяют реализовывать более быстрые ЛЭ, но имеют тот недостаток, что каждый спин связан со всеми остальными близлежащими спинами. Все это создает трудности при использовании таких взаимодействий в селективных способах, необходимых для работы ЛЭ, и кроме того, может приводить к быстрой декогерентности.

Кейн [271] недавно сформулировал весьма оригинальный подход, позволяющий решить эти проблемы, комбинируя твердотельный ЯМР с традиционной технологией, применяемой при изготовлении кремниевых микросхем. Этот подход предусматривает использование атомов ^{31}P в кремниевой матрице с электростатическими ЛЭ, как для контроля за возбуждением отдельных спинов, так и для модуляции взаимодействий между ними. Детектирование отдельного спина могло бы быть осуществлено при использовании ядерного спина для контроля за процессом переноса единичного электрона. Хотя это предложение сильно опережает возможности существующих технологий, похоже, что многие требования, которые к нему предъявляются, будут выполнены в течение следующих десяти лет.

[2] Т.н. ЯМР-томография (*Прим. переводчика*).

5.4.7 Перепутывание и смешанные состояния

Недавно была высказана мысль о том, что ЯМР вообще не может рассматриваться в качестве квантово-механического метода! Когда выносится такой вердикт необходимо помнить, что термин «квантово-механический» используется здесь в смысле «проявляющий неклассические свойства». ЯМР-эксперименты проводятся при высоких температурах (kT имеет большое значение, по сравнению с расщеплением между уровнями), матрица плотности, описывающая систему ядерных спинов, всегда близка к максимально смешанному состоянию, а такие состояния всегда могут быть представлены [272] в виде смеси независимых состояний (т.е. состояний, не содержащих перепутывания между различными ядрами). Так как ЯМР-состояния представляются без привлечения перепутывания, они могли бы быть описаны классическими моделями (хотя такие классические модели будут очень сложными). Однако, хотя классические модели и могут привлекаться для описания отдельного ЯМР-состояния, непонятно как такие модели будут описывать эволюцию состояния во время ЯМР-эксперимента [273]. Мотивировка таких заключений остается спорной и непонятной.

5.4.8 Следующие несколько лет

Метод ЯМР дает наиболее мощную технологию для реализаций квантовых компьютеров, доступных в настоящее время и, возможно, будет оставаться таковой в ближайшие годы. Несколько небольших квантовых компьютеров на ЯМР уже были построены, на их основе реализованы квантовые алгоритмы.

В последующие несколько лет кажется вероятным, что квантовые компьютеры на ЯМР с тремя – пятью кубитами станут тривиальными и что исследоваться будут все более сложные системы. Однако, без кардинальных изменений в имеющихся подходах, вряд ли будут сконструированы ЯМР-системы, состоящие более чем из десяти кубитов. Такие подходы, как твердотельный ЯМР-компьютер Кейна, в будущем обещают очень много.

6

Квантовые сети и многочастичное перепутывание

6.1 Введение

В предыдущих главах были рассмотрены основные концепции квантового перепутывания. В настоящей главе мы обсудим более детально несколько вопросов, связанных с квантовым перепутыванием. В разделе 6.2. рассматривается схема по установлению перепутывания между атомами и пространственно разнесенными узлами, посредством обмена фотонами. С помощью такого метода может быть построена квантовая сеть, объединяющая в себе достоинства систем заряженных атомов (ионов), характеризующихся большими временами хранения и возможностью осуществлять локальный доступ к квантовым состояниям, с преимуществами квантовой оптики, основанными на быстром и надежном обмене информацией на больших расстояниях.

Раздел 6.3 посвящен перепутанным состояниям более чем двух частиц. Такие состояния важны не только в области квантовой информации. Они были введены изначально Гринбергом, Хорном и Цайлингером (ГХЦ), чтобы рассмотреть конфликт, возникший между локальным реализмом и квантовой механикой, с наиболее конструктивной точки зрения. (Такой конфликт появляется при интерпретации парадокса Эйнштейна – Подольского – Розена (ЭПР)). Показано, как можно генерировать трех-фотонное ГХЦ-перепутывание и почему перепутывание между более чем двумя частицами проявляет квантовые свойства, полностью несовместные с любой (классической) точкой зрения, основанной на локальном реализме.

В разделе 6.4 показывается, что перепутывание между более чем двумя частицами представляет собой весьма нетривиальное понятие. В действительности, такое перепутывание не может быть установлено однозначно. Вводятся количественные меры перепутывания, а также рассматриваются близкие темы как, например, очищение перепутывания и относительная энтропия перепутывания.

6.2 Квантовые сети I; перепутывание частиц, находящихся в разных пространственных областях

Х.-Дж.Бригель, С.Дж. ван Энк, Дж.И.Цирак, П.Цоллер

6.2.1 Связывание атомов и фотонов

Квантовые сети состоят из пространственно разнесенных узлов, в которые помещены индивидуально управляемые кубиты, и квантовых коммуникационных каналов, соединяющих эти узлы. Обмен информацией внутри сети выполняется путем пересылки кубитов по каналам. Физически такие сети могли бы состоять, например, из кластеров или захваченных в ловушки ионов, представляющих собой узлы, а также оптических волокон или каких-нибудь устройств, передающих фотоны, что обеспечивало бы реализацию квантовых каналов, как показано на Рис.6.1.

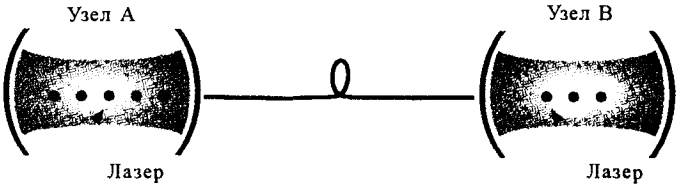


Рис. 6.1. Элемент квантовой сети. Атомы в высокодобротных резонаторах используются для локального хранения и манипулирования квантовой информацией между пространственно разделенными «узлами» сети.

Для хранения кубитов хорошо подходят атомы и ионы, находящиеся в долгоживущих внутренних состояниях. Недавно были предложены схемы для выполнения квантовых логических операций на атомах в ловушках или ионах, что дало привлекательную возможность для выполнения локальных манипуляций в пределах атомных (ионных) узлов [156, 274, 275]. С другой стороны, для быстрых и надежных способов передачи информации на большие расстояния, очевидно, именно фотоны являются лучшими носителями кубитов [276, 277]. В этом разделе мы рассмотрим схему [278], в которой реализуется интерфейс между атомами и фотонами, т.е. между сетевыми узлами и коммуникационными каналами. Такая схема позволяет осуществлять квантовую связь с единичной эффективностью (в принципе) между удаленными атомами 1 и 2. Сочетание локальных квантовых манипуляций с квантовой связью между сетевыми узлами открывает возможность для новых разнообразных приложений – от криптографии

на основе перепутанных состояний [279] и телепортации [280], до более сложных, таких как многочастичные средства связи и распределенные квантовые вычисления [281, 282].

Основная идея этой схемы состоит в использовании сильного взаимодействия между высокодобротным оптическим резонатором и атомами [276], образующими отдельный узел квантовой сети. При воздействии лазерных пучков можно преобразовать внутреннее состояние атома первого узла в оптическое состояние резонаторной моды. Возникающие при этом фотоны выходят из резонатора, распространяются как волновой пакет по линии передачи и попадают в резонатор второго узла. В конечном счете, оптическое состояние второго резонатора преобразуется во внутреннее состояние атома. При последовательном доступе к парам атомов (один атом в каждом узле) можно добиться много-кубитовых передач, поскольку в процессе записи состояния сохраняются перепутывания между произвольно расположенными атомами. Отличительная особенность этого протокола состоит в том, что управляя взаимодействием между атомом и резонатором, можно избежать отражения волновых пакетов от второго резонатора. Это достигается при помощи эффективного исключения тех доминирующих потерь в канале, которые отвечали бы за декогерентность в процессе передачи информации.

6.2.2 Модель передачи квантового состояния

Простая конфигурация для квантовой передачи между двумя узлами включает в себя два атома 1 и 2, которые сильно взаимодействуют со своими резонаторными модами, см. Рис.6.2.

Гамильтониан, описывающий взаимодействие каждого атома с соответствующей резонаторной модой (мы полагаем $\hbar = 1$), имеет вид:

$$\hat{H}_i = \omega_c \hat{a}_i^\dagger \hat{a}_i + \omega_0 |r\rangle_{i\,i}\langle r| + g\left(|r\rangle_{i\,i}\langle g|\hat{a}_i + \text{э.с.}\right) + \\ + \frac{1}{2}\Omega_i(t)\left[e^{-i[\omega_L t + \phi_i(t)]}|r\rangle_{i\,i}\langle e| + \text{э.с.}\right] \qquad (i = 1, 2). \qquad (6.1)$$

Здесь $\hat{a}_i$ и $\hat{a}_i^\dagger$ – операторы уничтожения и рождения для резонаторной моды 1 с частотой ω_c (Рис.6.2). Состояния $|g\rangle$, $|r\rangle$ и $|e\rangle$ образуют трех-уровневую систему с частотой возбуждения ω_0, а кубит представляется суперпозицией двух вырожденных основных состояний. Состояния $|e\rangle$ и $|g\rangle$ связаны благодаря рамановскому переходу [274, 275, 283], когда лазер с частотой ω_L возбуждает атом из состояния $|e\rangle$ в состояние $|r\rangle$ с зависящими от времени частотой Раби $\Omega_i(t)$ и фазой $\phi(t)$ и последующим за этим переходом $|r\rangle \rightarrow |e\rangle$, сопровождаемым испуска-

нием фотона в соответствующей резонаторной моде с постоянной связи g. Для подавления спонтанного излучения, происходящего из возбужденного состояния во время рамановского процесса, мы предполагаем, что лазер сильно отстроен по частоте от атомного перехода $|\Delta| >> \Omega_{1,2}(t)$, g, $|\phi_{1,2}|$ (где $\Delta = \omega_L - \omega_0$). В этом случае можно адиабатически исключить возбужденные состояния $|r\rangle_i$. Новый гамильтониан, описывающий динамику двух основных состояний в терминах частотных расстроек, приобретает вид:

$$\hat{H}_i = -\delta \hat{a}_i^\dagger \hat{a}_i + \frac{g^2}{\Delta} \hat{a}_i^\dagger \hat{a}_i |g\rangle_{i\,i}\langle g| + \delta\omega_i(t) |e\rangle_{i\,i}\langle e| -$$

$$-ig_i(t)\left[e^{i\phi_i(t)} |e\rangle_{i\,i}\langle g| a_i - \text{э.с.}\right] . \qquad (i = 1, 2) \qquad (6.2)$$

Первое слагаемое содержит рамановскую расстройку $\delta = \omega_L - \omega_0$. Два следующих слагаемых представляют динамические штарковские сдвиги основных состояний $|g\rangle$ и $|e\rangle$, возникающие из-за присутствия резонаторной моды и лазерного поля, соответственно, с $\delta\omega_i(t) = \Omega_i^2(t)/(4\Delta)$. Последнее слагаемое известно как взаимодействие Джейнса-Каммингса, с эффективной константой связи $g_i(t) = g\Omega_i(t)/(2\Delta)$. Здесь мы временно пренебрегаем слабыми эффектами, вызванными спонтанным излучением во время рамановского процесса. Обозначения $|e\rangle$ – возбужденного состояния и $|g\rangle$ – основного состояния мотивируются аналогией с моделью Джейнса-Каммингса.

Наша цель состоит в отборе зависящих от времени частот Раби и лазерных фаз[1] для достижения *идеальной квантовой передачи*;

$$\left(c_g|g\rangle_1 + c_e|e\rangle_1\right)|g\rangle_2 \otimes |0\rangle_1|0\rangle_2|vac\rangle$$

$$\rightarrow |g\rangle_1\left(c_g|g\rangle_2 + c_e|e\rangle_2\right) \otimes |0\rangle_1|0\rangle_2|vac\rangle \ , \qquad (6.3)$$

где $c_{g,e}$ – комплексные числа; вообще говоря, они должны быть заменены на ненормированные состояния других атомов – «наблюдателей», входящих в квантовую сеть. В (6.3) $|0\rangle_i$ и $|vac\rangle$ представляют вакуумное состояние резонаторных мод и свободных электромагнитных мод, связанных с резонаторами. Передача будет происходить путем обмена фотонами через эти моды.

В таком контексте удобно формулировать задачу на языке квантовых траекторий [284, 285]. Представим мысленный эксперимент, в котором выходное поле второго резонатора постоянно просматривается фотодетектором (см. рис.6.2). Эволюция квантовой системы при

[1] Можно также модулировать пропускание резонатора, но технически это гораздо сложнее.

непрерывном наблюдении, условная по отношению к наблюдению специальной траектории отсчетов, может быть описана чистым состоянием с волновой функцией $|\psi_c(t)\rangle$ в гильбертовом пространстве системы (где пренебрегается существованием радиационных мод вне резонатора). В течение интервалов времени, когда отсчета нет, эта волновая функция эволюционирует в соответствии с уравнением Шредингера, содержащего неэрмитовый эффективный гамильтониан:

$$\hat{H}_{eff}(t) = \hat{H}_1(t) + \hat{H}_2(t) - ik\left(\hat{a}_1^\dagger \hat{a}_1 + \hat{a}_2^\dagger \hat{a}_2 + 2\hat{a}_2^\dagger \hat{a}_1\right). \qquad (6.4)$$

Здесь, k – потери в резонаторе, которые предполагаются одинаковыми для первого и второго резонаторов. Регистрация отсчета за время t_r ассоциируется с квантовым скачком, в соответствии с $|\psi_c(t+dt)\rangle \propto c|\psi_c(t_r)\rangle$, где $c=a_1+a_2$[285, 286]. Плотность вероятности того, что скачок (отсчет детектора) произойдет в интервал времени от t до $t+dt$ равна $\langle\psi_c(t)|c^\dagger c|\psi_c(t)\rangle dt$ [285, 286].

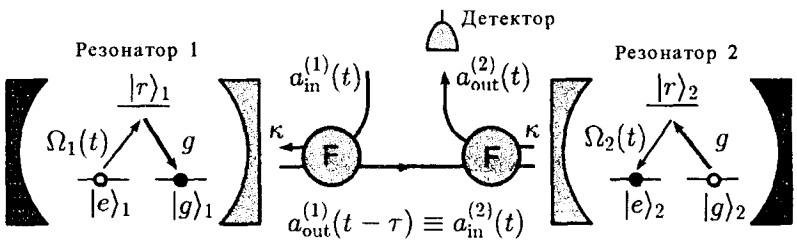


Рис. 6.2. Схематичное представление непрямой квантовой передачи между двумя атомами в оптических резонаторах, соединенных квантованной линией передачи.

6.2.3 *Лазерные импульсы для идеальной передачи*

Мы хотим подобрать лазерные импульсы в обоих резонаторах так, чтобы удовлетворить условиям идеальной квантовой передачи (6.3). Необходимое условие для эволюции во времени состоит в том, что квантовый сачок (отсчет детектора, см. Рис.6.2) никогда бы не происходил, т.е. $c|\psi_c(t)\rangle = 0 \forall t$, и таким образом, эффективный гамильтониан стал бы эрмитовым оператором. Другими словами, система будет оставаться в *темном* состоянии каскадной квантовой системы. Физически это означает, что волновой пакет не отражается от второго резонатора. Разложим состояние системы как

$$\begin{aligned}|\psi_c(t)\rangle = {} & c_g|gg\rangle|00\rangle + \\ & + c_e[\alpha_1(t)e^{-i\phi_1(t)}|eg\rangle|00\rangle + \alpha_2(t)e^{-i\phi_2(t)}|ge\rangle|00\rangle + \\ & + \beta_1(t)|gg\rangle|10\rangle + \beta_2(t)|gg\rangle|01\rangle]\,. \end{aligned} \qquad (6.5)$$

Идеальная квантовая передача (6.3) произойдет при

$$\alpha_1(-\infty)=\alpha_2(+\infty)=1,\quad \phi_1(-\infty)=\phi_2(+\infty)=0\,. \tag{6.6}$$

Первый член в (6.5) не изменяется при временной эволюции, генерируемой H_{eff}. Определяя симметричные и антисимметричные коэффициенты $\beta_{1,2}=(\beta_s \mp \beta_a)/\sqrt{2}$, мы находим следующие *уравнения эволюции*

$$\dot{\alpha}_1(t)=g_1(t)\beta_a(t)/\sqrt{2}\ , \tag{6.7}$$

$$\dot{\alpha}_2(t)=-g_2(t)\beta_a(t)/\sqrt{2}\ , \tag{6.8}$$

$$\dot{\beta}_a(t)=-g_1(t)\alpha_1(t)/\sqrt{2}+g_2(t)\alpha_2(t)/\sqrt{2}\ , \tag{6.9}$$

где мы выбрали лазерные частоты $\omega_L+\dot{\phi}_{1,2}(t)$ так, что $\delta = g^2/\Delta$ и

$$\dot{\phi}_{1,2}(t)=\delta\omega_i(t) \tag{6.10}$$

для того, чтобы компенсировать динамический эффект Штарка; таким образом, (6.7 – 6.9) становятся независимыми от фаз. *Условие темного состояния* подразумевает, что $\beta_s(t) = 0$, и поэтому

$$\dot{\beta}_s(t)=g_1(t)\alpha_1(t)/\sqrt{2}+g_2(t)\alpha_2(t)/\sqrt{2}+k\beta_a(t)\equiv 0\ , \tag{6.11}$$

при нормировке

$$|\alpha_1(t)|^2+|\alpha_2(t)|^2+|\beta_a(t)|^2=1\,. \tag{6.12}$$

Заметим, что коэффициенты $\alpha_{1,2}(t)$ и $\beta_S(t)$ – действительные.

Математическая задача теперь состоит в отыскании формы импульсов $\Omega_{1,2}(t) \propto g_{1,2}(t)$, такой, что будут выполнены условия (6.6 – 6.9, 6.11). В общем случае это довольно сложная задача, поскольку условия (6.6, 6.11) предопределяют в решениях дифференциальных уравнений (6.7 –6.9) функциональные ограничения на форму импульсов; такие решения не вполне очевидны. Мы построим класс таких решений, которые удовлетворяют следующей физической модели. Предположим, что фотон выходит из оптического резонатора и распространяется от него в виде волнового пакета. Представим, что мы в состоянии «обратить во времени» этот волновой пакет и направить его обратно в резонатор; это восстановило бы исходное (неизвестное) суперпозиционное состояние атома, в предположении, что мы также обратили во времени и лазерные импульсы. С другой стороны, если бы мы были способны поместить атом в передающий резонатор так, что выходящий импульс был бы всегда симметричен во времени, то волновой пакет, входящий в принимающий резонатор, «скопировал» бы такой процесс обращения времени и, таким образом, «восстановил» бы состояние первого атома на втором. Следо-

вательно, будем искать решения, удовлетворяющие условию симметричности импульса

$$g_2(t) = g_1(-t) \quad (\forall t) \ . \tag{6.13}$$

Это подразумевает, что $\alpha_1(t) = \alpha_2(-t)$, и $\beta_a(t) = \beta_a(-t)$. Последнее соотношение приводит к симметричной форме волнового пакета фотона, распространяющегося между резонаторами.

Предположим, что мы уточнили форму импульса $\Omega_1(t) \propto g_1(t)$ для второй половины импульса в первом резонаторе ($t \geq 0$)[2]. Мы хотим определить первую половину $\Omega_1(-t) \propto g_1(-t)$ для ($t > 0$), так что выполняются условия (6.3) для идеальной передачи. Из (6.6, 6.11) получаем

$$g_1(-t) = -\frac{\sqrt{2}k\beta_a(t) + g_1(t)\alpha_1(t)}{\alpha_2(t)} \ , \quad (t > 0) \ ; \tag{6.14}$$

Таким образом, форма импульса полностью определена, при условии, что мы знаем эволюцию системы для $t \geq 0$. Однако, при попытке найти эту эволюцию возникают определенные трудности, т.к. неизвестной еще остается величина $g_2(t) = g_1(-t)$ для $t > 0$ [см. (6.7 – 6.9)]. Для того, чтобы обойти эту проблему, мы используем (6.11) для уничтожения такой зависимости в (6.7, 6.9). Это дает

$$\dot{\alpha}_1(t) = g_1(t)\beta_a(t)/\sqrt{2} \ , \tag{6.15}$$

$$\dot{\beta}_a(t) = -k\beta_a(t) - \sqrt{2}g_1(t)\alpha_1(t) \tag{6.16}$$

для $t \geq 0$. Эти уравнения нужно дополнить начальными условиями

$$\alpha_1(0) = \left[\frac{2k^2}{g_1^2(0) + k^2}\right]^{\frac{1}{2}} \ , \tag{6.17}$$

$$\beta_a(0) = \left[1 - 2\alpha_1^2(0)\right]^{\frac{1}{2}} \ , \tag{6.18}$$

которые немедленно следуют из $\alpha_1(0) = \alpha_2(0)$ и (6.11, 6.12) при $t = 0$. Найдя решение (6.15, 6.16), мы можем определить $\alpha_2(0)$ из условия нормировки (6.12). Двигаясь таким путем, мы полностью решаем задачу, т.к. все величины, имеющиеся в (6.14) теперь известны для $t \geq 0$. Таким образом, непосредственно находится аналитическое выражение для формы импульсов, например, полагая $\Omega_1(t) = const$ для $t > 0$.

[2] $\Omega_1(t)$ должна быть такова, чтобы $\alpha_1(\infty) = 0$. Это выполняется, если $\Omega_1(t) > 0$, что также гарантирует отличие от нуля знаменателя в (6.14) при $t > 0$.

6.2.4 Несовершенные операции и коррекция ошибок

Мы предполагали, что все операции, включенные в процесс передачи, т.е. запись состояния с атома на резонаторное поле посредством лазерных импульсов, являются совершенными. Кроме того, мы не уделяли внимания потерям за счет поглощения и декогерентности в коммуникационном канале. На самом деле, с определенной вероятностью такие процессы всегда будут происходить. Система резонатор – оптоволокно, рассматриваемая вместе с рамановскими импульсами, представляют собой пример *зашумленного квантового канала*. Вообще говоря, квантовый шум приводит к уменьшению качества передачи и разрушает квантовые корреляции, установленные между узлами. Этот эффект, в особенности, становится доминирующим, когда узлы удалены друг от друга на большие расстояния, причем мера длины определяется в сравнении с длиной когерентности и/или длиной поглощения[3] канала. К счастью, благодаря методам квантовой коррекции ошибок [287] и очищения перепутывания [288], существует ряд приемов, позволяющих противостоять влиянию эффектов квантового шума и декогерентности. В разделе 8.6. будет показано, каким образом можно реализовать эффективную коррекцию ошибок, исправляющую ошибки в передачах всех типов, в применении к рассмотренной выше квантовой сети. Это позволит осуществлять связь высокого качества на небольших расстояниях. Для передач на большие расстояния, когда вероятность ошибки растет экспоненциально с длиной канала, мы развиваем концепцию квантового повторителя, который выполняет роль, аналогичную усилителям в классических системах связи.

6.3 Многочастичное перепутывание

Д.Боумейстер, Дж.-В.Пэн, М.Даниэль, Х.Вайнфуртер, А.Цайлингер.

6.3.1 Состояния Гринберга-Хорна-Цайлингера

Перепутывание между большим количеством частиц играет определяющую роль в большинстве квантовых коммуникационных схем, таких как схем коррекции ошибок, распределения секретного ключа и при квантовых вычислениях. Однако, исходная потребность в обсуждении и создании таких перепутанных состояний более чем двух частиц, т.н.

[3] Имеется в виду длина пробега, которая обратно пропорциональна коэффициенту поглощения. (*Прим. переводчика*)

состояний Гринберга-Хорна-Цайлингера (ГХЦ), возникла совершенно из других областей знания [289, 290]. А именно, из рассуждений о том, является ли квантовая механика полной теорией или нет. Хотя мы и не ставим своей задачей детальное освещение этой фундаментальной философской дискуссии, краткое описание проблемы все-таки будет дано. Это поможет читателю лучше представлять процессы хранения квантовой информации в системах с многочастичным перепутыванием, а также ответить на вопрос, почему квантовые свойства таких систем находятся в резком противоречии с эйнштейновским представлением о локальности. Изложение базируется на экспериментальной реализации трех-фотонного перепутывания, которое, по праву, занимает очень важное место в области квантовой информации [291].

6.3.2 Противоречие с локальным реализмом

Гринберг, Хорн и Цайлингер показали, что квантово-механические предсказания некоторых результатов измерений над тремя перепутанными частицами противоречат локальному реализму в случаях, когда квантовая теория дает достоверные, т.е. нестатистические предсказания [289-294]. Ситуация здесь отличается от случая с экспериментами типа Эйнштейна-Подольского-Розена с двумя перепутанными частицами по проверке неравенства Белла, где противоречие с локальным реализмом возникает только для статистических предсказаний [21, 23, 295, 297].

Почему же трех-фотонные состояния ГХЦ находятся в более сильном противоречии с локальным реализмом, чем двух-фотонные состояния?[4] Чтобы найти ответ на этот вопрос, рассмотрим состояние

$$\frac{1}{\sqrt{2}}\left(|H\rangle_1|H\rangle_2|H\rangle_3+|V\rangle_1|V\rangle_2|V\rangle_3\right) \quad , \tag{6.19}$$

где H и V обозначают горизонтальную и вертикальную поляризации. Это состояние показывает, что три фотона находятся в квантовой суперпозиции состояния $|H\rangle_1|H\rangle_2|H\rangle_3$ (все три фотона имеют горизонтальную поляризацию) и состояния $|V\rangle_1|V\rangle_2|V\rangle_3$ (три фотона имеют вертикальную поляризацию). Такое специфическое состояние симметрично по отношению к перестановкам всех фотонов, что упрощает аргументацию, приводимую ниже. Однако все рассуждения остаются справедливыми и для других максимально перепутанных трех-фотонных состояний.

[4] Для двухфотонных состояний Харди [298] нашел ситуации, когда локальный реализм предсказывает, что некоторый результат имеет место иногда, а квантовая механика предсказывает, что тот же самый результат не будет иметь места никогда [209].

Рассмотрим теперь некоторые специфические предсказания, следующие из вида состояния (6.19) и относящиеся к поляризационным измерениям, проводимыми над каждым фотоном либо в базисе, повернутом на 45^0 относительно H/V и обозначенного H'/V', либо в циркулярном базисе, обозначенном L/R (лево-циркулярный, право-циркулярный). Эти новые поляризационные базисы можно переписать в терминах исходного базиса:

$$|H'\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle + |V\rangle\right), \quad |V'\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle - |V\rangle\right), \tag{6.20}$$

$$|R\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle + i|V\rangle\right), \quad |L\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle - i|V\rangle\right). \tag{6.21}$$

Обозначим состояние $|H\rangle$ вектором (1, 0), а состояние $|V\rangle$ вектором (0,1); эти вектора представляют два собственных состояния оператора Паули σ_z, с соответствующими собственными значениями +1 и −1. Можно легко убедиться, что $|H'\rangle$ и $|V'\rangle$ или $|R\rangle$ и $|L\rangle$ являются собственными состояниями операторов Паули σ_x и σ_y с собственными значениями +1 и −1, соответственно. Будем называть измерение в базисе H'/V' – x-измерением, а в базисе L/R – y-измерением.

После представления состояния (6.19) в новых базисах можно получить предсказания измерений этих новых базисных поляризаций. Например, при измерении циркулярной поляризации, скажем, обоих фотонов 1 и 2 и измерении линейной поляризации H' и V' фотона 3, обозначенных как *yyx*-измерений, состояние принимает вид:

$$\frac{1}{2}\left(|R\rangle_1|L\rangle_2|H'\rangle_3 + |L\rangle_1|R\rangle_2|H'\rangle_3\right) + \\ + \left(|R\rangle_1|R\rangle_2|V'\rangle_3 + |L\rangle_1|L\rangle_2|V'\rangle_3\right). \tag{6.22}$$

Из этого выражения можно получить ряд существенных следствий. Во-первых, его специфика состоит в том, что любое отдельное или двух-фотонное измерение имеет абсолютно случайный результат. Например, фотон 1 будет обнаружен либо с R, либо с L поляризациями с одинаковой вероятностью 50%.

Во-вторых, это выражение содержит только члены, составленные из произведений, принимающих значение −1 при *yyx*-измерении. Это дает возможность достоверно предсказать результат измерения третьего фотона, зная результат измерения над двумя другими фотонами. Например, предположим, что в результате измерения над фотонами 1 и 2 получилась право-циркулярная поляризация (R) (т.е. оба собственных значения равны +1). Из третьего слагаемого выражения (6.22) находим, что фотон 3 достоверно имеет V'-поляризацию (т.е. собственное значение −1).

При циклической перестановке можно получить аналогичные выражения для любых типов измерения циркулярной поляризации двух фотонов и V'-, H'-поляризаций оставшегося фотона. И снова те слагаемые, которые представляются произведениями, дающими значение –1, являются результатами *yxy*- или *xyy*-измерений. Таким образом, результат измерения и циркулярной поляризации, и линейной V', H' может быть предсказан с достоверностью для любого отдельного фотона при условии, что имеется соответствующий результат измерения двух других фотонов.

Попробуем проанализировать следствия таких предсказаний с точки зрения локального реализма. Сперва заметим, что эти предсказания не зависят ни от пространственного положения фотонов, ни от очередности выполнения измерений во времени. Рассмотрим эксперимент, в котором три измерения выполняются одновременно в данной системе координат, скажем – для простоты – в системе координат источника. Применение эйнштейновского понятия локальности означает, что информация не может распространяться быстрее скорости света. Отсюда, результат специфического измерения, выполненного над отдельным фотоном не должен зависеть ни от того, выполнено ли специфическое измерение над двумя другими фотонами одновременно, ни от исхода таких измерений. Единственный способ объяснить обсуждаемые полные корреляции с точки зрения локального реалиста состоит в предположении что каждый фотон несет элемент реальности всех рассмотренных измерений и что эти элементы реальности определяют результат специфического измерения [289, 290, 294].

Теперь, давайте рассмотрим измерение линейной V', H' поляризации всех трех фотонов, т.е. *xxx*-измерения. Если элементы реальности существуют, то какие исходы вообще возможны? Состояние (6.19) и его всевозможные циклические перестановки подразумевает, что какой бы результат V', H' ни был получен для любого единичного фотона, два другие должны нести противоположные [идентичные] циркулярные поляризации. Предположим, что из каких-то трех фотонов, фотоны 2 и 3 были обнаружены в состоянии V'. Поскольку фотон 3 имеет V'-поляризацию, то фотоны 1 и 2 должны иметь идентичные циркулярные поляризации, а поскольку фотон 2 имеет V'-поляризацию, фотоны 1 и 3 опять должны нести идентичные циркулярные поляризации. Ясно, что если эти циркулярные поляризации являются элементами реальности, то все три фотона должны переносить идентичные циркулярные поляризации. Таким образом, если фотоны 2 и 3 имеют идентичные циркулярные поляризации, то фотон 1 должен достоверно иметь линейную поляризацию V'. Значит, существование элементов реально-

сти приводит к заключению о том, что результат $|V'\rangle_1|V'\rangle_2|V'\rangle_3$ является одним из возможных исходов, если выбрано измерение V'-, H'-поляризации всех трех частиц, т.е. выполняется измерение *xxx*. Выполняя аналогичные рассуждения, можно проверить, что существует только четыре возможных исхода

$$|V_1'\rangle|V_2'\rangle|V_3'\rangle\ , \quad |H_1'\rangle|H_2'\rangle|V_3'\rangle\ ,$$

$$|H_1'\rangle|V_2'\rangle|H_3'\rangle \text{ и } |V_1'\rangle|H_2'\rangle|H_3'\rangle\ . \tag{6.23}$$

Каким образом можно сравнить эти предсказания локального реализма с предсказаниями квантовой теории? Переписав состояние (6.19) в терминах V'-, H'-поляризаций, получим

$$\frac{1}{2}(|H'\rangle_1|H'\rangle_2|H'\rangle_3+|H'\rangle_1|V'\rangle_2|V'\rangle_3+$$

$$+|V'\rangle_1|H'\rangle_2|V'\rangle_3+|V'\rangle_1|V'\rangle_2|H'\rangle_3). \tag{6.24}$$

Сравнивая слагаемые, записанные в (6.23), со слагаемыми из (6.24) можно заметить, что всякий раз, когда локальный реализм предсказывает достоверный специфический результат измерения одного фотона при данном результате измерений над двумя другими фотонами, квантовая физика достоверно предсказывает прямо противоположный результат. Таким образом, в то время как в случае неравенств Белла для двух фотонов, разница между локальным реализмом и квантовой физикой состоит в статистических предсказаниях теории, то здесь любая статистика возникает только благодаря неизбежным ошибкам в измерениях, свойственных и классической и квантовой физике.

6.3.3 Источник трех-фотонного ГХЦ-перепутывания

Перепутывание между более чем двумя частицами было предложено осуществить в экспериментах с фотонами [300], атомами [301], ионами (см. разд. 4.3) и тремя ядерными спинами внутри одной молекулы, приготовленными так, что они локально проявляют трех-частичные корреляции [302]. В этом разделе рассматривается первая реализация поляризационного перепутывания трех пространственно разделенных фотонов [291]. Экспериментальная методика, по сути, является дальнейшим развитием той, которая была использована в экспериментах по квантовой телепортации [76] (разд. 3.7) и обмену перепутыванием [86] (разд. 3.10).

Как предлагалось в [300], основная идея состоит в преобразовании пар перепутанных по поляризации фотонов в три перепутанных и

один (четвертый) независимый фотон[5]. Идейная схема экспериментальной установки показана на Рис. 6.3. Пары перепутанных по поляризации фотонов генерируются 200-фемтосекундными импульсами ультрафиолетового диапазона, при прохождении через кристалл BBO (разд. 3.4.4). В результате перепутанное по поляризации состояние имеет вид [26]:

$$\frac{1}{\sqrt{2}}\left(|H\rangle_a|V\rangle_b + e^{i\alpha}|V\rangle_a|H\rangle_b\right). \tag{6.25}$$

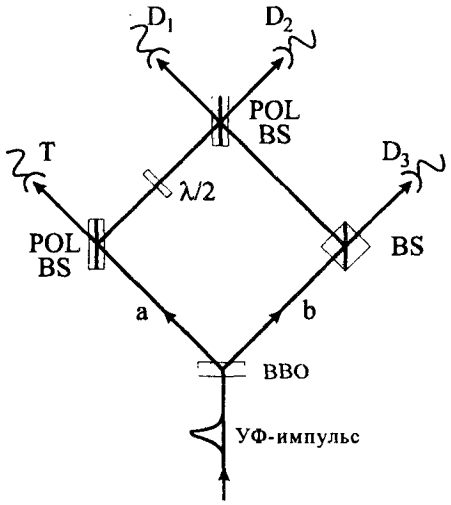


Рис. 6.3. Схематичное изображение экспериментальной установки для демонстрации перепутывания Гринберга – Хорна – Цайлингера для пространственно разнесенных фотонов. При условии регистрации одного фотона сигнальным детектором T, три других фотона, регистрируемых в D_1, D_2 и D_3, проявляют искомые ГХЦ-корреляции.

Это состояние представляет собой суперпозицию возможностей того, что фотон в плече *a* имеет горизонтальную поляризацию, а фотон в плече *b* –вертикальную поляризацию $|H\rangle_a|V\rangle_b$ и наоборот $|V\rangle_a|H\rangle_b$.

Изредка в кристалле возникает сразу две пары от одного лазерного импульса. Установка построена так, что регистрация одного фотона в каждом из четырех детекторов (четверное совпадение), соответствует наблюдению состояния

$$\frac{1}{\sqrt{2}}\left(|H\rangle_1|H\rangle_2|V\rangle_3 + |V\rangle_1|V\rangle_2|H\rangle_3\right) \tag{6.26}$$

с помощью детекторов D_1, D_2 и D_3.

[5] Этот метод получения трех-частичного перепутывания от источника пар перепутанных частиц может быть обобщен на случай создания перепутывания между гораздо большим числом частиц.

Понять это можно так. Когда происходит четверное совпадение, один фотон в плече *a* должен пройти через поляризационный светоделитель (PBS) в этом плече и поэтому должен иметь горизонтальную поляризацию при регистрации сигнальным детектором T. Тогда, коррелированный с ним фотон в плече *b*, должен иметь вертикальную поляризацию и с 50%-ой вероятностью проходить через светоделитель (см. рис. 6.3) либо в сторону детектора D_3, либо в сторону оконечного поляризационного светоделителя, от которого он отразится и попадет в D_2. В остальных случаях отсчеты в детекторах D_1 и D_2 вызваны наличием пары. Один из фотонов этой второй пары распространяется по плечу *a* и должен обязательно иметь *V*-поляризацию, для того, чтобы отразиться от поляризационного светоделителя в плече *a*. Коррелированный с ним фотон в плече *b* должен оказаться *H*-поляризованным и после отражения от светоделителя в плече *b* (с 50%-ой вероятностью), пройдет через оконечный светоделитель и будет зарегистрирован детектором D_1. Поэтому, фотон, зарегистрированный детектором D_2, должен иметь *H*-поляризацию, т.к. он проходит по плечу *a* и должен отразиться от последнего светоделителя. Заметим, что этот фотон изначально имел *V*-поляризацию, но после прохода через полуволновую пластинку (ориентированную под углом 22.5°) он становится поляризованным под 45°, что дает ему 50%-ую вероятность быть зарегистрированным в детекторе D_2 как *H*-фотон. Таким образом, можно сделать вывод, что если фотон, зарегистрированный детектором D_3, коррелирован с фотоном, зарегистрированным сигнальным детектором T, то регистрация совпадения детекторами D_1, D_2 и D_3 отвечает детектированию состояния

$$|H\rangle_1|H\rangle_2|V\rangle_3 . \tag{6.27}$$

Рассуждая таким же образом, приходим к выводу, что если фотон, зарегистрированный D_2, коррелирован с фотоном в T, то регистрация совпадения между D_1, D_2 и D_3 отвечает состоянию

$$|V\rangle_1|V\rangle_2|H\rangle_3 . \tag{6.28}$$

Вообще говоря, два состояния (6.27) и (6.28), соответствующие четверным совпадениям, не образуют когерентной суперпозиции, т.е. ГХЦ-состояния, потому что они, в принципе, могут быть различимыми. Состояния могут не перекрываться во времени на детекторах, и к тому же точное время детектирования каждого фотона показывает, какое состояние в настоящий момент зарегистрировано. Например, состояние (6.27) распознается, когда детекторы T и D_3 или D_1 и D_2 срабатывают одновременно. Для стирания этой информации необходимо, чтобы время когерентности фотонов значительно превышало длительность ультрафиолетовых импульсов накачки (составляющую

приблизительно 200 фс) [304]. Это можно сделать, если регистрировать фотоны после того, как они пройдут через узкополосные фильтры (с шириной 3.6 нм), что увеличивает время когерентности поля до 500 фс. Таким образом, в основном, различимость между состояниями (6.27) и (6.28) исчезает. Согласно основному правилу квантовой механики, состояние, детектируемое при регистрации совпадений в D_1, D_2 и D_3 при условии срабатывания T, является квантовой суперпозицией (6.26). Строго говоря, такой способ стирания информации является идеальным, т.е. воспроизводящим чистое ГХЦ-состояние, лишь в приближении бесконечно малой длительности импульсов и бесконечно малой ширины фильтров. Однако детальный расчет [305] показывает, что упомянутые выше экспериментальные параметры достаточны для того, чтобы получить четко наблюдаемое перепутывание, являющееся чистым на 80%, в соответствие с приведенными ниже экспериментальными данными. Знак «плюс» в (6.26) формально имеет следующее происхождение. Рассмотрим два процесса СПР, дающих вместе факторизованное состояние

$$\frac{1}{2}\left(|H\rangle_a|V\rangle_b - |V\rangle_a|H\rangle_b\right)\left(|H\rangle'_a|V\rangle'_b - |V\rangle'_a|H\rangle'_b\right). \tag{6.29}$$

Мы изначально предполагаем, что компоненты $|H\rangle_{a,b}$ и $|V\rangle_{a,b}$, полученные в результате одного акта СПР, можно отличить от компонент $|H\rangle'_{a,b}$ и $|V\rangle'_{a,b}$, полученных в другом. Эволюция отдельных компонент состояния (6.29) при распространении через установку по направлению к детекторам T, D_1, D_2 и D_3 описывается следующими соотношениями:

$$|H\rangle_a \to |H\rangle_T, \qquad |V\rangle_b \to \frac{1}{\sqrt{2}}\left(|V\rangle_2 + |V\rangle_3\right), \tag{6.30}$$

$$|V\rangle_a \to \frac{1}{\sqrt{2}}\left(|V\rangle_1 + |H\rangle_2\right), \quad |H\rangle_b \to \frac{1}{\sqrt{2}}\left(|H\rangle_1 + |H\rangle_3\right). \tag{6.31}$$

Такие же соотношения выполняются и для штрихованных компонент. Подставляя эти выражения в состояние (6.29) и оставляя только те члены, для которых на каждом выходе остается только по одному фотону, получаем:

$$-\frac{1}{4\sqrt{2}}\{|H\rangle_T\left(|V\rangle_1'|V\rangle_2|H\rangle_3' + |H\rangle_1'|H\rangle_2'|V\rangle_3\right) +$$

$$+|H\rangle_T'\left(|V\rangle_1|V\rangle_2'|H\rangle_3 + |H\rangle_1|H\rangle_2|V\rangle_3'\right)\}. \tag{6.32}$$

Если экспериментальные условия таковы, что состояния фотонов, получающиеся в разных актах СПР неразличимы, то мы получаем искомое (с точностью до общего знака «минус») состояние:

$$\frac{1}{\sqrt{2}}|H\rangle_T\left(|H\rangle_1|H\rangle_2|V\rangle_3+|V\rangle_1|V\rangle_2|H\rangle_3\right). \tag{6.33}$$

Заметим, что общее состояние фотонов, которое получается в установке, т.е. состояние до измерения, также содержит слагаемые, которые, например, описывают попадание двух фотонов на один детектор. Кроме этого, общее состояние содержит вклады от единичных актов СПР[6]. Регистрация четверного совпадения рассматривается как проекционное измерение искомого ГХЦ-состояния (6.33) и, таким образом, отфильтровывает лишние слагаемые. Эффективность того, что один импульс накачки даст четверное совпадение очень низка (порядка 10^{-10}). К счастью, за одну секунду у нас есть $7.6\text{x}10^7$ импульсов накачки, которые дают приблизительно одну двойную пару при детектировании за 150 секунд. Процессами же генерации тройных и более пар можно пренебречь.

6.3.4 Экспериментальное подтверждение ГХЦ-перепутывания

Для того, чтобы экспериментально продемонстрировать, что ГХЦ-перепутывание действительно может быть достигнуто рассмотренным выше способом, прежде всего необходимо проверить, что при условной регистрации одного фотона сигнальным детектором T, имеются обе компоненты $H_1H_2V_3$ и $V_1V_2H_3$ и нет никаких других. Это было сделано при сравнении скоростей счета восьми возможных комбинаций поляризационных измерений, $H_1H_2H_3$, $H_1H_2V_3$,..., $V_1V_2V_3$. Наблюдаемое отношение интенсивностей между нужными и нежелательными состояниями составило 12:1. Существование двух слагаемых, как было только что показано, является необходимым, но недостаточным условием демонстрации ГХЦ-перепутывания. В действительности, результат может оказаться лишь статистической смесью таких двух состояний. Поэтому, нужно доказать, что эти два слагаемых представляют собой когерентную суперпозицию. Это было сделано при измерении линейной поляризации фотона 1 вдоль направления $+45^0$, когда вклад дают оба направления V и H. Такое измерение проицируют фотон 1 в суперпозицию

$$\left|+45^0\right\rangle_1=\frac{1}{\sqrt{2}}\left(|H\rangle_1+|V\rangle_1\right), \tag{6.34}$$

что подразумевает, что состояние (6.33) проицируется в

[6] Поскольку рождение пары фотонов в процессе СПР происходит в случайные моменты времени, такие события существенно преобладают над теми, в которых одновременно рождаются две пары (*Прим. переводчика*).

$$\frac{1}{\sqrt{2}}|H\rangle_T|+45\rangle_1\left(|H\rangle_2|V\rangle_3+|V\rangle_2|H\rangle_3\right). \qquad (6.35)$$

Таким образом фотоны 2 и 3 становятся перепутанными, как и предсказывалось при введении понятия «перепутанное перепутывание» [306]. Записывая состояние фотонов в 45°-ом базисе получаем состояние

$$\frac{1}{\sqrt{2}}\left(|+45^0\rangle_2|+45^0\rangle_3-|-45^0\rangle_2|-45^0\rangle_3\right). \qquad (6.36)$$

Это означает, что если фотон 2 был зарегистрирован с поляризацией -45°, фотон 3 будет также поляризован в этом направлении. Отсутствие слагаемых $|+45^0\rangle_2|-45^0\rangle_3$ и $|-45^0\rangle_2|+45^0\rangle_3$ объясняется деструктивной интерференцией и, таким образом, подтверждает наличие когерентной суперпозиции двух слагаемых в ГХЦ-состоянии (6.33). Поэтому, эксперимент состоял в измерении четверных совпадений между детектором T, детектором 1, расположенным после +45°-ого поляроида, детектором 2 после –45°-ого поляроида и измерения фотона 3 либо после +45°-ого, либо –45°-ого поляроида. В эксперименте изменялась разность времен прибытия фотонов на последний поляроид (поляризационный светоделитель), или, точнее, между детекторами D_1 и D_2.

Точки, нанесенные на рис. 6.4а, представляют собой экспериментальные результаты, полученные при поляризационном анализе фотона, регистрируемого в D_3, при условии срабатывания сигнального детектора T и детектирования двух фотонов, поляризованных под +45° и -45°, двумя детекторами D_1 и D_2, соответственно.

Две кривых показывают четверные совпадения в случае поляроида, стоящего перед детектором D_3 и ориентированного под -45° (квадратики) и +45° (кружочки), как функцию пространственной задержки в канале *a*. Из этих двух кривых следует, что при нулевой задержке поляризация фотона, попавшего в D_3, ориентирована вдоль -45°, в соответствие с квантово-механическими предсказаниями, сделанными исходя из ГХЦ-состояния. Для ненулевой задержки, фотоны, распространяющиеся по каналу *a* по направлению к второму поляризационному светоделителю, и фотоны, распространяющиеся по каналу *b*, становятся различимыми. Поэтому, значительное увеличение задержки разрушает квантовую суперпозицию в трех-частичном состоянии.

Заметим, что из представленных данных можно одинаково уверенно сделать вывод о том, что фотоны в D_1 и D_3 были спроицированы в двух-частичное перепутанное состояние, при условии проицирования тона в D_2 в состояние с -45°-ой поляризацией. Только эти два вывода совместимы с истинным ГХЦ-состоянием.

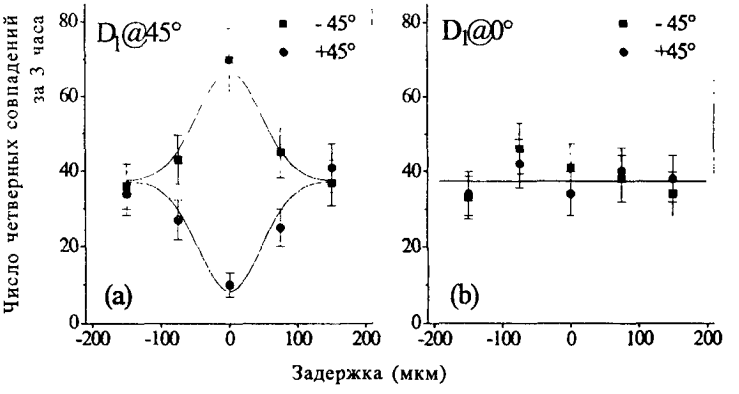


Рис.6.4. Экспериментальное подтверждение ГХЦ-перепутывания. На графике (а) показан поляризационный анализ фотона в D_3, при условии срабатывания сигнального детектора D_1, регистрирующего фотон, поляризованный в направлении 45^0 и одного фотона в детекторе D_2, поляризованного в направлении -45^0. Две кривые показывают четверные совпадения, когда поляризатор, расположенный перед детектором D_3, ориентирован под углом -45^0 и 45^0 соответственно, как функции задержки в канале *a*. Различие между двумя кривыми при нулевой задержке подтверждает наличие ГХЦ-перепутывания. Как и предсказывалось, разности в скоростях счета не обнаруживается, если поляризатор перед детектором D_1 установлен в положение 0^0 (график (b)).

Для дополнительного подтверждения наличия состояния (6.33) были выполнены измерения, в которых при условной регистрации фотона в D_1 он был поляризован вдоль направления 0^0 (т.е. *V*-поляризация). В случае ГХЦ-состояния $1/\sqrt{2}(H_1H_2V_3+V_1V_2H_3)$ это означает, что остающиеся два фотона должны находиться в состоянии V_2H_3, что не будет приводить ни к какой корреляции между этими двумя фотонами при регистрации в 45^0-ом базисе. Экспериментальные результаты этих измерений показаны на рис. 6.4b. Данные четко свидетельствуют об отсутствии двух-фотонных корреляций и подтверждают, таким образом, факт наблюдения ГХЦ-перепутывания между тремя пространственно разнесенными фотонами.

Напомним, что ГХЦ-перепутывание наблюдается только при условии регистрации сигнальных фотонов одновременно с тремя перепутанными фотонами. Это означает, что регистрация четверного совпадения выполняет двойную роль проицирования в искомое ГХЦ-состояние (6.26), и выполнения специфического измерения этого состояния.

Все вышеизложенное может вызвать определенные сомнения в возможности использования такого источника при проверке локального реализма. В действительности такого рода сомнения возникают и при

выполнении экспериментов по генерации состояний Белла, в которых используется свойство неразличимости фотонов [307, 308]. Хотя в ходе этих экспериментов были успешно приготовлены определенные квантово-механические корреляции на больших расстояниях, в недавнем прошлом существовало мнение [309, 310], что они никогда, даже в их идеальных реализациях, не смогут рассматриваться в качестве основы для истиной проверки локального реализма. Однако, Попеску, Харди и Жуковский [311] показали, что это общее мнение ошибочно, и что рассмотренные выше эксперименты действительно выполняют (исключая обычные проблемы, возникающие при фотодетектировании) действительные тесты локального реализма. Следуя той же аргументации, Жуковский [312] показал, что рассмотренный источник ГХЦ-состояний позволяет выполнить трех-частичный тест локального реализма. По сути, при проверке локального реализма ГХЦ-аргументы основаны на детектировании определенных событий, а знание лежащего в основе квантового состояния не является необходимым. Действительно, достаточно рассматривать только четверные совпадения, обсуждаемые выше, и полностью игнорировать вклады, возникающие от других слагаемых.

6.3.5 *Локальный реализм или квантовая механика: экспериментальная проверка*

Можно ли экспериментально разрешить конфликт, возникающий между локальным реализмом и квантовой механикой, используя источник ГХЦ-перепутывания, рассмотренный в предыдущем разделе? Как уже объяснялось в разд. 6.3.2, для этого необходимо выполнить набор экспериментов при *yyx*-, *yxy*- и *xyy*-измерениях. Каждый из этих трех экспериментов дает 2^3 возможных исходов.

На рис. 6.5 показаны экспериментально полученные вероятности для каждого из $3x2^3$ возможных исходов. Здесь, для того чтобы сравнить ГХЦ-аргументацию для состояния (6.19), представленную в разд. 6.3.2, мы просто переопределили поляризационные состояния фотона 3 в (6.26), т.е. обозначения $|H\rangle_3$ и $|V\rangle_3$ были переставлены местами.

Анализируя значения максимумов и минимумов на рис. 6.5, можно сделать вывод, что с точностью 71% ± 4%, т.е. когда видность $(\langle max\rangle - \langle min\rangle)/(\langle max\rangle + \langle min\rangle) = 0.71 \pm 0.04$, слагаемые, которые, как ожидалось, должны были присутствовать и те, которые должны были бы отсутствовать, могут быть идентифицированы. Несмотря на ограниченную видность, в основном связанную с конечной длительностью лазерных импульсов и конечной шириной частотных фильтров, для фун-

даментальной проверки – локальный реализм или квантовая механика – достаточно рассматривать данные, показанные на рис. 6.5.
Эти данные были получены из измерений ансамбля трех частиц, вылетающих из черного ящика. При таких измерениях никакие предварительные предположения об источнике ГХЦ-перепутывания не вовлекались в последующую демонстрацию конфликта с локальным реализмом.

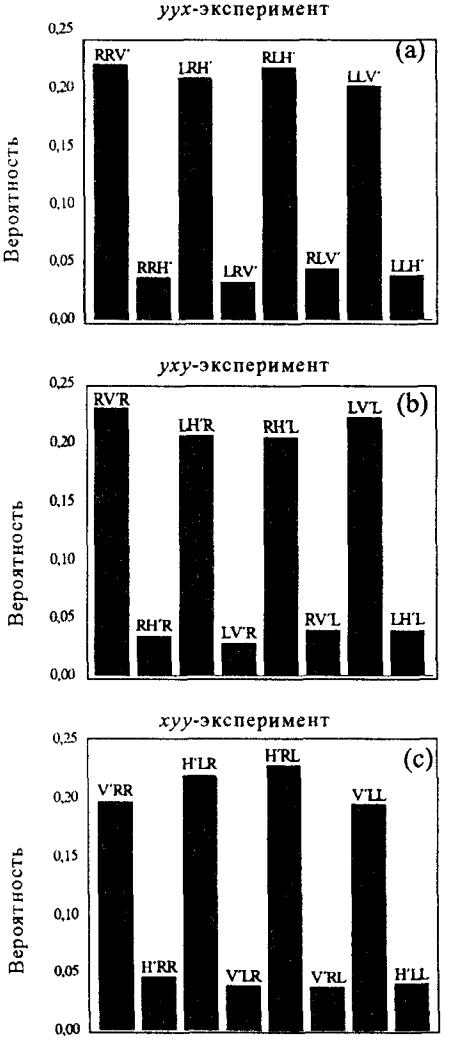


Рис.6.5. Экспериментально определенные вероятности всех трех возможных исходов при (a) *yyx*-измерении, (b) *yxy*-измерении и (c) *xyy*-измерении.

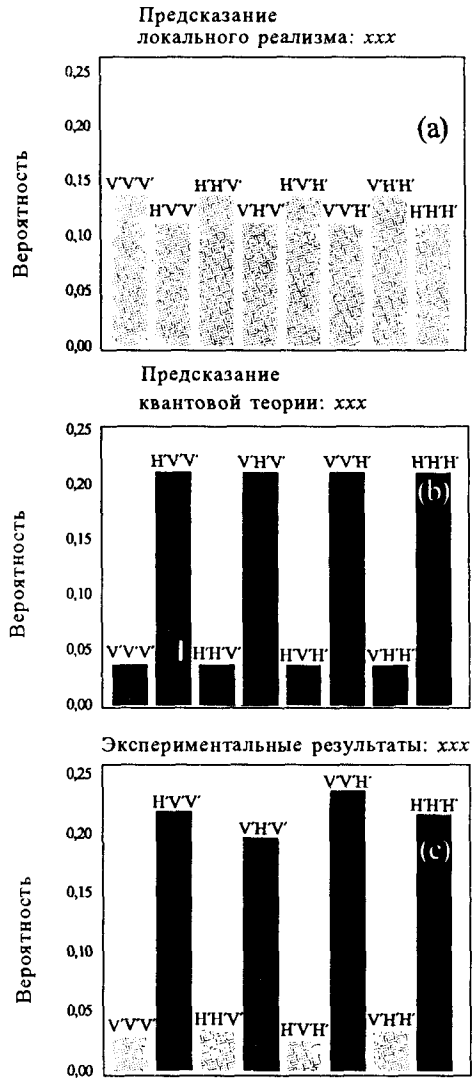


Рис. 6.6. (a): Предсказания локального реализма для вероятностей восьми трех-частичных корреляций при xxx-измерении (на основе данных, представленных на рис.6.5). (b): Соответствующие квантово-механические предсказания. (c): Экспериментальные результаты, которые резко противоречат предсказаниям локального реализма и находятся в хорошем соответствии с квантово-механическими предсказаниями в пределах ошибки измерений.

Из данных, показанных на Рис. 6.5 и, встав, на точку зрения локального реализма, т.е. предполагая, что исход определенного измерения над одной частицей не зависит от результата измерения, выполненного над другой частицей, которая пространственно удалена от первой,

можно предсказать (следуя аргументации, представленной в разд.6.3.2) возможные исходы для *xxx*-измерения. Эти предсказания показаны на Рис. 6.6a. Предсказания, сделанные на основе квантовой механики, показаны на Рис. 6.6b. Эти предсказания следуют из того факта, что данные, изображенные на Рис. 6.5 указывают на наличие перепутанных трех-частичных систем со степенью чистоты около 71%. И, наконец, на Рис.6.6c показаны экспериментальные результаты для *xxx*-измерений.

Эти результаты находятся в сильном противоречии с предсказаниями локального реализма и в полном согласии с квантово-механическими предсказаниями. В действительности, в пределах ошибки эксперимента, экспериментальные данные четко свидетельствуют о том, что происходят только те тройные совпадения, которые были предсказаны квантовой механикой, и не происходят те, которые предсказаны на основе локального реализма (см.(6.23)). В таком случае, в рассмотренном эксперименте была осуществлена первая проверка локального реализма без неравенств [313].

Поскольку невозможно выполнить эксперимент, удовлетворяющий полным корреляционными условиям, требуемым при ГХЦ-аргументации, локальный реалист может возразить, что предсказания ГХЦ никогда нельзя проверить в лаборатории полностью и поэтому, его не убеждает приведенный анализ. Чтобы преодолеть эту трудность, был получен ряд неравенств Белла для *N*-частичных ГХЦ-состояний [314-316]. Все эти работы показывают, что квантово-механические предсказания для ГХЦ-состояний нарушают эти неравенства на величину, растущую экспоненциально с ростом *N*. Например, оптимальное неравенство типа неравенства Белла для трех-частичного ГХЦ-состояния было написано Мермином и имеет вид

$$\left|\langle xyy\rangle + \langle yxy\rangle + \langle yyx\rangle - \langle xxx\rangle\right| \le 2 \ , \tag{6.37}$$

где, например, $\langle xyy\rangle$ обозначает ожидаемое значение произведения собственных значений для x, y и y при измерениях над частицами 1, 2, и 3, соответственно. Необходимая видность для нарушения неравенства типа Белла в случае эксперимента с трех-частичными ГХЦ-состояниями составляет 50% [314]. Видность, наблюдаемая в рассмотренных выше экспериментах, составляла около 70% и надежно превышает 50%-ый предел. Подставляя экспериментальные результаты в левую часть неравенства (6.37), получаем

$$\left|\langle xyy\rangle + \langle yxy\rangle + \langle yyx\rangle - \langle xxx\rangle\right| \le 2.83 \pm 0.09 \ . \tag{6.38}$$

Поэтому, экспериментальные результаты нарушают неравенство (6.37) на 9 стандартных отклонений, что подводит итог демонстрации противоречия с локальным реализмом. Необходимо подчеркнуть, что

рассмотренные тесты не выносят окончательного вердикта теориям, основанных на локальном реализме. Определенные «лазейки» все еще остаются открытыми, поскольку не было выполнено экспериментов с высоко эффективными приемниками, разнесенными на большое расстояние.

6.4 Характеристики перепутывания

В.Ведрал, М.Б.Пленио, П.Л.Найт

6.4.1 Разложение Шмидта и энтропия фон Неймана.

Смешанная квантовая система – это такая система, которая состоит из множества квантовых подсистем. Когда эти подсистемы являются перепутанными, ни к какой из них невозможно приписать определенный вектор состояния. Простой пример смешанной квантовой системы представляет собой пара перепутанных по поляризациям фотонов (см. разд. 3.4.4). Такая смешанная система математически записывается как

$$|\Psi^-\rangle_{12} = \frac{1}{\sqrt{2}}\left(|H\rangle_1|V\rangle_2 - |V\rangle_1|H\rangle_2\right). \qquad (6.39)$$

Свойство, которое здесь записано, состоит в том, что направления поляризации двух фотонов ортогональны вдоль любых осей[7]. Из выражения (6.39) можно сразу заметить, что никакой из фотонов не обладает определенным (поляризационным) состоянием. Лучший способ это показать состоит в том, что выполнив измерение над одним фотоном и, скажем, в результате которого будет обнаружена вертикальная поляризация ($|V\rangle$), мы найдем, что другой фотон окажется поляризованным горизонтально ($|H\rangle$). Однако, такой тип описания не может быть использован для общих смешанных систем, до тех пор, пока он не будет представлен в определенной форме. Это стимулирует нас к введению так называемого разложения Шмидта [317], которое оказывается удобным не только с математической точки зрения, но также дает глубокое понимание корреляций между двумя подсистемами.

Разложение Шмидта показывает, что любое состояние двух подсистем A и B (одна – размерности N, а другая – размерности $M \le N$) может быть записано в виде

$$|\Psi_{AB}\rangle = \sum_{i=1}^{N} c_i |u_i\rangle|v_i\rangle \ , \qquad (6.40)$$

[7]т.е. в любом поляризационном базисе (*Прим. переводчика*).

где $\{|u_i\rangle\}$ представляет собой базис для подсистемы A и $\{|v_j\rangle\}$ – базис для подсистемы B. Имеется два важных замечания, которые должны быть сделаны и которые являются абсолютно фундаментальными для понимания корреляций между двумя подсистемами, находящимися в совместном чистом состоянии:

• Редуцированные матрицы плотности обеих подсистем, записанные в базисах Шмидта, диагональны и имеют одинаковые положительные спектры. Мы находим, что редуцированная матрица плотности подсистемы A, найденная как след совместного состояния $\rho_A = |\Psi_{AB}\rangle\langle\Psi_{AB}|$ по всем состояниям подсистемы B, имеет вид

$$\rho_A = Tr_B \rho_{AB} := \sum_q \langle v_q|\rho|v_q\rangle = \sum_p |c_p|^2 |u_p\rangle\langle u_p| \ . \qquad (6.41)$$

Аналогично, находим $\rho_B = \sum_p |c_p|^2 |v_p\rangle\langle v_p|$.

• Если подсистема имеет размерность N, она может быть перепутанной не больше чем с N ортогональными состояниями другой системы.

Мы хотели бы подчеркнуть, что разложение Шмидта, в общем, невозможно выполнить для более чем двух перепутанных подсистем. Математические детали этого факта изложены в [318]. Для внесения ясности, мы однако, рассмотрим, как пример, три перепутанных подсистемы. Мы хотим записать общее состояние так, чтобы при наблюдении состояния одной из подсистем, результат мгновенно и с достоверностью говорил о состоянии двух оставшихся подсистем. Но это невозможно в общем случае, поскольку можно выполнить измерение одной из трех подсистем, такое, что оставшиеся две подсистемы будут являться перепутанными системами (см. разд.6.3.4). Очевидно, что вовлечение в рассмотрение большего числа подсистем еще более усложнит анализ. Такой же аргумент относится и к смешанным состояниям двух или более подсистем (т.е. состояний, для которых и $\rho^2 \neq \rho$), т. е. для которых мы не можем написать в общем случае разложение Шмидта. Единственная причина, приводящая к этому факту, состоит в том, что перепутывание двух подсистем в чистом состоянии понять и количественно описать очень просто, в то время как для смешанных состояний, или состояний, состоящих более чем из двух подсистем, проблема оказывается гораздо более сложной.

Для количественного описания перепутывания в чистом состоянии двух подсистем мы введем следующую «меру неопределенности» квантового состояния системы.

Определение. Энтропией фон Неймана квантовой системы, описываемой матрицей плотности ρ, называется

$$S_N(\rho) := -Tr(\rho \ln \rho). \tag{6.42}$$

(Мы будем опускать индекс N везде, где это не приводит к неясности). Таким образом, перепутывание между A и B можно понимать следующим образом. Неопределенность в системе B до измерения в A есть $S(\rho_B)$, где ρ_B – это редуцированная матрица плотности системы B. После измерения неопределенность исчезает, т.е. мы получаем $\{|u_i\rangle\}$ для A и затем мы узнаем, что состояние B есть $\{|v_i\rangle\}$. Поэтому приобретенная информация составляет $S(\rho_B) = S(\rho_A)$. Таким образом, A и B становятся наиболее перепутанными, когда их редуцированные матрицы плотности максимально смешаны. Конкретно, для системы из двух кубитов, получаем, что максимально перепутанное состояние имеет вид $(|00\rangle + |11\rangle)/\sqrt{2}$.

Имеется и другая физическая интерпретация такой меры неопределенности чистого состояния. А именно, можно показать, что количество перепутывания, которое можно извлечь из чистого состояния, записанного в форме $a|00\rangle + b|11\rangle$, ограничено редуцированной энтропией этого чистого состояния. С другой стороны, если мы хотим приготовить с помощью локальных операций ансамбль систем, каждая из которых находится в состоянии $a|00\rangle + b|11\rangle$, то среднее количество перепутывания на пару, которую нам нужно распределить, снова дается редуцированной энтропией этого чистого состояния.

Для смешанных состояний разложения Шмидта не существует, так что редуцированная энтропия больше не является хорошей мерой перепутывания. Для продолжения количественного определения перепутывания нам необходимо вернуться к процедуре очищения перепутывания. Сначала мы формализуем общую процедуру очищения, а затем, основываясь на этом, укажем три разных способа количественного определения перепутывания.

6.4.2 Процедура очищения

Имеется три разных компоненты, составляющие процедуру, ставящую целью локального выделения подансамбля сильно перепутанных состояний из исходного ансамбля менее перепутанных состояний.

1. Локальные общие измерения (ЛОИ): эти измерения выполняются над парой частиц A и B по отдельности и описываются двумя наборами операторов, удовлетворяющими условиям полноты $\Sigma_i A_i^\dagger A_i = I$ и $\Sigma_j B_j^\dagger B_j = I$. Совместное действие обоих операторов описывается соотношением $\Sigma_{ij} A_i \otimes B_j = \Sigma_i A_i \otimes \Sigma_j B_j$, которое снова является полным общим измерением и очевидно, локальным. Любое локальное общее измерение над системой может быть выполнено, если дать ей провзаимодействовать с дополнительной системой, а затем произ-

вести измерение над дополнительной системой. Ситуация изображена на рис.6.7.

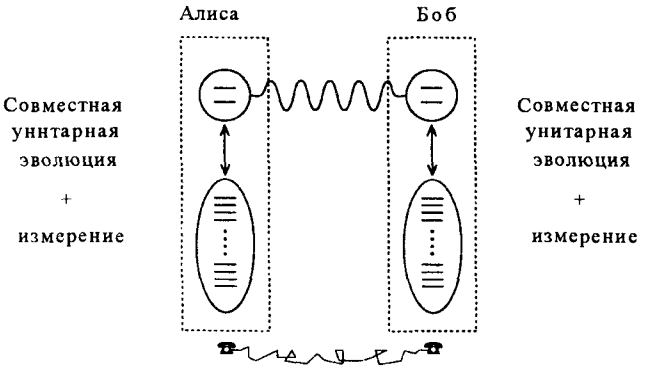


Рис. 6.7. Методы квантового очищения перепутывания позволяют выполнять локальные общие измерения, как показано пунктирными прямоугольниками. К тому же, многоуровневая система взаимодействует с нашим кубитом и, таким образом, происходит измерение над многоуровневой системой. Это наиболее общая форма измерения. Также доступными являются классические сообщения, символично показанные в виде телефонов.

2. *Классическое сообщение* (КС): оно подразумевает, что воздействия A и B должны быть коррелированы. Это может быть описано с помощью *полного измерения* в пространстве $A+B$, как в целом, когда нет необходимости разложения в сумму прямых произведений отдельных операторов (как ЛОИ). Если ρ_{AB} описывает начальное состояние, распределенное между A и B, то преобразование, включающее «ЛОИ + КС» будет выглядеть как

$$\rho_{AB} \to \sum A_i \otimes B_i \rho_{AB} A_i^{\dagger} \otimes B_i^{\dagger} \ , \tag{6.43}$$

т.е. воздействия A и B «коррелированы».

3. Пост-селекция (ПС) выполняется над итоговым ансамблем в соответствие с двумя изложенными выше процедурами (показано на рис. 6.8). Математически это означает, что общее измерение не является полным, т.е. мы пропускаем некоторые операции. Матрица плотности, описывающая вновь полученный ансамбль (подансамбль первоначального ансамбля), должна быть соответствующим образом перенормирована. Предположим, что мы сохраняем только те пары, для которых имелись исходы, соответствующие операторам A_i и B_j, тогда состояние выбранного подансамбля должно быть

$$\hat{\rho}_{AB} \to \frac{A_i \otimes B_j \rho_{AB} A_i^{\dagger} \otimes B_j^{\dagger}}{Tr\left(A_i \otimes B_j \rho_{AB} A_i^{\dagger} \otimes B_j^{\dagger}\right)} \ , \tag{6.44}$$

где знаменатель обеспечивает необходимую нормировку.

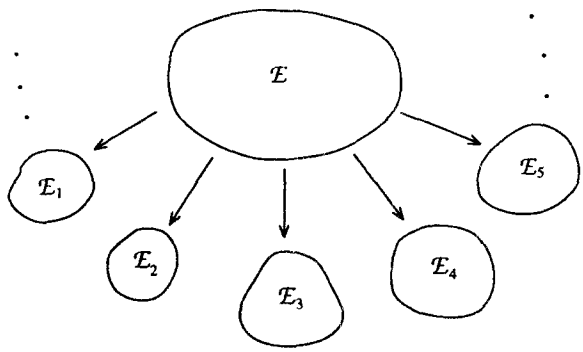


Рис.6.8. Субселекция, в соответствие с результатом локальных измерений, является ключевым компонентом процедуры очищения квантового состояния. Исходный ансамбль ε раскладывается на подансамбли ε_i. Некоторые из этих подансамблей могут иметь более высокую степень перепутывания приходящуюся на одну на пару, чем исходный ансамбль.

Любая манипуляция, включающая в себя три названных элемента, либо их комбинации, называется *процедурой очищения*. Необходимо заметить, что три операции, рассмотренные выше, являются локальными. Это подразумевает, что перепутывание общего ансамбля не может быть увеличено при воздействии таких операций. Однако, классические корреляции между двумя подсистемами могут быть увеличены даже для всего ансамбля, если мы установим классическое сообщение.

Мы предполагаем следующее определение: состояние ρ_{AB} является распутанным (*disentangled*) или сепарабельным, если и только если

$$\rho_{AB} = \sum_i p_i \rho_A^i \otimes \rho_B^i \quad , \tag{6.45}$$

где $\Sigma_i p_i = 1$, и $p_i \geq 0$ для всех i. В других случаях можно говорить, что состояние является перепутанным.

Заметим, что все состояния, которые фигурируют в представленном выше разложении могут быть чистыми. Это происходит потому, что каждое ρ^i может быть разложено по своим собственным векторам. Поэтому, в фигурирующей в разложении сумме можно потребовать дополнительно, чтобы $(\rho^i{}_A)^2 = \rho^i{}_A$ и $(\rho^i{}_B)^2 = \rho^i{}_B$ для всех i. Этот факт будет использован в дальнейшем.

6.4.3 Условия, накладываемые на меры перепутывания

Можно доказать, что кроме определенных состояний, возможно извлечь максимально перепутанные состояния с помощью операций ЛОИ + КС + ПС над субансамблем максимально перепутанных состояний [50]. Распутанные состояния, конечно, не дают перепутыва-

ния при очищении, но обратное утверждение, в общем, неверно; а именно, если состояние является перепутанным, то отсюда не следует с достоверностью, что оно может быть очищено [320]. Вопрос остается открытым – «как много перепутывания» содержит определенное состояние? Этот вопрос не является полностью корректным, если мы не утверждаем, что физические условия характеризуют величину перепутывания. Это утверждение сразу же подразумевает, что мера перепутывания не является единственной в своем роде; в дальнейшем мы кратко коснемся этого вопроса. До того как мы определим три различные меры перепутывания, мы сформулируем четыре условия, которым должны удовлетворять каждая мера перепутывания [321, 322].

E1. $E(\sigma) = 0$ если σ сепарабельно.

E2. Локальные унитарные операции оставляют $E(\sigma)$ инвариантной, т.е. $E(\sigma) = E(U_A \otimes U_B \sigma U^{\dagger}_A \otimes U^{\dagger}_B)$.

E3. Ожидаемое перепутывание не может увеличиться при ЛОИ + КС + ПС, представимом в виде $\Sigma V_i^{\dagger} V_i = I$, т.е.

$$\sum tr(\sigma_i) E(\sigma_i / tr(\sigma_i)) \le E(\sigma) \ , \tag{6.46}$$

где $\sigma_i = V_i \sigma V_i^{\dagger}$.

E4. Для чистых состояний мера перепутывания должна уменьшаться до энтропии редуцированного оператора плотности.

Условие E1 гарантирует, что распутанные и только распутанные состояния имеют нулевое значение перепутывания. Условие E2 гарантирует, что локальное изменение базиса не влияет на величину перепутывания. Условие 3 предназначено для уничтожения возможности увеличения перепутывания при выполнении локальных измерений, поддерживаемых классическими сообщениями. Имеется в виду, что нам достоверно известно конечное состояние. Точнее говоря, начиная с n состояний σ, мы точно знаем, что пары $m_i = n \times Tr(\sigma_i)$ окажутся, в конце концов, в состоянии σ_i после выполнения процедуры очищения. Поэтому, мы можем достигнуть перепутывания отдельно в каждом из возможных подансамблей, описываемых σ_i. Ясно, что в итоге общее перепутывание не должно превосходить исходного перепутывания, что и утверждается в E3. Это, конечно, не исключает возможности выбора подансамбля, перепутывание которого, приходящееся на одну пару, выше, чем исходное перепутывание на одну пару. Четвертое условие было введено в качестве критерия устойчивости, поскольку мера перепутывания чистого состояния является единственной. Введем теперь три различные меры перепутывания, которые удовлетворяют условиям E1-E4. Заметим, что мы могли бы ослабить условие E4. Это позволило бы нам ввести больше мер перепутыва-

ния, что могло бы быть использовано в особых случаях. Соответствующий пример будет приведен ниже.

Сначала обсудим перепутывание формирования (иногда, называемое перепутыванием создания) [323]. Беннет и др. определяют перепутывание формирования состояния ρ как

$$E_c(\rho) := \min \sum_i p_i S(\rho_A^i) \quad , \tag{6.47}$$

где $S(\rho_A) = -Tr\rho_A ln\ \rho_A$ – энтропия фон Неймана и минимум берется по всем возможным реализациям состояния, $\hat{\rho}_{AB} = \Sigma_j p_j |\psi_j\rangle\langle\psi_j|$ и $\hat{\rho}^i_A = Tr_B(|\psi_i\rangle\langle\psi_i|)$. Перепутывание формирования не может быть увеличено при совместном воздействии ЛОИ и КС и, поэтому, удовлетворяет всем четырем условиям E1-E4 [323]. Физическую основу этой меры составляет число синглетов, которые должны быть размещены, чтобы создать данное перепутанное состояние. Необходимо также добавить, что недавно была найдена закрытая форма такой меры [324].

Похожим на эту меру является перепутывание очищения [323]. Оно определяет величину перепутывания состояния σ как количество синглетов, которое должно быть очищено при использовании процедуры очищения. По существу, оно зависит от эффективности специфической процедуры очищения и может быть сделано более общим только при введении некоторого вида универсальных процедур очищения. В отличие от перепутывания формирования, для перепутывания очищения не существует аналитических выражений закрытых форм. Однако, можно рассмотреть некие верхние предельные границы; в дальнейшем мы еще вернемся к этому вопросу.

Введем теперь третью меру, которая в действительности может привести к целому семейству хороших мер перепутывания. Можно убедиться, что эта мера сильно связана с перепутыванием очищения, обеспечивая для нее верхнюю границу [322].

Если $\mathcal{D}$ является множеством всех распутанных состояний (см. Рис.6.9), то мера перепутывания для состояния σ определяется как

$$E(\sigma) := \min_{\rho \in \mathcal{D}} D(\sigma \| \rho) \quad , \tag{6.48}$$

где D – это любая мера расстояния (не обязательно метрическая) между двумя матрицами плотности ρ и σ, такая что $E(\sigma)$ удовлетворяет сформулированным выше условиям E1-E4.

Важный вопрос теперь состоит в том, какому условию должна удовлетворять $D(\sigma \|\rho)$, чтобы E1-E4 поддерживали меру перепутывания? Необходимые и достаточные условия неизвестны, хотя набор достаточных условий существует [321]. Не вдаваясь в математические подробности (при необходимости их можно найти в [322]), мы пред-

ставим одну меру, которая удовлетворяет E1-E4, и другую меру, удовлетворяющую только условиям E1-E3.

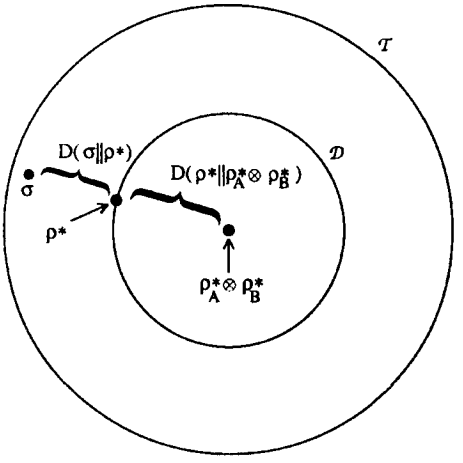


Рис. 6.9. Множество всех матриц плотности, τ представляется внешней окружностью. Его подмножество – набор распутанных состояний $\mathcal{D}$ представляется внутренней окружностью. Состояние σ принадлежит к перепутанным состояниям и ρ^* является распутанным состоянием, которое минимизирует расстояние $D(\sigma\|\rho)$, представляющее, таким образом, величину квантовых корреляций в σ. Состояние $\rho^*_A \otimes \rho^*_B$ получено при нахождения шпура ρ^* по всем A и B. $D(\rho^*\|\rho^*_A \otimes \rho^*_B)$ представляет классическую часть корреляций в состоянии σ.

6.4.4 Две меры расстояния между матрицами плотности

Сначала мы установим, что E1-E4 поддерживают квантовую относительную энтропию, т.е. $D(\sigma\|\rho) = S(\sigma\|\rho) := Tr\{\sigma(\ln\sigma - \ln\rho)\}$ [322]. Заметим, что квантовая относительная энтропия не является истинно метрической, т.к. она несимметрична и не удовлетворяет двойному неравенству. Причины этого факта будут четко установлены в следующем подразделе. Возникает вопрос, почему перепутывание не определяется как $E(\sigma) = \min_{\rho\in\mathcal{D}} S(\sigma\|\rho)$? Поскольку квантовая относительная энтропия асимметрична это приводит к результату, отличному от первоначального определения. Однако, основная проблема этого определения состоит в том, что для максимально перепутанных состояний такая мера бесконечна. Хотя это действительно имеет разумную статистическую интерпретацию (см. следующий раздел), ее трудно отнести к какой-нибудь физически оправданной схеме (как, например, к процедуре очищения перепутывания). Сказанное служит главной причиной, по которой такая форма будет исключена из дальнейшего рассмотрения. Мера перепутывания, генерируемая квантовой от-

носительной энтропией, будет, в дальнейшем, рассматриваться как относительная энтропия перепутывания. Важным результатом является следующая

Теорема (доказательство см. в [322]). Для чистых состояний относительная энтропия перепутывания равна редуцированной энтропии фон Неймана.

Физически это очень полезное свойство меры перепутывания, поскольку хорошо известно, что для чистых состояний редуцированная энтропия фон Неймана служит хорошей мерой перепутывания.

Мы также выделим другой важный результат, состоящий в том, что перепутывание формирования E_c никогда не может быть меньше, чем мера относительной энтропии перепутывания E. Позже мы покажем, что это свойство имеет важное следствие; величина перепутывания, которую мы хотим ввести для создания данного квантового состояния, обычно больше, чем то перепутывание, которое можно получить используя методы очищения квантовых состояний.

Теорема. $E_C(\sigma) \leq E(\sigma) = \min_{\rho \in \mathcal{D}} S(\sigma \| \rho)$.

Добавим, что и перепутывание формирования, и относительная энтропия перепутывания могут быть просто вычислены для диагональных состояний Белла [321]. Оказывается, что для этих состояний перепутывание формирования оказывается значительно больше, чем относительная энтропия перепутывания.

«Закрытая форма» для относительной энтропии перепутывания пока неизвестна, и необходим компьютерный поиск для нахождения минимума ρ^* для каждого данного σ. Однако, используя методы, рассмотренные в следующем разделе, мы можем очень эффективно численно оценить величину перепутывания для двух частиц со спином 1/2.

Пример меры перепутывания, которая удовлетворяет условиям E1-E3, но не удовлетворяет E4, дается (модифицированной) метрической мерой Бюрса, т.е. когда $D(\sigma \| \rho) = D_B(\sigma \| \rho) := 2 - 2F(\sigma,\rho)$, где $F(\sigma,\rho) := [Tr\{\sqrt{\rho}\sigma\sqrt{\rho}\}^{1/2}]^2$ – так называемое качество (для вероятности перехода Ульманна). Мы можем, как и в случае квантовой относительной энтропии, рассчитать меру перепутывания для некоторых простых состояний. Например, для максимально перепутанных состояний, получаем $E = 1$. Следуя логике приведенных выше аргументов, можно показать, что для общего чистого состояния $\alpha|00\rangle + \beta|11\rangle$[8] перепутывание оказывается равным $4\alpha^2\beta^2$. В общем же, необходим компьютерный поиск, как и в предыдущем случае. Обратимся теперь к

[8] То, что это, в действительности, наиболее общая форма, можно увидеть из разложения Шмидта [317].

описанию такого общего компьютерного расчета для относительной энтропии перепутывания.

6.4.5 Численный расчет для частиц со спином 1/2

Поскольку не существует закрытой аналитической формулы для относительной энтропии перепутывания, мы должны прибегнуть к численному поиску, чтобы найти перепутывание общего квантового состояния σ. Такой поиск может быть эффективно выполнен при использовании результатов конвекционного анализа [325]. В последующем, мы используем одно базовое определение и один важный результат конвекционного анализа [325]. Отталкиваясь от них, мы сконцентрируемся на квантовой относительной энтропии как мере перепутывания, хотя большая часть наших рассуждений имеет более общую природу. Для нашей проблемы минимизации, принципиально важной является следующая теорема, поскольку в ней доказывается, что для поиска нам не нужен бесконечный набор параметров в разложении распутанного состояния (6.45).

Теорема Каратеодори. Пусть $A \subset \boldsymbol{R}^N$. Тогда любой $x \in \mathrm{co}(A)$ представим в форме

$$x + \sum_{n=1}^{N+1} p_n a_n,$$

где

$$\sum_{n=1}^{N+1} p_n = 1$$

и для $n = 1,\ldots, N+1$, $p_n \geq 0$, а $a_n \in A$.

Прямое следствие теоремы Каратеодори состоит в том, что любое состояние в $\mathcal{D}$ может быть разложено на сумму не более чем

$$(\dim(H_1) \times \dim(H_2))^2$$

произведений чистых состояний. Поэтому, для двух частиц со спином 1/2 имеется не более 16 членов в разложении любого распутанного состояния в (6.45). Вдобавок, каждое чистое состояние можно описать, используя два действительных числа, так что в этом случае всего имеется не более $15 + 16 \times 4 = 79$ действительных параметров, необходимых для полного задания распутанного состояния.

Заметим, что этот эффективный компьютерный поиск дает альтернативный критерий того, является ли данное состояние σ двух систем со спином 1/2 распутанным, т.е. имеет форму (6.45). Существующий критерий был выведен Пересом и Городецки. Он утверждает, что состояние является распутанным, если его частичный след оказывается отрицательным оператором (см. вторую и третью

ссылки в [326]). Этот критерий работает только для двух систем со спином 1/2 или, когда одна система имеет спин 1/2, а вторая – спин, равный 1. При отсутствии более общего аналитического критерия, наш вычислительный метод дает способ решения этой проблемы.

В заключение этого раздела упомянем понятие *аддитивность*, как важное свойство меры перепутывания, т.е.

$$E(\sigma_{12}\otimes\sigma_{34}) = E(\sigma_{12}) + E(\sigma_{34}) \ , \tag{6.49}$$

где системы 1 + 2 и системы 3 + 4 перепутаны отдельно друг от друга. Точное определение того, что стоит в левой части этого равенства:

$$E(\sigma_{12}\otimes\sigma_{34}) = \min_{\rho_i,\rho_{13},\rho_{24}} S\left(\sigma_{12}\otimes\sigma_{34} \,\|\, \sum_i p_i \rho_{13}^i \otimes \rho_{24}^i\right) . \tag{6.50}$$

Почему нам следует выбрать именно эту форму? Прежде всего нужно было бы предположить, что $\sigma_{12}\otimes\sigma_{34}$ следует минимизировать по состояниям в форме $(\Sigma_i p_i \rho_1 \otimes \rho_2^i)\otimes(\Sigma_j p_j \rho_3 \otimes \rho_4^j)$. Однако, Алиса и Боб также могут выполнить произвольную унитарную операцию над их системами (т.е. локально). Это, очевидно, приводит к образованию перепутывания между 1 и 2, а также между 3 и 4 и отсюда – к форме (6.50). Конечно, как можно заметить из приведенного выше доказательства, аддитивность для чистых состояний уже существует, когда наша мера уменьшает энтропию фон Неймана. В более общем случае мы не в состоянии обеспечить какого бы то ни было аналитического доказательства, поэтому упомянутое выше свойство остается лишь предположением. Однако, для двух систем со спином 1/2, наша программа не нашла никакого контр-примера. Поэтому, мы будем полагать, что это свойство существует. Прямым свойством этого факта, а также условия E3, является то, что относительная энтропия перепутывания служит верхней границей эффективности любой процедуры очищения. А именно, если мы начинаем с n пар в состоянии σ и получаем m синглетов в качестве результата процедуры очищения, то

$$n \times E(\sigma) \geq m \ln 2 \ , \tag{6.51}$$

т.е. эффективность m/n всегда ограничена фактором $E(\sigma)$. Поскольку $E(\sigma)$ может быть меньше, чем перепутывание формирования, это подразумевает, что перепутывание формирования и очищения не обязательно совпадают.

6.4.6 Статистическая основа меры перепутывания

Посмотрим теперь, как можно интерпретировать нашу меру перепутывания с экспериментальной точки зрения, т.е. статистически [327].

Сначала покажем, каким образом в классической теории информации возникает понятие относительной энтропии, как меры различимости двух возможных распределений. Затем мы обобщим эту идею на квантовый случай, т.е. на различимость между двумя квантовыми состояниями (дискуссию о различимости чистых квантовых состояний можно найти, например, в работе [328]). Мы увидим, что это естественно ведет к понятию квантовой относительной энтропии. Далее уже нетрудно распространить эту концепцию для объяснения перепутывания. Предположим, что мы хотели бы проверить является ли данная монета «честной», т.е. описывается ли распределение «орел-решка» функцией $f = (1/2, 1/2)$. Если центр тяжести монеты смещен, то мы получим какие-то другие распределения, скажем, $uf = (1/3, 2/3)$, поэтому наша задача о честности монеты сводится к тому, насколько хорошо мы сумеем различить два данных распределения вероятности за ограниченное число экспериментов n. В случае с монетой мы должны подбросить ее n раз и записать количество нулей и единиц. Какова вероятность того, что честная монета будет названа нечестной, имеющей распределение (1/3, 2/3), при n испытаниях с честной монетой? Для большого n ответ дает теорема Санова [327, 329]:

$$p(\textit{честн.} \to \textit{нечестн.}) = e^{-nS_{cl}(uf\|f)} \quad , \tag{6.52}$$

где

$$S_{cl}(uf \,\|\, f) = 1/3\ln 1/3 + 2/3\ln 2/3 - 1/3\ln 1/2 - 2/3\ln 1/2$$

– классическая относительная энтропия для этих двух распределений. Поэтому,

$$p(\textit{честн.} \to \textit{нечестн.}) = 3^n 2^{-\frac{5}{3}n} \quad , \tag{6.53}$$

что экспоненциально стремится к нулю при $n \to \infty$. На самом деле мы видим, что уже после ~ 20 испытаний вероятность ошибки при идентификации двух распределений ничтожно мала и составляет $\leq 10^{-10}$.

Поэтому в квантовой теории мы формулируем теорему, аналогичную теореме Санова (см также [327])

Теорема (квантовая теорема Санова). Вероятность не различить два квантовых состояния (т.е. матрицы плотности) σ и ρ после n измерений равна

$$p(\rho \to \sigma) = e^{-nS(\sigma\|\rho)} \quad . \tag{6.54}$$

Можно с определенностью утверждать, что эта формулировка дает нижний предел вероятности спутать σ и ρ после проведения n измерений над ρ [327]. В действительности, как было доказано в [330], эта граница достигается асимптотически, а соответствующие измерения являются проекторами независимо от состояния σ [331]. Теперь ин-

терпретация относительной энтропии становится абсолютно прозрачной [327]. Вероятность ошибочной идентификации перепутанного состояния σ от ближайшего распутанного состояния ρ есть

$$e^{-n\times\min_{\rho\in\mathcal{D}} S(\sigma,\rho)} = e^{-nE(\sigma)}$$

Если перепутывание σ больше, то потребуется несколько меньшее число измерений, чтобы отличить его от распутанного состояния (или, при фиксированном n, имеется меньшая вероятность ложно принять его за распутанное состояние). Вот один пример. Рассмотрим состояние $(|00\rangle + |11\rangle)/\sqrt{2}$, которое, как известно, является максимально перепутанным. Ближайшее к нему распутанное состояние – это $(|00\rangle\langle 00| + |11\rangle\langle 11|)/\sqrt{2}$ [321]. Чтобы различить эти два состояния, нужно выполнить проицирование в $(|00\rangle+|11\rangle)/\sqrt{2}$. Если состояние, которое мы измеряем, оказывается указанной выше смесью, то набор результатов (1 для успешного проицирования и 0 для неуспешного) будет содержать в среднем одинаковое число нулей и единиц. Для ошибочно определенного чистого состояния этот набор должен состоять из всех n единиц. Вероятность этого оказывается 2^{-n}, что также можно получить из (6.54). С другой стороны, если мы выполнили проицирование чистого состояния самого на себя, мы никогда не должны были бы спутать его со смесью и из (6.54) вероятность бы оказалась $e^{-\infty}= 0$.

Мы видим, что такая обработка не нуждается в знании числа (или, на самом деле размерности) перепутанных систем. Это как раз то свойство, которое мы хотели бы иметь, поскольку оно делает нашу меру универсальной. Обобщение на случай трех или большего числа систем очевидно [322, 327]. (См. также разд.8.5 о многочастичном очищении перепутывания).

7

Декогерентность и квантовое исправление ошибок

7.1 Введение

Основным препятствием на пути к экспериментальной реализации обработки квантового состояния является квантовая декогерентность. В разделе 7.2 показано, что декогерентность состояния квантовой системы можно представить себе как следствие перепутывания квантовой системы с окружением. В качестве иллюстрации, в разделе 7.3 показан разрушительный эффект декогерентности, возникающей в результате спонтанного излучения в квантовом компьютере на ионной ловушке.

Одним из самых важных достижений в области квантовой информации является открытие методов, позволяющих преодолеть проблему декогерентности. Эти методы, называемые схемами квантового исправления или коррекции ошибок, описаны в разделе 7.4. Они основаны на том факте, что состояние единичного кубита можно закодировать в перепутанных состояниях нескольких кубитов. Симметрия этих состояний, в сочетании с тем фактом, что квантовый шум можно оцифровать с помощью проекционных измерений, делает возможным нахождение и исправление квантовых ошибок. Поскольку сами по себе перепутанные состояния более чувствительны к декогерентности, чем одиночные кубиты, в таких схемах необходим компромисс между добавлением ошибок и их исправлением. В разделе 7.5 мы обратимся к общей теории квантового исправления ошибок и устойчивых к ошибкам вычислений. Задача создания стандарта частоты с помощью рамзеевской спектроскопии является хорошей иллюстрацией реалистичной процедуры исправления ошибок. Она представлена в разделе 7.6.

Еще один способ преодолеть декогерентность состоит в том, чтобы из большого набора перепутанных частиц, чистота которых была испорчена декогерентностью, выделить поднабор частиц с перепутыванием повышенной чистоты. Очищению перепутывания посвящена глава 8.

7.2 Декогерентность

А.К.Экерт, Г.М.Палма, К.А.Суоминен

7.2.1 Декогерентность: перепутывание между кубитами и окружением.

Согласно четвертой главе этой книги, квантовый компьютер можно представить себе как своего рода «программируемый интерферометр», в котором различные вычислительные пути спланированы так, что их конструктивная интерференция приводит к желаемому результату. Чтобы такая интерференция имела место, эволюция компьютера должна быть когерентной – то есть, унитарной. Любое отклонение от унитарности из-за декогерентности испортит видность интерференции.

Декогерентность возникает тогда, когда наши кубиты связаны со своим окружением. Чтобы проиллюстрировать происхождение механизмов декогерентности, предположим, что связь кубита с окружением приводит к совместной унитарной эволюции следующего вида:

$$|0\rangle|E\rangle \xrightarrow{U(t)} |0\rangle|E_0(t)\rangle \qquad |1\rangle|E\rangle \xrightarrow{U(t)} |1\rangle|E_1(t)\rangle \tag{7.1}$$

где $|E\rangle$ – это некоторое фиксированное начальное состояние, и $U(t)$ - унитарный оператор совместной эволюции во времени. В (7.1) окружение действует как измеряющий аппарат, который получает информацию о нашем кубите [332]. Если начальное состояние кубита есть суперпозиция $|0\rangle$ и $|1\rangle$, то $U(t)$ создаст перепутывание между кубитом и окружением:

$$\left(a_0|0\rangle + a_1|1\rangle\right)\otimes|E\rangle \xrightarrow{U(t)} a_0|0\rangle|E_0(t)\rangle + a_1|1\rangle|E_1(t)\rangle \tag{7.2}$$

Декогерентность возникает именно из-за этого перепутывания, поскольку, когда мы возьмем след по степеням свободы окружения, появится неунитарность. Приведенная матрица плотности кубита, соответствующая состоянию (7.2), равна

$$\rho_q(t) = \mathrm{Tr}_E \rho_{q+E} = \begin{bmatrix} |a_0|^2 & a_0 a_1^* \langle E_1 | E_0 \rangle \\ a_1 a_0^* \langle E_0 | E_1 \rangle & |a_0|^2 \end{bmatrix} \tag{7.3}$$

В большинстве случаев состояния $|E_0(t)\rangle$, $|E_1(t)\rangle$ со временем становятся все более ортогональными друг другу, то есть, все больше информации о кубите перетекает к окружению. Этот факт удобно записать в виде

$$\langle E_0(t) | E_1(t)\rangle = e^{-\Gamma(t)} \tag{7.4}$$

где конкретная форма функции времени $\Gamma(t)$ будет зависеть от особенностей связи между кубитом и окружением [332]. Ее значение за-

висит от типа кубитов и их взаимодействия с окружением, и может находиться в пределах от 10^4 секунд для ядерных спинов в парамагнитном атоме до 10^{-12} секунд для электронно-дырочного взаимодействия в объеме полупроводника [334]. Как следствие, специфическое перепутывание, описываемое выражением (7.2), уничтожает недиагональные матричные элементы в матрице плотности – так называемые «когерентности», – оставляя без изменений диагональные элементы, известные как «населенности». Этот эффект называют также дефазировкой. Позже мы опишем перепутывание кубита с окружением другого рода. С точки зрения вычислительной сложности, важно знать, как меняется характерное время декогерентности в зависимости от размеров квантового компьютера. Для этого введем модель связи кубита с окружением, которая генерирует такую эволюцию во времени, которая описана уравнением (7.1). Мы представим окружение в виде резервуара гармонических осцилляторов [333, 335], и предположим, что гамильтониан взаимодействия между одиночным кубитом и его окружением имеет вид

$$H = \frac{1}{2}\sigma_z\omega_0 + \sum_{\mathbf{k}} b_{\mathbf{k}}^{\dagger} b_{\mathbf{k}}\omega_{\mathbf{k}} + \sum_{\mathbf{k}} \sigma_z (g_{\mathbf{k}} b_{\mathbf{k}}^{\dagger} + g_{\mathbf{k}}^{*} b_{\mathbf{k}}) \ , \tag{7.5}$$

где $\omega_{k'}$ $b_{\mathbf{k}}{}^{\dagger}$, $b_{\mathbf{k}}$ – это, соответственно, частота и бозонные операторы рождения и уничтожения в **k**-й моде в нашем резервуаре осцилляторов, и σ_Z – это оператор псевдоспина Паули. Первый и второй члены в правой части уравнения (7.15) описывают, соответственно, свободную эволюцию кубита и окружения, а третий член описывает взаимодействие между ними. Состояние всей системы (кубит + окружение) описывается оператором плотности $\mathcal{P}(t)$. Мы предполагаем, что в момент времени $t = 0$ он был равен

$$\mathcal{P}(0) = |\psi\rangle\langle\psi| \otimes \prod_{\mathbf{k},\mathbf{k}'} |0_{\mathbf{k}}\rangle\langle 0_{\mathbf{k}'}| = \rho(0) \otimes |vac\rangle\langle vac| \tag{7.6}$$

где $|\psi\rangle$ обозначает начальное состояние кубита, и $|vac\rangle = \Pi_{\mathbf{k}}|0_{\mathbf{k}}\rangle$ – это состояние вакуума всех мод в резервуаре. Поскольку $[\sigma_Z, H] = 0$, окружение не влияет на населенности в матрице плотности, и $\rho(t) = \mathrm{Tr}_R \mathcal{P}(t)$ не изменяется. В нашей модели, как и ожидалось, окружение просто разрушает квантовую когерентность. Эта модель, в которой решение находится точно, позволяет провести ясный анализ механизма перепутывания между кубитом и окружением. Похоже, именно этот механизм лежит в основе большинства процессов появления декогерентности.

Можно легко показать, что в представлении взаимодействия оператор эволюции $U(t)$ есть оператор условного сдвига для поля [333], причем знак сдвига зависит от логического значения кубита. Следовательно, $U(t)$ вызывает динамику того же типа, что описана в (7.2), с

$$|E_0\rangle = \prod_{\mathbf{k}} |-\phi_{\mathbf{k}}\rangle \qquad |E_1\rangle = \prod_{\mathbf{k}} |\phi_{\mathbf{k}}\rangle \ , \tag{7.7}$$

где состояния $|\phi_{\mathbf{k}}\rangle$ – это когерентные состояния с амплитудами $\phi_{\mathbf{k}} = g_{\mathbf{k}}(1 - e^{\omega_{\mathbf{k}} t})/\omega_{\mathbf{k}}$.
Детальное вычисление $\Gamma(t)$ и обобщение анализа на случай конечных температур можно найти в работах [333, 335].

7.2.2 Коллективное взаимодействие и масштабирование

Теперь у нас есть все необходимые данные, чтобы анализировать проявление декогерентности в регистре из n кубитов [333]. В этом случае гамильтониан принимает вид:

$$H = \frac{1}{2}\sum_i \sigma_{z,i}\omega_0 + \sum_{\mathbf{k}} b_{\mathbf{k}}^{\dagger} b_{\mathbf{k}} \omega_{\mathbf{k}} + \sum_{i,\mathbf{k}} \sigma_z (g_{i,\mathbf{k}} b_{\mathbf{k}}^{\dagger} + g_{i,\mathbf{k}}^{*} b_{\mathbf{k}}) \ , \tag{7.8}$$

где константы связи $g_{i,\mathbf{k}}$ теперь будут зависеть от координаты кубита под номером i. Перепутывание, описываемое этим гамильтонианом, будет иметь вид

$$\left(\sum_{i_1 \ldots i_n} c_{i_1 \ldots i_n} |i_1 \ldots i_n\rangle\right) \otimes |vac\rangle \xrightarrow{U(t)} \sum_{i_1 \ldots i_n} c_{i_1 \ldots i_n} |i_1 \ldots i_n\rangle |E_{i_1, i_2 \ldots i_n}\rangle \ , \tag{7.9}$$

где i_n обозначает логическое значение кубита под номером n. Резервуар гармонических осцилляторов будет теперь характеризоваться длиной когерентности λ_c, на которой их флуктуации скоррелированы. Будет полезно найти вид состояний

$$|E_{i_1 \ldots i_n}\rangle$$

в двух предельных физически важных случаях, в зависимости от отношения физического размера нашего регистра к λ_c.

Малые λ_c. В этом случае каждый кубит будет чувствовать свое собственное окружение, и терять когерентность он будет индивидуально. Мы получим

$$|E_{i_1 \ldots i_n}\rangle = |E_{i_1}\rangle |E_{i_2}\rangle \ldots |E_{i_n}\rangle \ , \tag{7.10}$$

где все $|E_{in}\rangle$ – такие же, как в (7.7), и матричные элементы в операторе матрицы плотности будут распадаться по закону

$$\rho_{i_1 \ldots i_n, j_1 \ldots j_n}(t) = \rho_{i_1 \ldots i_n, j_1 \ldots j_n}(0) \langle E_{i_1} | E_{j_1}\rangle \langle E_{i_2} | E_{j_2}\rangle \ldots \langle E_{i_n} | E_{j_n}\rangle \ . \tag{7.11}$$

Самый быстрый распад будет у матричного элемента

$$\rho_{11 \ldots 1, 00 \ldots 0}(t) = \rho_{11 \ldots 1, 00 \ldots 0}(0) \langle E_1 | E_0\rangle^n = \rho_{11 \ldots 1, 00 \ldots 0}(0) e^{-n\Gamma(t)} \ . \tag{7.12}$$

Большие λ_c. Если длина когерентности λ_c достаточно велика, то

можно предположить, что все кубиты взаимодействуют с окружением коллективно – то есть, можно предположить, что для всех кубитов $g_{i,k} = g_k$. Тогда U(t) будет оператором условного сдвига с амплитудой, зависящей от логического значения *всех* кубитов в регистре. В более явном виде,

$$\left|E_{i_1\ldots i_n}\right\rangle = \prod_{\mathbf{k}} \left|-\{(-1)^{i_1} + (-1)^{i_2}\ldots(-1)^{i_n}\}\phi_{\mathbf{k}}\right\rangle . \tag{7.13}$$

Быстрее всего будет распадаться

$$\rho_{11\ldots1,00\ldots0}(t) = \rho_{11\ldots1,00\ldots0}(0)\left\langle E_{11\ldots1} \mid E_{00\ldots0}\right\rangle = \rho_{11\ldots1,00\ldots0}(0)e^{-n^2\Gamma(t)} \tag{7.14}$$

Можно легко понять физическое происхождение коэффициента n^2 в экспоненте, если заметить, что $|E_{00\ldots0}\rangle$, $|E_{11\ldots1}\rangle$ есть тензорное произведение когерентных состояний амплитуды $n\phi_{\mathbf{k}}$.

Вышеприведенное обсуждение показывает, что распад когерентностей в регистре из n кубитов масштабируется как $\exp[-Poly(n)\gamma(t)]$, где $Poly(n) \sim n$ при индивидуальном взаимодействии кубитов с окружением, и $Poly(n) \sim n^2$ при коллективном взаимодействии.

7.2.3 Подпространство, не связанное с окружением

Надо заметить, что коллективные взаимодействия приводят не только к более быстрому распаду, но и к появлению областей, не связанных с окружением. Как ясно следует из уравнения (7.13), состояния с равным числом 0 и 1 не перепутываются с окружением и, следовательно, не подвержены декогерентности. Другими словами, взаимодействие не сдвигает амплитуду мод поля. Отсюда следует идея использовать изолированное подпространство в простой форме избыточного кодирования. Предположим, что мы создали в лаборатории квантовый регистр из 2L кубитов, составленный из пар кубитов, находящихся достаточно близко друг к другу, так что кубиты в каждой паре эффективно взаимодействуют с одним и тем же резервуаром. Разные пары могут взаимодействовать с разными резервуарами, хотя результат, который мы здесь хотим проиллюстрировать, не изменится, если все кубиты будут взаимодействовать с одним и тем же резервуаром. Тогда мы можем закодировать логические состояния следующим образом

$$\left|\tilde{0}\right\rangle = \left|0,1\right\rangle \ , \qquad \left|\tilde{1}\right\rangle = \left|1,0\right\rangle \ . \tag{7.15}$$

Идея состоит в том, что если мы сможем использовать пару кубитов, чтобы закодировать каждый бит, то мы сможем эффективно изолировать регистр от окружения.

При таком кодировании несколько вопросов остаются открытыми. Во-первых, надо гарантировать, что такие состояния будут устойчи-

выми также и к другим каналам декогерентности (к этому вопросу мы обратимся в следующем разделе). Во-вторых, остается проблема того, как приготовить такие состояния (состояния, изолированные от окружения, обычно также изолированы и от внешних пробных воздействий) и как их считывать (это будет означать коллективные измерения). Наконец, пока неясно, как осуществить квантовое вычисление, которое будет ограничено такими подсистемами. Управляемые взаимодействия между кубитами могут оказаться полезным инструментом при создании логического элемента [336, 337].

7.2.4 Другое определение связей

В оставшейся части этого раздела мы обсудим, какие из полученных результатов останутся в силе, если мы рассмотрим более реалистичный механизм взаимодействия кубитов с окружением. Модель, которую мы кратко проанализируем, используется при описании широкого круга различных физических явлений – таких, как обмен фотонами между электромагнитным полем и двухуровневым атомом в квантовой оптике [338]. В этой модели, гамильтониан системы из n кубитов, связанных с резервуаром гармонических осцилляторов, равен

$$H = \frac{1}{2}\sum_i \sigma_{z,i}\omega_0 + \sum_{\mathbf{k}} b_{\mathbf{k}}^{\dagger} b_{\mathbf{k}}\omega_{\mathbf{k}} + \sum_{i,\mathbf{k}} (g_{i,\mathbf{k}}\sigma_{-,i} b_{\mathbf{k}}^{\dagger} + g_{i,\mathbf{k}}^{*}\sigma_{+,i} b_{\mathbf{k}}) \ , \qquad (7.16)$$

где символы $\sigma_{-,i}$ и $\sigma_{+,i}$ обозначают понижающий и повышающий операторы для кубита i.

Динамику, порожденную гамильтонианом (7.16), нельзя найти точно. Однако в так называемом приближении Борна-Маркова, эволюцию во времени оператора приведенной матрицы плотности кубита можно описать с помощью мастер-уравнения [338, 339]. Если расстояние между кубитами меньше, чем длина волны в резонансных модах, то логично предположить, что $g_{i,\mathbf{k}} \sim g_0$, и нужное нам мастер-уравнение есть

$$\frac{\partial \rho}{\partial t} = i\omega_0 \rho - \frac{\gamma}{2}\left(S_+ S_- \rho + \rho S_+ S_- - 2S_- \rho S_+\right) \ , \qquad (7.17)$$

где мы ввели коллективные операторы $S_Z = \Sigma_i \sigma_{Z,i}, S_{\pm} = \Sigma_{\pm i}\sigma_{\pm}$, и константу связи $\gamma \propto |g_0|^2 \delta(\omega_k - \omega_0)$.

Очевидно, что динамика, порождаемая (7.17), неунитарна. Неунитарность возникает опять из-за перепутывания между кубитом и окружением, хотя здесь это и не столь очевидно, как в точно решаемой модели, рассмотренной в предыдущем разделе.

В случае диссипации одиночного кубита, приведенная матрица плотности в момент времени t будет равна

$$\rho(t)=\begin{pmatrix}(1-\rho_{11})e^{-\gamma t} & \rho_{10}e^{-\frac{\gamma}{2}t}\\ \rho_{01}e^{-\frac{\gamma}{2}t} & \rho_{11}e^{-\gamma t}\end{pmatrix}, \tag{7.18}$$

откуда ясно видно, что данная модель связи порождает декогерентность и распад населенностей.

Чтобы проиллюстрировать характерные черты коллективного взаимодействия в этом новом сценарии, будет полезно обсудить распад перепутанных белловских состояний $|\Psi_{\pm}\rangle = 1/\sqrt{2}(|01\rangle \pm |01\rangle)$. Амплитуда вероятности для распада в состояние $|00\rangle$ пропорциональна матричному элементу оператора S_+

$$\langle\Psi_{\pm}|S_{\pm}|00\rangle=\frac{1}{\sqrt{2}}\left\{\langle 01|\sigma_{+2}|00\rangle \pm \langle 10|\sigma_{+1}|00\rangle\right\}. \tag{7.19}$$

Отсюда ясно видно, каким образом конструктивно интерферируют *амплитуды* вероятности состояния $|\Psi_+\rangle$, что приводит к скорости распада вдвое большей, чем у одиночного кубита. В то же время, у состояния $|\Psi_-\rangle$ амплитуды интерферируют деструктивно. Для большого числа n кубитов, коллективный распад приведет к величинам констант распада от $n\gamma$ до $n^2\gamma$, в то время как синглетное коллективное состояние вообще не будет связано с окружением. В этом состоит хорошо известный эффект сверхизлучения [339,340]. Отсюда опять следует идея о возможности использовать несвязанные с окружением подпространства регистра из n кубитов [341]. Конечно, и в этом случае остаются все трудности, о которых говорилось в предыдущем разделе.

В заключение нам хотелось бы отметить, что, хотя различные модели приводят к различным механизмам распада и требуют различного описания, многие качественные черты процесса появления декогерентности не зависят от специфической модели связи. В частности, все процессы декогерентности приводят к неунитарой эволюции квантового регистра во времени. Кроме того, коллективное взаимодействие повысит скорость распада некоторых подпространств в регистре и запретит распад некоторых других. Следовательно, наше рассмотрение масштабирования времени декогерентности с размером нашего квантового компьютера, а также рассмотрение коллективных взаимодействий остается в силе вне зависимости от конкретных деталей связи кубитов с окружением.

7.3 Ограничения квантового вычисления из-за декогерентности.

М. Б. Пленио, П. Л. Найт

В предыдущем разделе были представлены модели, описывающие декогерентность и диссипацию в массиве кубитов, применимые, например, к набору ионов (см. главу 5). После этих общих рассмотрений, мы теперь оценим, насколько серьёзной будет роль шума в квантовом компьютере. В частности, хотелось бы понять, сколько операций мы в принципе можем совершить, например, с квантовым компьютером на ионной ловушке, принципы работы которого были описаны в разделе 4.3 и в главе 5 [156]. Здесь мы не будем обсуждать другие возможные реализации квантового компьютера – например, схемы на ядерном магнитном резонансе [342, 343] (см. также раздел 5.4).

Существует много различных механизмов возникновения шума в квантовом компьютере. В этом разделе мы опишем только эффект спонтанного излучения ионов [344 – 347], поскольку этот анализ весьма поучителен. Другие механизмы, например, шум в моде центра масс [348], лазерные нестабильности и взаимное влияние различных ионов из-за их малого пространственного разделения [349], здесь не будут обсуждаться. За описанием этих эффектов мы отсылаем читателя к цитированной литературе.

Сейчас мы хотим оценить влияние спонтанного излучения на квантовый компьютер. Обсудим для этого алгоритм факторизации больших чисел [350]. Это обсуждение можно легко обобщить на другие алгоритмы. Как было показано в разделе 4.2, задачу факторизации тяжело решить с помощью классического компьютера, и на нем не удается решить ее эффективно. Однако для квантового компьютера эффективный алгоритм был найден. В идеальных условиях, этот алгоритм позволил бы квантовому компьютеру найти простые множители большого числа экспоненциально быстрее, чем это возможно для классического компьютера. Теперь мы обсудим, чему равно наибольшее число, которое можно факторизовать на квантовом компьютере при условии, что единственным источником ошибок является спонтанная эмиссия ионов. Для простоты анализа, мы здесь не рассматриваем возможность квантового исправления ошибок, а отсылаем читателя к соответствующей литературе [346] и к следующему разделу этой главы.

Рассмотрим следующую экспериментальную установку. Цепоч-

ка ионов помещена в линейную ионную ловушку, и ее поступательное движение охлаждено до основного состояния. Каждый кубит представлен метастабильным оптическим переходом в ионе. Внутренняя структура ионов, которую мы рассматриваем, показана на Рис.7.1. Кубит представлен атомными уровнями 0 и 1. Переходы вызываются лазерным излучением с частотой Раби Ω_{0i}, а скорость спонтанной эмиссии с уровня i равна $2\Gamma_{ii}$. Наличие второго уровня 2 важно, его вклад будет обсуждаться далее. Конечно, возможны и более сложные методы описания такого кубита – например, с учетом зеемановских подуровней; но в этом случае анализ усложняется, в то время как выводы остаются теми же самыми. Поэтому за более подробным анализом мы отсылаем читателя к литературе [346].

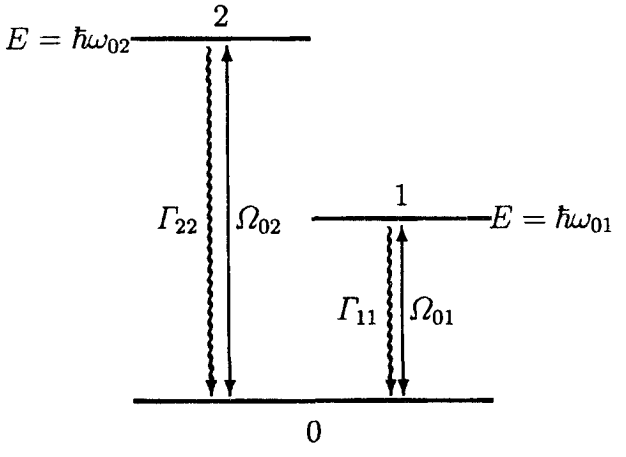


Рис. 7.1. Схематический вид уровней ионов, используемых в квантовом вычислении. Переход $0 \leftrightarrow 1$ представляет кубит. Он управляется лазерным полем с частотой Раби Ω_{01}. Скорость спонтанного распада с уровня 1 равна $2\Gamma_{11}$, и предполагается, что она мала. Лазерное поле, резонансное по отношению к переходу $0 \leftrightarrow 1$, неизбежно связывает уровень 0 еще и с другими нерезонансными уровнями, например, с уровнем 2. Частота Раби этого перехода равна Ω_{02}, и скорость распада $2\Gamma_{22}$ обычно гораздо больше, чем $2\Gamma_{11}$. Эффективная частота Раби перехода $0 \leftrightarrow 2$ очень мала, так как лазер отстроен на $\Delta_{02} >> \Omega_{02}$.

Наша цель – факторизация числа из L битов, то есть, числа, не превышающего 2^L. Из свойств алгоритма Шора [350] мы знаем, что эту задачу можно выполнить за εL^3 элементарных операций – таких, как, например, однобитные операции, CNOT (контролируемое НЕТ), или элементы Тоффоли. Были разработаны сети, выполняющие эту задачу [351], и оказывается, что алгоритму для факторизации числа из L битов требуется порядка $5L$ кубитов.

Сколько нужно времени, чтобы выполнить все эти операции? Для работы ячейки Тоффоли требуется в 1.5 раза больше времени, чем для логического элемента CNOT [156]. Следовательно, достаточно вычислить время, необходимое для выполнения CNOT. Однобитные логические элементы не рассматриваются, поскольку они работают гораздо быстрее. Причина этого в том, что, в отличие от элемента CNOT, для выполнения однобитных операций не требуется возбуждение моды центра масс (см. раздел 5.2.9).

Для выполнения операции CNOT требуется время

$$\tau_{el} = 4\pi \frac{\sqrt{5L}}{\eta \Omega_{01}} \quad . \tag{7.20}$$

Здесь $5L$ есть число ионов в ловушке, Ω_{01} обозначает рабиевскую частоту лазера, которая управляет переходом в кубите, и η – это параметр Лэмба-Дике (см. детали эксперимента в главе 5). Следовательно, полное время, необходимое для факторизации числа из L битов – это число операций CNOT, умноженное на τ_{el}:

$$T = \frac{4\pi\sqrt{5L}}{\eta \Omega_{01}} \varepsilon L^3 \quad . \tag{7.21}$$

Очевидно, что это выражение содержит в себе три параметра. В частности, может показаться, что мы можем насколько угодно увеличить рабиевскую частоту, чтобы произвести вычисление очень быстро. Это позволило бы нам избежать спонтанной эмиссии с верхнего уровня. Однако все не так просто. Дело в том, что рабиевская частота перехода и постоянная распада этого перехода связаны соотношением

$$\frac{\Omega^2}{\Gamma} = \frac{6\pi c^3 \varepsilon_0}{\hbar \omega_{01}^3} E^2 \quad , \tag{7.22}$$

где E – это амплитуда электрического поля лазера, c – скорость света, ε_0 – диэлектрическая проницаемость свободного пространства, ω_{01} – частота перехода. Даже согласно этому выражению видно, что можно произвольно увеличивать амплитуду поля. Очевидно, что у этого процесса должны быть какие-то верхние пределы. Если поле E настолько велико, что превышает электрическое поле между электроном и ядром, то ион немедленно ионизуется. Этот предел, однако, очень высок, так что более важны другие эффекты. На самом деле, при сильном поле лазера нельзя предполагать, что у иона задействованы только два энергетических уровня. Другие уровни будут также вносить вклад в динамику системы, поскольку они могут приобрести небольшие населенности благодаря нерезонансным переходам на них. Эта ситуация

представлена на Рис. 7.1. Кроме уровней кубита 0 и 1, вокруг присутствуют еще и другие, далеко отстроенные уровни. Мы учитываем влияние всех этих уровней с помощью одного дополнительного уровня 2, который связан с нижним состоянием кубита 0. Из-за того, что лазер далеко отстроен от перехода 0↔2, населенность верхнего уровня будет небольшой. Однако, спонтанная эмиссия с этого уровня все-таки может происходить – особенно, если у этого дополнительного уровня будет очень короткое время жизни. Чем сильнее поле управляющего лазера, тем больше населенность на этом дополнительном уровне. Следовательно, нам надо искать компромисс между спонтанным излучением с верхнего уровня кубита и спонтанным излучением с дополнительного уровня. Чем быстрее вычисление, тем меньше спонтанное излучение с верхнего состояния кубита 1, но тем сильнее спонтанное излучение с дополнительного уровня.

Ниже мы вычисляем полную вероятность p_{tot} излучения с уровней 1 и 2. Наша цель состоит в том, чтобы минимизировать эту вероятность. Минимизация дает не зависящий от интенсивности размер числа, которое можно факторизовать в квантовом компьютере со спонтанной эмиссией.

В течение всего квантового вычисления, в среднем, примерно половина кубитов находится в верхнем состоянии. Следовательно, вероятность спонтанной эмиссии с верхнего уровня в течение всего вычисления равна

$$p_1 = \frac{1}{2} 2\Gamma_{11}\, 5LT \ . \tag{7.23}$$

С другой стороны, дополнительный уровень населен только во время взаимодействия иона с лазерным полем. Следовательно, вероятность спонтанной эмиссии с дополнительного уровня равна

$$p_2 = \frac{\Omega_{02}^2}{8\Delta_{02}} 2\Gamma_{22} T \ . \tag{7.24}$$

Если мы теперь используем (7.22), что дает

$$\frac{\Omega_{01}^2}{\Gamma_{11}} = \frac{\omega_{02}^3}{\omega_{01}^3} \frac{\Omega_{02}^2}{\Gamma_{22}} \ , \tag{7.25}$$

и определим

$$x = \sqrt{\frac{\Omega_{01}^2}{\Gamma_{11}}} \ , \tag{7.26}$$

то получим, с помощью (7.21),

$$p_{tot} = p_1 + p_2 \tag{7.27}$$

$$= \frac{4\pi\sqrt{5L}}{\eta}\varepsilon L^4\sqrt{\Gamma_{11}}\left[\frac{1}{x}+\frac{1}{L}\frac{\omega_{01}^3}{\omega_{02}^3}\frac{\Gamma_{22}^2}{4\Delta_{02}\Gamma_{11}}x\right] . \qquad (7.28)$$

Теперь мы можем минимизировать это выражение по отношению к x, и получить выражение для минимума

$$p_{\min} = \frac{4\pi\sqrt{5}\varepsilon L^4}{\eta}\sqrt{\frac{\omega_{01}^3}{\omega_{02}^3}}\sqrt{\frac{\Gamma_{22}^2}{\Delta_{02}^2}} . \qquad (7.29)$$

Чтобы гарантировать, что с высокой вероятностью во время вычисления не будет спонтанного излучения, мы должны потребовать выполнение условия $p_{min} \ll 1$. Тогда (7.29) переходит в выражение для верхнего предела для L, которое дает

$$L_{\max}^8 \approx \frac{\eta^2\Delta_{02}^2}{80\Gamma_{22}^2\pi^2\varepsilon^2}\left(\frac{\omega_{02}}{\omega_{01}}\right)^3 . \qquad (7.30)$$

Читатель может поинтересоваться, откуда берется степенная зависимость вида L^8. Ее источником является управляющий цикл с положительной обратной связью, показанный на Рис. 7.2.

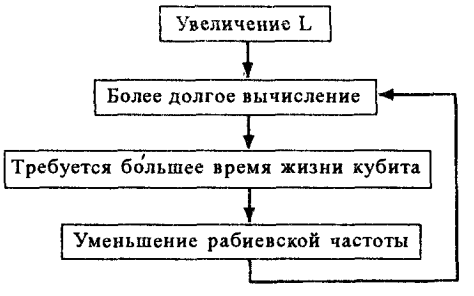


Рис. 7.2. Сильная зависимость от L в (7.30) вызвана положительной обратной связью. Если мы попробуем увеличить L, наше вычисление станет длиннее. Это потребует большего времени жизни кубита, что уменьшает допустимую рабиевскую частоту в переходе в кубите. Это еще больше увеличивает время вычисления.

Чтобы увидеть, насколько серьезно это ограничение, нам надо подставить в уравнение некоторые числа. Мы воспользуемся значениями для реальных ионов, то есть, для ионов, которые используются в экспериментах с ионными ловушками.

В Таблице 7.1 (взятой из работы [346]) приведены данные для некоторых реальных атомов. Получающиеся пределы для чисел, которые можно факторизовать, очень низки. Это значит, что даже шум

из-за спонтанной эмиссии накладывает серьезные ограничения на квантовое вычисление. Вот почему ученые в этой области стараются развить методы, которые позволили бы исправлять ошибки, возникающие из-за шума – например, из-за спонтанной эмиссии. Эти методы будут представлены в следующем разделе. Оказывается, что они могут смягчить ограничения, которые мы получили в этой главе.

Таблица 7.1. Для нескольких возможных квантовых систем посчитан размер в битах L числа N, которое можно факторизовать на квантовом компьютере. Значение кубита хранится в метастабильном оптическом переходе. Приведены атомные уровни, обозначенные на Рис. 7.1 как 0, 1 и 2. Атомные характеристики подставлены в (7.30), и результат приведен в последней строке таблицы.

Ион	Ca+	Hg+	Ba+
уровень 0	$4s^2S_{1/2}$	$5d^{10}6s^2{}^2S_{1/2}$	$6s^2S_{1/2}$
уровень 1	$3d^2D_{5/2}$	$5d^96s^2{}^2D_{5/2}$	$5d^2D_{5/2}$
уровень 2	$4s^2P_{3/2}$	$5d^{10}6p^2{}^2P_{1/2}$	$6s^2P_{3/2}$
$\omega_{01}[c^{-1}]$	$2.61\cdot10^{15}$	$6.7\cdot10^{15}$	$1.07\cdot10^{15}$
$\omega_{02}[c^{-1}]$	$4.76\cdot10^{15}$	$11.4\cdot10^{15}$	$4.14\cdot10^{15}$
$\Gamma_{22}[c^{-1}]$	$67.5\cdot10^{6}$	$5.26\cdot10^{8}$	$58.8\cdot10^{6}$
$L(\eta = 0.01)$	2.2	1.6	4.5

7.4 Исправление ошибок и устойчивое к сбоям вычисление.

С. Макиавелло, Г.М. Палма

7.4.1 Процедуры симметризации.

Первое средство, которое было предложено для борьбы с квантовым шумом, было основано на процедуре симметризации [352]. Здесь мы кратко опишем его основную идею. Предположим, что у вас есть квантовая система, приготовленная в некотором начальном состоянии $|\psi_i\rangle$, и вы хотите либо осуществить некоторую заданную унитарную эволюцию $|\psi(t)\rangle$, либо просто сохранить $|\psi_i\rangle$ в течение некоторого периода времени t. Теперь, предположим, что, вместо одной единственной системы, вы можете приготовить R копий $|\psi_i\rangle$, а затем спроектиро-

вать состояние полной комбинированной системы на симметричное подпространство – то есть, на подпространство, содержащее все состояния, инвариантные относительно перестановки подсистем. Утверждение состоит в том, что часто повторяемое проицирование на симметричное подпространство снизит количество ошибок, вызванных окружением. Интуитивное объяснение этой идеи основано на том наблюдении, что предписанное свободное от ошибок хранение либо эволюция R независимых копий системы начинается в симметричном подпространстве, и должно в нем же и оставаться. Следовательно, поскольку свободная от ошибки компонента любого состояния лежит в симметричном подпространстве, то при удачном проицировании она не изменится, тогда как часть ошибки будет удалена. Заметим, однако, что спроицированное состояние не будет, в общем случае, полностью свободным от ошибки, поскольку симметричное подпространство содержит и такие состояния, которые не являются простым произведением вида $|\psi\rangle|\psi\rangle...|\psi\rangle$. Тем не менее, было показано, что вероятность ошибки снизится в R раз [353].

Далее мы проиллюстрируем этот эффект на простейшем примере двух кубитов. В этом случае проекция на симметричное подпространство выполняется введением оператора симметризации

$$S = \frac{1}{2}\left(P_{12} + P_{21}\right) , \tag{7.31}$$

где P_{12} представляет собой тождественный оператор, а P_{21}– оператор перестановки, который меняет местами состояния двух кубитов. Симметричная проекция чистого состояния двух кубитов $|\psi\rangle$ есть просто состояние $S|\psi\rangle$, отнормированнное затем на единицу. Следовательно, получающееся отображение двух кубитов на смешанные состояния (с учетом перенормировки) есть

$$\rho_1 \otimes \rho_2 = \frac{S(\rho_1 \otimes \rho_2)S^\dagger}{\mathrm{Tr}\, S(\rho_1 \otimes \rho_2)S^\dagger} . \tag{7.32}$$

Состояние каждого кубита, взятого отдельно, получается тогда частичной сверткой по другому кубиту.

Предположим, что изначально приготовлены две копии чистого состояния $\rho_0 = |\psi\rangle\langle\psi|$, и что они независимо взаимодействуют, каждая со своим окружением. После некоторого короткого промежутка δt состояние двух копий $\rho^{(2)}$ претерпит эволюцию

$$\rho^{(2)}(0) = \rho_0 \otimes \rho_0 \qquad \rightarrow \qquad \rho^{(2)}(\delta t) = \rho_1 \otimes \rho_2 , \tag{7.33}$$

где $\rho_i = \rho_0 + \mathcal{P}_i$ для некоторой эрмитовой $\mathcal{P}_i$ с нулевым следом. Мы оставим только члены первого порядка по возмущениям $\mathcal{P}_i$. Тогда общее состояние в момент времени δt будет иметь вид

$$\rho^{(2)} = \rho_0 \otimes \rho_0 + \mathcal{P}_1 \otimes \rho_0 + \rho_0 \otimes \mathcal{P}_2 + \mathrm{O}(\mathcal{P}_1\mathcal{P}_2) \tag{7.34}$$

Мы можем найти среднюю степень чистоты двух состояний до симметризации, сосчитав средний след квадрата состояний:

$$\frac{1}{2}\sum_{i=1}^{2}\mathrm{Tr}\left(\left(\rho_0 + \mathcal{P}_i\right)^2\right) = 1 + \mathrm{Tr}\left(\rho_0\tilde{\mathcal{P}}\right) , \tag{7.35}$$

где $\mathcal{P} = 1/2(\mathcal{P}_1 + \mathcal{P}_2)$. Заметим, что след $\mathrm{Tr}(\rho_0\mathcal{P})$ отрицателен, так что выражение (7.35) не превышает единицы. После симметризации каждый кубит находится в состоянии

$$\rho_s = \left[1 - \mathrm{Tr}\left(\rho_0\tilde{\mathcal{P}}\right)\right]\rho_0 + \frac{1}{2}\tilde{\mathcal{P}} + \frac{1}{2}\left(\rho_0\tilde{\mathcal{P}} + \tilde{\mathcal{P}}\rho_0\right) \tag{7.36}$$

и обладает степенью чистоты

$$\mathrm{Tr}(\rho_s^2) = 1 + \mathrm{Tr}\left(\rho_0\tilde{\mathcal{P}}\right) . \tag{7.37}$$

Так как $\mathrm{Tr}\rho_s^2$ ближе к 1, чем (7.35), то получившееся симметризованное состояние системы ρ_s – более чистое.

Посмотрим теперь, как меняется точность воспроизведения при применении процедуры симметризации. Средняя точность воспроизведения до симметризации равна

$$F_{bs} = \frac{1}{2}\sum_i \langle\Psi|\rho_0 + \mathcal{P}_i|\Psi\rangle = 1 + \langle\Psi|\tilde{\mathcal{P}}|\Psi\rangle , \tag{7.38}$$

тогда как после успешной симметризации она равна

$$F_{as} = \langle\Psi|\rho_s|\Psi\rangle = 1 + \frac{1}{2}\langle\Psi|\tilde{\mathcal{P}}|\Psi\rangle . \tag{7.39}$$

Следовательно, состояние после симметризации ближе к начальному состоянию ρ_0.

Для общего случая R копий степень чистоты каждого кубита после симметризации равна [353]

$$\mathrm{Tr}(\rho_s^2) = 1 + 2\frac{1}{R}\mathrm{Tr}\left(\rho_0\tilde{\mathcal{P}}\right) , \tag{7.40}$$

где теперь

$$\tilde{\mathcal{P}} = \sum_{i=1}^{R}\mathcal{P}_i ,$$

и точность воспроизведения имеет вид

$$\langle\Psi|\rho_s|\Psi\rangle = 1 + \frac{1}{R}\langle\Psi|\rho_0\tilde{\mathcal{P}}|\Psi\rangle . \tag{7.41}$$

Можно сравнить формулы (7.40) и (7.41) с соответствующими выражениями до симметризации, т.е. (7.35) и (7.38). Видно, что, при R стремящемся к бесконечности, ρ_S приближается к невозмущенному состоянию ρ_0. Следовательно, если взять достаточно большое число

R и достаточно высокую частоту проицирования, то можно, в принципе, сделать так, чтобы конечная ошибка всего вычисления оставалась в допустимых произвольно малых пределах.

7.4.2 Классическое исправление ошибок

Еще один класс методов исправления ошибок происходит из распространения на квантовый случай классических кодов, исправляющих ошибки [354]. Разумеется, проблема того, как надежно передавать и преобразовывать информацию, несмотря на возможные ошибки, вызванные шумом, существует и в классической теории информации. Следовательно, прежде, чем мы начнем анализировать квантовые коды по исправлению ошибок, уместно провести краткий обзор того, как осуществляется исправление ошибок в классическом сценарии. Ниже мы будем называть кодом последовательность из c двоичных последовательностей $\mathbf{w}_1 \ldots \mathbf{w}_c$, называемых кодовыми словами, каждое длины n. Из-за шума, в процессе передачи и хранения значение некоторых битов перескакивает на противоположное. Такая смена значения бита – это единственно возможный тип классической ошибки. Если канал – двоично-симметричный и не обладает памятью (см. Рис. 7.3), то набор возможных последовательностей на выходе $\mathbf{v}_1 \ldots \mathbf{v}_{2^n}$ есть набор из всех 2^n возможных двоичных последовательностей длины n. Задача получателя информации состоит в том, чтобы по данной последовательности $\mathbf{v}_0$ определить наиболее вероятное кодовое слово $\mathbf{w}_i$, посланное отправителем, то есть, чтобы найти $\mathbf{w}_i$, самое близкое к $\mathbf{v}_0$. В этом контексте расстояние между двумя бинарными последовательностями $d(\mathbf{w}, \mathbf{v})$, называемое расстоянием Хемминга, измеряется как количество цифр, в которых эти две последовательности различны между собой. Для двоично-симметричного канала без памяти, строка $\mathbf{w}_i$ с наименьшим расстоянием Хемминга $d(\mathbf{w}_i, \mathbf{v}_0)$ является также и наиболее вероятной.

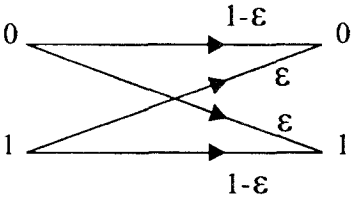


Рис. 7.3. В двоично-симметричном канале каждый бит передается с вероятностью ошибки ε.

Очевидно, что, чем больше расстояние между кодовыми словами, тем легче их различить при наличии шума, и, следовательно, тем

устойчивее код по отношению к шуму. Если $d(\mathbf{w}_i, \mathbf{w}_j) \geq 2\eta + 1$ для $i \neq j$, то тогда можно исправить вплоть до η ошибок.

Предел Хэмминга ограничивает сверху число c кодовых слов в коде, способном исправить не более, чем η ошибок. Каждое кодовое слово $\mathbf{w}_i$ можно себе представить как центр сферы радиуса η, содержащей все двоичные последовательности **v** с $d(\mathbf{w}_i, \mathbf{v}) \leq \eta$ – то есть, отличающиеся от $\mathbf{w}_i$ не более, чем на η позиций. На Рис.7.4 эта ситуация проиллюстрирована для $\eta = 4$. Чтобы код мог исправлять ошибки, сферы не должны пересекаться. Очевидно, что число двоичных последовательностей в каждой сфере, помноженное на число сфер, должно быть меньше, чем полное число последовательностей длины n. Так как каждая сфера содержит кодовое слово **w** плюс все последовательности, отличающиеся от него на 1, 2, ... η, то мы должны получить

$$c\left\{1 + n + \binom{n}{2} \ldots \binom{n}{\eta}\right\} = c\sum_{i=0}^{\eta}\binom{n}{i} \leq 2^n \ . \tag{7.42}$$

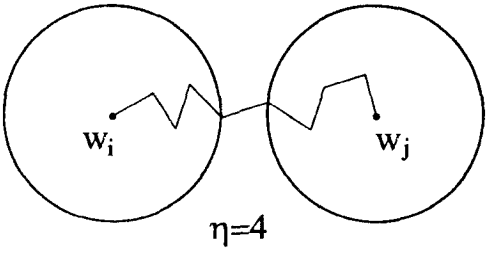


Рис. 7.4. В кодах с $d(\mathbf{w}_i, \mathbf{w}_j) \geq 2\eta + 1$ непересекающиеся сферы радиуса η с центрами на каждом кодовом слове содержат все последовательности с количеством ошибок, не превышающим η.

Одно семейство кодов, оказавшееся очень эффективным, в силу исторических причин известно как коды проверки четности [354]. В этих кодах кодовые слова **w** выбираются так, чтобы они удовлетворяли набору линейных уравнений. Получатель информации (приемник) проверяет, удовлетворяет ли полученная последовательность **v** этому набору уравнений. Если **v** не проходит тест, то приемник исправляет наименьшую ошибку, которая могла бы привести к появлению **v**. Рассмотрим более внимательно, как работает этот код. Набор линейных уравнений, которому должны удовлетворять кодовые слова **w**, характеризуется матрицей проверки четности **M** . Кодовые слова **w** удовлетворяют соотношению

$$\mathbf{M} \cdot \mathbf{w} = 0 \ . \tag{7.43}$$

Например, кодовые слова

$$\mathbf{w}_1 = 0000 \qquad \mathbf{w}_2 = 0101 \qquad \mathbf{w}_3 = 1110 \qquad \mathbf{w}_4 = 1011 \tag{7.44}$$

удовлетворяют уравнению (7.43) с

$$\mathbf{M} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}, \tag{7.45}$$

где все арифметические операции делаются по модулю 2. Если ранг **M** равен m, то $k = n - m$ битов в нашем кодовом слове можно определить произвольно, тогда как остальные m цифр – это проверочные цифры, определяемые соотношением (7.43). Следовательно, число линейно независимых компонентов равно $c = 2^{n-m} = 2^k$, и можно записать границу Хемминга (7.42) в виде

$$2^k \sum_{i=0}^{\eta} \binom{n}{i} \le 2^n \rightarrow 2^{n-k} = 2^m \ge \sum_{i=0}^{\eta} \binom{n}{i}, \tag{7.46}$$

что представляет собой нижний предел для количества проверочных цифр. Предположим, что передавалась последовательность **w**, и что получена последовательность **v**. Двоичная последовательность $\mathbf{z} = \mathbf{w} - \mathbf{v}$, называемая шаблоном ошибок, содержит единицы на тех позициях, где произошла ошибка, и нули на всех остальных позициях. Если $\mathbf{z} \neq 0$, то **v** не проходит проверку четности: $\mathbf{M} \cdot \mathbf{v} = \mathbf{M} \cdot (\mathbf{w} + \mathbf{z}) = \mathbf{M} \cdot \mathbf{z} = \mathbf{s}$. Вектор **s**, называемый синдромом ошибок, есть сумма столбцов в матрице проверки четности в тех местах, где у **z** есть единицы. Например, если при передаче **w** = 1110 получилось **v**=1000, то **z**=0110, и, при **M**, заданной (7.45), **s** = 10.

После того, как стал известен синдром ошибки **s**, задача приемника состоит в том, чтобы определить, какие шаблоны ошибки **z** могли произвести **s**, и затем исправить наименьшую ошибку, то есть, ту, в шаблоне которой меньше всего единиц. Надо заметить, что в случае единичной ошибки синдром есть просто столбец, в котором эта ошибка произошла. Если все столбцы **M** различны, то приемник может легко определить местонахождение ошибки и исправить ее.

7.4.3 Общие аспекты квантовых кодов, исправляющих ошибки

Как только мы попытаемся обобщить проиллюстрированные выше методы на квантовый сценарий, мы немедленно столкнемся с двумя проблемами:

1. Из-за внешнего шума, каждый кубит может не только поменять значение на обратное, но и потерять когерентность. В общем случае, он перепутается со своим окружением, как было показано в разделе 7.2.

2. Мы не можем считать состояние кубита до того, как вычисление закончено. Неисполнение этого правила ведет к декогерентности. Следовательно, мы должны узнать природу и местонахождение ошибки, не узнавая состояние кубитов.

Мы покажем, что можно решить проблему 2, используя в качестве «кодовых векторов» $|\mathbf{w}\rangle$ перепутанные состояния n кубитов. В этом случае информация, которую мы хотим защитить, размыта, благодаря перепутыванию, по всем n кубитам. Считывание (или разрушение когерентности) всего нескольких кубитов не приведет к необратимой потере квантовой информации. Кодовые вектора выбираются таким образом, что ошибка переводит $|\mathbf{w}\rangle$ во взаимно ортогональное подпространство. Тогда измерение синдрома проявит только то, в какое подпространство переместился вектор $|\mathbf{w}\rangle$. Ниже мы предположим, что в эволюции каждого кубита с вероятностью ε происходит ошибка, и что ошибки в разных кубитах независимы друг от друга. В рамках этих предположений вероятность ошибки в двух кубитах порядка $O(\varepsilon^2)$. Разумно предположить, что, при достаточно малых значениях ε, происходит только одна ошибка. Вероятность успешного вычисления равна $(1-\varepsilon)$. Если можно осуществить квантовую процедуру исправления единичных ошибок, то вероятность успешного вычисления возрастет до $(1-O(\varepsilon^2))$. В общем случае код, способный исправлять вплоть до t ошибок, увеличивает вероятность успешного вычисления до $(1-O(\varepsilon^{t+1}))$.

7.4.4 Код с тремя кубитами

В качестве первого ознакомления с квантовыми кодами, исправляющими ошибки и в качестве иллюстрации идей, которые были представлены выше, мы проанализируем трех-кубитный код, который может исправлять фазовые ошибки в одном кубите [355]. Предположим, что каждый кубит в кодовом слове может независимо от остальных быть подвержен перепутыванию с окружением вида (7.1). Мы покажем, что можно избавиться от эффекта фазового перепутывания, если мы сможем исправлять фазовые ошибки, определяемые как

$$|0\rangle \to |0\rangle \qquad |1\rangle \to -|1\rangle \tag{7.47}$$

возникающие из-за оператора ошибки σ_z. С этой целью, выберем в качестве кодовых слов следующие перепутанные состояния трех кубитов:

$$|\mathbf{w}_0\rangle = |000\rangle + |011\rangle + |101\rangle + |110\rangle \ ,$$

$$|\mathbf{w}_1\rangle = |111\rangle + |100\rangle + |010\rangle + |001\rangle \ . \tag{7.48}$$

Если только один кубит перепутается с окружением, то произвольная линейная суперпозиция $|\mathbf{w}_0\rangle$, $|\mathbf{w}_1\rangle$ превратится в

$$\begin{aligned}(a_0|\mathbf{w}_0\rangle + a_1|\mathbf{w}_1\rangle)|E\rangle \rightarrow\ & (a_0|\mathbf{w}_0\rangle_0 + a_1|\mathbf{w}_1\rangle_0)|E_0\rangle \\ &+ (a_0|\mathbf{w}_0\rangle_1 + a_1|\mathbf{w}_1\rangle_1)|E_1\rangle \\ &+ (a_0|\mathbf{w}_0\rangle_2 + a_1|\mathbf{w}_1\rangle_2)|E_2\rangle \\ &+ (a_0|\mathbf{w}_0\rangle_3 + a_1|\mathbf{w}_1\rangle_3)|E_3\rangle \quad , \end{aligned} \tag{7.49}$$

где ошибочное состояние $|\mathbf{w}_j\rangle_k$ есть кодовое слово j ($j = 0,1$) с фазовой ошибкой в k-том кубите ($k = 0$ означает, что ошибок нет). Например, $|\mathbf{w}_0\rangle_2 = |000\rangle - |011\rangle + |101\rangle - |110\rangle$. $|E_k\rangle$ обозначают соответствующие состояния окружения. Заметим, что ошибочные состояния ортогональны:

$$_k\langle \mathbf{w}_j | \mathbf{w}_l \rangle_i = \delta_{jl}\delta_{ki} \quad . \tag{7.50}$$

Коды, в которых ошибочные состояния ортогональны, называются невырожденными. Таким образом, процедура исправления ошибки состоит в следующем:

• Спроектируем пространство кодов на подпространства ошибок, покрытые $|\mathbf{w}_0\rangle_i, |\mathbf{w}_1\rangle_i$.

• В зависимости от результата измерения, исправим соответствующий кубит с фазовой ошибкой, применив σ_z. То есть, если результатом вышеописанной проекции является i, то применим σ_z к кубиту с номером i (если $i = 0$, то состояние не меняется).

Заметим, что в конце этой процедуры кодовое слово и окружение не перепутаны, и что амплитуды a_0, a_1 не изменены.

7.4.5 Квантовая граница Хэмминга

Теперь мы обратимся к кодам, которые могут исправлять перепутывание самого общего вида:

$$|0\rangle|E\rangle \rightarrow |0\rangle|E_{00}\rangle + |1\rangle|E_{01}\rangle \quad |1\rangle|E\rangle \rightarrow |0\rangle|E_{10}\rangle + |1\rangle|E_{11}\rangle \ . \tag{7.51}$$

Для линейной суперпозиции состояний кубита удобно записать действие перепутывания в виде

$$\begin{aligned}(a_0|0\rangle + a_1|1\rangle)|E\rangle \rightarrow\ & (a_0|0\rangle + a_1|1\rangle)|E_0\rangle \\ &+ \left[\sigma_x(a_0|1\rangle + a_1|0\rangle)\right]|E_x\rangle \\ &+ \left[\sigma_z(a_0|0\rangle - a_1|1\rangle)\right]|E_z\rangle \\ &+ \left[\sigma_y(a_0|1\rangle - a_1|0\rangle)\right]|E_y\rangle \quad , \end{aligned} \tag{7.52}$$

где σ_x – оператор ошибки для переворота битов (т.е. смены значения бита на обратное), σ_z – оператор ошибки для переворота фазы, и $\sigma_y = -i\sigma_z\sigma_x$ – оператор обеих ошибок. Как видно из выражения (7.52), общее взаимодействие кубита с окружением можно выразить через действие на кубит операторов Паули σ_x, σ_y и σ_z. Это значит, что состояние кубита превращается в суперпозицию компоненты, свободной от ошибки, и трех ошибочных компонент, с ошибками типа σ_x, σ_y и σ_z.

Теперь нам будет легко перевести на квантовый язык аргументы, которые привели нас к границе Хэмминга для «невырожденных кодов» [355] (менее строгие условия выполняются для общих квантовых кодов, см., например, [323]). Если код с 2^q кодовыми векторами может исправить вплоть до η ошибок, то кодовые вектора $|\mathbf{w}\rangle$ и все состояния, получаемые из $|\mathbf{w}\rangle$ действием не более чем η операторов ошибки, должны образовывать набор ортогональных состояний. Взаимодействие с окружением преобразует каждое кодовое слово в

$$|\mathbf{w}\rangle|E\rangle \rightarrow |\mathbf{w}\rangle|E_0\rangle + \sum_{i,k_i} |\mathbf{w}_i^{k_i}\rangle|E_i^{k_i}\rangle + \sum_{ij,k_i k_j} |\mathbf{w}_{ij}^{k_i k_j}\rangle|E_{ij}^{k_i k_j}\rangle + \sum_{ijl,k_i k_j k_l} |\mathbf{w}_{ijl}^{k_i k_j k_l}\rangle|E_{ijl}^{k_i k_j k_l}\rangle \ \ldots \ , \tag{7.53}$$

где индексы $i, j, \ldots$ маркируют кубиты в кодовых векторах, а

$$k_i, k_j, \ldots = x, y, z$$

отмечают ошибку в соответствующем кодовом слове. Если код исправляет вплоть до η ошибок, то все состояния, содержащие не более, чем η ошибок по отношению к начальным 2^q кодовым словам, должны быть ортогональны. Число ортогональных состояний не должно превышать размерность гильбертова пространства n кубитов, так что мы получаем

$$2^q \sum_{i=0}^{\eta} 3^i \binom{n}{i} \le 2^n \ \rightarrow \ 2^{n-q} \ge \sum_{i=0}^{\eta} 3^i \binom{n}{i} \ , \tag{7.54}$$

что устанавливает нижнюю границу для числа проверочных кубитов $n - q$ в квантовом исправляющем коде, способном исправить вплоть до η ошибок. Множитель 3^i появляется в выражении (7.54) из-за того, что в квантовом случае в каждом кубите может возникнуть три независимых ошибки – в отличие от классического случая, в котором единственно возможной ошибкой является переворот бита.

7.4.6 Код с семью кубитами

Теперь мы готовы рассмотреть квантовый код, который может исправить любую ошибку в одном кубите. Хотя известны коды, исполь-

зующие пять кубитов [323, 356], необходимых согласно границе Хэмминга, из педагогических соображений лучше описать код из семи кубитов, предложенный Стином [357, 358]. Сначала введем матрицу проверки четности:

$$\mathbf{M} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} . \qquad (7.55)$$

Так как все столбцы у **M** различны, то, если перевернется только один бит, то измерение синдрома выявит положение ошибочного кубита. Чтобы построить кодовые векторы, мы будем использовать в качестве исходных ингридиентов (классические) последовательности **u**, удовлетворяющие проверке четности $\mathbf{Mu} = 0$, и соответствующие состояния кубитов $|\mathbf{u}\rangle$, у которых логические значения кубитов соответствуют последовательностям **u**. Тогда кодовые вектора $|\mathbf{w}_0\rangle$, $|\mathbf{w}_1\rangle$ определяются как перепутанные суперпозиции состояний $|\mathbf{u}\rangle$ с четным и нечетным количеством единиц, соответственно:

$$|\mathbf{w}_0\rangle = \sum_{\text{четн.}} |\mathbf{u}\rangle_e \qquad |\mathbf{w}_1\rangle = \sum_{\text{нечетн.}} |\mathbf{u}\rangle_o \; . \qquad (7.56)$$

Последним ингредиентом является процедура измерения синдрома. С этой целью добавим дополнительные кубиты, по одному для каждого бита синдрома, т.е. по одному для каждой строки в **M** (см. Рис. 7.5). Если $\mathbf{M}_{ij} = 1$, то вводится логический элемент CNOT, у которого целевым является дополнительный кубит i, а контрольным – кубит j кодового вектора.

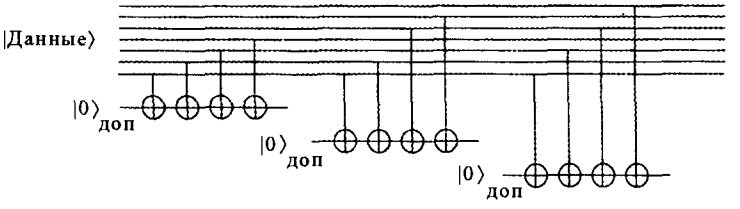


Рис. 7.5. Измерение синдрома переворота бита в коде с семью кубитами.

Если сначала кодовый вектор есть $|\mathbf{v}\rangle$, а вектор дополнительных кубитов есть $|\mathbf{0}\rangle$, то конечный вектор дополнительных кубитов (дополнение) будет равен $|\mathbf{s}\rangle = |\mathbf{Mv}\rangle$, в соответствии со значением синдрома:

$$|\mathbf{v}\rangle \otimes |0\rangle_{доп} \rightarrow |\mathbf{v}\rangle \otimes |\mathbf{Mv}\rangle_{доп} \; . \qquad (7.57)$$

Если произошла только одна ошибка, то измерение дополнения спроектирует кодовый вектор либо на правильное состояние, либо на

состояние с одним перевернутым битом. Кроме того, логическое значение дополнения выявит положение ошибочного бита, который затем можно будет исправить, применив оператор σ_x.

Описанный здесь метод можно легко развить таким образом, чтобы исправлять также и ошибки переворота фазы. Для этого надо только заметить, что переворот фазы в базисе $|0\rangle$, $|1\rangle$ превращается в переворот бита в базисе, повернутом преобразованием Адамара. Следовательно, задача сводится к исправлению переворотов бита в повернутом базисе. Если мы применим побитное вращение Адамара, то каждый кубит преобразуется в

$$|0\rangle \to |\tilde{0}\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \ , \quad |1\rangle \to |\tilde{1}\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \ , \tag{7.58}$$

и кодовые вектора преобразуются в

$$|\mathbf{w}_0\rangle \to |\tilde{\mathbf{w}}_0\rangle \equiv \frac{1}{\sqrt{2}}(|\mathbf{w}_0\rangle + |\mathbf{w}_1\rangle) \ ,$$

$$|\mathbf{w}_1\rangle \to |\tilde{\mathbf{w}}_1\rangle \equiv \frac{1}{\sqrt{2}}(|\mathbf{w}_0\rangle + |\mathbf{w}_1\rangle) \tag{7.59}$$

Заметим, что $|\tilde{\mathbf{w}}_0\rangle$, $|\tilde{\mathbf{w}}_1\rangle$ удовлетворяют проверке четности. Следовательно, процедура исправления фазовых ошибок состоит в следующем. Применяем побитное вращение Адамара к кодовым векторам, исправляем перевороты бита в повернутом базисе и делаем поворот обратно исходному базису $|0\rangle$, $|1\rangle$ (см. Рис. 7.6). Фазовая ошибка будет автоматически исправлена. Это значит, что код с семью кубитами может исправить любую фазовую и/или амплитудную ошибку в одном кубите.

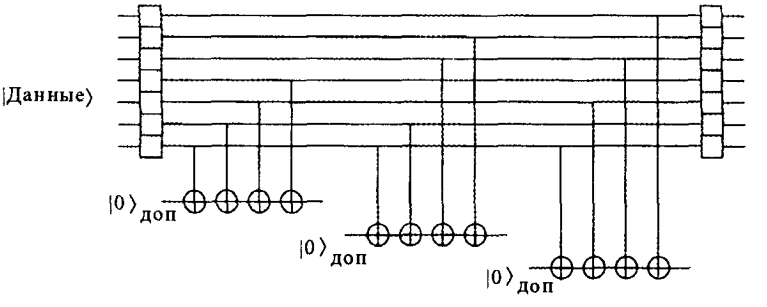


Рис. 7.6. Измерение синдрома переворота фазы в коде с семью кубитами.

7.4.7 Устойчивое к сбоям вычисление

До сих пор предполагалось, что шаги вычисления не вносят новые ошибки. На самом деле операции в логических ячейках сами по себе

подвержены ошибкам. Более того, кодирование, раскодирование и исправление ошибок – это тоже вычислительные операции. Поэтому возникает проблема – как осуществить надежное вычисление, используя ненадежные цепи. В оставшейся части этого раздела мы проиллюстрируем основные идеи, которые стоят за устойчивым к сбоям вычислением [359]. В качестве примера того, как ошибка при выполнении логической операции может испортить квантовые данные до такой степени, что их нельзя будет восстановить с помощью наших исправляющих кодов, рассмотрим измерение синдрома с помощью дополнительного кубита. Дополнительный кубит является целевым для нескольких операций CNOT. Так как в квантовых элементах CNOT фазовые ошибки в целевом кубите действуют обратно на контрольный кубит, любая фазовая ошибка в дополнительном кубите может распространиться на более, чем один кубит с данными. Заметим, однако, что наш код способен исправить только одну ошибку. Следовательно, если дополнительный кубит заражает два кубита с данными, то тогда искажение данных исправить невозможно.

Чтобы ограничить распространение ошибки, можно использовать в качестве целевых кубитов разные вспомогательные кубиты для различных кубитов с данными. Тогда значение синдрома будет найдено из коллективного измерения всех вспомогательных кубитов. При этом надо позаботиться, чтобы процедура измерения дала нам информацию только об ошибках, но не о состоянии кубитов с данными. Решение этой проблемы было найдено Шором (рис.7.7). В его схеме дополнительные кубиты приготавливаются в линейной суперпозиции состояний с четным числом единиц:

$$|Shor\rangle = \sum_{\text{четн.}} |\mathbf{x}\rangle \tag{7.60}$$

Например, дополнительные кубиты – по четыре на каждый бит синдрома – приготавливаются в состоянии

$$|Shor\rangle = \frac{1}{\sqrt{8}}\big(\,|0000\rangle + |0011\rangle + |0101\rangle + |1001\rangle + |0110\rangle + |1010\rangle + |1100\rangle + |1111\rangle\,\big)\,. \tag{7.61}$$

Каждый дополнительный кубит будет целевым для своего кубита с данными. В конце значение кубита синдрома будет получено измерением четности битов в дополнительном состоянии. Эта процедура гарантирует, что измерение дополнения дает нам информацию только об ошибках. Более того, она гарантирует, что ошибки в дополнительных кубитах не распространяются по данным.

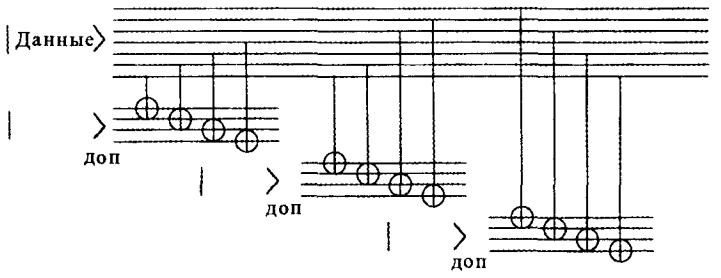


Рис. 7.7. Устойчивое к сбоям измерение синдрома в коде с семью кубитами.

Однако мы хотим не только хранить данные, но еще и производить над ними операции. Наиболее простой задачей было бы раскодировать данные, выполнить желаемое вычисление, и затем снова закодировать. Однако во время декодирования данные подвержены внешнему шуму. Следовательно, чтобы защитить наши кубиты, нам хорошо было бы произвести вычисление прямо на кодовых векторах. Более того, нам бы хотелось провести вычисление устойчивым к сбоям способом, чтобы избежать распространения ошибок. Это требование автоматически удовлетворяется во всех случаях, когда мы можем сконструировать логические операции на кодовых векторах в виде побитных операций на одиночных закодированных кубитах. Мы показали в (7.58), что это возможно для преобразования Адамара. Операцию CNOT на кодовых векторах также возможно осуществить попарно на кодовых векторах контрольного и целевого кубитов. Вместе две эти операции еще не составляют универсального набора. Но их можно дополнить устойчивой к сбоям версией элемента Тоффоли, и это позволит образовать такой универсальный набор.

7.5 Общая теория квантового исправления ошибок и устойчивости к сбоям

А. Стин

Вводный материал и примеры методов квантового исправления ошибок (КИО) были даны в предыдущем разделе. В этом разделе мы представим краткое изложение самых простых аспектов более общей теории.

КИО основано на трех центральных идеях: оцифровка шума, управление операторами ошибок и синдромами, и конструирование квантового кода, исправляющего ошибки (ККИО). Успех КИО основан на физике шума; мы вернемся к этой теме после обсуждения трех центральных идей.

7.5.1 Оцифровка шума

«Оцифровка шума» основана на наблюдении, что любое взаимодействие между набором кубитов и какой-либо другой системой (например, окружением) можно выразить через обобщение выражения (7.52):

$$|\phi\rangle|\psi\rangle_e \rightarrow \sum_i (E_i|\phi\rangle)|\psi_i\rangle_e \ , \tag{7.62}$$

где каждый «оператор ошибки» E_i есть тензорное произведение операторов Паули, действующих на кубиты, $|\phi\rangle$ обозначает начальное состояние кубитов, и $|\psi\rangle_e$ обозначает состояния окружения, не обязательно ортогональные или нормализованные. Таким образом, мы выражаем общий шум и/или декогерентность в терминах операторов Паули σ_x, σ_y, σ_z, действующих на кубиты. Их можно записать через $X \equiv \sigma_x$, $Z \equiv \sigma_z$, $Y \equiv -i\sigma_y = XZ$.

Чтобы записать тензорное проязведение матриц Паули, действующих на n кубитов, мы вводим обозначение $X_u Z_v$, где u и v – n-битные двоичные векторы. Ненулевые координаты в u и v показывают, где в произведении операторов появляются операторы X и Z. Например,

$$X \otimes I \otimes Z \otimes Y \otimes X \equiv X_{10011} Z_{00110} \ . \tag{7.63}$$

Исправление ошибок – это процесс, который переводит состояние вида $E_i|\phi\rangle$ в $|\phi\rangle$. Исправление ошибок X-типа переводит $X_u Z_v|\phi\rangle$ в $Z_v|\phi\rangle$; исправление ошибок Z-типа переводит $X_u Z_v|\phi\rangle$ в $X_v|\phi\rangle$. В целом, мы обнаружили чрезвычайно важный факт: для того, чтобы исправить шум *самого общего возможного вида* (7.62), достаточно исправить лишь ошибки X- и Z-типа.

7.5.2 Операторы ошибки, стабилизатор и извлечение синдрома

Теперь мы рассмотрим математику операторов ошибки, с помощью подхода, выдвинутого Готтсманом [360] и Сэлдербанком (с соавторами) [361, 362] на основе первых исследований Стина [357, 358], а также Сэлдербанка и Шора [363, 364].

Рассмотрим набор $\{I, X, Y, Z\}$, состоящий из тождественного оператора и трех операторов Паули. Все операторы Паули при возведении в квадрат дают I: $X^2 = Y^2 = Z^2 = I$, и их собственные значения равны ± 1. Два компонента этого набора всегда либо коммутируют ($XI = IX$), либо антикоммутируют: $XZ = -ZX$. Тензорные произведения операторов Паули также в квадрате дают единицу и либо коммутируют, либо антикоммутируют. Отметим: у нас термин «оператор ошибки» есть просто краткая форма сказать «произведение операторов Паули»; такой оператор будет иногда играть роль ошибки, а иногда – роль проверки четности, как в классической теории кодирования в разделе 7.4.2.

Если в квантовой системе n битов, то операторы ошибки будут иметь *длину n*. *Весом* оператора ошибки называется число членов, не равных I. Например, $X_{10011}Z_{00110}$ – это оператор длины 5 и веса 4.

Пусть $\mathcal{H} = \{M\}$ – это набор коммутирующих операторов. Поскольку операторы коммутируют, то у них могут быть общие собственные состояния. Пусть $C = \{|u\rangle\}$ обозначает ортонормальный набор одновременных собственных состояний, у каждого из которых собственное значение равно +1:

$$M|u\rangle = |u\rangle \quad \forall |u\rangle \in C, \ \forall M \in \mathcal{H} \ . \tag{7.64}$$

Набор C – это квантовый исправляющий код, а $\mathcal{H}$ – его *стабилизатор*. Ортонормированные состояния $|u\rangle$ называются *кодовыми векторами* или *квантовыми кодовыми словами*. В дальнейшем мы ограничим наше внимание случаем, когда $\mathcal{H}$ образует группу. Ее размер равен 2^{n-k}, и она покрыта n-k линейно независимыми членами $\mathcal{H}$. В этом случае C содержит 2^k членов, так что он кодирует k кубитов, поскольку его члены покрывают 2^k-мерное подпространство 2^n-мерного гильбертова пространства всей системы. Произвольное состояние из этого подпространства, называемое *закодированным состоянием* или *логическим состоянием*, можно выразить через суперпозицию кодовых векторов:

$$|\phi\rangle_L = \sum_{|u\rangle \in C} a_u |u\rangle \ . \tag{7.65}$$

Конечно, один заданный ККИО не может исправить все возможные ошибки. Каждый код позволяет исправить свой специфический набор $\mathcal{S} = \{E\}$ исправляемых ошибок. Задача конструирования кода состоит в том, чтобы найти коды, чьи исправляемые наборы включают в себя ошибки, наиболее вероятные в данной физической ситуации. Мы обратимся к этой важной задаче в следующем разделе. Сейчас мы начнем с того, что покажем, какое отношение исправляемый набор имеет к стабилизатору группы, и как именно происходит исправление ошибок.

Во-первых, все операторы ошибок в стабилизаторе исправляемы, $E \in \mathcal{S} \ \forall \ E \in \mathcal{H}$, так как они на самом деле не влияют на логическое состояние общего вида (7.65). Если в рассматриваемой системе эти операторы являются единственными членами, формирующими шум, то ККИО есть свободное от шума подпространство, называемое также свободным от декогерентности подпространством системы.

Существует также большой набор ошибок, которые изменяют закодированные состояние, но которые, тем не менее, можно исправить процессом извлечения синдрома ошибки, и затем действием на систему способом, зависящим от полученного синдрома. Мы покажем, что

$\mathcal{S}$ может быть любым набором ошибок $\{E_i\}$, таким, что любое произведение E_1E_2 либо принадлежит $\mathcal{H}$, либо антикоммутирует с любым элементом из $\mathcal{H}$. Чтобы это увидеть, рассмотрим сначала второй случай:

$$E_1E_2M = -ME_1E_2 \text{ для некоторого } M\in\mathcal{H} \tag{7.66}$$

Мы говорим, что совместный оператор ошибки E_1E_2 *наблюдаем*. Это может случиться, только если

$$\text{либо } \{ME_1 = -E_1M,\ ME_2 = E_2M\}$$

$$\text{либо } \{ME_1 = E_1M,\ ME_2 = -E_2M\}. \tag{7.67}$$

Чтобы извлечь синдром, мы измеряем все наблюдаемые в стабилизаторе. Для этого достаточно измерить любой набор из n-k линейно независимых M из $\mathcal{H}$. Заметим, что такое измерение не действует на состояние в закодированном подпространстве, поскольку это состояние является собственным состоянием для всех этих наблюдаемых. Измерение проицирует состояние с шумом на собственное состояния каждого M, с собственным значением ±1. Строка из n-k собственных значений образует синдром. Уравнения (7.67) гарантируют, что E_1 и E_2 порождают различные синдромы, так что их можно отличить друг от друга. Действительно, если взять испорченное состояние $E|\phi\rangle_L$ и измерить переменную M, то, согласно (7.67), ошибки $E = E_1$ и $E = E_2$ приведут к отличным друг от друга собственным значениям. Следовательно, ошибку можно сначала найти с помощью синдрома, а затем исправить, вызвав в системе найденную ошибку еще раз (воспользовавшись тем фактом, что квадрат всех операторов ошибки равен единице).

Посмотрим, как этот процесс выглядит в применении к состоянию с шумом общего вида. Состояние с шумом представляется как

$$\sum_i \left(E_i|\phi\rangle_L\right)|\psi_i\rangle_e \ . \tag{7.68}$$

Можно произвести извлечение синдрома, просто присоединив к системе $n-k$ кубитов дополнения a, и сохранив в них собственные значения системы с помощью последовательности операций CNOT и вращений Адамара. Конкретную вычислительную сеть можно построить, либо рассуждая в терминах проверки четности для информации, хранимой в дополнении (как на Рис. 7.5), либо с помощью следующего метода измерения собственного значения. Чтобы извлечь собственное значение $\lambda = \pm1$ оператора M, приготовим дополнение в состоянии $(|0\rangle + |1\rangle)/\sqrt{2}$. Произведем контролируемое-M с дополнением в качестве контроля и системой в качестве мишени, затем повернем дополнение преобразованием Адамара. Конечным состоянием дополнения будет $[(1+\lambda)|0\rangle + (1-\lambda)|1\rangle]/2$.

Выполнив этот процесс для $n - k$ операторов M, покрывающих $\mathcal{H}$, мы свяжем систему и окружение с дополнением следующим образом:

$$|0\rangle_a \sum_i \left(E_i|\phi\rangle_L\right)|\psi_i\rangle_e \rightarrow \sum_i |s_i\rangle_a \left(E_i|\phi\rangle_L\right)|\psi_i\rangle_e \quad . \tag{7.69}$$

Здесь s_i – это $(n - k)$-битные строки. Они все различны между собой, если синдромы у всех E_i различны. Проекционное измерение дополнения произведет коллапс всей этой суммы в один случайно взятый член $|s_i\rangle_a(E_i|\phi\rangle_L)|\psi_i\rangle_e$, и, в качестве результата измерения, даст s_i. Поскольку существует только одна ошибка E_i с таким синдромом, то мы можем узнать оператор E_i, который затем следует применить, чтобы избавиться от ошибки!

Можно себе представить этот замечательный процесс следующим образом. Сначала мы, через проекционное измерение, заставляем общее состояние с шумом «выбрать» между дискретным набором ошибок, а затем обращаем конкретную «выбранную» дискретную ошибку, используя тот факт, что результат измерения говорит нам, какой именно была эта ошибка. Альтернативный способ исправления состоит в осуществлении унитарной эволюции, состоящей из контролируемых операций с дополнением в качестве контроля и системы в качестве мишени, эффективно переводящей шум (включая перепутывание с окружением) из системы в дополнение.

Нам осталось рассмотреть вторую возможность, отмеченную выше перед уравнением (7.66), а именно

$$E_1 E_2 \in \mathcal{H}. \tag{7.70}$$

В этом случае у E_1 и E_2 будет один и тот же синдром, так что их нельзя различить с помощью процесса выделения синдрома. Но это и не важно! Мы просто интерпретируем общий синдром этих двух ошибок в том смысле, что надо применить процедуру, исправляющую E_1. Если в системе была именно ошибка E_1, то, очевидно, все в порядке. Если же это была ошибка E_2, то конечным состоянием будет $E_1E_2|\phi\rangle_L$, которое тоже не содержит ошибки! У этой ситуации нет аналогов в классической теории кодирования. Квантовые коды, которые ее используют, называются вырожденными, и не ограничены квантовой границей Хэмминга (7.54).

Обсуждение, основанное на стабилизаторе, полезно, поскольку оно фокусирует внимание на операторах, а не на состояниях. Тем не менее, квантовые кодовые слова - это очень интересные состояния, обладающие высокой симметрией и интересными формами перепутывания. Можно легко показать, что кодовые слова в ККИО допускает исправление набора S, если и только если [323, 365]

$$\langle u|E_1E_2|v\rangle = 0 \tag{7.71}$$

$$\langle u|E_1E_2|u\rangle = \langle v|E_1E_2|v\rangle \tag{7.72}$$

для всех $E_1, E_2 \in \mathcal{S}$ и $|u\rangle, |v\rangle \in C$, $|u\rangle \neq |v\rangle$. В случае, когда E_1E_2 всегда антикоммутирует с членом стабилизатора, мы получаем

$$\langle u|E_1E_2M|u\rangle = -\langle u|ME_1E_2|u\rangle = -\langle u|E_1E_2|u\rangle,$$

и, следовательно, $\langle u|E_1E_2|u\rangle = 0$. Это невырожденный код; все кодовые векторы и их ошибочные компоненты взаимно ортогональны, и квантовая граница Хемминга должна выполняться.

7.5.3 *Конструирование кода*

Мощь КИО происходит из сочетания понимания физики и уже обсуждавшихся математических методов с тем фактом, что ККИО реально можно найти. Конструирование кода – это сама по себе интересная и тонкая область, которую мы лишь кратко представим здесь.

Во-первых, вспомним наше требование, что все члены стабилизатора должны коммутировать между собой. Легко показать, что

$$X_uZ_v = (-1)^{u\cdot v}Z_vX_u,$$

где $u\cdot v$ – это бинарная операция проверки четности, или внутреннее произведение бинарных векторов, найденное в $GF(2)$. Отсюда,

$$M = X_uZ_v \text{ и } M' = X_{u'}Z_{v'},$$

коммутируют, если и только если

$$u\cdot v' + v\cdot u' = 0\,. \tag{7.73}$$

Стабилизатор полностью определен записью $n - k$ линейно независимых операторов ошибки, которые его покрывают. Удобно записать эти операторы ошибки с помощью двоичных строк u и v, которые относятся к частям X и Z, в форме двух двоичных матриц размера $(n - k) \times n$: H_x и H_Z. Тогда весь стабилизатор полностью определяется двоичной матрицей размера $(n - k) \times 2n$

$$H = \left(H_x \,|\, H_z\right), \tag{7.74}$$

и то требование, что все операторы между собой коммутируют (то есть, что $\mathcal{H}$ – абелева группа) выражается в виде

$$H_xH_z^T + H_zH_x^T = 0\,, \tag{7.75}$$

где знак ^{T} обозначает транспонирование матрицы.

Матрица H – это аналог матрицы проверки четности в классическом коде исправления ошибок. Аналогом производящей матрицы является матрица $G = (G_x \mid G_z)$, удовлетворяющая условию

$$H_x G_z^T + H_z G_x^T = 0 \ . \tag{7.76}$$

Другими словами, матрицы H и G являются дуальными по отношению к внутреннему произведению, определенному выражением (7.73). У матрицы G $n + k$ рядов. H можно получить непосредственно из G, если поменять местами части, относящиеся к X и Z, и затем взять обычную двоично-сопряженную матрицу к получившейся двоичной матрице размера $(n + k) \times 2n$.

Заметим, что выражения (7.76) и (7.75) означают, что G содержит в себе H. Пусть $\mathcal{G}$ обозначает множество операторов ошибки, порождаемое G. Тогда $\mathcal{G}$ содержит $\mathcal{H}$.

Поскольку, в силу определения (7.76), все члены $\mathcal{G}$ коммутируют со всеми членами $\mathcal{H}$, и поскольку (пересчетом) больше ни один оператор ошибки не может коммутировать со всеми членами $\mathcal{H}$, можно заключить, что все операторы ошибки, не содержащиеся в $\mathcal{G}$, антикоммутируют по крайней мере с одним членом H. Это приводит нас к важному наблюдению: если все члены $\mathcal{G}$ (кроме единичного оператора) обладают весом, не меньшим d, то все операторы ошибки (кроме единичного) веса не меньше, чем d, антикоммутируют с членом $\mathcal{H}$, и, следовательно, наблюдаемы. Следовательно, такой код может исправить все операторы ошибки с весом меньшим, чем $d/2$.

Что, если только члены $\mathcal{G}$ с весом меньшим, чем d, являются также и членами $\mathcal{H}$? В этом случае код все равно может исправить все ошибки с весом меньшим, чем $d/2$, с помощью свойства (7.70) (вырожденный код). Вес d называется минимальным расстоянием кода.

Таким образом, проблема построения кода сведена к задаче нахождения таких двоичных матриц H, которые удовлетворяют условию (7.75), и дуальные к которым матрицы G, определяемые выражением (7.76), обладают большим весом. Теперь мы запишем такой код, скомбинировав хорошо отобранные классические коды для исправления ошибок:

$$H = \left(\begin{array}{c|c} H_2 & 0 \\ 0 & H_1 \end{array}\right), \qquad G = \left(\begin{array}{c|c} G_1 & 0 \\ 0 & G_2 \end{array}\right). \tag{7.77}$$

Здесь H_i, $i = 1,2$, – это проверочная матрица классического кода C_i, произведенного G_i. Следовательно, $H_i G_i^T = 0$, и условие (7.76) выполнено. Чтобы удовлетворить условию коммутативности (7.75), мы берем $H_1 H_2^T = 0$, или, другими словами, $C_2^{\perp} \subset C_1$. По построению, если размеры классических кодов равны k_1 и k_2, то размер квантового кода равен $k = k_1 + k_2 - n$. Квантовые кодовые слова равны

$$|u\rangle_L = \sum_{x \in C_2^{\perp}} |x + u \cdot D\rangle \ , \tag{7.78}$$

где u – это двоичное слово из k битов, x – двоичное слово из n битов, и D – это матрица размера $(k \times n)$ из образующих элементов смежного класса. Таковы коды ССС (Сэлдербэнка-Шора-Стина). Их значение в том, что они, во-первых, могут быть эффективными, и, во-вторых, в том, что они используются в устойчивом к сбоям вычислении (см. ниже).

Говоря «эффективные», мы имеем в виду, что для данного d/n существуют такие коды, у которых отношение k/n остается выше некоторого конечного нижнего предела при $k, n, d \to \infty$. У кодов ССС $d = \min(d_1, d_2)$. Если при построении мы взяли два одинаковых классических кода $C_1 = C_2 = C$, то мы рассматриваем классический код, который содержит дуальный себе. Можно показать, что для отношения k/n в таких кодах существует конечный нижний предел [364]. Этот факт очень важен: он означает, что КИО может быть очень мощным средством для подавления шума (см. следующий раздел).

Существуют ККИО более эффективные, чем коды ССС. Хорошие коды могут быть найдены путем развития методов ССС, а также с помощью других методов. Для иллюстрации, в завершение этого раздела мы приводим стабилизатор и производящую матрицу совершенного кода с $[[n, k, d]] = [[5, 1, 3]]$. Он кодирует один кубит ($k = 1$) и исправляет все ошибки веса 1 (поскольку $d/2 = 1.5$).

$$H = \left(\begin{array}{c|c} 11000 & 00101 \\ 01100 & 10010 \\ 00110 & 01001 \\ 00011 & 10100 \end{array}\right), \qquad G = \left(\begin{array}{c|c} H_x & H_z \\ 11111 & 00000 \\ 00000 & 11111 \end{array}\right). \tag{7.79}$$

7.5.4 *Физика шума*

Шум и декогерентность сами по себе являются большими темами для изучения. Здесь мы всего лишь представим некоторые базовые идеи, чтобы прояснить, что может и чего не может сделать КИО. Под «шумом» мы понимаем просто любое неизвестное и нежелательное изменение матрицы плотности нашей системы.

Утверждение (7.62) об оцифровке шума эквивалентно утверждению, что любое взаимодействие между системой кубитов и окружением имеет вид

$$H_I = \sum_i E_i \otimes H_i^e, \tag{7.80}$$

где операторы H_i^e действуют на окружение. Под действием этой связи, матрица плотности системы (после усреднения по окружению)

переходит из ρ_0 в $\Sigma_i a_i E_i \rho_0 E_i$. КИО переводит все члены с исправляемыми E_i обратно в ρ_0. Следовательно, точность воспроизведения исправленного состояния по отношению к свободному от шума состоянию ρ_0 определяется суммой всех коэффициентов a_i, относящихся к неисправляемым ошибкам.

Математически строгий анализ этой проблемы дан в работах [365, 366]. Основные идеи таковы. Шум – это, как правило, непрерывный процесс, влияющий на все кубиты в течение всего времени. Однако, при обсуждении КИО мы всегда принимаем модель, в которой с помощью проекционного измерения извлекается синдром. Любое утверждение типа «вероятность того, что происходит ошибка E_i» есть просто сокращенная форма от «вероятность того, что извлечение синдрома проицирует состояние на такое, которое отличается от состояния без шума на оператор ошибки E_i» . Мы хотим вычислить эти вероятности.

Чтобы это сделать, будет полезно разделить (7.80) на сумму членов, содержащих операторы ошибки с разными весами:

$$H_I = \sum_{\text{вес}(E)=1} E \otimes H_E^e + \sum_{\text{вес}(E)=2} E \otimes H_E^e + \sum_{\text{вес}(E)=3} E \otimes H_E^e + \ldots \ . \qquad (7.81)$$

В первой сумме $3n$ членов, во второй – $3^2 n!/(2!(n\text{-}2)!)$, и так далее. Сила связи системы с окружением выражается через константы связи, которые стоят в операторах E^e_E. В том случае, когда в сумме присутствуют только члены с весом 1, мы говорим, что окружение действует независимо на каждый кубит: напрямую оно не производит коррелированные ошибки в двух и более кубитах. В этом случае в матрице плотности также будут присутствовать ошибки со всеми весами, но объем членов с весом w будет порядка $O(\varepsilon^{2w})$, где параметр ε обозначает силу связи системы с окружением.

Поскольку КИО восстанавливает в матрице плотности все элементы, вес ошибки у которых не превышает $t = d/2$, то можно оценить точность воспроизведения исправленного состояния, в модели некоррелированного шума, как один минус вероятность $P(t+1)$ того, что шум произведет ошибку веса $t+1$. Эта вероятность приблизительно равна

$$P(t+1) \simeq \left(3^{t+1} \binom{n}{t+1} \varepsilon^{t+1} \right)^2 , \qquad (7.82)$$

когда все одно-кубитные ошибки могут складываться когерентно (т.е. кубиты взаимодействуют с одним общим окружением), или

$$P(t+1) \simeq 3^{t+1} \binom{n}{t+1} \varepsilon^{2(t+1)} , \qquad (7.83)$$

когда ошибки складываются некогерентно (т.е. либо различное окружение, либо одно и то же окружение со связями со случайно меняющейся фазой). Значение формул (7.82) и (7.83) состоит в том, что КИО работает очень хорошо, если t большое, и $\varepsilon^2 < t/3n$. Поскольку хорошие коды существуют, t на самом деле может быть большим при фиксированных t/n и k/n. Следовательно, до тех пор, пока количество шума на кубит не превысит границу, приближенно равную $t/3n$, возможно почти полное восстановление состояния. Отношение t/n ограничивает скорость кода через квантовую границу Хэмминга или ее аналоги.

Такой некоррелированный шум является разумным приближением во многих физических ситуациях, однако, нам надо быть очень осторожными со степенью приближенности, поскольку нас интересуют очень малые члены порядка ε^d. Если мы ослабим приближение абсолютно некоррелированного шума, то уравнения (7.82) и (7.83) останутся, приближенно, такими же, если и только если константы связи в (7.81) для ошибок веса t сами по себе не превышают $\varepsilon^t/t!$

Совершенно другая ситуация, в которой КИО также работает очень хорошо, имеет место, когда в системе доминирует высоко коррелированный набор ошибок (так называемые ошибки разрыва), но мы можем найти КИО со стабилизатором, включающим в себя все эти коррелированные ошибки. Этот случай иногда называют «избеганием ошибок», а не «исправлением ошибок», поскольку нам даже не надо исправлять логическое состояние: оно уже не связано с окружением. Общий урок состоит в том, что чем больше мы знаем об окружении, и чем большей структурой обладает связь системы с окружением, тем лучше мы можем находить хорошие коды.

7.5.5 *Квантовое вычисление, устойчивое к сбоям*

Обсуждение КИО в предыдущих разделах относилось к передаче информации с высокой степенью точности по зашумленным квантовым каналам, но пока осталось неясным, какое отношение оно может иметь к квантовым вычислениям. Дело в том, что до сих пор мы предполагали, что сами квантовые операции, используемые при извлечении синдрома, защищены от шума. То есть, на самом деле, мы обрабатываем информацию для борьбы с шумом, но неясно, насколько точной должна быть обработка, чтобы что-нибудь получилось.

Устойчивое к сбоям вычисление занимается надежной обработкой информации, даже когда каждая элементарная операция и каждый период свободной эволюции сами по себе вносят шум. Один способ до-

биться этого состоит в многократном повторении КИО, но со специально сконструированной такой процедурой извлечения синдрома, чтобы она исправляла больше шума, чем порождала. Большинство важных новых идей, которые позволяют нам это сделать, было предложено Шором [367] и обсуждалось Прескилом [359]; см. также [368] – [370]. Здесь мы примем общий подход Шора, но с некоторыми существенными улучшениями, введенными Стином [371, 372]. Надо отметить, что эта тема гораздо меньше созрела для изложения, чем КИО; многие ее важные аспекты пока не исследованы. Здесь мы сконцентрируемся на том, чтобы объяснить один метод правильного извлечения синдрома.

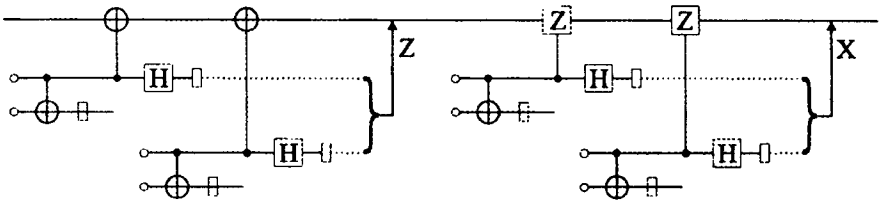


Рис. 7.8. Сеть для устойчивого к сбоям извлечения синдрома.

Полная квантовая сеть для устойчивого к сбоям извлечения синдрома показана на Рис. 7.8. Для краткости, рассмотрим простейший случай кода для исправления одной ошибки; все идеи можно обобщить на коды для исправления многих ошибок. Фундаментальные величины с двумя состояниями в компьютере называются физическими кубитами. Каждая горизонтальная линия в сети представляет не одиночный физический кубит, а блок из n таких кубитов. Операторы, например, оператор Адамара или CNOT, прикладываются к соответствующему блоку или блокам, т.е. всего применяется n операторов, по одному на каждый кубит или пару кубитов.

Наш метод основан на аккуратном использовании повторений, т.е. на том факте, что ошибки X- и Z-типа распространяются различным образом, а также на полезных свойствах кодов СШС. Определим позицию ошибки как любую 1 или 2-кубитную логическую операцию на физических кубитах (включая операции приготовления и измерения), или как свободную эволюцию любого физического кубита в течение одного шага по времени. Предполагается, что шум является некоррелированным и стохастическим, так что ошибки возникают независимо с вероятностью $\sim \gamma$. Цель всей сети состоит в том, чтобы исправить одну ошибку в блоке компьютера таким образом, чтобы ни один сбой на какой-либо одной позиции не привел к появлению ошибки веса ≥ 2 в блоке компьютера. Идея состоит в том, что извлечение синдрома должно сделать однобитные ошибки в компьютере более вероятными по

отношению к другим ошибкам, и, в то же время, именно однобитные ошибки легче исправлять. Важно также не создавать неисправимых ошибок с вероятностью $O(\gamma)$.

Мы начнем с того, что введем два дополнительных блока и приготовим каждый из них в нулевом состоянии $|0\rangle_L$. Каждое из этих приготовлений не устойчиво к сбоям; оно собьется так, что приготовленное состояние будет содержать любую ошибку любого веса с вероятностью $O(\gamma)$. Применяем CNOT поблочно между двумя дополнениями и измеряем все биты одного из них в вычислительном базисе. Таким способом мы пытаемся убедиться, что было приготовлено правильное состояние, пользуясь тем фактом, что поблочная физическая операция CNOT действует как логическая CNOT для кода СШС. Следовательно, результат измерения будет элементом классического кода $C_2^{\perp}$ (7.78). Если это не так, то приготовим дополнения снова, и будем повторять до тех пор, пока наше условие не будет выполнено. На этой стадии вероятность того, что оставшееся неизмеренное дополнение содержит ошибки с весом ≥ 2, равна $O(\gamma^2)$, так как это может случиться, только если произойдут сбои как минимум на двух позициях. Отметим, что дополнение может содержать ошибки Z-типа с любым весом.

Теперь свяжем проверенное дополнение с компьютером поблочным физическим CNOT. Еще раз, мы пользуемся тем фактом, что эта операция действует как логическая CNOT, так что на этой стадии сбоев не будет! На самом деле, кое-что при этом все-таки происходит: ошибки X-типа передаются от дополнения к компьютеру, а ошибки Z-типа передаются от компьютера к дополнению. Это хитрый и устойчивый к сбоям способ собрать синдром ошибок Z-типа в дополнении. Мы считываем его, преобразовывая дополнение вращением Адамара (чтобы превратить ошибки Z-типа в перевороты бита) и затем, производя измерение в стандартном вычислительном базисе. Здесь мы воспользовались тем свойством, верным для определенного класса кодов СШС, что поблочное физическое преобразование H действует как логическое H, так что состояние дополнения останется в закодированном подпространстве, за исключением ошибок Z-типа, которые превратятся в ошибки X-типа.

Пока еще в компьютере нет такой позиции, на которой могла бы произойти ошибка веса 2, но мы уже в опасности, так как уже есть много позиций, на которых единственный сбой привел бы к неверному синдрому. Если бы мы попытались «исправить» состояние компьютера на основе неверного синдрома, то на самом деле внесли еще больше ошибок. Поэтому надо повторить весь процесс, описанный выше. В результате появляется два синдрома. Если они согласуются друг с

другом, то тогда единственная ситуация, в которой они могут быть неправильными, состоит в том, что на двух разных позициях произошли сбои. Вероятность этого процесса порядка $O(\gamma^2)$, так что мы можем ею пренебречь и поверить синдромам. Если же они не согласуются, то надо извлечь третий синдром и поверить большинству из них.

Теперь мы выполнили исправление ошибок Z-типа в компьютере (в то же время, создавая новые ошибки Z-типа, которые будем вылавливать на следующем круге). Вторая половина сети действует аналогично, но собирает и исправляет в компьютере ошибки X-типа.

Отметим, что весь процесс зависит от того факта, что ошибки X- и Z-типа распространяются по-разному. Мы можем устойчивым к сбоям образом проверить дополнение на наличие ошибок X-типа, но только за счет риска создания в дополнении ошибок Z-типа. Это не страшно, поскольку эти ошибки Z-типа остаются на месте; они не переходят в компьютер, а просто портят синдром. Мы впоследствии проверяем систему на их наличие, вычисляя синдром еще раз. Отметим также, что мы сильно опираемся на полезные свойства кодов СШС, а именно, на их поведение под действием поблочных операций.

В повторяющейся серии исправления ошибок на каждом круге исправляются не только ошибки, возникшие в компьютере в течение этого круга, но также и ошибки, вызванные предыдущим кругом (если только они исправляемы). На каждом круге остаются неисправляемые ошибки, вызванные этим кругом. Следовательно, уровень шума, собранный после R повторений, подавляется с $O(R\gamma)$ до $O(R\gamma^2+\gamma)$, что выгодно при больших R и малых γ.

Чтобы выполнить задачу устойчивого к ошибкам *вычисления*, а не просто хранения данных в памяти, нам надо иметь возможность изменять состояние компьютера в желаемом квантовом алгоритме. Мы уже видели, как выполнять логические операции Адамара и CNOT на состоянии, закодированном кодом СШС: надо оперировать кубитами поблочно. Этот подход устойчив к сбоям, так как каждая физическая операция связывает только один кубит в соответствующем блоке. Чтобы получить полный набор операций, мы воспользуемся фактом, что элементы из непрерывного набора всех операций можно аппроксимировать элементами из дискретного набора. Чтобы сделать этот набор полным, достаточно иметь устойчивую к сбоям ячейку Тоффоли, или какую-либо родственную операцию, например, контролируемый поворот на $\pi/2$. Шор [367] предложил (несколько неясную) сеть для ячейки Тоффоли. Ее можно понять как конструкцию, родственную телепортации. Телепортацию можно понимать, как устой-

чивую к сбоям операцию обмена, и она может быть полезна для перемещения информации в квантовом компьютере устойчивым к сбоям образом [372, 373]. Этот и другие методы в настоящий момент активно исследуются.

На момент написания этой книги, устойчивое к сбоям вычисление на основе КИО выглядит наиболее многообещающим способом, чтобы осуществить большие квантовые алгоритмы, хотя требования к физической реализации квантового компьютера остаются весьма высокими.

7.6 Стандарты частоты

С.Ф.Хуэлга, С.Макчиавелло, М.Б.Пленио, А.К.Экерт

В этом разделе проанализированы прецизионные измерения частоты, основанные на захваченных ионах в присутствии декогерентности. Рассмотрены различные способы приготовления n двухуровневых систем, а также различные процедуры измерения. В частности, мы показываем, что стандартная рамзеевская спектроскопия на некоррелированных ионах и оптимальные измерения на максимально перепутанных состояниях дают одно и то же разрешение. Чтобы уменьшить нежелательное влияние декогерентности, мы предлагаем использовать процедуры симметризации. Мы показываем, как такие процедуры позволяют превысить даже оптимальную точность, достижимую с оптимизированным исходным приготовлением состояния n ионов и с оптимизированной схемой измерения.

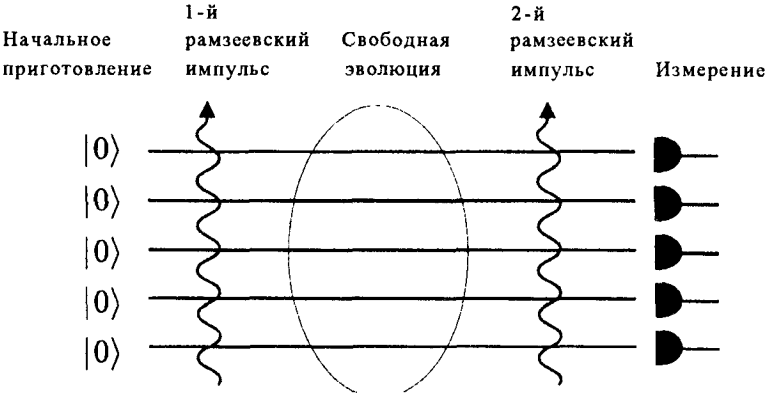


Рис. 7.9. Схематическое представление спектроскопии рамзеевского типа с нескоррелированными частицами.

Цель стандарта частоты состоит в том, чтобы стабилизировать стандартный осциллятор на данной атомной частоте. Осуществление стандарта оптической частоты в атомной ловушке на основе обычной рамзеевской интерферометрии показано на рис. 7.9.

В ионной ловушке находятся n ионов, исходно приготовленных в одном и том же внутреннем состоянии $|0\rangle$ (мы обозначаем через $|0\rangle$ и $|1\rangle$ основное и возбужденное состояние каждого иона). Ко всем ионам прикладывается рамзеевский импульс с частотой ω. Форма и частота импульса специально выбраны так, что он управляет атомным переходом $|0\rangle \leftrightarrow |1\rangle$, частота которого равна ω_0, и приготавливает для каждого иона равновесовую суперпозицию состояний $|0\rangle$ и $|1\rangle$.

$$|0\rangle \rightarrow \frac{|0\rangle + |1\rangle}{\sqrt{2}} \qquad |1\rangle \rightarrow \frac{-|0\rangle + |1\rangle}{\sqrt{2}} \ . \tag{7.84}$$

Далее система свободно эволюционирует в течение промежутка времени t. В системе отсчета, вращающейся с частотой осциллятора, свободная эволюция описывается гамильтонианом

$$H = -\hbar\Delta|1\rangle\langle 1| \ , \tag{7.85}$$

где $\Delta = \omega - \omega_0$ обозначает расстройку между классическим внешним полем и атомным переходом. Тогда эволюцию в базисе атомных состояний можно представить следующим образом:

$$|0\rangle \rightarrow |0\rangle \qquad |1\rangle \rightarrow e^{i\Delta t}|1\rangle \ , \tag{7.86}$$

и разность частоты между атомным переходом и опорным осциллятором приводит к накоплению относительной фазы. Если мы теперь приложим второй рамзеевский импульс, то вероятность, что ион будет после этого найден в состоянии $|1\rangle$, будет равна

$$P = \frac{1 + \cos(\Delta t)}{2} \ . \tag{7.87}$$

Если эта процедура повторяется в течение полного времени эксперимента T, то получающаяся в результате интерференционная кривая измеренной населенности на верхнем уровне позволяет нам узнать расстройку осциллятора и, после этого, настроить частоту опорного осциллятора. В этом месте возникает один вопрос. Какой наилучшей точности можно достичь, измеряя атомную частоту? Точнее говоря, при данном T и фиксированном данном числе ионов n, чему равен окончательный предел разрешения нашего стандарта частоты?

Статистические флуктуации, связанные с конечным образцом, дают для оцениваемой величины P неопределенность ΔP, которая равна

$$\Delta P = \sqrt{P(1-P)/N} \ , \tag{7.88}$$

где $N = nT/t$ обозначает реальное количество экспериментальных данных (мы предполагаем, что N большое). Следовательно, неопределенность в оценке ω_0 равна

$$|\delta\omega_0| = \frac{\sqrt{P(1-P)/N}}{|dP/d\omega|} = \frac{1}{\sqrt{nTt}} \quad . \tag{7.89}$$

Это соотношение часто называют *пределом дробового шума* [374]. Надо подчеркнуть, что этот предел возникает из-за внутреннестатистического характера квантовой механики, в отличие от других возможных источников технического шума. В то время как последние можно надеяться так или иначе уменьшить, дробовой шум накладывает фундаментальное ограничение на достижимое разрешение в прецизионной спектроскопии с n независимыми частицами.

Недавно была выдвинута идея о теоретической возможности преодолеть этот предел [375, 376]. Основная мысль состоит в том, чтобы исходно приготовить ионы в перепутанном состоянии. Чтобы увидеть преимущество этого подхода, рассмотрим случай двух ионов, приготовленных в максимально перепутанном состоянии

$$|\Psi\rangle = \left(|00\rangle + |11\rangle\right)/\sqrt{2} \quad . \tag{7.90}$$

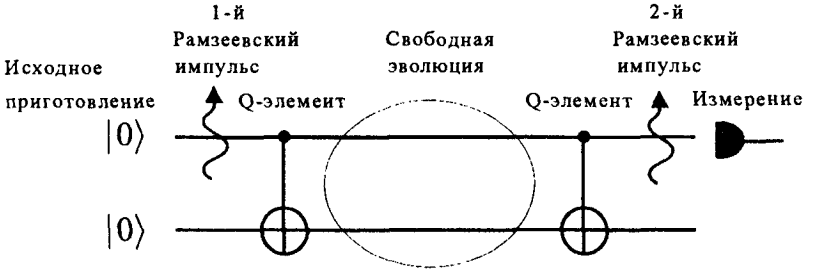


Рис. 7.10. Спектроскопия с двумя максимально перепутанными частицами. Перепутывание частиц создается и снимается с помощью элементов «контролируемое НЕ».

Это состояние можно создать, например, с помощью начальной части сети, показанной на Рис.7.10. За рамзеевским импульсом на первом ионе следует операция «контролируемое НЕ». После свободной эволюции, длящейся в течение периода t, состояние составной системы в координатной сетке, вращающейся вместе с частотой внешнего поля ω, выражается как

$$|\Psi\rangle = \left(|00\rangle + e^{2i\Delta t}|11\rangle\right)/\sqrt{2} \quad . \tag{7.91}$$

Вторая часть сети позволяет снять перепутывание ионов после периода свободной эволюции. Населенность в состоянии $|1\rangle$ первого иона будет теперь осциллировать с частотой 2Δ:

$$P_2 = \frac{1+\cos(2\Delta t)}{2} \quad . \tag{7.92}$$

Эту схему можно легко обобщить на случай n ионов с помощью последовательности элементов «контролируемое НЕ», связывающих первый ион с каждым из оставшихся. Таким образом, создается максимально перепутанное состояние n ионов вида

$$|\Psi\rangle = \left(|00...0\rangle + |11...1\rangle\right)/\sqrt{2} \quad . \tag{7.93}$$

Заключительное измерение первого иона, произведенное после периода свободной эволюции и второго набора элементов «контролируемое НЕ», даст сигнал

$$P_n = \frac{1+\cos(n\Delta t)}{2} \quad . \tag{7.94}$$

Преимущество этой схемы состоит в том, что теперь частота осцилляций сигнала увеличивается в n раз по отношению к случаю некоррелированных ионов, и соответствующая неопределенность частоты равна

$$|\delta\omega_0| = \frac{1}{n\sqrt{Tt}} \quad . \tag{7.95}$$

Заметим, что этот результат представляет собой улучшение в $1/\sqrt{n}$ раз по отношению к пределу дробового шума (7.89), при том же самом числе ионов n и той же полной продолжительности всего эксперимента T. Утверждалось [377], что это наилучшее возможное разрешение.

Рассмотрим теперь ту же ситуацию в реалистичном экспериментальном сценарии, в котором неизбежно присутствуют эффекты декогерентности. Основным типом декогерентности в ионной ловушке является дефазировка, вызванная процессами, которые вызывают случайные изменения в относительной фазе квантовых состояний, но сохраняют населенности атомных уровней. Важными механизмами, вызывающими дефазировку, являются столкновения ионов, случайные поля и лазерные нестабильности. Мы моделируем эволюцию во времени приведенного оператора плотности для одного иона ρ в присутствии декогерентности следующим мастер-уравнением [378]:

$$\frac{d\rho}{dt} = -i\Delta\left(\rho|1\rangle\langle 1| - |1\rangle\langle 1|\rho\right) + \gamma\left(\sigma_z\rho\sigma_z - \rho\right) . \tag{7.96}$$

Уравнение (7.96) написано в системе, вращающейся с частотой ω.

Здесь $\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$ обозначает оператор спина Паули. Мы также ввели скорость распада $\gamma = 1/\tau_{dec}$, где τ_{dec} есть время возникновения декогерентности. Для случая независимых частиц, это приведет к уширению сигнала:

$$P = \left(1 + \cos \Delta t e^{-\gamma t}\right)/2 \ . \tag{7.97}$$

В результате, соответствующая неопределенность в атомной частоте больше не зависит от величины расстройки. Теперь мы имеем

$$|\delta\omega_0| = \sqrt{\frac{1 - \cos^2(\Delta t)e^{-2\gamma t}}{nTte^{-2\gamma t}\sin^2(\Delta t)}} \ . \tag{7.98}$$

Чтобы достичь наилучшей точности, необходимо оптимизировать это выражение как функцию длительности каждого единичного измерения t. Наименьшее значение достигается при

$$\Delta t = k\pi/2 \ \ (k \ \text{нечетное}) \qquad t = \tau_{dec}/2 \ , \tag{7.99}$$

при условии, что $T > \tau_{dec}/2$. Таким образом, минимальная неопределенность частоты равна

$$|\delta\omega_0|_{opt} = \sqrt{\frac{2\gamma e}{nT}} = \sqrt{\frac{2e}{n\tau_{dec}T}} \ . \tag{7.100}$$

Для максимально перепутанного приготовления, сигнал (7.94) в присутствии дефазировки изменяется следующим образом:

$$P_n = \frac{1 + \cos(n\Delta t)e^{-n\gamma t}}{2} \ , \tag{7.101}$$

и получающаяся неопределенность оцененного значения атомной частоты минимальна при

$$\Delta t = k\pi/2n \ \ (k \ \text{нечетное}) \qquad t = \tau_{dec}/2n \ . \tag{7.102}$$

Интересно отметить, что мы воспроизводим в точности такую же минимальную неопределенность, как и в случае стандартной рамзеевской спектроскопии (7.100). Этот эффект иллюстрирован на Рис. 7.11. Модуль неопределенности по частоте $|\delta\omega_0|$ показан как функция длительности каждого одиночного эксперимента t для стандартной рамзеевской спектроскопии с n некоррелированными частицами и для максимально перепутанного состояния n частиц.

В присутствии декогерентности оба приготовления исходного состояния достигают одной и той же точности. Этот факт можно интуитивно понять, если учесть, что максимально перепутанные состояния наиболее хрупки в присутствии декогерентности: их время потери когерентности уменьшено в n раз, и, следовательно, длительность каждого одиночного эксперимента t должна быть во столько же раз меньше. Предыдущие выводы верны, когда полная длительность экс-

перимента превышает типичное время появления декогерентности. Следовательно, максимально перепутанные состояния обладают преимуществом только для кратковременной стабилизации. Что же касается длительных экспериментов, то недавно было показано [379], что наилучшее разрешение достигается при использовании частично перепутанных состояний с высокой степенью симметрии. Процедура включает в себя как оптимизацию исходного приготовления состояния n ионов, так и конечное измерение после этапа свободной эволюции. Однако, с практической точки зрения, ожидаемое улучшение не очень велико. Для $n = 7$ оптимальное улучшение точности составляет порядка 10% по отношению к пределу (7.100). Асимптотические пределы для больших n пока еще не найдены.

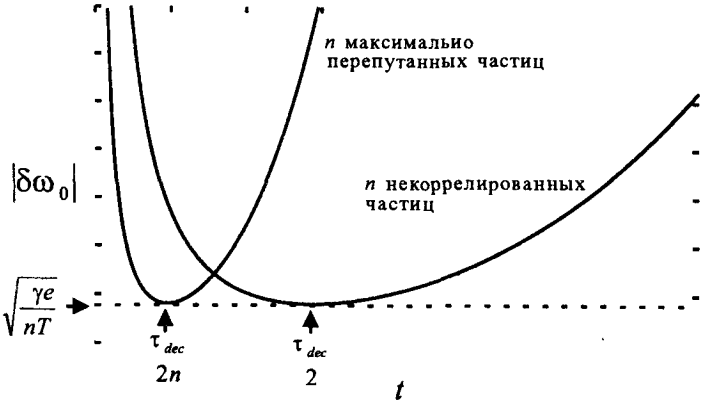


Рис. 7.11. Неопределенность по частоте $|\delta\omega_0|$ как функция длительности одиночного измерения t для максимально перепутанных и некоррелированных частиц. Заметим, что минимальная неопределенность абсолютно одинакова для обеих конфигураций.

Совершенно другой подход к улучшению разрешения стандарта частоты средствами квантового перепутывания состоит в использовании методов исправления ошибок. Как было показано в предыдущих разделах, эти процедуры могут эффективно уменьшить количество декогерентности и диссипации в квантовых системах. Однако, когда существующие протоколы по исправлению ошибок сбоя фазы применяются к этой конкретной проблеме, возникают трудности. Использование исправления ошибок не только исправляет фазовые ошибки, возникающие из-за внешнего шума, но еще и вредит желаемому изменению относительной фазы в квантовых состояниях в отстроенном осцилляторе, а ведь именно эту величину мы и хотим оценить. Этот факт уменьшает чувствительность стандарта частоты. Тем не

менее, как будет показано, все-таки можно *стабилизировать* систему по отношению к декогерентности и превзойти оптимальное разрешение, достижимое в спектроскопии некоррелированных частиц.

Ключевой момент состоит в том, чтобы понять следующее: в течение промежутка свободной эволюции, в отсутствие декогерентности, состояние n частиц, исходно приготовленных в состоянии, инвариантном относительно перестановок частиц, всегда остается в симметричном подпространстве гильбертова пространства составной системы n ионов (под симметричным подпространством мы подразумеваем подпространство, которое включает в себя все возможные состояния, инвариантные относительно перестановок n ионов). Проекция глобального состояния на симметричное подпространство [380] приведет тогда к частичному уничтожению эффектов, вызванных фазовыми ошибками из-за внешних воздействий. На Рис. 7.12 показано улучшение точности, в процентах, достижимое этим методом при $n = 2$. В этом случае была рассмотрена стандартная рамзеевская схема с исходно некоррелированными ионами, и в области свободной эволюции были применены повторяющиеся шаги с симметризацией. После каждого шага с симметризацией ионы оставляются, только если симметризация была успешной. В противном случае процедура прекращается, ионы устанавливаются в исходное состояние $|0\rangle$, и вся схема запускается с самого начала. Хотя такой подход уменьшает объем данных, которые можно использовать в статистике, Рис. 7.12 показывает, что эта стратегия удобна для улучшения общей точности эксперимента.

Пределы точности, достижимой с процедурами симметризации при произвольных n и произвольном приготовлении исходного состояния ионов, пока еще исследуются.

Следует отметить, что метод симметризации – это, скорее, метод детектирования ошибки, чем метод исправления ошибки. Метод симметризации просто удаляет ошибочные состояния, вместо того, чтобы их исправлять. Хотя остающийся ансамбль содержит меньше ошибок, статистика эксперимента становится хуже из-за того, что в симметричном подпространстве остается меньше систем. В целом получается небольшое улучшение. Возможность приложения к стандартам частоты настоящих квантовых кодов исправления ошибок в настоящее время исследуется. Прогресс в этом направлении мог бы привести к существенно улучшенным стандартам частоты. Но даже доказательство того, что квантовое исправление ошибок и перепутывание не могут существенно улучшить точность стандартов частоты, было бы очень интересным результатом.

В этом разделе мы представили приложение перепутывания и кван-

тового исправления ошибок к стандартам частоты. Мотивация для этого основана на том, что это приложение идей теории квантовой информации, которому требуются лишь небольшие квантовые ресурсы. Одним из направлений будущих исследований в теории квантовой информации является, безусловно, развитие других приложений, для которых требуются лишь небольшие ресурсы. Такие приложения могли бы быть реализованы экспериментально в ближайшем будущем.

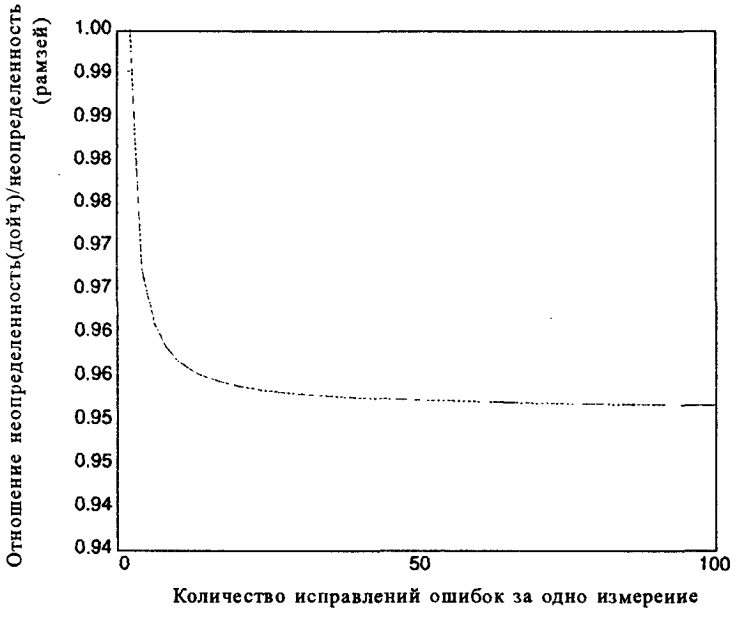


Рис. 7.12. Отношение неопределенностей для стандартной рамзеевской спектроскопии с симметризацией и без нее для $n = 2$ как функция числа шагов симметризации, выполняемых в течение одной области свободной эволюции.

Очищение перепутывания

8.1 Введение

В главе 7 была представлена теория квантовой коррекции ошибок. В настоящей главе рассматривается альтернативный метод преодоления последствий декогерентности, который особенно полезен при передаче квантового состояния. Основная идея состоит в выделении из большого набора (пар) перепутанных частиц, степень перепутывания которых, возможно, нарушена, набора частиц с увеличенной степенью перепутывания. В разделе 8.2 рассматриваются общие принципы очищения перепутывания. Обсуждаются специфические примеры, такие как локальная фильтрация (разд.8.3), пригодная для увеличения перепутывания чистых состояний и усиление квантовой секретности, разработанное для увеличения надежности квантовой криптографии при зашумленных квантовых каналах связи. В разд.8.5 будет рассмотрено обобщение очищения многочастичного перепутывания. В разд.8.6 показывается, как приготовить максимально перепутанные ЭПР-пары между пространственно разнесенными атомами, каждый из которых помещен внутрь высокодобротного оптического резонатора, когда фотоны направляются по зашумленным каналам, таким как обычное оптическое волокно. Поскольку вероятность поглощения фотонов при передаче растет экспоненциально с расстоянием, то для успешной передачи также потребуется увеличение числа повторных операций. В разделе 8.7 представлен метод квантового повторителя, который уменьшает рост числа таких операций, как функция расстояния передачи, с экспоненциального до полиномиального.

8.2 Принципы квантового очищения

Х.-Дж.Бригель

Центральная проблема квантовой связи состоит в точной передаче квантовой информации от одного участника А (Алиса) к другому – Б (Боб), когда коммуникационный канал связи, соединяющий А и Б, зашумлен. Качество, с которым квантовое состояние передается по зашумленно-

му каналу, уменьшается, в общем случае, экспоненциально с его длиной, так что точная передача оказывается ограниченной очень короткими расстояниями. Эта проблема, в принципе, решается в методе телепортации, который требует, чтобы Алиса и Боб имели определенный запас пар частиц в максимально перепутанном состоянии (ЭПР-пары). Однако остается вопрос, как А и Б могут приготовить такие перепутанные состояния, если они способны общаться только посредством зашумленных каналов? Поскольку перепутывание не может быть создано только при локальных операциях, А и Б должны будут посылать через канал квантовые биты на некотором этапе для того, чтобы осуществить нелокальные квантовые корреляции. Так как такие кубиты взаимодействуют с каналом, они подвергаются декогерентности и результирующие ЭПР-пары не являются максимально перепутанными, а будут описываться некоторым смешанным состоянием с определенным качеством перепутывания. Идея *очищения перепутывания* состоит в извлечении из большого ансамбля таких низкокачественных ЭПР-пар меньшего подансамбля с достаточно высоким качеством, который затем может быть использован для выполнения точной телепортации [49, 74] (глава 3) или для квантовой криптографии [46, 47] (глава 2).

С точки зрения перспективы осуществления квантовых сообщений имеется естественная связь между очищением перепутывания и квантовой коррекцией ошибок. Теория квантовой коррекции ошибок изначально развивалась, чтобы обеспечить возможность квантовых вычислений, несмотря на наличие эффектов декогерентности и влияния неидеальной аппаратуры. В то же время она может быть использована для исправления ошибок при передаче информации[1]. С другой стороны, очищение перепутывания является более специфическим, но и более мощным инструментом при обеспечении процесса передачи квантовой информации. При использовании классических сообщений между участниками, возможны высокоэффективные двусторонние протоколы, которые не могут быть реализованы в технике квантовой коррекции ошибок. Более того, этот метод чрезвычайно надежен в отношении к несовершенной аппаратуре, что делает его крайне привлекательным для разного рода приложений, таких как квантовые повторители. Количественный анализ связи между очищением перепутывания и квантовой коррекцией ошибок приводится в работе [323].

Следует подчеркнуть, что проблема очищения (и количественного измерения) перепутывания представляет фундаментальный инте-

[1] На самом деле, изначально развивалась *классическая* коррекция ошибок в точности для тех же целей.

рес вне зависимости от частных приложений в сфере коммуникации, которые *сегодня* мы можем себе представить. Вероятно, в будущем мы узнаем гораздо больше о (много-) частичном перепутывании, чем представляем себе сейчас, и его применение не будет ограничиваться только вычислительными и коммуникационными задачами. В любом случае, было бы очень хорошо иметь перепутанные состояния в лаборатории, поэтому нам нужно знать, как можно эффективно их приготавливать и очищать.

Что же из себя представляет очищение перепутывания?

Для иллюстрации основных идей прежде всего рассмотрим ансамбль частиц со спином 1/2, которые частично поляризованы вдоль определенного направления (скажем, вдоль оси z). Предположим, для простоты, что мы имеем дело с некогерентной смесью частиц в состоянии $|\uparrow\rangle \equiv |$*спин вверх*$\rangle$ и $|\downarrow\rangle \equiv |$*спин вниз*$\rangle$, соответственно, представляемой матрицей плотности

$$\rho = f|\uparrow\rangle\langle\uparrow| + (1-f)|\downarrow\langle\downarrow|\rangle \ , \tag{8.1}$$

хотя такое ограничение и не существенно для дальнейшей аргументации. Мы просто можем выбрать подансамбль частиц в состоянии $|\uparrow\rangle$, измеряя спин частиц, ориентированный вдоль оси z, т.е. пропуская их через магниты Штерна и Герлаха (ШГ), показанные на рис. 8.1. Отбирая только те частицы, которые выходят из верхней части прибора (что будет происходить, в среднем, для части f от общего числа частиц), мы будем, очевидно, готовить подансамбль частиц в чистом состоянии $\rho' = |\uparrow\rangle\langle\uparrow|$. Можно было бы сказать, что у нас имеется «очищенный» полный ансамбль при «дистилляции» частиц с нужной поляризацией, хотя такая терминология в данном случае слишком неестественна.

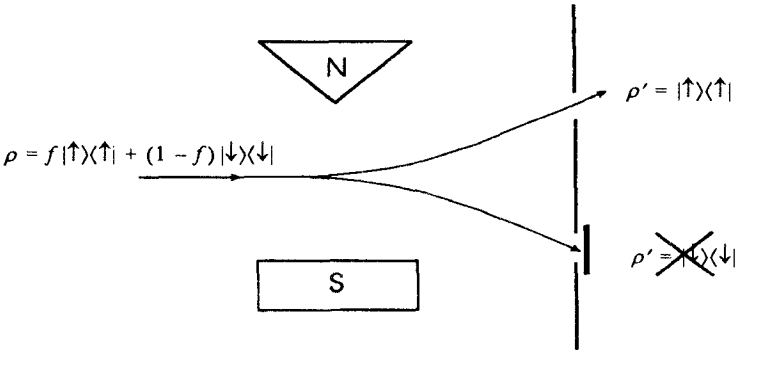


Рис.8.1. Отбор спин-поляризованных атомов с помощью магнитов Штерна-Герлаха: неоднородное магнитное поле в направлении оси z, создаваемое двумя магнитами (S и N), используется для пространственного разделения частиц с различными спинами. Для краткости будем называть такое устройство «прибор Штерна и Герлаха».

По причинам, которые позже станут ясны, представим себе несколько более сложную ситуацию, когда благодаря некоему неизвестному механизму, частицы разрушаются (т.е. поглощаются) после прохождения через прибор ШГ! Мы лишь предположим, что прибор выдает нам сигнал, если частица выходит из верхнего отверстия на Рис. 8.1 и не выдает сигнал в других случаях, поглощая все остальные частицы. Каким образом мы можем использовать такой дефектный прибор для очищения ансамбля? Такая возможность состоит в том, чтобы посылать через прибор ШГ не сами частицы, а их *копии*. Хотя в общем случае нельзя создать копию квантового состояния (теорема о запрете клонирования, разд.2.2.2 [88]), но оказывается возможным копировать выбранные базисные состояния, используя вспомогательную частицу С и измерительные ЛЭ (или ЛЭ CNOT). Измерительный ЛЭ был рассмотрен в разд.1.6: если начальное состояние частицы С представляет собой $|\uparrow\rangle_C$, его воздействие состоит в копировании базисных состояний $|\uparrow\rangle_A$ и $|\downarrow\rangle_A$ частицы А на частицу С[2, 3],

$$|\uparrow\rangle_A|\uparrow\rangle_C \to |\uparrow_A\rangle|\uparrow\rangle_C$$

$$|\downarrow\rangle_A|\uparrow\rangle_C \to |\downarrow_A\rangle|\downarrow\rangle_C \quad . \tag{8.2}$$

Применяя эти преобразования к ансамблю (8.1) измерительный ЛЭ приготавливает два (классических) коррелированных ансамбля в виде[4]:

$$\rho_{AC} = f|\uparrow\rangle_A\langle\uparrow|\otimes|\uparrow\rangle_C\langle\uparrow| + (1-f)|\downarrow\rangle_A\langle\downarrow|\otimes|\downarrow\rangle_C\langle\downarrow| \; . \tag{8.3}$$

Если мы теперь измерим значение спина вспомогательной частицы, мы разрушим *эту* частицу, но щелчок детектора будет указывать, что соответствующая частица А находится в чистом состоянии $\rho'_A = |\uparrow\rangle_A\langle\uparrow|$ (см. рис.8.2а). Измеряя копию каждой частицы, мы просто проверяем, какие из частиц находятся в правильном состоянии и поэтому, выбираем очищенный подансамбль.

---

[2] Это означает, что любая суперпозиция $(\alpha|\uparrow\rangle_A + \beta|\downarrow\rangle_A)$ преобразуется таким ЛЭ в соответствие с

$$(\alpha|\uparrow\rangle_A + \beta|\downarrow\rangle_A)\,|\uparrow\rangle_C \to \alpha|\uparrow\uparrow\rangle_{AC} + \beta|\downarrow\downarrow\rangle_{AC} \neq (\alpha|\uparrow\rangle_A + \beta|\downarrow\rangle_A)(\alpha|\uparrow\rangle_C + \beta|\downarrow\rangle_C)$$

Поэтому принцип неклонируемости [88] здесь не нарушается.

[3] В более общем случае спин частицы С переворачивается при условии, что частица А находится в состоянии $|\downarrow\rangle_A$. Т.е. (8.2) вместе с преобразованиями

$$|\uparrow\rangle_A|\downarrow\rangle_C \to |\uparrow\rangle_A|\downarrow\rangle_C \quad \text{и} \quad |\downarrow\rangle_A|\downarrow\rangle_C \to |\downarrow\rangle_A|\uparrow\rangle_C$$

описывают полный ЛЭ CNOT .

[4] Это действительно так, когда вспомогательные частицы С изначально находятся в состоянии $|\uparrow\rangle_C$.

Очевидно, что здесь используется некая уловка: предположение о том, что вспомогательные частицы находятся в *чистом* состоянии $|\uparrow\rangle_C$ означает, что идея очищения становится бессмысленной, поскольку мы могли бы с самого начала, вместо смешанного ансамбля, использовать вспомогательные частицы.

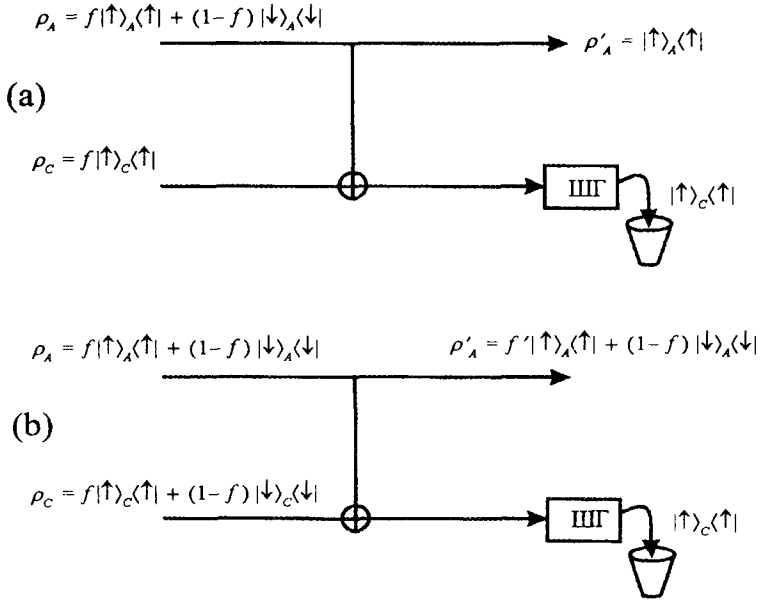


Рис.8.2. Отбор спин-поляризованных атомов воображаемым прибором ШГ, который поглощает атомы при измерении их состояний. Состояние атома смешанного ансамбля (верхняя линия) копируется (символ ⊕) в состояние вспомогательного атома С (нижняя линия), над которым и призводится разрушающее измерение. Вспомогательные атомы, используемые в (a) находятся в поляризационном состоянии $|\uparrow\rangle_C$; в (b) они выбираются из смешанного ансамбля.

Что мы должны сделать для приготовления копий, если у нас действительно есть полностью поляризованные спины? Важный момент состоит в том, что для этой цели, точно также мы можем использовать частицы, взятые из смешанного ансамбля. При условии $f > 1/2$, более вероятно, что некоторая случайно отобранная (для копирования) частица будет находиться в правильном внутреннем состоянии $|\uparrow\rangle_C$ и может быть, таким образом, использована для проверки неизвестного состояния некоторой другой частицы ансамбля. Для выполнения количественных оценок, представим, что мы делим начальный ансамбль, который мы хотим очистить, на два подансамбля ρ_A и ρ_C одинакового размера (мы обозначаем их разными индексами А и С, чтобы различать их вклад в измерительный ЛЭ). Оба подансамбля

будут описываться одной и той же матрицей плотности (8.6), см. также рис.8.2b. Теперь, для каждого атома из ансамбля A, мы выбираем атом из ансамбля C и копируем состояние A в состояние C при помощи измерительного ЛЭ. После того, как эта процедура выполнена для всех частиц, мы получаем следующий ансамбль:

$$\rho_{AC} = \left(f^2 |\uparrow\rangle_A \langle\uparrow| + (1-f)^2 |\downarrow\rangle_A \langle\downarrow|\right) \otimes |\uparrow\rangle_C \langle\uparrow|$$

$$f(1-f)\left(|\uparrow\rangle_A \langle\uparrow| + |\downarrow\rangle_A \langle\downarrow|\right) \otimes |\downarrow\rangle_C \langle\downarrow| \quad . \tag{8.4}$$

Теперь мы измеряем состояние частиц C и собираем все те частицы ансамбля A, копия которых была обнаружена в состоянии $|\uparrow\rangle_C$ («щелчок детектора»), в новый ансамбль. Такой новый ансамбль будет описываться оператором плотности

$$\rho'_A = f' |\uparrow\rangle_A \langle\uparrow| + (1-f') |\downarrow\rangle_A \langle\downarrow| \quad , \tag{8.5}$$

где $f' = f^2/(f^2 + (1-f)^2)$. Простая функция $f'(f)$ идентична той, которая изображена на рис. 8.4, когда мы будем обсуждать очищение смешанных перепутанных состояний. Таким образом, для $f > 1/2$ мы получаем *очищенный ансамбль* с большей частью $f' > f$ частиц, находящихся в состоянии $|\uparrow\rangle_A$. Выполняя несколько итераций такой процедуры, что изображено ступеньками на рис.8.4, нам удастся отделить частицы, находящиеся в состоянии, как угодно близком к чистому состоянию $|\uparrow\rangle_A$, при условии, что начальный ансамбль был достаточно большим[5].

Теперь мы готовы приступить к обсуждению очищения смешанных перепутанных состояний. Представим, что Алиса и Боб хотят очистить ансамбль двухчастичных перепутанных состояний ρ_{AB}, когда частицы A и B находятся в разных пространственных точках. Рассмотрим следующий простой пример:

$$\rho_{AB} = f |\Phi^+\rangle_{AB} \langle\Phi^+| + (1-f) |\Psi^+\rangle_{AB} \langle\Psi^+| \tag{8.6}$$

с состояниями Белла

$$|\Phi^+\rangle_{AB} = \{|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle\}/\sqrt{2}$$

и

$$|\Psi^+\rangle_{AB} = \{|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle\}/\sqrt{2} \quad ,$$

когда $1/2 < f < 1$. До тех пор пока $f = 1/2$, состояние (8.6) является

[5] По правде говоря, чтобы таким методом выделить чистое состояние, необходимо, чтобы начальный ансамбль был бесконечно большим.

несепарабельным. Мы можем рассматривать (8.6) как классическую смесь двух ансамблей (чистых) состояний Белла $|\Phi^+\rangle_{AB}$ и $|\Psi^+\rangle_{AB}$ с размерами f и $(1-f)$, соответственно[6]. Очевидно, что проводя обе частицы через соответствующие приборы ШГ, каждый со своей стороны, Алиса и Боб могут различить два подансамбля. Для пар в состоянии $|\Phi^+\rangle_{AB}$, обе частицы будут вылетать из одних и тех же выходов прибора (спины «вверх-вверх» или «вниз-вниз»), в то время как для пар, находящихся в состоянии $|\Psi^+\rangle_{AB}$, частицы будут выходить из прибора через разные выходы («вверх-вниз» или «вниз-вверх») в предположении, что и Алиса и Боб одинаково настроили свои приборы (магниты ориентированы в z-направлении). С другой стороны, такое измерение будет *разрушать* любое изначально существующее перепутывание и частицы будут выходить из приборов в смешанном состоянии. Поэтому возникает следующая проблема. Каким образом Алиса и Боб могут выбрать подансамбль, описываемый состоянием $|\Phi^+\rangle_{AB}$, если при локальном измерении они разрушают перепутывание?

Для разрешения этой проблемы мы можем использовать выводы, сделанные в ходе обсуждения одночастичного очищения. Могут ли Алиса и Боб применить прием с измерительным ЛЭ и пропустить «копии» A и B через приборы ШГ, вместо того, чтобы пропускать через них сами частицы? Оказывается, что могут, если начальное состояние частиц, используемых для копирования, само является перепутанным. Чтобы убедиться в этом, рассмотрим ситуацию, когда Алиса и Боб обладают двумя парами, причем одна пара AB принадлежит ансамблю (8.6), а вторая пара $A'B'$ находится в чистом состоянии $|\Phi^+\rangle_{A'B'}$. Теперь они копируют состояние пары AB в состояние пары $A'B'$, применяя измерительный ЛЭ (8.2) каждый со своей стороны, т.е. между частицами A и A', а также между B и B', соответственно. Результат такой операции может быть подытожен в следующем виде:

$$\left|\Phi^+\right\rangle_{AB}\left|\Phi^+\right\rangle_{A'B'} \rightarrow \left|\Phi^+\right\rangle_{AB}\left|\Phi^+\right\rangle_{A'B'}$$

$$\left|\Psi^+\right\rangle_{AB}\left|\Psi^+\right\rangle_{A'B'} \rightarrow \left|\Psi^+\right\rangle_{AB}\left|\Psi^+\right\rangle_{A'B'} \quad . \tag{8.7}$$

Такая билатеральная (CNOT) операция, очевидно, воздействует как измерительный ЛЭ для *пар*, когда состояния $|\Phi^+\rangle$ и $|\Psi^+\rangle$ играют роль, аналогичную $|\uparrow\rangle$ и $|\downarrow\rangle$ в (8.2). Это означает, что если Алиса и Боб обладают некоторыми парами в состоянии $|\Phi^+\rangle_{A'B'}$, они могут использовать их для проверки нужного подансамбля. При этом, конечно, проблема

[6] Часть $f = \langle\Phi^+|\,\rho_{AB}|\Phi^+\rangle_{AB}$ в (8.6) называется также «качеством перепутывания» (или просто качеством) смешанного состояния ρ_{AB} в отношении состояния Белла $|\Phi^+\rangle_{AB}$.

состоит в том, что у них нет вспомогательных пар в состоянии $|\Phi^+\rangle_{AB}$ (в противном случае, очищение вообще было бы не нужным)! Вспомним, однако, предыдущее обсуждение одночастичных состояний – Алиса и Боб могли одинаково хорошо использовать пары из смешанного ансамбля при условии, что большинство из них находится в правильном начальном состоянии $|\Phi^+\rangle$ (т.е. $f > 1/2$). Поэтому обсуждаемый протокол очень похож на протокол одночастичного очищения (см.Рис.8.3):

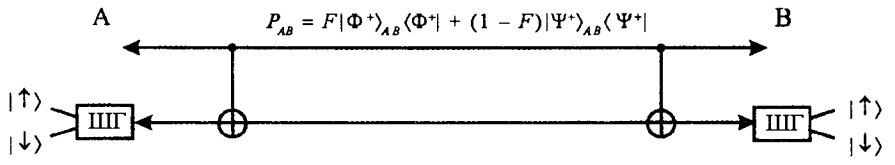


Рис.8.3. Очищение смешанного ансамбля перепутанных состояний с помощью локальных унитарных операциях, измерении и классических сообщений.

1. Алиса и Боб случайно выбирают пары из ансамбля (8.6) и используют одну из пар для измерения состояния другой пары, т.е.

2. они применяют ЛЭ CNOT к соответствующим частицам с каждой стороны;

3. они измеряют состояние вспомогательной пары, т.е. с помощью двух приборов ШГ, как и на Рис. 8.3 (разрушая, таким образом, перепутывание).

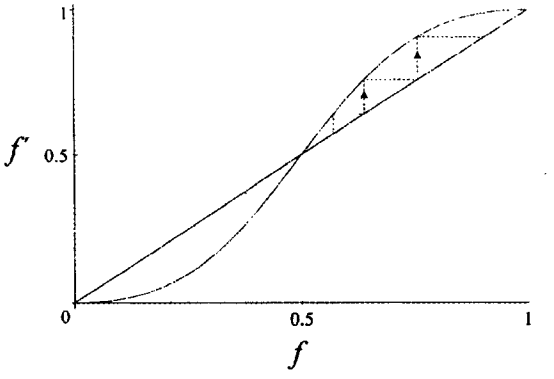


Рис.8.4. Очищение смешанных перепутанных состояний. Для $f > 1/2$ качество пар (8.6) увеличивается до величины f' (8.8). При итерациях (ступеньки) можно выделить из большого ансамбля низкокачественных пар, пары с высоким значением качества . Заметим, что для этого простого (т.н. реккурентного) метода более 50% всех пар теряется на каждом шаге.

Оставляя только те пары, для которых измерение дает одинаковое значение спинов («ввех-вверх» или «вниз-вниз») они могут отобрать новый ансамбль, который описывается оператором плотности

$$\rho'_{AB} = f'\left|\Phi^+\right\rangle_{AB}\left\langle\Phi^+\right| + (1-f')\left|\Psi^+\right\rangle_{AB}\left\langle\Psi^+\right|, \qquad (8.8)$$

с большей частью $f' = f^2/(f^2 + (1-f)^2) > f$ (для $f > 1/2$) пар в состоянии $|\Phi^+\rangle_{AB}$ (см.рис.8.4). Заметим, что для того, чтобы сравнить исходы своих измерений и, таким образом, решить, какие пары нужно отбросить, Алиса и Боб должны иметь возможность общаться и обмениваться классической информацией, что является неотъемлемым компонентом любого протокола очищения. Повторяя эту процедуру, как показано на рис.8.4 в виде ступенек, Алиса и Боб могут отобрать ансамбль пар с качеством перепутывания f, сколь угодно близким к единице.

Может показаться, что в случае (8.6) мы обсудили довольно специфический пример смешанного двухчастичного состояния. Однако такой метод также работает и для общих состояний ρ_{AB}, при условии, что они содержат достаточно большую часть $f = \langle\Phi_{me}|\rho_{AB}|\Phi_{me}\rangle > 1/2$ частиц в максимально перепутанных состояниях $|\Phi_{me}\rangle$[7]. Первый протокол очищения перепутывания был предложен Беннетом и соавторами в [49]. Он позволяет выделять из большого ансамбля перепутанных состояний с качеством $f > 1/2$ малый ансамбль пар с качеством, сколь угодно близким к единице. Эти пары могут затем быть использованы для точной телепортации через зашумленный канал. Второй протокол, названный «усилением квантовой секретности» (QPA) предложен Дойчем и соавторами в [47]. Не касаясь различий в деталях (таких как эффективность в синтезе синглетов), отметим, что оба протокола используют измерительный ЛЭ в качестве основного компонента при выполнении измерений над нелокальными перепутанными состояниями с разрушением их перепутывания. Исходная мотивация QPA протокола состоит в применении его в квантовой криптографии, основанной на перепутанных состояниях [46]. При этом выполняется процедура, которая позволяет Алисе и Бобу, в принципе, обнаружить потенциальное подслушивание в выбранном наборе пар. Это существенно может быть использовано при распределении квантовых клю-

[7] Под таким состоянием мы подразумеваем любое состояние, пригодное для выполнения локальных унитарных преобразований над частицами Алисы и Боба, эквивалентное одному из четырех (и, таким образом, для всех) состояний Белла. Обычно, в некотором месте протокола, который работает с общими смешанными состояниями ρ_{AB}, превалирующая компонента $|\Phi_{me}\rangle$ этого состояния ρ_{AB}, преобразуется в состояние Белла $|\Phi^+\rangle$ до применения билатеральной операции CNOT.

чей. Такой метод усиления квантовой секретности будет рассмотрен в разд.8.4.

Следует подчеркнуть, что метод, который мы рассматривали выше и иллюстрирующий идею очищения перепутывания, не является единственным для очищения перепутанных состояний. Имеются более изощренные способы (использующие т.н. многочастичные измерения), в которых разрабатываются идеи, заимствованные из классической теории информации, такие как случайная нарезка [49, 323], и служащие для увеличения эффективности протоколов. Другой интересный и простой метод, который особенно предпочтителен для увеличения перепутывания *чистых* состояний – это *локальная фильтрация* [117, 382], которая будет более подробно рассмотрена в разд.8.3. К настоящему времени выполнен целый ряд теоретических исследований по очищению перепутывания, в которых развиваются первые идеи, сформулированные несколько лет назад. Но, в силу понятных причин, мы не можем обсуждать их в этом элементарном введении. Примеры охватывают важное понятие «связанное перепутывание» [383], обсуждение оптимальных протоколов очищения [322, 323, 384, 385], а также эффективности и устойчивости протоколов очищения при несовершенных локальных операциях [381, 386, 387]. Обобщение очищения перепутывания для многочастичных перепутанных состояний обсуждается в разд.8.5.

8.3 Локальная фильтрация

Б.Хаттнер, Н.Жизан

При очищении перепутывания рассматривается неограниченное число пар квантовых систем; все они находятся в одинаковом (возможно, и в смешанном) состоянии ρ_{in}. Задача состоит в выделении из этого набора части максимально перепутанных чистых состояний при использовании только локальных операций и классических коммуникаций между участниками. Рассмотрим сначала случай чистого перепутанного состояния двух квантовых систем $\rho_{in} = |\Psi_{in}\rangle\langle\Psi_{in}|$. Мы покажем, что такое состояние всегда может быть «очищено» с помощью локальной фильтрации до 2-ух кубитового синглетного состояния $1/\sqrt{2}(|01\rangle - |10\rangle)$. Такая процедура описывает концепцию локальной фильтрации – особый простой пример очищения перепутывания – и показывает, что для очищения перепутывания, в общем, достаточно рассматривать очищение до синглетных состояний [382].

Используя разложение Шмидта, всегда можно представить в виде:

$$\psi_{in} = \sum_{j=1}^{N} c_j \alpha_j \otimes \beta_j \quad , \tag{8.9}$$

где $\{\alpha_j\}$ и $\{\beta_j\}$ – ортогональные базисы гильбертовых пространств двух перепутанных квантовых систем. Поскольку состояние ψ_n предполагается перепутанным, имеется по крайней мере 2 ненулевых c_j; отсюда мы можем положить, что $c_1 \neq 0$ и $c_2 \neq 0$. Чтобы очистить ψ_{in}, Алиса, система которой находится в состояниях α_j и Боб, система которого находится в состояниях β_j, первым делом измеряют проекторы $P_{\alpha_1}+P_{\alpha_2}$ и $P_{\beta_1}+P_{\beta_2}$, соответственно. Используя классические сообщения Алиса и Боб сохраняют только те пары, которые дают положительные исходы измерений. Эти пары находятся в следующих состояниях:

$$\psi_1 = c_1\alpha_1 \otimes \beta_1 + c_2\alpha_2 \otimes \beta_2 \ . \tag{8.10}$$

Отсюда, каждая подсистема включает в себя только два ортогональных состояния, подобно кубиту. Предположим, что $|c_1|^2 \geq |c_2|^2$, тогда Алиса и Боб применяют 2 фильтра F_A и F_B, которые подавляют α_1 и β_1, пропуская неизменными α_2 и β_2. Такие фильтры представляются следующими положительными операторами:

$$F_A = \sqrt{\frac{|c_2|}{|c_1|}}P_{\alpha_1} + P_{\alpha_2} \quad \text{и} \quad F_B = \sqrt{\frac{|c_2|}{|c_1|}}P_{\beta_1} + P_{\beta_2} \ . \tag{8.11}$$

Используя классический коммуникационный канал, Алиса и Боб выбирают только те пары систем, которые проходят через оба фильтра. (В действительности, достаточно, чтобы только Алиса или только Боб измеряли свой оператор и использовали фильтр). Заметим, что такие фильтры существуют на самом деле. Например, общеизвестны оптические элементы с потерями, зависящими от поляризации. Примеры из области экспериментальной квантовой оптики см. в [388]. Состояние отфильтрованных систем имеют одинаковые веса в конечных факторизуемых состояниях:

$$\psi_2 = F_A \otimes F_B\psi_1 = \frac{|c_2|}{|c_1|}c_1\alpha_1 \otimes \beta_1 + c_2\alpha_2 \otimes \beta_2 \ . \tag{8.12}$$

В итоге, Алисе и Бобу нужно фиксировать относительную фазу между $\alpha_1 \otimes \beta_1$ и $\alpha_2 \otimes \beta_2$ для получения нужного синглетного состояния (с точностью до несущественной общей фазы):

$$\psi_{filtered} = \alpha_1 \otimes \beta_1 - \alpha_2 \otimes \beta_2 \ . \tag{8.13}$$

В самом общем случае проблема очищения перепутывания оказывается гораздо сложнее (для более чем 2 перепутанных систем общее решение пока неизвестно). Однако, относительно простые фильтры, рассмотренные выше, можно использовать для очищения некоторых смешанных состояний. Это будет показано ниже. Основываясь на вышеизложенных результатах, рассмотрим следующую смесь 2-кубитовых состояний:

$$\rho_{in}(\lambda,c)=\lambda P_{\psi_c}+\frac{1-\lambda}{2}\left(P_{\psi_{11}}+P_{\psi_{00}}\right)\ , \tag{8.14}$$

где λ и c – два действительных числа, принимающих значения между 0 и 1, и

$$\psi_c=c|10\rangle-\sqrt{1-c^2}\,|01\rangle\ ,\quad \psi_{11}=|11\rangle\ ,\quad \psi_{00}=|00\rangle\ . \tag{8.15}$$

До того, как показать, что состояние $\rho(\lambda,\ c)$ может быть очищено, мы хотели бы доказать, что это состояние никогда не нарушает неравенство Белла-КХШ [12][8]. Для этой цели мы воспользуемся красивым результатом, полученным семьей Городецки [389]. Применяя его к состоянию $\rho(\lambda,\ c)$, можно сделать вывод о том, что

$$\frac{1}{2-2c\sqrt{1-c^2}}<\lambda\le\frac{1}{1+c^2\left(1-c^2\right)} \tag{8.16}$$

т.е. неравенство Белла-КХШ не нарушается. Отсюда, очевидно, что $\rho(\lambda,\ c)$ является локальным, хотя ниже мы покажем, что $\rho(\lambda,\ c)$ может быть очищено до синглетных состояний и, следовательно, что $\rho(\lambda,\ c)$ в действительности нелокально.

На самом деле, процедура по очищению $\rho(\lambda,\ c)$ очень похожа на пример, приведенный выше: Алиса и Боб применяют фильтры (8.11) с $c_1 = c$ и $c_2 = \sqrt{1-c^2}$. Отфильтрованное состояние принимает вид:

$$\rho_{filtered}(\lambda,c)=FA\otimes FB\,\rho_{in}(\lambda,c)\,FA\otimes FB=$$
$$\frac{1}{N}\left(2\lambda c\sqrt{1-c^2}P_{\text{sin}glet}+\frac{1-\lambda}{2}\left(P_{\psi_{11}}+P_{\psi_{00}}\right)\right), \tag{8.17}$$

где для нормировки введен фактор $N = 2\lambda c\sqrt{1-c^2}+(1-\lambda)$.

Снова используя теорему Городецки [389], можно получить, что это состояние нарушает неравенство Белла-КХШ, если

$$\lambda>\frac{1}{1+2c\sqrt{1-c^2}\left(\sqrt{2}-1\right)}\ . \tag{8.18}$$

Верхняя и нижняя границы λ, определенные условиями (8.16) и (8.18) совместны если $c\sqrt{1-c^2}\le\sqrt{2}-1$. Отсюда, существуют значения λ и c, такие что состояние $\rho(\lambda,\ c)$ является «локальным», в том смысле, что не нарушается неравенство Белла-КХШ, и такое, что соответствующее состояние, отфильтрованное локальным окружением – $\rho_{filtered}(\lambda,\ c)$ – нарушает некоторое неравенство типа Белла-КХШ.

[8] т.е. неравенство Белла-Клаузера-Хольта-Шимони (*Прим.переводчика*).

Выше мы ввели идентификацию – «локальное» ≈ «не нарушает неравенство Белла-КХШ». В этом смысле, результаты, полученные выше, выглядят более впечатляюще! Но, очевидно, что такая идентификация может и должна быть подвергнута критике. Состояние, которое является полностью нелокальным, после некоторых локальных взаимодействий не может быть квалифицировано как локальное. Вопрос остается открытым – допускают ли состояния $\rho(\lambda, c)$, удовлетворяющие (8.16) и (8.18), описания с помощью локальной модели со скрытыми параметрами, порождающей все имеющиеся корреляции. Поскольку они не нарушают никаких неравенств Белла-КХШ, возможно, что такая модель существует. Однако, даже если такая модель со скрытыми параметрами и существует, состояние может быть названо нелокальным, т.к. возникновение всех корреляций не является достаточным, как показано на примере, приведенном выше.

8.4 Усиление квантовой секретности

С.Макчиавелло

Основная цель использования схем по очищению перепутывания состоит в выделении подмножества состояний с повышенной чистотой из большого множества нечистых перепутанных состояний. Первая схема такого типа была предложена в работе [49], где было показано, что она позволяет выполнить достоверную квантовую телепортацию квантовых состояний через зашумленный канал. Следующая, более эффективная схема очищения, рассматривалась в [47]. Она получила название «усиление квантовой секретности» (QPA), поскольку была разработана для криптографических целей. Было доказано, что такая схема приводит к более высокой надежности квантовой криптографии, использующей зашумленные каналы связи (основанную на той схеме перепутывания, которая рассматривалась в гл.2). В данном разделе мы опишем принципы работы QPA-схемы.

Предположим, что пары кубитов в максимально перепутанных состояниях распределяются между двумя пользователями – Алисой и Бобом – посредством зашумленного канала связи. Из-за наличия шума, присутствующего по всему каналу, распределенные пары, взаимодействующие с окружением, перепутываются с ним, теряют чистоту их собственного перепутывания и становятся смешанными состояниями. Воздействуя на принимаемые пары, Алиса и Боб хотят повысить их чистоту. Предположим, что между Алисой и Бобом распределено большое количество пар и канал влияет на все пары одинаковым образом. Будем описывать состояния пар в представлении Белла:

$$\left|\Phi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|00\right\rangle \pm \left|11\right\rangle\right) \ , \tag{8.19}$$

$$\left|\Psi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|01\right\rangle \pm \left|10\right\rangle\right) \ , \tag{8.20}$$

где $\{|0\rangle, |1\rangle\}$ являются базисом для каждой частицы, принадлежащей парам. Предположим также, что каждая пара изначально была приготовлена в состоянии $|\Phi^+\rangle$ и обозначим как $\{a, b, c, d\}$ диагональные элементы оператора плотности ρ «зашумленных» пар, которые Алиса и Боб получают в базисе $\{|\Phi^+\rangle, |\Psi^-\rangle, |\Psi^+\rangle, |\Phi^-\rangle\}$. Первый диагональный элемент $a = \langle\Phi^+|\rho|\Phi^+\rangle$, который мы назовем «качеством», представляет собой вероятность того, что пара после проверки окажется в состоянии $|\Phi^+\rangle$. Задача QPA состоит в увеличении качества до значения 1 (что подразумевает равенство нулю остальных трех диагональных элементов). Заметим, что необязательно уточнять вид всей матрицы плотности зашумленных пар, поскольку в алгоритме QPA недиагональные элементы не дают вклад при усреднении (т.е. при усреднении по ансамблю распределенных пар на каждом шаге процедуры) в эволюции диагональных элементов и, поэтому, не являются существенными для анализа эффективности схемы.

В процедуре QPA Алиса и Боб разделяют принимаемые зашумленные пары на группы, состоящие из двух пар, и выполняют над каждой группой следующие операции. Алиса выполняет унитарную операцию

$$U_A = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix} \tag{8.21}$$

над каждым из двух, имеющихся у нее кубитов; Боб выполняет обратную операцию

$$U_B = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}. \tag{8.22}$$

Заметим, что если кубиты представляют собой частицы со спином 1/2 и вычислительный базис совпадает с собственными функциями z-компонент их спинов, то эти две операции соответствуют поворотам на $\pi/2$ и $-\pi/2$ вокруг оси x.

После этого, Алиса и Боб производят две операции, требуемые при реализации квантового элемента CNOT, рассмотренного в разд.1.6:

$$\overset{\text{контроль}}{\left|x\right\rangle}\ \overset{\text{мишень}}{\left|y\right\rangle} \rightarrow \overset{\text{контроль}}{\left|x\right\rangle}\ \overset{\text{мишень}}{\left|x \oplus y\right\rangle} \quad (x,y) \in \{0,1\} \ , \tag{8.23}$$

где одна пара заключает в себе два контрольных кубита, а другая пара – два кубита-мишени. Символ $\oplus$ означает сложение по модулю два (полезную таблицу, в которой приводятся все действия такой би-

латеральной операции CNOT в базисе состояний Белла, можно найти в работе [49]). Затем, Алиса и Боб измеряют кубиты-мишени в вычислительном базисе (т.е. они измеряют z-компоненты спинов мишеней). Если в результате имеет место совпадение (т.е. оба спина направлены вверх или вниз), они сохраняют контрольную пару для следующего цикла измерений и удаляют пару-мишень. Если совпадения нет, то обе пары выводятся из цикла. Основные операции процедуры QPA последовательно показаны на рис.8.5.

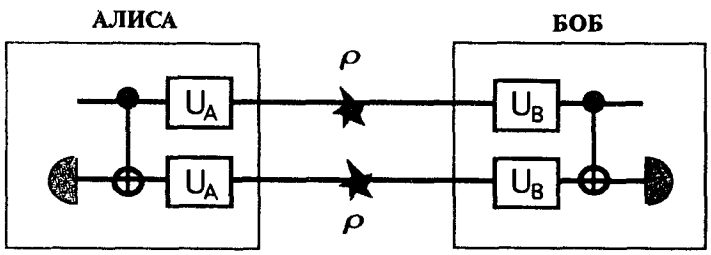


Рис.8.5. Схематичное представление одного шага QPA. Алиса выполняет операцию U_A над своей частицей и операцию «контроллируемое НЕ». Боб выполняет операцию U_B и операцию «контроллируемое НЕ». Затем, Алиса и Боб измеряют пару-мишень и сохраняют контрольную пару для следующей итерации, если их результаты совпадают.

Для получения результата действия такой процедуры, предположим, что каждая пара, изначально, находится в одном и том же состоянии с диагональными элементами $\{a, b, c, d\}$. В случае, когда контрольные кубиты оставляются, их оператор плотности будет содержать диагональные элементы $\{A, B, C, D\}$, которые при усреднении зависят *только* от диагональных элементов $\{a, b, c, d\}$:

$$A = \frac{a^2 + b^2}{p}, \tag{8.24}$$

$$B = \frac{2cd}{p}, \tag{8.25}$$

$$C = \frac{c^2 + d^2}{p}, \tag{8.26}$$

$$D = \frac{2ab}{p}, \tag{8.27}$$

где $p = (a + b)^2 + (c + d)^2$ – представляет вероятность того, что Алиса и Боб имеют совпадающие результаты при измерении пары-мишени. Уравнения (8.24-8.27) описывают элементарный шаг алгоритма QPA.

Процедура состоит в итерационном повторении элементарного шага с сохранением пар из предыдущей итерации. Заметим, что если усредненное значение «качества» близко к единице, то каждая оставленная пара должна удовлетворять требованию чистого состояния $|\Phi^+\rangle\langle\Phi^+|$.

Обращаем внимание на то обстоятельство, что если две входных пары описываются разными операторами плотности ρ и ρ' с диагональными элементами $\{a, b, c, d\}$ и $\{a', b', c', d'\}$, соответственно, то сохраняемые контрольные пары, в среднем, будут иметь диагональные элементы:

$$A = \frac{aa' + bb'}{p}, \tag{8.28}$$

$$B = \frac{c'd + cd'}{p}, \tag{8.29}$$

$$C = \frac{cc' + dd'}{p}, \tag{8.30}$$

$$D = \frac{ab' + a'b}{p}, \tag{8.31}$$

где $p = (a + b)(a' + b') + (c + d)(c' + d')$. Эти соотношения обобщают (8.24-8.27).

Можно легко проверить несколько интересных свойств процедуры QPA (8.24-8.27). Например, если на любой стадии качество a превосходит 1/2, то после следующей итерации оно также будет превосходить 1/2. Хотя качество a не обязательно монотонно возрастает как функция числа итераций, наша конечная точка $A = 1, B = C = D = 0$, является фиксированной точкой процедуры и является единственной фиксированной точкой для области $a > 1/2$. Легко можно убедиться аналитически, что это именно локальный аттрактор, т.е. что $A > a$ если a близко к 1.

Аналитическое доказательство того, что имеется также и глобальный аттрактор в области $a > 1/2$, было получено недавно в [390]. Доказательство основано на том, что функция $f(a, b) = (2a - 1)(1 - 2b)$ является монотонной функцией числа итераций и асимптотически стремится к единице. Такое утверждение подразумевает, что если мы начинаем с пар, усредненное качество которых превышает 1/2, но которые, в противном случае, находятся в произвольном состоянии, содержащем произвольные корреляции с окружением, то состояния пар, оставляемых в результате процедуры, после нескольких итераций всегда сходятся к чистому состоянию $|\Phi^+\rangle$ с единичным качеством. Мож-

но показать, что процедура QPA всегда будет успешно завершена для любых начальных значений $b > 1/2$ (т.е. будет приводить к чистому состоянию $|\Phi^+\rangle$) и для любых начальных значений $c > 1/2$ или $d > 1/2$ (т.е. будет приводить к чистому состоянию $|\Psi^+\rangle$). И наоборот, когда ни один из диагональных элементов начального оператора плотности не превосходит 1/2, процедура работать не будет.

Заметим также, что QPA пригодно для очищения набора пар, находящихся в любом состоянии ρ, среднее качество в котором, по отношению, по крайней мере, к одному из максимально перепутанных состояний (т.е. состояний Белла или состояний, полученных из состояний Белла при локальных унитарных операциях) превосходит 1/2. Это происходит из-за того, что любое состояние такого типа может быть преобразовано в $|\Phi^+\rangle$ при локальных унитарных операциях [73]. Если мы обозначим $\mathcal{B}$ класс чистых максимально перепутанных состояний (обобщенных состояний Белла), то условие того, что ρ может быть очищено принимает вид:

$$\max_{\Phi\in\mathrm{B}} \langle\Phi|\rho|\Phi\rangle > \frac{1}{2} \quad . \tag{8.32}$$

Быстродействие и сходимость процедуры зависят от значений диагональных элементов оператора плотности. В качестве примера, на рис. 8.6 показано качество, как функция начального качества и числа итераций в случаях, когда изначально $a > 1/2$ и $b = c = d$.

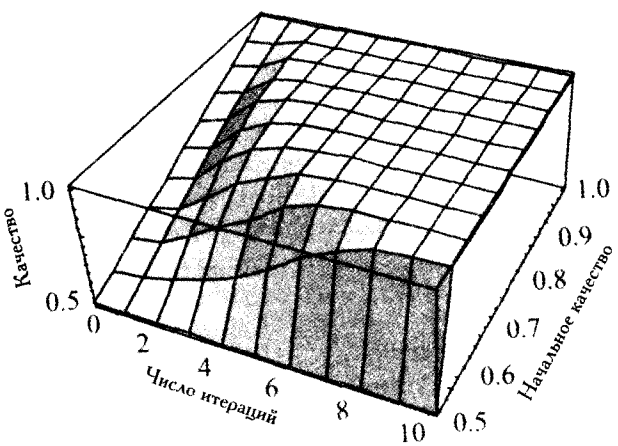


Рис.8.6. Среднее качество как функция начального качества и числа итераций для начальных состояний у которых $b = c = d$.

Процедура QPA неэкономична в терминах выведенных из нее частиц: по крайней мере половина частиц (те, которые используются в

качестве мишеней) теряются при каждой итерации. Все же эффективность этой схемы превосходит эффективность первой схемы по очищению перепутывания, рассмотренной в [49] (примерно в 1000 раз эффективнее при a близких к 0.5, т.е. число оставляемых пар в 1000 раз больше для заданной величины конечного качества).

8.5 Обобщение очищения для многочастичного перепутывания

М.Мурао, М.Б.Пленио, С.Попеску, В.Ведрал, П.Л.Найт

В этом разделе рассматриваются полные протоколы очищения, предложенные в [391], пригодные для широкого класса смешанных диагональных состояний N-частичного перепутывания. Хотя такие процедуры не являются столь общими, как при двухчастичном перепутывании, предложенном Беннетом и соавторами [49], а также Дойчем и соавторами в [47], они важны для понимания многочастичного перепутывания и имеют большое значение для различных приложений. Для многих частиц со спином 1/2, максимально перепутанные состояния имеют вид:

$$\left|\Phi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|00....0\right\rangle \pm \left|11....1\right\rangle\right) . \tag{8.33}$$

Такой же вид имеет их локальный унитарный эквивалент. Состояние каждой частицы записан в базисе $\{|0\rangle, |1\rangle\}$; в случае трех частиц они называются ГХЦ-состояниями [290].

Процедуры очищения [47, 49, 117, 382] «выделяют» из ансамбля перепутанных смешанных состояний подансамбль максимально перепутанных чистых состояний с использованием локальных операций и классических коммуникационных связей. Для двух частиц синглетное состояние $|\Psi^{-}\rangle = (|10\rangle - |01\rangle)/\sqrt{2}$, которое полностью антисимметрично, является инвариантом при любых билатеральных вращениях. Оно играет важную роль в таких схемах очищения.

Однако, для трех и более частиц, не существует перепутанного состояния, которое было бы инвариантом при три-латеральных (много-латеральных) вращениях (классификация перепутанных состояний, основанных на инвариантности при локальных преобразованиях рассмотрена в [392]). Локальные вращения переводят максимально перепутанные состояния в суперпозицию максимально перепутанных состояний (за исключением тривиальных поворотов на $n\pi$, где n – целое число). Несколько труднее оказывается преобразовать произвольное состояние в одно из состояний Вернера, что делает поиск общих протоколов по очищению гораздо менее эффективным.

Хотя и не существует максимально перепутанных состояний, инвариантных при случайных билатеральных вращениях при $N \geq 3$ (где N – число перепутанных частиц), тем не менее можно назвать состояние

$$\rho_W = x\left|\Phi^+\right\rangle\left\langle\Phi^+\right| + \frac{1-x}{2^N}\mathbf{1} \tag{8.34}$$

состоянием «типа состояния Вернера», по причине его сходства с двухчастичным случаем.

Заметим, что мы для удобства пишем $|\Phi^+\rangle$ вместо $|\Psi^-\rangle$. Цель очищения состоит в выделении подансамбля, находящегося в состоянии $|\Phi^+\rangle$. Качество

$$f = \langle\Phi^+|\rho_w|\Phi^+\rangle \tag{8.35}$$

состояния типа Вернера равно $f = x + (1-x)/2^N$. Состояния типа состояний Вернера важны на практике, поскольку смешанные перепутанные состояния возникают с большей вероятностью, когда имеется ансамбль изначально максимально перепутанных состояний (например, $|\Phi^+\rangle$) N частиц, которые передаются N участникам через зашумленные каналы (Рис.8.7).

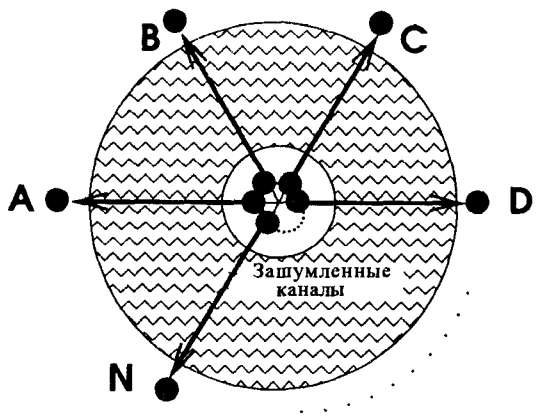


Рис.8.7. Передача N частиц, находящихся в максимально перепутанном состоянии к различным участникам (A, B, C, D,....N) через зашумленные каналы.

Рассмотрим эффект зашумленного канала, действие которого на каждую частицу сводится к случайным вращениям вокруг случайных направлений. Каждый зашумленный канал вызывает случайные вращения (вокруг случайного направления и на случайный угол) с вероятностью $(1-x)$, и оставляет частицу неизмененной с вероятностью x. Состояние после передачи через такой канал становится состоянием типа Вернера и описывается формулой (8.34).

Далее, представляется протокол (P1 + P2 см. рис.8.8), который осу-

ществляет очищение состояния типа вернеровского, при условии, что качество начального смешанного состояния выше некоторого критического значения. Преимущество такого протокола заключается в том, что могут быть непосредственно очищены состояния типа вернеровских для *любого числа частиц*.

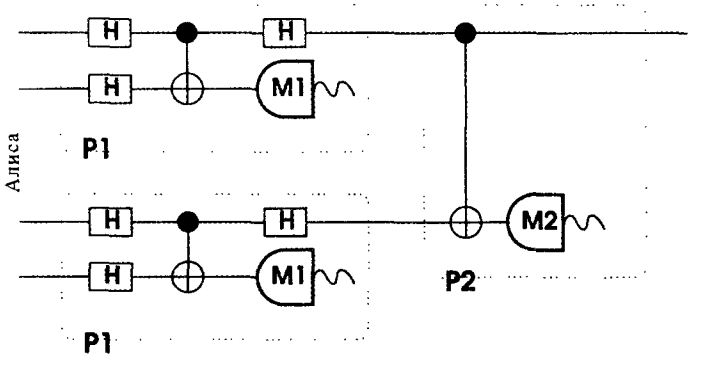


Рис. 8.8. Протокол очищения P1 + P2. H – преобразование Адамара, M1 и M2 – локальное измерение и классическое сообщение. Эта диаграмма показана для четырех частиц, принадлежащих Алисе. Боб и другие участники выполняют точно такую же процедуру.

В протоколе P1 + P2 каждая часть (Алиса, Боб и т.д.) выполняет последовательности операций P1, сопровождаемые P2 – каждый над своими частицами.

• Операция P1 заключается в локальном преобразовании Адамара, которое переводит $|0\rangle \to (|0\rangle + |1\rangle)/\sqrt{2}$, $|1\rangle \to (|0\rangle - |1\rangle)/\sqrt{2}$, локальной операции CNOT (контроллируемое HE), измерения M1 и другого преобразования Адамара. В процессе M1 сохраняются контрольные кубиты, если четное число кубитов-мишеней находятся в состоянии $|1\rangle$. В противном случае контрольные кубиты удаляются. Например, при очищении трех частиц, сохраняются только $|000\rangle$, $|101\rangle$, $|110\rangle$, $|011\rangle$.

• Операция P2 состоит из локальной операции CNOT и измерения M2, в котором сохраняются контрольные кубиты, если все кубиты-мишени при измерении оказались в том же состоянии. В противном случае контрольные кубиты удаляются. Например, при очищении трех частиц, сохраняются лишь $|000\rangle$, $|111\rangle$. При такой операции диагональные и недиагональные элементы матрицы плотности независимы друг от друга, поэтому недиагональные элементы не оказывают влияния на очищение.

Схема очищения, однако, не ограничивается только состояниями Вернера. Существует несколько типов состояний, которые могут быть очищены протоколами P1, либо P2 по отдельности. Например, если начальное смешанное состояние не имеет никакого веса в спаренном

состоянии (мы называем состояние $|\Phi^-\rangle$ «спаренным состоянием» по отношению к $|\Phi^+\rangle$), а веса других состояний равны (или распределены равномерно, когда некоторые веса равны нулю), достаточно только операции P2, чтобы очистить начальный ансамбль до состояния $|\Phi^+\rangle$ (детали см. в [39]).

В обсуждаемых выше протоколах очищения многочастичное перпутывание очищается прямым способом. Это необходимо при фундаментальном исследовании характеристик многочастичного перепутывания. Однако, можно себе представить схемы, в которых многочастичное перепутывание очищается посредством двухчастичного. В одной из таких схем для трех частиц (Алиса, Боб и Клара) используется тот факт что нам известно как очистить две частицы. Поэтому такая схема преобразует трехчастичные состояния в двухчастичные и затем очищает уже двухчастичные состояния, после чего преобразует их обратно в трехчастичные. Алгоритм такого протокола выглядит более сложным при описании на словах, поэтому мы снабдили его иллюстрацией (рис.8.9), чтобы помочь читателю представить себе схему в целом. Она состоит из следующих частей

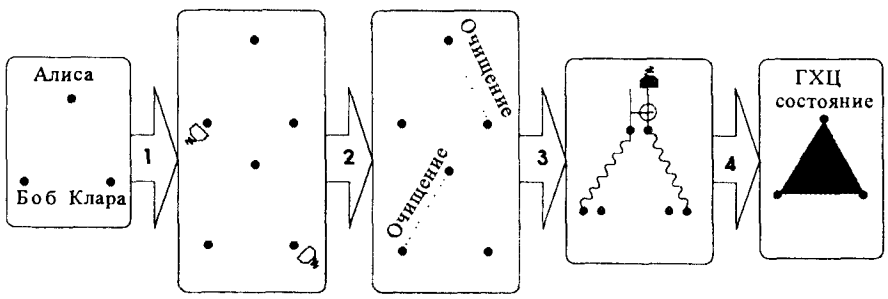


Рис.8.9 Схема очищения посредством двухчастичного очищения. Пунктирные линии изображают частичное перепутывание, а волнистые линии - максимальное перепутывание. Первые измерения (изображенные белыми детекторами) производятся в состоянии $|\chi^{\pm}\rangle \rightarrow (|0\rangle \pm |1\rangle)/\sqrt{2}$, а второе измерение (изображенное черными детекторами) – в состоянии $|0\rangle$ или $|1\rangle$.

1. Расщепление полного ансамбля состояния трех частиц на два одинаковых подансамбля.

2. Затем, Боб проектирует частицы одного подансамбля в

$$|\chi^{\pm}\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2} \ ,$$

а Клара выполняет такое же проектирование, используя другой подансамбль. Когда Боб и Клара получают проекцию в $|\chi^-\rangle$, они дают команду Алисе выполнить операцию σ_z над ее частицами. Если Боб и

Клара получают проекцию $|\chi^+\rangle$, то Алиса, по их команде, не делает ничего. Конечный результат этих операций – два подансамбля двухчастичных состояний (одна пара распределена между Алисой и Бобом, а другая – между Алисой и Кларой).

3. После этого, Алиса и Боб и, отдельно Алиса с Кларой, осуществляют протокол по двухчастичному очищению [47, 117], в отношении каждого из перепутанных подансамблей двух частиц. Это приводит к двум максимально перепутанным ансамблям пар частиц, распределенных между Алисой и Бобом, а также между Алисой и Кларой.

4. Теперь Алиса хочет получить единое ГХЦ-состояние, составленное из двух максимально перепутанных пар, распределенных между нею и Бобом, и Бобом и Кларой. Для достижения этой цели она выбирает одну перепутанную пару из каждого подансамбля и выполняет операцию CNOT над своими частицами. Затем она проицируют частицу-мишень в $|0\rangle$ или в $|1\rangle$. Если после действий Алисы частица оказалась в $|1\rangle$, то она командует Кларе выполнить операцию σ_z над ее частицей. В другом случае, Клара не делает ничего. Таким образом, получается подансамбль, содержащий максимально перепутанное ГХЦ-состояние [300, 303].

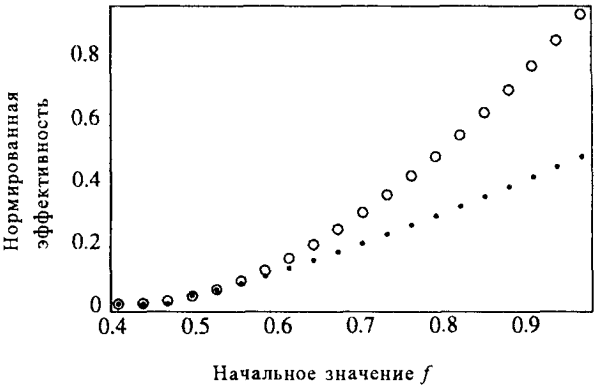


Рис.8.10. Нормированная эффективность очищения состояний типа вернеровских для трех частиц как функция начального качества f. Кружочки получены численно при использовании протокола очищения P1 + P2 с выбранной точностью 10^{-7}. Точки получены при использовании схемы очищения посредством двухчастичного очищения с такой же точностью.

Теперь проанализируем такую непрямую схему и сравним ее с прямыми способами очищения. Любая эффективная прямая схема трехчастичного очищения должна работать лучше, чем такой непрямой метод, использующий две частицы. Заметим, что в этой схеме мы получили только *одно* максимально перепутанное состояние трех частиц из *двух* максимально перепутанных состояний двух частиц

(Рис.8.10, подробнее см.[391]). Для очищения N-частичных перепутанных состояний мы берем одно максимально перепутанное состояние из $N-1$ максимально перепутанных состояний двух частиц. Добавим, что число двух-кубитовых операций CNOT, каждую из которых практически трудно реализовать с высокой точностью, здесь больше, чем в нашей прямой схеме. Такого рода «неэффективность» является основным практическим недостатком двухчастичной схемы.

При двухчастичном перепутывании начального качества $f > 1/2$ оказывается достаточно для успешного очищения [47], если мы ничего не знаем о входном состоянии. Ситуация меняется, если у нас есть дополнительная информация об этом состоянии. В этом случае любое перепутанное состояние может быть очищено [50]. Однако, достаточное условие не является таким простым в случае более чем трех частиц. Нами было найдено несколько критериев, зависящих от типа смешанных состояний.

Для состояний вернеровского типа в форме

$$\rho_W = x\left|\Phi^+\right\rangle\left\langle\Phi^+\right| + \frac{1-x}{2^N}\mathbf{1}$$

и очищению по протоколу P1 + P2 мы численно получили результаты, представленные в таблице 8.1.

Таблица 8.1. A: Наблюдаемый предел качества очищенных начальных состояний для N частиц состояний вернеровского типа в прямом протоколе P1 + P2, B: теоретический предел качества в непрямой схеме очищения посредством двухчастичного очищения, C: теоретическое минимальное качество, достаточное для очищения.

N	A	B	C
2	$f \geq 0.5395$	$f > 1/2 = 0.5$	$f > 1/2$
3	$f \geq 0.4073$	$f > 5/12 \approx 0.4167$	неизвестно
4	$f \geq 0.313$	$f > 3/8 = 0.375$	неизвестно
5	$f \geq 0.245$	$f > 17/48 \approx 0.3542$	неизвестно
6	$f \geq 0.20$	$f > 11/32 \approx 0.3438$	неизвестно

Теоретическое предельное качество для состояний вернеровского типа ρ_w в схеме двухчастичного очищения определяется условием, что качество f_r редуцированных двухчастичных состояний должно удовлетворять неравенству $f_r > 1/2$. Например, для трех частиц, состояние Вернера, имеющее начальное качество $f = x + (1-x)/8$, при измерении Боба и Клары редуцируется к двухчастичному состоянию:

$$\rho_r = x\left|\Phi^+\right\rangle\left\langle\Phi^+\right| + \frac{1-x}{4}\mathbf{1} \,. \tag{8.36}$$

Качество редуцированного двухчастичного состояния теперь $f_r = (1 + 6f)/7$. Для четырех частиц, мы имеем $f_r = (1 + 4f)/5$, для пяти частиц – $f_r = (7 + 24f)/31$, для шести – $f_r = (5 + 16f)/21$ и т.д. Из табл.8.1 видно, что протокол P1 + P2 не оптимален для двух частиц. Поэтому, он может оказаться неоптимальным и для $N > 2$. Однако для более чем трех частиц, наш предел оказывается ниже, чем предел, полученный в схеме очищения посредством двухчастичного очищения.

Для состояний, не содержащих веса при $|\Phi^-\rangle\langle\Phi^-|$, и содержащих равные веса при всех других состояниях, кроме $|\Phi^+\rangle\langle\Phi^+|$, предел качества очищения в протоколе P2 составляет $f > 2^{-(N-1)}$. Предел качества, полученный в схеме очищения посредством двухчастичного очищения, оказывается 2/5 = 0.4 в трехчастичном случае, 65/23 ≈ 0.35846 в четырехчастичном случае, 125/377 ≈ 0.328912 для пяти частиц и т.д., т.е. хуже, чем в наших протоколах.

Как мы видим, предел качества очищаемых начальных состояний зависит от распределения весов других диагональных состояний. Это условие другого рода, по отношению к случаю двух частиц [47]. Для двух частиц распределение весов других диагональных элементов, в основном, было не существенно для очищения, поскольку любое распределение весов других диагональных элементов может быть преобразовано в четное распределение при случайных локальных вращениях обеих частиц, без изменения величины перепутывания. Это указывает на то, что могут найтись дополнительные образования многочастичных перепутанных смешанных состояний, которые не существуют для двухчастичных смешанных состояний.

8.6 Квантовые сети II: Связь через зашумленные каналы

Х.-Дж.Бригель, У.Дюр, У.Дж. ван-Энк, Дж.И.Цирак, П.Коллер

Мы покажем, каким образом можно создать перепутанные ЭПР-пары между пространственно удаленными атомами, каждый из которых находится внутри высоко-добротного оптического резонатора. Они обмениваются фотонами, в общем случае через зашумленный канал, например, по обычному оптическому волокну. Схема коррекции ошибок, которая использует несколько вспомогательных атомов в каждом резонаторе, эффективно убирает поглощение фотонов и другие ошибки, возникающие при передаче. При осуществлении связи на расстояниях во много раз превышающих длину поглощения или длину когерентности канала, мы рассмотрим новый протокол очи-

щения, который реализует аналог повторителя в классических системах связи.

8.6.1 Введение

В этом разделе будут развиты и обобщены идеи, рассмотренные в разд.6.2., будет предложена реализация квантовой сети [278], использующей долгоживущие состояния атомов – в качестве физической основы для хранения кубитов, и фотонов, как способа передачи этих кубитов от одного атома к другому. Для осуществления контролируемой передачи кубитов, атомы заключены в высокодобротные оптические резонаторы, которые соединены оптическим волокном, как показано на Рис.6.1.

Составные системы атом-волокно, вместе с лазерными импульсами, образуют то, что мы называем *зашумленный квантовый канал* связи, см. Рис.8.11. Когда фотоны распространяются через оптические волокна, поглощение является превалирующей ошибкой при передаче информации. Потери возникают также и при некогерентном рассеянии на поверхностях резонаторных зеркал и в местах соединений между резонаторами и волокном. Другой характерный источник ошибок вызван несовершенством лазерных импульсов, используемых для рамановских переходов. Примером ошибки, возникающей в локальном ЛЭ, служит спонтанное излучение одного из атомов во время работы этого ЛЭ.

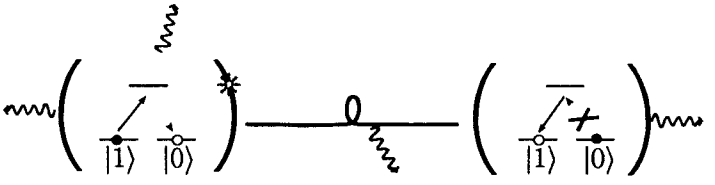


Рис.8.11. Зашумленный фотонный канал: Типичные ошибки, возникающие при передаче, включающие поглощение фотонов, некогерентное рассеяние и несовершенные рамановские переходы.

В данном разделе показано, как можно осуществить высококачественную связь даже в присутствии ошибок, вызванных потерями или шумом и как можно бороться с эффектами декогерентности. Прежде всего, мы кратко напомним аргументацию, приведенную в разд.6.2, которая дает возможность ввести читателя в терминологию коррекции ошибок и квантовой теории информации. В разд.8.6.3 и 8.6.4 мы сконцентрируемся на ошибках, возникающих при передаче фотонов и покажем как их можно обнаружить и исправить [393-395]. Для этого

мы предположим, что операции локальных ЛЭ и соответствующие измерения могут быть выполнены без ошибок. В разд.8.7 мы освободимся от этого допущения и рассмотрим *несовершенные* операции, выполняемые как локально, так и при передачах. Такой подход отражает общую ситуацию, когда мы использовали все способы коррекции ошибок, но не можем исключить вероятность того, что некоторые ошибки не были учтены и, таким образом, не исправлены. Или, когда используемые операции и измерения, в некоторых случаях, не являются точными. В таком общем контексте мы исследуем важную проблему «дальней» связи и использование квантовых повторителей [381, 387].

С формальной точки зрения выгодно представить квантовую связь, как проблему приготовления дальнодействующих квантовых корреляций, распределенных по каналу связи, вместо непосредственного распространения через канал неизвестного кубита. Как только создается ЭПР-пара, она *может* быть использована для телепортации [74], которая представляет собой реальную передачу информации, а также и в других целях, таких как распределение секретных ключей для квантовой криптографии [46]. Следует отметить, что такой подход отличается от квантового вычисления в том смысле, что до тех пор, пока не будет установлена ЭПР-корреляция, никакой реальной информации воспроизвести нельзя. Все, что действительно нужно сделать – это установить нелокальные квантовые корреляции, которые позже могут быть использованы в целях передачи информации. На самом деле, в этот более поздний момент, уже отпадает необходимость существования канала связи.

Предмет обсуждения этого раздела, поэтому, состоит в поиске ответа на вопрос: как приготовить ЭПР-пару между двумя участниками A и B при помощи зашумленного канала произвольной длины l, который соединяет A и B.

8.6.2 Идеальная связь

В идеальном случае схема, показанная на рис. 6.2, реализует следующую передачу:

$$\left[\alpha|0\rangle_A+\beta|1\rangle_A\right]|0\rangle_B \rightarrow |0\rangle_A\left[\alpha|0\rangle_B+\beta|1\rangle_B\right] , \qquad (8.37)$$

где неизвестная суперпозиция состояний $|0\rangle = |e\rangle$ и $|1\rangle = |g\rangle$ атома в первом резонаторе передается атому B во втором резонаторе, см. Рис.8.12. Резонаторы могут составлять часть большей сети, поэтому мы часто будем обращаться к ним, как к узлу A и узлу B, соответственно. Выбранные внутренние состояния $|0\rangle$ и $|1\rangle$ атомов определяют, на языке теории квантовой информации, вычислительный базис для кубита.

Важно, чтобы атом A был перепутан с другими атомами, находящимися в том же резонаторе, или с другими узлами сети. В такой ситуации коэффициенты α и β в (8.37) не являются больше комплексными числами, а обозначают ненормированные состояния других атомов. Таким образом, передача (8.37) может быть использована при переносе состояний единичного атома, а также для переноса *перепутывания*. Например, если начать с состояний отдельных частиц, ЭПР-пару можно приготовить в двухступенчатом процессе:

$$\left[\alpha|0\rangle_A+\beta|1\rangle_A\right]|0\rangle_{A_2}|0\rangle_B \rightarrow \left[\alpha|0\rangle_{A_2}|0\rangle_A+\beta|1\rangle_{A_2}|1\rangle_A\right]|0\rangle_B$$

$$\rightarrow |0\rangle_{A_2}\left[\alpha|0\rangle_A|0\rangle_B+\beta|1\rangle_A|1\rangle_B\right]. \qquad (8.38)$$

Здесь первая стрелка относится к *локальной* операции CNOT между атомами A и A_2 в первом резонаторе. Вторая стрелка преобразует состояние A_2 в B, перенося, таким образом, перепутывание между атомами A и A_2 на атомы A и B. В конце этого составного преобразования состояние вспомогательного атома A_2 оказывается таким же, как и было до преобразования и ни на что не влияет. При $\alpha=\beta$ приготавливается идеальная ЭПР-пара.

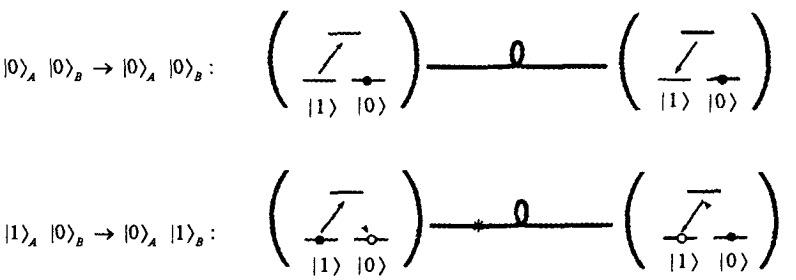


Рис.8.12. Обмен состояниями атома между узлами A и B. Когда атом в узле A находится в состоянии $|1\rangle_A$, может быть использована последовательность рамановских переходов, рассмотренных в разд.6.2, для обмена его состояния с состоянием атома, находящемся в узле B в процессе передачи фотонов. Когда атом A находится в состоянии $|0\rangle_A$, рамановский импульс не изменяет состояние. Суперпозиция состояний $|0\rangle_A$ и $|1\rangle_A$, таким образом, передается к узлу B в соответствие с (8.38).

8.6.3 *Исправление ошибок, возникающих при передачах: фотонный канал*

В реалистичной модели мы должны рассматривать возможность того, что передача атомного состояния от резонатора A к резонатору B не является совершенной. Существует определенная вероятность, что атом в B не будет возбужден, даже когда атом в A уже находится в

возбужденном состоянии. Это происходит из-за взаимодействия составной системы атом-резонатор-волокно с окружением, которое, даже если оно мало, все равно, в принципе, существует. Результат взаимодействия заключается в установлении перепутывания между состояниями атома в (8.37) и окружением, т.е. стенками резонатора, волокна и полем излучения свободного пространства.

Далее, мы будем предполагать, что фотоны в канале могут поглощаться, но не могут рождаться. Это служит хорошим приближением для оптических фотонов, поскольку среднее число тепловых фотонов в резонаторе и в волокне пренебрежимо мало. В такой ситуации, наиболее общее выражение для несовершенной операции передачи имеет вид:

$$|0\rangle_A|0\rangle_B|E\rangle \to |0\rangle_A|0\rangle_B|E_0\rangle ,$$

$$|1\rangle_A|0\rangle_B|E\rangle \to |0\rangle_A|1\rangle_B|E_1\rangle + |0\rangle_A|0\rangle_B|E_a\rangle \quad , \tag{8.39}$$

где $|E\rangle$, $|E_0\rangle$,... обозначают ненормированные состояния внешнего окружения. Здесь используется некий прием, когда записывают, что $|E_0\rangle = \tau_0|E\rangle$, $|E_1\rangle = \tau_1|E\rangle$, $|E_a\rangle = \tau_a|E\rangle$, вводя таким образом, операторы, перепутывающие систему с внешним окружением. Учитывая такие обозначения, выражение (8.39) может быть представлено в компактном виде[9]:

$$|0\rangle_A|0\rangle_B \to |0\rangle_A|0\rangle_B\tau_0 \quad ,$$

$$|1\rangle_A|0\rangle_B \to |0\rangle_A|1\rangle_B\tau_1 + |0\rangle_A|0\rangle_B\tau_a \quad , \tag{8.40}$$

что и служит определением фотонного канала [394].

Оптические резонаторы вместе с волокном образуют составную оптическую систему с определенной резонансной структурой, которая определяет спектр ее квази-мод, постоянных релаксации и проч. В особом случае, когда существенно только поглощение фотонов, операторы в (8.40) имеют простой вид. На оптических частотах, состояние окружения может быть хорошо аппроксимировано вакуумным состоянием, поэтому можно считать, что $\tau_0 = 1$, $\tau_1 = \alpha(\tau) \sim e^{-k\tau}$, $\tau_a = \Sigma_j\beta_j(\tau)b^\dagger_j$ когда $\Sigma_j|\beta_j(\tau)|^2 \sim 1 - e^{-2k\tau}$ и, где κ постоянная затухания общей системы (атом) резонатор – волокно, τ – время передачи. Операторы $b^\dagger_j$, b_j – это амплитудные операторы j-ой колебательной моды окружения.

В более общем случае операторы $\tau_{0,1,\alpha}$ в (8.10) могут описывать и процессы спонтанного испускания, поглощения фотонов, а также переходы между другими внутренними состояниями атомов. Таким об-

[9] Понятно, что в выражениях такого типа и правая, и левая части действуют на данное состояние внешнего окружения. Использование компактного обозначения сохраняет выражение в гораздо более наглядном виде, в то время когда исследуются более сложные приложения канала связи.

разом, все сложные физические процессы заключены в этих трех операторах. В таком общем (нестационарном) случае необходимо принимать во внимание и временную зависимость тех членов, которые описывают внешнее окружение. Следовательно, операторы $\tau_{0,1,a}$ зависят от начального времени, в которое начинается передача. Как следствие, в (8.40) становится существенным упорядочивание операторов во времени, т.е. $\tau_1(t_1)\tau_0(t_0) \neq \tau_0(t_1)\tau_1(t_0)$.

При использовании (8.40) для создания ЭПР-пары, как и в (8.38) мы получаем:

$$\left[\alpha|0\rangle_A + \beta|1\rangle_A\right]|0\rangle_B \rightarrow \left[\alpha|0\rangle_A|0\rangle_B\tau_0 + \beta|1\rangle_A|1\rangle_B\tau_1\right] + \beta|1\rangle_A|0\rangle_B\tau_a \,. \tag{8.41}$$

При $\alpha = \beta$ это выражение может быть записано в виде[10]:

$$\left|\Phi^+_{AB}\right\rangle\left[\tau_0+\tau_1\right] + \left|\Phi^-_{AB}\right\rangle\left[\tau_0-\tau_1\right] + \left(\left|\Psi^+_{AB}\right\rangle + \left|\Psi^-_{AB}\right\rangle\right)\tau_a \,, \tag{8.42}$$

где мы используем белловский базис

$$\left|\Phi^\pm_{AB}\right\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B \pm |1\rangle_A|1\rangle_B\right), \quad \left|\Psi^\pm_{AB}\right\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A|1\rangle_B \pm |1\rangle_A|0\rangle_B\right).$$

Качество конечной пары (8.42) может быть определено как степень перекрытия ее состояния с идеальным состоянием $|\Phi^+_{AB}\rangle$. Такое перекрытие дается нормой:

$$F = \left\| \frac{\left[\tau_0+\tau_1\right]|E\rangle}{2} \right\|^2 \sim \left| \frac{1+e^{-k\tau}}{2} \right|^2 . \tag{8.43}$$

Оценка F во втором члене показывает, насколько связь мод системы резонатор-волокно с внешним окружением уменьшает достижимое качество ЭПР-пары. В частности, F падает экспоненциально при увеличении времени передачи и длины волокна.

Для того, чтобы приготовить ЭПР-пары на расстояниях сравнимых или превышающих длину поглощения фотонного канала, нам нужно найти метод *детектирования и коррекции* фотонных потерь, которые могут иметь место при передаче. Вообще говоря, нам нужно уничтожить член, связанный с поглощением τ_a в (8.42) и минимизировать другой член $\tau_0 - \tau_1$.

В последующем, мы рассмотрим метод, который использует один или пару вспомогательных атомов, находящихся в каждом резонаторе. При этом мы выделим только наиболее существенные этапы. Для

[10] Повсюду в данном разделе мы пренебрегаем нормировочными коэффициентами там, где без них можно обойтись.

уточнения деталей читатель может обратиться к работам [393-395].

8.6.4 Очищение с помощью ограниченных средств

Основная идея состоит в перепутывании атома первого резонатора со вспомогательными (запасными) атомами до передачи информации. Эта процедура напоминает схему излишнего кодирования; фундаментальное отличие заключается в том, что наша схема позволяет исправлять ошибки *во всех порядках* вероятности поглощения света. Измеряя определенное совместное состояние двух атомов в принимающем резонаторе, можно зарегистрировать фотонные потери при одновременном сохранении уровня начальной когерентности передаваемого атомного состояния. Поэтому процесс передачи может повторяться так часто, как это необходимо, до тех пор, пока не будет зарегистрирована ошибка.

Говоря более подробно, такой процесс включает три этапа.

(1) Кодировка состояния атома в трех-частичном перепутанном состоянии

$$\alpha|0\rangle_A+\beta|1\rangle_A \to \alpha\left[|0\rangle_A|0\rangle_{A_2}|0\rangle_{A_3}+|1\rangle_A|1\rangle_{A_2}|1\rangle_{A_3}\right] \qquad (8.44)$$

$$+\beta\left[|0\rangle_A|0\rangle_{A_2}|1\rangle_{A_3}+|1\rangle_A|1\rangle_{A_2}|0\rangle_{A_3}\right] .$$

Такая кодировка может быть реализована путем действия двух операций CNOT между A_3 и A, а также A и A_2, соответственно.

(2) *Двукратная передача* фотона, используя (8.40), между атомами A_2 и B_2, а также A_2 и B и действия локальной операции сброса атома A между двумя актами передачи. В результате образуется многочастичное перепутанное состояние [395], вид которого мы здесь не приводим.

(3) Измерение состояния некоторых вспомогательных атомов в обоих резонаторах. В сочетании с подходящим локальным унитарным преобразованием, получается один из двух результатов.

Действие такой процедуры можно свести к созданию следующего свободного от поглощения (т.е. исправляющего) канала

$$\left[\alpha|0\rangle_A+\beta|1\rangle_A\right]|0\rangle_B \to \alpha|0\rangle_A|0\rangle_B\,\mathcal{S}_0+\beta 1_A|1\rangle_B\,\mathcal{S}_1$$

$$\searrow \text{ошибка} \qquad \left[\alpha|0\rangle_A+\beta|1\rangle_A\right]|0\rangle_B\,\mathcal{S}_a \ . \qquad (8.45)$$

Возникающие в результате процесса двойной передачи, операторы $\mathcal{S}$, стоящие в (8.45), являются произведениями операторов τ, т.е. $\mathcal{S}_0=\tau_0\tau_1$, $\mathcal{S}_0=\tau_1\tau_0$, или в другом порядке. Важно отметить, что в зависимости от результатов измерения на этапе (3), возможно два исхода.

Если детектируется ошибка, состояние проицируется во вторую строчку (8.45) и передача может быть повторена; если же ошибка не была зарегистрирована, то состояние проицируется в первую строчку (8.45), что закрывает канал связи.

При использовании (8.45) вместо (8.40) получается

$$\left[|0\rangle_A+|1\rangle_A\right]|0\rangle_B \to |0\rangle_A|0\rangle_B \mathcal{S}_0+|1\rangle_A|1\rangle_B \mathcal{S}_1$$

$$=\left|\Phi^+_{AB}\right\rangle\frac{1}{2}[\mathcal{S}_0+\mathcal{S}_1]+\left|\Phi^-_{AB}\right\rangle\frac{1}{2}[\mathcal{S}_0-\mathcal{S}_1] \quad . \qquad (8.46)$$

Для простого примера, разобранного после (8.40), когда $\tau_0 = 1$ и $\tau_1 = e^{-k\tau}$, получаем $\mathcal{S}_0 = e^{-k\tau}$ и $\mathcal{S}_1 = e^{-k\tau}$; таким образом второй член в (8.46) исчезает. В такой ситуации возникает идеальная ЭПР-пара после однократного использования канала (8.45). Это отвечает среднему числу световых передач $e^{2k\tau}$.

В более общем случае, похожий результат может быть получен, когда состояние окружения не зависит от упорядочивания во времени операторов τ_0 и τ_1. Такое *стационарное окружение* определяется условием $\tau_1(t_1)\tau_0(t_0)|E\rangle = \tau_0(t_1)\tau_1(t_0)|E\rangle$, т.е. $\mathcal{S}_0|E\rangle = \mathcal{S}_1|E\rangle$. Для любой системы со стационарным окружением, идеальная ЭПР-пара приготавливается при единичном применении (8.45).

При обсуждении общего нестационарного случая прежде всего перепишем результат (8.46) в виде:

$$\left|\Psi^{(1)}\right\rangle=\left|\Phi^+_{AB}\right\rangle\left|E^{(1)}_+\right\rangle+\left|\Phi^-_{AB}\right\rangle\left|E^{(1)}_-\right\rangle , \qquad (8.47)$$

где $|E^{(1)}_\pm\rangle = 1/2(\mathcal{S}_0 \pm \mathcal{S}_1)|E\rangle$. Норма (квадрат) окружения $|E^{(1)}_\pm\rangle$ определяет качество пары.

В этот момент, в игру вступает ключевое преимущество канала, свободного от поглощения (AFC), а именно то, что он исправляет ошибки в процессе передачи, в то же время поддерживая когерентность и возможное перепутывание состояния, к которому он применяется. Это дает возможность повторно использовать протокол очищения [394]. На каждом шаге очищения пара временно перепутывается с двумя вспомогательными атомами, каждый из которых находится в своем узле, при использовании и локальных операций CNOT, и AFC. В некотором смысле, при этом создается вспомогательная ЭПР-пара, что используется при очищении (8.47). Детальный протокол схематично показан на Рис.8.13*а*.

Этот протокол преобразует (8.47) в последовательность состояний вида

$$\left|\Psi^{(N)}\right\rangle=\left|\Phi^+_{AB}\right\rangle\left|E^{(N)}_+\right\rangle+\left|\Phi^-_{AB}\right\rangle\left|E^{(N)}_-\right\rangle , \qquad (8.48)$$

где либо

$$\left|E_{\pm}^{(N)}\right\rangle = \frac{1}{2}\left(\mathcal{S} \pm \mathcal{S}\right)\left|E_{\pm}^{(N-1)}\right\rangle \text{, либо } \left|E_{\pm}^{(N)}\right\rangle = \frac{1}{2}\left(\mathcal{S} \mp \mathcal{S}\right)\left|E_{\pm}^{(N-1)}\right\rangle \quad ,$$

в зависимости от результата измерения. В первом случае, который имеет место с вероятностью $P_{up} = P_{up}^{(N)}$, качество пары увеличивается. Во втором случае, происходящем с вероятностью $P_{down} = 1 - P_{up}$, качество уменьшается. Можно показать, что в результате возникает стохастический процесс, соответствующий одностороннему процессу блужданий, как показано на Рис.8.13*b*. В среднем, качество $F_N = \langle E_+^{(N)} | E_+^{(N)} \rangle$ сходится к единице экспоненциально быстро с ростом числа шагов очищения.

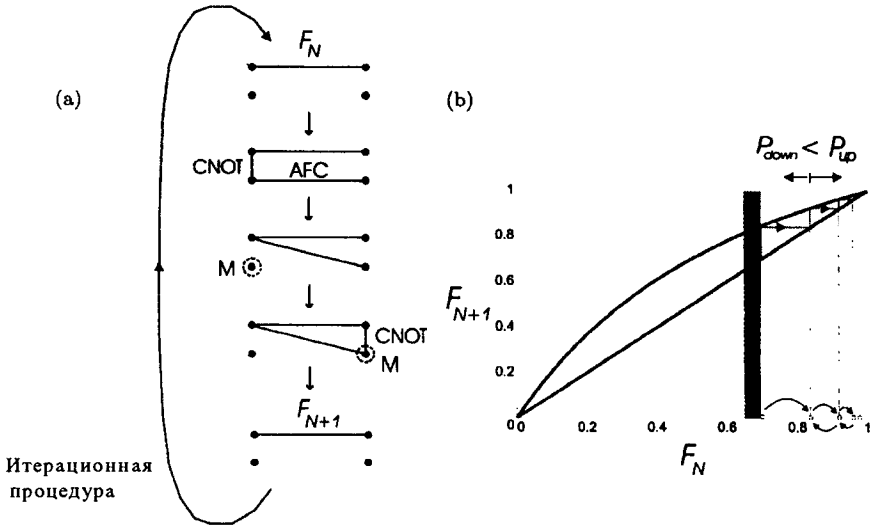


Рис.8.13 Очищение ЭПР-пары с помощью ограниченных средств. (*a*) – протокол повторного очищения. На каждом шаге очищения ЭПР-пара в виде (8.48) с качеством F_N временно перепутывается с двумя вспомогательными атомами. Это происходит при воздействии двух операций CNOT, использовании канала, свободного от поглощения (AFC) и измерений M. К тому же применяются некие преобразования Адамара, не показанные на рисунке. Значение нового качества F_{N+1} зависит от результата измерений M, как объясняется в (*b*). Заметим, что подобная схема имеет дело с одним и тем же набором атомов на каждом шаге, и следовательно реализует «процесс самоочищения». (*b*) – односторонний случайный процесс блуждания для качества. После каждого шага итерации в (*a*) качество F_N возрастает (уменьшается) с определенной вероятностью P_{up} (P_{down}), которая зависит от N. Если F_N падает ниже начального значения F_0, мы устанавливаем пару к этому значению качества при однократном использовании канала AFC, как в (8.46). Это эквивалентно одностороннему процессу блуждания с отражениями от нижнего барьера F_0, как показано на рисунке. Поэтому, в среднем, качество приближается к единице экспоненциально быстро, $F_N \sim 1 - e^{-const \cdot xN}$

8.7 Квантовые повторители

Используя методы, рассмотренные в предыдущих разделах, возможно приготовить ЭПР-пару высокого качества при посылке единичных фотонов через диссипативный и зашумленный канал, который соединяет атомы. Однако, в этом методе имеется некое ограничение, возникающее, когда время передачи через канал становится намного больше, чем время релаксации, т.е. когда $k\tau >> 1$. Вероятность поглощения растет экспоненциально с ростом τ, также ведет себя и число повторений, требуемых для одной успешной передачи.

Потери за счет поглощения – хорошо известная проблема, возникающая при передаче электрического сигнала через классические каналы. Для ее решения через регулярные промежутки в канал вводятся повторители. В классической (цифровой) технике такие повторители используют и для усиления, и для восстановления сигнала. Расстояние между повторителями определяется скоростью затухания в волокне и скоростью передачи битов (дисперсионными эффектами).

Для квантовой связи мы не можем использовать повторители. Для построения ЭПР-корреляций нужно передавать единичные кубиты, а они не могут быть усилены [88, 396] без разрушения квантовых корреляций. Все, что мы можем здесь сделать – это зарегистрировать, поглотился ли фотон и, в таком случае, повторить передачу.

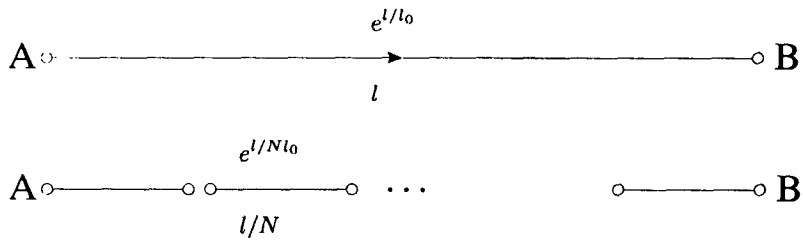


Рис.8.14. Простое и составное волокно для передачи единичных кубитов от A к B. Как и в классических повторителях, для передачи единичных кубитов на большие расстояния, мы делим волокно (канал) на несколько сегментов, на концах которых измеряются ошибки.

Для последующего обсуждения предположим, что превалирующей ошибкой передачи является поглощение фотонов и, что окружение стационарно. Этот случай отвечает фотонному каналу (8.40) с $\tau_0 = 1$ и $\tau_1 = e^{-k\tau} = e^{-l/2l_0}$, где $l_0 = c/2k$ определяет эффективную полу-длину волокна. Вероятность успешной передачи кубита от A к B, как показано на Рис.8.14(вверху) становится $p(l) = e^{-l/l_0}$, где l – длина волокна. Следовательно, среднее число требуемых повторений равно

$$n(l) = \frac{1}{p(l)} = e^{l/l_0} \ . \tag{8.49}$$

Ясно, что такой результат приводит к нереально высоким значениям для любого эксперимента, в котором волокно существенно длиннее, чем несколько полу-длин l_0.

Следуя идее использования повторителей в классической связи мы разделим канал на определенное число N сегментов, содержащих в точках соединений узлы. В узлах происходит измерение того, произошла ли ошибка передачи (см.рис.8.14 (внизу)). Это можно сделать также, как и в методе, рассмотренном в разд.5.2, при использовании нескольких дополнительных ионов, помещенных в резонатор. Если регистрируется ошибка, вызванная поглощением, передача через этот сегмент повторяется. Затем, фотон посылается через следующий сегмент и т.д. Таким образом, в идеале, состояние атома в узле A передается от одной точки к другой, пока оно не достигнет узла B. Среднее полное число повторений, приходящееся на каждый сегмент, равно $n(l/N) = e^{l/l_0 N}$. Соответственно, полное число передач, требуемых для успешного прохождения кубита через *составное волокно* будет равно

$$n_{составн.} = \frac{N}{p\left(\frac{l}{N}\right)} = Ne^{l/Nl_0} \ . \tag{8.50}$$

Это выражение следует сравнивать с (8.49). Составное волокно, таким образом, выглядит предпочтительнее простого волокна, когда

$$Ne^{l/Nl_0} < e^{l/l_0} \ . \tag{8.51}$$

Оптимальное число сегментов дается фактором N, который минимизирует левую часть приведенного выше уравнения, т.е. $N \equiv N_{\min}$, или

$$n_{\min} = N_{\min} e^{l/N_{\min} l_0} = l/l_0 e^1 \ . \tag{8.52}$$

Такая ситуация реализуется, когда точки соединений размещены вдоль волокна на расстояниях, соответствующих эффективной полудлине волокна l_0.

Вплоть до этого момента, мы полагали, что локальные операции могут быть выполнены без ошибок. Действительно, существуют схемы [397], которые позволяют детектировать ошибки и исправлять локальные двух-битовые операции. Однако, даже при использовании таких методов, имеется вероятность возникновения такой ошибки, которая не будет зарегистрирована, т.к. механизм регистрации сам по себе использует одно-битовые операции и измерения, которые могут и не быть совершенными. Это ведет к двум эффектам: (1) локальные опе-

рации в каждой контрольной точке на Рис.8.14 (внизу) становятся причиной некоего шума, возникающего в процессе передачи; (2) качество передачи через каждый сегмент уже является ограниченным некоторым максимальным значением F_{max}. Это ясно из того факта, что и поглощение в свободном канале, и протокол очищения на Рис.8.13а включают локальные операции, которые становятся источниками шума и, отсюда, ограничивают максимальное достижимое качество. Оба этих эффекта нарастают (экспоненциально) с числом контрольных точек и в конечном счете полностью разрушают качество передачи.

Рис.8.15. Соединение последовательности N ЭПР-пар, см. текст.

Чтобы прояснить этот момент, рассмотрим следующую эквивалентную задачу. Сначала мы приготовим N элементарных ЭПР-пар с качеством $F_1 < F_{max}$ и распределим их между узлами $A\&C_1$, $C_1\&C_2$,...$C_{N-1}\&B$, как показано на Рис. 8.15. Затем, объединим эти пары с помощью выполнения измерений состояний Белла в узлах C_i и классическим образом распределим результаты так же, как и в схемах по телепортации [74] и обмену перепутывания [74, 398]. В результате отдельная ЭПР-пара окажется распределенной между конечными точками A и B (рис.8.15). К сожалению, в каждом соединении качество результирующей пары будет уменьшаться, поскольку процесс соединения заключает в себе несовершенные операции и является причиной возникновения шума. К тому же, даже при идеальных соединениях, качество уменьшается: соединение, например, двух состояний Вернера с качеством F_1 при измерении состояний Белла, дает новое состояние Вернера с качеством

$$F_2 = \frac{1}{4}\left\{1+3\left(\frac{4F-1}{3}\right)^2\right\}, \qquad (8.53)$$

так, что $F_2 \sim F_1^2$ для $F_1 \sim 1$. Оба эффекта накапливаются с каждым новым соединением и приводят к экспоненциальному уменьшению качества F_N конечной пары, распределенной между A и B, с ростом N. В итоге, величина F_N падает ниже определенного порогового уровня $F_{min} \geq 1/2$, т.е. состояние, в принципе, не может быть очищено. Это означает, что качество нельзя увеличить методами очищения [47, 49].

Таким образом, разбивая канал на более короткие сегменты, удается ликвидировать эффект экспоненциального увеличения числа повторных передач, ценой введения экспоненциального уменьшения качества!

Возможность уйти от этого ограничения состоит в соединении меньшего числа $L << N$ пар, так, чтобы $F_L > F_{min}$, когда очищение станет возможно. Идея заключается в соединении результирующих пар и продолжения действий в таком же ключе. Метод, в котором выполняются чередующиеся последовательности соединений и очищений, должен быть реализован так, чтобы количество требуемых затрат не росло экспоненциально с ростом N и, таким образом, с ростом l.

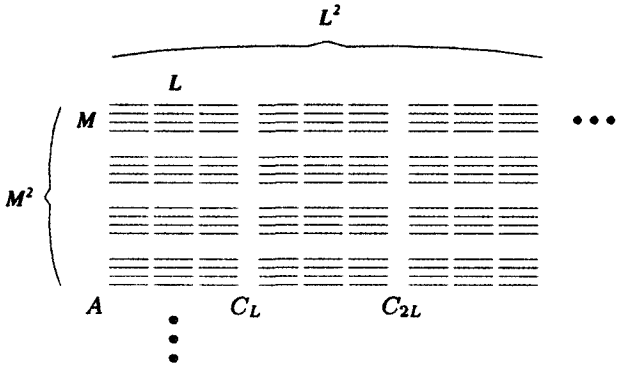


Рис.8.16. Вложенное очищение с рядом элементарных ЭПР-пар.

В заключение этого раздела мы рассмотрим *вложенный протокол очищения* [381], состоящий в одновременном объединении и очищении пар. Смысл его состоит в следующем (см.Рис.8.16). Предположим, для простоты, что $N = L^n$ для некоторого целого n. На первом уровне мы одновременно объединяем пары (с начальным качеством F_1) во всех точках соединений, кроме C_L, C_{2L},...C_{N-L}. В итоге у нас оказывается N/L пар длиной L (и качеством F_L) между $A\&C_L$, $C_L\&C_{2L}$ и т.д. Чтобы очистить эти пары нам необходимо иметь определенное число M копий, которые мы строим следующим образом. Удобнее расположить их в виде ряда элементарных пар, как показано на Рис.8.16 для $L = 3$ и $M = 4$. Затем, мы используем эти копии в сегментах $A\&C_L$, $C_L\&C_{2L}$ и т.д. для очищения и (вос)создания по одной паре с качеством F_1 на каждый сегмент. Последнее условие определяет (среднее) число копий M, которое нам необходимо и которое будет зависеть от начального качества, уменьшении этого качества при соединении и эффективности протокола очищения. Общее количество элементарных пар, которое мы использовали до этого момента, составляет LM. [На Рис.8.16 это означает, что каждая группа $L \times M = 3 \times 4$ пар должна быть заменена на одну пару с начальным качеством.] На втором уровне мы объединяем L таких пар в каждой точке соединений $C_{kL}(k = 1, 2...)$, кроме C_L, C_{2L},..., C_{N-L^2}. В результате, мы получаем N/L^2 пар длиной L^2 между

$A\&C_L$, $C_L\&C_{2L}$ и т.д. с качеством F_L. И снова, нам нужно M параллельных копий таких длинных пар, чтобы очистить их до качества $\geq F_1$. Общее число элементарных пар, участвующих в процессе до этого момента, составляет $(LM)^2$. [Теперь, полный набор из $3^2 \times 4^2$ пар на рис.8.16 должен быть заменен одной парой с качеством F_1.] Мы продолжаем такую операцию на все более высоких уровнях, пока не достигнем n-го уровня. В результате, мы получаем конечную пару между $A\&B$ длиной N и качеством F_1. Таким образом, общее число R элементарных пар будет составлять $(LM)^n$, где M^n дает число требуемых «параллельных каналов» на рис.8.16. Можно выразить этот результат в форме

$$R = N^{\log_L M + 1}, \tag{8.54}$$

которая показывает, что затраты ресурсов растут полиномиально с расстоянием N.

Метод вложенного очищения восходит к идее объединенной кодировки [399], которая используется в контексте квантовых вычислений, нечувствительных к ошибкам [400]. Эта схема позволяет, в принципе, передавать кубит на произвольно большие расстояния с полиномиальными затратами ресурсов. Однако, это требует кодировать единичный кубит в перепутанном состоянии большого числа кубитов, которое посылается через канал и оперировать таким кодом несколько раз во время процесса передачи. Напротив, в схеме вложенного очищения мы не посылаем произвольного кубита через канал, а создаем ЭПР-корреляции по всему каналу одновременно. При создании таких корреляций, никакой квантовой информации не передается (хотя ЭПР-пара может впоследствии использоваться для связи посредством телепортации). В результате, мы получаем требование на качество при локальных операциях, которое не превышает нескольких процентов. В случае же квантовых вычислений, нечувствительных к ошибкам, эта величина составляет 10^{-5} [399].

Ряд на рис.8.16 представляет ансамбль идентичных (элементарных) ЭПР-пар, с помощью которых выполняется очищение. И наоборот, можно выполнять очищение при помощи единственной вспомогательной пары на каждом уровне (см. [381, 387]). В этом смысле, вертикальное направление на диаграмме 8.16 переводится, таким образом, во временную шкалу (число повторных операций). Тогда, именно полное время, необходимое для создания ЭПР-пары между A и B растет полиномиально в (8.54), в то время как число вспомогательных атомов, необходимых при каждом соединении, растет только логарифмическим образом с увеличением $N = l/l_0$. Итоговая схема квантового повторителя показана схематично на рис.8.17. Каждая точка соедине-

ния в канале состоит из простого «квантового процессора», который содержит малое число атомов, используемых для выполнения логических операций и выполняет измерения, необходимые для очищения. Некоторые атомы используются для повторного приготовления ЭПР-пар между соседними точками соединений (здесь $L = 2$), например, при использовании методов, рассмотренных в разд.8.6. Такие повторно приготовленные пары применяются для очищения перепутывания. Затем, методом обмена перепутывания создаются все более удаленные пары. Для очищения таких удаленных пар, необходимо иметь по одному вспомогательному атому на каждом уровне. Поэтому, общее число таких процессоров растет лишь логарифмически с увеличением l [381, 387].

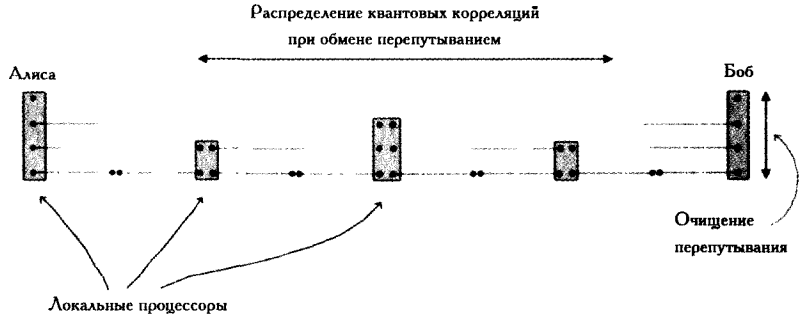


Рис.8.17. Схема квантового повторителя. В каждой точке соединения используется небольшой «квантовый процессор» (состоящий всего из нескольких кубитов) для выполнения протокола очищения перепутывания и обмена перепутыванием. Распределение перепутывания высокого качества через составной канал координируется глобальным протоколом, который называется вложенным очищением перепутывания [381].

В противоположность случаю классических вычислений, квантовый повторитель не является локальным усилителем, а включает и контрольные точки, и глобальный (вложенный) протокол очищения. Таким образом, мы только что рассмотрели схему, которая нечувствительна к ошибкам при локальных операциях и измерениях, не выходя из процентного диапазона. Для выяснения деталей, читатель может обратиться к работам [381, 387].

Литература

1. R.P. Feynman, R.B. Leighton, and M. Sands, *The Feynman Lectures of Physics, Vol. III, Quantum Mechanics*, Addison-Wesley, Reading (1965).
2. G.I. Taylor, Proc. Camb. Phil. Soc. **15**, 114 (1909).
3. G. Möllenstedt and C. Jönsson, Z. Phys. **155**, 472 (1959); A. Tonomura, J. Endo, T. Matsuda, and T. Kawasaki, Am. J. Phys. **57**, 117 (1989).
4. A. Zeilinger, R. Gähler, C.G. Shull, W. Treimer, and W. Mampe, Rev. Mod. Phys. **60**, 1067 (1988).
5. O. Carnal and J. Mlynek, Phys. Rev. Lett. **66**, 2689 (1991).
6. S.L. Braunstein, A. Mann, and M. Revzen, Phys. Rev. Lett. **68**, 3259 (1992).
7. A. Zeilinger, Am. J. Phys. **49**, 882 (1981).
8. M.P. Silverman, *More than One Mystery: Explorations in Quantum Interference*, Springer, Berlin (1995).
9. E. Schrödinger, "Die gegenwärtige Situation in der Quantenmechanik", Naturwissenschaften, **23**, 807; 823; 844 (1935). English translation, "The Present Situation in Quantum Mechanics". Proc. of the American Philosophical Society, **124**, 323 (1980); reprinted in *Quantum Theory and Measurement* edited by J.A. Wheeler and W.H. Zurek, Princeton, 152 (1983).
10. M.A. Horne and A. Zeilinger, in: *Proceedings of the Symposium Foundations of Modern Physics*, P. Lahti, P. Mittelstaedt (Eds.), World Scientific, Singapore 435 (1985); M.A. Horne and A. Zeilinger, in: *Microphysical Reality and Quantum Formalism*, A. van der Merwe, et al. (Eds.), Kluwer, Dordrecht, 401 (1988).
11. J.S. Bell, Phys. World **3**, 33 (1990).
12. J.F. Clauser, M.A. Horne, A. Shimony, and R.A. Holt, Phys. Rev. Lett. **23**, 880 (1969).
13. D. Greenberger, M.A. Horne, A. Zeilinger, *Going beyond Bell's Theorem, in "Bell's Theorem, Quantum Theory, and Conceptions of the Universe"*, M. Kafatos (Ed.), Kluwer, Dordrecht, 69 (1989).
14. N.D. Mermin, Phys. Today **43**, No. 6, 9 (1990); D.M. Greenberger, M.A. Horne, A. Shimony, and A. Zeilinger, Am. J. Phys. **58**, 1131 (1990).
15. D. Bohm, *Quantum Theory*, Prentice-Hall, Englewood Cliffs, 614 (1951).
16. P.G. Kwiat, H. Weinfurter, T. Herzog, and A. Zeilinger, Phys. Rev. Lett. **74**, 4763 (1995).
17. K.F. Weizsäcker, Z. Phys. **40**, 114 (1931).
18. D. Bouwmeester, J-W. Pan, M. Daniell, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **82**, 1345 (1999).
19. D. Bruss, A. Ekert, F. Huelga, J.-W. Pan, and A. Zeilinger, Phil. Trans. R. Soc. (London) A **355**, 2259 (1997).
20. N. Bohr, "Discussions with Einstein on Epistemological Problems in Atomic Physics" in *Albert Einstein: Philosopher-Scientist*, Edited by P.A. Schilpp, The Library of Living Philosophers, Evanston, 200 (1949).

21. A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).
22. N. Bohr, Phys. Rev. **48**, 696 (1935).
23. J.S. Bell, *On the Einstein-Podolsky-Rosen paradox*, Physics **1**, 195 (1964), reprinted in J.S. Bell, *Speakable and Unspeakable in Quantum Mechanics*, Cambridge U.P., Cambridge (1987).
24. S.J. Freedman and J.S. Clauser, Phys. Rev. Lett. **28**, 938 (1972); A. Aspect, J. Dalibard, and G. Roger, Phys. Rev. Lett. **47**, 1804 (1982); W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **81**, 3563 (1998); G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **81**, 5039 (1998).
25. A. Aspect, P. Grangier, and G. Roger, Phys. Rev. Lett. **47**, 460 (1981); **49**, 91 (1982); A. Aspect, J. Dalibard, and G. Roger, ibid. **49**, 1804 (1982).
26. P.G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A.V. Sergienko, and Y.H. Shih, Phys. Rev. Lett. **75**, 4337 (1995).
27. P.M. Pearle, Phys. Rev. D **2**, 1418 (1970); J.F. Clauser, A. Shimony, Rep. Prog. Phys. **41**, 1881 (1978).
28. E.P. Wigner, Am. J. Phys. 38, 1005 (1970).
29. D. Kahn, *The Codebreakers: The Story of Secret Writing*, Macmillan, New York (1967).
30. A.J. Menezes, P.C. van Oorschot, and S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press (1996).
31. B. Schneier, *Applied cryptography: protocols, algorithms, and source code in C*, John Wiley & Sons (1994).
32. D. Welsh, *Codes and Cryptography*, Clarendon Press, Oxford, (1988).
33. C.E. Shannon, Bell Syst. Tech. J, **28**, 656 (1949).
34. W. Diffie, and M.E. Hellman, IEEE Trans. Inf. Theory, **IT-22**, 644 (1976).
35. R. Rivest, A. Shamir, and L. Adleman, *On Digital Signatures and Public-Key Cryptosystems*, MIT Laboratory for Computer Science, Technical Report, MIT/LCS/TR-212 (January 1979).
36. P. Shor, (1994) *Proc. of 35th Annual Symposium on the Foundations of Computer Science*, (IEEE Computer Society, Los Alamitos), p. 124 (Extended Abstract). Full version of this paper appears in S. I. A. M. Journal on Computing, **26** (1997), 1484 and is also available at quant-ph/9508027.
37. S. Wiesner, *SIGACT News*, **15**, 78 (1983); original manuscript written *circa* 1970.
38. C.H. Bennett and G. Brassard, in *"Proc. IEEE Int. Conference on Computers, Systems and Signal Processing"*, IEEE, New York, (1984).
39. J.F. Clauser and M.A. Horne, *Phys. Rev. D* **10**, 526 (1974).
40. B. Huttner and A. Ekert, J. Mod. Opt., **41**, 2455 (1994).
41. P.D. Townsend, Nature **385**, 47 (1997).
42. C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Cryptol. **5**, 3 (1992).
43. A. Muller, J. Breguet, and N. Gisin, Europhys. Lett. **23**, 383 (1993).
44. A.K. Ekert, J.G. Rarity, P.R. Tapster, and G.M. Palma, Phys. Rev. Lett. **69** 1293 (1992).
45. C.H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
46. A.K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
47. D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996); C. Macchiavello, Phys. Lett. A **246**, 385 (1998).
48. Q.A. Turchette, C.J. Hood, W. Lange,H. Mabuchi, and H.J. Kimble, Phys. Rev. Lett. **75**, 4710 (1995).

49. Bennett, C. H., Brassard, G., Popescu, S., Schumacher, B., Smolin, J. A., Wootters, W. K. Purification of noisy entanglement and faithful teleportation via noisy channels. Phys. Rev. Lett. **76**, 722-725 (1996).
50. M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **78** 574 (1997).
51. G. Brassard and L. Salvail, *Eurocrypt '93, Lofthus, Norway* (1993).
52. B.A. Slutsky, R. Rao, P.-C. Sun and Y. Fainman, Phys.Rev.A **57**, 2383 (1998).
53. J.I. Cirac and N. Gisin, Phys. Lett. A **229**, 1 (1997)
54. C.A. Fuchs, N. Gisin, R.B. Griffiths, C.-S. Niu, and A. Peres, Phys. Rev. A **56**, 1163 (1997).
55. H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A **59**, 4238 (1999).
56. N. Lütkenhaus, Phys. Rev. A **59**, 3301 (1999).
57. C.H. Bennett, G. Brassard, C. Crépeau, and U. Maurer, *1994 IEEE International Symposium on Information Theory*, Trondheim, Norway, June (1994).
58. A. Peres, *Quantum Theory: Concepts and Methods*, Kluwer Academic Publishers, (1995).
59. E. Biham, M. Boyer, G. Brassard, J. van de Graaf, and T. Mor, *Security of Quantum Key Distribution against all Collective attacks*, quant-ph/9801022 (1998).
60. D. Mayers, *Unconditional security in Quantum Cryptography*, quant-ph/9802025 (1998).
61. M.N. Wegman, J.L. Carter, Journal of Computer and System Sciences **22**, 265-279 (1981).
62. G. Ribordy, J.D. Gautier, H. Zbinden, and N. Gisin, Applied Optics **37**, 2272 (1998).
63. R.Y. Chiao and Y.S. Wu, Phys. Rev. Lett. **57**, 933 (1986).
64. B.C. Jacobs and J.D. Franson, Opt. Lett. **21**, 1854 (1996).
65. W.T. Buttler, R.J. Hughes, P.G. Kwiat, S.K. Lamoreaux, G.G. Luther, G.L. Morgan, J.E. Nordholt, C.G. Peterson, and C.M. Simmons, Los Alamos preprint, quant-ph/9805071.
66. P.D. Townsend, C. Marand, S.J.D. Phoenix, K.J. Blow, and S.M. Barnett, Phil. Trans. Roy. Soc. London A **354**, 805 (1996).
67. R.J. Hughes, G.G. Luther, G.L. Morgan, C.G. Peterson, C.G. and C. Simmons, C. *Quantum cryptography over underground optical fibres*, Advances in Cryptology - Proceedings of Crypto'96, Springer, Berlin, Heidelberg (1996).
68. G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, Electronics Letters **34**, 2116-2117 (1998).
69. J.D. Franson, Phys. Rev. Lett. **62**, 2205 (1989).
70. J.G. Rarity, P.C.M. Owens, and P.R. Tapster, Phys. Rev. Lett. **73**, 1923 (1994).
71. W. Tittel, J. Brendel, B. Gisin, T. Herzog, H. Zbinden and N. Gisin, Phys. Rev. A **57**, 3229 (1998); W. Tittel, J. Brendel, H. Zbinden and N. Gisin, Phys. Rev. Lett. **81**, 3563 (1998).
72. G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **81**, 5039 (1998).
73. C.H. Bennett and S.J. Wiesner, Phys. Rev. Lett., **69**, 2881 (1992).
74. C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W.K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
75. K. Mattle, H. Weinfurter, P.G. Kwiat, and A. Zeilinger, Phys. Rev. Lett. **76**, 4656 (1996).
76. D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eible, H. Weinfurter, and A. Zeilinger, Experimental quantum teleportation. Nature **390**, 575-579 (1997).
77. S. Popescu, LANL E-print quant-ph 9501020.

78. D. Boschi, S. Branca, F. De Martini, L. Hardy, and S. Popescu, Phys. Rev. Lett. **80**, 1121 (1998).
79. L. Vaidman, Phys. Rev. A **49**, 1473 (1994).
80. S.L. Braunstein and H.J. Kimble, Phys. Rev. Lett. **80**, 869 (1998).
81. A. Furusawa, J.L. Sørensen, S.L. Braunstein, C.A. Fuchs, H.J. Kimble, and E.S. Polzik, Science Oct23 1998 pp 706-709.
82. Comment by F. De Martini, and Reply by A. Zeilinger, Physics World **11**, nr.3, 23-24 (March 1998).
83. Comment by S.L. Braunstein and H.J. Kimble, and Reply by D. Bouwmeester, J-W. Pan, M. Daniell, H. Weinfurter, M. Zukowski, and A. Zeilinger, Nature (London) **394**, 840-841 (1998).
84. D. Bouwmeester, J.-W. Pan, H. Weinfurter, and A. Zeilinger, High-fidelity teleportation of qubits, J. Mod. Opt. **47**, 279 (2000).
85. M. Zukowski, A. Zeilinger, M.A. Horne, and A. Ekert, Phys. Rev. Lett. **71**, 4287 (1993).
86. J.-W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger, Experimental entanglement swapping: Entangling photons that never interacted. Phys. Rev. Lett. **80**, 3891-3894 (1998).
87. S. Bose, V. Vedral, and P.L. Knight, *A multiparticle generalisation of entanglement swapping* Phys. Rev. A **57**, 822 (1998).
88. W.K. Wootters and W.H. Zurek, Nature (London) **299**, 802, (1982).
89. D.N. Klyshko, Sov. Phys. JETP **28**, 522 (1969).
90. D.C. Burnham and D.L. Weinberg, Phys. Rev. Lett. **25**, 84 (1970).
91. J.D. Franson and K.A. Potocki, Phys. Rev. A **37**, 2511 (1988).
92. J. Brendel, E. Mohler, and W. Martiennsen, Europhys. Lett. **20**, 575 (1992); P.G. Kwiat, A.M. Steinberg and R.Y. Chiao, Phys. Rev. A **47**, R2472 (1993).
93. J. Brendel, N. Gisin, W. Tittel and H. Zbinden, Phys. Rev. Lett. **82**, 2594 (1999).
94. J.G. Rarity and P.R. Tapster, Phys. Rev. Lett. **64**, 2495 (1990).
95. R. Loudon, *Coherence and Quantum Optics VI*, ed. Eberly, J.H. and Mandel, L. Plenum New York, 703 (1990).
96. A. Zeilinger, H.J. Bernstein, and M.A. Horne, J. Mod. Optics, **41**, 2375, (1994).
97. H. Weinfurter, Europhys. Lett. **25**, 559 (1994).
98. S.L. Braunstein and A. Mann, Phys. Rev. **A 51**, R1727 (1995).
99. M. Michler, K. Mattle, H. Weinfurter, and A. Zeilinger, Phys. Rev. A **53**, R1209 (1996).
100. A. Zeilinger, *Proc. of the Nobel Symp. 104* "Modern Studies of Basic Quantum Concepts and Phenomena" E.B. Karlsson and E. Brändes (Eds.), Physica Scripta, T76, 203 (1998).
101. M. Zukowski, A. Zeilinger and H. Weinfurter in *Fundamental Problems in Quantum Theory* vol. 755 Annals of the New York Academy of Sciences (Greenberger and Zeilinger Eds.) p. 91 (1995).
102. J. Kim, S. Takeuchi, Y. Yamamoto, and H.H. Hogue, Appl. Phys. Lett, **74**,902 (1999).
103. E. Hagley, X. Maître, G. Nogues, C. Wunderlich, M. Brune, J.M. Raimond, and S. Haroche, Generation of Einstein-Podolsky-Rosen pairs of atoms. Phys. Rev. Lett. **79**, 1-5 (1997).
104. H-J. Briegel, W. Dür, J.I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).
105. M. Zukowski, Phys. Lett. A 157, 198 (1991).
106. R. Loudon, *The Quantum Theory of Light, second edition.* Clarendon Press, Oxford, (1983).

107. A. Yariv, *Quantum Electronics, third edition.* John Wiley& Sons (1989).
108. D.F. Walls and G.J. Milburn, *Quantum Optics, second edition.* Springer, Berlin, Heidelberg (1994).
109. P.W. Milonni, *The Quantum Vacuum* Academic Press, San Diego, 1994.
110. Z.Y. Ou, S.F. Pereira, H.J. Kimble, and K.C. Peng, Rhys. Rev. Lett. **68**, 3663 (1992).
111. Z.Y. Ou, S.F. Pereira, and H.J. Kimble, Appl. Phys. B **55**, 265 (1992).
112. H.J. Kimble, in *Fundamental Systems in Quantum Optics, Les Houches, 1990*, eds. J. Dalibard, J.M. Raimond, J. Zinn-Justin (Elsevier Science Publishers, Amsterdam, 1992), pp, 549-674.
113. Ling-An Wu, H.J. Kimble, J.L. Hall, and Huifa Wu, Phys. Rev. Lett. **57**, 2520 (1986).
114. See, for example, S.J. Freedman and J.S. Clauser, Phys. Rev. Lett **28**, 938 (1972).
115. M. Lamehi-Rachti and W. Mittig, Phys. Rev. D **14**, 2543 (1976).
116. E. Biham, B. Huttner and T. Mor, Phys. Rev. A **54**, 2651 (1996).
117. C.H Bennett, H.J. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A **53**, 2046 (1996).
118. S. Bose, V. Vedral, and P.L. Knight, Phys. Rev. A **60**, 194 (1999).
119. A. Zeilinger, M.A. Horne, H. Weinfurter, and M. Zukowski, Phys. Rev. Lett **78**, 3031 (1997).
120. L. Grover, *Proc. 28 Annual ACM Symposium on the Theory of Computing*, ACM Press New York, 212 (1996).
121. G. Brassard, Science **275**, 627 (1997).
122. R. Rivest, A. Shamir, and L. Adleman, *On Digital Signatures and Public-Key Cryptosystems*, MIT Laboratory for Computer Science, Technical Report, MIT/LCS/TR-212 (January 1979).
123. R. Feynman, Int. J. Theor. Phys. **21**, 467, (1982).
124. D. Deutsch, Proc. R. Soc. London A **400**, 97 (1985).
125. D. Deutsch, Proc. R. Soc. London A: **425**, 73, (1989).
126. S.F. Huelga, C. Macchiavello, T. Pellizzari, A.K. Ekert, M.B. Plenio, and J.I. Cirac, Phys. Rev. Lett. **79**, 3865 (1997).
127. D. Deutsch, *The Fabric of Reality* (Allen Lane, Penguin Press, London).
128. D. Deutsch and A. Ekert, Phys. World **11**, 47 (March 1998).
129. A. Barenco, C.H. Bennett, R. Cleve, D. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter, Phys. Rev. A **52**, 3457 (1995).
130. D. Deutsch, A. Barenco, and A. Ekert, Proc. Roy. Soc. Lond. A **449**, 669 (1995).
131. C.H. Papadimitriou, *Computational Complexity* (Addison-Wesley, Reading, MA, 1994).
132. M. Garey, and D. Johnson, *Computers and Intractability: A Guide to the Theory of NP Completeness* (W. H. Freeman and Co., 1979).
133. R. Jozsa, Entanglement and Quantum Computation in *The Geometric Universe*, 369, eds. S. Huggett, L. Mason, K.P. Tod, S.T. Tsou and N.M.J. Woodhouse (Oxford University Press, 1998).
134. A. Ekert and R. Jozsa, Phil. Trans. Roy. Soc. London Ser A, **356**, 1769 (1998).
135. A.S. Holevo, Probl. Inf. Transm **9**, 177 (1973).
136. C. Fuchs and A. Peres, Phys. Rev. A. **53**, 2038 (1996).
137. T. Cover and J. Thomas, *Elements of Information Theory*, John Wiley and Sons (1991).
138. D. Deutsch and R. Jozsa, Proc. Roy. Soc. Lond. A **439**, 553 (1992).
139. R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca, Proc. Roy. Soc. London Ser A, **454**, 339 (1998) .

140. E. Bernstein and U. Vazirani, *Proc. 25th Annual ACM Symposium on the Theory of Computing*, (ACM Press, New York), p. 11-20 (1993) (Extended Abstract). Full version of this paper appears in S. I. A. M. Journal on Computing, **26**, 1411 (1997).
141. D. Simon, (1994) *Proc. of 35th Annual Symposium on the Foundations of Computer Science*, (IEEE Computer Society, Los Alamitos), p. 116 (Extended Abstract). Full version of this paper appears in S. I. A. M. Journal on Computing, **26**, 1474 (1997).
142. G.H. Hardy and E.M. Wright *An Introduction to the Theory of Numbers* (4th edition, Clarendon, Oxford, 1965).
143. M.R. Schroeder, *Number Theory in Science and Communication* (2nd enlarged edition, Springer, New York, 1990).
144. A. Ekert and R, Jozsa, Rev. Mod. Phys. **68**, 733 (1996).
145. D.K. Maslen and D.N. Rockmore, "Generalised FFT's – A Survey of Some Recent Results", in *Proc. DIMACS Workshop on Groups and Computation – II* (1995).
146. R. Jozsa, Proc. Roy. Soc. London Ser A, **454**, 323 (1998).
147. G. Brassard and P. Hoyer, "An exact polynomial-time algorithm for Simon's problem", *Proc. 5th Israeli Symposium on Theory of Computing and Systems (ISTCS 97)*, 12 (1997), also available at quant-ph/9704027.
148. A. Kitaev, Russian Math. Surveys **52**, 1191 (1997), also available at quant-ph/9511026.
149. R. Beals, *Proc. 29th Annual ACM Symposium on the Theory of Computing – STOC* (ACM Press, New York), 48 (1997).
150. L. Grover, Phys. Rev. Lett.**78**, 325 (1997).
151. M. Boyer, G. Brassard, P. Hoyer, and A. Tapp, *Proc. of fourth workshop on Physics and Computation – PhysComp'96*, 36-43 (1996).
152. L. Grover, "A Framework for Fast Quantum Algorithms", *Proc. 30th ACM Symposium on Theory of Computation (STOC'98)*, 53 (1998), also available at quant-ph/9711043.
153. G. Brassard, P. Hoyer, and A. Tapp, "Quantum Counting", *Proc. 25th ICALP*, Vol 1443, Lecture Notes in Computer Science, 820 (Springer, 1998), also available at quant-ph/9805082.
154. L. Grover, Phys. Rev. Lett. **80**, 4325 (1997).
155. C.H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, S. I. A. M. Journal on Computing, **26**, 1510 (1997).
156. J.I. Cirac and P. Zoller, Phys. Rev. Lett. **74**, 4091 (1995).
157. J.F. Poyatos, J.I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 1322 (1998).
158. C. Monroe, D.M. Meekhof, B.E. King, W.M. Itano, and D. J. Wineland, Phys. Rev. Lett. **75**, 4714 (1995).
159. E.T. Jaynes and F.W. Cummings, Proc. IEEE **51**, 89 (1963).
160. *Cavity Quantum Electrodynamics, Advances in atomic, molecular and optical physics, Supplement 2*, P. Berman editor, Academic Press (1994).
161. S. Haroche, in *Fundamental systems in quantum optics, les Houches summer school session LIII*, J. Dalibard, J.M. Raimond and J. Zinn-Justin eds, North Holland, Amsterdam (1992).
162. D.G. Hulet and D. Kleppner, Phys. Rev. Lett. **51**, 1430 (1983).
163. P. Nussenzvzeig, F. Bernardot, M. Brune, J. Hare, J.M. Raimond, S. Haroche and W. Gawlik, Phys. Rev. A **48**, 3991 (1993).
164. M. Brune, P. Nussenzveig, F. Schmidt-Kaler, F. Bernardot, A. Maali, J.M. Raimond, and S. Haroche, Phys. Rev. Lett, **72**, 3339 (1994)
165. M. Brune, F. Schmidt-Kaler, A. Maali, J. Dreyer, E. Hagley, J.M. Raimond, and S. Haroche, Phys. Rev. Lett. **76**, 1800 (1996).

166. M. Brune, E. Hagley, J. Dreyer, X. Maître, A. Maali, C. Wunderlich, J.M. Raimond, and S. Haroche, Phys. Rev. Lett.,**77**, 4887 (1996).
167. X. Maître, E. Hagley, G. Nogues, C. Wunderlich, P. Goy, M. Brune, J.M. Raimond and S. Haroche, Phys. Rev. Lett. **79**, 769 (1997).
168. E. Hagley, X. Maître, G. Nogues, C. Wunderlich, M. Brune, J.M. Raimond and S. Haroche, Phys. Rev. Lett. **79**, 1 (1997).
169. G. Nogues, A. Rauschenbeutel, S. Osnaghi, M. Brune, J.M. Raimond and S. Haroche, Nature **400**, 239 (1999).
170. G. Raithel, C. Wagner, H. Walther, L.M. Narducci and M.O. Scully, in *Cavity Quantum Electrodynamics*, P. Berman ed. 57, Academic, New York (1994).
171. J.H. Eberly, N.B. Narozhny and J.J. Sanchez-Mondragon, Phys. Rev. Lett. **44**, 1323 (1980).
172. R.J. Thompson, G. Rempe and H.J. Kimble, Phys. Rev. Lett. **68**, 1132 (1992).
173. F. Bernardot, P. Nussenzveig, M. Brune, J.M. Raimond and S. Haroche , Euro. Phys. Lett. **17**, 33 (1992).
174. P. Domokos, J.M. Raimond, M. Brune and S. Haroche, Phys. Rev. A **52**, 3554 (1995).
175. J.I. Cirac and P. Zoller, Phys. Rev. A **50**, R2799 (1994).
176. D.M. Greenberger, M.A. Horne, A. Shimony, and A. Zeilinger, Am.J.Phys **58**, 1131 (1990). N.D. Mermin, Physics Today (June 9, 1990).
177. S. Haroche in *Fundamental problems in quantum theory*, D. Greenberger and A. Zeilinger Eds, Ann. N.Y. Acad. Sci. **755**, 73 (1995).
178. E. Schrödinger, *Naturwissenschaften* **23**, 807, 823, 844 (1935). Reprinted in english in J.A. Wheeler and W.H. Zurek, *Quantum theory of measurement*, Princeton University Press (1983).
179. W.H. Zurek, Phys. Rev. D **24**, 1516 (1981).
180. W.H. Zurek, Phys. Rev. D **26**, 1862 (1982).
181. A.O. Caldeira and A.J. Leggett Physica A, **121**, 587 (1983).
182. E. Joos and H.D. Zeh, Z.Phys.B **59**, 223 (1985).
183. W.H. Zurek, Physics Today **44**, 10 p.36 (1991).
184. R. Omnès, *The Interpretation of Quantum Mechanics*, Princeton University Press (1994).
185. D.F. Walls and G.J. Milburn, Phys. Rev. A **31**, 2403.
186. L. Davidovich, M. Brune, J.M. Raimond and S. Haroche, Phys. Rev. A **53**, 1295 (1996).
187. M.O. Scully and H. Walther, Phys. Rev. A **39**, 5299 (1989).
188. J.M Raimond, M. Brune and S. Haroche, Phys. Rev. Lett. **79**, 1964 (1997).
189. C.A. Blockey, D.F. Walls, and H. Risken, Europhys. Lett. **17**, 509 (1992).
190. J.I. Cirac, R. Blatt, A.S. Parkins, and P. Zoller, Phys. Rev. Lett. **70**, 762 (1993).
191. J.I. Cirac, R. Blatt, A.S. Parkins, and P. Zoller, Phys. Rev. A **49**, 1202 (1994).
192. J.I. Cirac, R. Blatt, and P. Zoller, Phys. Rev. A **49**, R3174 (1994).
193. Proc.5th Symp.Freq.Standards and Metrology, ed. J.C. Bergquist, (World Scientific, 1996).
194. D.J. Berkeland, J.D. Miller, J.C. Bergquist, W.M. Itano, and D.J. Wineland, Phys. Rev. Lett. **80**, 2089 (1998).
195. R. Blatt, in *Atomic Physics* **14**, 219, ed. D.J. Wineland, C. Wieman, S.J. Smith, AIP New York (1995).
196. W. Paul, O. Osberghaus, and E. Fischer, Forschungsberichte des Wirtschafts- und Verkehrsministerium Nordrhein-Westfalen **415** (1958).
197. P.K. Ghosh, Ion traps, Clarendon, Oxford (1995).
198. D.J. Wineland, and H. Dehmelt, Bull. Am. Phys. Soc. **20**, 637 (1975).

199. D.J. Wineland, R.E. Drullinger, and F.L. Walls, Phys. Rev. Lett. **40**, 1639 (1978).
200. A. Steane, Appl. Phys. B **64**, 623 (1997), see Table 1 in which a list of candidate ions is given together with relevant experimental parameters.
201. *http : //www.bldrdoc.gov/timefreq/ion/index.htm*
202. *http : //horology.jpl.nasa.gov/research.html*
203. *http : //mste.laser.physik.uni – muenchen.de/lg/worktop.html*
204. *http : //p23.lanl.gov/Quantum/quantum.html*
205. *http : //dipmza.physik.uni – mainz.de/ www$_w$erth/calcium/calcium.html*
206. *http : //www – phys.rrz.uni – hamburg.de/home/vms/group$_a$/index.html*
207. *http : //heart – c704.uibk.ac.at/*
208. D.J. Wineland, W.M. Itano, J.C. Bergquist, and R.G. Hulet, Phys. Rev. A **36**, 2220 (1987).
209. J.I. Cirac, A.S. Parkins, R. Blatt, and P. Zoller, Phys. Rev. Lett. **70**, 556 (1993).
210. S. Stenholm, Rev. Mod. Phys. **58**, 699 (1986).
211. C. Monroe, D.M. Meekhof, B.E. King, S.R. Jeffers, W.M. Itano, D.J. Wineland, and P. Gould, Phys. Rev. Lett. **74**, 4011 (1995).
212. H.C. Nägerl, W. Bechter, J. Eschner, F. Schmidt-Kaler, and R. Blatt, Appl. Phys. B **66**, 603 (1998).
213. H.C. Nägerl, D. Leibfried, H. Rohde, G. Thalhammer, J. Eschner, F. Schmidt-Kaler, and R. Blatt, Phys. Rev. A. **60**, 145 (1999).
214. F. Diedrich, J.C. Bergquist, W.M. Itano, and D.J. Wineland, Phys. Rev. Lett. **62**, 403 (1989).
215. Ch. Roos, Th. Zeiger, H. Rohde, H.C. Nägerl, J. Eschner, D. Leibfried, F. Schmidt-Kaler, and R. Blatt, Phys. Rev. Lett. **83**, 4713 (1999).
216. B.E. King, C.S. Wood, C.J. Myatt, Q.A. Turchette, D. Leibfried, W.M. Itano, C. Monroe, and D.J. Wineland, Phys. Rev. Lett. **81**, 1525 (1998).
217. H. Dehmelt, Bull. Am. Phys. Soc. **20** 60 (1975).
218. D.J. Wineland, C. Monroe, W.M. Itano, D. Leibfried, B. King, and D.M. Meekhof, Journal of Research of the National Institute of Standards and Technology **103**, 259 (1998).
219. D. Leibfried, D.M. Meekhof, B.E. King, C. Monroe, W.M. Itano, and D.J. Wineland, Phys. Rev. Lett **77**, 4281 (1996).
220. D.M. Meekhof, C. Monroe, B.E. King, W.M. Itano, and D.J. Wineland, Phys. Rev. Lett. **76**, 1796 (1996).
221. C. Monroe, D.M. Meekhof, B.E. King, and D.J. Wineland, Science **272**, 1131 (1996)
222. J.F. Poyatos, J.I. Cirac, and P. Zoller, Phys. Rev. Lett. **77**, 4728 (1996).
223. C. Monroe, D.M. Meekhof, B.E. King, W.M. Itano, and D.J. Wineland, Phys. Rev. Lett. **75**, 4714 (1995).
224. L.G. Lutterbach and L. Davidovich, Phys. Rev. Lett. **78**, 2547 (1997).
225. M.B. Plenio and P.L. Knight Phys. Rev. A **53**, 2986 (1996).
226. J.I. Cirac, A.S. Parkins, R. Blatt, and P. Zoller, Adv. At. Molec. Opt. Physics **37**, 238 (1996).
227. D.P. DiVincenzo, Phys. Rev. A **51**, 1015 (1995).
228. D.J. Wineland, C. Monroe, W.M. Itano, D. Leibfried, B. King, and D.M. Meekhof, Rev. Mod. Phys. (1998).
229. G. Morigi, J. Eschner, J.I. Cirac, and P. Zoller, Phys. Rev. A. **59**, 3797 (1999).
230. E. Peik, J. Abel, T. Becker, J. von Zanthier, and H. Walther, Phys. Rev. A **60**, 439 (1999).
231. I. Waki, S. Kassner, G. Birkl, and H. Walther, Phys. Rev. Lett. **68**, 2007 (1992); G. Birkl, S. Kassner, H. Walther, Nature 357, 310 (1992).

232. D.F.V. James, Appl. Phys. B **66** 181 (1998).
233. C. Monroe, D. Leibfried, B.E. King, D.M. Meekhof, W.M. Itano, and D.J. Wineland, Phys. Rev. **A55**, R2489 (1997)
234. W. Nagourney, J. Sandberg, and H. Dehmelt, Phys. Rev. Lett. **56**, 2797 (1986); Th. Sauter, W. Neuhauser, R. Blatt, and P.E. Toschek, Phys. Rev. Lett. **57**, 1696 (1986); J.C. Bergquist, R. Hulet, W.M. Itano, and D.J. Wineland, Phys. Rev. Lett. **57**, 1699 (1986).
235. P.J. Hore, *Nuclear Magnetic Resonance*, Oxford University Press, Oxford (1995).
236. R.R. Ernst, G. Bodenhausen, and A. Wokaun, *Principles of Nuclear Magnetic Resonance in One and Two Dimensions*, Oxford University Press, Oxford (1987).
237. D.G. Cory, A.F. Fahmy, and T.F. Havel, *Proceedings of the Fourth Workshop on Physics and Computation, Nov. 22–24, 1996*, New England Complex Systems Institute, Cambridge, MA (1996).
238. D.G. Cory, A.F. Fahmy, and T.F. Havel, Proc. Natl. Acad. Sci. USA **94**, 1634 (1997).
239. N.A. Gershenfeld and I.L. Chuang, Science **275**, 350 (1997).
240. A. Abragam, *Principles of Nuclear Magnetism*, Clarendon Press, Oxford (1961).
241. C.P. Slichter, *Principles of Magnetic Resonance* 3rd ed. Springer, Berlin, Heidelberg (1990).
242. M. Goldman, *Quantum Description of High-Resolution NMR in Liquids*, Clarendon Press, Oxford (1988).
243. J.A. Jones and M. Mosca, J. Chem. Phys. **109**, 1648 (1998).
244. A. Barenco. C.H. Bennett, R. Cleve, D.P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J.A. Smolin, and H. Weinfurter, Phys. Rev. A, **52**, 3457 (1995).
245. J.A. Jones, R.H. Hansen, and M. Mosca, J. Magn. Reson. **135**, 353 (1998).
246. L.M.K. Vandersypen, C.S. Yannoni, M.H. Sherwood, and I.L. Chuang, Phys. Rev. Lett. **83**, 3085 (1999).
247. E. Knill, I. Chuang, and R. Laflamme, Phys. Rev. A, **57**, 3348 (1998).
248. T.F. Havel, S.S. Somaroo, C.-H. Tseng, and D.G. Cory, LANL E-print quant-ph/9812026.
249. R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca, Proc. R. Soc. Lond. A **454**, 339 (1998).
250. I.L. Chuang, L.M.K. Vandersypen, X.L. Zhou, D.W. Leung, and S. Lloyd, Nature, **393**, 143 (1998).
251. I.L. Chuang, N. Gershenfeld, and M. Kubinec, Phys. Rev. Lett. **80**, 3408 (1998).
252. J.A. Jones, M. Mosca, and R.H. Hansen, Nature, **393**, 344 (1998).
253. L.K. Grover, Science, **280**, 228 (1998).
254. J.A. Jones and M. Mosca, Phys. Rev. Lett. **83**, 1050 (1999).
255. R. Laflamme, E. Knill, W.H. Zurek, P. Catasti, and S.V.S. Mariappan, Phil. Trans. Roy. Soc. Lond A, **356**, 1941 (1998).
256. R.J. Nelson, D.G. Cory, S. Lloyd, LANL E-print quant-ph/9905028.
257. D.G. Cory, M.D. Price, W. Maas, E. Knill, R. Laflamme, W.H. Zurek, T.F. Havel, and S.S. Somaroo, Phys. Rev. Lett. **81**, 2152 (1998).
258. D. Leung, L. Vandersypen, X. Zhou, M. Sherwood, C. Yannoni, M. Kubinec, and I. Chuang, Phys. Rev. A **60**, 1924 (1999).
259. M.A. Nielsen, E. Knill, and R. Laflamme, Nature, **396**, 52 (1998).
260. N. Linden, H. Barjat, and R. Freeman, Chem. Phys. Lett. **296**, 61 (1998).
261. R. Marx, A. F. Fahmy, J. M. Myers, W. Bermel, and S. J. Glaser, LANL E-print quant-ph/9905087.

262. W.S. Warren, Science, **277**, 1688 (1997).
263. G. Navon, Y.-Q. Song, T. Rõõm, S. Appelt, R.E. Taylor, and A. Pines, Science, **271**, 1848 (1996).
264. L. J. Schulman and U. Vazirani, LANL E-print quant-ph/9804060.
265. R. Freeman, *Spin Choreography*, Spektrum, Oxford, (1997).
266. N. Linden, H. Barjat, R.J. Carbajo, and R. Freeman, Chem. Phys. Lett. **305**, 28 (1999).
267. D.W. Leung, I.L. Chuang, F. Yamaguchi, and Y. Yamamoto, LANL E-print quant-ph/9904100.
268. J.A. Jones and E. Knill, J. Magn. Reson. in press, LANL E-print quant-ph/9905008.
269. N. Linden, Ē. Kupče, and R. Freeman, LANL E-print quant-ph/9907003.
270. P.T. Callaghan, *Principles of Nuclear Magnetic Resonance Microscopy*, Clarendon Press, Oxford (1991).
271. B.E. Kane, Nature **393**, 133 (1998).
272. S.L. Braunstein, C.M. Caves, R. Jozsa, N. Linden, S. Popescu, and R. Schack, Phys. Rev. Lett. **83**, 1054 (1999).
273. R. Schack and C. M. Caves, LANL E-print quant-ph/9903101.
274. T. Pellizzari *et al*, Phys. Rev. Lett. **75** , 3788 (1995).
275. C. Monroe *et al.*, Phys. Rev. Lett. **75**, 4714 (1995).
276. Q. Turchette *et al.*, Phys. Rev. Lett. **75**, 4710 (1995).
277. K. Mattle *at al.*, Phys. Rev. Lett. **76**, 4656 (1996).
278. J. I. Cirac, P. Zoller, H.J. Kimble, and H. Mabuchi, Phys. Rev. Lett. **78**, 3221 (1997).
279. C.H. Bennett, Physics Today **24**, (October 1995) and references cited; A.K. Ekert, Phys. Rev. Lett. **67**, 661 (1991); W. Tittel *et al.*, quant-ph/9707042; W.T. Buttler *et al.*, quant-ph/9801006.
280. C.H. Bennett *et al*, Phys. Rev. Lett. **70**, 1895 (1993); D. Bouwmeester *et al.*, Nature **390**, 575 (1997); D. Boschi *et al.*, Phys. Rev. Lett. **80**, 1121 (1998).
281. L.K. Grover, quant-ph/9704012.
282. A.K. Ekert *et al.*, quant-ph/9803017.
283. C.K. Law and J.H. Eberly, Phys. Rev. Lett. **76**, 1055 (1996).
284. H.J. Carmichael, Phys. Rev. Lett. **70**, 2273 (1993).
285. For a review see P. Zoller and C.W. Gardiner in *Quantum Fluctuations*, Les Houches, ed. E. Giacobino *et al.*, Elsevier, NY, in press.
286. C.W. Gardiner, Phys. Rev. Lett.**70**, 2269 (1993).
287. P.W. Shor, Phys. Rev. A **52**, R2493 (1995); A.M. Steane, Phys. Rev. Lett. **77**, 793 (1996); J.I. Cirac, T. Pellizzari and P. Zoller, Science **273**, 1207 (1996); P. Shor, *Fault-tolerant quantum computation*, quant-ph/9605011; D. DiVincenzo and P.W. Shor, Phys. Rev. Lett. **77**, 3260 (1996).
288. C.H. Bennett *et al.*, Phys. Rev. Lett. **76**, 722 (1996); D. Deutsch *et al.*, Phys. Rev. Lett. **77** , 2818 (1996); N. Gisin, Phys. Lett. A **210**, 151 (1996).
289. D.M. Greenberger, M.A. Horne, A. Zeilinger, A. Going beyond Bell's theorem, in *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, edited by M. Kafatos, (Kluwer, Dordrecht, 1989) pp. 73-76.
290. D.M. Greenberger, M.A. Horne,A. Shimony, A. Zeilinger, Bell's theorem without inequalities. Am. J. Phys. **58**, 1131 (1990).
291. D. Bouwmeester, J.-W.. Pan, M. Daniell, H. Weinfurter, and A. Zeilinger, Observation of three-photon Greenberger-Horne-Zeilinger entanglement. Phys. Rev. Lett. **82**, 1345 (1999).
292. D.M. Greenberger, M.A. Horne, A. Zeilinger, Multiparticle interferometry and the superposition principle. Physics Today, 22, August 1993.
293. N.D. Mermin, Am. J. Phys. **58**, 731 (1990).

294. N.D. Mermin, What's wrong with these elements of reality? Physics Today, 9, June 1990.
295. S.J. Freedman and J.S. Clauser, Experimental test of local hidden-variable theories. Phys. Rev. Lett. **28**, 938-941 (1972).
296. A. Aspect, J. Dalibard, and G. Roger, Experimental test of Bell's inequalities using time-varying analysers. Phys. Rev. Lett. **47**, 1804-1807 (1982).
297. G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger, Violation of Bell's inequality under strict Einstein locality conditions. Phys. Rev. Lett. **81**, 5039-5043 (1998).
298. L. Hardy, Nonlocality for two particles without inequalities for almost all entagled states. Phys. Rev. Lett. **71**, 1665-1668 (1993).
299. D. Boschi, S. Branca, F. De Martini, and L. Hardy, Ladder proof of nonlocality without inequalities: Theoretical and experimental results. Phys. Rev. Lett. **79**, 2755 (1997).
300. A. Zeilinger, M.A. Horne, H. Weinfurter, and M. Zukowski, Three particle entanglements from two entangled pairs. Phys. Rev. Lett. **78**, 3031-3034 (1997).
301. S. Haroche, Ann. N. Y. Acad. Sci. **755**, 73 (1995); J.I. Cirac, P. Zoller, Phys. Rev. A **50**, R2799 (1994).
302. S. Lloyd, Phys. Rev. A **57**, R1473 (1998); R. Laflamme, E. Knill, W.H. Zurek, P. Catasti, S.V.S. Mariappan, Phil.Trans. R. Soc. Lond. A **356**, 1941 (1998).
303. S. Bose, V. Vedral, P.L. Knight, Phys. Rev. A **57**, 822 (1998).
304. M. Zukowski, A. Zeilinger, H. Weinfurter, Entangling photons radiated by independent pulsed source. Ann. NY Acad. Sci. **755**, 91-102 (1995).
305. M.A. Horne, Fortschr. Phys. **46**, 6 (1998).
306. G. Krenn, A. Zeilinger, Phys. Rev. A. **54**, 1793 (1996).
307. Z.Y. Ou and L. Mandel, Violation of Bell's inequality and classical probability in a two-photon correlation experiment. Phys. Rev. Lett. **61**, 50-53 (1988).
308. Y.H. Shih and C.O. Alley, New type of Einstein-Podolsky-Rosen-Bohm experiment using pairs of light quanta produced by optical parametric down conversion. Phys. Rev. Lett. **61**, 2921-2924 (1988).
309. P. Kwiat, P.E. Eberhard, A.M. Steinberger, and R.Y. Chiao, Proposal for a loophole-free Bell inequality experiment. Phys. Rev. A **49**, 3209-3220 (1994).
310. L. De Caro and A. Garuccio, Reliability of Bell-inequality measurements using polarisation correlations in parametric-down-conversion photons. Phys. Rev. A **50**, R2803-R2805 (1994).
311. S. Popescu, L. Hardy, and M. Zukowski, Revisiting Bell's theorem for a class of down-conversion experiments. Phys. Rev. A. **56**, R4353-4357 (1997).
312. M. Zukowski, Violations of local realism in multiphoton interference experiments. quant-ph/9811013.
313. J.-W. Pan, D. Bouwmeester, M. Daniell, H. Weinfurter, and A. Zeilinger, Experimental test of quantum nonlocality in three-photn Greenberger–Horne–Zeilinger entanglement, Nature **403**, 515 (2000).
314. N.D. Mermin, Extreme quantum entanglement in a superposition of macroscopically distinct states. Phys. Rev. Lett. **65**, 1838-1841 (1990).
315. S.M. Roy and V. Singh,Tests of signal locality and Einstein-Bell locality for multiparticle systems. Phys. Rev. Lett. **67**, 2761-2764 (1991).
316. M. Zukowski and D. Kaszlikowski, Critical visibility for N-particle Greenberger-Horne-Zeilinger correlations to violate local realism. Phys. Rev. A **56**, R1682-1685 (1997).
317. The original reference is E. Schmidt, *Zur Theorie der linearen und nicht linearen Integralgleichungen*, Math. Annalen **63**, 433 (1907), in the context of quantum theory see H. Everett III, in *The Many-World Interpretation of Quantum Mechanics*, ed. B.S. DeWitt and N. Graham, Princeton University Press, Princeton, 3 (1973), and H. Everett III, Rev. Mod. Phys. **29**, 454 (1957). A graduate level textbook by A. Peres, *Quantum Theory: Concepts*

and Methods, Kluwer, Dordrecht, (1993), Chapt. 5 includes a brief description of the Schmidt decomposition; A. Ekert and P.L. Knight, Am. J. Phys., **63**, 415 (1995).
318. A. Peres, "Higher order Schmidt Decompositions", lanl-gov e-print server no. 9504006, 1995.
319. J. von Neumann, "Mathematische Grundlagen der Quantenmechanik" (Springer, Berlin, 1932; English Translation, Princeton University Press, Princeton, 1955).
320. M. Horodecki, P. Horodecki, and R. Horodecki, *Mixed-state entanglement and distillation: is there a "bound" entanglement in nature?*, lanl gov e-print quant-ph/9801069.
321. V. Vedral, M.B. Plenio, M.A. Rippin, and P.L. Knight, Phys. Rev. Lett. **78**, 2275 (1997).
322. V. Vedral and M. B. Plenio, Phys. Rev. A **57**, 1619 (1998).
323. C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, and W.K. Wootters, Phys. Rev. A **54**, 3824 (1996).
324. W.K. Wootters, *Entanglement of Formation of an Arbitrary State of Two Qubits*, lanl e-print server quant-ph/9709029, (1997); S. Hill and W.K. Wootters, Phys. Rev. Lett. **78**, 5022 (1997).
325. T. Rockafeller, *Convex Analysis*, Princeton University Press, New Jersey, (1970).
326. N. Gisin, Phys. Lett. **A 210**, 151 (1996), and references therein; A. Peres, Phys. Rev. A **54**, 2685 (1996); M. Horodecki, P. Horodecki, R. Horodecki, Phys. Lett. A **223**, 1 (1996).
327. V. Vedral, M.B. Plenio, K. Jacobs, and P.L. Knight, Phys. Rev. A **56**, 4452 (1997).
328. W.K. Wootters, Phys. Rev. D **23**, 357 (1981).
329. T.M. Cover and J.A. Thomas, *Elements of Information Theory*, Wiley-Interscience,(1991).
330. F. Hiai and D. Petz, Comm. Math. Phys. **143**, 99 (1991).
331. M. Hayashi, *Asymptotic Attainment for Quantum Relative Entropy*, lanl e-print server: quant-ph/9704040 (1997).
332. W.H. Zurek, Physics Today, 36 (October 1991).
333. G.M. Palma, K.-A. Suominen, and A.K. Ekert, Proc. R. Soc. London A. **452**, 567 (1996).
334. D. DiVincenzo, Phys. Rev. A, **50**, 1015 (1995).
335. W. Unruh, Phys. Rev. A, **51**, 992 (1995).
336. D. Loss and D. DiVincenzo, Phys. Rev. A, **57**, 120 (1998).
337. A. Barenco et.al, Phys. Rev. Lett. **74**, 4083 (1995).
338. C. Cohen-Tannoudji, J. Dupont-Roc, and Grynberg, *Atom Photon Interaction*, John Wiley (1992).
339. M. Gross and S. Haroche, Phys. Rep. **93**, 301 (1982).
340. A. Crubellier, S. Liberman, D. Pavolini, and A. Pillet, J. Phys. B, **18**, 3811 (1985).
341. P. Zanardi and M. Rasetti, Phys. Rev. Lett. **79**, 3306 (1997).
342. D.G. Cory, M.D. Price, T.F. Havel, Physica D **120**, 82 (1998).
343. N.A. Gershenfeld and I.L. Chuang, Science, **275**, 350 (1997).
344. P.L. Knight, M.B. Plenio and V. Vedral, Phil. Trans. Roc. Soc. Lond. A, **355**, 2381 (1997).
345. M.B. Plenio and P.L. Knight, Phys. Rev. A, **53**, 2986 (1996).
346. M.B. Plenio and P.L. Knight, Proc. R. Soc. Lond. A, **453**, 2017 (1997).
347. M.B. Plenio and P.L. Knight, *New Developments on Fundamental Problems in Quantum Physics*, edited by M. Ferrero and A. van der Merwe, Kluwer, Dordrecht, 311 (1997).
348. A. Garg, Phys. Rev. Lett. **77**, 964 (1996).

349. R.J. Hughes, D.F.V. James, E.H. Knill, R. Laflamme, and A.G. Petschek, Phys. Rev. Lett. **77**, 3240 (1996).
350. P.W. Shor, in *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, Los Alamitos,* CA IEEE Computer Society Press, New York, 124 (1994).
351. V. Vedral, A. Barenco, and A. Ekert, Phys. Rev. A, **54**, 147 (1996).
352. D. Deutsch, (1993) talk presented at the Rank Prize Funds Mini-Symposium on Quantum Communication and Cryptography, Broadway, England; A. Berthiaume, D. Deutsch and R. Jozsa, in *Proceedings of Workshop on Physics and Computation — PhysComp94*, IEEE Computer Society Press, Dallas, Texas, (1994).
353. A. Barenco, A. Berthiaume, D. Deutsch, A. Ekert, R. Jozsa and C. Macchiavello, SIAM J. Comput. **26**, 1541 (1997).
354. Ash, *Information Theory*, Dover (1996).
355. A. Ekert and C. Macchiavello, Phys. Rev. Lett. **77**, 2585 (1996).
356. R. Laflamme, C. Miquel, J.P. Paz and W.H. Zurek, Phys. Rev. Lett. **77**, 198 (1996).
357. A. Steane, Error correcting codes in quantum theory, Phys. Rev. Lett. **77**, 793 (1995).
358. A. Steane, Multiple particle interference and quantum error correction, Proc. R. Soc. Lond. A, **452**, 2551 (1995).
359. J. Preskill, Reliable quantum computers, Proc. Roy. Soc. Lond. A, **454**, 469 (1998).
360. D. Gottesman, Class of quantum error-correcting codes saturating the quantum Hamming bound, Phys. Rev. A, **54**, 1862 (1996).
361. A.R. Calderbank, E.M. Rains, N.J.A. Sloane and P.W. Shor, Quantum error correction and orthogonal geometry, Phys. Rev. Lett. **78** 405 (1997).
362. A.R. Calderbank, E.M. Rains, P.W. Shor and N.J.A. Sloane, Quantum error correction via codes over $GF(4)$, IEEE Trans. Information Theory **44** 1369 (1998).
363. P.W. Shor, Scheme for reducing decoherence in quantum computer memory, Phys. Rev. A, **52**, R2493 (1995).
364. A.R. Calderbank and P.W. Shor, Good quantum error-correcting codes exist, Phys. Rev. A, **54**, 1098 (1996).
365. E. Knill and R. Laflamme, A theory of quantum error correcting codes, Phys. Rev. A, **55**, 900 (1997).
366. E. Knill and R. Laflamme, Concatenated quantum codes, LANL eprint quant-ph/9608012.
367. P.W. Shor, Fault-tolerant quantum computation, in *Proc. 37th Symp. on Foundations of Computer Science*, (Los Alamitos, CA: IEEE Computer Society Press), pp15-65 (1996).
368. A.M. Steane, Space, time, parallelism and noise requirements for reliable quantum computing, Fortschr. Phys. **46**, 443 (1998). (LANL eprint quant-ph/9708021).
369. D. Aharonov and M. Ben-Or, Fault-Tolerant Quantum Computation With Constant Error Rate, LANL eprint quant-ph/9906129.
370. E. Knill, R. Laflamme and W.H. Zurek, Resilient quantum computation: Error Models and Thresholds, Proc. Roy. Soc. Lond A **454**, 365 (1998); Science **279**, 342 (1998). (LANL eprint quant-ph/9702058).
371. A.M. Steane, Active stabilisation, quantum computation and quantum state synthesis, Phys. Rev. Lett. **78**, 2251 (1997).

372. A.M. Steane, Efficient fault-tolerant quantum computing, Nature, vol. **399**, 124-126 (May 1999). (LANL eprint quant-ph/9809054).
373. D. Gottesman, A theory of fault-tolerant quantum computation, Phys. Rev. A **57**, 127 (1998). (LANL eprint quant-ph/9702029).
374. W.H. Itano et al., Phys. Rev. A, **47**, 3554 (1993).
375. W.J. Wineland et al., Phys. Rev. A, **46**, R6797 (1992).
376. D. J. Wineland et al., Phys. Rev. A, **50**, 67 (1994).
377. J.J. Bollinger et al., Phys. Rev. A, **54**, R4649 (1996).
378. C.W. Gardiner, *Quantum Noise*, Springer–Verlag, Berlin (1991).
379. S.F. Huelga, C. Macchiavello, T. Pellizari, A.K. Ekert, M.B. Plenio and J.I. Cirac, Phys. Rev. Lett. **79**, 3865 (1997).
380. A. Barenco, A. Berthiaume, D. Deutsch, A. Ekert, R. Jozsa and C. Macchiavello, SIAM J. Comput. **26**, 1541 (1997).
381. H.-J. Briegel, W. Dür, J.I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).
382. N. Gisin, Phys. Lett. A **210**, 151 (1996).
383. M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998); Phys. Rev. Lett. **82**, 1056 (1999).
384. E.M. Rains, Phys. Rev. A **60**, 173 (1999).
385. A. Kent, N. Linden, and S. Massar, Los Alamos preprint quant-ph/9802022.
386. G. Giedke, H.-J. Briegel, J.I. Cirac, and P. Zoller, Phys. Rev. A **59**, 2641 (1999).
387. W. Dür, H.-J. Briegel, J.I. Cirac, and P. Zoller, Phys. Rev. A **59**, 169 (1999); ibid. **60**, 729 (1999).
388. B. Huttner, J.D. Gautier, A. Muller, H. Zbinden and N. Gisin, Phys. Rev. A, **54**, 3783 (1996).
389. M. Horodecki P. Horodecki and M. Horodecki. Violating bell inequality by mixed spin 1/2 states: necessary and sufficient condition. Phys. Lett. A, **200**, 340 (1995).
390. C. Macchiavello, Phys. Lett. A **246**, 385 (1998).
391. M. Murao, M.B. Plenio, S. Popescu, V. Vedral and P.L. Knight, Phys. Rev. A **57**, R4075 (1998).
392. N. Linden S. Popescu, Fortsch. Phys. **46**, 567 (1998).
393. S.J. van Enk, J.I. Cirac, and P. Zoller, Phys. Rev. Lett., **78**, 4293 (1997).
394. S.J. van Enk, J.I. Cirac, and P. Zoller, Science, **279**, 205 (1998).
395. J.I. Cirac, et al, Physica Scripta, Proceedings of the Nobel Symposium 104, Modern Studies of Basic Quantum Concepts and Phenomena, Uppsala, Sweden, June 13-17 (1997).
396. R.J. Glauber, In *Frontiers in Quantum Optics*, (eds. E.R. Pike and S. Sarkar), 534, Adam Hilger, Bristol (1986).
397. S.J. van Enk, J.I. Cirac, and P. Zoller, Phys. Rev. Lett. **79**, 5178 (1997).
398. M. Zukowski *et al.*, Phys. Rev. Lett. **71**, 4287 (1993); see also S. Bose *et al.*, Phys. Rev. A, **57**, 822 (1998); J.-W. Pan *et al.*, Phys. Rev. Lett. **80**, 3891 (1998).
399. E. Knill and R. Laflamme, quant/ph-9608012. See also A. Yu. Kitaev, Russ. Math. Surv. **52**, 1191 (1997); D. Aharonov and M. Ben-Or, quant-ph/9611025; C. Zalka, quant-ph/ 9612028.
400. P. Shor, quant-ph/9605011; A.M. Steane, Phys. Rev. Lett. **78**, 2252 (1997). D. Gottesman, Phys. Rev. A **57**, 127 (1998); For a review see, for example, J. Preskill, in *Introduction to Quantum Computation*, ed. by H.K. Lo, S. Popescu and T.P. Spiller.

Предметный указатель

Физика квантовой информации

Квантовая криптография. Квантовая телепортация. Квантовые вычисления.

Под редакцией
Д.Боумейстера, А.Экерта, А.Цайлингера

Перевод с английского С.П. Кулика и Е.А.Шапиро
под редакцией С.П. Кулика и Т.А.Шмаонова

ПОСТМАРКЕТ
МОСКВА
2002

Dirk Bouwmeester
Artur Ekert
Anton Zeilinger (Eds.)

The Physics of Quantum Information

Quantum Cryptography
Quantum Teleportation
Quantum Computation

With 125 Figures

Springer

Список авторов оригинального издания

H. Baldauf
Sect. 5.3
Max–Planck–Institut
für Quantenoptik
Hans–Kopfermann–Str. 1
85748 Garching, Germany

R. Blatt
Sects. 5.2, 5.3
Institut für Experimentalphysik
Universität Innsbruck
Technikerstrasse 25
6020 Innsbruck, Austria

S. Bose
Sect. 3.11
Centre for Quantum Computation
Clarendon Laboratory
University of Oxford
OX1 3PU Oxford, England

D. Bouwmeester
Chap. 1, Sects. 3.1–3.3, 3.5–3.10, 6.3
Centre for Quantum Computation
Clarendon Laboratory
University of Oxford
OX1 3PU Oxford, England

H.-J. Briegel
Sects. 6.2, 8.2, 8.6, 8.7
Sektion Physik
Ludwig–Maximilians–Universität
Theresienstrasse 37
80333 München, Germany

M. Brune
Sect. 5.2
Laboratoire Kastler Brossel
Département de Physique
de l'Ecole Normale Supérieure
24 rue Lhomond
75231 Paris, Cedex 05, France

J.I. Cirac
Sects. 4.3, 6.2, 8.6, 8.7
Institut für Theoretische Physik
Universität Innsbruck
Technikerstrasse 25
6020 Innsbruck, Austria

M. Daniell
Sect. 6.3
Institut für Experimentalphysik
Universität Wien
Boltzmanngasse 5
1090 Wien, Austria

D. Deutsch
Sect. 4.1
Centre for Quantum Computation
Clarendon Laboratory
University of Oxford
OX1 3PU Oxford, England

W. Dür
Sects. 8.6, 8.7
Institut für Theoretische Physik
Universität Innsbruck
Technikerstrasse 25
6020 Innsbruck, Austria

A. Ekert
Chap. 2, Sects. 4.1, 7.2, 7.6
Centre for Quantum Computation
Clarendon Laboratory
University of Oxford
OX1 3PU Oxford, England

S.J. van Enk
Sects. 6.2, 8.6
Norman Bridge Laboratory of Physics
California Institute
of Technology 12-22
Pasadena, California 91125, USA

J. Eschner
Sects. 5.2, 5.3
Institut für Experimentalphysik
Universität Innsbruck
Technikerstrasse 25
6020 Innsbruck, Austria

N. Gisin
Chap. 2, Sects. 3.4, 8.3
University of Geneva
Group of Applied Physics
20 Rue de l'Ecole de Médecine
1211 Geneva 4, Switzerland

S. Haroche
Sect. 5.2
Laboratoire Kastler Brossel
Département de Physique
de l'Ecole Normale Supérieure
24 rue Lhomond
75231 Paris, Cedex 05, France

S.F. Huelga
Sect. 7.6
Departamento de Fisica
Universidad de Oviedo
Calvo Sotelo s/n.
33007 Oviedo, Spain

B. Huttner
Chap. 2, Sect. 8.3
University of Geneva
Group of Applied Physics
20 Rue de l'Ecole de Médecine
1211 Geneva 4, Switzerland

H. Inamori
Chap. 2
Centre for Quantum Computation
Clarendon Laboratory
University of Oxford
OX1 3PU Oxford, England

J.A. Jones
Sect. 5.4
Centre for Quantum Computation
Clarendon Laboratory
University of Oxford
OX1 3PU Oxford, England

R. Jozsa
Sect. 4.2
Department of Computer Science
University of Bristol
Merchant Venturers Building
Woodland Road
BS8 1UB Bristol, England

P.L. Knight
Sects. 3.11, 6.4, 7.3, 8.5
Optics Section
Blackett Laboratory
Imperial College London
London SW7 2BZ, England

W. Lange
Sect. 5.3
Max–Planck–Institut
für Quantenoptik
Hans–Kopfermann–Str. 1
85748 Garching, Germany

D. Leibfried
Sect. 5.2
Institut für Experimentalphysik
Universität Innsbruck
Technikerstrasse 25
6020 Innsbruck, Austria

C. Macchiavello
Sects. 7.4, 7.6, 8.4
Dipartimento di Fisica "A.Volta"
and INFM-Unité di Pavia
via Bassi 6
27100 Pavia, Italy

M. Murao
Sect. 8.5
Optics Section
Blackett Laboratory
Imperial College London
London SW7 2BZ, England

H.C. Nägerl
Sects. 5.2, 5.3
Institut für Experimentalphysik
Universität Innsbruck
Technikerstrasse 25
6020 Innsbruck, Austria

G.M. Palma
Sects. 7.2, 7.4
Dipartimento di Scienze Fisiche
ed Astronomiche & unita'INFM
via Archirafi 36
90123 Palermo, Italy

J.-W. Pan
Sects. 3.7, 3.10, 6.3
Institut für Experimentalphysik
Universität Wien
Boltzmanngasse 5
1090 Wien, Austria

M.B. Plenio
Sects. 6.4, 7.3, 7.6, 8.5
Optics Section
Blackett Laboratory
Imperial College London
London SW7 2BZ, England

S. Popescu
Sect. 8.5
5BRIMS Hewlett–Packard
Laboratories
Stoke Gifford
Bristol BS12 6QZ, England

J.F. Poyatos
Sect. 4.3
Centre for Quantum Computation
Clarendon Laboratory
University of Oxford
OX1 3PU Oxford, England

J.-M. Raimond
Sect. 5.2
Laboratoire Kastler Brossel
Département de Physique
de l'Ecole Normale Supérieure
24 rue Lhomond
75231 Paris, Cedex 05, France

J.G. Rarity
Sect. 3.4
DERA Malvern
St. Andrews Road, Malvern
Worcester WR14 3PS, England
and
Centre for Quantum Computation
Clarendon Laboratory
University of Oxford
OX1 3PU Oxford, England

F. Schmidt-Kaler
Sects. 5.2, 5.3
Institut für Experimentalphysik
Universität Innsbruck
Technikerstrasse 25
6020 Innsbruck, Austria

A. Steane
Sect. 7.5
Centre for Quantum Computation
Clarendon Laboratory
University of Oxford
OX1 3PU Oxford, England

K.-A. Suominen
Sect. 7.2
Helsinki Institute of Physics
PL 9, FIN-00014 Helsingin
Yliopisto, Finland

V. Vedral
Sects. 3.11, 6.4, 8.5
Centre for Quantum Computation
Clarendon Laboratory
University of Oxford
OX1 3PU Oxford, England

G. Weihs
Sect. 3.4
Institut für Experimentalphysik
Universität Wien
Boltzmanngasse 5
1090 Wien, Austria

H. Weinfurter
Chap. 2, Sects. 3.1–3.3, 3.5–3.7, 3.10, 6.3
Sektion Physik
Ludwig–Maximilians–Universität
München
Schellingstr. 4/III
80799 München, Germany

H. Walther
Sect. 5.3
Max–Planck–Institut
für Quantenoptik
Hans–Kopfermann–Str. 1
85748 Garching, Germany

A. Zeilinger
Chap. 1, Sects. 3.1–3.3, 3.5–3.7, 3.10, 6.3
Institut für Experimentalphysik
Universität Wien
Boltzmanngasse 5
1090 Wien, Austria

P. Zoller
Sects. 4.3, 6.2, 8.6, 8.7
Institut für Theoretische Physik
Universität Innsbruck
Technikerstrasse 25
6020 Innsbruck, Austria

Оглавление