ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ

МОСКОВСКИЙ ИНЖЕНЕРНО-ФИЗИЧЕСКИЙ ИНСТИТУТ
(ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ)

С.Д. Кулик, А.В. Берков, В.П. Яковлев

ВВЕДЕНИЕ В ТЕОРИЮ КВАНТОВЫХ ВЫЧИСЛЕНИЙ

(методы квантовой механики в кибернетике)
Книга 2

Рекомендовано УМО "Ядерные физика и технологии"
в качестве учебного пособия
для студентов высших учебных заведений

Москва 2008

УДК 530.145:007(075)
ББК 22.31я7+32.81я7
К 90

Кулик С.Д., Берков А.В., Яковлев В.П. Введение в теорию квантовых вычислений (методы квантовой механики в кибернетике): учебное пособие.– В 2 кн.– Кн. 2.– М.: МИФИ, 2008.–532 с.

Изложены основные понятия и методы теории квантовых вычислений — новой дисциплины, сформировавшейся на стыке квантовой механики и кибернетики. Представлены начальные основы квантовой схемотехники. На многочисленных примерах детально рассмотрены основные идеи, а также даны решения задач прямого и обратного анализа квантовой схемы и задачи синтеза квантовой схемы, удовлетворяющей требуемым условиям.

Пособие в основном ориентировано на студентов МИФИ кафедр “Теоретическая ядерная физика” и “Управляющие интеллектуальные системы”, изучающих не только квантовую механику, но и теорию принятия решений, и схемотехнику вычислительных устройств.

В первой книге представлены начала волновой кибернетики, отражающие важные сведения из классической кибернетики, необходимые для понимания квантовых вычислений.

Во второй книге представлены основы квантовых вычислений.

Пособие подготовлено в рамках Инновационной образовательной программы.

Рецензент
д-р физ.-мат. наук, профессор С. Г. Рубин

ISBN 978-5-7262-0976-0
ISBN 978-5-7262-0997-5 (кн. 2)

ОГЛАВЛЕНИЕ

Во многих источниках есть ошибки, опечатки, упущения и т.п. дефекты. Конечно, и эта работа не исключение. В любом случае будем рады информации об обнаруженных опечатках и неточностях.

Авторы

sedmik@mail.ru
sedmik@hotmail.com

ВВЕДЕНИЕ

За последние два–три десятилетия сформировалась новая область *знания* о природе, объединившая в себе квантовую механику и теорию информации. К этой междисциплинарной науке относятся такие понятия как *«квантовая информация»* и *«квантовые вычисления»*. Они обозначают принципиально иной, квантовый подход – в отличие от традиционного классического – к самому понятию информации и к законам, позволяющим этой информацией манипулировать, т.е записывать, хранить, обрабатывать, передавать, а также производить вычисления.

В ближней ретроспективе отправным пунктом можно считать доклад *Ричарда Фейнмана* «Моделирование физики на компьютерах», который был сделан в 1981 г. в Массачусетском технологическом институте (MIT) и опубликован в 1982 г. вместе со статьей «Квантово-механические компьютеры» (Int. J. Theor. Phys., 1982, V.21, P.467-488), и работу *Дэвида Дойча* «Квантовая теория, принцип Чёрча – Тьюринга и универсальный квантовый компьютер» (Proc. R.Soc. Lond., 1985, V. A400, P. 97-117). Эти работы положили начало пониманию того факта, что вычисления, основанные на законах квантовой механики, или, говоря более общим языком, процессы манипулирования квантовой информацией могут быть гораздо (например, даже экспоненциально) быстрее и эффективнее, чем для классической информации. Количественный аспект этого утверждения является следствием нового качества, связанного с понятием квантовой информации. В статье «Информация по сути физична» (Physics Today, May 1991, P.23-29) *Рольф Ландауэр* высказал важное концептуальное положение, что *информация*, вообще говоря, *не независима* от физических процессов, которые используются для ее записи и обработки. Законы классической информации никак не связаны с физическими законами, которые определяют поведение устройств, применяемых для манипулирования собственно информацией. Это относится и к существующим классическим компьютерам. Ситуация становится совершенно иной, когда носителями информации являются квантовые системы, а роль элементарной ячейки для записи единицы информации играет, например, спиновое состояние ядра или электронные состоя-

ния двухуровневого атома. Такие состояния и, следовательно, представляемая ими информация подчиняются законам квантовой механики.

На сегодняшний день квантовая информатика синтезирует целый ряд актуальных областей современной фундаментальной и прикладной физики, дискретной математики и кибернетики, а также передовые достижения в области квантовых технологий. Усилия многих мировых научных групп, сконцентрированные в этих направлениях исследований, привели к целому ряду впечатляющих результатов, которые экспериментально подтверждают фундаментальные основы квантовой информатики и открывают реалистические перспективы ее дальнейшего развития. Поскольку границы этой области исследований оказываются чрезвычайно обширными и включают много взаимосвязанных дисциплин, то путешествие по ней удобно начать, взглянув на схематическую карту, представленную на рис.**В1**. По этой схеме, не претендующей на полноту, можно составить представление о том, какова роль и место вопросов, затронутых в данной книге.

Сейчас представляется совершенно ясным, что изучение основ квантовой информатики и квантовых вычислений должно войти как обязательный компонент в систему подготовки как физиков, так и специалистов по теории информации, которых готовит МИФИ и которым адресуется данная книга. Авторы ставили своей целью написать учебник, который, с одной стороны, адекватным образом представлял бы достаточно широкий круг вопросов, связанных с этой областью, а с другой стороны, был бы без ущерба для научной строгости доступным для понимания как студентам физических специальностей, так и студентам, обучающимся в области кибернетики и схемотехники вычислительных устройств. Определенная разнонаправленность этих «граничных условий» неизбежно диктовала и отбор материала, а также метод и стиль изложения. Поскольку основной задачей было дать введение в предмет, то целый ряд важных вопросов, таких, например, как коды коррекции квантовых ошибок или реализация квантовых логических элементов на основе метода ядерного магнитного резонанса, не вошли в данную книгу. В методическом плане изложение ведется в двух плоскостях. Представлен подход к проблемам квантовых вычислений, отталкивающийся от кибернетики, от фунда-

ментального здания классической теории информации, в которую эмпирическим образом вводятся элементы аппарата квантовой механики, выступающего как формальная математическая структура. По мнению авторов, это поможет кибернетику легче войти в новый для него мир квантовых законов. С другой стороны, фундаментальные понятия квантовой информации излагаются на основе принципов квантовой механики как физической теории реального квантового мира, что позволит студенту-физику освоить начала кибернетики, необходимые для изучения квантовых вычислений.

Опыт создания *информационных систем* (ИС) показал, что современный специалист в области ИС и, в частности, *автоматизированных систем обработки информации и управления* (АСОИУ) неизбежно столкнется с проблемой принятия решения, а также с необходимостью разрабатывать эффективный алгоритм для решения заданной технической задачи. Ему следует быть готовым к этому. А для того чтобы разрабатывать эффективные алгоритмы, он должен знать, как это можно сделать.

Современные исследования убедительно показывают, что элементная база вычислительных средств, построенная на квантовых объектах, обеспечит возможность реализовывать не просто эффективные, а очень эффективные алгоритмы для решения практических задач. Инструментарий квантовых вычислений предоставляет для квантовой схемотехники широкие возможности эффективного решения очень важных для практики задач, которые либо слишком трудны, либо просто «неподвластны» классическим алгоритмам. Квантовая механика открыла возможность разработки квантовых алгоритмов для выполнения квантовых вычислений. Именно основам квантовых вычислений и посвящено данное пособие.

Авторы благодарны студентам кафедры “Теоретическая ядерная физика” и кафедры “Управляющие интеллектуальные системы” МИФИ, которые были первыми слушателями, и на них апробировалась часть материалов, представленных в пособии. ВПЯ благодарит П.А. Жукова и К.Е. Городничева за техническую помощь в оформлении рукописи. СДК признателен А.В. Жижилеву, и П.В. Чамкину за дополнительную проверку примеров из главы 5.

В пособии в книге 2 главу 1 написал *А.В. Берков*, главы 2, 3, 4 — *В.П. Яковлев,* главу 5 (и главу 1 в книге 1) — *С.Д. Кулик*.

Авторы

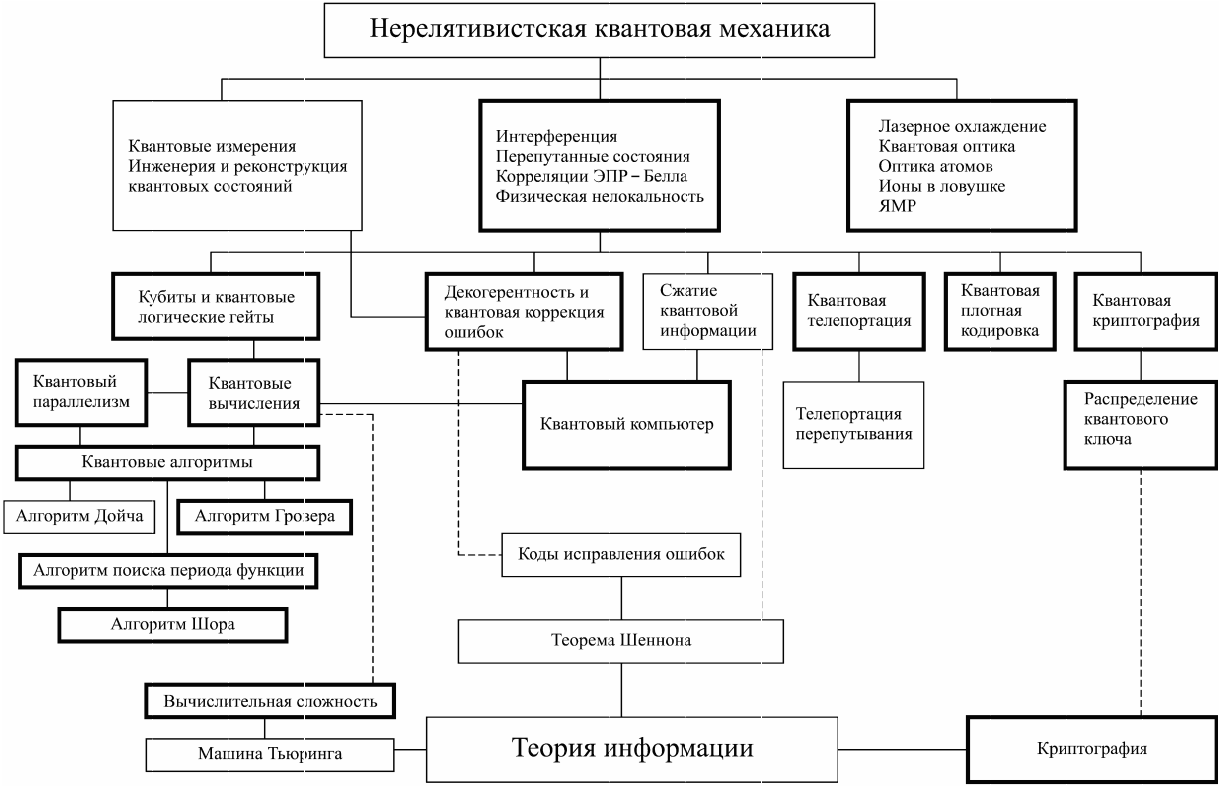

Нерелятивистская квантовая механика
Квантовые измерения
Инженерия и реконструкция квантовых состояний
Интерференция
Перепутанные состояния
Корреляции ЭПР – Белла
Физическая нелокальность
Лазерное охлаждение
Квантовая оптика
Оптика атомов
Ионы в ловушке
ЯМР
Кубиты и квантовые логические гейты
Декогерентность и квантовая коррекция ошибок
Сжатие квантовой информации
Квантовая телепортация
Квантовая плотная кодировка
Квантовая криптография
Квантовый параллелизм
Квантовые вычисления
Квантовый компьютер
Телепортация перепутывания
Распределение квантового ключа
Квантовые алгоритмы
Алгоритм Дойча
Алгоритм Гровера
Коды исправления ошибок
Алгоритм поиска периода функции
Алгоритм Шора
Теорема Шеннона
Вычислительная сложность
Машина Тьюринга
Теория информации
Криптография

Рис. В1

«…я смело могу сказать, что квантовой механики никто не понимает…»

Р. Фейнман

Основные понятия квантовой механики

Г л а в а 1

ОСНОВНЫЕ ПОНЯТИЯ КВАНТОВОЙ МЕХАНИКИ

Содержание

Возникновение квантовой механики. Поляризация фотонов. Основные принципы. Фундаментальные принципы квантовой механики. Кэт-пространство. Бра-пространство. Операторы. Внешнее произведение. Собственные значения и собственные векторы. Наблюдаемые. Измерения. Средние значения. Вырождение. Совместные наблюдаемые. Соотношение неопределенностей. Непрерывный спектр. Чистые и смешанные состояния. Матрица плотности.

1.1. Почему возникла квантовая механика?

Начало новой эры в физике положила работа Макса Карла Эрнста Людвига Планка, опубликованная в декабре 1900 г., в последние дни уходящего XIX в. Планк занимался поисками формулы, правильно описывающей спектральное распределение интенсивности излучения *абсолютно черного тела*, т. е. тела, поглощающего все падающее на него излучение. Как было доказано еще в середине XIX в. на основании самых общих термодинамических рассуждений, это распределение должно зависеть только от абсолютной температуры тела T. Методами статистической термодинамики из общих законов взаимодействия между веществом и излучением можно вывести классическую формулу для спектрального распределения интенсивности излучения. Эта формула находится в резком противоречии с опытом.

Планку удалось устранить это противоречие, но ценой отказа от классического закона взаимодействия между веществом и излучением. Он выдвинул гипотезу о том, что обмен энергией между веществом и излучением происходит не непрерывным образом, а путем передачи дискретных и неделимых порций энергии, или *квантов энергии*. Планк показал, что квант энергии пропорционален частоте ν излучения: $\varepsilon = h\nu$, и получил согласующееся с опытом выражение для спектрального распределения, выбирая соответствующим образом постоянную пропорциональности. Эта постоянная h с тех пор носит название *постоянной Планка*. В даль-

нейшем мы будем использовать технически более удобную постоянную $\hbar = h/(2\pi)$.

При появлении гипотезы Планка она казалась неприемлемой, большинство физиков видело в ней только математический прием, который удастся в дальнейшем объяснить на основе классических представлений. Однако гипотеза Планка была в дальнейшем подтверждена и дополнена целой серией опытов, позволившей проанализировать элементарные процессы и доказать скачкообразность и прерывность эволюции физических систем на микроуровне.

К 20-м гг. XX в. нарастающее количество экспериментальных фактов ясно демонстрировало необходимость отказа от классической физики.

1. *Аномальная стабильность атомов и молекул*. В опытах Резерфорда была установлена планетарная модель атома, согласно которой электроны вращаются по орбитам вокруг центрального ядра. Однако, как утверждает классическая физика, электрон, вращающийся вокруг ядра, должен терять энергию за счет излучения и постепенно падать по спирали на ядро. Опыт не подтверждает этот вывод.

2. *Аномально низкие значения удельных теплоемкостей атомов и молекул*. Согласно теореме равнораспределения классической физики, каждая степень свободы атомной или молекулярной системы должна вносить величину $R/2$ в молярную теплоемкость, где R — газовая постоянная. На самом деле, создается впечатление, что вклад вносят только трансляционные и некоторые вращательные степени свободы, а колебательные степени свободы, похоже, не вносят никакого вклада. Кстати, эта фундаментальная проблема классической физики была известна и принималась во внимание еще в середине XIX в. Поэтому истории о том, что физики в начале XX в. считали, что классическая физика сумела объяснить все, за исключением нескольких мелочей, являются в значительной степени апокрифическими (см. *Фейнмановские лекции по физике*, гл. 40, §6).

3. *Ультрафиолетовая катастрофа*. Согласно классической физике, плотность энергии электромагнитного поля в вакууме бесконечна благодаря расходимости энергии, переносимой коротковолновыми модами. Экспериментально такая расходимость не на-

блюдается, и полная плотность энергии конечна.

4. *Корпускулярно–волновой дуализм*. Классическая физика имеет дело с волнами *или* частицами. Однако различные эксперименты (например, интерференция света, фотоэффект, дифракция электронов, эффект Комптона) ясно показывают, что волны иногда ведут себя как потоки частиц, а потоки частиц ведут себя как волны. Это совершенно необъяснимо в рамках классической физики.

Итак, физика начала XX в. была готова к решительным переменам. Следующими шагами после гипотезы Планка стали теория фотоэффекта Эйнштейна, полуклассическая теория строения атома Бора, затем возникли гипотеза де Бройля, матричная механика Гейзенберга, Борна и Иордана, волновое уравнение Шрёдингера и т. д. Взрыв интеллектуальной активности позволил в период с 1923 по 1930 гг. сформулировать основные постулаты новой науки и получить важнейшие практические результаты.

Одновременно выяснилось, что квантовая механика кардинальным образом отличается от классической физики. Понимание основных законов квантовой механики требует отказа от общепринятых классических представлений. На смену им приходят вероятностные представления. Одновременно требуют изменения привычные взгляды на причинность. Понимание этих особенностей квантовой механики далось не сразу и потребовало нескольких лет научных споров, в том числе таких корифеев как Бор и Эйнштейн. Сложившаяся к середине 30-х гг. так называемая «копенгагенская интерпретация» квантовой механики была принята не сразу и не всеми. Даже в наши дни продолжаются жаркие споры о том, как следует понимать тот странный и удивительный мир, законы которого носят название квантовой механики.

1.2. Поляризация фотонов. Основные принципы

Экспериментально известно, что когда для выбивания фотоэлектронов используется плоскополяризованная электромагнитная волна, у электронов возникает предпочтительное направление эмиссии. Ясно, что поляризационные свойства света, которые обычно связываются с его волновой природой, также распространяются и на корпускулярную природу. В частности, можно припи-

сать определенную поляризацию каждому отдельному фотону в пучке света.

Рассмотрим следующий хорошо известный эксперимент. Пучок плоскополяризованного света проходит через поляризатор (например, поляроидную пленку), обладающий тем свойством, что он пропускает только свет, плоскость поляризации которого перпендикулярна оптической оси поляризатора. Согласно классической теории электромагнитных волн, если световой пучок поляризован перпендикулярно оптической оси поляроида, то весь свет проходит, если же пучок поляризован параллельно оптической оси поляроида, то свет не проходит вовсе. Наконец, если свет поляризован под углом α к оптической оси, то проходит доля интенсивности пучка, равная $\sin^2\alpha$ (закон Малюса). Рассмотрим теперь эти эксперименты с точки зрения представлений о свете как об отдельных фотонах.

Плоскополяризованный в каком-то направлении пучок света состоит из потока фотонов, каждый из которых плоскополяризован в том же направлении. Подобная интерпретация не вызывает никаких трудностей, если плоскость поляризации лежит параллельно или перпендикулярно оптической оси поляроида. В первом случае ни один из фотонов не проходит через поляроидную пленку, во втором проходят все фотоны. Но что произойдет в случае падения пучка, поляризованного под углом к оптической оси?

Этот вопрос задан не очень точно. Переформулируем его как вопрос, относящийся к результату некоторого эксперимента, который мы можем осуществить. Предположим, что мы пускаем на поляроидную пленку один фотон, а затем смотрим, появился ли этот фотон по другую сторону от пленки. Возможные результаты эксперимента: либо наблюдается целый фотон, энергия которого равна энергии падающего фотона, либо фотон не наблюдается вообще. Любой фотон, прошедший через пленку, должен быть поляризован перпендикулярно оптической оси. Кроме того, невозможно представить (в рамках физики), что по другую сторону пленки будет наблюдаться часть фотона. Если мы много раз повторим описанный эксперимент, то в среднем доля $\sin^2\alpha$ фотонов пройдет через пленку, а доля $\cos^2\alpha$ поглотится. Таким образом, мы заключаем, что фотон с *вероятностью* $\sin^2\alpha$ проходит через пленку как фотон, поляризованный в плоскости, перпендикулярной оптиче-

ской оси, а с вероятностью $\cos^2\alpha$ поглощается пленкой. Эти значения вероятностей приводят к правильным классическим пределам для пучка, содержащего большое количество фотонов.

Заметим, что нам удалось во всех случаях сохранить индивидуальность фотонов, отвергнув детерминизм классической теории и приняв фундаментально вероятностный подход. У нас нет способов узнать, собирается ли отдельный поляризованный под углом фотон пройти через пленку или поглотиться. Мы только знаем вероятность каждого события. Это довольно неопределенное утверждение, однако вспомним, что *состояние* фотона полностью задается его энергией, направлением распространения и поляризацией. Если мы проводим эксперименты, используя монохроматический свет, падающий по нормали на поляроидную пленку, с определенной поляризацией под углом к оптической оси, тогда состояние каждого отдельного фотона в пучке полностью задано, и ничто не мешает однозначно определить, пройдет ли фотон через пленку или нет.

Предыдущее обсуждение результатов эксперимента с отдельным поляризованным под углом фотоном, падающим на поляроидную пленку, отвечает на все вопросы, которые могут быть на законном основании заданы относительно судьбы фотона, достигшего пленки. Вопросы типа «Что решает, пройдет ли фотон через пленку или нет? Как изменится направление поляризации фотона?»» или, что еще хуже, «Кто это решает?» являются незаконными, так как они не связаны с результатом возможного эксперимента. Тем не менее, требуются некоторые дополнительные рассуждения, чтобы результаты этого эксперимента были скоррелированы с результатами других экспериментов, которые можно осуществить, используя фотоны.

Предполагается, что поляризованный под углом к оптической оси фотон можно рассматривать как находящийся частично в состоянии поляризации, параллельной оси, а частично — в состоянии поляризации, перпендикулярной оси. Иными словами, состояние поляризации под углом к оси есть определенная *суперпозиция* двух *состояний* параллельной и перпендикулярной поляризаций. Так как в нашем эксперименте ориентация оптической оси никак не выделена, мы должны заключить, что любое состояние поляриза-

ции можно рассматривать как суперпозицию двух взаимно перпендикулярных состояний поляризации.

Когда мы сталкиваем фотон с поляроидной пленкой, мы осуществляем над фотоном *наблюдение*. На самом деле, мы наблюдаем, поляризован ли фотон параллельно или перепендикулярно оптической оси. Результат осуществления этого наблюдения состоит в том, чтобы заставить фотон перейти полностью в состояние с параллельной или перпендикулярной поляризацией. Иными словами, фотон должен внезапно перескочить из состояния, являющегося смесью двух базисных состояний, в состояние, в котором у фотона поляризация точно определена (либо параллельно, либо перпендикулярно оси). Невозможно предсказать, в какое из двух состояний он перескочит, и это определяется вероятностными законами. Если фотон перескакивает в состояние с параллельной поляризацией, он поглощается. В противоположном случае он проходит через пленку. Заметим, что в этом примере введение в задачу недетерминированности ясно связано с актом наблюдения. Иными словами, недетерминированность возникает в результате неизбежного возмущения состояния, связанного с актом наблюдения.

1.3. Фундаментальные принципы квантовой механики

В рассмотренном примере с фотоном, проходящим через поляроидную пленку, нет ничего особенного. В точности такие же заключения можно получить, изучая другие простые эксперименты (интерференция фотонов, опыт Штерна–Герлаха и пр.) Изучение этих простых экспериментов позволяет сформулировать ряд фундаментальных принципов квантовой механики.

1. *Бритва Дирака*. Квантовая механика может отвечать только на вопросы, связанные с результатами возможных экспериментов. Любые другие вопросы лежат вне сферы физики.

2. *Принцип суперпозиции состояний*. Любая микроскопическая система (например, атом, молекула или частица) в данном состоянии может рассматриваться как находящаяся частично в каждом из двух или более других состояний. Иными словами, любое состояние можно рассматривать как суперпозицию двух или более других состояний. Такие суперпозиции можно реализовать бесконечным числом разных способов.

3. *Принцип недетерминированности*. Наблюдение, производимое над микроскопической системой, заставляет ее перескочить в одно или более конкретное состояние (которые связаны с типом наблюдения). Невозможно предсказать, в какое конечное состояние перейдет конкретная система, однако можно предсказать вероятность перехода данной системы в данное конечное состояние.

Первый из этих принципов был сформулирован в 1920-е гг. (в наиболее ясной форме это сделал П. Дирак), чтобы уйти от ужасных вопросов типа «Как может система перепрыгивать из одного состояния в другое?» или «Как система решает, в какое состояние ей перепрыгнуть?» Как мы увидим далее, второй принцип есть основа математической формулировки квантовой механики. Третий принцип все еще довольно туманен. Необходимо расширить его так, чтобы мы научились предсказывать, в какие возможные состояния может перескочить система после конкретного типа наблюдений, а также чему равна вероятность перехода системы из одного конкретного состояния в другое.

1.4. Кэт-пространство

Этим разделом мы начинаем изучение основ математического аппарата квантовой механики.

Рассмотрим микроскопическую систему, составленную из частиц или тел с определенными свойствами (масса, момент инерции, заряд и пр.), которые взаимодействуют согласно определенному силовому закону. Существуют различные возможные движения частиц или тел, совместимые с заданными силовыми законами. Назовем каждое такое движение *состоянием* системы. Согласно принципу суперпозиции состояний любое заданное состояние может рассматриваться как суперпозиция двух или более других состояний. Следовательно, состояния должны быть связаны с математическими величинами определенного типа, которые можно складывать, получая при этом другие величины того же типа. Наиболее очевидным примером подобных величин являются *векторы*.

Рассмотрим конкретную микроскопическую систему в определенном состоянии, которое мы обозначим A, например, фотон с

определенными значениями энергии, импульса и поляризации. Можно рассматривать это состояние как определенный вектор, который мы также обозначим A, лежащий в определенном векторном пространстве, причем другие элементы пространства представляют все другие возможные состояния системы. Такое пространство называется *кэт-пространством* (по предложению Дирака). Вектор состояния по соглашению записывается как

$$|A\rangle. \tag{1.1}$$

Предположим, что состояние A является на самом деле суперпозицией двух различных состояний B и C. В кэт-пространстве связь этих состояний записывается как

$$|A\rangle = |B\rangle + |C\rangle, \tag{1.2}$$

где $|B\rangle$ — вектор, связанный с состоянием B и т. д. Например, состояние $|B\rangle$ может представлять фотон, распространяющийся в направлении оси z и поляризованный вдоль оси x, а состояние $|C\rangle$ может представлять аналогичный фотон, поляризованный вдоль оси y. В этом случае сумма двух таких состояний представляет фотон, плоскость поляризации которого составляет угол 45° с осями x и y (по аналогии с классической физикой). Такое состояние представляется суммой $|B\rangle + |C\rangle$ в кэт-пространстве.

Предположим, что мы хотим построить состояние, плоскость поляризации которого составляет произвольный угол α с осью x. Это можно сделать путем подходящей суперпозиции состояний B и C, взятых с нужным весом. По аналогии с классической физикой, мы выбираем состояние B с весом $\cos\alpha$, а состояние C — с весом $\sin\alpha$. Новое состояние задается суммой

$$\cos\alpha\,|B\rangle + \sin\alpha\,|C\rangle \tag{1.3}$$

в кэт-пространстве. Заметим, что мы не получим нового состояния,

если возьмем суперпозицию состояния с самим собой. Например, суперпозиция поляризованного вдоль оси *y* фотона с таким же фотоном (с той же энергией и импульсом) описывает тот же фотон. Отсюда следует, что кэт-вектор

$$c_1 \left| A \right\rangle + c_2 \left| A \right\rangle = (c_1 + c_2) \left| A \right\rangle \qquad (1.4)$$

соответствует тому же состоянию, что и $\left| A \right\rangle$. Следовательно, кэт-векторы отличаются от обычных векторов тем, что их величины или длины физически несущественны. Все состояния системы находятся в одно-однозначном соответствии со всеми возможными направлениями векторов в кэт-пространстве, причем не делается никакого различия между кэт-векторами $\left| A \right\rangle$ и $-\left| A \right\rangle$. Правда, существует одно исключение. Если $c_1 + c_2 = 0$, то результат суперпозиции — это отсутствие состояния. Оно представляется нулевым вектором $\left| 0 \right\rangle$ в кэт-пространстве. Нулевой вектор обладает довольно очевидным свойством:

$$\left| A \right\rangle + \left| 0 \right\rangle = \left| A \right\rangle \qquad (1.5)$$

для любого вектора $\left| A \right\rangle$. Тот факт, что кэт-векторы, направленные в одну сторону, представляют одно и то же состояние, тесно связан с *квантованием* материи, т. е. с тем, что она представляется в виде более неделимых групп, называемых фотонами, электронами, атомами и т. д. Если мы наблюдаем микроскопическую систему, то или видим состояние (т. е. фотон, атом, молекулу и т. п.), или не видим ничего, но ни при каких условиях мы не можем видеть долю состояния или кратное число состояний. В классической физике, если наблюдаем волну, то ее амплитуда может принимать любое значение от нуля до бесконечности. Таким образом, если бы мы описывали классическую волну вектором, то его величина или длина соответствовала бы амплитуде волны, а направление — частоте или длине волны, так что два вектора разной длины, направленные в одну сторону, представляли бы различные состояния волны.

Как следует из формулы (1.3), любое состояние фотона с плоской поляризацией можно представить как линейную суперпозицию двух ортогональных состояний поляризации с весами, являющимися вещественными числами. Предположим, что мы хотим построить состояние фотона с циркулярной поляризацией. Из классической физики известно, что циркулярно поляризованная волна есть суперпозиция двух волн равной амплитуды, плоскополяризованных в ортогональных направлениях и *сдвинутых по фазе* на 90°. Это означает, что циркулярно поляризованный фотон есть суперпозиция с равными весами фотона, поляризованного вдоль оси x (состояние B), и фотона, поляризованного вдоль оси y (состояние C), при условии, что состояние C сдвинуто по фазе на 90° относительно состояния B. По аналогии с классической физикой, мы можем использовать комплексные числа для одновременного описания веса и относительной фазы в линейной суперпозиции. Так, циркулярно поляризованный фотон представляется как

$$\left|B\right\rangle + i\left|C\right\rangle \tag{1.6}$$

в кэт-пространстве. В общем случае, эллиптически поляризованный фотон представляется вектором

$$c_1\left|B\right\rangle + c_2\left|C\right\rangle, \tag{1.7}$$

где c_1 и c_2 — комплексные числа. Мы приходим к выводу, что если кэт-пространство должно правильно представлять взаимосвязи между возможными состояниями микроскопической системы, это пространство должно быть *комплексным векторным пространством*.

Предположим, что кэт-вектор $\left|R\right\rangle$ линейно выражается через кэт-векторы $\left|A\right\rangle$ и $\left|B\right\rangle$, так что

$$\left|R\right\rangle = c_1\left|A\right\rangle + c_2\left|B\right\rangle. \tag{1.8}$$

Мы говорим, что $\left|R\right\rangle$ *линейно зависит* от $\left|A\right\rangle$ и $\left|B\right\rangle$. Отсюда сле-

дует, что состояние R может рассматриваться как линейная суперпозиция состояний A и B. Поэтому можно также сказать, что состояние R зависит от состояний A и B. На самом деле, любой кэт-вектор (или состояние), который линейно выражается через другие кэт-векторы (или состояния), называется *линейно зависимым* от них. Если же ни один из кэт-векторов не выражается линейно через другие кэт-векторы, то множество таких кэт-векторов называется множеством *линейно независимых* векторов.

Размерность обычного векторного пространства определяется как число содержащихся в этом пространстве линейно независимых векторов. Аналогично, размерность кэт-пространства эквивалентна числу содержащихся в нем линейно независимых кэт-векторов. Эти векторы называют *базисными* векторами, а их совокупность — *базисом*. Таким образом, кэт-пространство, представляющее возможные состояния поляризации фотона, распространяющегося в направлении оси z, двумерно (два линейно независимых базисных вектора соответствуют фотонам, линейно поляризованным вдоль осей x и y). Некоторые микроскопические системы имеют конечное число независимых состояний (например, спиновые состояния электрона в магнитном поле). Если существуют N линейно независимых состояний, то возможные состояния системы представляются как векторы в N-мерном кэт-пространстве. Ряд микроскопических систем обладает счетным бесконечным числом независимых состояний (например, частица в бесконечно глубокой одномерной потенциальной яме). Возможные состояния такой системы представляются векторами кэт-пространства бесконечной счетной размерности. Такое пространство можно рассматривать более или менее так же, как и конечномерное пространство. К сожалению, ряд микроскопических систем обладает бесконечным несчетным числом независимых состояний (например, свободная частица). Возможные состояния такой системы представляются кэт-векторами в пространстве, размерность которого бесконечна и несчетна. Этот тип пространств требует особого рассмотрения.

Как все рассказанное формулируется на более точном математическом языке? Состояния произвольной микроскопической системы могут быть представлены векторами в комплексном линейном векторном пространстве (возможно) бесконечной размерности. Такое пространство называется *гильбертовым пространством*

(по имени великого математика *Д. Гильберта*, в начале XX в. изучившего свойства этих пространств). Наша ближайшая задача — более подробно обсудить свойства гильбертова пространства и его связь с физическим пространством состояний.

1.5. Бра-пространство

Автомат по продаже кофе в МИФИ принимает монеты и некоторый код, вводимый с клавиатуры на передней стенке автомата. Если повезет, автомат выдает стаканчик кофе. Все это делается детерминированным образом, т. е. одна и та же сумма денег плюс один и тот же код приводят к появлению на выходе стаканчика с тем же напитком (или той же надписи об ошибке). Обратим внимание, что вход и выход автомата имеют совершенно различную природу. Можно представить себе абстрактный автомат, который принимает на входе кэт-векторы и детерминированным образом выдает на выходе комплексные числа. Математики называют такую машину *функционалом*. Представим произвольный функционал F, действующий на произвольный кэт-вектор A и выдающий на выходе произвольное число φ_A. Этот процесс можно математически представить в виде

$$\langle F|\big(|A\rangle\big) = \varphi_A. \tag{1.9}$$

Сосредоточимся на таких функционалах, которые сохраняют линейные зависимости кэт-векторов, на которые эти функционалы действуют. Неудивительно, что такие функционалы называются *линейными функционалами*. Произвольный линейный функционал F удовлетворяет равенству

$$\langle F|\big(|A\rangle + |B\rangle\big) = \langle F|\big(|A\rangle\big) + \langle F|\big(|B\rangle\big), \tag{1.10}$$

где $|A\rangle$ и $|B\rangle$ — два любых кэт-вектора в данном кэт-пространстве.

Рассмотрим N-мерное (т. е. конечномерное или счетное бесконечномерное при $N \to \infty$) кэт-пространство. Пусть $\left|i\right\rangle$, $i = 1, \ldots, N$, представляют N независимых кэт-векторов в этом пространстве. Произвольный кэт-вектор можно представить в виде[1]

$$\left|A\right\rangle = \sum_{i=1}^{N} \alpha_i \left|i\right\rangle, \tag{1.11}$$

где α_i — произвольный набор комплексных чисел. Функционал F может удовлетворять соотношению (1.10) для всех векторов в кэт-пространстве только в случае, если

$$\left\langle F\right|\left(\left|A\right\rangle\right) = \sum_{i=1}^{N} f_i \, \alpha_i, \tag{1.12}$$

где f_i — множество комплексных чисел, связанных с функционалом.

Определим N базисных функционалов $\left\langle i\right|$, удовлетворяющих условию

$$\left\langle i\right|\left(\left|j\right\rangle\right) = \delta_{ij}. \tag{1.13}$$

Из предыдущих трех соотношений следует, что

$$\left\langle F\right| = \sum_{i=1}^{N} f_i \left\langle i\right|. \tag{1.14}$$

---

[1] Строго говоря, такое *свойство полноты* верно только для конечномерных пространств. В случае счетных бесконечномерных пространств это верно только для определенного подмножества таких пространств, но поскольку кэт-пространство обязано быть полным, если мы с его помощью хотим представить состояния микросистемы, то нам достаточно рассматривать только это подмножество.

Но отсюда следует, что множество всех возможных линейных функционалов, действующих в *N*-мерном кэт-пространстве, само представляет *N*-мерное векторное пространство. Такой тип векторного пространства называется (следуя Дираку) *бра-пространством*, а составляющие его векторы (которые, на самом деле, являются функционалами в кэт-пространстве) называются бра-векторами. Заметим, что бра-векторы существенно отличаются по своей природе от кэт-векторов (поэтому они записываются зеркальным образом по отношению к кэт-векторам, $\langle ... |$ и $| ... \rangle$, так что их невозможно перепутать). Бра-пространство есть пример того, что математики называют *дуальным векторным пространством* (т. е. дуальным к исходному кэт-пространству). Между элементами кэт-пространства и соответствующими элементами бра-пространства существует взаимно однозначное соответствие. Так, для каждого элемента *A* кэт-пространства существует соответствующий элемент в бра-пространстве, который тоже удобно обозначить *A*, иными словами,

$$|A\rangle \xleftrightarrow{\text{ДС}} \langle A|, \tag{1.15}$$

где ДС означает *дуальное соответствие*.

Существует бесконечное число способов установить соответствие между векторами в кэт-пространстве и соответствующем бра-пространстве. Однако только одно из них имеет хоть какое-то физическое значение. Для произвольного кэт-вектора *A*, определенного разложением (1.11), соответствующий бра-вектор записывается в виде

$$\langle A| = \sum_{i=1}^{N} \alpha_i^* \langle i|, \tag{1.16}$$

где α_i^* — числа, комплексно сопряженные к α_i. Вектор $\langle A|$ называют *дуальным* к вектору $|A\rangle$. Из предыдущего следует, что дуальным вектором к $c|A\rangle$, где *c* — комплексное число, является

вектор $c^* \langle A|$. В более общей форме

$$c_1 |A\rangle + c_2 |B\rangle \xleftrightarrow{\text{ДС}} c_1^* \langle A| + c_2^* \langle B|. \tag{1.17}$$

Вспомним, что бра-вектор есть функционал, действующий на произвольный кэт-вектор и возвращающий комплексное число. Рассмотрим функционал, дуальный к кэт-вектору

$$|B\rangle = \sum_{i=1}^{N} \beta_i |i\rangle \tag{1.18}$$

и действующий на кэт-вектор $|A\rangle$. Эта операция обозначается $\langle B|(|A\rangle)$. Заметим, однако, что можно без ущерба отбросить круглые скобки и записать эту операцию как $\langle B||A\rangle$. Еще один упрощающий шаг приводит к выражению $\langle B|A\rangle$. Согласно формулам (1.11), (1.12), (1.16) и (1.18),

$$\langle B|A\rangle = \sum_{i=1}^{N} \beta_i^* \alpha_i. \tag{1.19}$$

Математики называют $\langle B|A\rangle$ *внутренним произведением* бра и кэт.[1] Внутреннее произведение практически совпадает со скалярным произведением ковариантного и контравариантного векторов в некотором криволинейном пространстве. Легко показать, что

$$\langle B|A\rangle = \langle A|B\rangle^*. \tag{1.20}$$

[1] Теперь становится понятной элегантность обозначений Дирака: комбинация бра и кэт образует «бракэт», (т. е. скобку bra(c)ket), которая является обычным числом.

Рассмотрим частный случай, когда $|B\rangle \to |A\rangle$. Из соотношений (1.12) и (1.20) следует, что $\langle A|A\rangle$ является действительным числом и

$$\langle A|A\rangle \geq 0. \tag{1.21}$$

Знак равенства имеет место только в случае, когда $|A\rangle$ — нулевой вектор (т. е. когда в формуле (1.11) все $\alpha_i = 0$). Как станет ясно в дальнейшем, это свойство бра- и кэт-векторов существенно для вероятностной интерпретации квантовой механики.

Говорят, что два кэт-вектора $|A\rangle$ и $|B\rangle$ *ортогональны*, если

$$\langle A|B\rangle = 0, \tag{1.22}$$

откуда также следует, что $\langle B|A\rangle = 0$.

Если задан ненулевой кэт-вектор $|A\rangle$, то можно определить *нормированный* кэт-вектор $|\tilde{A}\rangle$, где

$$|\tilde{A}\rangle = \left(\frac{1}{\sqrt{\langle A|A\rangle}}\right)|A\rangle, \tag{1.23}$$

обладающий свойством

$$\langle \tilde{A}|\tilde{A}\rangle = 1. \tag{1.24}$$

Здесь $\sqrt{\langle A|A\rangle}$ называется *нормой* (или «длиной») кэт-вектора $|A\rangle$ и аналогична длине или величине обычного вектора. Поскольку кэт-векторы $|A\rangle$ и $c|A\rangle$ представляют одно и то же физическое состояние, имеет смысл потребовать, чтобы все кэт-векторы, соот-

ветствующие физическим состояниям, обладали единичной нормой.

Теперь можно определить и дуальное бра-пространство к кэт-пространству несчетного бесконечного числа измерений. Делается это способом, во многом аналогичным описанному выше. Главные различия состоят в том, что суммирование по дискретным индексам переходит в интегрирование по непрерывным индексам, дельта–символ Кронекера становится дельта–функцией Дирака, условие полноты постулируется (в бесконечномерном несчетном случае его доказать нельзя) и несколько изменяется условие нормировки.

1.6. Операторы

Мы видели, что функционал представляет собой машину, которая забирает на входе кэт-вектор и выбрасывает на выходе комплексное число. Рассмотрим несколько иную машину, которая забирает кэт-вектор и детерминировано выбрасывает другой кэт-вектор. Математики называют такую машину *оператором*. Нас будут интересовать только операторы, сохраняющие линейные зависимости кэт-векторов, на которые они действуют. Такие операторы называются *линейными операторами*. Рассмотрим оператор X. Предположим, что когда этот оператор действует на произвольный кэт-вектор $|A\rangle$, он в виде результата выдает новый кэт-вектор, обозначаемый $X|A\rangle$. Оператор X линеен, т. е. для всех кэт-векторов $|A\rangle$ и $|B\rangle$ и всех комплексных чисел c выполнены условия

$$X\left(|A\rangle+|B\rangle\right)=X|A\rangle+X|B\rangle, \tag{1.25}$$

$$X\left(c|A\rangle\right)=cX|A\rangle. \tag{1.26}$$

Говорят, что операторы X и Y равны, если равенство

$$X|A\rangle=Y|A\rangle \tag{1.27}$$

выполнено для всех кэт-векторов рассматриваемого кэт-пространства. Оператор X называется *нулевым оператором*, если

$$X\left|A\right\rangle = 0 \tag{1.28}$$

для всех кэт-векторов пространства.

Операторы можно складывать друг с другом. Такое сложение подчиняется правилам коммутативной и ассоциативной алгебры:

$$X + Y = Y + X, \tag{1.29}$$

$$X + (Y + Z) = (X + Y) + Z. \tag{1.30}$$

Операторы можно умножать на числа. Умножение ассоциативно:

$$X\left(Y\left|A\right\rangle\right) = (XY)\left|A\right\rangle = XY\left|A\right\rangle, \tag{1.31}$$

$$X(YZ) = (XY)Z = XYZ. \tag{1.32}$$

Однако в общем случае оно некоммутативно:

$$XY \neq YX. \tag{1.33}$$

До сих пор мы рассматривали только линейные операторы, действующие на кэт-векторы. Но можно также придать смысл их действию на бра-векторы. Рассмотрим внутреннеее произведение произвольного бра-вектора $\left\langle B\right|$ и кэт-вектора $X\left|A\right\rangle$. Это произведение есть число, линейно зависящее от $\left|A\right\rangle$. Следовательно, его можно рассматривать как внутреннее произведение $\left|A\right\rangle$ с некоторым бра-вектором. Этот бра-вектор линейно зависит от $\left\langle B\right|$, так что можно рассматривать его как результат действия некоторого линейного оператора, примененного к $\left\langle B\right|$. Этот оператор однозначно определяется исходным оператором X, так что с тем же

успехом можно назвать этот оператор действующим на $|B\rangle$. Удобное обозначение для действия оператора X на $\langle B|$ есть $\langle B|X$. Формула, определяющая этот вектор, имеет следующий вид:

$$\big(\langle B|X\big)|A\rangle = \langle B|\big(X|A\rangle\big) \tag{1.34}$$

для любых $|A\rangle$ и $\langle B|$. Тройное произведение $\langle B|$, X и $|A\rangle$ можно однозначно записать в виде $\langle B|X|A\rangle$, если принять соглашение, что бра-векторы всегда стоят слева, оператор в середине, а кэт-векторы справа.

Рассмотрим дуальный бра-вектор к $X|A\rangle$. Этот бра-вектор антилинейно зависит от $|A\rangle$ и поэтому должен линейно зависеть от $\langle A|$. Следовательно, этот вектор следует рассматривать как результат применения к $\langle A|$ некоторого линейного оператора. Этот оператор называют сопряженным к X и обозначают $X^\dagger$. Таким образом,

$$X|A\rangle \xleftrightarrow{\text{ДС}} \langle A|X^\dagger. \tag{1.35}$$

Легко показать, что

$$\langle B|X^\dagger|A\rangle = \langle A|X|B\rangle^*, \tag{1.36}$$

а также

$$(XY)^\dagger = Y^\dagger X^\dagger. \tag{1.37}$$

Также легко показать, что сопряженный к сопряженному линейному оператору эквивалентен исходному оператору. Эрмитовый оператор ξ обладает тем свойством, что он сопряжен самому себе, т. е.

$$\xi = \xi^\dagger. \tag{1.38}$$

1.7. Внешнее произведение

До сих пор мы строили следующие произведения:

$$\langle B|A\rangle, X|A\rangle, \langle A|X, XY, \langle B|X|A\rangle.$$

Можно ли образовать какие-то другие произведения? Как насчет

$$|B\rangle\langle A|? \tag{1.39}$$

Ясно, что это выражение линейно зависит от кэт-вектора $|A\rangle$ и бра-вектора $\langle B|$. Умножим это выражение справа на произвольный кэт-вектор $|C\rangle$. Тогда

$$|B\rangle\langle A|C\rangle = \langle A|C\rangle|B\rangle, \tag{1.40}$$

так как $\langle A|C\rangle$ есть просто число. Таким образом, $|B\rangle\langle A|$, действуя на произвольный кэт-вектор $|C\rangle$, приводит к другому кэт-вектору. Ясно, что произведение $|B\rangle\langle A|$ является линейным оператором. Этот оператор действует также на бра-векторы, что легко проверяется путем умножения выражения (1.39) слева на произвольный бра-вектор $\langle C|$. Нетрудно показать, что

$$\left(|B\rangle\langle A|\right)^{\dagger} = |A\rangle\langle B|. \tag{1.41}$$

Математики называют оператор $|B\rangle\langle A|$ *внешним произведением* векторов $\langle B|$ и $|A\rangle$. Это произведение не следует путать с внутренним произведением $\langle A|B\rangle$, которое является просто числом.

1.8. Собственные значения и собственные векторы

В общем случае, кэт-вектор $X|A\rangle$ не равен константе, умноженной на $|A\rangle$. Однако имеются специальные кэт-векторы, которые называются *собственными векторами* оператора X. Они обозначаются

$$\left|\chi'\right\rangle, \left|\chi''\right\rangle, \left|\chi'''\right\rangle, \ldots \tag{1.42}$$

и обладают свойством

$$X\left|\chi'\right\rangle = \chi'\left|\chi'\right\rangle, \quad X\left|\chi''\right\rangle = \chi''\left|\chi''\right\rangle, \ldots, \tag{1.43}$$

где χ', χ'' — числа, называемые *собственными значениями*. Таким образом, действие оператора X на один из его собственных векторов дает тот же самый собственный вектор, умноженный на соответствующее собственное значение.

Рассмотрим собственные векторы и собственные значения эрмитового оператора ξ. Для них выполнено уравнение

$$\xi\left|\xi'\right\rangle = \xi'\left|\xi'\right\rangle \ , \tag{1.44}$$

где $|\xi'\rangle$ — собственный вектор, связанный с собственным значением ξ'. Легко выводятся три важных результата.

1) Все собственные значения являются действительными числами, а собственные векторы, отвечающие разным собственным значениям, ортогональны. Так как оператор ξ эрмитовый, то уравнение, дуальное к (1.44) (для собственного значения ξ'') имеет следующий вид:

$$\left\langle\xi''\right|\xi = \xi'' * \left\langle\xi''\right|. \tag{1.45}$$

Если умножить (1.44) слева на $\left\langle\xi''\right|$, а (1.45) — справа на $|\xi'\rangle$ и вычесть одно из другого, то

$$(\xi' - \xi''*)\left\langle\xi''\right|\left.\xi'\right\rangle = 0. \tag{1.46}$$

Предположим, что собственные значения ξ' и ξ'' равны друг другу. Тогда из (1.46) следует, что

$$\xi' = \xi'^*, \tag{1.47}$$

где мы использовали тот факт, что $|\xi'\rangle$ является ненулевым кэт-вектором. Отсюда можно сделать вывод, что собственные значения являются действительными числами. Пусть теперь собственные значения ξ' и ξ'' не равны друг другу. Отсюда следует, что

$$\langle \xi'' | \xi' \rangle = 0, \tag{1.48}$$

т. е. собственные векторы, отвечающие различным собственным значениям, ортогональны.

2) Собственные значения, связанные с собственными кэт-векторами, совпадают с собственными значениями, связанными с собственными бра-веторами. Собственный бра-вектор оператора ξ, соответствующий собственному значению ξ', определяется уравнением

$$\langle \xi' | \xi = \langle \xi' | \xi' . \tag{1.49}$$

3) Дуальным к собственному кэт-вектору является собственный бра-вектор, принадлежащий тому же собственному значению, и обратно.

1.9. Наблюдаемые

Мы развили математический формализм, содержащий объекты трех типов: бра-векторы, кэт-векторы и линейные операторы. Как было показано, кэт-векторы можно использовать для представления возможных состояний микроскопической системы. Однако существует одно-однозначное соответствие между элементами кэт-пространства и дуальными им элементами бра-пространства. Поэтому мы вправе заключить, что бра-векторы также можно использовать для представления состояний микроскопической системы. А что можно сказать о динамических переменных, описывающих систему (например, ее координате, импульсе, энергии, спине и пр.)? Каким образом они могут быть включены в развиваемый нами формализм? Мы видим, что единственные оставшиеся неиспользованными объекты — это операторы. Таким образом, мы

высказываем предположение, что *динамические переменные микроскопической системы представляются линейными операторами, действующими на бра- и кэт-векторы, которые соответствуют различным возможным состояниям системы*. Заметим, что операторы должны быть линейными, в противном случае, действуя на бра/кэт, которые направлены в одну сторону, но имеют разную длину, эти операторы могут в общем случае выдавать на выходе бра/кэт, направленные в разные стороны. Так как длины бра- и кэт-векторов не имеют физического смысла, разумно предположить, что это же относится к нелинейным операторам.

Мы видели, что если наблюдать состояние поляризации фотона, поместив на пути фотона поляроид, то в результате фотон перейдет в состояние с поляризацией, параллельной или перпендикулярной оптической оси поляроида. Первое состояние поглощается, а второе проходит сквозь поляроид. В общем случае, мы не можем предсказать, в какое состояние перейдет данный фотон, такое предсказание может быть только статистическим. Однако мы знаем, что если фотон начально поляризован параллельно оптической оси, то он безусловно будет поглощен поляроидом, а если фотон начально поляризован перпендикулярно оптической оси, то он безусловно пройдет сквозь поляроид. Мы знаем также, что после прохождения пленки фотон должен находиться в состоянии поляризации, перпендикулярной оптической оси (в противном случае он не мог бы пройти сквозь поляроид). Можно вторично провести наблюдение состояния поляризации такого фотона, поместив сразу за первым поляроидом точно такой же второй поляроид (с той же ориентацией оптической оси). Ясно, что фотон безусловно пройдет сквозь второй поляроид.

Состояния поляризации фотона не являются чем-то особенным. Таким образом, в более общем виде можно сказать, что когда производится измерение динамической переменной микроскопической системы, сама система совершает переход в одно из ряда *независимых* состояний (заметим, что перпендикулярные и параллельные состояния поляризации фотона линейно независимы). В общем случае, каждое из этих конечных состояний связано с разным результатом измерения, т. е. с разным значение динамической переменной. Заметим также, что результатом измерения должно быть *действительное* число (не существует измерительных приборов,

дающих на выходе комплексные числа). Наконец, если наблюдение сделано и получено, что система находится в некотором определенном конечном состоянии с определенным значение динамической переменной, то второе наблюдение, сделанное немедленно после первого, *с достоверностью* обнаружит систему в том же состоянии с тем же значением динамической переменной.

Как отразить все эти факты в развиваемом математическом формализме? Призвав на помощь интуицию, мы предполагаем, что *измерение динамической переменной, соответствующей оператору X в кэт-пространстве, заставляет систему перейти в состояние, соответствующее одному из собственных кэт-векторов оператора X*. Неудивительно, что такое состояние называется *собственным состоянием*. Кроме того, *результат измерения есть собственное значение, связанное с собственным вектором, в который перешла система*. Тот факт, что результат измерения должен быть действительным числом, приводит к условию, что *динамические переменные могут описываться только эрмитовыми операторами* (так как только такие операторы гарантированно имеют действительные собственные значения). Утверждение, что собственные векторы эрмитового оператора, соответствующие разным собственным значениям (т. е. разным результатам измерения), ортогональны, находится в соответствии с нашим высказанным ранее требованием, что состояния, в которые перескакивает система, должны быть взаимно независимыми. Можно сделать вывод, что результат измерения динамической переменной, представленной эрмитовым оператором ξ, должен быть одним из собственных значений этого оператора. Обратно, каждое собственное значение ξ является возможным результатом измерения, осуществленного над соответствующей динамической переменной. Это позволяет придать собственным значениям физический смысл. (С этого момента для простоты мы не будем делать различия между состоянием и представляющим его кэт-вектором, а также между динамической переменной и представляющим ее оператором.)

Разумно предположить, что *если измеряется некоторая динамическая переменная* ξ *и при этом система находится в определенном состоянии, то состояния, в которые может перейти система в результате измерения, таковы, что исходное состояние зависит от них*. Это довольно безобидное утверждение имеет

два очень важных следствия. Во-первых, сразу же после наблюдения, результатом которого является определенное собственное значение ξ', система остается в соответствующем собственном состоянии. Однако это собственное состояние ортогонально (т. е. независимо) любому другому собственному состоянию, отвечающему другому собственному значению. Отсюда следует, что второе измерение, совершенное немедленно после первого, должно оставить систему в собственном состоянии, соответствующем собственному значению ξ'. Иными словами, второе измерение вынуждено дать тот же результат, что и первое. Более того, *если система находится в собственном состоянии ξ, соответствующем собственному значению ξ', то измерение ξ обязательно приводит к результату ξ'*. Это следует из того, что система не может перейти в собственное состояние, соответствующее другому собственному значению ξ, так как подобное состояние не зависит от исходного. Во-вторых, можно утверждать, что измерение ξ должно всегда давать какой-то результат. Отсюда вытекает, что вне зависимости от начального состояния системы всегда возможно перейти в одно из собственных состояний ξ. Другими словами, произвольный кэт-вектор всегда должен зависеть от собственных векторов оператора ξ. Такое возможно только в том случае, если собственные векторы образуют полный набор состояний (т. е. на них натянуто пространство кэт-векторов). Следовательно, *чтобы эрмитовый оператор ξ соответствовал наблюдаемой величиной, его собственные векторы должны образовывать полный набор*. Часто сам эрмитовый оператор, удовлетворяющий этому условию, называется *наблюдаемой*. Таким образом, любая наблюдаемая величина должна быть эрмитовым оператором с полным набором собственных состояний.

1.10. Измерения

Мы видели, что измерение некоторой наблюдаемой ξ микроскопической системы вынуждает систему перейти в одно из собственных состояний ξ. Результатом измерения является соответствующее собственное значение (или некоторая функция этого значения). Невозможно определить, в какое собственное состояние пе-

рейдет данная система, но можно предсказать вероятность такого перехода. Чему же равна вероятность того, что система, находящаяся в некотором начальном состоянии $|A\rangle$, совершит переход в собственное состояние $|\xi'\rangle$ наблюдаемой ξ в результате осуществленного над системой измерения? Начнем с простейшего случая. Если система начально находится в состоянии $|\xi'\rangle$, то вероятность перехода в состояние $|\xi''\rangle$, соответствующее другому собственному значению, равна нулю, а вероятность перехода в то же самое собственное значение $|\xi'\rangle$ равна единице. Удобно нормировать собственные векторы таким образом, чтобы они все имели единичную норму. Из свойства ортогональности собственных векторов следует, что

$$\langle \xi' | \xi'' \rangle = \delta_{\xi'\xi''}, \tag{1.50}$$

где $\delta_{\xi'\xi''}$ равен единице, если $\xi' = \xi''$, и нулю в остальных случаях. Мы сейчас предполагаем, что все собственные значения ξ различны.

Заметим, что вероятность перехода из начального собственного состояния $|\xi'\rangle$ в конечное собственное состояние $|\xi''\rangle$ совпадает со значением внутреннего произведения $\langle \xi' | \xi'' \rangle$. Можно ли использовать это соответствие, чтобы получить общее правило для вычисления вероятностей переходов? Предположим, что система начально находится в состоянии $|A\rangle$, которое не является собственным состоянием ξ. Можно ли отождествить вероятность перехода в конечное состояние $|\xi'\rangle$ с внутренним произведением $\langle A | \xi' \rangle$? Ответ отрицателен, так как $\langle A | \xi' \rangle$ в общем случае является комплексным числом, а комплексные вероятности имеют мало смысла. Попробуем еще раз. А как насчет того, что мы отождествим вероятность перехода с квадратом модуля внутреннего произведения $|\langle A | \xi' \rangle|^2$? Эта величина есть безусловно положительное число (и может поэтому интерпретироваться как вероятность). Это

предположение дает также правильный ответ для вероятностей переходов между собственными состояниями. Мы, на самом деле, угадали верно.

Так как собственные состояния наблюдаемой ξ образуют полный набор, можно выразить любое данное состояние $|A\rangle$ как их линейную комбинацию. Легко показать, что

$$|A\rangle = \sum_{\xi'} |\xi'\rangle\langle\xi'|A\rangle, \tag{1.51}$$

$$\langle A| = \sum_{\xi'} \langle\xi'|A\rangle\langle\xi'|, \tag{1.52}$$

$$\langle A|A\rangle = \sum_{\xi'} \langle A|\xi'\rangle\langle\xi'|A\rangle = \sum_{\xi'} |\langle A|\xi'\rangle|^2, \tag{1.53}$$

где суммирование производится по всем различным собственным значениям ξ, и использованы формула (1.20) и тот факт, что собственные состояния взаимно ортогональны. Заметим, что все полученные выше результаты вытекают из чрезвычайно полезного (и легко доказываемого) результата:

$$\sum_{\xi'} |\xi'\rangle\langle\xi'| = \mathbf{1}, \tag{1.54}$$

где **1** означает тождественный оператор. Относительная вероятность перехода в состояние $|\xi'\rangle$, что эквивалентно относительной вероятности измерения ξ, приводящего к результату ξ', равна

$$P(\xi') \propto |\langle A|\xi'\rangle|^2. \tag{1.55}$$

Очевидно, что абсолютная вероятность равна

$$P(\xi') = \frac{|\langle A|\xi'\rangle|^2}{\sum_{\xi'} |\langle A|\xi'\rangle|^2} = \frac{|\langle A|\xi'\rangle|^2}{\langle A|A\rangle}. \tag{1.56}$$

Если кэт-вектор $|A\rangle$ нормирован так, что его норма равна единице, то эта вероятность сводится просто к

$$P(\xi') = |\langle A|\xi'\rangle|^2. \tag{1.57}$$

1.11. Средние значения

Рассмотрим *ансамбль* микроскопических систем, приготовленных в одном и том же начальном состоянии $|A\rangle$. Пусть над каждой системой производится измерение наблюдаемой ξ. Мы знаем, что каждое измерение дает значение ξ' с вероятностью $P(\xi')$. Чему равно *среднее значение* измеренной величины? Эта величина, которая в общем случае называется иначе *математическим ожиданием* ξ, задается выражением

$$\begin{aligned}\langle\xi\rangle &= \sum_{\xi'}\xi' P(\xi') = \sum_{\xi'}\xi'\left|\langle A|\xi'\rangle\right|^2 = \\ &= \sum_{\xi'}\xi'\langle A|\xi'\rangle\langle\xi'|A\rangle = \sum_{\xi'}\langle A|\xi|\xi'\rangle\langle\xi'|A\rangle,\end{aligned} \tag{1.58}$$

что сводится к

$$\langle\xi\rangle = \langle A|\xi|A\rangle \tag{1.59}$$

с помощью (1.54).

Рассмотрим тождественный оператор **1**. Все состояния являются собственными состояниями этого оператора с собственным значением единица. Таким образом, среднее значение этого оператора всегда равно единице, т. е.

$$\langle A|1|A\rangle = \langle A|A\rangle = 1 \tag{1.60}$$

для всех $|A\rangle$.

1.12. Вырождение

Предположим, что два разных собственных состояния $|\xi'_a\rangle$ и $|\xi'_b\rangle$ оператора ξ соответствуют *одному* собственному значению ξ'. Такие собственные состояния называют *вырожденными*. Эти состояния с необходимостью ортогональны любым собственным состояниям, соответствующим разным собственным значениям, но в общем случае они не ортогональны друг другу (т. е. доказатель-

ство ортогональности в разд. 1.8 в этом случае не работает). Это печально, так как значительная часть описанного формализма критически зависит от взаимной ортогональности разных собственных состояний наблюдаемой. Заметим, однако, что любая линейная комбинация $\left|\xi'_a\right\rangle$ и $\left|\xi'_b\right\rangle$ также является собственным состояниям, соответствующим собственному значению ξ'. отсюда вытекает, что всегда можно построить два взаимно ортогональных вырожденных собственных состояния. Например,

$$\left\langle \xi'_1 \right| = \left\langle \xi'_{a1} \right|, \tag{1.61}$$

$$\left|\xi'_2\right\rangle = \frac{\left|\xi'_b\right\rangle - \left\langle \xi'_a \middle| \xi'_b \right\rangle \left|\xi'_a\right\rangle}{1 - \left|\left\langle \xi'_a \middle| \xi'_b \right\rangle\right|^2}. \tag{1.62}$$

Этот результат легко обобщается на случай более чем двух вырожденных собственных состояний. Можно сделать вывод, что для любой данной наблюдаемой всегда возможно построить полный набор взаимно ортогональных собственных состояний.

1.13. Совместные наблюдаемые

Предположим, что мы хотим одновременно измерить две наблюдаемые ξ и η микроскопической системы. Допустим, что у нас есть два прибора, способных измерять две наблюдаемые ξ и η, соответственно. Например, двумя наблюдаемыми могут быть проекции спинового углового момента частицы со спином 1/2 на оси x и z, соответственно. Они могут быть измерены с помощью установки опыта Штерна–Герлаха. Предположим, что мы совершили измерение ξ, и система была переброшена в одно из собственных состояний ξ — $\left|\xi'\right\rangle$ с собственным значением ξ'. Что произойдет, если мы теперь осуществим измерение η? Предположим, что собственное состояние $\left|\xi'\right\rangle$ является также собственным состоянием η с собственным значением η'. В этом случае измерение η с определенностью даст результат η'. Вторичное измерение ξ с определенностью даст результат ξ', и т. д. В этом смысле мы можем сказать, что наблюдаемые ξ и η *одновременно* имеют собственные значения ξ' и η', соответственно. Ясно, что если все собственные состояния ξ

являются также собственными состояниями η, то всегда возможно совершить одновременное измерение наблюдаемых ξ и η. Такие наблюдаемые называются *совместными* (или *одновременно измеримыми*).

Предположим, однако, что собственные состояния ξ не являются собственными состояниями η. Возможно ли при этом измерить обе наблюдаемые одновременно? Совершим опять наблюдение x, переводящее систему в собственное состояние $|\xi'\rangle$ с собственным значением ξ'. Теперь можно совершить второе наблюдение для определения η. Это переведет систему в одно (из многих) собственных состояний η, зависящих от $|\xi'\rangle$. В принципе, каждое из этих собственных состояний связано с различными результатами измерения. Предположим, что система перешла в собственное состояние $|\eta'\rangle$ с собственным значением η'. Другое измерение ξ перебросит систему в одно (из многих) собственных состояний η, которое зависит от $|\eta'\rangle$. Каждое собственное состояние снова связано с различными возможными результатами наблюдений. Ясно, что если наблюдаемые ξ и η не имеют совместных собственных состояний, то, если значение ξ известно (т. е. система находится в собственном состоянии ξ), значение η не определено (т. е. система *не* находится в каком-то собственном состоянии η), и наоборот. Мы говорим, что две наблюдаемых *несовместны*.

Как мы видели, *условие одновременной измеримости двух наблюдаемых* ξ *и* η *состоит в том, что они должны иметь совместные собственные состояния* (т. е. каждое собственное состояние оператора ξ должно быть собственным состоянием оператора η). Предположим, что так оно и есть. Пусть произвольное собственное состояние ξ с собственным значением ξ' является также собственным состоянием η с собственным значением η'. Удобно обозначить это совместное собственное состояние $|\xi'\eta'\rangle$. Имеем:

$$\xi|\xi'\eta'\rangle = \xi'|\xi'\eta'\rangle, \tag{1.63}$$

$$\eta|\xi'\eta'\rangle = \eta'|\xi'\eta'\rangle. \tag{1.64}$$

Можно умножить первое уравнение слева на h, а второе на x, а затем взять их разность. В результате,

$$(\xi\eta - \eta\xi)\left|\xi'\eta'\right\rangle = \left|0\right\rangle \tag{1.65}$$

для каждого совместного собственного состояния. Вспомним теперь, что собственные состояния наблюдаемой должны образовывать полный набор. Отсюда следует, что совместные собственные состояния двух наблюдаемых также должны образовывать полный набор. Следовательно, из уравнения (1.65) вытекает, что

$$(\xi\eta - \eta\xi)\left|A\right\rangle = \left|0\right\rangle, \tag{1.66}$$

где $\left|A\right\rangle$ — произвольный кэт-вектор. Это может быть достигнуто единственным образом, если

$$\xi\eta = \eta\xi. \tag{1.67}$$

Таким образом, *условие одновременной измеримости двух наблюдаемых* ξ *и* η *состоит в том, что они должны коммутировать*.

1.14. Соотношение неопределенностей

Как мы видели, если ξ и η — две некоммутирующие наблюдаемые, то определение значения x оставляет неопределенным значение η, и наоборот. Оказывается, можно количественно описать эту неопределенность. Для произвольной наблюдаемой ξ можно определить эрмитов оператор

$$\Delta\xi = \xi - \left\langle\xi\right\rangle, \tag{1.68}$$

где среднее значение берется по рассматриваемому конкретному физическому состоянию. Очевидно, что среднее значение $\Delta\xi$ равно нулю. Среднее значение квадрата отклонения $(\Delta\xi)^2 \equiv \Delta\xi\,\Delta\xi$ называется *дисперсией* ξ и в общем случае не равно нулю. На самом деле, легко показывается, что

$$\left\langle(\Delta\xi)^2\right\rangle = \left\langle\xi^2\right\rangle - \left\langle\xi\right\rangle^2. \tag{1.69}$$

Дисперсия ξ есть мера неопределенности значения ξ для конкретного обсуждаемого состояния (т. е. мера ширины распределения вероятных значений ξ относительно среднего значения). Если дис-

персия равна нулю, то неопределенность отсутствует и измерение ξ вынужденным образом дает среднее значение $\langle\xi\rangle$.

Рассмотрим неравенство Шварца

$$\langle A|A\rangle\langle B|B\rangle \geq |\langle A|B\rangle|^2, \tag{1.70}$$

аналогичное неравенству

$$|\boldsymbol{a}|^2\,|\boldsymbol{b}|^2 \geq |\boldsymbol{a}\cdot\boldsymbol{b}|^2 \tag{1.71}$$

в евклидовом пространстве. Это неравенство можно доказать, заметив, что

$$\big(\langle A| + c^*\langle B|\big)\big(|A\rangle + c|B\rangle\big) \geq 0, \tag{1.72}$$

где c — произвольное комплексное число. Если это число принимает специальное значение $-\langle B|A\rangle/\langle B|B\rangle$, то предыдущее неравенство сводится к

$$\langle A|A\rangle\langle B|B\rangle - |\langle A|B\rangle|^2 \geq 0, \tag{1.73}$$

что совпадает с неравенством Шварца.

Подставим в неравенство Шварца

$$|A\rangle = \Delta\xi|\ \rangle, \tag{1.74}$$

$$|B\rangle = \Delta\eta|\ \rangle, \tag{1.75}$$

где пустой кэт-вектор обозначает любой произвольный кэт-вектор. Находим:

$$\langle(\Delta\xi)^2\rangle\langle(\Delta\eta)^2\rangle \geq |\langle\Delta\xi\Delta\eta\rangle|^2, \tag{1.76}$$

где использовано то, что $\Delta\xi$ и $\Delta\eta$ — эрмитовы операторы. Заметим далее, что

$$\Delta\xi\Delta\eta = \frac{1}{2}[\Delta\xi,\Delta\eta] + \frac{1}{2}\{\Delta\xi,\Delta\eta\}, \tag{1.77}$$

где коммутатор $[\Delta\xi,\Delta\eta]$ и антикоммутатор $\{\Delta\xi,\Delta\eta\}$ определены формулами

$$[\Delta\xi,\Delta\eta] \equiv \Delta\xi\Delta\eta - \Delta\eta\Delta\xi, \tag{1.78}$$

$$\{\Delta\xi, \Delta\eta\} \equiv \Delta\xi\Delta\eta + \Delta\eta\Delta\xi. \tag{1.79}$$

Очевидно, что коммутатор антиэрмитов, т. е.

$$\left([\Delta\xi, \Delta\eta]\right)^{\dagger} = \left(\Delta\xi\Delta\eta - \Delta\eta\Delta\xi\right)^{\dagger} = \Delta\eta\Delta\xi - \Delta\xi\Delta\eta = -[\Delta\xi, \Delta\eta], \tag{1.80}$$

в то время, как антикоммутатор, очевидно, эрмитов. Теперь легко показать, что среднее значение эрмитового оператора есть действительное число, а среднее значение антиэрмитового оператора есть чисто мнимое число. Очевидно, что правая часть равенства

$$\langle \Delta\xi\Delta\eta \rangle = \frac{1}{2}\langle [\Delta\xi, \Delta\eta] \rangle + \frac{1}{2}\langle \{\Delta\xi, \Delta\eta\} \rangle \tag{1.81}$$

представляет сумму чисто действительного и чисто мнимого чисел. Вычисляя квадрат модуля обеих сторон равенства, получаем:

$$\left|\langle \Delta\xi\Delta\eta \rangle\right|^2 = \frac{1}{4}\left|\langle [\Delta\xi, \Delta\eta] \rangle\right|^2 + \frac{1}{4}\left|\langle \{\Delta\xi, \Delta\eta\} \rangle\right|^2, \tag{1.82}$$

где использованы равенства $\langle \Delta\xi \rangle = 0$ и т. д. Последнее слагаемое в выражении (1.82) положительно определено, так что можно написать

$$\langle (\Delta\xi)^2 \rangle \langle (\Delta\eta)^2 \rangle \geq \frac{1}{4}\left|\langle [\xi, \eta] \rangle\right|^2, \tag{1.83}$$

где использовано соотношение (1.76). Приведенное выражение называется *соотношением неопределенностей*. Согласно этому соотношению, точное знание значения ξ предполагает отсутствие какого-либо знания о значении η, и наоборот. Единственным исключением из этого правила является случай, когда ξ и η коммутируют, так что в этом случае точное знание ξ не обязательно подразумевает отсутствие знания η.

1.15. Непрерывный спектр

До сих пор мы избегали иметь дело с наблюдаемыми, обладающими собственными значениями, лежащими в непрерывной области. Причина этого состоит в том, что непрерывные собственные значения требуют кэт-пространств несчетной бесконечной размер-

ности. К сожалению, непрерывные собственные значения в квантовой механике неизбежны. На самом деле, самые важные наблюдаемые, координата и импульс, в общем случае имеют непрерывные собственные значения. К счастью, многие результаты, полученные выше для кэт-пространства конечной размерности с дискретными собственными значениями, могут быть обобщены на кэт-пространства несчетных бесконечных размерностей.

Предположим, что ξ — наблюдаемая с непрерывными собственными значениями. Уравнение на собственные значения может быть записано, как и раньше, в виде

$$\xi\left|\xi'\right\rangle = \xi'\left|\xi'\right\rangle. \tag{1.84}$$

Однако ξ' могут теперь иметь значения, лежащие в непрерывной области. Для простоты предположим, что ξ' может принимать любое значение. Условие ортогональности (1.50) обобщается до условия

$$\left\langle\xi'\middle|\xi''\right\rangle = \delta(\xi' - \xi''), \tag{1.85}$$

где $\delta(x)$ обозначает дельта-функцию Дирака. Заметим, что в этом случае имеется несчетное бесконечное количество взаимно ортогональных собственных состояний ξ. Отсюда размерность кэт-пространства несчетно бесконечна. Заметим также, что собственные состояния, соответствующие непрерывному спектру собственных значений, *не могут* быть нормированы так, чтобы их норма равнялась единице. На самом деле, все эти состояния имеют *инфинитную* норму, т. е. их длина бесконечна. В этом — главное отличие между собственными состояниями в конечномерном и бесконечномерном кэт-пространстве.

Необычайно полезное соотношение (1.54) обобщается следующим образом:

$$\int d\xi\left|\xi'\right\rangle\left\langle\xi'\right| = 1. \tag{1.86}$$

Заметим, что суммирование по дискретным собственным значениям заменяется интегрирование по непрерывной области собственных значения. Если ξ — наблюдаемая, то собственные состояния

$|\xi'\rangle$ должны образовывать полный набор. Отсюда следует, что любой произвольный кэт-вектор может быть разложен по $|\xi'\rangle$. Разложения (1.51) – (1.53) обобщаются следующим образом:

$$|A\rangle = \int d\xi' |\xi'\rangle\langle\xi'|A\rangle, \tag{1.87}$$

$$\langle A| = \int d\xi' \langle A|\xi'\rangle\langle\xi'|, \tag{1.88}$$

$$\langle A|A\rangle = \int d\xi' \langle A|\xi'\rangle\langle\xi'|A\rangle = \int d\xi' |\langle A|\xi'\rangle|^2 = 1. \tag{1.89}$$

Эти результаты также просто следуют из (1.86). Заметим, что из (1.89) следует обобщенное условие нормировки состояний

$$\langle A|A\rangle = \int d\xi' |\langle A|\xi'\rangle|^2 = 1. \tag{1.90}$$

1.16. Чистые и смешанные состояния. Матрица плотности

Вернемся к понятию квантового состояния физической системы, с которого начинается построение аппарата квантовой механики. Физическое содержание и конкретная математическая форма этого вводимого *a priori* понятия подразумевает, что сформулировано некоторое описание (или, используя терминологию работы *Эрвина Шрёдингера* 1935 г., представлен к рассмотрению каталог), которое включает информацию о результатах всех возможных измерений, производимых над этой системой.

До сих пор мы говорили о том, что состояние замкнутой квантовой системы может быть описано кэт-вектором $|\psi\rangle$. Такое состояние называется *чистым состоянием*. Коснемся некоторых специфических особенностей чистых состояний. Прежде всего, сам вектор $|\psi\rangle$ данного чистого состояния можно рассматривать как один из собственных векторов некоторого полного набора наблюдаемых, т. е. он входит в некоторый полный набор базисных состояний. В каждом из базисных состояний и, следовательно, в состоянии $|\psi\rangle$ наблюдаемые указанного полного набора имеют определенные значения. Это означает, что для чистого состояния сущест-

вует полная совокупность измерительных процессов, которые приводят с достоверностью к определенным результатам. Поскольку процесс измерения, согласно постулату фон Неймана, представляет собой проектирование на базисные состояния, мы говорим, что чистое состояние возникает в результате полного набора измерений, т. е. в результате полного опыта.

Описание с помощью кэт-вектора $|\psi\rangle$ является наиболее полным возможным в квантовой механике описанием квантового состояния. Знание $|\psi\rangle$ позволяет предсказывать, каков может быть результат того или иного измерения, производимого над системой, и какова вероятность получения этого результата. Поскольку квантовое измерение обычно разрушает состояние, то вероятность реализуется в ансамбле измерений, производимых над одинаковыми системами, которые приготовлены в одном и том же состоянии $|\psi\rangle$.

Существуют, однако, квантовые состояния более общего вида, которые нельзя описать с помощью кэт-векторов. Другими словами, есть состояния, описание которых не обладает той максимальной степенью полноты, которая присуща чистым состояниям. Такие состояния называются *смешанными*, а для их описания используется формализм матрицы плотности, введенный в квантовую механику в 1927 г. *Львом Ландау* и *Иоганном фон Нейманом*.

Сам факт существования смешанных состояний легко понять, если рассмотреть квантовую систему, состоящую из двух подсистем *A* и *B*. Для простоты эти подсистемы можно считать невзаимодействующими друг с другом. Пространством состояний всей системы является прямое произведение $H_A \otimes H_B$ гильбертовых пространств H_A и H_B подсистем *A* и *B*. Пусть $\{|n\rangle_A\}$ и $\{|\nu\rangle_B\}$ есть полные ортонормированные наборы состояний[1] этих подсистем в пространстве, соответственно, H_A и H_B. Если взять прямые произведения $|n\rangle_A|\nu\rangle_B \equiv |n\rangle|\nu\rangle$, то их совокупность $\{|n\rangle|\nu\rangle\}$ образует пол-

[1] Для удобства базисные кэт-векторы подсистемы *A* мы будем идентифицировать с помощью латинских букв, а подсистемы *B* — с помощью греческих. Это позволит, в частности, опускать далее значки *A* и *B*.

ный набор состояний составной системы. Каждое из состояний имеет *факторизованный* вид, т. е. представляет собой произведение кэт-векторов, относящихся *к подсистемам A и B. Это означает, что каждая из подсистем находится в чистом состоянии, заданном своим кэт-вектором*.

В соответствии с принципом суперпозиции произвольное чистое квантовое состояние $|\psi_{AB}\rangle$ полной системы задается кэт-вектором

$$|\psi_{AB}\rangle = \sum_{n,\nu} c_{n\nu} |n\rangle|\nu\rangle, \tag{1.91}$$

удовлетворяющим условию нормировки

$$\langle\psi_{AB}|\psi_{AB}\rangle = \sum_{n,\nu} |c_{n\nu}|^2 = 1. \tag{1.92}$$

Физический смысл коэффициентов разложения $c_{n\nu}$ состоит в том, что величина $|c_{n\nu}|^2$ дает вероятность обнаружить подсистему A в состоянии $|n\rangle$ и одновременно подсистему B в состоянии $|\nu\rangle$. Таким образом, каждое конкретное состояние подсистемы A скоррелировано с каким-то состоянием подсистемы B.

Теперь обратим внимание, что коэффициенты $c_{n\nu}$ не могут быть, вообще говоря, представлены в виде произведения каких-то коэффициентов A_n и B_ν, т. е. в общем случае $c_{n\nu} \neq A_n B_\nu$. Это означает, что кэт-вектор $|\psi_{AB}\rangle$, вообще говоря, не может быть представлен в виде произведения кэт-векторов $|\varphi_A\rangle$ и $|\chi_B\rangle$, которые описывали бы независимым и полным образом чистые квантовые состояния подсистем, $|\psi_{AB}\rangle \neq |\varphi_A\rangle|\chi_B\rangle$. Поэтому описание квантового состояния одной из подсистем (например, A или B) будет характеризоваться меньшей степенью полноты, чем в случае чистого состояния.

Отметим следующую особенность рассмотренной нами ситуации. Вся система находится в чистом состоянии, и ее описание с помощью кэт-вектора является максимально полным. При этом описание каждой из подсистем, как мы видим, может не быть максимально полным. В этом суть отмеченного *Э. Шрёдингером* важ-

ного квантового свойства, что *полное знание о состоянии всей системы не соответствует такому же полному знанию о состоянии ее частей*.

В дальнейшем нам понадобится такая величина как *след оператора*. По определению, следом оператора $\hat{F}$ называется сумма его диагональных матричных элементов, вычисленных в каком-то базисе:

$$Sp\hat{F} \equiv \sum_j \langle j|\hat{F}|j\rangle. \tag{1.93}$$

Укажем несколько полезных свойств величины $Sp\hat{F}$:

1. След оператора не зависит от выбора базисных состояний.
2. Циклическая перестановка операторов, произведение которых стоит под знаком *Sp*, не меняет величину следа.
3. Если оператор имеет вид $\hat{F} = |\psi\rangle\langle\psi|$, то $Sp\hat{F} = Sp|\psi\rangle\langle\psi| = \langle\psi|\psi\rangle$.

Для описания состояния подсистемы *A* вводится оператор плотности

$$\hat{\rho}_A = Sp_B\left(|\psi_{AB}\rangle\langle\psi_{AB}|\right), \tag{1.94}$$

где символ $Sp_B(\ldots)$ обозначает операцию взятия следа по квантовым числам подсистемы *B* от оператора, стоящего в круглых скобках. Во избежание недоразумений обратим внимание, что вычисление следа в выражении (1.94) производится только по состояниям подсистемы *B*. Поэтому величина $\hat{\rho}_A$ представляет собой линейный оператор, действующий в гильбертовом пространстве H_A состояний подсистемы *A*. Подставляя разложение (1.91) в (1.94), получаем:

$$\begin{aligned}\hat{\rho}_A &= \sum_{n\nu,m\mu} c_{n\nu}c^*_{m\mu}|n\rangle\langle m|Sp_B|\nu\rangle\langle\mu| = \\ &= \sum_{nm}\left(\sum_{\nu} c_{n\nu}c^*_{m\nu}\right)|n\rangle\langle m| \equiv \sum_{nm}\rho_{nm}|n\rangle\langle m|.\end{aligned} \tag{1.95}$$

При вычислении мы воспользовались тем, что операция взятия следа относительно подсистемы B дает $Sp_B |\nu\rangle\langle\mu| = \langle\mu|\nu\rangle = \delta_{\mu\nu}$. Совокупность величин

$$\left(\hat{\rho}_A\right)_{nm} \equiv \rho_{nm} \equiv \sum_{\nu} c_{n\nu} c^*_{m\nu} \tag{1.96}$$

образует матрицу оператора $\hat{\rho}_A$ в базисе состояний $\{|n\rangle\}$.

Перечислим основные свойства оператора плотности.

1. Из выражений (1.95) и (1.96) следует, что $\hat{\rho}_A$ есть эрмитовый оператор, т. е.

$$\hat{\rho}_A = \hat{\rho}_A^+ .$$

2. Из эрмитовости $\hat{\rho}_A$ следует, что в H_A существует такой полный ортонормированный базис $\{|i\rangle\}$, в котором оператор $\hat{\rho}_A$ диагонализуется, т. е. может быть записан в виде спектрального разложения

$$\hat{\rho}_A = \sum_i p_i |i\rangle\langle i|, \tag{1.97}$$

где p_i — действительные собственные значения $\hat{\rho}_A$.

3. Используя этот базис в разложении (1.95), получаем, что

$$p_i = \rho_{ii} = \sum_{\nu} c_{i\nu} c^*_{i\nu} = \sum_{\nu} |c_{i\nu}|^2 \geq 0, \tag{1.98}$$

т. е. собственные значения оператора $\hat{\rho}_A$ неотрицательны. Такой оператор называется *неотрицательно определенным оператором*.

4. $Sp_A \hat{\rho}_A = \sum_n |c_{n\nu}|^2 = \sum_i p_i = 1$, т. е. $0 \leq p_i \leq 1$. (1.99)

5. Матрица плотности $\hat{\rho}_A$ позволяет вычислить вероятность получения того или иного результата измерения любой физической величины (наблюдаемой), относящейся к подсистеме A. Действительно, пусть $\hat{F}_A$ есть оператор такой величины.

Тогда, например, для среднего значения $\hat{F}_A$ в состоянии (1.89) получаем:

$$\begin{aligned}\langle F_A \rangle &= \langle \psi_{AB} | \hat{F}_A | \psi_{AB} \rangle = \\ &= \sum_{nm\nu} c_{n\nu} c^*_{m\nu} \langle m | \hat{F}_A | n \rangle = \\ &= \sum_{nm} \rho_{nm} (\hat{F}_A)_{mn} = Sp_A(\hat{\rho}_A \hat{F}_A).\end{aligned} \tag{1.100}$$

Пусть $|F\rangle$ есть собственное состояний оператора $\hat{F}_A$, отвечающее собственному значению *F*. Чтобы найти вероятность получения результата *F* при измерении данной физической величины в состоянии (1.91), нужно вычислить среднее значение проекционного оператора $\hat{P}_F = |F\rangle\langle F|$, т. е. вычислить

$$W_F = \langle \hat{P}_F \rangle = Sp_F \left(\hat{\rho}_A \hat{P}_F \right). \tag{1.101}$$

Используя спектральное разложение (1.97), получаем

$$W_F = Sp_A \left(\hat{\rho}_A \hat{P}_F \right) = \sum_i p_i \left| \langle F | i \rangle \right|^2 . \tag{1.102}$$

Выражение (1.102) допускает прозрачную физическую интерпретацию. Величина $W_F^{(i)} = \left| \langle F | i \rangle \right|^2$ есть вероятность того, что при измерении величины *F* в состоянии $|i\rangle$ мы обнаружим указанное собственное значение *F*. Что же касается величин p_i, то согласно (1.97), они имеют смысл вероятности обнаружить чистое состояние $|i\rangle$ в смешанном состоянии подсистемы *A*, которое описывается с помощью матрицы плотности $\hat{\rho}_A$. Поэтому вероятность получения результата *F* при измерении в состоянии с матрицей плотности $\hat{\rho}_A$ строится стандартным образом как произведение указанных вероятностей $W_F^{(i)}$ и p_i, просуммированное по всем состояниям *i*: $W_F = \sum_i p_i W_F^{(i)}$. Итак, матрица плотности полностью отвечает тем

требованиям, которые предъявляются к описанию квантового состояния.

6. Если подсистема A совпадает со всей системой, либо $c_{n\nu}=A_nB_\nu$, так что кэт-вектор $|\psi_{AB}\rangle$ факторизуется, $|\psi_{AB}\rangle=|\varphi_A\rangle|\chi_B\rangle$, то подсистема A находится в чистом состоянии с кэт-вектором $|\varphi_A\rangle$ и ее оператор плотности имеет вид

$$\begin{aligned}\hat{\rho}_A &= Sp_B\left(|\varphi_A\rangle|\chi_B\rangle\langle\chi_B|\langle\varphi_A|\right)\\ &= |\varphi_A\rangle\langle\varphi_A|Sp_B|\chi_B\rangle\langle\chi_B| = |\varphi_A\rangle\langle\varphi_A|.\end{aligned} \tag{1.103}$$

Это выражение показывает, что любому чистому состоянию $|\psi\rangle$ тоже можно сопоставить оператор плотности

$$\hat{\rho}=|\psi\rangle\langle\psi|, \tag{1.104}$$

который представляет собой эрмитовый оператор проектирования. Из (1.103) или (1.104) следует, что матрица плотности чистого состояния удовлетворяет условию

$$\hat{\rho}^2=\hat{\rho},\ Sp\hat{\rho}^2=Sp\hat{\rho}=1. \tag{1.105}$$

Для произвольного состояния с матрицей плотности (1.97) имеем

$$\begin{aligned}Sp_A(\hat{\rho}_A^2) &= Sp_A\sum_{ij}p_ip_j\left(|i\rangle\langle i|\right)\left(|j\rangle\langle j|\right)=\\ &= \sum_i p_i^2 Sp_A\left(|i\rangle\langle i|\right)=\sum_i p_i^2\le 1.\end{aligned} \tag{1.106}$$

Поскольку $\sum_i p_i=1,$ то равенство имеет место только тогда, когда все собственные значения p_i, кроме одного, равны нулю, т. е. $\hat{\rho}_A$ является оператором плотности чистого состояния. Таким образом, условие (1.105) является критерием чистого состояния. Если же оно не выполнено, то состояние является *смешанным*.

Разложение (1.97) можно интерпретировать следующим образом. В состоянии, которое описывается матрицей плотности, заданы только вероятности p_i присутствия тех или иных чистых состояний $|i\rangle$. О совокупности величин $\{p_i,|i\rangle\}$ говорят как об *ансамбле*, реализующем состояние, которое описывается матрицей

плотности $\hat{\rho}_A$ (1.97) (*И. фон Нейман*). Никакой фазовой информации выражение (1.97) не содержит. В этом смысле состояние, которое описывается матрицей плотности, является некогерентной смесью чистых состояний. Этим оно принципиально отличается от суперпозиции чистых состояний, которая содержит фазовые соотношения между составляющими ее компонентами.

Отсутствие в выражении (1.97) фазовой информации означает, что описание с помощью матрицы плотности является *менее полным*, чем с помощью кэт –вектора. Эта неполнота описания является органическим свойством рассмотренных нами состояний подсистем, входящих в составную квантовую систему. Ее нельзя понимать как незнание каких-то характеристик квантового объекта. Просто есть такие квантовые состояния, которые допускают описание не с помощью кэт-вектора, но только с помощью матрицы плотности. Забавно отметить, что матрица плотности возникает, если угодно, когда мы применяем принцип суперпозиции для состояний (1.91) составной системы. В этой ситуации матрица плотности служит способом описания отдельных подсистем, входящих в составную квантовую систему. Тот факт, что состояния подсистем *A* и *B* оказываются скоррелированными, играет, как мы увидим в главе 2, ключевую роль в теории квантовой информации.

В заключение коснемся информационного аспекта понятия квантового состояния. Мерой информации, которая содержится в квантовом состоянии физической системы, служит *энтропия фон Неймана*. Чем больше энтропия рассматриваемого объекта, тем меньше его информационное содержание. В этом суть естественного соответствия между количеством информации и энтропией. Энтропия квантового состояния с матрицей плотности $\hat{\rho}$ определяется формулой

$$S(\hat{\rho}) = -Sp\left(\hat{\rho}\log_2\hat{\rho}\right). \tag{1.107}$$

Воспользуемся спектральным разложением (1.97) оператора плотности. По определению спектрального разложения функции от оператора имеем

$$\log_2\hat{\rho} = \sum_j \left(\log_2 p_j\right)|j\rangle\langle j|. \tag{1.108}$$

Подставляя (1.97) и (1.108) в формулу (1.107), получаем

$$Sp\left(\hat{\rho}\log_2\hat{\rho}\right) = Sp\sum_i\left(p_i\left|i\right\rangle\left\langle i\right|\right)\left[\sum_j \log_2 p_j\left|j\right\rangle\left\langle j\right|\right] =$$

$$= Sp\sum_{ij} p_i \log_2 p_j \left|i\right\rangle\left\langle i\middle|j\right\rangle\left\langle j\right| = \sum_i p_i \log_2 p_i Sp\left|i\right\rangle\left\langle i\right| = \qquad (1.109)$$

$$= \sum_i p_i \log_2 p_i .$$

Здесь мы воспользовались условием ортонормированности $\left\langle i\middle|j\right\rangle = \delta_{ij}$ базисных состояний и правилом вычисления следа

$$Sp\left|i\right\rangle\left\langle i\right| = \left\langle i\middle|i\right\rangle = 1.$$

Таким образом энтропия фон Неймана имеет вид

$$S(\hat{\rho}) = -\sum_i p_i \log_2 p_i \qquad (1.110)$$

и по форме совпадает с классической энтропией Шеннона. Вероятность изменяется в интервале $0 \le p_i \le 1$, поэтому энтропия $S \ge 0$, а ее минимальное значение равно нулю.

Легко видеть, что минимальное значение $S = 0$ реализуется тогда и только тогда, когда состояние системы является чистым, т. е. описывается кэт-вектором $\left|\psi\right\rangle$. Действительно, в этом случае матрица плотности имеет вид (1.104), т. е. ее спектральное разложение содержит только одно слагаемое с коэффициентом $p = 1$. Поэтому

$$S = -1\cdot\log_2 1 = 0.$$

Таким образом, энтропия чистого состояния имеет минимальное возможное значение, и мы говорим, что в состоянии, которое описывается кэт-вектором $\left|\psi\right\rangle$, содержится наиболее полная возможная в квантовой механике информация о данной физической системе.

Для иллюстрации вычислим энтропию фон Неймана для смешанного состояния. Пусть спектральное разложение (1.97) оператора плотности содержит только два слагаемых с $p_1 = p_2 = 1/2$. Тогда

$$S(\hat{\rho}) = -(p_1 \log_2 p_1 + p_2 \log p_2) = \log_2 2 = 1. \qquad (1.111)$$

Это значение энтропии является максимально возможным для системы, которая может находиться только в двух состояниях. Поэтому информационное содержание квантового состояния, которое описывается рассмотренной матрицей плотности, является минимальным.

Список используемой литературы (источники)

1. Дирак П.А.М. Принципы квантовой механики. — М.: Физматгиз, 1960.
2. Мессиа А. Квантовая механика. Т. 1. — М.: Наука, 1979.
3. Боум А. Квантовая механика. Основы и приложения. — М.: Мир, 1990.
4. Ландау Л.Д., Лифшиц Е.М. Квантовая механика. Нерелятивистская теория. — М.: Наука, 2006.
5. Давыдов А.С. Квантовая механика. — М.: Физматгиз, 1963.

«Квантовая механика – это полная загадок и парадоксов дисциплина, которую мы не понимаем до конца, но умеем применять.»

Марри Гелл-Ман

Инструментарий квантовых вычислений

Г л а в а 2

ИНСТРУМЕНТАРИЙ КВАНТОВЫХ ВЫЧИСЛЕНИЙ

Содержание

Кубиты. Однокубитовые гейты. Многокубитовый регистр. Перепутанные состояния. Двухкубитовые гейты. Мультикубитовые гейты.

Для записи единицы информации одного бита используется ячейка, представляющая собой некоторый физический элемент, который имеет два устойчивых состояния. Такой элемент называют триггером. В качестве такого элемента обычно используется полупроводник. Для наглядности можно говорить, например, о некоторой области с достаточно высокой концентрацией примесей, которыми допирован полупроводник. Тогда физически различимые состояния определяются, например, отсутствием или наличием заряда (потенциала) на такой примеси. Это могут быть токи в микроконтурах электронной схемы, сверхпроводящие элементы с джозефсоновскими контактами, квантовые точки и т.д., и т.п. Состояния триггера отождествляются с нулем (0) и единицей (1) и, тем самым, реализуют два значения бита информации.

Следует подчеркнуть, что практически используемые в настоящее время те или иные ячейки для записи единицы информации являются вполне макроскопическими физическими системами, содержащими большое число таких собственно квантовых объектов как атомы или электроны. Когда мы говорим, что ячейка заряжена (или не заряжена), то речь идет о вполне макроскопическом заряде, который на несколько порядков больше заряда электрона $e = 4{,}80 \cdot 10^{-10}$ ед. СГСЭ. Другими словами, атрибуты информации (логические 0 и 1) связаны с макроскопическими характеристиками триггера. Конечно, поведение зарядов, токов, потенциалов определяется физическими, как правило, квантовыми законами. Именно эти законы определяют такие важные характеристика как скорости необратимых релаксационных процессов, степень чувствительности системы к воздействию управляющих элементов и возможные механизмы таких воздействий.

Вся архитектура систем обработки информации, их *масштабируемость*, объем памяти, быстродействие имеют отчетливую тенденцию к миниатюризации составных элементов, реализуемость которой неразрывно связана с физическими законами. О степени миниатюризации можно судить по минимальному контролируемому размеру в архитектуре микросхем. Эту величину называют *топологическим стандартом*. На сегодняшний день он составляет 45 нм. Моноатомный слой в виде площадки с таким линейным размером содержит порядка 1.5 – 2 тыс. атомов. Тогда в ячейку, содержащую несколько слоев, будет входить порядка 5 – 10 тыс. атомов. Согласно реалистическим прогнозам, уже чуть ли не в этом году возможен переход на топологический стандарт 22 нм.

Физические законы, управляющие поведением ячеек, однако, никак не связаны с математическими законами, которые описывают процессы манипулирования информацией, представленной системой битов. В такой ситуации мы говорим о классической информации. Можно сказать и по-другому: математические законы, управляющие классической информацией, не связаны с физическими законами, описывающими поведение ячеек – носителей бита информации.

Обратим внимание на некоторые простые и совершенно очевидные черты классической информации. В данный момент времени каждый бит может иметь только одно из двух значений – либо 0, либо 1. Если у нас есть регистр, содержащий n битов, то в нем будет записана некоторая цепочка $a = (C_{n-1}, C_{n-2}, \ldots, C_1, C_0)$, состоящая из нулей и единиц, которая представляет собой двоичную запись числа

$$a = C_{n-1}2^{n-1} + C_{n-2}2^{n-2} + \ldots + C_1 2^1 + C_0 2^0 . \qquad (2.1)$$

Это означает, что в каждый момент времени в n-битовом классическом регистре записано только одно число. Всего же в n-битовом регистре можно записать любое из $N=2^n$ различных чисел a от 0 до 2^n-1. Поэтому, как уже говорилось в книге 1, информационная емкость такого регистра, т.е. количество записанной в нем информации, есть

$$H = \log_2 N = \log_2 2^n = n . \qquad (2.2)$$

Отметим еще одну особенность классической информации. Ее можно копировать практически без всякого ущерба для самой информации. Данное свойство, как мы увидим дальше, используется для реализации так называемых обратимых вычислений. Оно также играет существенную роль в такой важной проблеме как коррекция ошибок.

Совершенно очевидно, что технологическая составляющая задачи миниатюризации элементов информационных устройств стоит на первом месте и играет ключевую роль. Нас же интересует другой аспект этой проблемы.

По-видимому, в обозримом будущем технологический прогресс приведет к тому, что вместо двух классических макроскопических состояний триггера, которые служат для идентификации двух значений бита информации, мы будем иметь дело с двумя квантовыми состояниями той или иной простой квантовой системы, т.е. окажемся в области квантовых законов манипулирования информации. В такой ситуации само понятие информации приобретает качественно новое звучание, поскольку носителем информации являются квантовые состояния, поведение которых подчиняется законам квантовой механики. Сказанное включает фактически два принципиальных положения. Во-первых, делается физическое утверждение, что информация, вообще говоря, *не независима* от физических законов, которые используются для ее записи и обработки. Это важное концептуальное положение высказал *Рольф Ландауэр* (1991 г.). Во-вторых, как отметил *Антон Цайлингер* в 1998 г., квантовая механика открывает такие возможности манипулирования информацией, которые принципиально отсутствуют в любых классических устройствах.

В этой главе мы поговорим о том, что входит в такое первичное понятие как квантовая информация, продолжим обсуждение основных элементов — кубитов, квантовых логических гейтов и квантовых схем, а также квантового параллелизма и других важных особенностей квантовых вычислений. Будут рассмотрены примеры физических систем, реализующих кубиты и простейшие логические гейты.

2.1. Кубиты

Рассмотрим ситуацию, когда для записи одного бита информации используются два квантовых состояния какой-либо простой квантовой системы. Такую систему называют *кубитом*. Это название было предложено *Б. Шумахером* и является сокращением выражения "*квантовый бит*" (по-английски qubit, т.е. quantum bit). На первый взгляд может показаться, что такая система просто играет роль классического триггера, но только разве что существенно меньшего размера. В действительности, ситуация совершенно иная.

Речь идет о двух квантовых состояниях, которые образуют полный набор базисных состояний рассматриваемой квантовой системы. Как говорилось в главе 1, совокупность всех возможных состояний такой системы образует двумерное гильбертово пространство. Каждое квантовое состояние описывается абстрактным вектором, который обозначается символом $|\ldots\rangle$ (это кэт-вектор в обозначениях Дирака). Внутри скобки пишется тот или иной значок, идентифицирующий данное квантовое состояние. Для записи информации каждому из двух базисных векторов ставится в соответствие одно из двух значений, 0 или 1, двоичной переменной. Поэтому вполне естественно использовать эти значения двоичной переменной для идентификации соответствующих базисных векторов, т.е. обозначить их как

$$|0\rangle \quad \text{и} \quad |1\rangle . \tag{2.3}$$

Таким образом, два базисных состояния (2.3) кубита соответствуют двум возможным значениям бита информации. Такой набор состояний называется вычислительным базисом. Напомним также (см. главу 1), что базисные векторы удовлетворяют условиям нормировки

$$\langle 0|0\rangle = \langle 1|1\rangle = 1, \tag{2.4}$$

ортогональности

$$\langle 0|1\rangle = \langle 1|0\rangle = 0, \tag{2.5}$$

и полноты

$$|0\rangle\langle 0| + |1\rangle\langle 1| = 1. \tag{2.6}$$

Иногда бывает удобно записывать базисные векторы (2.3) в виде

$$|C\rangle,$$

где величина C является двоичной переменной, пробегающей значения 0 и 1. Тогда выражения (2.4) – (2.6) имеют вид

$$\langle C'|C\rangle = \delta_{CC'}, \tag{2.5'}$$

$$\sum_{C=0,1} |C\rangle\langle C| = 1, \tag{2.6'}$$

где $\delta_{CC'}$ — символ Кронекера.

Принципиальной особенностью кубита как квантового объекта является то, что он может находиться не только в одном из своих базисных состояний (2.3), но и в когерентной суперпозиции

$$|\Psi\rangle = a|0\rangle + b|1\rangle \tag{2.7}$$

базисных состояний с произвольными комплексными коэффициентами a и b. Физическая интерпретация суперпозиционного состояния (2.7) состоит в том, что если в этом состоянии произвести измерение в вычислительном базисе (2.3), то с вероятностью

$$w_0 = |a|^2 \tag{2.8}$$

получится состояние $|0\rangle$, отвечающее нулевому значению двоичной переменной, а с вероятностью

$$w_1 = |b|^2 \tag{2.9}$$

реализуется состояние $|1\rangle$, отвечающее единице. Поэтому единственным ограничением, накладываемым на амплитуды a и b, является условие нормировки

$$w_0 + w_1 = |a|^2 + |b|^2 = 1 \tag{2.10}$$

для полной вероятности.

Итак, в отличие от классической ячейки, которая может находиться либо в состоянии “0”, либо в состоянии “1”, произвольное состояние кубита оказывается таким, что в нем с некоторыми вероятностями, но одновременно, представлены и “0” и ”1”. Этот факт, однако, нельзя интерпретировать в терминах классической стохастической двоичной переменной, значения которой реализуются с той или иной вероятностью. Суть в том, что состояния вычислительного базиса входят в (2.7) в виде когерентной суперпозиции, комплексные коэффициенты которой определяют не только меру (вероятность) присутствия в квантовом состоянии кубита каждого из базисных векторов, но и фиксируют фазовое соотношение между ними. С учетом (2.10) комплексные амплитуды a и b можно представить в форме

$$a = e^{i\alpha}\cos\frac{\theta}{2},\ b = e^{i\beta}\sin\frac{\theta}{2}, \tag{2.11}$$

где α, β, θ – действительные параметры. Тогда (2.7) принимает вид

$$\begin{aligned} |\psi\rangle &= e^{i\alpha}\cos\frac{\theta}{2}|0\rangle + e^{i\beta}\sin\frac{\theta}{2}|1\rangle = \\ &= e^{i\alpha}\left(\cos\frac{\theta}{2}|0\rangle + e^{i(\beta-\alpha)}\sin\frac{\theta}{2}|1\rangle\right). \end{aligned} \tag{2.12}$$

Если отвлечься от общего фазового множителя, который не меняет квантовое состояние и может быть опущен, то вектор $|\psi\rangle$ произвольного состояния кубита определяется двумя действительными параметрами — углом θ и относительной фазой γ = β–α, о которой говорилось ранее.

Выражения (2.7) и (2.12) демонстрируют своеобразную природу информации, которая записана с помощью кубитов. Будем называть ее *квантовой информацией*. При этом кубит выступает как простейший элемент квантовой информации. Поскольку используемые для записи информации символы “0” и ”1” ставятся в соответствие базисным состояниям $|0\rangle$ и $|1\rangle$, то можно сказать с определенной долей условности, что в произвольном состоянии кубита эти символы представлены в виде когерентной суперпозиции, которая содержит сведения о вероятностях и фазах. Как известно, фазовые соотношения играют определяющую роль в таком явлении как интерференция. Манипулирование квантовой информацией, например, в процессе вычисления будет определяться тем, как меняются квантовые состояния, т.е. сам процесс вычисления будет подчиняться квантовым законам. Другими словами, в таком процессе, который будем обозначать термином *«квантовые вычисления»*, могут проявляться сугубо квантовые эффекты, такие, например, как одновременная эволюция вдоль разных путей, дифракция, интерференция. Тем самым открываются принципиально новые возможности для манипулирования информацией.

При выбранном базисе для любого вектора состояния кубита $|\psi\rangle$ комплексные коэффициенты *a* и *b* в суперпозиции (2.7) или (2.12) определяются однозначно. Действительно, из условий ортогональности (2.5) следует, что *a* и *b* имеют вид скалярных произведений

$$a = \langle 0|\psi\rangle,\ b = \langle 1|\psi\rangle, \qquad (2.13)$$

т.е. представляют собой “проекции” вектора $|\psi\rangle$ на два базисных вектора. Взаимно однозначное соответствие между $|\psi\rangle$ и

коэффициентами (2.13), т.е.

$$|\psi\rangle \leftrightarrow \begin{pmatrix} a \\ b \end{pmatrix}, \tag{2.14}$$

позволяет описывать состояние кубита с помощью вектор-столбца, составленного из пары комплексных чисел[1] и изображенного в правой части соотношения (2.14). Напомним, что описание состояния с помощью вектор-столбца (2.14) называется матричным представлением (см. главу 1). С учетом параметризации (2.11) вектор-столбец записывается в виде

$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} \exp(i\alpha)\cos(\theta/2) \\ \exp(i\beta)\sin(\theta/2) \end{pmatrix}. \tag{2.15}$$

Базисным состояниям соответствуют вектор-столбцы вида

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \; |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{2.16}$$

Поэтому суперпозицию (2.7) можно представить в эквивалентной форме

$$\begin{pmatrix} a \\ b \end{pmatrix} = a\begin{pmatrix} 1 \\ 0 \end{pmatrix} + b\begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{2.17}$$

Это соотношение выражает стандартное правило матричной алгебры о покомпонентном умножении вектор-столбцов на комплексные числа и их сложении.

Свойства кубитов и законы, определяющие их поведение, неотъемлемы от тех физических систем, квантовые состояния которых используются в качестве кубита. Поэтому рассмотрим простые примеры физической реализации одного кубита.

---

[1] Эту пару чисел можно рассматривать как функцию $f(C)=\langle C|\Psi\rangle$ двоичной переменной C. Тогда $a=\langle 0|\Psi\rangle=f(0)$, $b=\langle 1|\Psi\rangle=f(1)$.

Примеры физических систем, реализующих кубиты

Важным и широко используемым для этой цели физическим объектом является фотон. Если не вдаваться в некоторые тонкости, связанные с квантовым описанием этой физической системы, то она представляется простой и наглядной; с фотонов началась квантовая механика и наш рассказ о ней в главе 1.

Состояние свободного фотона с волновым вектором $\vec{k}$, т.е. с определенной частотой $\omega = kc$ и направлением пространственного движения, характеризуется еще и поляризацией. Поляризационное состояние задается[1], единичным вектором $\vec{e}$, который ортогонален вектору $\vec{k}$, т.е.

$$\vec{e}^{\,2} = 1, \ \vec{k}\ \vec{e} = 0. \tag{2.18}$$

Для определенности мы здесь говорим о линейной поляризации, когда вектор $\vec{e}$ действительный.

Отметим важное свойство рассматриваемого нами состояния свободного фотона. Оно состоит в том, что пространственные и поляризационные степени свободы являются фактически независимыми. Единственное ограничение заключается во взаимной ортогональности векторов $\vec{k}$ и $\vec{e}$ (2.18). Поэтому кэт-вектор такого квантового состояния фотона удобно записать в факторизованном виде

$$\left|\vec{k}, \vec{e}\right\rangle = \left|\vec{k}\right\rangle \left|\vec{e}\right\rangle, \tag{2.19}$$

где $\left|\vec{k}\right\rangle$ и $\left|\vec{e}\right\rangle$ отвечают, соответственно, пространственным и поляризационной степеням свободы.

Далее мы будем говорить о поляризационном состоянии, кото-

[1]В классической электромагнитной волне этот вектор задает направление вектора напряженности электрического поля. В квантовой механике электромагнитному полю фотона отвечает векторный оператор. Тогда вектор $\vec{e}$ описывает направление векторного оператора электрического поля.

рое описывается кэт-вектором $|\vec{e}\rangle$.

В плоскости, ортогональной вектору $|\vec{k}\rangle$, можно выбрать два линейно независимых базисных вектора поляризации $\vec{e}_1$ и $\vec{e}_2$, удовлетворяющих условиям

$$\vec{e}_1^{\,2} = \vec{e}_2^{\,2} = 1,\ \vec{e}_1\,\vec{e}_2 = \vec{k}\,\vec{e}_1 = \vec{k}\,\vec{e}_2 = 0\,. \qquad (2.20)$$

Эта тройка векторов изображена на рис. 2.1
На этом же рисунке показан произвольный вектор поляризации $\vec{e}$, который, очевидно, можно разложить по базисным векторам

$$\vec{e} = \vec{e}_1 \cos\alpha + \vec{e}_2 \sin\alpha\,. \qquad (2.21)$$

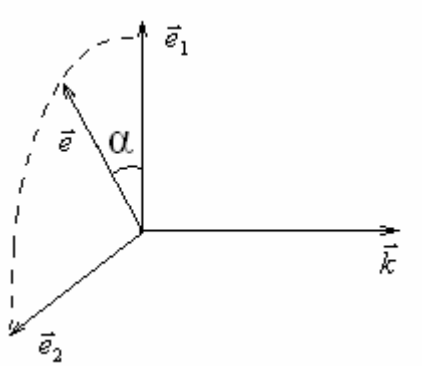


Рис. **2.1**

Два линейно независимых поляризационных состояния

$$|\vec{e}_1\rangle \equiv |0\rangle,\ |\vec{e}_2\rangle \equiv |1\rangle \qquad (2.22)$$

можно выбрать в качестве базисных состояний кубита. Они удовлетворяют необходимым условиям ортонормированности и полноты (2.4)-(2.6). Линейную комбинацию базисных состояний (2.22), аналогичную разложению (2.21), можно отождествить с поляризационным состоянием $|\vec{e}\rangle$. Произвольное состояние поляризацион-

ного кубита описывается выражением (2.7) с произвольными комплексными амплитудами a и b. В дальнейшем мы будем использовать и другие обозначения для базисных состояний поляризационного кубита, например, с помощью букв v и h

$$\left|\vec{e}_1\right\rangle \equiv \left|v\right\rangle \equiv \left|0\right\rangle, \ \left|\vec{e}_2\right\rangle \equiv \left|h\right\rangle \equiv \left|1\right\rangle , \qquad (2.23)$$

которые показывают вертикальную (v) и горизонтальную (h) линейные поляризации. В оптике широко используется циркулярно-поляризованные фотоны. Состояния фотона с правой и левой поляризациями, которым отвечают комплексные векторы

$$\vec{e}_{\pm} \equiv \vec{e}_1 \ \pm i\vec{e}_2 , \qquad (2.24)$$

тоже могут быть использованы в качестве базисных состояний поляризационного кубита.

Целый ряд впечатляющих экспериментов, таких как проверка неравенств Белла, квантовая телепортация, которые продемонстрировали возможности манипулирования квантовой информацией, был выполнен с кубитами, построенными на поляризационных состояниях фотонов.

Еще одним примером физической системы, которая, можно сказать, самой природой создана для реализации кубита, является частица со спином s = 1/2, т.е. имеющая собственный механический момент $\hbar s$. Наличие такого момента является сугубо квантовым свойством, не имеющим аналога в классической физике. Общие свойства оператора спина 1/2 и спиновых состояний рассматриваются в разделе 2.2. Сейчас мы используем только некоторые из них.

Проекция спина 1/2 на любую ось может принимать только два значения: +1/2 и –1/2. Два спиновых состояния

$$\left|S_z = \frac{1}{2}\right\rangle \equiv \left|0\right\rangle \ \text{ и } \left|S_z = -\frac{1}{2}\right\rangle \equiv \left|1\right\rangle \qquad (2.25)$$

с определенными значениями проекции спина на некоторую ось z, которую называют осью квантования, образуют полный набор спиновых состояний. Они выбираются в качестве базисных состояний кубита и, с определенной долей условности, изображены на рис.2.2.

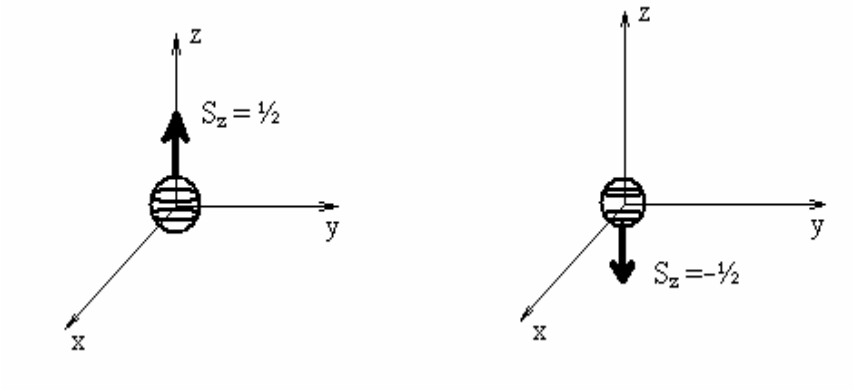


Рис. **2.2**

Ось квантования может быть выбрана произвольно. Если же в системе есть какое-либо выделенное направление, заданное, например, внешним магнитным полем, с помощью которого манипулируют кубитами, то это направление обычно и выбирается в качестве оси квантования *z*.

Многие частицы — электроны, нейтроны, протоны и другие обладают спином 1/2 и в принципе могут быть использованы для реализации кубитов на спиновых состояниях. При этом надо помнить о пространственных степенях свободы. С ними могут быть связаны определенные трудности, так как эффективное манипулирование спиновыми кубитами предполагает в принципе, что они достаточно хорошо локализованы в пространстве.

В настоящее время для экспериментальной реализации спиновых кубитов используется атомные ядра со спином 1/2 такие, например, как ^{1}H, т.е. ядро водорода – протон, изотоп углерода ^{13}C, ядро азота ^{15}N, которые входят в состав больших органических молекул. Пространственное расположение этих кубитов определяется внутримолекулярным взаимодействием. Воздействие на кубиты осуществляется с помощью магнитных полей разной конфигурации и основано на эффекте Зеемана для ядерных магнитных моментов. Такие подходы детально разработаны в методе ядерного магнитного резонанса (ЯМР).

В качестве кубита, наконец, можно использовать два внутрен-

них (электронных) состояния атома или иона. Перспективность таких систем обусловлена структурным многообразием связанных атомных состояний. В качестве базисных состояний используются, например, две компоненты тонкой или сверхтонкой структуры атомного спектра, которые разделены малым энергетическим интервалом. Такую двухуровневую систему иногда называют энергетическим спином. Ее управление осуществляется с помощью резонансного микроволнового поля. Существенным фактором является то, что с помощью внешних электромагнитных полей, действующих на других переходах той же атомной системы, можно осуществить эффективное охлаждение и пространственную локализацию атомов и ионов.

2.2. Однокубитовые гейты

С физической точки зрения, кубит эквивалентен спиновой подсистеме частицы со спином S=1/2. Поэтому при описании состояний кубита и способов манипулирования этими состояниями мы будем использовать свойства спиновых состояний и операторов, действующих на спиновую переменную. Напомним сначала некоторые общие положения квантовой механики, касающиеся понятия спина.

Наличие спиновой степени свободы является сугубо квантовым свойством частиц, которого нет в классической физике. Спин выступает как квантовое число, определяющее трансформационные свойства состояния квантового объекта по отношению к преобразованию поворота системы координат.

Так, при повороте системы координат на угол Ф вокруг оси, направление которой задано единичным вектором $\vec{n}$, состояние частицы, обладающей тем или иным спином, преобразуется по закону:

$$\left|\psi'\right\rangle = \exp(i\Phi\,\vec{n}\,\hat{\vec{S}})\left|\psi\right\rangle. \qquad (2.26)$$

Это есть унитарное преобразование[1], генератором которого является эрмитовый векторный оператор спина

[1] Понятие унитарного оператора обсуждается в этом разделе ниже.

$$\hat{\vec{S}} = \{\hat{S}_x,\ \hat{S}_y,\ \hat{S}_z\}. \tag{2.27}$$

Его компоненты, т.е. эрмитовые операторы $\hat{S}_x$, $\hat{S}_y$, $\hat{S}_z$ проекций спина на координатные оси *x*, *y*, *z*, подчиняются следующим коммутационным соотношениям:

$$[\hat{S}_j \hat{S}_k] = \hat{S}_j \hat{S}_k - \hat{S}_k \hat{S}_j = i\varepsilon_{jkl}\hat{S}_l\ , \tag{2.28}$$

где индексы *j, k, l* пробегают значения *x, y, z*, а ε_{jkl} – антисимметричный тензор третьего ранга. Из этих коммутационных соотношений следует, что эрмитовый неотрицательный
оператор

$$\hat{\vec{S}}^2 = \hat{S}_x^{\,2} + \hat{S}_y^{\,2} + \hat{S}_z^{\,2} \tag{2.29}$$

коммутирует со всеми генераторами $\hat{S}_x$, $\hat{S}_y$, $\hat{S}_z$, но сами эти операторы, как видно из (2.28), между собой не коммутируют. Поэтому в качестве полного набора наблюдаемых можно взять два эрмитовых оператора $\hat{\vec{S}}^2$ и $\hat{S}_z$, которые коммутируют между собой и обладают полной общей системой собственных состояний. При этом собственные значения оператора $\hat{\vec{S}}^2$ равны

$$S(S+1),$$

где неотрицательное число S называется спином частицы и может быть либо целым, либо полуцелым. Подчеркнем, что величина спина есть фундаментальное свойство квантовой частицы.

При данном S полный набор спиновых состояний характеризуется собственными значениями оператора $\hat{S}_z$ проекции спина на ось *z*, которые представляют собой целые или полуцелые числа, лежащие в пределах от $-S$ до S через единицу. Таким образом,

полный набор включает

$$2S+1$$

базисное спиновое состояние с определенными значениями проекции спина на ось квантования z. Такое описание называется S_z – представлением.

В качестве оси квантования можно выбрать и любую другую ось. При данном S проекция спина на эту ось также будет принимать целые или полуцелые значения от $-S$ до S через единицу, т.е. всего $2S+1$ значение. Использование такого базиса означает просто переход к другому унитарно эквивалентному представлению и никак не влияет на физическую картину. Действительно, чтобы осуществить такой переход, надо повернуть исходную систему координат и совместить ее ось z с направлением новой оси квантования. Тогда старый и новый базисы связаны унитарным преобразованием (2.26)

Перейдем теперь к более детальному обсуждению интересующего нас конкретного случая спина 1/2.

Спиноры и матрицы Паули

Если $S=1/2$, то $2S+1=2$, и два базисных состояния имеют вид (2.25). Произвольное спиновое состояние описывается кэт-вектором (2.12) или эквивалентным ему двухкомпонентным столбцом (2.15), т.е.

$$|\psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} \exp(i\alpha)\cos(\theta/2) \\ \exp(i\beta)\sin(\theta/2) \end{pmatrix}. \qquad (2.30)$$

Такой вектор-столбец называется спинором первого ранга или просто спинором. При этом параметры α, β и θ имеют наглядный физический смысл, а именно, они задают, как это показано на рис. 2.3, пространственную ориентацию вектора $<\vec{S}>$, который представляет собой среднее значение операторного вектора спина

$\hat{\vec{S}}$ в состоянии (2.30). Длина этого вектора $|<\vec{S}>|= 1/2$.

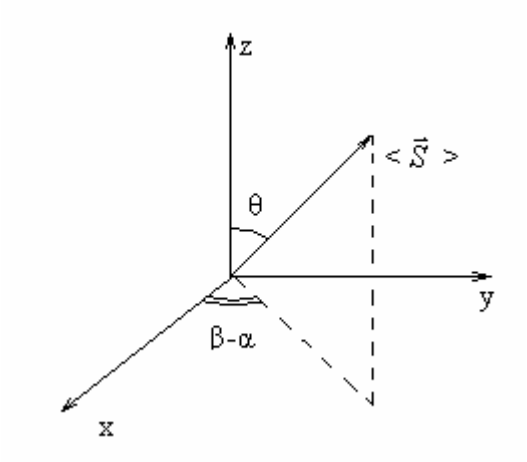


Рис. **2.3**

Доказательство этих утверждений, т.е. вычисление компонент вектора $<\vec{S}>$, приведено в задаче 2 в конце данного раздела.

Так как спинор (2.30) написан в S_z-представлении, то его верхняя (нижняя) компонента имеет смысл амплитуды вероятности обнаружить первое (второе) базисное состояние, указанное в (2.25), при измерении проекции спина на ось z. Сами вероятности получить то или иное значение проекции определяются, соответственно, выражениями:

$$w(S_z = 1/2) = \cos^2\frac{\theta}{2}\ , \qquad w(S_z = -1/2) = \sin^2\frac{\theta}{2}\ . \qquad (2.31)$$

Таким образом, в произвольном спиновом состоянии, которое описывается кэт-вектором (2.12), проекция спина на ось квантования z не имеет определенного значения. Но всегда можно выбрать такую ось $\vec{n}$, что проекция спина на эту ось будет иметь определенное значение (см. задачу 3 в конце данного раздела). Для полноты картины отметим, что базисным состояниям (2.25) соответствует спиноры (2.16), т.е.

$$\left| S_z = \frac{1}{2} \right\rangle \equiv |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad \left| S_z = -\frac{1}{2} \right\rangle \equiv |1> = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \qquad (2.32)$$

а произвольный спинор записывается в виде суперпозиции (см. (2.7), (2.12), (2.17)):

$$|\psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix} = a \begin{pmatrix} 1 \\ 0 \end{pmatrix} + b \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \qquad (2.33)$$

Перейдем теперь к рассмотрению линейных операторов, действующих в двумерном пространстве спиновых состояний.

Пусть в результате действия оператора $\hat{F}$ на состояние $|\psi\rangle$ получается состояние $|\Phi\rangle$, т.е.

$$\hat{F}\,|\psi\rangle = |\Phi\rangle. \qquad (2.34)$$

Записываем кэт-векторы $|\psi\rangle$ и $|\Phi\rangle$ в виде разложений

$$|\psi\rangle = \sum_{c=0,1} a_c\,|c>, \qquad |\Phi\rangle = \sum_{c'=0,1} b_{c'}\,|c'> \qquad (2.35)$$

по базисным состоянием (2.32) и подставляем в уравнение (2.34). Используя свойство линейности оператора $\hat{F}$, имеем

$$|\Phi\rangle = \sum_{c'=0,1} b_{c'}\,|c'> = \hat{F} \sum_{c=0,1} a_c\,|c> = \sum_{c=0,1} a_c \hat{F}\,|c>,$$

т.е.

$$\sum_{c'=0,1} b_{c'} \mid c'> = \sum_{c=0,1} a_c \hat{F} \mid c > . \qquad (2.36)$$

Проектируя обе части этого уравнения на базисные векторы $\left|c\right\rangle$ с учетом условий их ортонормированности, получаем

$$b_{c'} = \sum_{c=0,1} < c' \mid \hat{F} \mid c > a_c \equiv \sum_{c=0,1} F_{c'c} a_c , \quad (c`=0, 1) . \qquad (2.37)$$

Совокупность четырех комплексных чисел

$$F_{c'c} = < c' \mid \hat{F} \mid c >, \quad (c, c'=0, 1) \qquad (2.38)$$

образует 2x2 матрицу оператора $\hat{F}$ в базисе (2.32). Выражение (2.37) показывает, что спинор, описывающий состояние

$$\left|\Phi\right\rangle = \hat{F} \mid \psi\rangle ,$$

получается из спинора, соответствующего состоянию $\mid \psi\rangle$, как результат умножения слева (по стандартным правилам матричной алгебры) на матрицу $F_{c'c}$, которая представляет линейный оператор $\hat{F}$, т.е.

$$\begin{pmatrix} b_0 \\ b_1 \end{pmatrix} = \begin{pmatrix} F_{00} & F_{01} \\ F_{10} & F_{11} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} = \begin{pmatrix} F_{00}a_0 + F_{01}a_1 \\ F_{10}a_0 + F_{11}a_1 \end{pmatrix} . \qquad (2.39)$$

Итак, спиновые состояния образуют двумерное гильбертово пространство и описываются спинорами. Действующие в этом пространстве линейные операторы имеют вид матриц 2x2, что вполне естественно, поскольку оператор преобразует линейным образом две компоненты одного спинора в две компоненты другого спино-

ра, а две линейные комбинации из двух величин содержат четыре коэффициента.

Среди всего многообразия линейных операторов фундаментальную роль играет сам векторный оператор спина. Поэтому рассмотрим матрицы компонент оператор спина

$$\hat{\vec{S}} = \{\hat{S}_x, \hat{S}_y, \hat{S}_z\},$$

которые в дальнейшем будут широко использоваться при описании различных логических операций с кубитами.

В S_z-представлении для спина 1/2 эти матрицы записываются в следующем виде:

$$\hat{S}_x = \frac{1}{2}\sigma_x \ , \ \hat{S}_y = \frac{1}{2}\sigma_y , \ \hat{S}_z = \frac{1}{2}\sigma_z \ , \qquad (2.40)$$

где

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} , \ \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} , \ \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad (2.41)$$

и называются матрицами Паули. Поскольку в качестве базиса используются собственные состояния (2.32) оператора $\hat{S}_z$, то матрица этого оператора согласно (2.38) является диагональной, а на диагонали стоят собственные значения +1/2 и –1/2. Так как операторы $\hat{S}_x$, $\hat{S}_y$ не коммутируют с $\hat{S}_z$ (см.(2.28)), то они представляются недиагональными матрицами. Приведенный в (2.40) и (2.41) явный вид этих матриц следует из коммутационных соотношений (2.28). Более подробно этот вопрос рассматривается в задаче 1 в конце этого раздела.

Сформулируем основные свойства матриц Паули, которые нам понадобятся в дальнейшем.

1. Матрицы Паули являются эрмитовыми матрицами

$$\sigma_i^+ = \sigma_i \ , \ i = x, y, z. \qquad (2.42)$$

2. Единичная матрица и три матрицы Паули образуют полный набор матриц 2x2, т.е. любую матрицу M можно представить в следующем виде:

$$M = a_0 + a_1\,\sigma_x + a_2\,\sigma_y + a_3\,\sigma_z \equiv a_0 + \vec{a}\vec{\sigma}\,. \qquad (2.43)$$

3. Произведение матриц Паули обладает следующим свойством:

$$\sigma_j\,\sigma_k = \delta_{jk} + i\varepsilon_{jkl}\,\sigma_1 \qquad (j,\ k,\ l = x,\ y,\ z)\,. \qquad (2.44)$$

Это соотношение означает, в частности, что

$$\sigma_x^2 = \sigma_y^2 = \sigma_z^2 = \mathbf{1}. \qquad (2.45)$$

Если взять произведение разноименных матриц Паули, то, например,

$$\sigma_x\,\sigma_y = -\sigma_y\,\sigma_x = i\sigma_z\,. \qquad (2.46)$$

Это и еще два соотношения, которые получаются из (2.46) циклической перестановкой индексов *x, y, z*, означают, что разноименные матрицы Паули антикоммутируют друг с другом. Свойства (2.42), (2.45) и (2.46) легко проверить непосредственными вычислениями, используя явный вид (2.41) матриц Паули. При этом соотношение (2.44) представляет собой единую форму записи свойств (2.45) и (2.46). Соотношение (2.43) более подробно обсуждается в задаче 4 в конце раздела.

Иногда вместо матриц Паули (2.41) удобно использовать соответствующие им операторы, записанные с помощью внешних произведений (см. главу 1) базисных векторов (2.32). В соответствии с определением (2.38) матричных элементов

(см. задачу 6 в конце раздела) эти операторы имеют вид

$$\sigma_x \equiv \sigma_1 = |S_z = \frac{1}{2}\rangle\langle S_z = -\frac{1}{2}| + |S_z = -\frac{1}{2}\rangle\langle S_z = \frac{1}{2}| =$$

$$= |0\rangle\langle 1| + |1\rangle\langle 0|,$$

$$i\sigma_y \equiv i\sigma_2 = |S_z = \frac{1}{2}\rangle\langle S_z = -\frac{1}{2}| - |S_z = -\frac{1}{2}\rangle\langle S_z = \frac{1}{2}| = \tag{2.47}$$

$$= |0\rangle\langle 1| - |1\rangle\langle 0|,$$

$$\sigma_z \equiv \sigma_3 = |S_z = \frac{1}{2}\rangle\langle S_z = \frac{1}{2}| - |S_z = -\frac{1}{2}\rangle\langle S_z = -\frac{1}{2}| =$$

$$= |0\rangle\langle 0| - |1\rangle\langle 1|.$$

Здесь для полноты картины представлены все используемые нами обозначения базисных векторов — как с помощью квантового числа $S_z = \pm\frac{1}{2}$, так и с помощью значений $C = 0, 1$ двоичного числа. Заметим также, что индексы x, y, z могут быть заменены соответственно на 1, 2 и 3.

Унитарные преобразования и однокубитовые гейты

Остановимся более подробно на свойствах линейного оператора

$$\hat{R}(\Phi, \vec{n}) = e^{i\Phi\,\vec{n}\hat{\vec{S}}}, \tag{2.48}$$

который определяет закон преобразования (2.26) спинового состояния при повороте системы координат на угол Φ вокруг оси, заданной единичным вектором $\vec{n}$. Повороту на угол $-\Phi$ вокруг

той же оси отвечает, очевидно, оператор

$$\hat{R}(-\Phi,\vec{n}) = e^{-i\Phi\,\vec{n}\hat{\vec{S}}} \equiv \hat{R}^{-1}(\Phi,\vec{n}), \qquad (2.49)$$

для которого выполняются условия

$$\hat{R}\hat{R}^{-1} = \hat{R}^{-1}\hat{R} = \mathbf{1}\ , \qquad (2.50)$$

т.е. он является обратным по отношению к оператору $\hat{R}$. Входящий в показатель экспоненты в формулах (2.48) и (2.49) оператор

$$\hat{S}_{\vec{n}} \equiv \vec{n}\hat{\vec{S}} = n_x\hat{S}_x + n_y\hat{S}_y + n_z\hat{S}_z \qquad (2.51)$$

проекции спина на ось $\vec{n}$ является эрмитовым,

$$\hat{S}_{\vec{n}}{}^{+} = \hat{S}_{\vec{n}}\,.$$

Тогда при эрмитовом сопряжении оператора $\hat{R}$ получаем, учитывая (2.49), что

$$\hat{R}^{+}(\Phi,\vec{n}) = e^{-i\Phi\,\vec{n}\hat{\vec{S}}} \equiv \hat{R}^{-1}(\Phi,\vec{n}), \qquad (2.52)$$

т.е. эрмитово сопряженный оператор совпадает с обратным. Этим свойством определяется важный класс так называемых унитарных операторов. А именно, оператор $\hat{U}$, у которого существует обратный оператор $\hat{U}^{-1}$, совпадающий с $\hat{U}^{+}$, т.е.

$$\hat{U}^{-1} = \hat{U}^{+}, \qquad (2.53)$$

называется унитарным. Условие (2.53) можно представить в эквивалентной форме, умножая его слева или справа на оператор $\hat{U}$.

В результате получаем

$$\hat{U}\,\hat{U}^{+}=\hat{U}^{+}\,\hat{U}=\mathbf{1}. \tag{2.54}$$

Из этого соотношения следует, что скалярное произведение векторов состояний инвариантно относительно унитарного преобразования. Действительно, пусть действие унитарного оператора $\hat{U}$ имеет вид

$$\left|\psi_1^{'}\right\rangle=\hat{U}\left|\psi_1\right\rangle$$

$$\left|\psi_2^{'}\right\rangle=\hat{U}\left|\psi_2\right\rangle, \text{ т.е. } \left\langle\psi_2^{'}\right|=\left\langle\psi_2\right|\hat{U}^{+}.$$

Тогда

$$\left\langle\psi_2^{'}\middle|\,\psi_1^{'}\right\rangle=\left\langle\psi_2\right|\hat{U}^{+}\,\hat{U}\left|\psi_1\right\rangle=\left\langle\psi_2\middle|\,\psi_1\right\rangle. \tag{2.55}$$

Это важное свойство означает, что при унитарном преобразовании сохраняются условия нормировки и ортогональности векторов состояний. Кроме того, существование обратного оператора гарантирует взаимно однозначное соответствие между состояниями, которые получаются друг из друга под действием унитарного оператора. Из сказанного выше следует, что унитарный оператор преобразует один полный набор базисных состояний системы в другой полный набор. При этом все гильбертово пространство состояний квантовой системы переходит само в себя с сохранением своей линейной структуры, а также метрики, основанной на скалярном произведении.

Благодаря указанным свойствам, именно унитарные преобразования играют ключевую роль в процессах манипулирования квантовой информацией. Суть в том, что, сохраняя во всей полноте память о фазовых соотношениях между компонентами любой суперпозиции квантовых состояний, унитарные преобразования сохраняют весь “объем” записанной с помощью этой суперпозиции квантовой информации. При этом информация не стирается, и весь

процесс манипулирования ею является обратимым. Проблема обратимости вычислений, в частности, ее термодинамический аспект, обсуждается в разделе 2.6.

Унитарные операции, производимые над кубитами, называются квантовыми логическими гейтами. Начнем с простейшего случая однокубитовых гейтов, которым отвечают унитарные преобразования в двумерном гильбертовом пространстве спиновых состояний для $S = 1/2$.

Из свойств (2.42) и (2.45) следует, что сами матрицы Паули являются унитарными, $\sigma_i^+ = \sigma_i = \sigma_i^{-1}$, поэтому они описывают некоторые элементарные логические операции. Рассмотрим, например, действие матрицы (или операторы) σ_1 на базисные векторы. Используя (2.41) и (2.47), получаем

$$\sigma_1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{2.56}$$

или

$$\left(|0\rangle\langle 1| + |1\rangle\langle 0| \right) |0\rangle = |0\rangle\langle 1|0\rangle + |1\rangle\langle 0|0\rangle = |1\rangle, \tag{2.57}$$

так как $\langle 1|0\rangle = 0$, а $\langle 0|0\rangle = 1$. Аналогично, имеем

$$\sigma_1 \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{2.58}$$

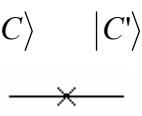
или

$$\left(|0\rangle\langle 1| + |1\rangle\langle 0| \right) |1\rangle = |0\rangle\langle 1|1\rangle + |1\rangle\langle 0|1\rangle = |0\rangle, \tag{2.59}$$

так как $\langle 0|1\rangle = 0$, а $\langle 1|1\rangle = 1$.

Таким образом, операция σ_1 переворачивает кубит, т.е. $|0\rangle \leftrightarrow |1\rangle$, что соответствует логическому гейту NOT (НЕ). Графическое изображение гейта NOT представлено на рис. 2.4. Слева

показано, как начальное состояние кубита $|C\rangle$ переходит в конечное состояние $|C'\rangle$. Крестиком обозначена операция NOT. Справа приведена таблица истинности для начального *C* и конечного *C*' значений двоичной переменной, идентифицирующей состояние кубита.



NOT:

C	*C*'
0	1
1	0

Рис. **2.4**

Операция σ_3 приводит к обращению относительной фазы. Действительно, если подействовать σ_3 на произвольное состояние кубита, то, используя (2.41) и (2.47), получим

$$\sigma_3 \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a \\ -b \end{pmatrix} \tag{2.60}$$

или

$$\begin{aligned} \big(|0\rangle\langle 0| - |1\rangle\langle 1|\big)\big((a|0\rangle + b|1\rangle\big) &= a|0\rangle\langle 0|0\rangle + a|1\rangle\langle 1|0\rangle + \\ + b|0\rangle\langle 0|1\rangle + b|1\rangle\langle 1|1\rangle &= a|0\rangle - b|1\rangle. \end{aligned} \tag{2.61}$$

Более сложный однокубитовый гейт, который описывается оператором,

$$P(\varphi) \equiv |0\rangle\langle 0| + e^{i\varphi}|1\rangle\langle 1|, \tag{2.62}$$

приводит к сдвигу относительной фазы на величину φ. В частности, если $\varphi = \pi$, то $P(\pi) = \sigma_3$, и мы получаем предыдущий случай.

Если $\varphi = 0$, то (2.62) имеет вид

$$P(0) \equiv |0\rangle\langle 0| + |1\rangle\langle 1| = I, \tag{2.63}$$

т.е. представляет собой, как это следует из условия полноты (2.6), тождественное преобразование, которое не меняет состояние кубита.

В теории квантовых вычислений важную роль играет так называемое преобразование Адамара (его называют также преобразованием Уолша-Адамара). Матричная и операторная формы этого преобразования имеют вид

$$\begin{aligned} H &\equiv \frac{1}{\sqrt{2}}(\sigma_1 + \sigma_3) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \\ &= \frac{1}{\sqrt{2}}\Big[\big(|0\rangle + |1\rangle\big)\langle 0| + \big(|0\rangle - |1\rangle\big)\langle 1|\Big]. \end{aligned} \tag{2.64}$$

В результате действия этого преобразования, например, на базисное состояние $|0\rangle$, представляющее число 0, получаем состояние

$$H|0\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big),$$

которое является однородной суперпозицией “нуля” и “единицы”. Унитарная действительная матрица H удовлетворяет условию (см. задачу 9 в конце этого раздела):

$$H^2 = \mathbf{1}, \tag{2.65}$$

т.е. совпадает со своей обратной матрицей, а ее собственные значения равны ± 1.

Рассмотрим теперь произвольный однокубитовый гейт. Он описывается некоторой унитарной матрицей 2×2

$$\hat{U} = \begin{pmatrix} u & w \\ v & z \end{pmatrix}.$$

Эта матрица содержит 4 комплексных матричных элемента, т.е. 8 действительных величин, на которые накладывается ряд ограничений, вытекающих из условия унитарности (2.54)

$$\hat{U}^{+}\hat{U}=\begin{pmatrix} u^{*} & v^{*} \\ w^{*} & z^{*} \end{pmatrix}\begin{pmatrix} u & w \\ v & z \end{pmatrix}=\begin{pmatrix} |u|^{2}+|v|^{2} & u^{*}w+v^{*}z \\ uw^{*}+vz^{*} & |w|^{2}+|z|^{2} \end{pmatrix}=\mathbf{1}.$$

Отсюда следует, что

$$\begin{gathered} |u|^{2}+|v|^{2}=|w|^{2}+|z|^{2}=1 \\ uw^{*}+vz^{*}=0. \end{gathered} \tag{2.66}$$

Эти уравнения представляют собой 4 действительные условия, накладываемые на элементы матрицы $\hat{U}$. Поэтому произвольная унитарная матрица характеризуется четырьмя действительными параметрами. Если выделить в $\hat{U}$ некоторый общий фазовый множитель, то оставшаяся матрица сводится к оператору конечных вращений (2.48) для спина 1/2.

Переходя к матрицам Паули, получаем

$$\hat{U}=e^{i\alpha}\cdot e^{i\frac{\Phi}{2}\vec{n}\vec{\sigma}}. \tag{2.67}$$

Эта матрица зависит, как и говорилось выше, от четырех действительных параметров – фазы α, угла Φ и двух углов θ и φ, определяющих направление единичного вектора $\vec{n}=\{\sin\theta\cos\varphi,\sin\theta\sin\varphi,\cos\theta\}$. Если воспользоваться свойством (2.44) матриц Паули, то произвольную унитарную матрицу (2.67) можно представить (см. задачу 10 в конце этого раздела) в виде

$$\hat{U}=e^{i\alpha}[\cos\frac{\Phi}{2}+i(\vec{n}\vec{\sigma})\sin\frac{\Phi}{2}]=$$

$$= e^{i\alpha}\begin{pmatrix} \cos\frac{\Phi}{2} + i\sin\frac{\Phi}{2}\cos\theta & ie^{-i\phi}\sin\frac{\Phi}{2}\sin\theta \\ ie^{i\cdot\phi}\sin\frac{\Phi}{2}\sin\theta & \cos\frac{\Phi}{2} - i\sin\frac{\Phi}{2}\cos\theta \end{pmatrix}. \quad (2.68)$$

Унитарную матрицу можно параметризировать и другими способами. Для некоторых конкретных вычислений, которые будут проводиться в разделе 2.5, оказывается удобной такая параметризация, когда вместо углов θ и φ вводятся параметры γ и χ с помощью следующих соотношений:

$$\begin{aligned} &\sin\theta\,\sin\frac{\Phi}{2} = \sin\frac{\gamma}{2}, \\ &\cos\frac{\Phi}{2} + i\cos\theta\sin\frac{\Phi}{2} = e^{i\chi}\cos\frac{\gamma}{2}. \end{aligned} \quad (2.69)$$

Тогда унитарная матрица (2.68) принимает следующий вид:

$$\hat{U} = e^{i\alpha}\begin{pmatrix} e^{i\chi}\cos\frac{\gamma}{2} & e^{-i\psi}\sin\frac{\gamma}{2} \\ -e^{i\psi}\sin\frac{\gamma}{2} & e^{-i\chi}\cos\frac{\gamma}{2} \end{pmatrix}, \quad (2.70)$$

где $\psi = \varphi - \frac{\pi}{2}$. Как и должно быть, эта матрица зависит от четырех параметров. Помимо общей фазы α, есть две разные фазы χ и ψ, которые входят в диагональные и недиагональные матричные элементы. Можно показать (см. задачу 11 в конце этого раздела), что параметры χ, ψ и γ связаны с преобразованиями поворотов вокруг осей *y* и *z*.

Произвольный однокубитовый гейт $\hat{U}$, преобразующий входное состояние кубита $|C\rangle$ в состояние $|C'\rangle = \hat{U}|C\rangle$ на выходе, изображается в виде квантовой схемы, показанной на рис. 2.5.

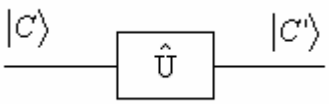


Рис. **2.5**

Ради удобства для гейта NOT мы сохраним изображение в виде крестика, как это сделано на рис. 2.4.

Так как произведение унитарных операторов представляет собой унитарный оператор (см. задачу 7 в конце этого раздела), то последовательное применение нескольких однокубитовых гейтов эквивалентно некоторому результирующему однокубитовому гейту. На рис. 2.6 это показано как эквивалентность двух квантовых схем с одним и с несколькими однокубитовыми гейтами, если они удовлетворяют условию, что $\hat{U} = \hat{U}_3\,\hat{U}_2\,\hat{U}_1$, и цепочка преобразований выглядит так:

$$|C\rangle \rightarrow |d\rangle = \hat{U}_1\,|C\rangle \rightarrow |d'\rangle = \hat{U}_2\,|d\rangle = \hat{U}_2\,\hat{U}_1\,|C\rangle \rightarrow |C'\rangle =$$

$$= \hat{U}_3\,|d'\rangle = \hat{U}_3\,\hat{U}_2\,\hat{U}_1\,|C\rangle$$

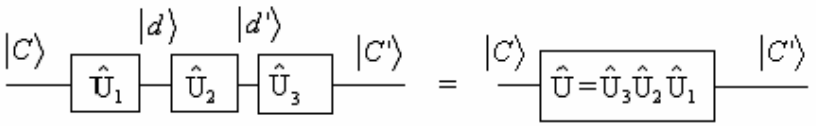


Рис. **2.6**

Подчеркнем, что результирующее преобразование $\hat{U}$ зависит, вообще говоря, от порядка, в котором выполняются операции $\hat{U}_1$, $\hat{U}_2$,…, так как преобразования поворота в общем случае не коммутируют друг с другом.

Теперь рассмотрим несколько примеров физической реализации однокубитовых гейтов.

Спин в магнитном поле

В самом общем виде однокубитовые гейты сводятся фактически к унитарным преобразованиям поворота (2.70) в двумерном гильбертовом пространстве.

Естественным физическим процессом, который реализует однокубитовые гейты, является вращение спина в постоянном внешнем магнитном поле $\vec{H}$. Дело в том, что частица, обладающая собственным механическим моментом (спином $\hbar s$), имеет и собственный магнитный момент, который из соображений симметрии оказывается параллельным или антипараллельным спину. Поэтому для спина 1/2 оператор магнитного момента записывается в виде

$$\hat{\vec{\mu}} = \mu\vec{\sigma}\,, \tag{2.71}$$

где σ_i — матрицы Паули, а характерная величина μ называется магнитным моментом[1]. Взаимодействие магнитного момента с магнитным полем описывается гамильтонианом

$$\hat{\mathrm{H}} = -\hat{\vec{\mu}}\vec{H} = -\mu\vec{\sigma}\vec{H} = -\mu H\vec{n}\,\vec{\sigma}\,, \tag{2.72}$$

в котором направление постоянного магнитного поля задается еди-

[1] Для электрона магнитный момент направлен против спина, а по абсолютной величине равен магнетону Бора $\mu_0 = |e|\hbar/2m_ec =$ $= 0{,}927\cdot10^{-20}$ эрг/гаусс. Магнитный момент тяжелых частиц – нуклонов, ядер – пропорционален ядерному магнетону, который на три порядка меньше, так как в нем вместо массы электрона стоит масса протона.

ничным вектором $\vec{n}$, т.е. $\vec{H} = H\vec{n}$. Тогда временная эволюция вектора состояния $|\psi(t)\rangle$ спиновой системы подчиняется уравнению Шрёдингера

$$i\hbar\frac{\partial}{\partial t}|\psi(t)\rangle = -\mu H\vec{n}\vec{\sigma}\,|\psi(t)\rangle. \qquad (2.73)$$

Решение этого уравнения с начальным условием $|\psi(0)\rangle$ имеет вид

$$|\psi(t)\rangle = e^{i\frac{\Omega}{2}t\vec{n}\vec{\sigma}}\,|\psi(0)\rangle, \qquad (2.74)$$

где $\Omega = \dfrac{2\mu H}{\hbar}$ есть частота прецессии спина в магнитном поле. Мы видим, что временная эволюция представляет собой преобразование поворота спинора на угол $\Phi(t) = \Omega t$ вокруг оси $\vec{n}$, т.е. описывается матрицей конечных вращений $\hat{R}(\Omega t, \vec{n})$ (2.68). Варьируя величину и направление магнитного поля, а также продолжительность времени взаимодействия, можно реализовать любые однокубитовые гейты.

Рассмотрим для иллюстрации несколько частных случаев. Если магнитное поле направлено вдоль оси *x*, то матрица поворота имеет вид

$$e^{i\frac{\Omega}{2}t\sigma_x} \equiv \hat{R}_x = \begin{pmatrix} \cos\dfrac{\Omega t}{2} & i\sin\dfrac{\Omega t}{2} \\ i\sin\dfrac{\Omega t}{2} & \cos\dfrac{\Omega t}{2} \end{pmatrix}. \qquad (2.75)$$

Если $\Omega t = \pi$, то

$$\hat{R}_x(\pi) = i\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = i\sigma_x. \qquad (2.76)$$

Такая операция с точностью до фазового множителя *i* представляет

собой, как мы знаем, логический гейт NOT (2.56). Если $\Omega t = 2\pi$, то $\hat{R}(2\pi) = -1$, так что происходит только изменение общей фазы кубита на противоположную.

Если магнитное поле направлено по оси $-y$, то матрица поворота имеет вид

$$e^{-i\frac{\Omega}{2}t\sigma_y} \equiv \hat{R}_y(-\Omega t) = \begin{pmatrix} \cos\frac{\Omega t}{2} & -\sin\frac{\Omega t}{2} \\ \sin\frac{\Omega t}{2} & \cos\frac{\Omega t}{2} \end{pmatrix}. \qquad (2.77)$$

Положив $\Omega t = \frac{\pi}{2}$, получим

$$\hat{R}_y(-\frac{\pi}{2}) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}. \qquad (2.78)$$

Такая операция действует на базисное состояние $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ как преобразование Адамара (2.64):

$$\hat{R}_y(-\frac{\pi}{2})|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right). \qquad (2.79)$$

Наконец, направив магнитное поле вдоль оси z, получим

$$e^{i\frac{\Omega}{2}t\sigma_z} \equiv \hat{R}_z(\Omega t) = \begin{pmatrix} e^{i\Omega t/2} & 0 \\ 0 & e^{-i\Omega t/2} \end{pmatrix}. \qquad (2.80)$$

С помощью такого процесса можно осуществить операцию сдвига относительной фазы (2.62), так как

$$\hat{R}_z(\Omega t)\left(a|0\rangle + b|1\rangle\right) = \begin{pmatrix} e^{i\frac{\Omega t}{2}} & 0 \\ 0 & e^{-i\frac{\Omega t}{2}} \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} ae^{i\frac{\Omega t}{2}} \\ be^{-i\frac{\Omega t}{2}} \end{pmatrix} =$$

$$= e^{i\frac{\Omega t}{2}} \left(a|0\rangle + be^{-i\Omega t}|1\rangle\right). \qquad (2.81)$$

Мы рассмотрели простейший способ манипулирования спиновым кубитом. В более сложной схеме используется постоянное магнитное поле в сочетании с переменным электромагнитным полем. Такая схема применяется, в частности, к ядерным спинам и составляет суть метода ядерного магнитного резонанса (ЯМР).

Направление постоянного магнитного поля $\vec{H}$ выберем в качестве оси квантования *z*. Базисные векторы кубита $|0\rangle$ и $|1\rangle$, т.е. состояния $\left|S_z = \pm\frac{1}{2}\right\rangle$, являются собственными состояниями гамильтониана (2.72) взаимодействия магнитного момента с магнитным полем

$$\hat{\mathrm{H}}\left|S_z = \pm\frac{1}{2}\right\rangle = -\mu H\sigma_z\left|S_z = \pm\frac{1}{2}\right\rangle = \mp\mu H\left|S_z = \pm\frac{1}{2}\right\rangle. \qquad (2.82)$$

Следовательно, этим состояниям отвечают два собственных значения энергии

$$E_{0,1} = \mp\mu H\,. \qquad (2.83)$$

Эти два уровня энергии, описывающие эффект Зеемана, соответствуют тому, что спиновый магнитный момент может быть ориентирован либо по постоянному магнитному полю, либо против него.

Расстояние между энергетическими уровнями (2.83) определяет частоту перехода

$$\omega_0 = 2 \mid \mu \mid \frac{H}{\hbar} . \qquad (2.84)$$

Для типичных значений ядерных магнитных моментов и используемых в экспериментах постоянных магнитных полей ω_0 составляет величину порядка 500 МГц, т.е. находится в радиочастотном диапазоне. Два таких энергетических состояния можно эффективно перемешивать с помощью магнитной компоненты переменного электромагнитного поля, частота которого настраивается в резонанс с частотой перехода (2.84). Для электрона в зеемановские сдвиги (2.83) и, следовательно, в частоту перехода (2.84) входит магнетон Бора, который, как уже отмечалось выше, на три порядка больше ядерного магнетона. Поэтому частоты переходов, используемые в экспериментах с электронами, как правило, в несколько раз больше.

Таким образом, рассмотренная схема манипулирования кубитом сводится к взаимодействию двухуровневой квантовой системы с резонансным внешним полем. Поскольку такая модель эффективно работает во многих физических ситуациях, мы остановимся на ней более подробно.

Двухуровневая система в резонансном поле

Помимо рассмотренной выше ситуации с зеемановским расщеплением спиновых магнитных подуровней, есть много других практически важных примеров физической реализации двухуровневой системы, взаимодействующей с резонансным внешним полем. Это могут быть специально выбранные уровни энергии связанных электронных состояний атома или иона. Благодаря богатой структуре спектра связанных состояний, частоты таких двухуровневых атомных систем могут варьироваться в очень широких пределах – от оптического до микроволнового диапазонов. Для иллюстрации многообразия возможностей упомянем, что двухуровневая

модель реализуется, например, на колебательных состояниях молекул, или же на квантовых состояниях поступательного движения центра инерции атома или иона в разного типа электромагнитных ловушках. Двухуровневая модель эффективно работает также в задачах квантовой электродинамики резонаторов (КЭР) для описания взаимодействия атома с квантованным электромагнитным полем высокодобротного резонатора.

Все эти системы существенно различаются по масштабам характерных параметров и по физическим механизмам взаимодействия с внешними полями. Тем не менее, структура гамильтонианов, описывающих квантовое поведение этих систем, оказывается одинаковой.

Рассмотрим для определенности изображенную на рис. 2.7 двухуровневую атомную систему, взаимодействующую электродипольным образом с полем электромагнитной волны, частота которой находится в резонансе с частотой выбранного атомного перехода. Заметим, что именно резонансный характер взаимодействия позволяет ограничиться только двумя атомными уровнями и пренебречь остальными состояниями, так как для них условия резонанса не будут выполняться из-за существенно неэквидистантной структуры спектра связанных состояний.

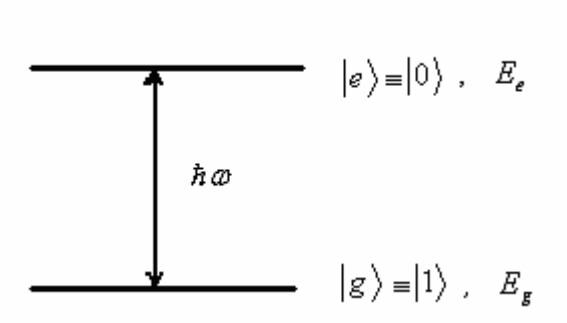


Рис. **2.7**

Собственные состояния $|e\rangle$ и $|g\rangle$ невозмущенного гамильтониана $\hat{H}_0$ “двухуровневого” атома образует полный ортонормированный базис этой квантовой системы. Им соответствуют два соб-

ственных значения энергии E_e и E_g, т.е.

$$\hat{H}_0 \left|g\right\rangle = E_g \left|g\right\rangle ,$$
$$\hat{H}_0 \left|e\right\rangle = E_g \left|e\right\rangle . \tag{2.85}$$

Верхнее состояние $\left|e\right\rangle$ будем называть возбужденным, а нижнее состояние $\left|g\right\rangle$ — основным. Если данная двухуровневая система представляет кубит, то можно использовать стандартные обозначения, например, $\left|e\right\rangle = \left|0\right\rangle$ и $\left|g\right\rangle = \left|1\right\rangle$ для состояний кубита.

Будем отсчитывать энергию от середины расстояния между уровнями. Тогда

$$E_{e,g} = \pm \frac{\hbar\omega}{2}, \tag{2.86}$$

а величина $\omega = \dfrac{(E_e - E_g)}{\hbar}$ представляет собой частоту перехода. С учетом выражений (2.85) и (2.86) невозмущенный гамильтониан $\hat{H}_0$ записывается в виде

$$\hat{H}_0 = \frac{\hbar\omega}{2}\left\{\left|e\right\rangle\left\langle e\right| - \left|g\right\rangle\left\langle g\right|\right\} \equiv \frac{\hbar\omega}{2}\sigma_3, \tag{2.87}$$

где σ_3 — матрица Паули (2.41). Она представляет собой матрицу оператора, который стоит в фигурной скобке, вычисленную в базисе $\left\{\left|e\right\rangle, \left|g\right\rangle\right\}$.

Электродипольное взаимодействие атома с классической линейно поляризованной (по оси z) волной описывается оператором

$$\hat{H}_{\text{int}} = -\hat{\vec{d}}\vec{\varepsilon}(t) = -\hat{d}_z \varepsilon(t), \tag{2.88}$$

который строится из оператора $\hat{\vec{d}}$ дипольного момента атома и направленного по оси z вектора $\vec{\varepsilon}(t)$ напряженности электрического поля волны. Для максимального упрощения вычислений считаем, что частота монохроматической волны совпадает с частотой атомного перехода ω, т.е. электрическое поле имеет вид

$$\varepsilon(t) = \varepsilon_0 \cos \omega t = \frac{\varepsilon_0}{2}(e^{-i\omega t} + e^{i\omega t}) . \qquad (2.89)$$

Следующее требование касается структуры рабочих уровней атомной системы. Взаимодействие с полем будет перемешивать состояния $|e\rangle$ и $|g\rangle$ двухуровневой системы, если недиагональные матричные элементы оператора $\hat{d}_z$ между этими состояниями отличны от нуля[1]. Без ущерба для общности считаем их действительными и обозначим одной буквой d, т.е.

$$\langle e|\hat{d}_z|g\rangle = \langle e|\hat{d}_z|g\rangle^* \equiv d \ . \qquad (2.90)$$

Заметим, что при этом диагональные члены $\langle e|\hat{d}_z|e\rangle = \langle g|\hat{d}_z|g\rangle \equiv 0$ из-за правил отбора по четности для дипольных матричных элементов. Тогда оператор взаимодействия (2.88) принимает вид

$$\hat{H}_{\text{int}} = -d\varepsilon(t)\{|e\rangle\langle g| + |g\rangle\langle e|\} = -d\varepsilon(t)\sigma_1 . \qquad (2.91)$$

---

[1] Пусть, например, момент нижнего состояния J_g=0, а момент верхнего состояния J_e=1. Оператор $\hat{d}_z$ имеет отличные от нуля матричные элементы только между состояниями с одинаковыми значениями проекции момента на ось квантования z. Поскольку в нижнем состоянии проекция равна нулю, то линейно поляризованное (по оси z) электрическое поле индуцирует переходы только на магнитный подуровень возбужденного состояния с нулевой проекцией момента. В результате мы имеем "чистую" двухуровневую систему на переходе $|g,J=0,m=0\rangle \Leftrightarrow |e,J=1,m=0\rangle$.

Здесь, аналогично (2.87), σ_1 матрица Паули представляет матрицу оператора, который стоит в фигурной скобке, вычисленную в базисе $\{|e\rangle, |g\rangle\}$.

Эволюция вектора состояния $|\psi(t)\rangle$ системы подчиняется уравнению Шрёдингера

$$i\hbar \frac{\partial}{\partial t}|\psi(t)\rangle = \hat{H}|\psi(t)\rangle \tag{2.92}$$

с гамильтонианом

$$\hat{H} = \hat{H}_0 + \hat{H}_{\text{int}} = \frac{\hbar\omega}{2}\sigma_3 - d\varepsilon(t)\sigma_1 . \tag{2.93}$$

Если представить $|\psi(t)\rangle$ в виде разложения

$$|\psi(t)\rangle = C_e(t)|e\rangle + C_g(t)|g\rangle \tag{2.94}$$

по базисным состояниям, то зависящие от времени амплитуды $C_e(t)$ и $C_g(t)$ подчиняются условию нормировки

$$|C_g(t)|^2 + |C_e(t)|^2 = 1 \tag{2.95}$$

и выступают как компоненты вектор-столбца (“спинора”)

$$|\psi(t)\rangle = \begin{pmatrix} C_e(t) \\ C_g(t) \end{pmatrix}, \tag{2.96}$$

на который действует гамильтониан (2.93), выраженный через матрицы Паули. В этом проявляется аналогия со случаем спина 1/2. Поэтому двухуровневую атомную систему часто называют энергетическим спином.

Подставляя (2.96) и (2.93) в уравнение Шрёдингера (2.92),

получаем следующую систему уравнений для амплитуд $C_e(t)$ и $C_g(t)$:

$$i\frac{dC_e}{dt} = \frac{\omega}{2}C_e - \Omega\cos\omega t C_g$$

$$i\frac{dC_g}{dt} = -\frac{\omega}{2}C_g - \Omega\cos\omega t C_e, \tag{2.97}$$

где величина

$$\Omega = \frac{d\varepsilon_0}{\hbar} \tag{2.98}$$

называется частотой Раби.

Обычно энергия электродипольного взаимодействия $d\varepsilon_0$ гораздо меньше расстояния $\hbar\omega$ между уровнями, т.е. $d\varepsilon_0 << \hbar\omega$ или

$$\Omega = \frac{d\varepsilon_0}{\hbar} << \omega\,. \tag{2.99}$$

В этом практически важном случае можно использовать так называемое *резонансное приближение* и получить простое аналитическое решение системы уравнений (2.97).

Итак, будем искать решение системы (2.97) в виде

$$C_e(t) = a(t)\ e^{-i\frac{\omega t}{2}},$$

$$C_g(t) = b(t)\ e^{i\frac{\omega t}{2}}. \tag{2.100}$$

Подставляя эти выражения в (2.97), получаем следующую систему

уравнений для новых функций $a(t)$ и $b(t)$:

$$i\frac{da}{dt} = -\frac{\Omega}{2}\ (1 + e^{2i\omega t})\ b\,,$$
$$i\frac{db}{dt} = -\frac{\Omega}{2}\ (1 + e^{-2i\omega t})\ a\,. \qquad (2.101)$$

Зависимость функций $a(t)$ и $b(t)$ от времени характеризуется двумя существенно отличающимися частотами Ω и ω, которые удовлетворяют сильному неравенству (2.99). Медленная зависимость с частотой Ω определяется первыми членами в круглых скобках в правых частях уравнений (2.101). Вторые слагаемые в круглых скобках являются знакопеременными быстро осциллирующими с частотой $\omega >> \Omega$ величинами. Этими членами можно пренебречь, так как их вклад в решение будет мал по параметру $\Omega/\omega << 1$. После этого уравнения (2.101) принимают вид:

$$i\frac{da}{dt} = -\frac{\Omega}{2}b\,,$$
$$i\frac{db}{dt} = -\frac{\Omega}{2}a\,. \qquad (2.102)$$

Пренебрежение малыми быстро осциллирующими членами на фоне медленной зависимости от времени с характерной частотой Ω, в результате чего получаются уравнения (2.102), с физической точки зрения представляет собой переход к резонансному приближению. Действительно, рассмотрим первое из уравнений (2.97). Полевой член в этом уравнении описывает вынужденный переход в возбужденное состояние $|e\rangle$ с энергией $E_e = \frac{\hbar\omega}{2}$ из основного

Состояния $|g\rangle$, имеющего энергию $E_g = -\frac{\hbar\omega}{2}$. Такой процесс будет резонансным, если происходит поглощение энергии $\hbar\omega$ из переменного внешнего поля, и тем самым выполняется закон сохранения энергии $E_g+\hbar\omega=E_e$. Временная зависимость внешнего поля описывается функцией $\cos\omega t = \frac{1}{2}(e^{-i\omega t} + e^{i\omega t})$, в которой первая экспонента соответствует поглощению атомом энергии $\hbar\omega$, а вторая экспонента отвечает процессу излучения. Поэтому в резонансном приближении в первом из уравнений (2.97) надо в функции $\cos\omega t$ оставить только $e^{-i\omega t}$, а во втором уравнении — соответственно, $e^{i\omega t}$. После этого подстановка (2.100) приводит к уравнениям (2.102).

Складывая и вычитая уравнения (2.102), получаем два независимых уравнения

$$i\frac{d}{dt}(a \pm b) = \mp\frac{\Omega}{2}(a \pm b), \tag{2.103}$$

решения которых имеют вид

$$a(t) \pm b(t) = (A \pm B)e^{\pm i\frac{\Omega t}{2}}, \tag{2.104}$$

где $a(0) = A$ и $b(0) = B$ есть произвольное (с точностью до нормировки $|A|^2+|B|^2=1$) начальное условие. Подставляя далее эти выражения в (2.100), получаем окончательные выражения

$$\begin{aligned} C_e(t) &= e^{-i\frac{\omega t}{2}}\left(A\cos\frac{\Omega t}{2} + iB\sin\frac{\Omega t}{2}\right), \\ C_g(t) &= e^{i\frac{\omega t}{2}}\left(iA\sin\frac{\Omega t}{2} + B\cos\frac{\Omega t}{2}\right) \end{aligned} \tag{2.105}$$

для интересующих нас амплитуд

$$C_e(t) \text{ и } C_g(t),$$

удовлетворяющих начальным условиям

$$C_e(0) = A \text{ и } C_g(0) = B.$$

Если записать эту пару функций в виде “спинора” (2.96), то его временная эволюция

$$\begin{pmatrix} C_e(t) \\ C_g(t) \end{pmatrix} = \hat{U}(t) \begin{pmatrix} A \\ B \end{pmatrix} \tag{2.106}$$

описывается унитарной матрицей

$$\hat{U}(t) = \begin{pmatrix} e^{-i\frac{\omega t}{2}} \cos\frac{\Omega t}{2} & ie^{-i\frac{\omega t}{2}} \sin\frac{\Omega t}{2} \\ ie^{i\frac{\omega t}{2}} \sin\frac{\Omega t}{2} & e^{i\frac{\omega t}{2}} \cos\frac{\Omega t}{2} \end{pmatrix}, \tag{2.107}$$

которую можно представить как произведение

$$\hat{U}(t) = e^{-i\frac{\omega t}{2}\sigma_3} e^{i\frac{\Omega t}{2}\sigma_1}$$

двух поворотов – сначала на угол Ωt вокруг первой оси, а потом на угол $-\omega t$ вокруг третьей оси.

Первое из этих преобразований совпадает, очевидно, с выражением (2.75), а второе эквивалентно (2.80).

Задачи

1. Построить матрицы операторов $\hat{S}_x$, $\hat{S}_y$, $\hat{S}_z$ для спина $\frac{1}{2}$ в S_z – представлении.

Решение

Собственные состояния оператора $\hat{S}_z$, отвечающие собственным значениям $\sigma = \pm\frac{1}{2}$, обозначим как $|\sigma\rangle$, т.е. $\hat{S}_z|\sigma\rangle = \sigma|\sigma\rangle$. В S_z – представлении эти состояния используются в качестве базиса для вычисления матричных элементов. Поэтому сам оператор $\hat{S}_z$ имеет отличные от нуля только диагональные матричные элементы

$$\langle 1/2|\hat{S}_z|1/2\rangle = \frac{1}{2}, \quad \langle -1/2|\hat{S}_z|-1/2\rangle = -\frac{1}{2}, \quad \langle -1/2|\hat{S}_z|1/2\rangle = 0,$$

т.е. матрица имеет вид

$$\hat{S}_z = \begin{pmatrix} 1/2 & 0 \\ 0 & -1/2 \end{pmatrix} = \frac{1}{2}\sigma_z, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Далее введем операторы $\hat{S}_\pm = \hat{S}_x \pm i\hat{S}_y$. Из коммутационных соотношений (2.28) следует, что

$$[\hat{S}_z, \hat{S}_\pm] = \hat{S}_z\hat{S}_\pm - \hat{S}_\pm\hat{S}_z = \pm\hat{S}_\pm.$$

Здесь надо везде брать либо верхний знак, либо нижний. Рассмотрим состояние $|\Psi\rangle = \hat{S}_+|\sigma\rangle$, которое получается из базисного вектора $|\sigma\rangle$ под действием оператора $\hat{S}_+$. Подействуем на него опера-

тором $\hat{S}_z$ и, воспользовавшись одним из приведенных выше коммутационных соотношений, получим

$$\hat{\hat{S}}_z\left|\Psi\right\rangle = \hat{S}_z\hat{S}_+\left|\sigma\right\rangle = \left(\hat{S}_+\hat{S}_z + \hat{S}_+\right)\left|\sigma\right\rangle = (\sigma+1)\hat{S}_+\left|\Psi\right\rangle = \left(\sigma+1\right)\left|\Psi\right\rangle \ .$$

Таким образом, под действием оператора $\hat{S}_+$ собственное состояние $\left|\sigma\right\rangle$ оператора $\hat{S}_z$ переходит в другое собственное состояние $\left|\psi\right\rangle$, отвечающее собственному значению $\sigma+1$. Поэтому $\hat{S}_+$ называют повышающим оператором. Так как максимальное собственное значение равно $1/2$, то отличный от нуля результат получается, если $\hat{S}_+$ действует на состояние $\left|-1/2\right\rangle$. Итак, у оператора $\hat{S}_+$ есть единственный отличный от нуля матричный элемент $\langle 1/2\,|\,\hat{S}_+\,|-1/2\,\rangle \equiv \lambda$, который без ущерба для общности можно считать действительным и положительным. Итак, матрица $\hat{S}_+$ имеет вид

$$\hat{S}_+ = \begin{pmatrix} 0 & \lambda \\ 0 & 0 \end{pmatrix} = \lambda \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Читателю предлагается самостоятельно показать, что оператор $\hat{S}_-$ понижает проекцию на единицу, т.е.

$$\hat{S}_z\left(\hat{S}_-\left|\sigma\right\rangle\right) = \left(\sigma-1\right)\left(\hat{S}_-\left|\sigma\right\rangle\right).$$

Для этого надо воспользоваться коммутационным соотношением $[\,\hat{S}_z\ \hat{S}_-\,] = -\hat{S}_-$. Так как минимальное собственное значение равно $-1/2$, то у $\hat{S}_-$ есть единственный отличный от нуля матричный элемент

$$\langle -1/2 \,|\, \hat{S}_- \,|\, 1/2 \rangle \;=\; \langle -1/2 \,|\, \hat{S}_+^{\,+} \,|\, 1/2 \rangle \;=\; \langle 1/2 \,|\, \hat{S}_+ \,|\, -1/2 \,\rangle^{\,*} = \lambda^{\,*} = \lambda \,.$$

Здесь мы учли, что операторы $\hat{S}_+$ и $\hat{S}_-$ получаются друг из друга эрмитовым сопряжением

$$\hat{S}_+^{\,+} = (\,\hat{S}_x + i \cdot \hat{S}_y\,)^+ = \hat{S}_x - i \cdot \hat{S}_y = \hat{S}_- \,.$$

Для матриц это эквивалентно операциям транспонирования (повороту вокруг главной диагонали) и комплексного сопряжения. Поэтому матрица $\hat{S}_-$ имеет вид

$$\hat{S}_- = \lambda \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

Чтобы найти λ, рассмотрим произведение операторов $\hat{S}_+$ и $\hat{S}_-$:

$$\hat{S}_+ \;\hat{S}_- = (\,\hat{S}_x + i\hat{S}_y\,)(\,\hat{S}_x - i\hat{S}_y\,) = \hat{S}_x^2 + \hat{S}_y^2 - i[\,\hat{S}_x \hat{S}_y\,] = \hat{\vec{S}}^{\,2} - \hat{S}_z^2 + \hat{S}_z \,,$$

где оператор квадрата спина $\hat{\vec{S}}^{\,2}$ есть число $S(S{+}1) = 3/4$, а $[\,\hat{S}_x \hat{S}_y\,] = i\hat{S}_z$. Тогда

$$\hat{S}_+ \;\hat{S}_- = \frac{3}{4} - \hat{S}_z^2 + \hat{S}_z \,.$$

Вычислив диагональный матричный элемент $\langle\, 1/2 \,|\ldots|\, 1/2 \,\rangle$ от обеих частей этого равенства, получим

$$\langle 1/2 \,|\, \hat{S}_+ \;\hat{S}_- \,|\, 1/2 \,\rangle = \langle 1/2 \,|\, \hat{S}_+ \,|\, -1/2 \,\rangle \langle -1/2 \,|\, \hat{S}_- \,|\, 1/2 \,\rangle = \lambda^2 =$$

$$= \frac{3}{4} - \left(\frac{1}{2}\right)^2 + \frac{1}{2} = 1, \text{ т.е. } \lambda = 1.$$

Тогда

$$\hat{S}_x = \frac{\hat{S}_+ + \hat{S}_-}{2} = \frac{1}{2}\sigma_x, \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$
$$\hat{S}_y = \frac{\hat{S}_+ - \hat{S}_-}{2i} = \frac{1}{2}\sigma_y, \; \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}.$$

2. Вычислить среднее значение оператора спина $\hat{\vec{S}}$ в состоянии (2.30).

Решение

Среднее значение оператора спина $\hat{\vec{S}} = \frac{1}{2}\{\sigma_x, \sigma_y, \sigma_z\}$ представляет собой вектор

$$\langle \hat{\vec{S}} \rangle = \frac{1}{2}\{\langle \sigma_x \rangle, \langle \sigma_y \rangle, \langle \sigma_z \rangle\},$$

компоненты которого получаются усреднением матриц Паули (2.41) по состоянию (2.30).

Вычислим $< \sigma_x >$:

$$\langle \sigma_x \rangle = \begin{pmatrix} e^{i\cdot\alpha} \cdot \cos\frac{\theta}{2} \\ e^{i\cdot\beta} \cdot \sin\frac{\theta}{2} \end{pmatrix}^* \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} e^{i\alpha} \cdot \cos\frac{\theta}{2} \\ e^{i\beta} \cdot \sin\frac{\theta}{2} \end{pmatrix} =$$

$$= \begin{pmatrix} e^{-i\cdot\alpha}\cdot\cos(\frac{\theta}{2}) \\ e^{-i\cdot\beta}\cdot\sin(\frac{\theta}{2}) \end{pmatrix} \cdot \begin{pmatrix} e^{i\beta}\cdot\sin\frac{\theta}{2} \\ e^{i\alpha}\cdot\cos\frac{\theta}{2} \end{pmatrix} =$$

$$= \left(e^{i(\beta-\alpha)} + e^{-i(\beta-\alpha)}\right)\cdot \sin\frac{\theta}{2}\cdot\cos\frac{\theta}{2} = \sin\theta\cdot\cos(\beta-\alpha) \quad .$$

Аналогично, имеем

$$\langle\sigma_y\rangle = \begin{pmatrix} e^{i\cdot\alpha}\cdot\cos\frac{\theta}{2} \\ e^{i\cdot\beta}\cdot\sin\frac{\theta}{2} \end{pmatrix}^* \cdot \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \cdot \begin{pmatrix} e^{i\alpha}\cdot\cos\frac{\theta}{2} \\ e^{i\beta}\cdot\sin\frac{\theta}{2} \end{pmatrix} =$$

$$= -i\cdot\left(e^{i\cdot(\beta-\alpha)} - e^{-i\cdot(\beta-\alpha)}\right)\cdot \sin\frac{\theta}{2}\cdot\cos\frac{\theta}{2} =$$

$$= \sin\theta\cdot\sin(\beta-\alpha) \quad ,$$

$$\langle\sigma_z\rangle = \begin{pmatrix} e^{i\cdot\alpha}\cdot\cos\frac{\theta}{2} \\ e^{i\cdot\beta}\cdot\sin\frac{\theta}{2} \end{pmatrix}^* \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} e^{i\alpha}\cdot\cos\frac{\theta}{2} \\ e^{i\beta}\cdot\sin\frac{\theta}{2} \end{pmatrix} = \cos\theta \, .$$

Таким образом, компоненты вектора $\langle\hat{\vec{S}}\rangle$ имеют вид

$$\langle\hat{\vec{S}}\rangle = \frac{1}{2}\cdot\{\sin\theta\cdot\cos(\beta-\alpha)\,,\ \sin\theta\cdot\sin(\beta-\alpha)\,,\cos\theta\}.$$

Длина этого вектора равна $\frac{1}{2}$, а направление задается углами $\theta,\ \beta-\alpha$, как показано на рис. 2.3.

3. Доказать, что спинор $\begin{pmatrix} e^{i\alpha}\cos\frac{\theta}{2} \\ e^{i\beta}\cos\frac{\theta}{2} \end{pmatrix}$ описывает собственное состояние оператора $\hat{s}_{\vec{n}} = \hat{\vec{s}}\vec{n}$ проекции спина $1/2$ на ось $\vec{n} = \{\sin\theta\cos(\beta-\alpha), \sin\theta\sin(\beta-\alpha), \cos\theta\}$, отвечающее собственному значению $1/2$. Сравнить вектор $\vec{n}$ с направлением вектора $\langle\hat{\vec{S}}\rangle$ из предыдущей задачи. Какой вид имеет спинор, отвечающий собственному значению проекции на ось $\vec{n}$, равному $-1/2$?

4. Доказать, что любую матрицу M (2×2) можно представить в виде

$$M=a_0+a_1\sigma_x+a_2\sigma_y+a_3\sigma_z,$$

где σ_i — матрицы Паули.

Доказательство

Пусть $M=\begin{pmatrix} u & w \\ v & z \end{pmatrix}$ – некоторая произвольная матрица 2×2. Тогда неизвестные коэффициенты a_i (i=0, 1, 2, 3) находятся из условия, что

$$\begin{pmatrix} u & w \\ v & z \end{pmatrix} = a_0\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + a_1\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + a_2\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} + a_3\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} =$$

$$= \begin{pmatrix} a_0 + a_3 & a_1 - i \cdot a_2 \\ a_1 + i \cdot a_2 & a_0 - a_3 \end{pmatrix},$$

т.е.

$$\begin{cases} a_0 + a_3 = u \\ a_0 - a_3 = z \end{cases} \qquad \begin{cases} a_1 - i \cdot a_2 = w \\ a_1 + i \cdot a_2 = v \end{cases}.$$

Отсюда получаем

$$a_0 = \frac{u+z}{2}, \quad a_3 = \frac{u-z}{2}, \quad a_1 = \frac{w+v}{2}, \quad a_3 = i \cdot \frac{w-v}{2}.$$

Соотношение (2.44) показывает, что произведение двух (и более) матриц Паули редуцируется к единичной матрице и первым степеням матриц Паули, как и должно быть, так как $\{1,\ \sigma_i\}$ образуют полный набор матриц 2×2. Если в (2.44) сделать замену $i \leftrightarrow k$, а потом вычесть из исходного выражения, то получится коммутационное соотношение $[\sigma_i\ \sigma_k] = 2 \cdot i \cdot \varepsilon_{ikl}\ \sigma_l$, которое эквивалентно (2.28), если учесть, что $\hat{\vec{S}}_j = \frac{1}{2}\ \sigma_j$.

5. Доказать соотношение $(\vec{a} \cdot \vec{\sigma}) \cdot (\vec{b} \cdot \vec{\sigma}) = (\vec{a} \cdot \vec{b}) + i \cdot [\vec{a} \times \vec{b}]\vec{\sigma}$.

Указание

Воспользоваться свойством (2.44).

6. Пусть $\{|n\rangle\}$ есть полный ортонормированный базис гильбертова пространства состояний квантовой системы, а $F_{mn} = \langle m | \hat{F} | n \rangle$ – матричные элементы линейного оператора $\hat{F}$.

Покажите, что оператор $\hat{F}$ можно представить в виде

$$\hat{F} = \sum_{mn} F_{mn} |m\rangle\langle n| .$$

В частности, в двумерном пространстве состояний с базисом $\{|0\rangle, |1\rangle\}$ произвольный линейный оператор записывается в виде

$$\hat{F} = F_{00}|0\rangle\langle 0| + F_{01}|0\rangle\langle 1| + F_{10}|1\rangle\langle 0| + F_{11}|1\rangle\langle 1| .$$

Убедитесь, что матрицы операторов $|0\rangle\langle 1| + |1\rangle\langle 0|$, $-i\left(|0\rangle\langle 1| - |1\rangle\langle 0|\right)$ и $|0\rangle\langle 0| - |1\rangle\langle 1|$, которые написаны справа в формулах (2.47), совпадают с матрицами Паули, соответственно, σ_x, σ_y и σ_z. Какой вид имеют матрицы операторов $(\sigma_x \pm i\sigma_y)/2$?

7. Доказать следующие свойства унитарного оператора $\hat{U}$.

(а) Собственные значения $\hat{U}$ по модулю равны 1.

(б) $\left|Det\hat{U}\right| = 1$, где $Det\hat{U}$ – определитель матрицы $\hat{U}$.

(в) Если $\hat{U}(\lambda) = \exp\left(i\lambda\hat{F}\right)$, где λ – действительный параметр, то $\hat{F} = \hat{F}^{+}$. Эрмитовый оператор $\hat{F}$ называется генератором непрерывного унитарного преобразования $\hat{U}(\lambda)$.

(г) $Det\hat{U}(\lambda) = \exp\left(i\lambda Sp\hat{F}\right)$, где $Sp\hat{F}$ обозначает след оператора $\hat{F}$.

(д) $\hat{U}(\lambda_1 + \lambda_2) = \hat{U}(\lambda_1)\hat{U}(\lambda_2)$. Это соотношение называется групповым свойством.

(г) Произведение унитарных операторов является унитарным оператором.

Доказательство

Пусть операторы $\hat{U}_1$ и $\hat{U}_2$ являются унитарными, т.е. удовлетворяют условиям

$$\hat{U}_1 \hat{U}_1^{+}=\hat{U}_1^{+}\hat{U}_1=1,\ \hat{U}_2 \hat{U}_2^{+}=\hat{U}_2^{+}\hat{U}_2=\mathbf{1}.$$

Рассмотрим оператор $\hat{U}=\hat{U}_2 \hat{U}_1$. Так как операция эрмитового сопряжения означает комплексное сопряжение и транспонирование оператора, то при эрмитовом сопряжении произведения операторов каждый из них подвергается эрмитовому сопряжению, и они располагаются в обратном порядке, т.е. $\hat{U}^{+}=(\hat{U}_2 \hat{U}_1)^{+}=\hat{U}_1^{+}\hat{U}_2^{+}$. Тогда имеем

$$\hat{U}\ \hat{U}^{+}=\hat{U}_2 \hat{U}_1(\hat{U}_1^{+}\hat{U}_2^{+})=\hat{U}_2(\hat{U}_1 \hat{U}_1^{+})\hat{U}_2^{+}=\hat{U}_2 \hat{U}_2^{+}=\mathbf{1}.$$

Аналогичным способом получаем, что $\hat{U}^{+}\hat{U}=\mathbf{1}$. Таким образом, оператор $\hat{U}$ удовлетворяет условию унитарности.

8. Доказать, что оператор сдвига относительной фазы $P(\varphi)\equiv|0\rangle\langle 0|+e^{i\cdot\varphi}|1\rangle\langle 1|$ является унитарным.

Доказательство

В вычислительном базисе $\{|0\rangle,|1\rangle\}$ матрица оператора $P(\varphi)$ является, очевидно, диагональной

$$P(\varphi)=\begin{pmatrix} P_{00} & P_{01} \\ P_{10} & P_{11} \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & e^{i\cdot\phi} \end{pmatrix}.$$

Поэтому

$$P(\varphi)\ P(\varphi)^{+} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\cdot\varphi} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\cdot\varphi} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbf{1}.$$

С методической точки зрения представляется полезным проверить выполнение условия унитарности непосредственным перемножением операторных выражений для $P(\varphi)$ и $P(\varphi)^{+}$. Тогда имеем

$$P(\phi)P^{+}(\phi) = \left(|0\rangle\langle 0| + e^{i\phi}|1\rangle\langle 1|\right)\left(|0\rangle\langle 0| + e^{-i\phi}|1\rangle\langle 1|\right) =$$
$$= |0\rangle\langle 0| + |1\rangle\langle 1| = \mathbf{1}.$$

На последнем шаге мы использовали условие полноты (2.6) базисных состояний, которое называют спектральным разложением единицы.

9. Доказать, что оператор Адамара H обладает следующими свойствами:

(а) $H^2 = \mathbf{1}$

Доказательство

Воспользуемся выражением для H через матрицы Паули, т.е. $H = \frac{1}{\sqrt{2}} \cdot (\sigma_1 + \sigma_3)$.

Тогда

$$H^2 = \frac{1}{2} \cdot (\sigma_1 + \sigma_3)^2 = \frac{1}{2}(\sigma_1^{\,2} + \sigma_3^{\,2} + \sigma_1\sigma_3 + \sigma_3\sigma_1) = \mathbf{1}.$$

Здесь мы использовали свойство (2.45), т.е. $\sigma_1^{\,2} = \sigma_3^{\,2} = \mathbf{1}$; а также свойство (2.46) антикоммутации разноименных матриц Паули, т.е. $\sigma_1\sigma_3 = -\sigma_3\sigma_1$.

(б) Собственные значения λ оператора H равны $\lambda = \pm 1$.

(в) Собственные состояния H, отвечающие этим собственным значениям, имеют вид

$$u_1 = \begin{pmatrix} \cos\dfrac{\pi}{8} \\ \sin\dfrac{\pi}{8} \end{pmatrix}, \quad u_{-1} = \begin{pmatrix} \sin\dfrac{\pi}{8} \\ -\cos\dfrac{\pi}{8} \end{pmatrix}.$$

(г) Унитарный оператор H есть преобразование поворота спина на угол π вокруг оси $\vec{n} = \left\{\dfrac{1}{\sqrt{2}}, 0, \dfrac{1}{\sqrt{2}}\right\}$.

Указание

Записать H в виде $H = \vec{\sigma}\vec{n} = \exp\left(-i\dfrac{\pi}{2}\right)\exp\left[i\pi\left(\hat{\vec{s}}\vec{n}\right)\right]$.

10. Написать матрицу конечных вращений для спина $\dfrac{1}{2}$.

Решение

Оператор конечных вращений $\hat{R}(\Phi, \vec{n}) = e^{i\frac{\Phi}{2}\vec{n}\vec{\sigma}}$ представляет собой экспоненциальную функцию от матриц Паули. Воспользуемся известным разложением экспоненты в ряд Тейлора

$$e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!}$$

и запишем $\hat{R}$ в виде

$$\hat{R} = \sum_{k=0}^{\infty} \frac{(i\Phi/2)^k}{k!}(\vec{n}\vec{\sigma})^k =$$

$$= \sum_{s=0}^{\infty} \frac{(i\Phi/2)^{2s}}{(2s)!}(\vec{n}\vec{\sigma})^{2s} + \sum_{s=0}^{\infty} \frac{(i\Phi/2)^{2s+1}}{(2s+1)!}(\vec{n}\vec{\sigma})^{2s+1},$$

где на последнем шаге вся сумма разбита на две части – по четным (k=2s) и нечетным (k=2s+1) значениям k. Рассмотрим величину $(\vec{n}\vec{\sigma})^2$. С учетом свойства (2.44) имеем

$$(\vec{n}\vec{\sigma})^2 = n_j n_k \sigma_j \sigma_k = n_j n_k (\delta_{jk} + i\varepsilon_{jkl}\sigma_l) = \vec{n}^2 + i[\vec{n}\times\vec{n}]\vec{\sigma} = 1,$$

так как

$$\vec{n}^2 = 1, \text{ а } [\vec{n}\times\vec{n}] = 0.$$

Тогда

$$\sum_{s=0}^{\infty} \frac{(i\Phi/2)^{2s}}{(2s)!}[(\vec{n}\vec{\sigma})^2]^s = \sum_{s=0}^{\infty} \frac{(-1)^s(\Phi/2)^{2s}}{(2s)!} = \cos\frac{\Phi}{2},$$

и

$$\sum_{s=0}^{\infty} \frac{(i\Phi/2)^{2s+1}}{(2s+1)!}(\vec{n}\vec{\sigma})[(\vec{n}\vec{\sigma})^2]^s = \\ = i\vec{n}\vec{\sigma}\sum_{s=0}^{\infty} \frac{(-1)^s(\Phi/2)^{2s+1}}{(2s+1)!} = i\vec{n}\vec{\sigma}\sin\frac{\Phi}{2}.$$

Здесь были использованы известные разложения функций $\cos x$ и $\sin x$ в ряд Тейлора.

Таким образом

$$\hat{R}(\Phi,\vec{n}) = e^{i\frac{\Phi}{2}\vec{n}\vec{\sigma}} = \cos\frac{\Phi}{2} + i\vec{n}\vec{\sigma}\sin\frac{\Phi}{2}.$$

Подставляя сюда явный вид матриц Паули и компоненты единичного вектора

$$\vec{n} = \{\sin\theta\cos\varphi, \sin\theta\sin\varphi, \cos\theta\},$$

получаем матрицу

$$\hat{R}(\Phi,\vec{n})=\begin{pmatrix}\cos\dfrac{\Phi}{2}+in_z\sin\dfrac{\Phi}{2} & i(n_x-in_y)\sin\dfrac{\Phi}{2}\\ i(n_x+in_y)\sin\dfrac{\Phi}{2} & \cos\dfrac{\Phi}{2}-in_z\sin\dfrac{\Phi}{2}\end{pmatrix}=$$

$$=\begin{pmatrix}\cos\dfrac{\Phi}{2}+i\cos\theta\sin\dfrac{\Phi}{2} & i\cdot e^{-i\cdot\phi}\cdot\sin\dfrac{\Phi}{2}\cdot\sin\theta\\ ie^{i\cdot\phi}\sin\dfrac{\Phi}{2}\sin\theta & \cos\dfrac{\Phi}{2}-i\cos\theta\sin\dfrac{\Phi}{2}\end{pmatrix},$$

которая входит в формулу (2.68) и вместе с фазовыми множителем $e^{i\cdot\alpha}$ определяет общий вид унитарной матрицы 2×2.

11. Вычислить результирующую матрицу вращения $\hat{R}(\beta,\gamma,\delta)=\hat{R}_z(\beta)\hat{R}_y(\gamma)\hat{R}_z(\delta)$, где $\hat{R}_z$ и $\hat{R}_y$ описывают вращение спина $1/2$ вокруг осей *z* и *y* на углы, указанные в аргументах. Сравнить с выражением (2.70).

12. То же самое, когда вместо вращения $\hat{R}_y$ происходит преобразование $\hat{R}_x$.

13. Найти явный вид операторов $\sqrt{\sigma_i}$, где σ_i – матрицы Паули.

Указание

Если взять, например, преобразование вращения спина $1/2$ вокруг оси *x* на угол π, то $\exp\left(i\dfrac{\pi}{2}\sigma_1\right)=i\sigma_1$,

$$\sqrt{\sigma_1}=\exp\left(-i\frac{\pi}{4}\right)\exp\left(i\frac{\pi}{4}\sigma_1\right)=e^{-i\frac{\pi}{4}}\frac{1+i\sigma_1}{\sqrt{2}}.$$

2.3. Многокубитовый регистр

В этом разделе мы рассмотрим квантовую систему, состоящую из n кубитов. Такую систему называют n-кубитовым регистром. Обсудим пространство состояний многокубитового квантового регистра и линейные операторы, действующие в этом пространстве, а также методы описания состояний и операторов.

Базисные векторы n-кубитовой системы строятся как произведения n штук базисных векторов отдельных кубитов

$$\left|C_{n\text{-}1}\right\rangle\left|C_{n\text{-}2}\right\rangle\ldots\left|C_1\right\rangle\left|C_0\right\rangle \equiv \left|C_{n\text{-}1}\ C_{n\text{-}2}\ \ldots C_1\,C_0\right\rangle. \qquad (2.108)$$

Здесь каждая из величин C_i принимает одно из двух значений, 0 или 1, так что символом $\left|C_i\right\rangle$ представлены базисные векторы отдельного кубита. Строго говоря, стоящее слева произведение однокубитовых векторов состояний представляет собой так называемое тензорное (или прямое) произведение[1]. Мы, однако, не будем использовать никаких специальных обозначений для такого тензорного произведения, а будем просто писать кэт-векторы однокубитовых состояний рядом как сомножители и называть такое состояние *факторизованным.* Заметим, что в предыдущем разделе такая запись была использована в формуле (2.19) для вектора состояния фотона как произведения соответствующих кэт-векторов, относящихся к пространственным и поляризационным степеням

[1] Если вектор |α> принадлежит гильбертову пространству H_1 с размерностью d_1, а вектор |β> — гильбертову пространству H_2 с размерностью d_2 , то вектор $|\alpha\rangle \otimes |\beta\rangle \equiv |\alpha\rangle|\beta\rangle$, являющийся тензорным произведением векторов, принадлежит гильбертову пространству $H = H_1 \otimes H_2$ с размерностью $d = d_1\, d_2$, которое называют тензорным произведением пространств H_1 и H_2. Размерность пространства каждого из кубитов равна 2. Поэтому вектор состояния $|\alpha\rangle \otimes |\beta\rangle \equiv |\alpha\rangle|\beta\rangle$ двухкубитовой системы принадлежит пространству с размерностью 2·2=4. Тензорное произведение пространств и тензорное произведение векторов сохраняет фундаментальный физический принцип суперпозиции (или, говоря математическим языком, линейную структуру пространства) при переходе к пространствам большей размерности.

свободы. Произведение однокубитовых базисных векторов мы будем писать также в виде одного вектора состояния, обозначенного скобкой $|...\rangle$, внутри которой стоит, как это написано в правой части (2.108), цепочка двоичных символов. В дальнейшем для определенности будем считать, что в произведении (2.108) кубиты расположены (перенумерованы) слева направо.

Поскольку каждый из кубитов имеет два базисных состояния (C_i=0, 1), то n-кубитовый регистр (i=0, 1,…, n–1) имеет 2^n базисных векторов, т.е. размерность пространства квантовых состояний n-кубитовой системы равна 2^n. Ниже мы увидим, что именно с этим простым, по сути, фактом связана экспоненциально большая информационная емкость квантового регистра, если он содержит достаточно большое число кубитов, $n >> 1$.

Обозначающая базисный вектор (2.108) цепочка

$$(C_{n-1}\, C_{n-2}\, \ldots\, C_1\, C_0),$$

состоящая из нулей и единиц, идентифицируется как двоичная запись некоторого целого числа S:

$$S = C_{n-1}\, 2^{n-1} + C_{n-2}\, 2^{n-2} + \ldots + C_1\, 2^1 + C_0\, 2^0 , \qquad (2.109)$$

находящегося в пределах от 0 до 2^n-1. Сам базисный вектор тоже можно для краткости обозначить как

$$\left| C_{n-1}\ C_{n-2}\ \ldots C_1\, C_0 \right\rangle = \left| S \right\rangle \qquad (2.110)$$

и считать, что базисные векторы перенумерованы с помощью этого числа, т.е. их последовательность выглядит так: $|00...00\rangle$, $|00...01\rangle$, $|11...11\rangle$.

Отметим также, что отдельные кубиты в базисных состояниях (2.110) многокубитового регистра считаются перенумерованными слева направо, так что первый кубит соответствует наибольшему двоичному разряду, а последний – наименьшему.

На квантовых схемах мы будем располагать линии отдельных кубитов сверху вниз в том же порядке, как это показано на рис. 2.8.

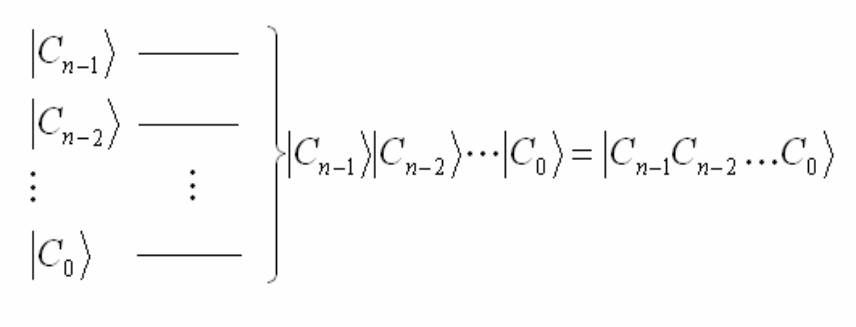


Рис. **2.8**

Совокупность базисных векторов (2.110) является полной ортонормированной системой, т.е. они удовлетворяют условиям нормировки, ортогональности и полноты:

$$\langle S'|S\rangle = \delta\, s`s\,, \tag{2.111}$$

$$\sum_{s=0}^{2^n-1} |S\rangle\langle S| = 1\ . \tag{2.112}$$

Этот набор состояний используется в качестве вычислительного базиса. На основании принципа суперпозиции произвольное состояние $|\psi\rangle$ рассматриваемого *n*-кубитового регистра имеет вид

$$|\psi\rangle = a_0|0\ldots00\rangle + a_1|0\ldots01\rangle + \ldots + a_{2^n-2}|1\ldots10\rangle + a_{2^n-1}|1\ldots11\rangle \equiv$$

$$\equiv \sum_{s=0}^{2^n-1} a_s\,|\,S\rangle\ . \tag{2.113}$$

Это означает, что с помощью такой квантовой системы можно одновременно записать 2^n различных чисел S от 0 до 2^n–1. В этом смысле можно говорить об экспоненциально большой информационной емкости квантового регистра, содержащего достаточно

большое число кубитов[1]. Еще раз обратим внимание, что, как и в случае одного кубита, состояния вычислительного базиса входят в (2.113) в виде когерентной суперпозиции, комплексные коэффициенты которой определяют не только меру (вероятность) присутствия в квантовом состоянии кубита каждого из базисных векторов, представляющих двоичные числа, но и фазовые соотношения между ними.

Рассмотрим для примера систему, состоящую из двух кубитов. Она имеет 4 базисных состояния

$$\left|00\right\rangle = \left|0\right\rangle\left|0\right\rangle,\ \left|01\right\rangle = \left|0\right\rangle\left|1\right\rangle,\quad \left|10\right\rangle = \left|1\right\rangle\left|0\right\rangle,\quad \left|11\right\rangle = \left|1\right\rangle\left|1\right\rangle, \quad (2.114)$$

представляющих в двоичной записи числа 0, 1, 2 и 3, соответственно. Данная двухкубитовая система может находиться, например, в состоянии

$$\left|\psi\right\rangle = \frac{1}{2}\left\{\left|00\right\rangle + \left|01\right\rangle + \left|10\right\rangle + \left|11\right\rangle\right\}, \quad (2.115)$$

в котором все указанные числа оказываются представленными в виде однородной и синфазной суперпозиции.

Состояние $\left|\psi\right\rangle$ полностью определяется совокупностью 2^n комплексных чисел $a_0, a_1, a_2, \ldots, a_2{}^n{}_{-1}$, которые стоят в виде коэффициентов при базисных векторах. Эти числа представляют собой скалярные произведения[2]

$$a_s = \left\langle S\middle|\psi\right\rangle,\ S = 0, 1, \ldots, 2^n - 1. \quad (2.116)$$

---

[1] Пусть n = 500, т.е. имеется регистр, содержащий 500 кубитов. В нем можно записать сразу 2^{500} чисел, а это больше, чем число атомов во Вселенной.

[2] Напомним, что скалярное произведение двух векторов $|\Psi_1\rangle$ и $|\Psi_2\rangle$ в гильбертовом пространстве состояний квантовой системы определяется как комплексное число $\langle\Psi_2|\Psi_1\rangle$, удовлетворяющее условию, что $\langle\Psi_1|\Psi_2\rangle = \langle\Psi_2|\Psi_1\rangle^*$. Это гарантирует, что квадрат нормы любого вектора состояния $|\Psi\rangle$, т.е. скалярное произведение $\langle\Psi|\Psi\rangle$ строго больше нуля. О скалярных произведениях (2.116) можно говорить как о проекциях вектора $|\Psi\rangle$ на базисные векторы $|S\rangle$.

Они занумерованы с помощью индекса, совпадающего со значением (2.109) числа S, двоичная запись которого представлена цепочкой из нулей и единиц, написанной внутри скобок $|...\rangle$, обозначающих базисные кэт-векторы. Комплексные числа a_s в суперпозициях вида (2.113) могут быть произвольными.

Единственное ограничение связано с условием нормировки

$$\langle\psi|\psi\rangle = 1 \tag{2.117}$$

состояния $|\psi\rangle$, которое эквивалентно соотношению

$$\sum_{s=0}^{2^n-1} |a_s|^2 = 1. \tag{2.118}$$

Действительно, подставляя условие полноты (2.112) в левую часть (2.117), получаем

$$\langle\psi|\psi\rangle = \langle\psi|\sum_{s=0}^{2^n-1}|S\rangle\langle S|\psi\rangle = \sum_{s=0}^{2^n-1}\langle\psi|S\rangle\langle S|\psi\rangle =$$

$$= \sum_{s=0}^{2^n-1}|\langle S|\psi\rangle|^2 = \sum_{s=0}^{2^n-1}|a_s|^2 = 1.$$

Здесь при вычислениях мы воспользовались выражением (2.116) для коэффициентов a_s и свойством скалярного произведения

$$\langle\psi|S\rangle = \langle S|\psi\rangle^* = a_s^* .$$

Итак, в базисе (2.110) любое состояние $|\psi\rangle$ взаимно однозначно задается совокупностью коэффициентов разложения $\{a_s\}$, которые,

тем самым, можно использовать для описания состояния $|\psi\rangle$. Этот набор комплексных чисел мы будем писать в виде 2^n — компонентного вектор-столбца

$$|\psi\rangle = \begin{pmatrix} a_0 \\ a_1 \\ \dots \\ a_{2^n-1} \end{pmatrix}, \qquad (2.119)$$

расположив его компоненты в порядке возрастания индекса сверху вниз.

Теперь перейдем к рассмотрению линейных операторов, действующих в гильбертовом пространстве состояний *n*-кубитового регистра. Пусть в результате действия оператора $\hat{F}$ на состояние $|\psi\rangle$ получаем состояние $|\Phi\rangle$, т.е.

$$\hat{F}\,|\psi\rangle = |\Phi\rangle\ . \qquad (2.120)$$

Представим векторы $|\psi\rangle$ и $|\Phi\rangle$ в виде разложений по базисным состояниям $|S\rangle$:

$$|\psi\rangle = \sum_{s'} a_{s'} |S'\rangle, \quad |\Phi\rangle = \sum_{s} b_s |S\rangle. \qquad (2.121)$$

Подставляем эти разложения в (2.120) и, учитывая линейность оператора $\hat{F}$, имеем

$$|\Phi\rangle = \sum_{s} b_s |S\rangle = \hat{F} \sum_{s'} a_{s'} |S'\rangle = \sum_{s'} a_{s'} \hat{F} |S'\rangle,$$

т.е.

$$\sum_{s} b_s |S\rangle = \sum_{s'} a_{s'} \hat{F} |S'\rangle. \qquad (2.122)$$

Проектируя обе части (2.122) на базисные векторы $|S\rangle$ с учетом условия ортонормированности (2.111), получаем

$$b_s = \sum_{s'} \langle S|\hat{F}|S'\rangle a_{s'} = \sum_{s'} F_{ss'} a_{s'} , \qquad (2.123)$$

где $s, s' = 0, 1, \ldots, 2^n - 1$. Совокупность $2^n \times 2^n$ комплексных чисел

$$F_{ss'} \equiv \langle S|\hat{F}|S'\rangle , \qquad (2.124)$$

которые называются матричными элементами оператора $\hat{F}$ в базисе $\{|S\rangle\}$, образуют матрицу

$$\hat{F} = \begin{pmatrix} F_{00} & F_{01} & \ldots & F_{0,2^n-1} \\ F_{10} & \ldots & \ldots & F_{1,2^n-1} \\ \ldots & \ldots & F_{ss'} & \ldots \\ F_{2^n-1,0} & \ldots & \ldots & F_{2^n-1,2^n-1} \end{pmatrix}. \qquad (2.125)$$

Первый индекс матричного элемента — номер строки, а второй — номер столбца. Компактная алгебраическая запись (2.123) показывает, что вектор-столбец $\{b_s\}$, описывающий состояние $|\Phi\rangle = \hat{F}|\psi\rangle$, получается из вектор-столбца $\{a_s\}$, описывающего состояние $|\psi\rangle$, как результат умножения слева (по стандартным правила матричной алгебры) на матрицу $F_{ss'}$, которая соответствует линейному оператору $\hat{F}$, т.е.

$$\begin{pmatrix} b_0 \\ b_1 \\ \ldots \\ b_{2^n-1} \end{pmatrix} = \begin{pmatrix} F_{00} & F_{01} & \ldots & F_{0,2^n-1} \\ F_{10} & \ldots & \ldots & F_{1,2^n-1} \\ \ldots & \ldots & F_{ss'} & \ldots \\ F_{2^n-1,0} & \ldots & \ldots & F_{2^n-1,2^n-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \ldots \\ a_{2^n-1} \end{pmatrix}. \qquad (2.126)$$

Представление, которое описывается соотношениями (2.119), (2.123)-(2.126), называется матричным представлением. В дальнейшем мы будем применять его, используя, как правило, компактные формулы вида (2.116), (2.121), (2.123), (2.124).

Что касается "многоэтажных" конструкций типа (2.126), то мы иногда будем прибегать к ним, иллюстрируя вид матриц тех или иных операторов, действующих в пространстве состояний небольшого числа кубитов.

Тензорное произведение

Мы уже говорили, что с помощью тензорного произведения пространств меньшей размерности можно построить пространство большей размерности.

Рассмотрим для примера пространство состояний 2-кубитовой системы, которое есть тензорное произведение (его называют также прямым произведением) $H_2 = H_1 \otimes H_1$ пространств состояний двух однокубитовых систем, и продемонстрируем правила вычисления тензорного произведения двух однокубитовых вектор-столбцов, а также матриц операторов, действующих на состояния отдельных кубитов.

Вектор-столбцы, соответствующие базисным состояниям $|0\rangle$ и $|1\rangle$ каждого кубита, имеют вид

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{2.127}$$

Полному набору базисных состояний 2-кубитовой системы

$$|00\rangle = |0\rangle\,|0\rangle, \; |01\rangle = |0\rangle\,|1\rangle, \; |10\rangle = |1\rangle\,|0\rangle \;\text{ и }\; |11\rangle = |1\rangle\,|1\rangle,$$

которые строятся как тензорные произведения базисных векторов каждого из кубитов, отвечают, в соответствии с общими формулами (2.113) и (2.119) перехода к спинорному представлению,

4-компонентные вектор-столбцы

$$|00\rangle = \begin{pmatrix}1\\0\\0\\0\end{pmatrix},\ |01\rangle = \begin{pmatrix}0\\1\\0\\0\end{pmatrix},\ |10\rangle = \begin{pmatrix}0\\0\\1\\0\end{pmatrix} \text{ и } |11\rangle = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}. \quad (2.128)$$

Поэтому эти вектор-столбцы являются тензорными произведениями однокубитовых вектор-столбцов (2.127). Чтобы понять правило вычисления тензорного произведения вектор-столбцов, рассмотрим вектор состояния 2-кубитовой системы

$$|ab\rangle = |a\rangle_1 |b\rangle_2, \quad (2.129)$$

который есть произведение векторов состояний

$$\begin{aligned} |a\rangle_1 &= a_0|0\rangle_1 + a_1|1\rangle_1 = \begin{pmatrix}a_0\\a_1\end{pmatrix}_1, \\ |b\rangle_2 &= b_0|0\rangle_2 + b_1|1\rangle_2 = \begin{pmatrix}b_0\\b_1\end{pmatrix}_2 \end{aligned} \quad (2.130)$$

двух кубитов, отмеченных индексами 1 и 2. Подставляем (2.130) в (2.129) и перемножаем почленно, располагая кубиты в порядке нумерации слева направо. Тогда

$$\begin{aligned} |ab\rangle &= (a_0|0\rangle_1 + a_1|1\rangle_1)(b_0|0\rangle_2 + b_1|1\rangle_2) = a_0b_0|0\rangle_1|0\rangle_2 + \\ &+ a_0b_1|0\rangle_1|1\rangle_2 + a_1b_0|1\rangle_1|0\rangle_2 + a_1b_1|1\rangle_1|1\rangle_2 = \\ &= a_0b_0|00\rangle + a_0b_1|01\rangle + a_1b_0|10\rangle + a_1b_1|11\rangle. \end{aligned} \quad (2.131)$$

Из этого разложения видно, что вектор-столбец двухкубитовой системы получается из вектор-столбцов (2.130) с помощью равенства

$$\begin{pmatrix} a_0 \\ a_1 \end{pmatrix}_1 \otimes \begin{pmatrix} b_0 \\ b_1 \end{pmatrix}_2 = \begin{pmatrix} a_0\, b_0 \\ a_0\, b_1 \\ a_1\, b_0 \\ a_1\, b_1 \end{pmatrix} = \begin{pmatrix} a_0 \begin{pmatrix} b_0 \\ b_1 \end{pmatrix} \\ a_1 \begin{pmatrix} b_0 \\ b_1 \end{pmatrix} \end{pmatrix}. \qquad (2.132)$$

На последнем шаге в (2.132) 4-компонентный вектор-столбец специально записан в такой форме, что процедура вычисления выглядит вполне очевидной. Обратим также внимание, что результирующий вектор-столбец в (2.132), т.е. расположение его компонент, зависит от порядка сомножителей. Соблюдение такого порядка расположения однокубитовых вектор-столбцов, когда на первом месте стоит первый кубит, на втором месте – второй кубит и так далее, позволяет сохранить единую нумерацию базисных векторов (2.110) и, соответственно, компонент спинора (2.119). Сформулированное правило вычисления тензорного произведения, которое называют также *кронекеровым произведением*, очевидным образом обобщается на произведение любого числа любых вектор-столбцов. В качестве иллюстрации можно проверить, что вычисленные с помощью формулы (2.132) тензорные произведения вектор-столбцов (2.127), отвечающих однокубитовым базисным состояниям, действительно дают вектор-столбцы (2.128), которые описывают базисные состояния двухкубитовой системы.

Теперь рассмотрим правило вычисления кронекерова произведения матриц. Пусть на состояние (2.129) двухкубитовой системы действует линейный оператор $\hat{F} \otimes \hat{G} = \hat{F}\hat{G}$, представляющий собой произведение двух операторов. При этом каждый из операторов действует на состояние только одного из кубитов. Для определенности считаем, что $\hat{F}$ действует на $|a\rangle_1$, а $\hat{G}$ действует на $|b\rangle_2$ следующим образом:

$$(\hat{F} \otimes \hat{G})|ab\rangle = \left(\hat{F}|a\rangle_1\right) \otimes \left(\hat{G}|b\rangle_2\right). \qquad (2.133)$$

В матричном представлении состояния $|a\rangle_1$ и $|b\rangle_2$ изображаются вектор-столбцами (2.130), а операторам $\hat{F}$ и $\hat{G}$ отвечают матрицы 2×2:

$$\hat{F} = \begin{pmatrix} F_{00} & F_{01} \\ F_{10} & F_{11} \end{pmatrix}, \quad \hat{G} = \begin{pmatrix} G_{00} & G_{01} \\ G_{10} & G_{11} \end{pmatrix}, \qquad (2.134)$$

матричные элементы которых $F_{ss'}$ и $G_{rr'}$ $(s,s',r,r'=0, 1)$ вычислены в базисе состояний $\{|0\rangle, |1\rangle\}_{1,2}$ для каждого из кубитов. В правой части (2.133) стоит тензорное произведение двух вектор-столбцов

$$\hat{F}\,|a\rangle_1 = \begin{pmatrix} F_{00} & F_{01} \\ F_{10} & F_{11} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \end{pmatrix}_1 \equiv \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} \qquad (2.135)$$

и

$$\hat{G}\,|b\rangle_2 = \begin{pmatrix} G_{00} & G_{01} \\ G_{10} & G_{11} \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \end{pmatrix}_2 \equiv \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix}, \qquad (2.136)$$

которое, согласно (2.132), имеет вид

$$\begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} \otimes \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix} = \begin{pmatrix} \alpha_0\,\beta_0 \\ \alpha_0\,\beta_1 \\ \alpha_1\,\beta_0 \\ \alpha_1\,\beta_1 \end{pmatrix} = \begin{pmatrix} \alpha_0 \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix} \\ \alpha_1 \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix} \end{pmatrix}. \qquad (2.137)$$

Дальнейшая, довольно скучная, процедура вычислений состоит в следующем. С помощью (2.135) и (2.136) выражаем α_0 и α_1 через a_0, a_1, а также β_0 и β_1 через b_0, b_1 вместе с соответствующими матричными элементами операторов $\hat{F}$ и $\hat{G}$, а затем подставляем

их в выражение (2.137) для 4-компонентного вектор-столбца. Получившийся вектор-столбец, как это и следует из левой части (2.133), будет представлять собой результат действия некоторой 4×4 матрицы на 4-компонентный вектор-столбец (см. (2.132)):

$$\begin{pmatrix} a_0 \\ a_1 \end{pmatrix}_1 \otimes \begin{pmatrix} b_0 \\ b_1 \end{pmatrix}_2 = \begin{pmatrix} a_0\, b_0 \\ a_0\, b_1 \\ a_1\, b_0 \\ a_1\, b_1 \end{pmatrix},$$

описывающий исходное состояние $|ab\rangle$ 2-кубитовой системы. В силу линейности (2.133) по a_s и $b_{s'}$ указанная матрица зависит только от матричных элементов $F_{ss'}$ и $G_{rr'}$. Она и представляет собой интересующую нас 4×4 матрицу оператора $(\hat{F}\otimes\hat{G})$, т.е. кронекерово произведение матриц операторов $\hat{F}$ и $\hat{G}$. Проделав описанные выше вычисления, получаем

$$\hat{F}\otimes\hat{G} = \begin{pmatrix} F_{00}\cdot\hat{G} & F_{01}\cdot\hat{G} \\ F_{10}\cdot\hat{G} & F_{11}\cdot\hat{G} \end{pmatrix}. \qquad (2.138)$$

Для компактности мы использовали символическую запись, в которой $\hat{G}$ обозначает 2×2 матрицу оператора $\hat{G}$ (см. (2.134)). Поэтому, например, символ $F_{01}\cdot\hat{G}$ обозначает 2×2 матрицу

$$F_{01}\cdot\hat{G} \equiv F_{01}\begin{pmatrix} G_{00} & G_{01} \\ G_{10} & G_{11} \end{pmatrix}. \qquad (2.139)$$

Сформулированное правило вычисления кронекерова произведения матриц очевидным образом обобщается на случай матриц более высокой размерности.

В качестве примера рассмотрим тензорное произведение

$H^{\otimes 2} \equiv H \otimes H$ двух однокубитовых преобразований Адамара (2.64). Используя правило (2.138), получаем

$$H^{\otimes 2} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} =$$

$$= \frac{1}{2}\begin{pmatrix} 1\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} & 1\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \\ 1\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} & -1\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}. \quad (2.140)$$

Эта матрица представляет собой некоторый унитарный оператор, действующий в пространстве состояний двухкубитового регистра, т.е. является простым примером двухкубитового гейта. На рис. 2.9 слева изображена квантовая схема, показывающая, как на каждый из двух кубитов действует преобразование Адамара H. Справа изображена эквивалентная схема с двухкубитовым гейтом $H^{\otimes 2}$.

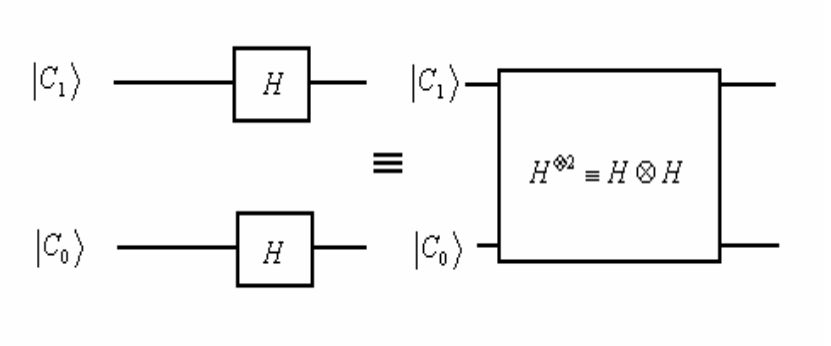


Рис. **2.9**

Продемонстрируем действие данного преобразования на двухкубитовый регистр, который сначала находится в состоянии $|C_1 C_0\rangle = |00\rangle$. С точки зрения левой схемы, это выглядит следующим образом:

$$(H\otimes H)\left|00\right\rangle=(H\left|0\right\rangle)(H\left|0\right\rangle)=$$
$$=\frac{\left|0\right\rangle+\left|1\right\rangle}{\sqrt{2}}\frac{\left|0\right\rangle+\left|1\right\rangle}{\sqrt{2}}=\frac{1}{2}\left\{\left|00\right\rangle+\left|01\right\rangle+\left|10\right\rangle+\left|11\right\rangle\right\}. \qquad (2.141)$$

Здесь при вычислении состояния $H\left|0\right\rangle$ мы использовали операторную форму преобразования Адамара (2.64). Эквивалентный результат дает и правая схема

$$H^{\otimes 2}\left|00\right\rangle=\frac{1}{2}\begin{pmatrix}1&1&1&1\\1&-1&1&-1\\1&1&-1&-1\\1&-1&-1&1\end{pmatrix}\begin{pmatrix}1\\0\\0\\0\end{pmatrix}=$$
$$=\frac{1}{2}\begin{pmatrix}1\\1\\1\\1\end{pmatrix}=\frac{1}{2}\left\{\begin{pmatrix}1\\0\\0\\0\end{pmatrix}+\begin{pmatrix}0\\1\\0\\0\end{pmatrix}+\begin{pmatrix}0\\0\\1\\0\end{pmatrix}+\begin{pmatrix}0\\0\\0\\1\end{pmatrix}\right\}. \qquad (2.142)$$

Здесь мы использовали выражение (2.140) для матрицы $H^{\otimes 2}$, записали начальное состояние в виде вектор-столбца $\begin{pmatrix}1\\0\\0\\0\end{pmatrix}$, а получившийся вектор-столбец разложили по спинорам (2.128), описывающим базисные состояния двухкубитового регистра. Примечательной чертой рассматриваемого преобразования является то, что в результате его действия на начальное состояние $\left|00\right\rangle$ получается состояние (2.141), которое является однородной и синфазной суперпозицией всех состояний, представляющих в двоичной записи числа 0, 1, 2 и 3.

Это свойство имеет место, разумеется, и для произвольного

n-кубитового регистра. Действительно, пусть *n*-кубитовый регистр находится в состоянии $|00...0\rangle$. Подействуем на каждый кубит преобразованием Адамара и получим состояние

$$(H \otimes H)|00...0\rangle = (H|0\rangle)(H|0\rangle)...(H|0\rangle) = \\ = \frac{|0\rangle+|1\rangle}{\sqrt{2}}\frac{|0\rangle+|1\rangle}{\sqrt{2}}\cdot...\cdot\frac{|0\rangle+|1\rangle}{\sqrt{2}} = 2^{-\frac{n}{2}}\sum_{x=0}^{2^n-1}|x\rangle \equiv |\psi_0\rangle, \quad (2.143)$$

в котором с одинаковыми амплитудами и фазами представлены все базисные векторы (2.110), изображающие в двоичном коде все числа *x* от 0 до $2^n - 1$. Квантовая схема этого процесса показана на рис. 2.10.

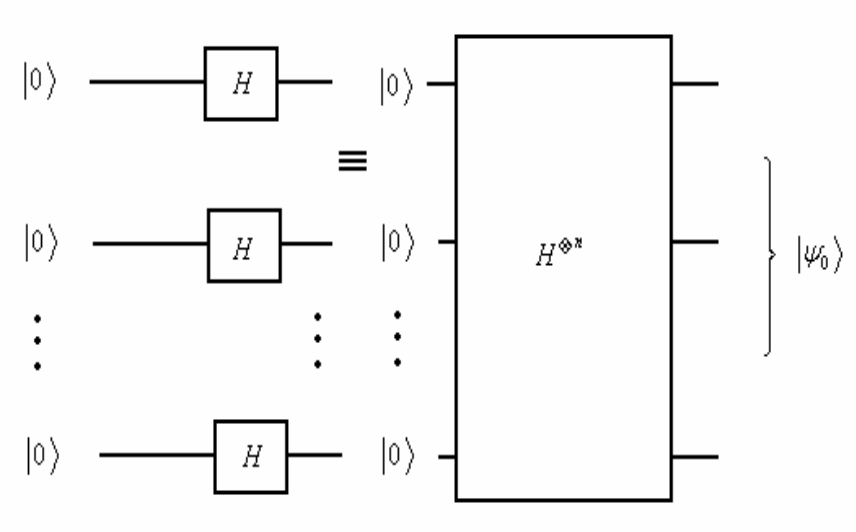


Рис. **2.10**

Суперпозиционное состояние (2.143) *n*-кубитового регистра часто используется в различных протоколах квантовой информатики. При этом мультикубитовый гейт $H^{\otimes n}$, порождающий данное состояние из начального вектора $|00...0\rangle$, является достаточно простым и целиком определяется свойством однокубитового преобразования Адамара (2.64). С помощью тензорного произведения всевозможных однокубитовых операторов можно построить много разнообразных мультикубитовых гейтов. Однако такие приводимые многокубитовые преобразования не содержат фактически ничего нового по сравнению со свойствами однокубитовых гейтов, из которых они построены. Но самое главное состоит в том, что указанные приводимые гейты не исчерпывают всего многообразия многокубитовых унитарных преобразований. Двухкубитовые и более сложные гейты мы обсудим в разделах 2.5 и 2.6.

Квантовый параллелизм

Квантовые вычисления сводятся к выполнению тех или иных унитарных преобразований в пространстве состояний квантового регистра, т.е. к унитарным преобразованиям полного набора базисных векторов системы. Сразу отметим важную особенность квантовых вычислений, обусловленную принципом суперпозиции. Если связанное с процедурой вычисления унитарное преобразование применено к такому квантовому состоянию регистра, которое имеет вид суперпозиции (2.113), то вычислительная операция оказывается выполненной сразу для всех чисел, представленных в этой суперпозиции. Это фундаментальное свойство квантовых вычислений называется *квантовым параллелизмом*. Идея квантового параллельного вычисления была сформулирована *Давидом Дойчем* в пионерской работе 1985 г.

Пусть, например, сконструировано унитарное преобразование, которое обеспечивает вычисление функции $f(x)$. Применяя это преобразование к состоянию $|\psi_0\rangle$ (2.143), мы за один проход данной вычислительной процедуры получаем значение функции $f(x)$ для всех 2^n значений аргумента *x*. Для многокубитового регистра,

когда n>>1, функция $f(x)$ оказывается вычисленной сразу в экспоненциально большом числе точек. Так работает квантовый параллелизм.

Во избежание недоразумений сделаем два замечания, касающиеся изложенного выше принципа квантового параллелизма. Во-первых, мы пока совершенно не касались вопроса о том, как сконструировать унитарное преобразование, т.е., как построить набор унитарных гейтов, реализующих интересующую нас вычислительную операцию. Некоторые аспекты этого важного вопроса будут обсуждаться в разделе 2.6. Во-вторых, полученные в результате квантового вычисления двоичные записи численных значений функции $f(x)$ будут представлены в квантовом состоянии регистра все сразу, но в виде квантовой суперпозиции соответствующих базисных векторов. В этом смысле, как уже отмечалось выше, в квантовом состоянии регистра содержится в принципе огромный объем информации. Но это есть квантовая информация, обладающая той особенностью, что при считывании большая ее часть, как правило, теряется.

Действительно, для считывания надо произвести измерение каждого кубита n-кубитовой системы в базисе состояний $|0\rangle$ и $|1\rangle$. Согласно постулату фон Неймана, это означает проектирование состояния кубита на указанный измерительный базис, а для всей системы – проектирование на полный набор базисных состояний (2.110). В результате получится один из кэт-векторов, которые входят в суперпозиционное состояние регистра с отличными от нуля коэффициентами. Другими словами, в результате измерения исходное квантовое состояние регистра будет разрушено, и система случайно окажется в одном из состояний измерительного базиса. Это принципиальное свойство процесса квантового измерения.

Так, например, проводя указанное измерение в состоянии $|\psi_0\rangle$ (2.143), мы случайным образом получим одну из 2^n равновероятных двоичных строк $x \equiv (C_{n-1}...C_1C_0)$, представленных векторами $|x\rangle$ в суперпозиции (2.143), т.е. извлечем, согласно (2.2), только $\log_2 2^n = n$ битов информации. Это ровно столько же, сколько содержится в классическом n-битовом регистре.

Поэтому можно задать вполне резонный вопрос о том, в чем же преимущества квантовых вычислений. А они в том, что экспоненциально большая информационная емкость квантового состояния позволяет эффективно манипулировать квантовой информацией со скоростью, которая не доступна никаким классическим вычислительным машинам. Поясним это на простом примере.

Пусть *n*-кубитовый регистр находится в некотором суперпозиционном состоянии вида (2.113). Применим к этому состоянию однокубитовую унитарную операцию $\hat{U}$, которая, для определенности, действует на первый кубит. Преобразование этого кубита

$$\hat{U}\left|C\right\rangle = \sum_{C'=0,1} U_{C'C}\left|C'\right\rangle \qquad (2.144)$$

описывается унитарной 2×2 матрицей $U_{c'c} = \left\langle C'\middle|\hat{U}\middle|C\right\rangle$. Для сокращения записи представим базисные векторы (2.110) в виде $\left|S\right\rangle \equiv \left|C\right\rangle\left|x\right\rangle$, где $\left|C\right\rangle$ — базисный вектор первого кубита, а $\left|x\right\rangle \equiv \left|C_{n-2}...C_1C_0\right\rangle$ — базисные состояния остальной (*n*–1) — кубитовой системы, т.е.

$$\left|\Psi\right\rangle = \sum_{S=0}^{2^{n-1}-1} a_S\left|S\right\rangle \equiv \sum_{C=0,1}\ \sum_{x=0}^{2^{n-1}-1} a_{Cx}\left|C\right\rangle\left|x\right\rangle\ . \qquad (2.145)$$

Применяем к этому состоянию операцию $\hat{U}$ и, учитывая соотношение (2.144), получаем

$$\hat{U}\left|\Psi\right\rangle = \sum_{C,x} a_{Cx}\left(\hat{U}\left|C\right\rangle\right)\left|x\right\rangle = \sum_{C,x} a_{Cx}\left(\sum_{C'} U_{c'c}\left|C'\right\rangle\right)\left|x\right\rangle =$$

$$= \sum_{C',x}\ \sum_{C=0,1}\left(U_{c'c}a_{Cx}\right)\left|C'\right\rangle\left|x\right\rangle \equiv \sum_{S=0}^{2^{n-1}-1} b_S\left|S\right\rangle, \qquad (2.146)$$

где $|S\rangle \equiv |C'\rangle|x\rangle$ опять представляют собой базисные векторы n-кубитового регистра, а новые коэффициенты b_S имеют вид

$$b_S \equiv b_{C'x} = \sum_{C=0,1} U_{c'c} a_{Cx} \ . \qquad (2.147)$$

Мы видим, что однократное применение операции $\hat{U}$, т.е. один шаг квантового вычисления позволяет получить все 2^n коэффициентов b_S из 2^n начальных коэффициентов $a_S \equiv a_{Cx}$.

Сравним с классическим вычислением, которое необходимо произвести, чтобы описать в общем виде такое же преобразование информации. Для этого надо вычислить совокупность коэффициентов b_S, имея на входе совокупность коэффициентов a_S. Выражение (2.147) показывает, что для такой операции потребуется применить 2×2 матрицу $U_{C'C}$ для каждого значения двоичной строки $x \equiv | C_{n-2}...C_1C_0 >$, т.е. 2^{n-1} раз. Повторяем, что квантовое вычисление производится за один шаг. При n>>1 это означает экспоненциальное сокращение количества операций.

В чем же корни столь разительного отличия эффективностей квантовой и классической вычислительных операций?

Прежде всего, это обусловлено принципом суперпозиции, гарантирующим существование квантовых состояний n-кубитового регистра, которые описываются кэт-векторами вида (2.113). Вычислительная операция, примененная к такому состоянию, работает сразу для всех входящих в него базисных векторов. Более того, в процессе вычисления проявляются все интерференционные квантовые эффекты, зависящие от фазовых соотношений между компонентами суперпозиционного состояния.

Наряду с квантовой суперпозицией и интерференцией фундаментальную роль играет явление *перепутывания* квантовых состояний. Суть перепутанных состояний легко понять, если сравнить, например, структуру любого из базисных векторов (2.108) и таковую кэт-вектора (2.113) суперпозиционного состояния. Базисные состояния (2.108) представляют собой произведения кэт-векторов однокубитовых состояний, т.е. имеют, как принято гово-

рить, *факторизованный* вид. Это означает, что не только состояние всего n-кубитового регистра, но и состояние каждого из входящих в него кубитов является *чистым* состоянием. Состояние каждого кубита описывается некоторым кэт-вектором и не зависит от того, в каких состояниях находятся остальные кубиты. Иная ситуация с кэт-вектором (2.113) суперпозиционного состояния. В общем случае этот вектор не может быть записан как произведение однокубитовых состояний, т.е. он не имеет факторизованного вида. Поэтому квантовое состояние отдельного кубита оказывается перепутанным с состояниями других кубитов и не описывается каким-либо кэт-вектором. Такое состояние квантовой подсистемы, в данном случае отдельного кубита, называется *смешанным* состоянием. Оно описывается с помощью *матрицы плотности* (см. главу 1). В этом контексте перепутанные квантовые состояния нескольких подсистем, входящих в некоторую более сложную систему, являются совершенно обычным объектом в аппарате квантовой механики.

Отличительным свойством перепутанных квантовых состояний является высокая степень *корреляции*[1] между рассматриваемыми подсистемами. Подчеркнем, что степень корреляции может быть больше той, которая следует из классических представлений.

В приведенном выше примере операция $\hat{U}$ (2.144) была применена к одному кубиту, квантовое состояние которого перепутано с состояниями остальной части регистра. Если n достаточно велико, то мы имеем дело с большой перепутанной системой кубитов. Корреляции между кубитами, т.е. между отдельными подсистемами полной квантовой системы, приводят к переработке экспоненциально большого объема квантовой информации. Классическому компьютеру для этого потребуется, вообще говоря, экспоненциально большой ресурс. Благодаря своим корреляционным свойствам, перепутанные состояния играют фундаментальную роль в процессах манипулирования квантовой информацией. По существу явление перепутывания состояний выступает как *парадигма* квантовой информатики.

---

[1] Корреляционные свойства перепутанных состояний, а также связанные с ними нарушения неравенств Белла обсуждаются в разделе 3.4.

Задачи

1. С помощью формулы (2.132) вычислить тензорные произведения вектор-столбцов, соответствующих базисным состояниям кубита, и получить вектор-столбцы, которые описывают базисные состояния двухкубитовой системы.

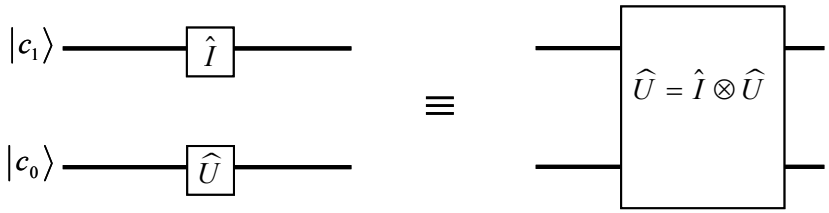
2. Для системы трех кубитов

(а) Написать кэт-векторы базисных состояний, используя однокубитовые состояния $|0\rangle$ и $|1\rangle$.

(б) Написать спинорное представление этих векторов.

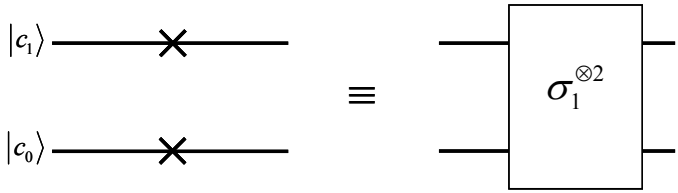
(в) Получить их как тензорное произведение базисных вектор-столбцов трех кубитов.

3. Рассмотреть две эквивалентные квантовые схемы



Написать матрицу двухкубитового гейта $\hat{I} \otimes \widehat{U}$, который является тензорным произведением однокубитовых гейтов $\hat{I}$ и $\widehat{U}$.

4. Рассмотреть две эквивалентные квантовые схемы и найти матрицу двухкубитового гейта $\sigma_1^{\otimes 2} \equiv \sigma_1 \otimes \sigma_1$. Как он действует на двухкубитовый базис?



5. Доказать, что оператор $H^{\otimes n}$ можно представить в виде $H^{\otimes n} = 2^{-n/2} \sum_{s,t} (-1)^{s \cdot t} |s\rangle\langle t|$, где $|s\rangle$ обозначает базисные векторы (2.110) *n*-кубитового регистра.

2.4. Перепутанные состояния

Применение принципа суперпозиции к составной квантовой системе с неизбежностью приводит к появлению перепутанных квантовых состояний подсистем. Поэтому, с точки зрения законов квантовой механики, перепутанные состояния являются вполне рутинным свойством составных систем. Такие системы являются, очевидно, стандартным объектом квантово-механических расчетов. При этом перепутывание состояний подсистем учитывается автоматически и не требует никакого специального внимания.

Интрига заключена в той роли, которую играют перепутанные состояния в квантовой информации. Первый намек на существование специфической связи между теорией информации и квантовой физикой восходит к 1935 г., когда *Альберт Эйнштейн*, *Борис Подольский* и *Натан Розен* в статье под заголовком «Можно ли считать квантово-механическое описание физической реальности полным?» (Phys. Rev., 1935, V.47, P.777–780) сформулировали свой знаменитый парадокс, отражающий одну из принципиальных особенностей квантового мира, о которой теперь принято говорить как об отсутствии локального реализма. Суть в том, что перепутывание квантовых состояний может выражаться в столь высокой степени корреляции между подсистемами, которую невозможно описать в терминах только локальных характеристик этих подсистем. Такие корреляции существенным образом влияют на процессы манипулирования квантовой информацией. Важность явления перепутывания была понята *Эрвином Шрёдингером*, который в том же 1935 г. опубликовал серию статей под общим заголовком «Современная ситуация в квантовой механике» (Die Naturwissenschaften, 1935, V. 23, P. 807-812, 823-828, 844-849). В этой работе, одним из побудительных мотивов которой явилось обсуждение вопросов, поставленных в статье тремя авторами, были проанализированы основы квантово-механического описания состояний физических систем и процессов измерения. В том числе было введено само понятие перепутывания двух квантовых систем (от немецкого Verchraenktheit zweier Quantesysteme). Две квантовые системы, находящиеся в перепутанном состоянии, называют ЭПР-парой. С количественным описанием степени корреляции

перепутанных состояний связаны так называемые неравенства Белла, сформулированные в 1964 г. (Bell J.S. *On the Einstein-Podolsky-Rosen paradox* //Physics, 1964, V.1, P.195). Квантовая информация придала этим проблемам, лежащим в основаниях квантовой механики, современное звучание.

Сложение двух спинов

Рассмотрим спиновые состояния системы, состоящей из двух частиц со спинами $s_1 = s_2 = 1/2$. Операторы спинов этих подсистем обозначаются как $\hat{\vec{s}}_1$ и $\hat{\vec{s}}_2$. Для квадратов этих операторов выполняется соотношение $\hat{\vec{s}}_1^2 = \hat{\vec{s}}_2^2 = s_1(s_1+1) = 3/4$. В качестве одночастичных базисных векторов выберем, как обычно, состояния $\left|\sigma^{(1),(2)}\right\rangle$ с определенными значениями $\sigma^{(1),(2)} = \pm 1/2$ проекций спинов каждой из подсистем 1 и 2 на некоторую ось квантования *z*. Тогда четыре кет-вектора

$$\left|\sigma^{(1)}\right\rangle\left|\sigma^{(2)}\right\rangle \equiv \left|\pm 1/2\right\rangle_1 \left|\pm 1/2\right\rangle_2 \qquad (2.148)$$

образуют полный набор двухчастичных спиновых состояний. Именно такие состояния мы использовали в предыдущем разделе в качестве базиса двухкубитового регистра. Подчеркнем, что в этих состояниях проекция спина каждой частицы на ось *z* имеет определенное значение. При поворотах системы координат происходит изменение каждой из этих проекций, и все базисные состояния (2.148) перемешиваются друг с другом.

Представляет интерес другой базис, в котором спиновые состояния классифицируются по величине суммарного спина системы. Сейчас мы покажем, что суммарный спин принимает два значения, 1 и 0, а пространство спиновых состояний разбивается на два инвариантных подпространства, отвечающих этим значениям полного спина.

При повороте системы координат спиновые состояния $\left|\Psi(1)\right\rangle$ и $\left|\Psi(2)\right\rangle$ подсистем преобразуются по закону (2.26) с генераторами,

соответственно, $\hat{\vec{s}}_1$ и $\hat{\vec{s}}_2$. Спиновое состояние $|\Psi(1,2)\rangle$ всей системы преобразуется так же, как тензорное произведение $|\Psi(1)\rangle \otimes |\Psi(2)\rangle$, т.е. закон преобразования определяется тензорным произведением операторов поворота для каждой из подсистем:

$$|\Psi'(1,2)\rangle = e^{i\Phi\vec{n}\hat{\vec{s}}_1} \otimes e^{i\Phi\vec{n}\hat{\vec{s}}_2} |\Psi(1,2)\rangle = \tag{2.149}$$

$$= e^{i\Phi\vec{n}\hat{\vec{S}}} |\Psi(1,2)\rangle.$$

Здесь

$$\hat{\vec{S}} = \hat{\vec{s}}_1 + \hat{\vec{s}}_2 \tag{2.150}$$

есть векторный оператор суммарного спина, компоненты которого $\hat{S}_i$ (i=x ,y ,z) подчиняются коммутационным соотношениям (2.28). Из этих соотношений следует, как уже говорилось в разделе 2.2, что: (1) операторы $\hat{\vec{S}}^2$ и $\hat{S}_z$ могут быть диагонализованы одновременно; (2) собственные значения $\hat{\vec{S}}^2$ равны $S(S+1)$, где $S \geq 0$; (3) собственные значения μ оператора $\hat{S}_z$ есть действительные числа, лежащие в пределах от –S до S через единицу. Поэтому вопрос сводится к определению возможных значений величины суммарного спина S при заданных значениях s_1 и s_2 спинов подсистем. Это есть теорема о сложении моментов. Хотя общий случай не представляет никаких затруднений, ограничимся, для простоты, только интересующей нас ситуацией, когда $s_1 = s_2 = 1/2$.

Собственные векторы операторов $\hat{\vec{S}}^2$ и $\hat{S}_z$ обозначим как $|S,\mu\rangle$. Из (2.150) следует, что $\hat{S}_z = \hat{s}_{1z} + \hat{s}_{2z}$. Поэтому собственные

значения этих операторов удовлетворяют соотношению

$$\mu = \sigma^{(1)} + \sigma^{(2)} . \qquad (2.151)$$

Каждое из состояний $\left|S, \mu\right\rangle$ можно разложить по полному базису (2.148):

$$\left|S, \mu\right\rangle = \sum_{\sigma^{(1)}+\sigma^{(2)}=\mu} C^{S\mu}_{\sigma^{(1)}\sigma^{(2)}} \left|\sigma^{(1)}\right\rangle \left|\sigma^{(2)}\right\rangle . \qquad (2.152)$$

В этой формуле суммирование по $\sigma^{(1)}$ и $\sigma^{(2)}$ ограничено условием (2.151), а $C^{S\mu}_{\sigma^{(1)}\sigma^{(2)}}$ называются коэффициентами Клебша-Гордана.

Легко видеть, что есть единственное состояние с максимальными проекциями $\sigma^{(1)} = \sigma^{(2)} = 1/2$. В этом случае $\mu = 1$. Так как это максимальное возможное значение проекции суммарного спина на ось *z*, то ему отвечает значение квантового числа $S = \max \mu = 1$. Далее, есть два состояния с противоположными значениями проекций спинов, $\sigma^{(1)} = -\sigma^{(2)} = 1/2$ и $\sigma^{(1)} = -\sigma^{(2)} = -1/2$, которые дают $\mu = 0$. Из этих двух линейно независимых состояний можно образовать две линейно независимые суперпозиции вида (2.152). Одна из них будет представлять состояние с уже известным значением $S = 1$ полного спина, но с проекцией $\mu = S - 1 = 0$, которая на единицу меньше максимальной. Тогда вторая линейно независимая суперпозиция должна относиться к состоянию с другим значением квантового числа *S*, а именно, к *S* = 0, для которого $\mu = 0$ является максимально возможным значением проекции. Наконец, последнее оставшееся состояние, для которого $\sigma^{(1)} = \sigma^{(2)} = -1/2$ и $\mu = -1$ отвечает суммарному спину *S* =1 и минимально возможному значению проекции,

$$\min \mu = - S = -1.$$

Таким образом, два спина $1/2$ могут сложиться в суммарный спин[1] $S = 1,0$. При $S = 1$ есть три состояния с проекциями $\mu = 0, \pm 1$. Их называют триплетом. При $S = 0$ есть одно состояние с проекцией $\mu = 0$. Это синглет.

При преобразовании поворота (2.149) величина S не меняется, так как оператор $\hat{\vec{S}}^2$ коммутирует со всеми генераторами $\hat{S}_i$, и, следовательно, с полным оператором вращений. Это означает, что состояния с $S = 1$ и с $S = 0$ при вращениях преобразуются сами через себя, образуя инвариантные подпространства.

Кэт-векторы $|S, \mu\rangle$ являются собственными состояниями полного набора операторов $\hat{\vec{S}}^2$ и $\hat{S}_z$. Поэтому они образуют полный ортонормированный базис. С прежним базисом (2.148) он связан соотношением (2.152), которое представляет собой унитарное преобразование, заданное матрицей коэффициентов Клебша-Гордана.

Найдем явный вид спиновых состояний $|S, \mu\rangle$ системы с определенными значениями суммарного спина S и его проекции μ на ось z. Это эквивалентно нахождению коэффициентов Клебша-Гордана.

Поскольку максимальная проекция $\mu = 1$, отвечающая спину $S=1$, может быть получена, как говорилось выше, единственным образом, то в разложении (2.152) присутствует только одно слагаемое, т.е.

$$|1,1\rangle = |1/2\rangle_1 |1/2\rangle_2 . \qquad (2.153)$$

Аналогично, для минимальной проекции $\mu = -1$ имеем

$$|1,-1\rangle = |-1/2\rangle_1 |-1/2\rangle_2 . \qquad (2.154)$$

---

[1] В общем случае при сложении двух спинов s_1 и s_2 суммарный спин S может принимать значения от $s_1 + s_2$ до $|s_1 - s_2|$ через единицу.

В состояние с $S = 1$ и $\mu = 0$ дают вклад два слагаемых

$$\left|1,0\right\rangle = a\left|1/2\right\rangle_1\left|-1/2\right\rangle_2 + b\left|-1/2\right\rangle_1\left|1/2\right\rangle_2 . \qquad (2.155)$$

Для нахождения коэффициентов Клебша-Гордана, которые здесь для краткости обозначены как a и b, поступим следующим образом. Рассмотрим оператор

$$\hat{S}_- = \hat{S}_x - i\hat{S}_y = \hat{S}_{1-} + \hat{S}_{2-} , \qquad (2.156)$$

где $\hat{S}_{1-} = \hat{S}_{1x} - i\hat{S}_{1y}$ и $\hat{S}_{2-} = \hat{S}_{2x} - i\hat{S}_{2y}$ являются операторами, которые понижают на единицу проекцию спина первой и второй частицы (см. задачу 1 в конце раздела 2.2). Поэтому оператор $\hat{S}_-$ понижает на единицу проекцию полного спина, т.е.

$$\hat{S}_-\left|1,1\right\rangle = \text{const}\cdot\left|1,0\right\rangle . \qquad (2.157)$$

Выражение, стоящее в левой части этого соотношения, симметрично относительно перестановки индексов 1 и 2, обозначающих подсистемы. Действительно, состояние $\left|1,1\right\rangle$ описывается выражением (2.153), которое не меняется при замене $1 \Leftrightarrow 2$. Оператор $\hat{S}_-$ (2.156) тоже не меняется при такой замене. Следовательно, вектор состояния $\left|1,0\right\rangle$, который имеет вид (2.155), должен быть симметричным относительно перестановки частиц. Это означает, что $a = b$. С учетом условия нормировки $\left\langle 1,0\middle|1,0\right\rangle = 1$ получаем, что состояние (2.155) имеет следующий вид:

$$\left|1,0\right\rangle = \frac{1}{\sqrt{2}}\left\{\left|1/2\right\rangle_1\left|-1/2\right\rangle_2 + \left|-1/2\right\rangle_1\left|1/2\right\rangle_2\right\} . \qquad (2.158)$$

Таким образом, триплет состояний с $S=1$ описывается формулами (2.153), (2.154) и (2.158). Все эти состояния симметричны относительно операции перестановки частиц.

В синглетное состояние с $S=0$ и $\mu=0$ тоже дают вклад два слагаемых

$$\left|0,0\right\rangle = \tilde{a}\left|1/2\right\rangle_1\left|-1/2\right\rangle_2 + \tilde{b}\left|-1/2\right\rangle_1\left|1/2\right\rangle_2 . \qquad (2.159)$$

Поскольку это состояние отвечает собственному значению $\hat{\vec{S}}^2 = S(S+1) = 0$, то оно должно быть ортогонально состоянию (2.158), для которого $\hat{\vec{S}}^2 = S(S+1) = 2$. Тогда $\left\langle 1,0\middle|0,0\right\rangle = 0 = (\tilde{a}+\tilde{b})/\sqrt{2}$, т.е. $\tilde{b} = -\tilde{a}$. С учетом условия нормировки имеем окончательно следующее выражение:

$$\left|0,0\right\rangle = \frac{1}{\sqrt{2}}\left\{\left|1/2\right\rangle_1\left|-1/2\right\rangle_2 - \left|-1/2\right\rangle_1\left|1/2\right\rangle_2\right\}. \qquad (2.160)$$

Мы видим, что синглетное состояние антисимметрично относительно перестановки частиц.

Перепутанные спиновые состояния. Состояния Белла

Векторы состояний (2.153) и (2.154) имеют факторизованный вид, и каждая из частиц находится в чистом спиновом состоянии с определенной проекцией спина на ось *z*. Это означает, что измерение проекции спина одной из подсистем даст с достоверностью определенный результат.

Иная ситуация с векторами состояний (2.158) и (2.160). Эти состояния не имеют факторизованного вида. Проекция спина ни той, ни другой подсистем не имеет определенного значения, а с равными вероятностями может быть равной и $1/2$, и $-1/2$. При этом спиновые состояния подсистем жестко (на все 100 %) скоррелированны друг с другом. Имеется в виду, что результат совместного

измерения спинов подсистем проявляет максимальную степень корреляции. Действительно, произведем измерение проекции спина, например, первой частицы и получим тот или иной результат: либо $1/2$, либо $-1/2$. Любой из этих результатов является случайным. Тогда вторая частица, которая не имела определенной проекции спина, после измерения, произведенного не над ней, а над другой частицей, будет с достоверностью находиться в состоянии с определенной, а именно, с противоположной проекцией спина. Например, если измерение проекции спина первой частицы дало результат $+1/2$, то последующее измерение проекции спина второй частицы даст с достоверностью значение $-1/2$. Тем самым значение указанной проекции оказывается однозначно скоррелированным со случайным результатом измерения, произведенного над первой частицей.

Подчеркнем, что между частицами нет никакого взаимодействия. Они могут, например, находиться сколь угодно далеко друг от друга. Тогда кажущуюся парадоксальность ситуации можно выразить в виде следующего рассуждения по поводу спинового состояния одной из частиц, например второй. Сначала ее спиновое состояние было полностью неопределенным, так как в состоянии (2.158) или (2.160) обе возможные проекции спина этой частицы являются равноправными. Но как только измерена проекция спина первой частицы, с которой наша частица никак не взаимодействует, ее спиновое состояние становится совершенно определенным. Такая корреляция означает наличие у квантовых объектов качеств, которые нельзя описать в терминах только локальных характеристик этих объектов. Подобные корреляции не имеют аналога в классическом мире.

Состояния (2.158) и (2.160) являются перепутанными спиновыми состояниями. Поскольку проекция спина каждой из подсистем принимает с равными вероятностями любое из своих возможных значений, то такие состояния называются максимально перепутанными.

Заметим, что из факторизованных векторов состояний (2.153) и (2.154) можно построить еще два линейно независимых максимально перепутанных состояния.

Взяв симметричную и антисимметричную комбинации выражений (2.153) и (2.154), получаем:

$$\frac{1}{\sqrt{2}}\left\{\left|1,1\right\rangle \pm \left|1,-1\right\rangle\right\} = \frac{1}{\sqrt{2}}\left\{\left|1/2\right\rangle_1 \left|1/2\right\rangle_2 \pm \left|-1/2\right\rangle_1 \left|-1/2\right\rangle_2\right\}. \quad (2.161)$$

Совокупность четырех состояний (2.158), (2.160) и (2.161) образует полный ортонормированный базис, состоящий из максимально перепутанных спиновых состояний. Их называют *состояниями Белла*.

Отождествляя, как обычно, два спиновых состояния с кубитом, т.е. $\left|1/2\right\rangle \equiv \left|0\right\rangle$ и $\left|-1/2\right\rangle \equiv \left|1\right\rangle$, запишем четыре состояния Белла в следующем виде:

$$\left|\Phi^{(\pm)}\right\rangle = \frac{1}{\sqrt{2}}\left\{\left|00\right\rangle \pm \left|11\right\rangle\right\}, \quad (2.162)$$

$$\left|\Psi^{(\pm)}\right\rangle = \frac{1}{\sqrt{2}}\left\{\left|01\right\rangle \pm \left|10\right\rangle\right\}. \quad (2.163)$$

Во избежание недоразумений заметим, что в этих последних выражениях символы 0 и 1, написанные внутри кэт-векторов, не следует путать с обозначениями величины спина и его проекции, как это было в предыдущих формулах.

Рассмотрим теперь некоторые свойства максимально перепутанных состояний на примере синглетного состояния (2.160) с нулевым суммарным спином. В соответствии с обозначениями (2.163) это есть двухкубитовое состояние Белла $\left|\Psi^{(-)}\right\rangle$, т.е.

$$\begin{aligned}\left|\Psi^{(-)}\right\rangle &= \frac{1}{\sqrt{2}}\left\{\left|1/2\right\rangle_1 \left|-1/2\right\rangle_2 - \left|-1/2\right\rangle_1 \left|1/2\right\rangle_2\right\} = \\ &= \frac{1}{\sqrt{2}}\left\{\begin{pmatrix}1\\0\end{pmatrix}_1 \begin{pmatrix}0\\1\end{pmatrix}_2 - \begin{pmatrix}0\\1\end{pmatrix}_1 \begin{pmatrix}1\\0\end{pmatrix}_2\right\}.\end{aligned} \quad (2.164)$$

На последнем шаге для полноты картины использовано спинорное представление.

Вид выражения (2.164), которое описывает максимально перепутанное состояние $\left|\Psi^{(-)}\right\rangle$, не меняется при переходе к другому базису одночастичных спиновых состояний. Покажем это, например, для базиса состояний с определенными проекциями спина на ось *x*. Собственные состояния оператора $\hat{s}_x$, отвечающие собственным значениям $s_x = \pm 1/2$, имеют следующий вид:

$$\left|s_x = 1/2\right\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix},\ \left|s_x = -1/2\right\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}. \quad (2.165)$$

Раскладывая по этим состояниям спиноры, которые входят в выражение (2.164), получаем:

$$\begin{aligned}\left|\Psi^{(-)}\right\rangle &= \frac{1}{\sqrt{2}}\left\{\frac{1}{2}\left[\begin{pmatrix}1\\1\end{pmatrix}_1 + \begin{pmatrix}1\\-1\end{pmatrix}_1\right]\cdot\frac{1}{2}\left[\begin{pmatrix}1\\1\end{pmatrix}_2 - \begin{pmatrix}1\\-1\end{pmatrix}_2\right] - (1 \rightleftarrows 2)\right\} = \\ &= -\frac{1}{\sqrt{2}}\left\{\frac{1}{2}\begin{pmatrix}1\\1\end{pmatrix}_1\begin{pmatrix}1\\-1\end{pmatrix}_2 - \frac{1}{2}\begin{pmatrix}1\\-1\end{pmatrix}_1\begin{pmatrix}1\\1\end{pmatrix}_2\right\} = \\ &= -\frac{1}{\sqrt{2}}\left\{\left|s_x = 1/2\right\rangle_1\left|s_x = -1/2\right\rangle_2 - \left|s_x = -1/2\right\rangle_1\left|s_x = 1/2\right\rangle_2\right\}.\end{aligned} \quad (2.166)$$

Мы видим, что $\left|\Psi^{(-)}\right\rangle$ остается максимально перепутанным состоянием, антисимметричным относительно перестановки частиц. Проекции спинов на ось *x* остаются жестко скоррелированными. Точно так же, как это было с проекциями спинов на ось *z*.

В случае произвольной оси $\vec{n}$ формальное доказательство проводится аналогичным образом с помощью разложений по собственным состояниям оператора $\vec{s}\vec{n}$ проекции спина на эту ось (см. задачу 2 в конце этого раздела). С физической точки зрения результат легко понять из следующего рассуждения. Действительно, выбор оси квантования $\vec{n}$ вместо *z* эквивалентен преобразованию

поворота системы координат, которое, как уже говорилось выше, не меняет величину суммарного спина. Поскольку в синглетном состоянии $\left|\Psi^{(-)}\right\rangle$ суммарный спин $S=0$, а следовательно, и его проекция на любую ось $\vec{n}$ тоже равна нулю, то структура выражения (2.164) остается неизменной при выборе любого базиса.

Таким образом, в состоянии $\left|\Psi^{(-)}\right\rangle$ проекции спинов на любую ось остаются жестко скоррелированными: если измерение одной из проекций на эту ось дает значение $+1/2$, то измерение другой проекции даст с достоверностью результат $-1/2$, и наоборот.

Инвариантность структуры выражения (2.164) относительно выбора базиса одночастичных спиновых состояний, т.е., фактически относительно преобразования поворота системы координат, представляет интерес для анализа свойств двухкубитовых гейтов.

При повороте системы координат состояние двухкубитовой спиновой системы преобразуется по закону (2.149), который определяется унитарным оператором вращений $\exp(i\Phi\vec{n}\hat{\vec{S}})$. Этот оператор представляет собой некоторый приводимый двухкубитовый гейт, который строится как тензорное произведение двух одинаковых однокубитовых преобразований $\exp(i\Phi\vec{n}\hat{\vec{s}}_{1,2})$. В результате такого преобразования состояние $\left|\Psi^{(-)}\right\rangle$ остается перепутанным состоянием и не может быть записано в факторизованном виде. Поэтому мы приходим к выводу, что с помощью двух одинаковых однокубитовых гейтов перепутанное состояние $\left|\Psi^{(-)}\right\rangle$ нельзя преобразовать ни в какое факторизованное состояние. В силу обратимости унитарных преобразований справедливо и обратное утверждение, что с помощью двух одинаковых однокубитовых гейтов из факторизованных двухкубитовых состояний нельзя получить перепутанное состояние $\left|\Psi^{(-)}\right\rangle$.

Сформулированные утверждения можно существенно усилить. Рассмотрим приводимый двухкубитовый гейт $\hat{U}=\hat{U}_1\otimes\hat{U}_2$, который имеет вид тензорного произведения двух произвольных одно-

кубитовых преобразований. В общем случае $\hat{U}_1$ и $\hat{U}_2$ представляют собой однокубитовые вращения, но вокруг разных осей и на разные углы. Напомним, что унитарные преобразования сохраняют скалярные произведения и переводят один полный набор базисных состояний в другой полный набор. Поэтому в результате действия оператора $\hat{U}_1$ на базисные векторы $\left|\pm 1/2\right\rangle_1$ первого кубита

$$\hat{U}_1\left|1/2\right\rangle_1 = \left|\alpha\right\rangle_1,\ \hat{U}_1\left|-1/2\right\rangle_1 = \left|\beta\right\rangle_1 \qquad (2.167)$$

получается полный ортонормированный набор состояний $\left|\alpha\right\rangle_1$ и $\left|\beta\right\rangle_1$. Эти состояния являются линейно независимыми[1]. Аналогично, в результате действия оператора $\hat{U}_2$ на базисные векторы $\left|\pm 1/2\right\rangle_2$ второго кубита получаем ортонормированный базис $\left|\gamma\right\rangle_2$ и $\left|\delta\right\rangle_2$. Эти состояния тоже линейно независимые. Тогда

$$\begin{aligned}
&\hat{U}\left|\Psi^{(-)}\right\rangle = (\hat{U}_1 \otimes \hat{U}_2)\left|\Psi^{(-)}\right\rangle = \\
&= \frac{1}{\sqrt{2}}\left\{(\hat{U}_1\left|1/2\right\rangle_1)(\hat{U}_2\left|-1/2\right\rangle_2) - (\hat{U}_1\left|-1/2\right\rangle_1)(\hat{U}_2\left|1/2\right\rangle_2)\right\} = \\
&= \frac{1}{\sqrt{2}}\left\{\left|\alpha\right\rangle_1\left|\delta\right\rangle_2 - \left|\beta\right\rangle_1\left|\gamma\right\rangle_2\right\}.
\end{aligned} \qquad (2.168)$$

Получившийся вектор состояния может быть записан в факторизованном виде $\left|a\right\rangle_1\left|b\right\rangle_2$ тогда и только тогда, когда между парой векторов $\left|\alpha\right\rangle_1$ и $\left|\beta\right\rangle_1$, либо между $\left|\gamma\right\rangle_2$ и $\left|\delta\right\rangle_2$ существует линейная зависимость.

---

[1] Линейная зависимость этих состояний означала бы, что у оператора $\hat{U}_1$ есть нулевое собственное значение. У унитарного оператора таких собственных значений нет.

Таким образом, перепутанное состояние $\left|\Psi^{(-)}\right\rangle$ нельзя превратить в факторизованное состояние с помощью одних только однокубитовых унитарных операций. Это утверждение справедливо не только для $\left|\Psi^{(-)}\right\rangle$, но для всех состояний Белла (2.162) и (2.163). Дело в том, что сами состояния Белла можно получить друг из друга с помощью однокубитовых гейтов. Применяя, например, в состоянии $\left|\Psi^{(-)}\right\rangle$ ко второму кубиту операцию $\sigma_1^{(2)}$, т.е. однокубитовый гейт NOT (2.56), получаем

$$\begin{aligned}\sigma_1^{(2)}\left|\Psi^{(-)}\right\rangle &= \frac{1}{\sqrt{2}}\left\{\left|0\right\rangle(\sigma_1^{(2)}\left|1\right\rangle) - \left|1\right\rangle(\sigma_1^{(2)}\left|0\right\rangle)\right\} = \\ &= \frac{1}{\sqrt{2}}\left\{\left|00\right\rangle - \left|11\right\rangle\right\} = \left|\Phi^{(-)}\right\rangle.\end{aligned} \tag{2.169}$$

Можно написать также ряд других соотношений вида

$$\begin{aligned}\sigma_3^{(1)}\left|\Psi^{(-)}\right\rangle &= \left|\Psi^{(+)}\right\rangle, \\ \sigma_3^{(1)}\left|\Phi^{(-)}\right\rangle &= \left|\Phi^{(+)}\right\rangle.\end{aligned} \tag{2.170}$$

Если с помощью однокубитовых операций можно было бы факторизовать одно из состояний Белла, то это можно было бы сделать и для всех остальных.

Итак, для построения унитарных преобразований в пространстве двухкубитовых состояний одних только однокубитовых гейтов недостаточно. С их помощью, как мы видим, нельзя «распутать» перепутанные состояния Белла, т.е. связать их с факторизованными двухкубитовыми состояниями. Это означает, что нужны более сложные – неприводимые двухкубитовые операции.

Если на факторизованное состояние подействовать однокубитовыми операциями, то оно, конечно, останется факторизованным. При этом каждый кубит переходит, вообще говоря, в суперпозицию исходных базисных состояний $\left|0\right\rangle$ и $\left|1\right\rangle$, а кэт-вектор системы принимает форму перепутанного состояния этих базисных векторов. Это означает, что в отличие, скажем, от состояний Белла, ко-

торые остаются перепутанными в любом вычислительном базисе, есть множество других состояний, являющихся перепутанными в одном базисе, но факторизующихся при переходе к другому базису. Например, двухкубитовое состояние (2.115) является перепутанным в базисе $\{|0\rangle, |1\rangle\}$. С другой стороны, из соотношения (2.141) следует, что оно имеет факторизованный вид в базисе состояний

$$\frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}, \quad \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}, \qquad (2.171)$$

которые представляют собой собственные векторы (2.165) оператора проекции спина на ось *x*. Этим свойством обладает и *n*-кубитовое состояние (2.143).

Перепутанные поляризационные состояния фотонов

В задачах, связанных с передачей квантовой информации, т.е. в квантовых коммуникационных схемах, широко используются кубиты, построенные на поляризационных состояниях фотонов. Определяющую роль в этих процессах играют перепутанные поляризационные состояния.

Хотя квантовая суть явления перепутывания поляризационных состояний такая же, как для спина, сами физические системы и способы манипулирования их состоянием существенно разные. Поэтому мы остановимся более подробно на описании перепутанных поляризационных состояний.

Напомним, что два базисных состояния

$$\left|\vec{k}v\right\rangle \equiv |v\rangle\left|\vec{k}\right\rangle \quad \text{и} \quad \left|\vec{k}h\right\rangle \equiv |h\rangle\left|\vec{k}\right\rangle \qquad (2.172)$$

фотона характеризуются волновым вектором $\vec{k}$ и двумя направлениями поляризации. Эти направления ортогональны $\vec{k}$, и мы будем называть их вертикальной (*v*) и горизонтальной (*h*) поляризациями. Кроме того, можно формально считать, что базисные векторы имеют факторизованный вид (2.172), в котором $\left|\vec{k}\right\rangle$ относит-

ся к пространственным степеням свободы, а $|v\rangle$ и $|h\rangle$ описывают поляризационную степень свободы. Поляризационные состояния отождествляются с кубитом: $|v\rangle \equiv |0\rangle$ и $|h\rangle \equiv |1\rangle$.

Рассмотрим систему, состоящую из двух фотонов с одинаковыми волновыми векторами $\vec{k}$, но разными поляризациями. Так как фотоны являются бозонами, то вектор состояния системы должен быть симметричным относительно операции перестановки частиц 1 и 2. Поэтому вектор состояния имеет следующий вид:

$$|\Psi(1,2)\rangle = \left(|v\vec{k}\rangle_1 |h\vec{k}\rangle_2 + |h\vec{k}\rangle_1 |v\vec{k}\rangle_2\right)/\sqrt{2} = \\ = \frac{1}{\sqrt{2}}\left(|v\rangle_1 |h\rangle_2 + |h\rangle_1 |v\rangle_2\right)|\vec{k}\rangle_1 |\vec{k}\rangle_2 . \quad (2.173)$$

Выражение, стоящее в круглой скобке, представляет собой перепутанное поляризационное состояние, которое совпадает с симметричным состоянием Белла $|\Psi^{(+)}\rangle$ (2.164):

$$|\Psi^{(+)}\rangle = \left(|v\rangle_1 |h\rangle_2 + |h\rangle_1 |v\rangle_2\right)/\sqrt{2} = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right). \quad (2.174)$$

Тот факт, что получилось симметричное перепутанное поляризационное состояние, легко понять из следующих соображений. Поскольку волновые векторы одинаковые, то пространственная, т.е. зависящая от $\vec{k}$ часть вектора состояния может быть только симметричной относительно перестановки частиц. Поэтому поляризационная часть должна быть тоже симметричной, чтобы обеспечить бозонную перестановочную симметрию вектора состояния.

Для системы двух фотонов с разными волновыми векторами можно реализовать остальные перепутанные поляризационные состояния Белла $|\Phi^{(\pm)}\rangle$ и $|\Psi^{(-)}\rangle$.

Светоделитель и измерение антисимметричного поляризационного состояния Белла

Рассмотрим простую модель светоделителя и покажем, как с помощью такой системы можно измерить одно из перепутанных поляризационных состояний Белла для двух фотонов, а именно антисимметричное состояние

$$\left|\Psi^{(-)}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|v\right\rangle_1\left|h\right\rangle_2 - \left|h\right\rangle_1\left|v\right\rangle_2\right). \qquad (2.175)$$

Эта модель схематически изображена на рис. 2.11

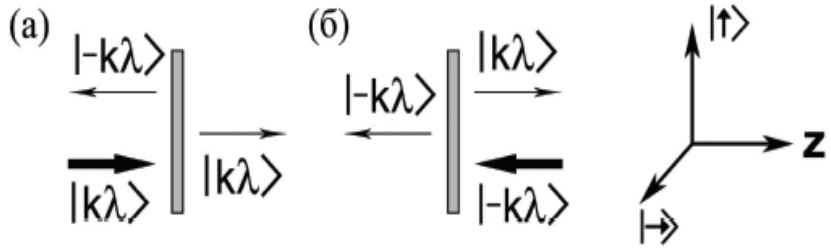


Рис. **2.11**

Тонкая плоскопараллельная пластина, изготовленная из диэлектрического материала и частично посеребренная с одной стороны, разделяет пространство на две части. Световое поле, падающее на эту пластину слева (а) или справа (б), с некоторыми вероятностями проходит через пластину или отражается от нее. О такой системе принято говорить, что у нее есть два входных и два выходных канала. Пусть поглощение отсутствует, а вероятности прохождения $\left|T\right|^2$ и отражения $\left|R\right|^2$ равны, т.е.

$$\left|T\right|^2 = \left|R\right|^2 = 1/2\,. \qquad (2.176)$$

Это светоделитель 50/50.

Рассмотрим поведение монохроматической моды в одномерной геометрии, когда фотоны с волновыми векторами $\pm k$ распространяются вдоль оси *z*. Для простоты считаем, что оба входных канала совершенно симметричны. Кроме того, предполагается, что процессы отражения и прохождения не зависят от поляризации и не меняют эту поляризацию. Два линейно независимых поляризационных состояния, отвечающие вертикальной и горизонтальной поляризациям, обозначим как $|\lambda\rangle \equiv \{|v\rangle, |h\rangle\}$.

В отсутствие светоделителя состояния $|\pm k\lambda\rangle$ являются независимыми. Действие светоделителя приводит к когерентному перемешиванию этих состояний. Так, падающий на светоделитель слева фотон в состоянии $|k\lambda\rangle$, переходит в следующее суперпозиционное состояние (рис. 2.11**а**):

$$|k\lambda\rangle \to \hat{D}|k\lambda\rangle \equiv |a\rangle = T|k\lambda\rangle + R|-k\lambda\rangle, \qquad (2.177)$$

где $\hat{D}$ представляет собой оператор, описывающий действие светоделителя, а *T* и *R* являются амплитудами вероятности прохождения и отражения. Аналогично, для фотона, падающего справа (рис. 2.11**б**), имеет место следующее преобразование:

$$|-k\lambda\rangle \to \hat{D}|-k\lambda\rangle \equiv |b\rangle = T|-k\lambda\rangle + R|k\lambda\rangle. \qquad (2.178)$$

В преобразованиях (2.177) и (2.178) использовано в явном виде предположение, что воздействие светоделителя симметрично, сохраняет поляризацию и не зависит от нее.

Исходные состояния $|\pm k\lambda\rangle$ образуют полный ортонормированный базис. Сохранение полной вероятности в отсутствие поглощения эквивалентно сохранению нормировки, т.е.

$$\begin{aligned} \langle k\lambda|k\lambda\rangle = \langle a|a\rangle = \langle k\lambda|\hat{D}^{+}\hat{D}|k\lambda\rangle = |T|^2 + |R|^2 = 1, \\ \langle -k\lambda|-k\lambda\rangle = \langle b|b\rangle = \langle -k\lambda|\hat{D}^{+}\hat{D}|-k\lambda\rangle = |T|^2 + |R|^2 = 1. \end{aligned} \qquad (2.179)$$

Поскольку базис полный, то оператор

$$\hat{D}^{+}\hat{D} = \mathbf{1}. \tag{2.180}$$

Кроме условия (2.179) на амплитуды T и R накладывается еще одно условие. У оператора $\hat{D}$ не может быть нулевых собственных значений. Иначе это означало бы, что воздействие светоделителя на какое-то однофотонное состояние приводит к исчезновению этого фотона. Поэтому оператор $\hat{D}$ является обратимым, т.е. у него есть обратный оператор $\hat{D}^{-1}$. Совместно с условием (2.180) это означает, что оператор $\hat{D}$ является унитарным. Такой оператор сохраняет скалярные произведения, и, следовательно, состояния $|a\rangle$ и $|b\rangle$ ортогональны. Это дает

$$\begin{aligned}\langle b|a\rangle &= \left(T^{*}\langle -k\lambda| + R^{*}\langle k\lambda|\right)\left(T|k\lambda\rangle + R|-k\lambda\rangle\right) = \\ &= T^{*}R + R^{*}T = 0.\end{aligned} \tag{2.181}$$

Без ущерба для общности можно считать, что амплитуда прохождения T действительная и неотрицательная величина. Это регулируется выбором некоторого общего фазового множителя. Тогда, учитывая (2.176), имеем

$$T = 1/\sqrt{2}\,. \tag{2.182}$$

После этого из (2.181) получаем, что

$$R + R^{*} = 2\,\mathrm{Re}\,R = 0\,,$$

т.е. амплитуда отражения R является величиной чисто мнимой. Принимая во внимание (2.176), ее можно положить равной

$$R = -i/\sqrt{2}\,. \tag{2.183}$$

Как мы увидим ниже, именно это обстоятельство формально обеспечивает возможность проектирования на антисимметричное поляризационное состояние (2.175).

Из выражений (2.177), (2.178), (2.182) и (2.183) следует, что в базисе состояний $\left|\pm k\lambda\right\rangle$ унитарная матрица $\hat{D}$, описывающая воздействие светоделителя на поле, имеет вид

$$\hat{D}=\begin{pmatrix} T & R \\ R & T \end{pmatrix}=\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix}=\frac{1}{\sqrt{2}}\left(1-i\sigma_1\right) . \qquad (2.184)$$

Интересно отметить, что изложенное выше описание работы светоделителя аналогично стандартному расчету квантовых эффектов отражения и прохождения частицы через одномерный потенциальный барьер (см. задачу 3 в конце этого раздела).

Перейдем теперь к вопросу о том, как в результате измерения состояния двух фотонов после воздействия светоделителя получается поляризационное состояние Белла (2.175).

Итак, пусть в два входных канала светоделителя приходят два фотона – один слева, другой справа. Один – с вертикальной поляризацией, другой – с горизонтальной. Поскольку это бозоны, вектор исходного состояния системы

$$\left|in\right\rangle=\frac{1}{\sqrt{2}}\left\{\left|kv\right\rangle_1\left|-kh\right\rangle_2+\left|-kh\right\rangle_1\left|kv\right\rangle_2\right\} \qquad (2.185)$$

симметричен относительно перестановки частиц ($1\rightleftarrows 2$). Воздействие светоделителя задается преобразованиями (2.177) и (2.178) для одночастичных векторов состояний, так что состояние системы на выходе имеет следующий вид:

$$\left|out\right\rangle=\frac{1}{\sqrt{2}}\times$$
$$\times\left\{\frac{1}{\sqrt{2}}\left(\left|kv\right\rangle_1-i\left|-kv\right\rangle_1\right)\cdot\frac{1}{\sqrt{2}}\left(\left|-kh\right\rangle_2-i\left|kh\right\rangle_2\right)+(1\rightleftarrows 2)\right\}. \qquad (2.186)$$

Здесь для коэффициентов T и R использованы значения (2.182) и (2.183), а последнее слагаемое в фигурной скобке, обозначенное как $(1 \rightleftarrows 2)$, получается из первого слагаемого перестановкой индексов.

Выходное состояние $\left|out\right\rangle$ (2.186) содержит слагаемые, которые отвечают следующим трем возможным результатам воздействия светоделителя:

(1) оба фотона имеют волновой вектор k,

(2) оба фотона имеют волновой вектор $-k$,

(3) фотоны имеют противоположные волновые векторы, k и $-k$.

Как видно из рис. 2.11, в первом случает оба фотона оказываются справа от светоделителя, а во втором случае — слева. Таким образом для этих двух исходов оба фотона находятся по одну сторону от светоделителя. В третьем случае фотоны оказываются по одному с каждой стороны от светоделителя.

Произведем такое совместное измерение над системой двух фотонов, когда два детектора, расположенные в выходных каналах светоделителя по одному с каждой стороны, регистрируют совпадение фотоотсчетов[1]. Амплитуда вероятности такого события определяется, очевидно, только теми слагаемыми в выражении (2.186), в которые входят однофотонные состояния с противоположными волновыми векторами. Эти члены имеют вид

$$\begin{aligned}&\frac{1}{2\sqrt{2}}\left\{\left|kv\right\rangle_1\left|-kh\right\rangle_2-\left|-kv\right\rangle_1\left|kh\right\rangle_2+(1\rightleftarrows 2)\right\}=\\&=\frac{1}{\sqrt{2}}\frac{\left|k\right\rangle_1\left|-k\right\rangle_2-\left|-k\right\rangle_1\left|k\right\rangle_2}{\sqrt{2}}\left|\Psi^{(-)}\right\rangle,\end{aligned}\qquad(2.187)$$

где $\left|\Psi^{(-)}\right\rangle$ определяется формулой (2.175).

[1] Детекторы регистрируют акты попадания на них фотонов безотносительно к их поляризациям.

При преобразовании выражения, стоящего в фигурной скобке в (2.187), было учтено, что одночастичные состояния $\left|\pm k\lambda\right\rangle$ можно записать формально как произведение $\left|\lambda\right\rangle\left|\pm k\right\rangle$ векторов состояний, относящихся к пространственным (внешним) и поляризационным (внутренним) степеням свободы. В результате вектор двухчастичного состояния (2.187) факторизовался. Обратим внимание на важные особенности состояния (2.187). Прежде всего, оно, конечно, симметрично относительно перестановки фотонов 1 и 2. Далее, знак минус при втором слагаемом в фигурной скобке возник, как это видно из предыдущего выражения (2.186), из-за величины $R^2 = \left(-i/\sqrt{2}\right)^2 = -1/2$. В факторизованном выражении (2.187) пространственные и поляризационные состояния являются антисимметричными относительно перестановки частиц. Подчеркнем, что при заданном нами начальном условии результат (2.187) формируется единственным образом, когда на выходе два фотона находятся по разные стороны от светоделителя. Результатом регистрации совпадения фотоотсчетов двух детекторов является проектирование поляризационного состояния двухфотонной системы на антисимметричное состояние Белла $\left|\Psi^{(-)}\right\rangle$.

Светоделитель является линейной оптической системой. Выше было продемонстрировано, как с его помощью можно выделить состояние $\left|\Psi^{(-)}\right\rangle$. Светоделитель можно использовать для идентификации состояния $\left|\Psi^{(+)}\right\rangle$. При этом надо регистрировать пару фотонов по одну сторону от светоделителя. Далее потребуются еще поляризационные измерения, чтобы отличить симметричное состояние $\left|\Psi^{(+)}\right\rangle$ от других симметричных состояний $\left|\Phi^{(\pm)}\right\rangle$. Анализ же последних нуждается в более сложных нелинейно-оптических процессах.

В настоящее время экспериментально реализовано измерение полного набора поляризационных состояний Белла.

Состояния Гринбергера-Хорна-Цайлингера

Рассмотренные выше двухчастичные спиновые или поляризационные системы позволяют понять квантовую суть явления перепутывания. В процессах хранения и манипулирования квантовой информацией в многокубитовых регистрах определяющую роль играет перепутывание состояний большого числа частиц. Перепутанные состояния более чем двух частиц называют состояниями Гринбергера-Хорна-Цайлингера (ГХЦ). По сравнению с двухкубитовой ситуацией ГХЦ-перепутывание обладает гораздо более широким спектром специфических корреляционных свойств, находящихся в резком противоречии с классическими представлениями. Это важно не только с точки зрения принципиальных оснований квантовой механики, но и применительно к задачам квантовой информации. Мы не будем вдаваться в обсуждение этих вопросов, но для полноты картины приведем один пример трехчастичного максимально перепутанного состояния ГХЦ.

Рассмотрим систему, состоящую из трех частиц со спином $1/2$. Суммарный спин может быть равен $S = 3/2$. Это максимальное значение. При таком S максимальное значение проекции на ось z равно $3/2$ и получается, когда каждый спин имеет проекцию $1/2$. Минимальное значение проекции, равное $-3/2$, получается, когда каждый спин имеет проекцию $-1/2$. Состояние

$$\frac{1}{\sqrt{2}}\left\{\left|1/2\right\rangle_1\left|1/2\right\rangle_2\left|1/2\right\rangle_3+\left|-1/2\right\rangle_1\left|-1/2\right\rangle_2\left|-1/2\right\rangle_3\right\}= \\ =\frac{1}{\sqrt{2}}\left(\left|000\right\rangle+\left|111\right\rangle\right) \tag{2.188}$$

является, очевидно, максимально перепутанным. Оно симметрично относительно перестановки частиц. Ни один из трех кубитов не несет сам по себе определенной информации о своем спиновом состоянии. Любое из двух возможных значений проекции его спина является равновероятным. Но как только будет произведено измерение проекции спина на ось z одного из кубитов и получено

какое-то значение, состояния двух других кубитов станут строго определенными. И этот результат не зависит от пространственного расположения частиц, над которыми производятся измерения.

Задачи

1. Доказать, что кэт-векторы

$$\left|S,0\right\rangle = \frac{1}{\sqrt{2}}\left\{\left|1/2\right\rangle_1\left|-1/2\right\rangle_2 \pm \left|-1/2\right\rangle_1\left|1/2\right\rangle_2\right\}$$

являются собственными состояниями квадрата оператора суммарного спина $\hat{\vec{S}}^2 = \left(\hat{\vec{s}}_1 + \hat{\vec{s}}_2\right)^2$ двух частиц со спином $1/2$, отвечающими собственным значениям $S\left(S+1\right)$ соответственно для $S=1$ и $S=0$.

Указание

В спинорном представлении рассматриваемые состояния имеют вид

$$\frac{1}{\sqrt{2}}\left\{\begin{pmatrix}1\\0\end{pmatrix}_1\begin{pmatrix}0\\1\end{pmatrix}_2 \pm \begin{pmatrix}0\\1\end{pmatrix}_1\begin{pmatrix}1\\0\end{pmatrix}_2\right\}.$$

Выразить оператор $\hat{\vec{S}}^2$ через матрицы Паули $\sigma_i^{(1)}$ и $\sigma_i^{(2)}$, т.е.

$$\hat{\vec{S}}^2 = \hat{\vec{s}}_1^2 + \hat{\vec{s}}_2^2 + 2\hat{\vec{s}}_1\hat{\vec{s}}_2 = \frac{3}{2} + \frac{1}{2}\left[\sigma_x^{(1)}\sigma_x^{(2)} + \sigma_y^{(1)}\sigma_y^{(2)} + \sigma_z^{(1)}\sigma_z^{(2)}\right],$$

где верхние индексы показывают номер частицы.

2. Доказать, что перепутанное состояние

$$\left|\Psi^{(-)}\right\rangle = \frac{1}{\sqrt{2}}\left\{\left|1/2\right\rangle_1\left|-1/2\right\rangle_2 - \left|-1/2\right\rangle_1\left|1/2\right\rangle_2\right\}$$

описывается таким же по форме выражением в базисе собственных векторов оператора проекции спина на любую ось $\vec{n}$.

Указание

Написать собственные векторы оператора

$$\hat{s}_{\vec{n}} \equiv \hat{\vec{s}}\vec{n} = \frac{1}{2}\left(n_x\sigma_x + n_y\sigma_y + n_z\sigma_z\right)$$

проекции спина $1/2$ на ось $\vec{n} = \{n_x, n_y, n_z\}$, $\vec{n}^2 = 1$, и разложить однокубитовые состояния $\left|\pm 1/2\right\rangle_{1,2}$ по этому базису.

3. Написать матрицу плотности произвольного чистого спинового состояния (2.30).

Решение

Произвольное (чистое) спиновое состояние описывается кэт-вектором

$$\left|\psi\right\rangle = \sum_{\sigma=1/2,-1/2} C_\sigma \left|\sigma\right\rangle, \qquad \sum_\sigma \left|C_\sigma\right|^2 = 1.$$

Тогда для оператора плотности $\hat{\rho}$ получаем

$$\hat{\rho} = \left|\psi\right\rangle\left\langle\psi\right| = \sum_{\sigma,\sigma'} C_\sigma C^*_{\sigma'} \left|\sigma\right\rangle\left\langle\sigma'\right| \equiv \sum_{\sigma,\sigma'} \rho_{\sigma\sigma'} \left|\sigma\right\rangle\left\langle\sigma'\right|,$$

где матрица плотности $\rho_{\sigma\sigma'}$ в S_z – представлении имеет вид

$$\rho_{\sigma\sigma'} = C_\sigma C^*_\sigma, \quad \text{т.е.} \quad \hat{\rho} = \begin{pmatrix} C_{1/2}C^*_{1/2} & C_{1/2}C^*_{-1/2} \\ C_{-1/2}C^*_{1/2} & C_{-1/2}C^*_{-1/2} \end{pmatrix}.$$

Из этого выражения видно, что

$$Sp\hat{\rho} = \sum_\sigma \rho_{\sigma\sigma} = \sum_\sigma \left|C_\sigma\right|^2 = 1.$$

Для матрицы $\hat{\rho}^2$ имеем

$$\hat{\rho}^2 = |\psi\rangle\langle\psi|\psi\rangle\langle\psi| = |\psi\rangle\langle\psi| = \hat{\rho}\,.$$

В этом можно убедиться и непосредственным перемножением матриц:

$$\left(\hat{\rho}^2\right)_{\sigma\sigma'} = \sum_{\sigma_1} \rho_{\sigma\sigma_1}\rho_{\sigma_1\sigma'} = C_\sigma C^*_{\sigma'} \sum_{\sigma_1} \left|C_{\sigma_1}\right|^2 = C_\sigma C^*_{\sigma'} = \rho_{\sigma\sigma'}\,.$$

4. Доказать, что для энтропии фон Неймана квантового состояния с матрицей плотности $\hat{\rho}$ имеет место следующее соотношение:

$$S(\hat{\rho}) = -Sp(\hat{\rho}\log_2\hat{\rho}) = -\sum_j p_j \log_2 p_j\,,$$

где p_j – собственные значения эрмитового неотрицательного оператора $\hat{\rho}$.

Доказательство

Пусть $\{|j\rangle\}$ – полный ортонормированный базис, который диагонализует матрицу плотности, т.е. имеет место следующее спектральное разложение оператора $\hat{\rho}$

$$\hat{\rho} = \sum_j p_j |j\rangle\langle j|,$$

где числа $p_j \geq 0$ ($\sum_j p_j = 1$) есть собственные значения оператора $\hat{\rho}$. По определению спектрального разложения функции от оператора имеем

$$\log_2\hat{\rho} = \sum_j \left(\log_2 p_j\right)|j\rangle\langle j|\,.$$

Тогда

$$Sp\left(\hat{\rho}\log_2\hat{\rho}\right) = Sp\left(\sum_j p_j \left|j\right\rangle\left\langle j\right|\right)\left(\sum_i \log_2 p_i \left|i\right\rangle\left\langle i\right|\right) =$$

$$= Sp\sum_{ij} p_j \log_2 p_j \left|j\right\rangle\left\langle j\middle|i\right\rangle\left\langle i\right| = \sum_j p_j \log_2 p_j Sp\left|j\right\rangle\left\langle j\right| =$$

$$= \sum_j p_j \log_2 p_j .$$

Тем самым, интересующее нас соотношение доказано. При вычислении мы воспользовались условием ортонормированности базиса, $\left\langle j\middle|i\right\rangle = \delta_{ji}$, линейностью операции взятия следа и тем, что

$$Sp\left|j\right\rangle\left\langle j\right| = \left\langle j\middle|j\right\rangle = 1 .$$

5. Матрицу плотности произвольного (чистого) спинового состояния привести к диагональному виду и вычислить для этого состояния энтропию фон Неймана.

Решение

Поскольку произвольное (чистое) спиновое состояние $\left|\psi\right\rangle$ является собственным состоянием оператора проекции спина $\hat{s}_{\vec{n}}$ на некоторую ось $\vec{n}$ (см. задачу 3 в конце раздела 2.2), отвечающее, например, собственному значению $s_{\vec{n}} = 1/2$, то в базисе состояний $\left|s_{\vec{n}} = \pm 1/2\right\rangle$ кэт-вектор имеет вид

$$\left|\psi\right\rangle = \sum_\sigma C_\sigma \left|\sigma\right\rangle = \left|s_{\vec{n}} = 1/2\right\rangle .$$

Тогда для $\hat{\rho}$ получаем

$$\hat{\rho} = \left|\psi\right\rangle\left\langle\psi\right| = \left|s_{\vec{n}} = 1/2\right\rangle\left\langle s_{\vec{n}} = 1/2\right| ,$$

т.е. в этом базисе матрица плотности

$$\hat{\rho} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

имеет единственный отличный от нуля матричный элемент, который стоит на диагонали и равен 1. Другими словами, спектральное разложение $\hat{\rho}$ содержит только одно слагаемое, отвечающее собственному значению $p = 1$. Тогда $\log_2 \hat{\rho} = 0$, и энтропия фон Неймана чистого состояния $S(\hat{\rho}) = 0$.

6. Написать матрицу плотности спинового состояния одной из частиц ЭПР-пары, находящейся в состоянии Белла.

Решение

Рассмотрим перепутанное состояние $\left|\Psi^{(-)}\right\rangle$. Матрица плотности одной из частиц, например первой, получается из выражения для оператора плотности системы $\left|\Psi^{(-)}\right\rangle\left\langle\Psi^{(-)}\right|$ с помощью операции взятия следа по квантовым числам второй частицы, т.е.

$$\hat{\rho}_1 = Sp_2 \left|\Psi^{(-)}\right\rangle\left\langle\Psi^{(-)}\right| =$$

$$= \frac{1}{2} Sp_2 \left(\left|1/2\right\rangle_1 \left|-1/2\right\rangle_2 - \left|-1/2\right\rangle_1 \left|1/2\right\rangle_2\right)\left({}_1\left\langle 1/2\right|{}_2\left\langle -1/2\right| - {}_1\left\langle -1/2\right|{}_2\left\langle 1/2\right|\right) =$$

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

$$= \frac{1}{2}\left(\left|1/2\right\rangle_1 {}_1\left\langle 1/2\right| + \left|-1/2\right\rangle_1 {}_1\left\langle -1/2\right|\right).$$

Следовательно, матрица плотности $\hat{\rho}_1$ имеет диагональный вид

$$\hat{\rho}_1 = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Собственные значения $p_{\pm 1/2} = 1/2$, стоящие на диагонали, оказываются одинаковыми в полном соответствии с тем, что в максимально перепутанном состоянии $\left|\Psi^{(-)}\right\rangle$ проекция спина одной из частиц ЭПР-пары является полностью неопределенной и с равными вероятностями принимает любое из своих возможных значений $\pm 1/2$. Тогда энтропия фон Неймана состояния с матрицей плотности $\hat{\rho}_1$ имеет вид

$$S(\hat{\rho}_1) = -Sp\hat{\rho}_1 \log_2 \hat{\rho}_1 = -\left(p_{1/2} \log_2 p_{1/2} + p_{-1/2} \log_2 p_{-1/2}\right) =$$

$$= -\log_2 \frac{1}{2} = 1.$$

Это есть максимально возможное значение энтропии фон Неймана для состояния, которое описывается матрицей плотности 2×2 (см. следующую задачу).

7. Доказать, что $S(\hat{\rho}) = -\sum_{j=1}^{2} p_j \log_2 p_j$, где $p_j \geq 0$ и $p_1 + p_2 = 1$, имеет максимальное значение 1 при условии, что $p_1 = p_2 = 1/2$.

Указание

Представить S в виде $S(p) = -p \log_2 p - (1-p)\log_2(1-p)$ и найти максимум функции $S(p)$.

8. Написать матрицу плотности спинового состояния одной из частиц ЭПР-пары, находящейся в перепутанных состояниях $\left|\Phi^{(\pm)}\right\rangle$, $\left|\Psi^{(+)}\right\rangle$. Вычислить энтропию фон Неймана.

9. Показать, что произвольная спиновая матрица плотности $\hat{\rho}$ может быть представлена в виде

$$\hat{\rho} = \frac{1}{2}\left(1 + \vec{a}\vec{\sigma}\right),$$

где σ_i – матрицы Паули, вектор $\vec{a}$ является действительным, а его длина $|\vec{a}| \le 1$.

Указание

Воспользоваться результатом задачи 4 в конце раздела 2.2, а также свойствами матриц Паули (2.41). В случае чистого состояния, когда $\hat{\rho}^2 = \hat{\rho}$, величина $|\vec{a}| = 1$. Для произвольного смешанного состояния неравенство $|\vec{a}| \le 1$ следует из условия, что $Sp\hat{\rho}^2 \le 1$.

10. Рассмотреть задачу об отражении и прохождении частицы с энергией $E = \dfrac{\hbar^2 k^2}{2m}$ через одномерный потенциальный барьер $U(z) = \alpha\delta(z)$, $\alpha > 0$. Убедиться, что при $\dfrac{m\alpha}{\hbar^2 k} \equiv \vartheta = 1$ амплитуды прохождения и отражения совпадают с формулами (2.182) и (2.183) с точностью до общего фазового множителя.

Решение

Так как $U(z) = \alpha\delta(z)$, то стационарное уравнение Шрёдингера

$$\frac{d^2\Psi}{dz^2} + \frac{2m}{\hbar^2}\left(E - U(z)\right)\Psi = 0$$

при $z \neq 0$ имеет вид

$$\frac{d^2\Psi}{dz^2} + k^2 z = 0.$$

Ищем решение, описывающее частицу, падающую на потенциальный барьер слева.

Тогда решение в области $z < 0$

$$\Psi\left(z<0\right) = e^{ikz} + Be^{-ikz}$$

является суперпозицией падающей (e^{ikz}) и отраженной (e^{-ikz}) волн. В области $z > 0$ есть только прошедшая волна:

$$\Psi\left(z>0\right) = Ce^{ikz}.$$

Волновая функция $\Psi\left(z\right)$ должна быть непрерывной в точке $z = 0$, т.е. $\Psi\left(+0\right) = \Psi\left(-0\right) \equiv \Psi\left(0\right)$ и удовлетворять условию на скачок производной $\Psi'\left(+0\right) - \Psi'\left(-0\right) \equiv \frac{2m\alpha}{\hbar^2}\Psi\left(0\right)$, которое связано с наличием в точке $z = 0$ сингулярного $\delta-$*функционного* потенциала. Из этих двух условий получаем уравнение для коэффициентов *B* и *C*:

$$\begin{cases} 1 + B = C \\ 1 - B = \left(1 + 2i\vartheta\right)C, \ \ \vartheta = \dfrac{m\alpha}{\hbar^2 k} \end{cases}.$$

Тогда

$$C = \frac{1}{1+i\vartheta}, \ B = -\frac{i\vartheta}{1+i\vartheta}.$$

Эти коэффициенты удовлетворяют условию $\left|B\right|^2 + \left|C\right|^2 = 1$, которое выражает тот факт, что плотность потока вероятности $j = \frac{i\hbar}{2m}\left(\Psi\frac{\partial\Psi^*}{\partial z} - к.с.\right)$ не зависит от *z*. Коэффициент *C* описывает амплитуду прошедшей волны, а *B* – амплитуду отраженной волны.

Если $\vartheta = 1$, то

$$C = \tfrac{1}{\sqrt{2}}\, e^{-i\pi/4}, \quad B = -\tfrac{i}{\sqrt{2}}\, e^{-i\pi/4}.$$

Мы видим, что с точностью до общего фазового множителя $e^{-i\pi/4}$, амплитуды C и B совпадают, соответственно, с выражениями (2.182) и (2.183).

11. На светоделитель падают два одинаковых по частоте фотона – один слева, другой справа. Фотоны находятся в симметричном перепутанном по поляризациям состоянии (ЭПР-пара)

$$\left|\Psi^{(+)}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|v\right\rangle_1\left|h\right\rangle_2 + \left|h\right\rangle_1\left|v\right\rangle_2\right).$$

Где могут быть зарегистрированы фотоны после взаимодействия со светоделителем? По одну или по разные стороны от светоделителя?

Решение

Вектор исходного состояния системы двух фотонов симметричен относительно перестановки частиц ($1 \rightleftarrows 2$) и имеет вид

$$\left|in\right\rangle = \frac{1}{\sqrt{2}}\left(\left|k\right\rangle_1\left|-k\right\rangle_2 + \left|-k\right\rangle_1\left|k\right\rangle_2\right)\left|\Psi^{(+)}\right\rangle =$$

$$= \frac{1}{2}\left\{\left|kv\right\rangle_1\left|-kh\right\rangle_2 + \left|-kh\right\rangle_1\left|kv\right\rangle_2 + (k \rightleftarrows -k)\right\},$$

где ($k \rightleftarrows -k$) означает, что эти члены получаются изменением знака у волновых векторов.

Используя преобразования (2.177) и (2.178), получаем состояние системы на выходе из светоделителя:

$$
\begin{aligned}
&\left|out\right\rangle = \\
&= \frac{1}{4}\left\{\left[\left(\left|kv\right\rangle_1 - i\left|-kv\right\rangle_1\right)\left(\left|-kh\right\rangle_2 - i\left|kh\right\rangle_2\right) + \left(1 \rightleftarrows 2\right)\right] + \left(k \rightleftarrows -k\right)\right\} = \\
&= -\frac{i}{2}\left\{\left|kv\right\rangle_1\left|kh\right\rangle_2 + \left|kh\right\rangle_1\left|kv\right\rangle_2 + \left(k \rightleftarrows -k\right)\right\} = \\
&= -\frac{i}{\sqrt{2}}\left(\left|k\right\rangle_1\left|k\right\rangle_2 + \left|-k\right\rangle_1\left|-k\right\rangle_2\right)\left|\Psi^{(+)}\right\rangle.
\end{aligned}
$$

Мы видим, что оба фотона будут иметь одинаковые волновые векторы — либо k, либо $-k$. Это означает, что после взаимодействия со светоделителем они могут быть зарегистрированы только по одну сторону от светоделителя – либо справа, либо слева. Для выбранного начального условия деструктивная квантовая интерференция обращает в нуль амплитуду вероятности выхода пары фотонов с разными волновыми векторами.

2.5. Двухкубитовые гейты

Произвольное унитарное преобразование в пространстве состояний двухкубитовой системы нельзя сконструировать с помощью только однокубитовых гейтов. Было показано, например, что максимально перепутанные и факторизованные состояния не могут переходить друг в друга под воздействием только однокубитовых операторов. В том, что произвольное двухкубитовое унитарное преобразование не может быть представлено в виде тензорного произведения однокубитовых операторов, можно формально убедиться следующим образом. Любое число унитарных операторов, примененных к одному кубиту, эквивалентно некоторой результирующей унитарной матрице $\hat{U}_1$, которая определяется, как мы знаем, четырьмя действительными параметрами. Поэтому тензорное произведение двух таких произвольных матриц содержит, в общем

случае, 4+4–1=7 параметров, поскольку общие фазы суммируются. Унитарная 4×4 матрица $\hat{U}_2$ двухкубитового преобразования содержит 16 комплексных чисел, т.е. 32 действительных параметра, на которые накладывается условие унитарности $\hat{U}_2^{+}\hat{U}_2=\mathbf{1}$. Поскольку 4×4 матрица $\hat{U}_2^{+}\hat{U}_2$ является эрмитовой, то ее диагональные элементы действительные, а симметрично расположенные недиагональные элементы комплексно сопряжены по отношению друг к другу. Поэтому из уравнения

$$\hat{U}_2^{+}\hat{U}_2=\begin{pmatrix} a_1 & b_1 & b_2 & b_3 \\ b_1^{*} & a_2 & c_1 & c_2 \\ b_2^{*} & c_1^{*} & a_3 & d_1 \\ b_3^{*} & c_2^{*} & d_1^{*} & a_4 \end{pmatrix}=\mathbf{1} \qquad (2.189)$$

получаются 4 действительных, $a_{1,2,3,4}=1$, и 6 комплексных, $b_{1,2,3}=c_{1,2}=d_1=0$, соотношений, т.е. всего 16 действительных условий. Это означает, что для задания произвольной двухкубитовой унитарной матрицы требуется 32–16=16 действительных параметров.

Гейт CNOT

Наиболее важным двухкубитовым гейтом является операция *Controlled NOT (*CNOT*)*, т.е. «*управляемое НЕ*». Как мы увидим, этот логический элемент играет фундаментальную роль в синтезе любых мультикубитовых гейтов.

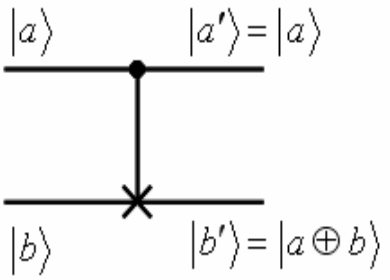
Гейт CNOT описывается унитарным оператором

$$CNOT=|0\rangle\langle 0|\otimes I+|1\rangle\langle 1|\otimes\sigma_1, \qquad (2.190)$$

который представляет собой сумму двух тензорных произведений. В каждом слагаемом операторы, стоящие слева, действуют на пер-

вый кубит, а операторы, стоящие справа – на второй кубит. Первые операторы являются проекторами на базисные состояния $|0\rangle$ и $|1\rangle$. На второй кубит действует либо тождественный оператор *I*, либо σ_1, который описывает однокубитовый элемент NOT (2.56). При этом воздействие на второй кубит того или иного однокубитового гейта зависит от состояния первого кубита, который, тем самым, управляет преобразованием своего партнера. Первый кубит называется *управляющим*, а второй – *управляемым*.

На рис. 2.12 слева изображена квантовая схема операции CNOT. Верхняя линия отвечает управляющему кубиту, а нижняя – управляемому. Темный кружок и крестик, расположенные на этих линиях и соединенные вертикальной прямой, собственно, и представляют операцию CNOT. Темный кружок стоит на линии управляющего кубита, а крестик, изображающий операцию NOT, расположен на линии управляемого кубита.



a	b		a'	$b' = a \oplus b$
0	0		0	0
0	1		0	1
1	0		1	1
1	1		1	0

Рис. **2.12**

Из структуры выражения (2.190) видно, что операция *CNOT* действует следующим образом. Если управляющий кубит $|a\rangle$ находится в состоянии $|0\rangle$, то с управляемым кубитом $|b\rangle$ ничего не происходит. Если же управляющий кубит находится в состоянии $|1\rangle$, то управляемый кубит проходит через операцию NOT, т.е. «переворачивается». Обратим внимание еще на одно полезное

свойство гейта CNOT. Если $|b\rangle$ находится сначала в состоянии $|0\rangle$, то после операции CNOT он будет в том же состоянии, что и кубит $|a\rangle$, т.е. происходит копирование кубита $|a\rangle$. Для аккуратности заметим, что управляющий кубит свое состояние не меняет. Таблица истинности для начальных (*a* и *b*) и конечных (a' и b') значений битов приведена на рис. 2.12 справа.

С точки зрения квантовых вычислений, гейт CNOT осуществляет операцию сложения битов *a* и *b* по модулю 2. Эта операция обозначена символом $a \oplus b$, а ее результат записан в выходном состоянии управляемого кубита, $|b'\rangle = |a \oplus b\rangle$. Тот факт, что в конечном состоянии системы сохраняется состояние управляющего кубита $|a\rangle$, обеспечивает обратимость данной вычислительной операции. Это есть прямое следствие унитарности преобразования (2.190).

При рассмотрении квантовых схем с участием гейта CNOT оказываются полезными различные представления этой операции.

Подставляя в (2.190) выражение (2.47) и (2.63) для операторов, соответственно, σ_1 и *I*, получаем

$$\begin{aligned} CNOT &= |0\rangle\langle 0| \otimes (|0\rangle\langle 0| + |1\rangle\langle 1|) + \\ &+ |1\rangle\langle 1| \otimes (|0\rangle\langle 1| + |1\rangle\langle 0|) = \\ &= |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10|. \end{aligned} \qquad (2.191)$$

Это операторное представление показывает, что при унитарном преобразовании CNOT базисные двухкубитовые состояния $|00\rangle$ и $|01\rangle$ остаются неизменными, а состояния $|10\rangle$ и $|11\rangle$ переходят одно в другое. Поэтому повторное применение гейта CNOT возвращает систему к исходному состоянию, т.е. $(CNOT)^2 = \mathbf{1}$, и обратное преобразование $(CNOT)^{-1}$ совпадает с *CNOT*.

Из выражения (2.191) так же непосредственно следует вид мат-

рицы оператора CNOT в двухкубитовом вычислительном базисе. Действительно, коэффициенты при внешних произведениях базисных кэт-векторов, которые входят в (2.191), суть отличные от нуля матричные элементы оператора CNOT. С методической целью найдем эту матрицу, используя правило (2.138) вычисления кронекерова произведения матриц. Вспоминая матрицы

$$|0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad |1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},$$

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

однокубитовых операторов, получаем

$$CNOT = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} =$$

$$= \left(\begin{array}{cc:cc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hdashline 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right) + \left(\begin{array}{cc:cc} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \hdashline 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{array}\right) = \left(\begin{array}{cc:cc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hdashline 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{array}\right). \quad (2.192)$$

Пунктирные линии в 4×4 матрицах выполняют роль, как принято говорить, «гида для взгляда», и не более того.

В таблице истинности на рис. 2.12 приведены результаты действия гейта CNOT в тех случаях, когда управляющий кубит $|a\rangle$ находится в одном из базисных состояний $|0\rangle$ или $|1\rangle$. Представляет интерес рассмотреть такую ситуацию, когда состояние системы на входе имеет вид $|in\rangle = |a\rangle|b\rangle$, а управляющий кубит находится в произвольном суперпозиционном состоянии $|a\rangle = \alpha|0\rangle + \beta|1\rangle$.

Применение операции CNOT дает

$$\begin{aligned}
&\left|out\right\rangle = CNOT\left|in\right\rangle = \left(\left|0\right\rangle\left\langle 0\right| \otimes I + \left|1\right\rangle\left\langle 1\right| \otimes NOT\right)\left|a\right\rangle\left|b\right\rangle = \\
&= \left\langle 0\middle|a\right\rangle\left|0\right\rangle\left|b\right\rangle + \left\langle 1\middle|a\right\rangle\left|1\right\rangle\left(NOT\left|b\right\rangle\right) = \\
&= \alpha\left|0\right\rangle\left|b\right\rangle + \beta\left|1\right\rangle\left|\bar{b}\right\rangle,
\end{aligned} \tag{2.193}$$

где результат действия операции NOT на управляемый кубит $\left|b\right\rangle$ обозначен как $\left|\bar{b}\right\rangle$. Если $\left|b\right\rangle = \left|0\right\rangle$, то $\left|\bar{b}\right\rangle = \left|1\right\rangle$ и

$$\left|out\right\rangle = \alpha\left|00\right\rangle + \beta\left|11\right\rangle. \tag{2.194}$$

Аналогично, если $\left|b\right\rangle = \left|1\right\rangle$, то $\left|\bar{b}\right\rangle = \left|0\right\rangle$ и

$$\left|out\right\rangle = \alpha\left|01\right\rangle + \beta\left|10\right\rangle. \tag{2.195}$$

Таким образом, под действием операции CNOT факторизованное состояние $\left|a\right\rangle\left|b\right\rangle$ переходит в перепутанное двухкубитовое состояние. Наряду с этим, с помощью гейта CNOT можно совершить и обратную операцию, т.е. факторизовать перепутанное состояние, поскольку оператор CNOT совпадает со своим обратным. Именно с этим свойством связана фундаментальная роль логического элемента CNOT при конструировании мультикубитовых гейтов.

Для примера покажем, как с помощью элементарных квантовых гейтов можно создать перепутанное состояние, например, $\left|\Psi^{+}\right\rangle$ двух кубитов, которые первоначально были в факторизованном базисном состоянии $\left|00\right\rangle \equiv \left|0\right\rangle\left|0\right\rangle$. Протокол такого преобразования изображается схемой, представленной на рис. 2.13.

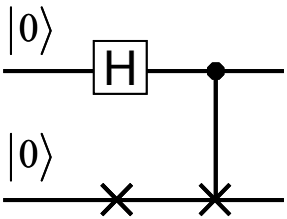


Рис. **2.13**

Соответствующая последовательность операций выглядит так:

$$\left|00\right\rangle \xrightarrow{NOT_2} \left|01\right\rangle \xrightarrow{H_1} \frac{\left|0\right\rangle+\left|1\right\rangle}{\sqrt{2}}\left|1\right\rangle \xrightarrow{CNOT} \xrightarrow{CNOT} \frac{1}{\sqrt{2}}\left(\left|01\right\rangle+\left|10\right\rangle\right) \equiv \left|\Psi^{+}\right\rangle , \quad (2.196)$$

т.е. сначала совершаются операция NOT (σ_1) над вторым кубитом и преобразование Адамара (H) над первым кубитом, а заключительный гейт CNOT переводит систему в состояние Белла $\left|\Psi^{+}\right\rangle$. Применяя далее к этому состоянию однокубитовые гейты σ_i, можно получить, как следует из соотношений типа (2.169) – (2.170), остальные состояния Белла.

Иногда бывает удобно модифицировать гейт CNOT к виду

$$\widetilde{CNOT} = \left|0\right\rangle\left\langle 0\right| \otimes \sigma_1 + \left|1\right\rangle\left\langle 1\right| \otimes I . \quad (2.197)$$

В этом случае состояния $\left|0\right\rangle$ и $\left|1\right\rangle$ управляющего кубита поменялись ролями. Теперь управляемый кубит подвергается операции NOT в том случае, когда управляющий кубит находится в состоянии $\left|0\right\rangle$.

Матрица преобразования (2.197) выглядит так:

$$\widetilde{CNOT} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \qquad (2.198)$$

На рис. 2.14 слева изображена квантовая схема операции $\widetilde{CNOT}$. На линии управляющего кубита теперь нарисован светлый кружок. Справа показана эквивалентная схема, которая отличается от гейта CNOT двумя дополнительными однокубитовыми операциями NOT на линии управляющего кубита. Роль этих однокубитовых гейтов сводится к тому, что исходное состояние управляющего кубита сначала подвергается операции NOT, а после обычного гейта CNOT возвращается назад. Легко убедиться в эквивалентности квантовых схем. Пусть, например, сначала управляющий кубит был в состоянии $|0\rangle$. После операции NOT он переходит в состояние $|1\rangle$. Затем следует обычная операция CNOT, которая изменяет состояние управляемого кубита. Наконец, последняя операция NOT возвращает управляющий кубит в исходное состояние $|0\rangle$. В результате получилось, что операция NOT применяется ко второму кубиту, если управляющий кубит находится в состоянии $|0\rangle$. Это соответствует гейту $\widetilde{CNOT}$.

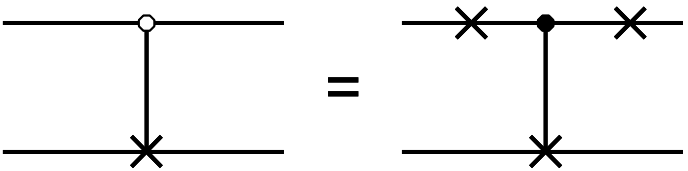


Рис. **2.14**

Формальное доказательство эквивалентности квантовых схем, представленных на рис. 2.14, можно получить с помощью «алгебраического» преобразования операторного выражения (2.197). Принимая во внимание, что

$$\sigma_1 |0\rangle = |1\rangle \text{ и } \sigma_1 |1\rangle = |0\rangle,$$

и подставляя эти соотношения в (2.197), получаем:

$$\begin{aligned} \widetilde{CNOT} &= \left(\sigma_1 |1\rangle\langle 1|\sigma_1\right) \otimes \sigma_1 + \left(\sigma_1 |0\rangle\langle 0|\sigma_1\right) \otimes I = \\ &= \sigma_1^{(1)} \left\{ |1\rangle\langle 1| \otimes \sigma_1 + |0\rangle\langle 0| \otimes I \right\} \sigma_1^{(1)} = \sigma_1^{(1)} CNOT \sigma_1^{(1)}. \end{aligned} \tag{2.199}$$

В первой строчке мы не снабжали операторы σ_1 верхним индексом, поскольку совершенно ясно, на какие кубиты они действуют. На следующем шаге верхний значок у оператора $\sigma_1^{(1)}$ подчеркивает, что этот оператор действует на первый (управляющий) кубит. В фигурной скобке σ_1 относится к управляемому кубиту, так что весь стоящий в этой скобке оператор есть CNOT (2.190).

Управляемое U

Обобщением операции CNOT является двухкубитовый гейт *Controlled U*, т.е. «*управляемое U*». Он описывается унитарным оператором

$$|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes \hat{U}, \tag{2.200}$$

который обобщает гейт CNOT в том плане, что на управляемый кубит действует некоторый произвольный унитарный однокубитовый оператор $\hat{U}$ в том случае, когда управляющий кубит находится в состоянии $|1\rangle$. Квантовая схема этого гейта показана на рис. 2.15.

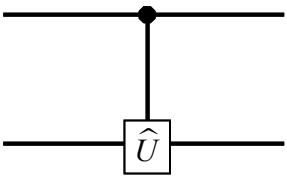


Рис. **2.15**

Если $\hat{U} = \begin{pmatrix} u & w \\ v & z \end{pmatrix}$, то оператору (2.200) отвечает матрица

$$\left(\begin{array}{cc:cc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hdashline 0 & 0 & u & w \\ 0 & 0 & v & z \end{array}\right). \qquad (2.201)$$

При $\hat{U} = \sigma_1$ мы получаем, очевидно, гейт CNOT.

В качестве простого примера рассмотрим операцию управляемого преобразования общей фазы второго кубита. В этом случае однокубитовый оператор

$$\hat{U} = e^{i\alpha} I = e^{i\alpha}$$

сводится к умножению состояния управляемого кубита на фазовый множитель $e^{i\alpha}$. При таком преобразовании два базисных вектора системы $|00\rangle$ и $|01\rangle$ не меняются, а два других приобретают фазовый множитель, $|10\rangle \to e^{i\alpha}|10\rangle$ и $|11\rangle \to e^{i\alpha}|11\rangle$. Этот фазовый множитель можно отнести к состоянию $|1\rangle$ управляющего кубита. Поскольку состояние $|0\rangle$ этого кубита не меняется, то результат описывается однокубитовым оператором $P(\alpha)$ (2.62) сдвига относительно фазы. Что касается управляемого кубита, то при таком

описании его состояние не меняется. Поэтому на рис. 2.16 показаны две эквивалентные квантовые схемы, описывающие операцию управляемого преобразования фазы.

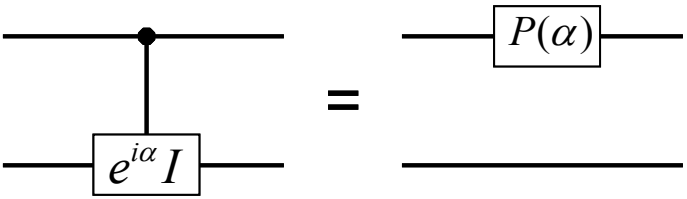


Рис. **2.16**

Эквивалентность схем можно, конечно, доказать с помощью простого преобразования операторов, а именно,

$$|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes e^{i\alpha} I = \left(|0\rangle\langle 0| + e^{i\alpha} |1\rangle\langle 1|\right) \otimes I = \\ = P(\alpha) \otimes I. \tag{2.202}$$

Покажем, что операцию «*управляемое U*» можно выразить через однокубитовые гейты и операцию CNOT. Напомним, что произвольный однокубитовый унитарный оператор $\hat{U}$ после выделения общего фазового множителя $e^{i\alpha}$ сводится к матрице конечных вращений (2.48)

$$\hat{R} \equiv \hat{R}(\Phi, \vec{n})$$

для спина $1/2$, т.е.

$$\hat{U} = e^{i\alpha} \hat{R}. \tag{2.203}$$

Что касается фазового множителя, то его можно описать, как мы показали, с помощью однокубитового оператора $P^{(1)}(\alpha)$ сдвига относительной фазы первого (управляющего) кубита.

Действительно, из преобразования операторов, аналогичного (2.202) следует, что

$$\begin{aligned}&|0\rangle\langle 0|\otimes I+|1\rangle\langle 1|\otimes e^{i\alpha}\hat{R}=|0\rangle\langle 0|\otimes I+e^{i\alpha}|1\rangle\langle 1|\otimes\hat{R}=\\&=P^{(1)}(\alpha)\left\{|0\rangle\langle 0|\otimes I+|1\rangle\langle 1|\otimes\hat{R}\right\}.\end{aligned}\tag{2.204}$$

Выражение, стоящее в фигурной скобке, описывает, очевидно, операцию «*управляемое R*». Общий вид матрицы конечных вращений $\hat{R}$, которая входит в (2.204), удобно задать с помощью параметров γ, ψ и χ, (2.69)-(2.70), т.е.

$$\hat{R}=\begin{pmatrix}e^{i\chi}\cos\dfrac{\gamma}{2} & e^{-i\psi}\sin\dfrac{\gamma}{2}\\ -e^{i\psi}\sin\dfrac{\gamma}{2} & e^{-i\chi}\cos\dfrac{\gamma}{2}\end{pmatrix}.\tag{2.205}$$

Такую матрицу можно представить в виде произведения вращений вокруг осей *z* и *y* (см. задачу 11 в конце раздела 2.2). Матрицы вращений вокруг этих осей получаются из общего выражения (2.48)

$$\hat{R}(\Phi,\vec{n})=e^{i\frac{\Phi}{2}(\vec{n}\vec{\sigma})}=\cos\frac{\Phi}{2}+i(\vec{n}\vec{\sigma})\sin\frac{\Phi}{2}\tag{2.206}$$

и имеют вид

$$\hat{R}_z(\beta)=\cos\frac{\beta}{2}+i\sigma_z\sin\frac{\beta}{2}=\begin{pmatrix}e^{i\beta/2} & 0\\ 0 & e^{-i\beta/2}\end{pmatrix},\tag{2.207}$$

$$\hat{R}_y(\gamma)=\cos\frac{\gamma}{2}+i\sigma_y\sin\frac{\gamma}{2}=\begin{pmatrix}\cos\gamma/2 & \sin\gamma/2\\ -\sin\gamma/2 & \cos\gamma/2\end{pmatrix}.\tag{2.208}$$

Непосредственным перемножением матриц убеждаемся, что выражение (2.205) записывается в виде:

$$\hat{R} = \hat{R}_z(\beta)\hat{R}_y(\gamma)\hat{R}_z(\delta). \qquad (2.209)$$

При этом углы β и δ двух поворотов вокруг оси *z* влияют только на фазы χ и ψ, а именно:

$$\chi = \frac{\delta+\beta}{2},\ \psi = \frac{\delta-\beta}{2}. \qquad (2.210)$$

Представим теперь матрицу $\hat{R}$ (2.209) в виде

$$\hat{R} = \hat{A}\sigma_1\hat{B}\sigma_1\hat{C}, \qquad (2.211)$$

где унитарные матрицы $\hat{A}$, $\hat{B}$ и $\hat{C}$ удовлетворяют соотношению

$$\hat{A}\hat{B}\hat{C} = \mathbf{1}. \qquad (2.212)$$

Проверим, что интересующие нас матрицы $\hat{A}$, $\hat{B}$ и $\hat{C}$ имеют следующий вид:

$$\begin{aligned}
&\hat{A} = \hat{R}_z(\beta)\hat{R}_y(\gamma/2),\\
&\hat{B} = \hat{R}_y(-\gamma/2)\hat{R}_z\left(-\frac{\delta+\beta}{2}\right),\\
&\hat{C} = \hat{R}_z\left(\frac{\delta-\beta}{2}\right).
\end{aligned} \qquad (2.213)$$

Каждая из матриц $\hat{R}_y$ и $\hat{R}_z$, входящих в (2.213), представляет собой операцию вращения. Вращение на нулевой угол есть, очевидно, тождественное преобразование. Если совершаются одно за другим два вращения вокруг одной и той же оси, то результатом

является вращение вокруг той же оси на суммарный угол[1]. Например,

$$\hat{R}_z(\chi)\hat{R}_z(\psi) = \hat{R}_z(\chi+\psi)\,.$$

Тогда

$$\hat{A}\hat{B}\hat{C} = \hat{R}_z(\beta)\hat{R}_y(\gamma/2)\hat{R}_y(-\gamma/2)\hat{R}_z\left(-\frac{\delta+\beta}{2}\right)\hat{R}_z\left(\frac{\delta-\beta}{2}\right) =$$

$$= \hat{R}_z(\beta)\hat{R}_z(-\beta) = \mathbf{1},$$

и условие (2.212) выполняется. Произведение, написанное в правой части (2.211), преобразуется следующим образом:

$$\begin{aligned}
&\hat{A}\sigma_1\hat{B}\sigma_1\hat{C} = \\
&= \hat{R}_z(\beta)\hat{R}_y(\gamma/2)\sigma_1\hat{R}_y(-\gamma/2)\hat{R}_z\left(-\frac{\delta+\beta}{2}\right)\times \\
&\quad\times\sigma_1\hat{R}_z\left(\frac{\delta-\beta}{2}\right) = \\
&= R_z(\beta)\hat{R}_y(\gamma/2)\left(\sigma_1\hat{R}_y(-\gamma/2)\sigma_1\right)\times \\
&\quad\times\left(\sigma_1\hat{R}_z\left(-\frac{\delta+\beta}{2}\right)\sigma_1\right)\hat{R}_z\left(\frac{\delta-\beta}{2}\right) = \\
&= \hat{R}_z(\beta)\hat{R}_y(\gamma/2)\hat{R}_y(\gamma/2)\hat{R}_z\left(\frac{\delta+\beta}{2}\right)\hat{R}_z\left(\frac{\delta-\beta}{2}\right) = \\
&= \hat{R}_z(\beta)\hat{R}_y(\gamma)\hat{R}_z(\delta).
\end{aligned} \qquad (2.214)$$

---

[1] Непрерывное унитарное преобразование $\hat{U}(\lambda) = \exp(i\lambda\hat{F})$, где λ – действительный параметр, а $\hat{F} = \hat{F}^+$, обладает групповым свойством $\hat{U}(\lambda_1+\lambda_2) = \hat{U}(\lambda_1)\hat{U}(\lambda_2)$ (см. задачу 7 в конце раздела 2.2).

Здесь на втором шаге между соседними множителями, матрицами $\hat{R}_y\left(-\gamma/2\right)$ и $\hat{R}_z\left(-\frac{\delta+\beta}{2}\right)$, вместо 1 написали $\sigma_1^2=1$. В результате каждая из этих матриц оказывается взятой в «обкладки» из оператора σ_1, что эквивалентно изменению знака угла поворота. Так, например, генератором поворота (2.206) вокруг оси *y* является матрица Паули $\sigma_y\equiv\sigma_2$, которая согласно (2.46) антикоммутирует с σ_1. Следовательно,

$$\begin{aligned}&\sigma_1 R_y\left(-\gamma/2\right)\sigma_1=\sigma_1\exp\left(-i\frac{\gamma}{4}\sigma_2\right)\sigma_1=\\&=\exp\left(i\frac{\gamma}{4}\sigma_2\right)=R_y\left(\gamma/2\right).\end{aligned}\qquad(2.215)$$

Аналогичное соотношение имеет место и для вращения $R_z\left(-\frac{\delta+\beta}{2}\right)$, так как оно генерируется матрицей Паули $\sigma_z\equiv\sigma_3$, которая антикоммутирует с σ_1. С учетом этих соотношений мы приходим к окончательному выражению, стоящему в правой части (2.214). Поскольку параметры γ, β и δ произвольные, то (2.214) представляет согласно (2.207)-(2.210) общий вид унитарной матрицы конечных вращений $\hat{R}$, как того требует условие (2.211).

На рис. 2.17 представлена квантовая схема гейта «*управляемое U*», основанная на выражениях (2.203), (2.204) и (2.211).

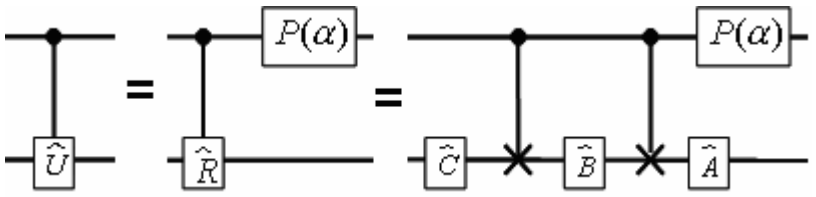


Рис. **2.17**

Первый шаг иллюстрирует соотношение (2.204), которое описывает процедуру выделения из $\hat{U}$ фазового множителя $e^{i\alpha}$ с помощью однокубитового гейта $P(\alpha)$. Окончательная схема содержит еще три однокубитовых оператора $\hat{C}$, $\hat{B}$ и $\hat{A}$ и два гейта CNOT.

Действительно, если управляющий кубит в состоянии $|0\rangle$, то он не оказывает влияния на другой кубит, и отмеченные крестиками операторы σ_1 на линии управляемого кубита отсутствуют. На этой линии остаются только операторы $\hat{C}$, $\hat{B}$, $\hat{A}$, произведение которых есть тождественное преобразование, $\hat{A}\hat{B}\hat{C} = 1$. Фаза управляющего кубита в состоянии $|0\rangle$ не меняется, и мы получаем следующее преобразование состояния двухкубитовой системы:

$$|0b\rangle = |0\rangle|b\rangle \to |0\rangle|b\rangle = |0b\rangle. \qquad (2.216)$$

Если же управляющий кубит в состоянии $|1\rangle$, то на управляемый кубит действуют дополнительно две операции σ_1. Поэтому его состояние подвергается преобразованию $\hat{A}\sigma_1\hat{B}\sigma_1\hat{C} = \hat{R}$. Кроме того, состояние управляющего кубита приобретает дополнительный фазовый множитель $e^{i\alpha}$. Результирующее преобразование двухкубитового состояния имеет вид

$$|1b\rangle = |1\rangle|b\rangle \to e^{i\alpha}|1\rangle\left(\hat{R}|b\rangle\right) = |1\rangle\left(\hat{U}|b\rangle\right). \qquad (2.217)$$

Законы преобразования (2.216) и (2.217) в точности соответствуют операции (2.200).

Таким образом, мы видим, что операцию «*управляемое U*» можно выразить с помощью конечного числа однокубитовых гейтов и операций CNOT. Обобщим это утверждение на случай произвольной унитарной двухкубитовой операции.

Универсальный набор гейтов для двухкубитовых операций

Оператор (2.200) перемешивает только два базисных кэт-вектора $|10\rangle$ и $|11\rangle$ системы, не затрагивая состояния $|00\rangle$ и $|01\rangle$. Матрица (2.201) этого оператора содержит унитарную 2×2 подматрицу $\hat{U}$. Такие операторы и соответствующие им матрицы, которые перемешивают только два базисных состояния, называются двухуровневыми. Они существенным образом перемешивают проекции векторов состояний на двухмерное подпространство, натянутое на два базисных кэт-вектора, и не затрагивают другие проекции.

Сначала покажем, что операцию, которая описывается двухуровневой унитарной 4×4 матрицей, можно выразить с помощью набора однокубитовых преобразований и гейта CNOT.

Заметим, что в нашем случае есть всего 6 различных видов двухуровневых матриц в соответствии с числом пар, которые можно составить из четырех базисных векторов. Для четырех пар перемешиваемые состояния отличаются значением одного бита, например $|00\rangle$ и $|01\rangle$. Сюда же относится и рассмотренный случай с матрицей (2.201), которая, напомним, перемешивает состояния $|10\rangle$ и $|11\rangle$. Квантовые схемы для указанных матриц получаются, как мы покажем, простой модификацией схемы, изображенной на рис. 2.15. Есть еще две пары состояний, $|00\rangle$ и $|11\rangle$, а также $|01\rangle$ и $|10\rangle$, которые отличаются значениями двух битов и будут рассмотрены отдельно.

Начнем, например, с двухуровневой 4×4 матрицы

$$\begin{pmatrix} u & 0 & w & 0 \\ 0 & 1 & 0 & 0 \\ v & 0 & z & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \qquad (2.218)$$

Она перемешивает состояния $|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$ и $|10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$ с помощью унитарной 2×2 подматрицы $\hat{U} = \begin{pmatrix} u & w \\ v & z \end{pmatrix}$. Сравнивая эти два состояния с парой $|10\rangle$ и $|11\rangle$, делаем вывод, что квантовую схему рис. 2.15 надо изменить так, чтобы управляющим стал второй кубит. При этом операция $\hat{U}$ должна действовать на первый кубит в том случае, когда управляющий кубит находится в состоянии $|0\rangle$. Такая схема показана на рис. 2.18 в двух эквивалентных видах.

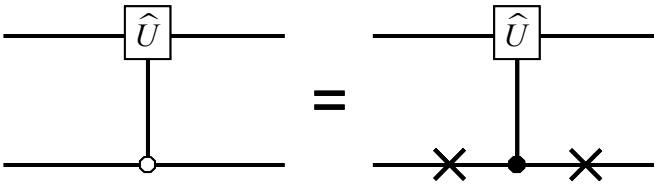


Рис. **2.18**

Для проверки найдем результат действия этой схемы, например, на следующее состояние $|00\rangle$:

$$|00\rangle = |0\rangle|0\rangle \to \left(\hat{U}|0\rangle\right)|0\rangle = \left(u|0\rangle + v|1\rangle\right)|0\rangle = u|00\rangle + v|10\rangle .$$

Это совпадает с результатом действия матрицы (2.218) на вектор-столбец входного состояния, так как

$$\begin{pmatrix} u & 0 & w & 0 \\ 0 & 1 & 0 & 0 \\ v & 0 & z & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} u \\ 0 \\ v \\ 0 \end{pmatrix} = u \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + v \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}.$$

Точно так же проверяется, что преобразование остальных базисных состояний

$$\begin{aligned}
&|10\rangle \to \left(\hat{U}|1\rangle\right)|0\rangle = w|00\rangle + z|10\rangle,\\
&|01\rangle \to |01\rangle,\\
&|11\rangle \to |11\rangle
\end{aligned}$$

эквивалентно действию матрицы (2.218) на соответствующие вектор-столбцы.

Так как операция «*управляемое U*» выражается, как было показано ранее, через однокубитовые преобразования и гейты CNOT, то это утверждение справедливо и для квантовой схемы, которая представлена на рис. 2.18 и отвечает матрице (2.218). Аналогичным образом строятся еще две квантовые схемы, которые отвечают матрицам, перемешивающим состояния $|00\rangle$ и $|01\rangle$, а также $|01\rangle$ и $|11\rangle$. Они предлагаются в качестве задачи в конце данного раздела. Еще раз подчеркнем, что все эти схемы относятся к преобразованиям, которые перемешивают пару базисных состояний, отличающихся значением одного бита, с помощью однокубитовой подматрицы $\hat{U}$. Поэтому рецепт построения таких схем очевиден: кубит с совпадающим для двух перемешиваемых состояний значением бита надо взять в качестве управляющего и совершить над другим кубитом преобразование типа «*управляемое U*».

Рассмотрим теперь двухуровневую матрицу

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & u & w & 0 \\ 0 & v & z & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \qquad (2.219)$$

Она перемешивает два базисных состояния $|01\rangle$ и $|10\rangle$, которые отличаются значениями двух битов. Чтобы использовать подмат-

рицу $\hat{U} = \begin{pmatrix} u & w \\ v & z \end{pmatrix}$ как однокубитовое преобразование, надо поменять местами состояния $|01\rangle$ и $|00\rangle$, не затрагивая другие базисные векторы. Такая перестановка осуществляется с помощью операции $\widetilde{CNOT}$. После этого состояния $|00\rangle$ и $|10\rangle$ отличаются значением только одного бита, и можно применить операцию «*управляемое U*», в которой управляющее воздействие осуществляется вторым кубитом в состоянии $|0\rangle$. На последнем шаге надо с помощью гейта $\widetilde{CNOT}$ совершить обратную перестановку состояний $|00\rangle$ и $|01\rangle$. Описанная квантовая схема показана на рис. 2.19.

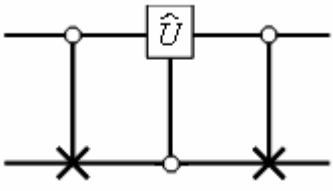


Рис. **2.19**

Рассмотрим для примера действие этой схемы на состояние $|10\rangle$. Поскольку в этом случае первая операция $\widetilde{CNOT}$ не работает, то цепочка преобразований входного состояния выглядит так:

$$\begin{aligned} |10\rangle \to \left(\hat{U}|1\rangle\right)|0\rangle = \left(w|0\rangle + z|1\rangle\right)|0\rangle = \\ = w|00\rangle + z|10\rangle \to w|01\rangle + z|10\rangle. \end{aligned} \qquad (2.220)$$

Это, конечно, совпадает с результатом действия матрицы (2.219) на соответствующий вектор-столбец. Аналогичным образом строится квантовая схема для матрицы, перемешивающей базисные состоя-

ния $|00\rangle$ и $|11\rangle$. Заметим, что процедура построения этих схем отличается от предыдущего рецепта дополнительным преобразованием, которое выравнивает значения одного из битов, делая тем самым возможным применение однокубитовой операции $\hat{U}$.

Можно показать (см. задачу 4 в конце этого раздела), что любая унитарная матрица записывается в виде конечного произведения унитарных двухуровневых матриц. С учетом этого свойства утверждение о том, что однокубитовые преобразования и операция CNOT составляют универсальный набор гейтов, является доказанным. Ради аккуратности заметим, что пока мы ограничились двухкубитовыми операциями. Представляется, однако, вполне очевидным, что рецепты построения квантовых схем могут быть обобщены на случай любых мультикубитовых гейтов. Мы вернемся к этому вопросу в разделе 2.6.

Неклонируемость квантовых состояний

Классическую информацию можно неограниченно копировать с помощью процессов, которые не зависят от сути копируемой информации и никак не влияют на нее. Это делает и компьютер, и светокопировальное устройство, да и самая обычная пишущая машинка.

Иначе обстоит дело с квантовой информацией, носителем которой являются кубиты. Свойства квантового копирования являются еще одним примером разительного различия квантовой и классической информации.

Уточним постановку задачи. Пусть имеются две одинаковые по своим физическим свойствам квантовые системы. Одна из них находится в некотором чистом квантовом состоянии, кэт-вектор которого $|\Psi\rangle$ произволен и, в общем случае, нам не известен. Вторая система находится в каком-то известном начальном состоянии $|0\rangle$. Вопрос в том, существует ли для этих квантовых систем какой-нибудь универсальный процесс, который, не меняя состояние первой системы, переводит вторую в состояние $|\Psi\rangle$, т.е. создает копию произвольного квантового состояния. Такой процесс можно

назвать квантовым клонированием. Отрицательный ответ на поставленный вопрос дает теорема о неклонируемости квантовых состояний, которая была сформулирована в 1982 г. Вуттерсом и Зуреком, а также Диксом.

Суть теоремы достаточно проста, и ее можно доказать, исходя из свойств унитарных преобразований двухкубитовой системы. Пусть эта система находится в факторизованном начальном состоянии $|\Psi\rangle|0\rangle$, где кэт-вектор $|\Psi\rangle$ первого кубита подлежит клонированию с помощью некоторого унитарного двухкубитового преобразования $\hat{C}$, т.е.

$$\hat{C}|\Psi\rangle|0\rangle = |\Psi\rangle|\Psi\rangle. \qquad (2.221)$$

Если вспомнить, например, операцию CNOT (2.190), то она производит копирование базисных состояний первого кубита:

$$CNOT|0\rangle|0\rangle = |0\rangle|0\rangle,$$
$$CNOT|1\rangle|0\rangle = |1\rangle|1\rangle.$$

Если же первый кубит находится в произвольном суперпозиционном состоянии $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$, то состояние системы на выходе имеет вид (2.194):

$$CNOT|\Psi\rangle|0\rangle = \alpha|00\rangle + \beta|11\rangle \neq |\Psi\rangle|\Psi\rangle,$$

т.е. оно является перепутанным состоянием двух кубитов, а не факторизованным. Приведенный пример показывает, что копирование с помощью гейта CNOT двух ортогональных состояний $|0\rangle$ и $|1\rangle$ возможно, но при этом неортогональное им состояние $|\Psi\rangle$ клонировать нельзя.

Рассмотрим теперь произвольный оператор клонирования $\hat{C}$. Поскольку он должен копировать любые исходные состояния пер-

вого кубита, то для двух таких состояний $|\Psi\rangle$ и $|\Phi\rangle$ имеем:

$$\begin{aligned}\hat{C}|\Psi\rangle|0\rangle &= |\Psi\rangle|\Psi\rangle,\\ \hat{C}|\Phi\rangle|0\rangle &= |\Phi\rangle|\Phi\rangle.\end{aligned} \tag{2.222}$$

Из условия сохранения скалярного произведения при унитарном преобразовании получаем:

$$\langle\Phi|\Psi\rangle = \left(\langle\Phi|\Psi\rangle\right)^2. \tag{2.223}$$

Поэтому либо

$$\langle\Phi|\Psi\rangle = 0, \tag{2.224}$$

т.е. состояния $|\Psi\rangle$ и $|\Phi\rangle$ ортогональны, либо $\langle\Phi|\Psi\rangle = 1$, что с учетом нормировки дает совершенно неинтересное соотношение

$$|\Psi\rangle = |\Phi\rangle.$$

Таким образом, доказано, что не существует унитарного оператора, который может клонировать два различных неортогональных состояния. Основное содержание утверждения может быть распространено на более общие постановки задачи.

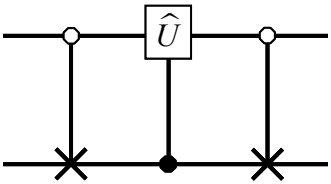
Невозможность клонирования неортогональных квантовых состояний играет ключевую роль в квантовой криптографии. Тот факт, что нельзя получить копию некоторого неизвестного нам произвольного квантового состояния, означает также, что, не разрушив состояние системы, невозможно получить информацию об этом состоянии. Этот аспект теоремы неклонируемости оказывается очень важным для правильной интерпретации результатов измерений перепутанных состояний, которые проводятся разными участниками квантовой коммуникационной схемы.

Задачи

1. Для системы двух кубитов построить квантовые схемы, отвечающие унитарным двухуровневым матрицам, которые перемешивают базисные состояния:

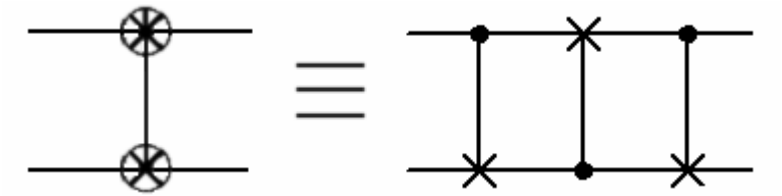
(а) $|00\rangle$ и $|10\rangle$, (б) $|01\rangle$ и $|11\rangle$.

2. Проверить, что квантовая схема



отвечает двухуровневой матрице, которая перемешивает базисные состояния $|00\rangle$ и $|11\rangle$ с помощью унитарной 2×2 подматрицы $\hat{U}$.

3. Показать, что квантовая схема



описывает операцию перестановки кубитов. Сравнить со схемой, показанной на рис. 2.19, если в той положить $\hat{U} = \sigma_1$.

4. Показать, что унитарную матрицу можно представить в виде конечного произведения унитарных двухуровневых матриц.

Решение

Сначала рассмотрим для примера унитарную матрицу 3×3

$$\hat{U}=\begin{pmatrix} a & . & . \\ b & . & . \\ c & . & . \end{pmatrix}.$$

В ней вписаны в явном виде только те элементы, за которыми мы будем следить в процессе дальнейших вычислений. Напомним, что условие унитарности $\hat{U}^{+}\hat{U}=1$ приводит к равенству $|a|^2+|b|^2+|c|^2=1$. Аналогичные равенства имеют место для элементов каждой строки и каждого столбца. Найдем такую унитарную матрицу $\hat{U}_1$, которая удовлетворяет соотношению

$$\hat{U}_1\hat{U}=\begin{pmatrix} a' & . & . \\ 0 & . & . \\ c' & . & . \end{pmatrix}.$$

Решив несложную систему двух линейных алгебраических уравнений, получаем

$$\hat{U}_1=\begin{pmatrix} a^*/d & b^*/d & 0 \\ -b/d & a/d & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

где $d=\sqrt{|a|^2+|b|^2}$. Матрица $\hat{U}_1$ является, очевидно, унитарной и двухуровневой. Вычислив произведение $\hat{U}_1\hat{U}$, находим, что $a'=d$ и $c'=c$, т.е.

$$\hat{U}_1\hat{U}=\begin{pmatrix} d & . & . \\ 0 & . & . \\ c & . & . \end{pmatrix}.$$

Теперь ищем матрицу $\hat{U}_2$, которая удовлетворяет соотношению

$$\hat{U}_2\hat{U}_1\hat{U} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & . & . \\ 0 & . & . \end{pmatrix}.$$

Простые алгебраические вычисления дают следующее выражение для унитарной двухуровневой матрицы $\hat{U}_2$:

$$\hat{U}_2 = \begin{pmatrix} d & 0 & c^* \\ 0 & 0 & 0 \\ -c & 0 & d \end{pmatrix}.$$

Так как $\hat{U}$, $\hat{U}_1$ и $\hat{U}_2$ – унитарные матрицы, то их произведение

$$\hat{U}_2\hat{U}_1\hat{U} = \hat{U}_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & u & w \\ 0 & v & z \end{pmatrix}$$

представляет собой двухуровневую унитарную матрицу $\hat{U}_3$, в которой выделилась унитарная подматрица $\begin{pmatrix} u & w \\ v & z \end{pmatrix}$. После этого исходная матрица $\hat{U}$ окончательно записывается в виде

$$\hat{U} = \hat{U}_1^+\hat{U}_2^+\hat{U}_3$$

произведения трех унитарных двухуровневых матриц, что и требовалось доказать.

Применительно к общему случаю унитарной матрицы $r \times r$ изложенная схема вычислений работает следующим образом.

Сначала умножаем исходную матрицу $\hat{U}$ на $(r-1)$ подходящую двухуровневую матрицу. Элементы каждой матрицы этой последовательности находятся из линейных алгебраических уравнений, которые задаются условием обращения в нуль очередного элемента первого столбца получившегося произведения матриц. В результате получается матрица вида

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \begin{pmatrix} . & . & . \\ . & . & . \\ . & . & . \end{pmatrix}_{r-1} & & \\ \vdots & & & \\ 0 & & & \end{pmatrix}_{r}.$$

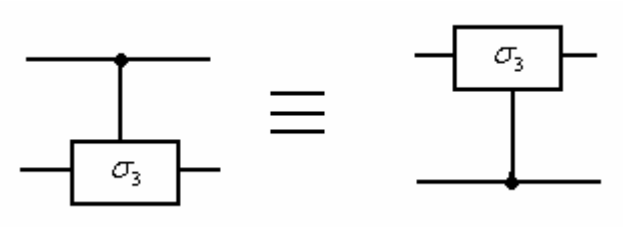
Здесь индексы r и $r-1$ указывают размерности соответствующих матриц. Затем умножаем на такие $(r-2)$ двухуровневые матрицы, чтобы уже в выделенной подматрице с размерностью $(r-1)\times(r-1)$ обратить в нуль все элементы первого столбца, кроме диагонального. Из-за условия унитарности будут равны нулю и соответствующие элементы первой строки. Продолжаем эту процедуру до тех пор, пока все произведение не превратится в двухуровневую матрицу, которая в правом нижнем углу содержит унитарную 2×2 подматрицу, а из остальных элементов отличны от нуля и равны единице только диагональные. Умножая на обратные матрицы, приходим к окончательному выражению для исходной матрицы $\hat{U}$

$$\hat{U} = \hat{V}_1 \hat{V}_2 \cdots \hat{V}_k$$

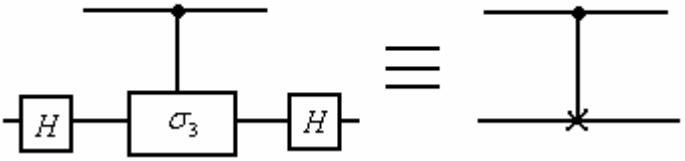
в виде произведения k штук унитарных двухуровневых матриц. Среди этих матриц могут быть единичные, так что $k \le r(r-1)/2$. Унитарные преобразования n-кубитового регистра описываются матрицами $2^n \times 2^n$. Поэтому $d = 2^n$ и $k \le 2^{n-1}\left(2^n - 1\right)$.

5. Доказать эквивалентность квантовых схем:

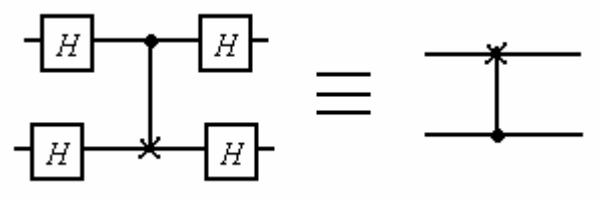
а)



б)



в)



Указание

Случай в) рассмотреть с помощью базисов $\{|0\rangle, |1\rangle\}$ и $\{\frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)\}$.

2.6. Мультикубитовые гейты

Детальное обсуждение двухкубитовых преобразований, проведенное в предыдущем разделе, содержит все необходимое для понимания того, как сделать заключительный шаг и перейти к общему случаю унитарных преобразований в пространстве состояний произвольного *n*-кубитового регистра. Эти вопросы составляют содержание данного раздела.

Сначала для наглядности рассматриваются некоторые конкретные трехкубитовые и более сложные гейты. Они представляют в том числе и самостоятельный интерес, поскольку используются как готовые блоки в архитектуре сложных квантовых схем. Демонстрируется также, каким образом эти гейты можно представить с помощью простейших логических элементов, рассмотренных ранее. Затем формулируется окончательное утверждение об универсальном наборе квантовых гейтов.

Трехкубитовые условные операции

Результаты предыдущего раздела показали, насколько полезной оказывается операция *Controlled U* (обозначим ее, для краткости, с помощью аббревиатуры *CU*) для конструирования произвольных двухкубитовых преобразований. Обобщением этой условной операции на случай трехкубитовых систем является гейт *Controlled Controlled U* (C^2U), показанный на рис. 2.20.

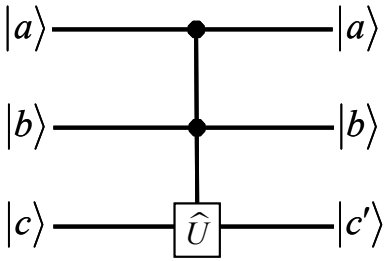


Рис. **2.20**

Теперь есть два управляющих кубита, которым отвечают две верхние линии с темными кружками, и один управляемый кубит, представленный нижней линией с изображением однокубитовой унитарной операции $\hat{U}$.

Гейт C^2U действует таким образом, что управляемый кубит $|c\rangle$ подвергается унитарному преобразованию $\hat{U}$ в том и только том случае, когда оба управляющих кубита находятся в базисном состоянии $|1\rangle$, т.е. $|a\rangle = |1\rangle$ и $|b\rangle = |1\rangle$. Если хотя бы один из управляющих кубитов находится в состоянии $|0\rangle$, то управляемый кубит остается в исходном состоянии. Как обычно, состояния управляющих кубитов во всех случаях остаются неизменными. Из восьми ($2^3 = 8$) базисных векторов трехкубитовой системы операция C^2U перемешивает только два, $|110\rangle$ и $|111\rangle$. Остальные базисные кэт-векторы не меняются. Мы не будем выписывать в явном виде довольно громоздкую 8×8 матрицу гейта C^2U, а просто дадим ее словесное описание. В этой матрице в правом нижнем углу стоит унитарная подматрица $\hat{U} = \begin{pmatrix} u & w \\ v & z \end{pmatrix}$. Что касается остальных элементов, то диагональные равны единице, а недиагональные – нулю.

Покажем, что трехкубитовая условная операция C^2U может быть выражена через несколько двухкубитовых условных гейтов.

Для этого представим $\hat{U}$ в виде

$$\hat{U} = \hat{V}^2 \tag{2.225}$$

квадрата некоторого унитарного оператора $\hat{V}$. Последний, тем самым, равен квадратному корню из $\hat{U}$ и может быть найден в общем виде. Действительно, воспользуемся формулой (2.67), которая выражает произвольный унитарный оператор $\hat{U}$ через матрицу

конечных вращений $\hat{R}(\Phi,\vec{n})$, т.е.

$$\hat{U} = e^{i\alpha}\ \hat{R}\left(\Phi,\vec{n}\right) = e^{i\,\alpha} e^{i\frac{\Phi}{2}\vec{n}\vec{\sigma}}.$$

Тогда

$$\hat{V} = \left(\hat{U}\right)^{1/2} = e^{i\frac{\alpha}{2}} e^{i\frac{\Phi}{4}\vec{n}\vec{\sigma}} = e^{i\frac{\alpha}{2}}\ \hat{R}\left(\frac{\Phi}{2},\vec{n}\right). \qquad (2.226)$$

С помощью двухкубитовых условных операций CNOT, CV и CV^+ квантовая схема гейта C^2U может быть представлена в виде

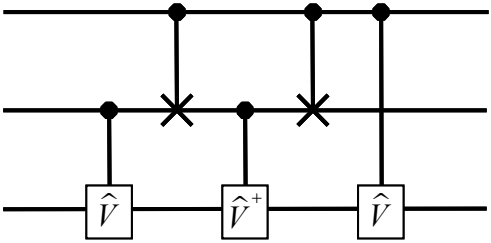


Рис. **2.21**

Проверим, что это схема действительно описывает операцию C^2U и эквивалентна той, что изображена на рис. 2.20. Пусть состояние на входе имеет вид $|1\rangle|1\rangle|c\rangle$, т.е. оба управляющих кубита находятся в базисном состоянии $|1\rangle$, а состояние управляемого кубита есть $|c\rangle$. Сначала CV переводит управляемый кубит в состояние $\hat{V}|c\rangle$. Последующая операция CNOT меняет состояние второго кубита $|1\rangle \to |0\rangle$, и он не воздействует на управляемый кубит, т.е. операции $\hat{V}^+$ нет. Следующий гейт CNOT возвращает второй ку-

бит в исходное состояние $|1\rangle$, а CV переводит управляемый кубит из состояния $\hat{V}|c\rangle$ в $\hat{V}^2|c\rangle = \hat{U}|c\rangle$. Таким образом, цепочка преобразований

$$\begin{aligned} |11\rangle|c\rangle \to |11\rangle\left(\hat{V}|c\rangle\right) \to |10\rangle\left(\hat{V}|c\rangle\right) \to \\ \to |11\rangle\left(\hat{V}|c\rangle\right) \to |11\rangle\left(\hat{V}^2|c\rangle\right) = |11\rangle\left(\hat{U}|c\rangle\right) \end{aligned} \quad (2.227)$$

дает результат действия операции C^2U. Проведем еще одну контрольную проверку, например, для начального состояния $|10\rangle|c\rangle$. Поскольку второй кубит в состоянии $|0\rangle$, то первый оператор $\hat{V}$ на управляемый кубит не действует. Гейт CNOT меняет состояние второго кубита $|0\rangle \to |1\rangle$, и на управляемый кубит действует оператор $\hat{V}^+$, т.е. $|c\rangle \to \hat{V}^+|c\rangle$. Еще один гейт CNOT возвращает второй кубит в исходное состояние $|0\rangle$, а операция CV подвергает состояние управляемого кубита преобразованию $\hat{V}$, т.е. $\hat{V}^+|c\rangle \to \hat{V}\hat{V}^+|c\rangle = |c\rangle$. Поэтому данная цепочка преобразований

$$\begin{aligned} |10\rangle|c\rangle \to |11\rangle|c\rangle \to |11\rangle\left(\hat{V}^+|c\rangle\right) \to \\ \to |10\rangle\left(\hat{V}^+|c\rangle\right) \to |10\rangle\left(\hat{V}\hat{V}^+|c\rangle\right) = |10\rangle|c\rangle \end{aligned} \quad (2.228)$$

не меняет состояние системы, как и должно быть согласно операции C^2U в том случае, когда один из управляющих кубитов сначала был в состоянии $|0\rangle$. Аналогичным образом проверяются и все остальные варианты начального состояния системы.

Как было показано в предыдущем разделе, все двухкубитовые операции могут быть представлены с помощью однокубитовых преобразований и фундаментального гейта CNOT. С учетом квантовой схемы, представленной на рис. 2.21, данное утверждение справедливо и для трехкубитового гейта *Controlled Controlled U*.

Гейт Тоффоли

Рассмотрим специальный случай преобразования C^2U, когда $\hat{U} = \sigma_1$ является однокубитовым гейтом NOT. Преобразование *Controlled Controlled NOT* (C^2NOT) называется *Тоффоли-гейтом* и изображается схемой, представленной на рис. 2.22.

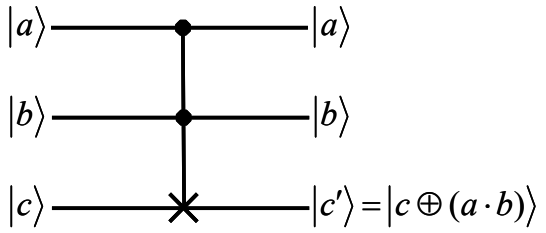


Рис. **2.22**

Эта операция действует таким образом, что управляемый кубит $|c\rangle$ испытывает операцию NOT только в том случае, когда оба управляющих кубита $|a\rangle$ и $|b\rangle$ находятся в состоянии $|1\rangle$. В остальных случаях состояние $|c\rangle$ не меняется.

С точки зрения квантовых вычислений, гейт Тоффоли осуществляет с битами *a*, *b* и *c* операцию

$$c \oplus (a \cdot b), \tag{2.229}$$

результат которой записан в выходном состоянии управляемого регистра $|c'\rangle = |c \oplus (a \cdot b)\rangle$. Символ $\oplus$, как уже говорилось, означает сложение по модулю 2. Это классический логический элемент (см. книгу 1) *XOR* (*исключающее ИЛИ*). Символ $a \cdot b$ обозначает произведение битов *a* и *b* и соответствует классическому логическому элементу *AND* (*И*). Из (2.229) видно, что если либо *a*, либо *b*,

либо оба бита равны нулю, то $c \oplus \left(a \cdot b \right) = c$. Если же $a = b = 1$, то $c \oplus \left(a \cdot b \right) = c \oplus 1 = \overline{c}$, где $\overline{c}$ есть *НЕ c*, т.е. $\overline{c} = 1$ для $c = 0$ и $\overline{c} = 0$ для $c = 1$.

Заметим, что в классических вычислениях элемент Тоффоли является универсальным обратимым гейтом, с помощью которого можно моделировать все необходимые логические элементы. Что же касается квантового гейта Тоффоли, то в соответствии с общей схемой, представленной на рис. 2.21, он сводится к некоторому набору двухкубитовых операций. Так как $\hat{U} = \sigma_1$, то в эту схему входит оператор

$$\hat{V} = \sqrt{\sigma_1} = \exp\left(-i\pi/4 \right) \frac{1 + i\sigma_1}{\sqrt{2}} = \exp\left[i \frac{\pi}{4} \left(\sigma_1 - 1 \right) \right]. \quad (2.230)$$

Непосредственным умножением можно убедиться, что $\hat{V}^2 = \sigma_1$ (см. также задачу 13 в конце раздела 2.2).

Трехкубитовый гейт Тоффоли оказывается очень полезным и удобным элементом при конструировании квантовых схем. При этом используются и модифицированные формы гейта Тоффоли, например такие, которые показаны на рис. 2.23 вместе с эквивалентными схемами.

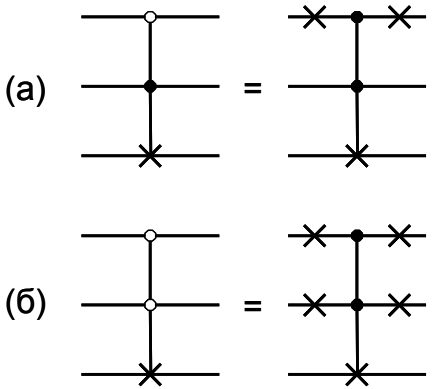
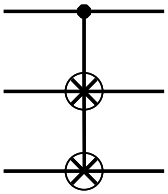


Рис. **2.23**

Для схемы (а) управляемый кубит проходит через операцию NOT, когда управляющие кубиты находятся в состоянии $|10\rangle$, а в случае (б) это происходит для управляющих кубитов в состоянии $|00\rangle$.

Приведем два примера использования гейта Тоффоли как элемента квантовых схем.

Рассмотрим трехкубитовое унитарное преобразование, которое перемешивает с помощью подматрицы σ_1 только два базисных состояния системы, $|101\rangle$ и $|110\rangle$, а остальные базисные векторы не меняются. Эта операция называется управляемым обменом, или элементом Фредкина. Квантовую схему такого преобразования будем изображать в виде

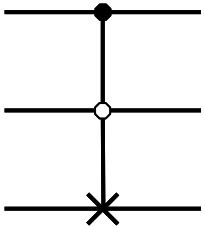


Соединенными между собой знаками $\otimes$ на линиях второго и третьего кубитов обозначена операция обмена значениями битов, которая происходит, если первый (управляющий) кубит находится в состоянии $|1\rangle$. Поскольку элемент Фредкина перемешивает только два базисных состояния, он представляет собой двухуровневое преобразование, о которых мы говорили в предыдущем разделе, и описывается двухуровневой матрицей. В данном случае эта 8×8 матрица имеет вид

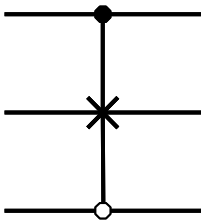
$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

а пунктиром выделена подматрица σ_1. Явный вид столь громоздкой матрицы нам не нужен, а приведен он здесь только для полноты картины.

Идея конструктивного построения квантовой схемы уже была изложена в предыдущем разделе. Перемешиваемые состояния $|101\rangle$ и $|110\rangle$ отличаются значениями двух битов – второго и третьего. Чтобы эффективно использовать подматрицу σ_1 как однокубитовый гейт, надо выровнять значения одного из этих битов, например третьего. С этой целью поменяем местами состояние $|101\rangle$ и $|100\rangle$, что делается с помощью модифицированного Тоффоли-гейта



Далее в состояниях $|100\rangle$ и $|110\rangle$ применяем операцию NOT ко второму кубиту при фиксированных состояниях первого и третьего кубитов. Это делается опять с помощью Тоффоли-гейта вида



Возвращение на место переставленных состояний осуществляется тем же Тоффоли-гейтом, который применялся на первом шаге, так как Тоффоли-гейт совпадает со своим обратным. Таким образом, вся схема элемента Фредкина может быть представлена с помощью

трех гейтов Тоффоли, как это было описано выше и показано в середине рис. 2.24.

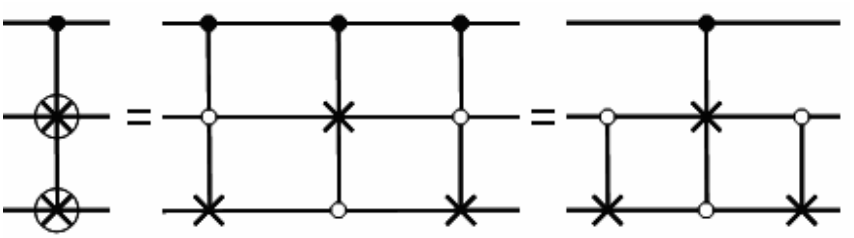


Рис. **2.24**

Справа на рис. 2.24 показана эквивалентная схема, в которой первый и третий Тоффоли-гейты заменены двухкубитовыми операциями $\widetilde{CNOT}$. Проверка правильности действия этих схем предоставляется читателю.

Второй пример демонстрирует применение Тоффоли-гейта для построения квантовой схемы условной операции U с произвольным числом управляющих кубитов, т.е. гейта C^nU.

Пусть, для простоты рассуждений, число управляющих кубитов n=3. Нас интересует условная операция такая, что управляемый кубит подвергается воздействию унитарного однокубитового оператора $\hat{U}$, когда все управляющие кубиты находятся в состоянии $|1\rangle$. В других случаях состояние управляемого кубита не меняется.

В квантовой схеме, показанной на рис. 2.25, три верхние линии отвечают управляющим кубитам, которые находятся в начальных состояниях $|a\rangle$, $|b\rangle$ и $|c\rangle$. Далее нарисованы линии двух вспомогательных кубитов, находящихся сначала в состоянии $|0\rangle$. Наконец, последняя линия изображает управляемый кубит $|d\rangle$.

После первого гейта Тоффоли, согласно (2.229), состояние первого вспомогательного кубита, который является управляемым, принимает вид $|0 \oplus (a \cdot b)\rangle = |a \cdot b\rangle$.

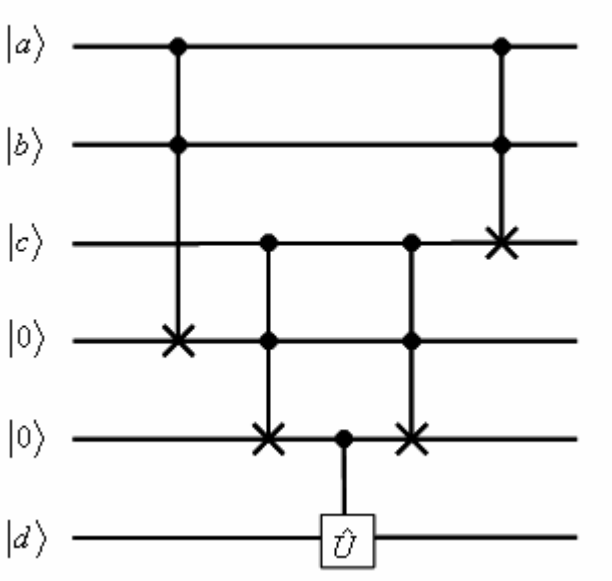


Рис. **2.25**

Следующий Тоффоли гейт сделает состояние второго вспомогательного кубита равным $\left|0 \oplus (a \cdot b \cdot c)\right\rangle = \left|a \cdot b \cdot c\right\rangle$. Это будет состояние $\left|1\right\rangle$ тогда и только тогда, когда $a = b = c = 1$. Второй вспомогательный кубит является управляющим для двухкубитовой операции CU над интересующим нас управляемым кубитом $\left|d\right\rangle$. Поэтому, если $\left|a \cdot b \cdot c\right\rangle = \left|1\right\rangle$, то $\left|d\right\rangle \to \hat{U}\left|d\right\rangle$. Если же $\left|a \cdot b \cdot c\right\rangle = \left|0\right\rangle$, то $\left|d\right\rangle$ не изменится. В этом и состоит операция C^3U. Два Тоффоли-гейта в правой части схемы возвращают вспомогательные кубиты в исходное состояние. В принципе, это нужно делать, так как вспомогательные кубиты могут быть использованы для других действий до или после рассмотренной нами операции.

Условные операции с несколькими управляемыми кубитами описываются схемами вида

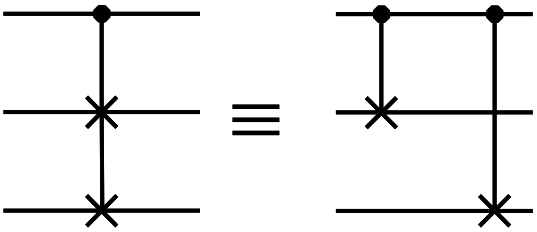


Рис. **2.26**

Здесь операция CNOT применяется ко второму и третьему кубитам.

Универсальный набор гейтов

Вернемся к общей постановке вопроса об универсальном наборе гейтов, с помощью которых можно описать любую унитарную операцию в пространстве состояний *n*-кубитового регистра.

Как уже говорилось, любую унитарную матрицу можно представить в виде конечного произведения двухуровневых матриц. Формальное доказательство этого свойства приведено в задаче 4 в конце раздела 2.5. Поэтому достаточно рассмотреть произвольную унитарную двухуровневую $2^n \times 2^n$ матрицу $\hat{M}$, которая существенно перемешивает только два базисных вектора

$$\left|s\right\rangle \equiv \left|s_{n-1}s_{n-2}...s_0\right\rangle \text{ и } \left|t\right\rangle \equiv \left|t_{n-1}t_{n-2}...t_0\right\rangle \qquad (2.231)$$

n-кубитовой системы с помощью унитарной подматрицы $\hat{U} = \begin{pmatrix} u & w \\ v & z \end{pmatrix}$ и не затрагивает остальную часть базиса. Как обычно, $\left(s_{n-1}s_{n-2}...s_0\right)$ и $\left(t_{n-1}t_{n-2}...t_0\right)$ есть двоичные записи чисел *s* и *t*, которые нумеруют базисные векторы. Пусть, для определенности, $s < t$.

Тогда матрица $\hat{M}$ имеет вид

$$\hat{M} = \begin{array}{c} \\ \\ \\ \\ s \\ \\ \\ \\ t \\ \\ \\ \\ \end{array} \begin{array}{c} \begin{array}{cccccccccc} & & & s & & & & t & & \end{array} \\ \begin{pmatrix} 1 & & & \vdots & & & & \vdots & & & \\ & \ddots & & \vdots & & 0 & & \vdots & & 0 & \\ & & 1 & 0 & & & & 0 & & & \\ \cdots & \cdots & 0 & u & 0 & \cdots & 0 & w & 0 & \cdots & \\ & & & 0 & 1 & & & 0 & & & \\ & 0 & & \vdots & & \ddots & & \vdots & & 0 & \\ & & & 0 & & & 1 & 0 & & & \\ \cdots & \cdots & 0 & v & 0 & \cdots & 0 & z & 0 & \cdots & \\ & & & \vdots & & & & 0 & 1 & & \\ & 0 & & \vdots & & 0 & & \vdots & & \ddots & \\ & & & \vdots & & & & \vdots & & & 1 \end{pmatrix} \end{array} . \quad (2.232)$$

Номера строк и столбцов, на которых располагаются элементы 2×2 матрицы $\hat{U}$, отмечены числами (*s*) и (*t*). В общем случае состояния $|s\rangle$ и $|t\rangle$ отличаются значениями нескольких битов. Для того чтобы применить оператор $\hat{U}$ как однокубитовое преобразование, надо чтобы перемешиваемые состояния отличались значением только одного бита. Для этого можно последовательно переставлять вектор $|s\rangle$ с другими базисными векторами до тех пор, пока все значения его битов, кроме одного, не выровняются с $|t\rangle$. На каждом шаге последовательности перестановок меняется значение только одного бита. Поэтому такое преобразование реализуется с помощью гейтов условных операций типа $C^k NOT$. Те кубиты, которые не меняются, являются управляющими. Тот кубит, значение которого надо изменить, является управляемым, и он проходит через операцию NOT. Цепочка преобразований, в ходе которых каждое следующее двоичное число отличается от преды-

дущего в одном двоичном знаке, называется кодом Грея. Приведем пример такой цепочки преобразований. Пусть нам нужно перейти от $|101001\rangle$ к $|110011\rangle$. Тогда код Грея выглядит так

$$\begin{aligned} |g_1\rangle &= |101001\rangle, \\ |g_2\rangle &= |101011\rangle, \\ |g_3\rangle &= |100011\rangle, \\ |g_4\rangle &= |110011\rangle. \end{aligned} \tag{2.233}$$

После перестановок $|s\rangle$ переходит в $|\tilde{s}\rangle$, и двоичная запись числа $\tilde{s}$ отличается от t в одном двоичном знаке. Применяя далее преобразование типа $C^k U$, совершаем необходимое перемешивание состояний с помощью унитарной однокубитовой матрицы $\hat{U}$. После этого все переставленные состояния надо вернуть на место с помощью таких же гейтов $C^k NOT$, которые использовались на первом этапе. Они, как известно, обратимые, Надо только применять их в обратном порядке.

Поясним эту процедуру на примере трехкубитовой системы. Пусть двухуровневая унитарная 8×8 матрица перемешивает состояния $|000\rangle$ и $|111\rangle$, т.е. имеет вид

$$\begin{pmatrix} u & 0 & 0 & 0 & 0 & 0 & 0 & w \\ 0 & 1 & 0 & & & & & 0 \\ 0 & 0 & 1 & & & & & 0 \\ 0 & & & \ddots & & & & 0 \\ 0 & & & & \ddots & & & 0 \\ 0 & & & & & 1 & 0 & 0 \\ 0 & & & & & 0 & 1 & 0 \\ v & 0 & 0 & 0 & 0 & 0 & 0 & z \end{pmatrix}.$$

Перестановка состояний в соответствии с кодом Грея имеет

вид $|000\rangle \to |001\rangle \to |011\rangle$ и реализуется с помощью двух Тоффоли-гейтов. В результате состояния $|011\rangle$ и $|111\rangle$ отличаются значением одного бита и могут быть перемешаны с помощью операции C^2U. При этом второй и третий кубиты являются управляющими, а управляемый первый кубит подвергается однокубитовому унитарному преобразованию $\hat{U} = \begin{pmatrix} u & w \\ v & z \end{pmatrix}$. Квантовая схема изображена на рис. 2.27

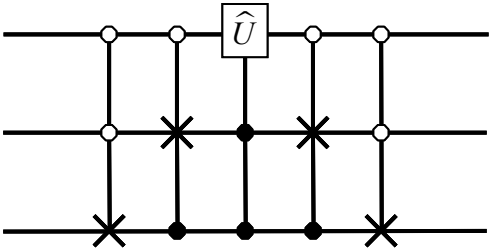


Рис. **2.27**

Мы видим, таким образом, что матрица $\hat{M}$ может быть выражена с помощью операций $C^k NOT$ и $C^k U$. Сами же эти операции могут быть записаны, как мы знаем из предыдущего раздела, с помощью однокубитовых преобразований и двухкубитового гейта CNOT, которые, тем самым, составляют универсальный набор гейтов (*Ди Винченцо*, 1995 г.). Тот факт, что нужен только один двухкубитовый гейт и не нужны никакие специальные многокубитовые гейты, очень важен. Формальные математические унитарные преобразования наполняются содержанием по мере их физической реализации на основе того или иного гамильтониана. Если были бы нужны сложные гамильтонианы с произвольными многочастичными взаимодействиями, то о перспективах квантовых вычислений даже с небольшим числом кубитов было бы вообще трудно говорить.

Оценим число универсальных логических гейтов – однокубитовых и CNOT элементов, необходимых для реализации унитарной операции общего вида в пространстве состояний *n*-кубитового регистра.

Напомним, что произвольную унитарную матрицу $2^n \times 2^n$ можно представить в виде произведения порядка 2^{2n} двухуровневых матриц (см. задачу 4 в конце раздела 2.5). Далее, двухуровневое унитарное преобразование осуществляется, как было показано выше, с помощью многокубитовых условных операций $C^k NOT$ и $C^k U$. При $k \sim n$ требуется порядка $2n$ таких операций. Каждую указанную многокубитовую условную операцию можно осуществить с помощью порядка n однокубитовых преобразований и гейтов CNOT. Перемножая все эти числа, получаем окончательную оценку, что требуемое количество универсальных логических гейтов составляет величину порядка $n^2 2^{2n}$. При больших n это экспоненциально большая величина. В принципе, есть задачи, которые могли бы потребовать столь большого ресурса, если их решать, идя «напролом». Преодоление этих трудностей есть проблема поиска быстрых квантовых алгоритмов.

Классические и квантовые вычисления

Употребляя термин «квантовая информация», мы фактически отождествляем ее с понятием квантового состояния n-кубитового регистра, которое описывается абстрактным кэт-вектором гильбертова пространства. Взаимодействие кубитов с внешними полями, либо между собой, либо с другой физической системой приводит к изменению квантового состояния, в результате чего квантовая информация модифицируется. В условиях унитарной эволюции квантовая информация не теряется. Поскольку в реальных физических системах есть много причин, нарушающих унитарную эволюцию, первостепенное значение имеет разработка методов, минимизирующих такие нарушения, а также способов контролировать и исправлять возникающие ошибки.

Основные логические операции над кубитами могут быть реализованы с помощью тех или иных физических механизмов. В разделе 2.2 мы обсудили этот вопрос применительно к однокубитовым операциям. Реализация гейта CNOT будет рассмотрена в главе 4.

Проанализированные выше примеры квантовых схем показывают, что с их помощью можно, в принципе, контролируемым

образом манипулировать квантовой информацией. О таких процессах принято говорить как о *квантовых вычислениях*, а устройство, их выполняющее, будем называть *квантовым вычислителем*.

По сравнению с классическими вычислениями процессы манипулирования квантовой информацией содержат в себе принципиально новое качество. Мы уже отмечали выше такие факторы как экспоненциально большую емкость многокубитового квантового регистра, возможность квантового параллельного вычисления, а также, например, несовместимую с классическими представлениями степень корреляции в перепутанных квантовых состояниях. При этом вполне естественным представляется желание, приобретая что-то новое, не потерять то лучшее, что было наработано в прежнем. Другими словами, нас интересует, могут ли квантовые схемы воспроизводить классические логические элементы.

Напомним элементарные логические элементы, которые используются в классических вычислительных схемах(см. книгу 1). Это однобитовый элемент NOT (*НЕ*), который инвертирует значение бита, $a \to \overline{a}$ (*НЕ a*). Есть целый ряд нужных двухбитовых элементов, которые переводят два входных бита a и b в один выходной c. Вот некоторые из них. Элемент *AND* (*И*) выдает 1 тогда и только тогда, когда оба входных бита равны 1, т.е. $a,b \to c = a \cdot b$. Операция *XOR* (*исключающее ИЛИ*) складывает входные биты по модулю 2, что обозначается как $a \oplus b$, т.е. $a,b \to c = a \oplus b$. Важную роль играет операция *NAND* (сокращении от *NOT-AND*, *НЕ-И*), которая сначала выполняет над входными битами преобразование *AND*, а потом инвертирует получившийся бит, т.е. $a,b \to \overline{a \cdot b}$. Таблица истинности для этой операции выглядит так

ВХОД			AND	ВЫХОД
a	b		$a \cdot b$	$c' = \overline{a \cdot b}$
0	0		0	1
0	1		0	1
1	0		0	1
1	1		1	0

Рис. **2.28**

Если один из входных битов равен 1, то результатом операции является обращение второго бита. Так, если $a = 1$, то $c' = \overline{a \cdot b} = \overline{b}$, если же $b = 1$, то $c' = \overline{a \cdot b} = \overline{a}$. В классике, конечно, можно получить копию бита. Операция копирования называется *FANOUT*.

Имеет место важное утверждение, что с помощью элементов *NAND* и с учетом возможности копирования можно реализовать любые классические логические элементы, т.е. выполнить вычисления любой функции битов.

Операция NOT является обратимой, так как по результату на выходе однозначно восстанавливается значение входного бита. Что же касается упомянутых выше двухбитовых операций *AND*, *XOR*, *NAND*, то они, очевидно, необратимые, поскольку по значению одного выходного бита нельзя восстановить значения двух входных битов. Какая-то информация оказалась утерянной. В этом смысле формальное свойство необратимости операций эквивалентно потере некоторой информации, которую нельзя восстановить, зная только результат операции. Аналогичная потеря информации происходит, например, если просто стереть значение бита. Такую операцию называют примитивным стиранием (примитивный *ERASE*-гейт).

Пусть одиночный бит представлен как пара равновероятных классических состояний некоторой частицы. Если информация о значении бита оказывается уничтоженной (стертой), то это означает, что объем фазового пространства состояний частицы уменьшился в 2 раза. С точки зрения термодинамики, уменьшение объема фазового пространства системы приводит к уменьшению ее статистической энтропии на величину $k_Б \ln 2$, где постоянная Больцмана $k_Б$ связана с единицами, в которых измеряется энтропия[1]. Если в нашей системе, которая находится вместе с окружающей средой при температуре T, происходит адиабатический процесс возвращения объема фазового пространства к исходному значению, то это приведет к выделению в окружающую среду количе-

[1] В теоретической физике энтропия часто измеряется в единицах энергии, и коэффициент $k_Б$ отсутствует.

ства теплоты $k_Б T \ln 2$. В более общем случае можно сказать, что при стирании компьютером одного бита информации энтропия окружающей среды возрастает не менее, чем на $k_Б \ln 2$, т.е. в среду диссипирует энергия $\geq k_Б T \ln 2$. Это утверждение называется принципом Ландауэра и было сформулировано им в 1961 г.

Приведенное выше максимально упрощенное рассуждение призвано лишь проиллюстрировать истоки связи между диссипацией энергии и информацией. С принципом Ландауэра связано современное понимание этого вопроса, который восходит к идее демона Максвелла, сформулированной в 1871 г.

Столь пространное обращение к вопросу о необратимости классических логических элементов объясняется тем фактом, что квантовые гейты представляют собой унитарные преобразования, которые безусловно обратимы. Поэтому применимость квантовых схем для воспроизведения классических операций требует дальнейшего анализа.

Ключевым моментом является тот факт, что любой классический элемент можно представить с помощью схемы, содержащей только обратимые операции (*Тоффоли Т.*, 1980 г.). Другими словами, принципиально возможно проводить универсальные вычисления без потери информации. Для наших целей наиболее удобным способом построения обратимых операций является классический элемент Тоффоли.

Действие квантового элемента Тоффоли в системе трех кубитов подробно описано в этом разделе ранее. Поэтому сейчас достаточно кратко напомнить это описание, но уже применительно к классическому регистру, содержащему три бита – два управляющих (*a* и *b*) и один управляемый (*c*), который проходит через операцию NOT, если только $a = b = 1$, т.е. $a, b, c \to a, b, c' = c \oplus (a \cdot b)$. Из алгебры операций следует, что двукратное применение элемента Тоффоли возвращает биты в исходное состояние. Действительно, $a, b, c \to a, b, c \oplus (a \cdot b) \to a, b, c \oplus (a \cdot b) \oplus (a \cdot b) = a, b, c$. Это доказывает обратимость элемента Тоффоли, который совпадает со своим обратным.

Схема, представленная на рис. 2.29, показывает, что логическая операция *NAND* реализуется при помощи элемента Тоффоли, если

третий бит первоначально установлен в состоянии 1.

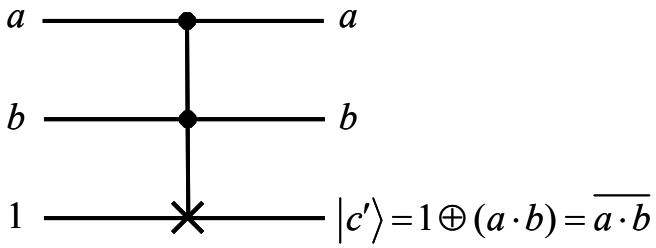


Рис. **2.29**

Два верхних бита являются входными для операции *NAND*, а третий бит описывает выход. Результат совпадает с описанием действия операции *NAND* (см. рис. 2.28). Следует подчеркнуть, что сохранение на выходе начальных значений битов *a* и *b* обеспечивает, в отличие от стандартного элемента *NAND*, обратимость. Информация не теряется.

Для универсального набора элементов нужна еще операция *FANOUT*. На рис. 2.30 показана ее реализация на основе элемента Тоффоли.

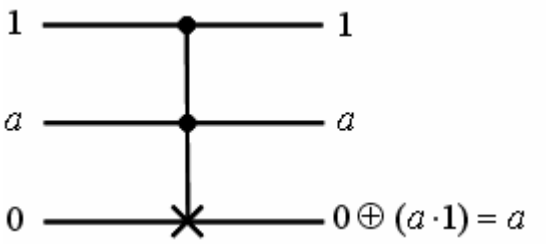


Рис. **2.30**

Второй бит является входным для операции *FANOUT*. Выход описывается вторым и третьим битами, которые теперь дают два таких же бита как и входной.

Поскольку квантовый элемент Тоффоли меняет базисные состояния $|a\rangle|b\rangle|c\rangle$ трехкубитового регистра точно таким же образом, как это делает со значениями битов классический элемент Тоффоли, квантовый вычислитель может выполнить любые вы-

числительные операции, возможные на классическом компьютере. Это означает, в том числе, что для квантовых вычислений можно использовать, если нужно, все алгоритмы, разработанные для классических устройств. В этом результате нет ничего неожиданного.

В разделе 2.3, говоря о квантовом параллелизме, мы вынесли за рамки обсуждения вопрос о том, как сконструировать унитарное преобразование $\hat{U}_f$, осуществляющее вычисление функции $f(x)$, аргумент которой представляет двоичную запись числа x. Теперь можно ответить на этот вопрос следующим образом.

Возьмем такую классическую схему вычисления функции битов $f(x)$, в которой все универсальные логические элементы представлены с помощью классического обратимого элемента Тоффоли. Тогда аналогичная схема с квантовыми элементами Тоффоли будет осуществлять интересующее нас унитарное преобразование $\hat{U}_f$. На рис. 2.31 эта операция изображена в виде блока, у которого есть два входа и два выхода. Операция $\hat{U}_f$ действует на квантовом регистре $|x\rangle|0\rangle$, состоящем из двух регистров $|x\rangle$ и $|0\rangle$. Первый из них есть регистр данных, в котором представлены состояния, изображающие числа x. Второй регистр, первоначально находящийся в состоянии $|0\rangle$, называется регистром значений, и в него записываются числа $f(x)$ в двоичном представлении. Действие $\hat{U}_f$ на базисные состояния $|x\rangle|0\rangle$ имеет вид

$$\hat{U}_f|x\rangle|0\rangle = |x\rangle|f(x)\rangle. \qquad (2.234)$$

Если n-кубитовый регистр данных первоначально находится в состоянии (2.143)

$$|\Psi_0\rangle = 2^{-\frac{n}{2}}\sum_{x=0}^{2^n-1}|x\rangle, \qquad (2.235)$$

то состояние системы на выходе описывается кэт-вектором

$$|out\rangle = \hat{U}_f|\Psi_0\rangle|0\rangle = 2^{-n/2}\sum_{x=0}^{2^n-1}|x\rangle|f(x)\rangle, \qquad (2.236)$$

в котором, как уже говорилось, представлены значения функции $f(x)$ для всех значений аргумента x. На рис. 2.31 мы показали эту ситуацию, опустив для краткости нормировочный коэффициент $2^{-n/2}$.

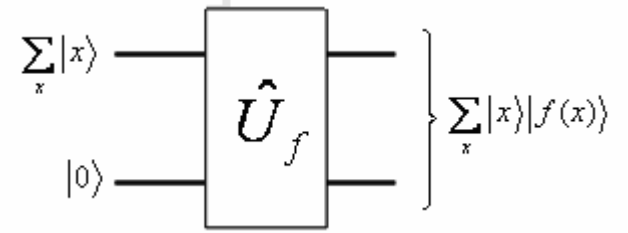


Рис. **2.31**

Прежде всего, обратим внимание, что $|out\rangle$ является перепутанным состоянием двух регистров. Кроме того, состояние системы на выходе содержит информацию обо всех значениях функции $f(x)$. В такой информации проявляются глобальные свойства функции, например, периодичность и тому подобное. Такие свойства, как мы увидим в следующей главе, играют важную роль в целом ряде квантовых алгоритмов, которые демонстрируют, что с помощью квантовых вычислений можно превзойти возможности классических вычислительных схем.

Список используемой литературы (источники)

1. Ландау Л.Д., Лифшиц Е.М. Квантовая механика. Нерелятивистская теория. — М.: Наука, 2006.
2. Мессиа А. Квантовая механика. Т. 1. — М.: Наука, 1979.
3. Боум А. Квантовая механика. Основы и приложения. — М.: Мир, 1990.
4. Стин Э. Квантовые вычисления. – Ижевск: НИЦ «Регулярная и хаотическая динамика», 2000.
5. Квантовые вычисления: За и против. – Ижевск: Издательский дом «Удмуртский университет», 1999.
6. Квантовый компьютер и квантовые вычисления. – Ижевск: Ижевская республиканская типография, 1999.
7. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация /Пер. с англ. – М.: Мир, 2006.

«*Квантовый параллелизм* — это фундаментальное свойство многих квантовых алгоритмов.»

М. Нильсен, И. Чанг

Квантовые алгоритмы

Г л а в а 3

КВАНТОВЫЕ АЛГОРИТМЫ

Содержание

Задача Дойча. Алгоритм квантового поиска. Квантовый алгоритм Шора. Корреляции ЭПР–Белла в квантовых коммуникационных схемах.

Современный статус теории квантовой информации вообще и квантовых вычислений в частности в значительной степени определяется тем фактом, что известен целый ряд трудных задач, которые можно решить с помощью квантовых методов вычислений гораздо эффективнее, чем это способен сделать любой классический компьютер. В этой главе рассматриваются такие важные квантовые алгоритмы как алгоритм Дойча-Джозса, алгоритм квантового поиска Гровера и алгоритм факторизации Шора, которые особенно ярко демонстрируют разницу между возможностями классических и квантовых вычислений. Открытие этих алгоритмов явилось мощным стимулирующим импульсом к развитию всей области квантовых вычислений. В заключительном разделе данной главы рассматриваются удивительные свойства некоторых квантовых коммуникационных процессов, связанных с передачей квантовой информации. Эти свойства обусловлены несовместимой с классическими представлениями высокой степенью квантовых корреляций между подсистемами в перепутанных квантовых состояниях. Обсуждаются протоколы квантовой плотной кодировки, квантового распределения ключа и процесс квантовой телепортации.

3.1. Задача Дойча

В 1985 г. *Давид Дойч* предложил простой алгоритм, чтобы продемонстрировать потенциальные возможности квантового параллельного вычисления.

Пусть имеется некоторое устройство, на вход которого подается число x, а оно вычисляет функцию $f(x)$ и выдает ее значение на выходе. Такое устройство называется «черным ящиком» или «оракулом». Нас интересует, можно ли, приготовив входные данные и узнав результат на выходе, выяснить, что делает «черный ящик»?

Задача Дойча, как ее называют, формализует эту проблему следующим образом. Пусть функция f имеет однобитовую область определения, x=0,1, и однобитовую область значений, $f(x)$=0,1. Другими словами, $f(x)$ отражает один бит в один бит, $\{0,1\} \to \{0,1\}$. Четыре возможные комбинации входных и выходных значений можно разделить на две группы, которые характеризуются разными глобальными свойствами функции $f(x)$. Для двух комбинаций $f(0)=f(1)$, и функция $f(x)$ является постоянной. Для двух оставшихся комбинаций $f(0) \neq f(1)$, и такую функцию называют сбалансированной. Спрашивается, сколько раз надо обратиться к «оракулу», чтобы узнать указанное глобальное свойство вычисляемой функции?

Если на входе и выходе имеются классические биты, то ответ очевиден – необходимо обратиться к «оракулу» дважды, получить значения $f(0)$ и $f(1)$, а затем сравнить их. Для квантового «оракула», который вычисляет функцию $f(x)$ обратимым образом с помощью некоторого унитарного преобразования $\widehat{U}_f$, действующего на состояния кубитов, ситуация совершенно другая. Как показывает алгоритм Дойча, ответ можно получить, обратившись к «оракулу» только один раз.

Алгоритм Дойча

Поскольку сама функция $f(x)$ может быть, вообще говоря, необратимой, для обеспечения унитарности преобразования надо сохранять входные данные. Поэтому $\widehat{U}_f$ действует в пространстве состояний двухкубитовой системы, выполняя преобразование:

$$|x\rangle|y\rangle \to \widehat{U}_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle. \qquad (3.1)$$

Здесь первый кубит описывает входные данные, а второй нужен для записи результата. Вычисления сводятся к нахождению величины $f(x)$, которая затем складывается по модулю 2 с начальным значением y второго кубита. Если $f(x)=0$, то второй кубит не

меняется. Если же $f(x)=1$, то значение второго кубита инвертируется. Заметим, что частный случай соотношения (3.1) для $y=0$ совпадает с выражением (2.234), которое уже использовалось ранее.

Если подавать на вход базисные состояния $|0\rangle$ или $|1\rangle$ кубита данных, то ситуация не будет отличаться от классической, так как выходное состояние будет содержать информацию о значении функции только для одного *x*. Идея алгоритма Дойча состоит в том, чтобы состояние на входе было суперпозицией базисных состояний. Схема, реализующая алгоритм Дойча, показана на рис. 3.1.

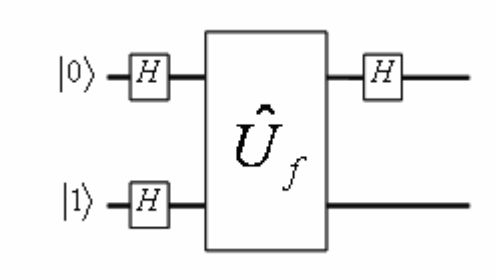


Рис. **3.1**

Первый шаг состоит в том, что стоящие в левой части преобразования Адамара из начального состояния $|0\rangle|1\rangle$ двухкубитовой системы, приготавливают состояние

$$H^{\otimes 2}|0\rangle|1\rangle=\frac{|0\rangle+|1\rangle}{\sqrt{2}}\cdot\frac{|0\rangle-|1\rangle}{\sqrt{2}}=\frac{1}{2}\sum_{x=0,1}|x\rangle\left(|0\rangle-|1\rangle\right). \quad (3.2)$$

На это состояние действует «оракул» $\widehat{U}_f$. Возьмем произвольное слагаемое суммы (3.2) и подействуем оператором $\widehat{U}_f$, используя соотношение (3.1).

Тогда

$$\hat{U}_f |x\rangle\big(|0\rangle - |1\rangle\big) = |x\rangle\big(|f(x)\rangle - |1 \oplus f(x)\rangle\big) = \\ = (-1)^{f(x)} |x\rangle\big(|0\rangle - |1\rangle\big). \tag{3.3}$$

Вся «изюминка» вычислений заключена в последнем шаге, который показывает, что «оракул» не меняет состояние второго кубита, а зависимость от функции $f(x)$ записывается в виде фазового множителя $(-1)^{f(x)}$. Этот результат легко проверить. Действительно, если $f(x) = 0$, то $|x\rangle\big(|f(x)\rangle - |1 \oplus f(x)\rangle\big) = |x\rangle\big(|0\rangle - |1\rangle\big)$. Если $f(x) = 1$, имеем

$$|x\rangle\big(|f(x)\rangle - |1 \oplus f(x)\rangle\big) = |x\rangle\big(|1\rangle - |0\rangle\big) = -|x\rangle\big(|0\rangle - |1\rangle\big).$$

Применяя далее операцию $\widehat{U}_f$ к состоянию (3.2), с учетом (3.3) получаем

$$\widehat{U}_f \frac{1}{2} \sum_{x=0,1} |x\rangle\big(|0\rangle - |1\rangle\big) = \frac{1}{2} \sum_x (-1)^{f(x)} |x\rangle\big(|0\rangle - |1\rangle\big) = \\ = \frac{1}{\sqrt{2}} \Big[(-1)^{f(0)} |0\rangle + (-1)^{f(1)} |1\rangle\Big] \cdot \frac{1}{\sqrt{2}} \big(|0\rangle - |1\rangle\big). \tag{3.4}$$

Это состояние имеет факторизованный вид, и второй кубит можно не рассматривать. Поэтому последнее преобразование Адамара просто меняет состояние первого кубита:

$$H \frac{1}{\sqrt{2}} \Big[(-1)^{f(0)} |0\rangle + (-1)^{f(1)} |1\rangle\Big] = \\ = (-1)^{f(0)} \frac{|0\rangle + |1\rangle}{2} + (-1)^{f(1)} \frac{|0\rangle - |1\rangle}{2} = \\ = \frac{(-1)^{f(0)} + (-1)^{f(1)}}{2} |0\rangle + \frac{(-1)^{f(0)} - (-1)^{f(1)}}{2}. \tag{3.5}$$

Амплитуда состояния $|0\rangle$ отлична от нуля и равна ± 1 тогда и только тогда, когда функция $f(x)$ постоянная, $f(0) = f(1)$. Если же $f(x)$ — сбалансированная функция, то отлична от нуля и равна ± 1 амплитуда состояния $|1\rangle$. Вектор состояния (3.5) можно записать в компактном виде как

$$\pm|f(0) \oplus f(1)\rangle,$$

поскольку два одинаковых значения складываются в нуль, а два разных — в единицу.

Таким образом, обратившись к «оракулу» один раз и измерив конечное состояние первого кубита, мы с достоверностью определим глобальное свойство функции $f(x)$.

Физической причиной является принцип суперпозиции и вытекающий из него квантовый параллелизм вычислений, а также интерференция, которая приводит к когерентному суммированию разных вкладов в амплитуды состояний $|0\rangle$ и $|1\rangle$ первого кубита.

Алгоритм Дойча-Джозса

Задача обобщается на случай произвольного *n*-кубитового регистра данных. Это делается с помощью алгоритма Дойча-Джозса.

«Черный ящик» вычисляет функцию $f(x)$, область определения которой есть все числа *x* от 0 до $2^n - 1$, отвечающие базовым состояниям *n*-кубитового регистра данных.

Область значений есть один бит, т.е. эта функция осуществляет отображение *n* битов в один бит, $\{0,1\}^{\otimes n} \to \{0,1\}$. При этом функция $f(x)$ либо постоянная, т.е. принимает то или иное возможное значение при всех *x*, либо сбалансированная, когда она равна нулю точно для половины значений аргумента и, соответственно, равна 1 для остальной половины. Измерив результат на выходе, мы хотим узнать, является ли f постоянной или сбалансированной.

Схема, решающая проблему Дойча-Джозса, показана на рис. 3.2.

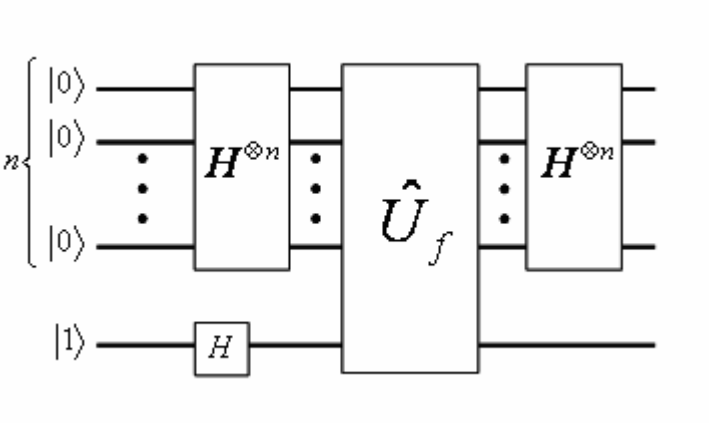


Рис. **3.2**

Она отличается от рис. 3.1 только тем, что регистр данных содержит *n*-кубитов. Начальное состояние $|0\rangle^{\otimes n}|1\rangle$ системы *n*+1 кубита после применения преобразований Адамара принимает вид:

$$H^{\otimes(n+1)}|0\rangle^{\otimes n}|1\rangle = \left(2^{-n/2}\sum_{x=0}^{2^n-1}|x\rangle\right)\frac{1}{\sqrt{2}}\left(|0\rangle-|1\rangle\right). \qquad (3.6)$$

Здесь мы воспользовались, в том числе, формулой (2.143) для *n*-кубитового регистра. Далее на это состояние действует оператор $\widehat{U}_f$. Этот оператор линейный, а его действие на отдельное слагаемое суммы по *x* определяется соотношением (3.3), так как область значений функции $f(x)$, является, как и раньше, однобитовой. Тогда

$$\begin{aligned}&\widehat{U}_f\left(2^{-n/2}\sum_{x=0}^{2^n-1}|x\rangle\right)\frac{1}{\sqrt{2}}\left(|0\rangle-|1\rangle\right) = 2^{-\frac{n+1}{2}}\sum_{x=0}^{2^n-1}\widehat{U}_f|x\rangle\left(|0\rangle-|1\rangle\right) = \\ &= 2^{-n/2}\sum_{x=0}^{2^n-1}(-1)^{f(x)}|x\rangle\frac{1}{\sqrt{2}}\left(|0\rangle-|1\rangle\right) \Rightarrow 2^{-n/2}\sum_{x=0}^{2^n-1}(-1)^{f(x)}|x\rangle.\end{aligned} \qquad (3.7)$$

Поскольку состояние $\frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$ самого последнего, $(n+1)$-го, кубита факторизовалось, его можно опустить, что и было сделано на последнем шаге в выражении (3.7). По сравнению с состоянием n-кубитового регистра на входе «черного ящика», которое было однородной суперпозицией всех двоичных строк, состояние на выходе имеет знакопеременные коэффициенты, если f не является постоянной. Осталось применить к вектору в правой части (3.7) n-кубитовое преобразование Адамара $H^{\otimes n}$.

Можно показать (см. задачу 1 в конце этого раздела), что

$$H^{\otimes n}|x\rangle = 2^{-n/2}\sum_{y=0}^{2^n-1}(-1)^{x\cdot y}|y\rangle, \qquad (3.8)$$

где $x\cdot y$ представляет собой взятое по модулю 2 побитовое скалярное произведение $x_{n-1}y_{n-1} + x_{n-2}y_{n-2} + \cdots + x_0y_0$, построенное с помощью двоичных представлений $x = x_{n-1}x_{n-2}\ldots x_0$ и $y = y_{n-1}y_{n-2}\ldots y_0$.

С помощью соотношения (3.8) получаем, что состояние n-кубитового регистра на выходе имеет вид суперпозиции

$$H^{\otimes n}\left(2^{-\frac{n}{2}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}|x\rangle\right) = 2^{-n}\sum_{x,y=0}^{2^n-1}(-1)^{f(x)+xy}|y\rangle = \sum_{y=0}^{2^n-1}a_y|y\rangle, \qquad (3.9)$$

коэффициенты которой определяются выражением

$$a_y = 2^{-n}\sum_{x=0}^{2^n-1}(-1)^{f(x)+x\cdot y}. \qquad (3.10)$$

Нет необходимости вычислять эту сумму при всех y. Достаточно рассмотреть только случай $y=0$, то есть величину

$$a_0 = 2^{-n}\sum_{x=0}^{2^n-1}(-1)^{f(x)}. \qquad (3.11)$$

Если f постоянная, т.е. $f(x)=c$, где $c=0,1$, то

$$a_0=(-1)^c=\pm 1. \qquad (3.12)$$

Поскольку $|a_0|^2=1$, то из условия нормировки, которая сохраняется при унитарном преобразовании, следует, что $a_{y\neq 0}=0$. Таким образом, если f постоянная, то *n*-кубитовый регистр с достоверностью будет находиться в состоянии $|y=0\rangle\equiv|00\ldots0\rangle$. Если же f — сбалансированная функция, которая для одной половины значений аргумента равна нулю, а для другой – единице, то в сумме (3.11) положительные и отрицательные слагаемые компенсируют друг друга, и $a_0=0$. Это означает, что будут отличны от нуля, по крайней мере, некоторые коэффициенты $a_{y\neq 0}$. Следовательно, для сбалансированной функции *n*-кубитовый регистр будет находиться в состояниях, отвечающих ненулевым значениям тех или иных битов. Состояние $|00\ldots0\rangle$ строго отсутствует.

Итак, к квантовому «оракулу» можно обратиться один раз и, получив результат, узнать глобальное свойство функции f. Интересно сравнить с классической ситуацией. Если на входе и выходе мы имеем дело с классическими битами, то надо обращаться к «оракулу», выбирая раз за разом какие-то числа от 0 до 2^n-1, и сравнивать получающиеся результаты. Если очередной ответ отличается от предыдущего, то функция, очевидно, сбалансированная. Чтобы быть уверенным, что функция постоянная, надо получить подряд $2^{n-1}+1$ раз одинаковый результат, т.е. такое число случаев, которое на единицу больше половины. В этом смысле можно сказать, что при больших *n* классическое вычисление требует экспоненциально большого числа обращений к вычислителю. Поскольку в квантовом случае нужно только одно обращение, можно говорить об экспоненциальном увеличении скорости вычислений. Обратим внимание еще на один важный момент. Результат квантового вычисления (3.11) формируется благодаря эффекту интерферен-

ции. Амплитуда a_0 содержит сумму различных вкладов. Для постоянной функции f интерференция этих вкладов оказывается конструктивной и дает значение $|a_0| = 1$. Напротив, для сбалансированной функции f интерференция является деструктивной, и амплитуда a_0 обращается в нуль.

В качестве забавной иллюстрации алгоритм Дойча-Джозса можно переложить на язык квантовой игры. Играют Алиса и Боб, как обычно именуют участников коммуникационной сети. Алиса посылает Бобу какие-то числа *x* из промежутка от 0 до $2^n - 1$. Боб для каждого числа вычисляет функцию $f(x)$, которая может принимать только два значения: 0 или 1. Вычисление делается с помощью унитарного преобразования, а вычисляемая функция может быть только либо постоянной, либо сбалансированной. Результаты вычислений Боб посылает Алисе. Спрашивается, сколько ответов нужно Алисе, чтобы выяснить, какую вычислительную манипуляцию – постоянную или сбалансированную – выполняет Боб?

При классических вычислениях в самом неблагоприятном случае Алисе нужно получить количество ответов Боба, равное $2^{n-1}+1$. Если использовать алгоритм Дойча-Джозса, то квантовое вычисление нуждается только в одном запросе.

Задачи

1. Вычислить результат действия преобразования Адамара $H^{\otimes n}$ на базисные состояния *n*-кубитового регистра.

Решение

Результат действия преобразования Адамара *H* на базисные однокубитовые состояния

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \quad \text{и} \quad H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

можно представить в форме единого выражения

$$H\left|c\right\rangle = \frac{1}{\sqrt{2}} \sum_{c'=0,1} (-1)^{cc'} \left|c'\right\rangle, \qquad c, c' = 0,1 \ .$$

Пусть $\left|x\right\rangle = \left|x_{n-1} x_{n-2} \ldots x_0\right\rangle \equiv \left|x_{n-1}\right\rangle \left|x_{n-2}\right\rangle \ldots \left|x_0\right\rangle$ есть базисный вектор n-кубитового регистра, в котором, как обычно, состоящая из 0 и 1 цепочка $\left(x_{n-1} \ldots x_0\right)$ является записью числа x. Тогда

$$H^{\otimes n}\left|x\right\rangle = \left(H\left|x_{n-1}\right\rangle\right)\left(H\left|x_{n-2}\right\rangle\right)\ldots\left(H\left|x_0\right\rangle\right) =$$

$$= 2^{-n/2} \left(\sum_{y_{n-1}=0,1} (-1)^{x_{n-1} y_{n-1}} \left|y_{n-1}\right\rangle \right) \left(\sum_{y_{n-2}=0,1} (-1)^{x_{n-2} y_{n-2}} \left|y_{n-2}\right\rangle \right) \ldots$$

$$\ldots \left(\sum_{y_0=0,1} (-1)^{x_0 y_0} \left|y_0\right\rangle \right) =$$

$$= 2^{-n/2} \sum_{y_0, y_1, \ldots y_{n-1}} (-1)^{x_{n-1} y_{n-1} + x_{n-2} y_{n-2} + \ldots + x_0 y_0} \left|y_{n-1}\right\rangle \left|y_{n-2}\right\rangle \ldots \left|y_0\right\rangle =$$

$$= 2^{-n/2} \sum_{y=0}^{2^n - 1} (-1)^{x \cdot y} \left|y\right\rangle.$$

В этом выражении $\left|y\right\rangle \equiv \left|y_{n-1} y_{n-2} \ldots y_0\right\rangle$; состоящая из 0 и 1 цепочка $\left(y_{n-1} y_{n-2} \ldots y_0\right)$ есть двоичная запись числа y; суммирование ведется по всем значениям y от 0 до $2^n - 1$; символ $x \cdot y$ означает побитовое скалярное произведение $x_{n-1} y_{n-1} + x_{n-2} y_{n-2} + \ldots + x_0 y_0$, взятое по модулю 2. Из полученного выражения следует, что матрица оператора $H^{\otimes n}$ в n-кубитовом базисе имеет вид

$$\left\langle y\right| H^{\otimes n} \left|x\right\rangle = 2^{-n/2} (-1)^{x \cdot y},$$

т.е. состоит из чисел ± 1, умноженных на общий коэффициент $2^{-n/2}$. Поэтому сам оператор $H^{\otimes n}$ можно представить в такой форме

$$H^{\otimes n} = 2^{-n/2} \sum_{x,y} (-1)^{x \cdot y} |y\rangle\langle y|.$$

3.2. Алгоритм квантового поиска

Из классической теории информации известно, что для отыскания нужной записи в неупорядоченной базе данных, надо перебрать, в среднем, приблизительно половину элементов базы (см. задачу 1 в конце этого раздела). Так, если в базе данных хранится *N* записей, то для поиска той, которая нам нужна, потребуется, в среднем, *N*/2 обращений к функции, определяющей искомый элемент. Это означает, что время поиска пропорционально размеру *N* этой базы. Типичный пример из жизни, который напрашивается, это телефонная книга, где есть фамилии и номера телефонов. Фамилии расположены в алфавитном порядке, а принадлежащие этим лицам номера телефонов образуют большую неупорядоченную совокупность чисел. Нас интересует фамилия человека, имеющего данный телефонный номер. Это задача поиска некоторого определенного числа среди неупорядоченной совокупности других чисел. Процедура поиска сводится к тому, что надо брать, например, случайно, одно за другим числа *x* из этой совокупности и сравнивать с тем, которое нам нужно. С математической точки зрения, наличие признака, отличающего нужное число от ненужного, означает, что есть некоторая функция $f(x)$, которая для интересующего нас значения *x* становится равной, например, единице, а для всех других *x* она отличается от единицы. Это простейший случай, когда задача поиска имеет только одно решение. Для его нахождения классический компьютер должен провести операцию вычисления функции $f(x)$, в среднем, для половины значений *x* из области определения.

В 1996 г. *Лов Гровер* показал, что если заняться поиском «кван-

товой иголки в квантовом стоге сена», воспользовавшись сформулированным им алгоритмом, то время поиска сокращается до величины, пропорциональной $\sqrt{N}$, т.е. до корневой зависимости от размеров базы. При больших N ускорение процедуры поиска оказывается весьма ощутимым.

Квантовый «оракул»

Сформулируем задачу поиска следующим образом. Пусть имеется некоторая неупорядоченная база данных. Запись каждого элемента этой базы идентифицируется числом x, которое может принимать значения от 0 до N–1, где $N = 2^n$. Задача состоит в том, чтобы найти запись, у которой x равно интересующему нас значению ω. Для простоты полагаем, что в базе данных есть только одна такая запись. Другими словами, надо найти определенное число ω среди некоторой неупорядоченной совокупности чисел x.

С этой целью введем функцию

$$f_\omega(x) = \begin{cases} 0, & \text{если } x \neq \omega \\ 1, & \text{если } x = \omega \end{cases}, \qquad (3.13)$$

которая определяет нужную запись, принимая значение 1 только для искомого значения $x = \omega$. Вычислением этой функции занимается «оракул», т.е. тот самый «черный ящик», о котором мы уже говорили в предыдущем разделе. На вход оракула подается значение x, а он выдает результат (3.13). Нас интересует, что нужно сделать, чтобы как можно быстрее получить то значение x, при котором $f_\omega(x) = 1$.

При квантовом поиске каждое обращение к «оракулу» может содержать не одно какое-то число x, а суперпозицию состояний, представляющих разные числа. Сам квантовый «оракул» описывается некоторым унитарным оператором $\widehat{U}_{f_\omega}$, которой осуществляет обратимое вычисление функции (3.13). По определению, этот оператор действует в пространстве состояний $|x\rangle|y\rangle$ системы,

состоящей из $n+1$ кубита. В этой системе к цепочке $n \simeq \log_2 N$ кубитов, представляющей числа x, добавлен еще один вспомогательный кубит $|y\rangle$. Действуя на базисное состояние $|x\rangle|y\rangle$, оператор $\widehat{U}_{f_\omega}$ вычисляет функцию $f_\omega(x)$, а получившееся значение, 0 или 1, складывает по модулю 2 с y, т.е. осуществляет преобразование:

$$\widehat{U}_{f_\omega}|x\rangle|y\rangle = |x\rangle|y \oplus f_\omega(x)\rangle. \tag{3.14}$$

Приготовим исходное состояние вспомогательного кубита $|y\rangle$ в виде

$$|y\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right). \tag{3.15}$$

Если, как обычно, стартовать с состояния $|0\rangle$, то кэт-вектор (3.15) можно получить с помощью двух однокубитовых операций, а именно

$$|0\rangle \xrightarrow{NOT} |1\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right).$$

Рассмотрим теперь действие квантового «оракула» на состояние $|x\rangle|y\rangle = |x\rangle\left(|0\rangle - |1\rangle\right)/\sqrt{2}$:

$$\begin{aligned}\widehat{U}_{f_\omega}|x\rangle\frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) &= \frac{1}{\sqrt{2}}|x\rangle\left(|0 \oplus f_\omega(x)\rangle - |1 \oplus f_\omega(x)\rangle\right) = \\ &= (-1)^{f_\omega(x)}|x\rangle\frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right).\end{aligned} \tag{3.16}$$

Это вычисление аналогично тому, которое мы уже проводили в

предыдущем разделе. Действительно, если $x \neq \omega$, то $f_\omega(x) = 0$, и сложение по модулю 2 не меняет состояние второго кубита:

$$\left|0 \oplus f_\omega(x)\right\rangle - \left|1 \oplus f_\omega(x)\right\rangle = \left|0\right\rangle - \left|1\right\rangle.$$

Если же $x = \omega$, то $f_\omega(x) = 1$, так что

$$\left|0 \oplus f_\omega(x)\right\rangle - \left|1 \oplus f_\omega(x)\right\rangle = \left|1\right\rangle - \left|0\right\rangle = -\left(\left|0\right\rangle - \left|1\right\rangle\right).$$

В выражении (3.16) два возможных знака записаны в виде фазового множителя $(-1)^{f_\omega(x)}$.

Вектор состояния (3.16) имеет факторизованный вид. Поэтому кэт-вектор второго кубита, который остался в исходном состоянии (3.15), можно в дальнейшем не писать. Тогда действие «оракула» эквивалентно следующему унитарному преобразованию $\widehat{U}_\omega$ базисных состояний $\left|x\right\rangle$ регистра данных:

$$\widehat{U}_\omega \left|x\right\rangle = (-1)^{f_\omega(x)} \left|x\right\rangle. \qquad (3.17)$$

Это преобразование просто меняет на противоположную фазу искомого состояния $\left|\omega\right\rangle$, а фазы остальных базисных векторов остаются неизменными. Поэтому его удобно представить в виде компактного выражения

$$\widehat{U}_\omega = 1 - 2\left|\omega\right\rangle\left\langle\omega\right|, \qquad (3.18)$$

куда входит только оператор проектирования $\left|\omega\right\rangle\left\langle\omega\right|$ на состояние $\left|\omega\right\rangle$. Подействовав этим оператором на произвольное состояние

$$\left|\Psi\right\rangle = \sum_{x=0}^{N-1} a_x \left|x\right\rangle, \qquad (3.19)$$

получим

$$\widehat{U}_\omega \left|\Psi\right\rangle = \sum_{x=0}^{N-1} a_x \left(1 - 2\left|\omega\right\rangle\left\langle\omega\right|\right)\left|x\right\rangle = \sum_{x\neq\omega} a_x \left|x\right\rangle - a_\omega \left|\omega\right\rangle . \quad (3.20)$$

Таким образом, оператор $\widehat{U}_\omega$, изменив знак коэффициента при состоянии $\left|\omega\right\rangle$ и оставив остальные коэффициенты без изменения, сделал тем самым «метку» на искомом состоянии $\left|\omega\right\rangle$. Поскольку о коэффициентах $a_x = \left\langle x\middle|\Psi\right\rangle$ в разложении (3.19) говорят как о проекциях вектора $\left|\Psi\right\rangle$ в ортонормированном базисе $\left\{\left|x\right\rangle\right\}$, то преобразованию (3.20) можно дать наглядную «геометрическую» интерпретацию. Изменение знака проекции на какую-то ось представляет собой отражение в гиперплоскости, ортогональной этой оси (см. задачу 2 в конце этого раздела).

Алгоритм Гровера

Сформулируем теперь идею алгоритма квантового поиска. Мы ищем состояние $\left|\omega\right\rangle$ среди всех состояний $\left\{\left|x\right\rangle\right\}$. Поэтому приготовим входной регистр, где записываются числа *x*, в состоянии (2.143)

$$\left|\Psi_0\right\rangle \equiv \left|s\right\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \left|x\right\rangle, \quad (3.21)$$

которое, как мы знаем, получается применением преобразования Адамара $H^{\otimes n}$ к *n*-кубитовому состоянию $\left|00\ldots0\right\rangle$. Для этого потребуется число операций, которое просто совпадает с числом кубитов $n \simeq \log_2 N$.

В однородной суперпозиции (3.21) все состояния, изображающие числа *x* в двоичном коде, представлены с одинаковой вероятностью 1/*N*. Суть алгоритма Гровера заключается в последователь-

ном применении к состоянию регистра, начиная с (3.21), некоторого унитарного оператора $\widehat{G}$, который модифицирует состояние таким образом, что с каждым шагом амплитуда вероятности состояния $|\omega\rangle$ возрастет.

Этот оператор имеет вид

$$\widehat{G} = \widehat{U}_s \widehat{U}_\omega . \tag{3.22}$$

Он включает, помимо уже известного преобразования $\widehat{U}_\omega$ (3.18), которое выделяет искомое состояние $|\omega\rangle$, меняя знак соответствующего коэффициента (3.20), еще и оператор

$$\widehat{U}_s = 2|s\rangle\langle s| - 1, \tag{3.23}$$

построенный с помощью внешнего произведения кэт-вектора (3.21). Структура этого оператора похожа на (3.18). В него входит оператор проектирования на состояние $|s\rangle$. Поэтому преобразование (3.23) тоже допускает простую «геометрическую» интерпретацию. Действительно, подействуем оператором $\widehat{U}_s$ на произвольное состояние (3.19) и, учитывая определение (3.22) вектора $|s\rangle$, получим:

$$\begin{aligned}
\widehat{U}_s |\Psi\rangle &= \left(2|s\rangle\langle s| - 1\right) \sum_{x=0}^{N-1} a_x |x\rangle = \\
&= 2|s\rangle \sum_{x=0}^{N-1} a_x \langle s|x\rangle - \sum_{x=0}^{N-1} a_x |x\rangle = \\
&= \sum_{x=0}^{N-1} \left(\frac{2}{N} \sum_{x'=0}^{N-1} a_{x'} - a_x \right) |x\rangle .
\end{aligned}$$

Здесь на последнем шаге проделаны следующие алгебраические преобразования. В первой сумме использовано значение скалярного произведения

$$\langle s|x\rangle = \frac{1}{\sqrt{N}},$$

которое следует из разложения (3.21), а потом индекс суммирования обозначен буквой x'. Для кэт-вектора $|s\rangle$ использовано разложение (3.21).

Таким образом, имеем следующее соотношение

$$\hat{U}_s \sum_{x=0}^{N-1} a_x |x\rangle = \sum_{x=0}^{N-1} b_x |x\rangle, \qquad (3.24)$$

в котором новые коэффициенты разложения

$$b_x = \frac{2}{N} \sum_{x'=0}^{N-1} a_{x'} - a_x \equiv 2 < a > - a_x \qquad (3.25)$$

содержат не зависящую от x величину

$$< a >= \frac{1}{N} \sum_{x=0}^{N-1} a_x . \qquad (3.26)$$

Ее естественно назвать средним значением амплитуды, с которой $|x\rangle$ представлено в исходном состоянии $|\Psi\rangle$. Если положить, что

$$a_x =< a > + \delta a_x, \qquad (3.27)$$

т.е. δa_x имеет смысл отклонения от среднего в исходном состоянии, то коэффициенты после преобразования

$$b_x = a < a > - a_x =< a > - \delta a_x \qquad (3.28)$$

отличаются от исходных значений изменением знака отклонения от среднего. Поэтому $\widehat{U}_s$ называется оператором инверсии относительно среднего.

Покажем, что применение операции Гровера $\widehat{G}$ (3.22) приводит к возрастанию амплитуды вероятности искомого состояния $|\omega\rangle$. Поясним это на примере первой итерации, когда происходит однократное воздействие оператора $\widehat{G} = \widehat{U}_s \widehat{U}_\omega$ на начальное однородное суперпозиционное состояние $|\Psi_0\rangle$. Тогда

$$\widehat{U}_\omega |\Psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{x \neq \omega} |x\rangle - \frac{1}{\sqrt{N}} |\omega\rangle \equiv \sum_x a_x |x\rangle, \qquad (3.29)$$

где

$$a_x = \begin{cases} \dfrac{1}{\sqrt{N}}, & x \neq \omega \\ -\dfrac{1}{\sqrt{N}}, & x = \omega \end{cases}. \qquad (3.30)$$

В состоянии $|\Psi_0\rangle$ средняя амплитуда равна $1/\sqrt{N}$. После действия оператора $\widehat{U}_\omega$ средняя амплитуда $< a >$ уменьшилась. Действительно, с учетом (3.30) имеем для $N \geq 2$

$$< a >= \frac{1}{N} \sum_{x=0}^{N-1} a_x = \frac{1}{N} \left(\frac{N-1}{\sqrt{N}} - \frac{1}{\sqrt{N}} \right) = \frac{1}{\sqrt{N}} \left(1 - \frac{2}{N} \right). \qquad (3.31)$$

Применяя далее операцию $\widehat{U}_s$, т.е. инвертируя коэффициенты a_x (3.30) относительно среднего значения $< a >$ (3.31),

получим, что амплитуда b_ω состояния $|\omega\rangle$

$$b_\omega = 2\langle a \rangle - a_\omega = \frac{2}{\sqrt{N}}\left(1-\frac{2}{N}\right)+\frac{1}{\sqrt{N}} = \frac{1}{\sqrt{N}}\left(3-\frac{4}{N}\right) > \frac{1}{\sqrt{N}} \quad (3.32)$$

возрастает по сравнению с начальным значением $1/\sqrt{N}$, если, конечно, $N > 2$.

Таким образом, применение оператора $\hat{G}$ к начальному состоянию (3.21) «поворачивает» вектор этого состояния в направлении к искомому состоянию $|\omega\rangle$. Уже из результата (3.32) первой итерации Гровера можно понять, что амплитуда состояния $|\omega\rangle$ возрастает пропорционально числу итераций. Поэтому после числа шагов порядка $\sqrt{N}$ состояние $|\omega\rangle$ будет входить с коэффициентом, близким к единице, а амплитуды остальных состояний будут стремиться к нулю. После этого надо только измерить состояние регистра и получить двоичную запись числа ω. На этом процедура квантового поиска заканчивается.

Приведенные здесь качественные рассуждения по поводу возрастания амплитуды вероятности искомого состояния $|\omega\rangle$ и оценка числа шагов как $\sqrt{N}$ показывают, что алгоритм квантового поиска в неупорядоченной базе данных дает полиномиальное ускорение по сравнению с классическим вычислением.

Алгоритм Гровера допускает точное описание для произвольного числа итераций, к которому мы сейчас перейдем.

Многократная итерационная процедура

Рассмотрим процедуру многократного применения оператора Гровера $\hat{G} = \hat{U}_s \hat{U}_\omega$. В начальном состоянии $|\Psi_0\rangle$ (3.21) все коэффициенты одинаковые. Каждое последующее состояние $|\Psi_{k+1}\rangle$

получается из предыдущего $|\Psi_k\rangle$ под действием оператора $\widehat{G}$:

$$|\Psi_{k+1}\rangle = \widehat{G}|\Psi_k\rangle, \quad k = 0,1,2,\ldots \tag{3.33}$$

Напомним результат первой итерации

$$|\Psi_1\rangle = \widehat{G}|\Psi_0\rangle = \widehat{U}_s\widehat{U}_\omega|\Psi_0\rangle = \widehat{U}_s\left(\frac{1}{\sqrt{N}}\sum_{x\neq\omega}|x\rangle - \frac{1}{\sqrt{N}}|\omega\rangle\right) = \\ = \sum_{x\neq\omega} b_x|x\rangle + b_\omega|\omega\rangle, \tag{3.34}$$

где, согласно (3.24) – (3.32),

$$b_{x\neq\omega} = 2 < a > - \frac{1}{\sqrt{N}}, \\ b_\omega = 2 < a > + \frac{1}{\sqrt{N}}, \tag{3.35} \\ < a >= \frac{1}{\sqrt{N}}\left(1 - \frac{2}{N}\right).$$

Отметим, что все коэффициенты $b_{x\neq\omega}$ одинаковые, т.е. не зависят от *x*. Это свойство будет иметь место и при всех последующих итерациях, т.е. на каждом шаге будет своя, но одинаковая для всех $x \neq \omega$ амплитуда состояний. Кроме того, все амплитуды являются действительными, так как рассматриваемые унитарные преобразования описываются действительными матрицами и начальные значения амплитуд тоже действительные. Для *k*-ой итерации обозначим одинаковые действительные амплитуды всех состояний с $x \neq \omega$ как α_k, а действительную амплитуду состояния с $x = \omega$ как β_k, т.е.

$$|\Psi_k\rangle = \alpha_k \sum_{x\neq\omega}|x\rangle + \beta_k|\omega\rangle. \tag{3.36}$$

Тогда

$$
\begin{aligned}
&\left|\Psi_{k+1}\right\rangle = \alpha_{k+1}\sum_{x\neq\omega}\left|x\right\rangle + \beta_{k+1}\left|\omega\right\rangle = \widehat{G}\left|\Psi_{k}\right\rangle = \\
&= \widehat{U}_s\widehat{U}_\omega\left(\alpha_k\sum_{x\neq\omega}\left|x\right\rangle + \beta_k\left|\omega\right\rangle\right) = \\
&= \widehat{U}_s\left(\alpha_k\sum_{x\neq\omega}\left|x\right\rangle - \beta_k\left|\omega\right\rangle\right) = \\
&= \left(2<a_k> - \alpha_k\right)\sum_{x\neq\omega}\left|x\right\rangle + \left(2<a_k> + \beta_k\right)\left|\omega\right\rangle.
\end{aligned}
\tag{3.37}
$$

Здесь

$$
<a_k> = \frac{1}{N}\sum_x a_x^{(k)} = \frac{1}{N}\left[\left(N-1\right)\alpha_k - \beta_k\right]. \tag{3.38}
$$

Приравнивая коэффициенты при одинаковых состояниях в первой и последней строчках уравнения (3.37), получаем с учетом (3.38) следующие рекуррентные соотношения для коэффициентов α_k и β_k:

$$
\begin{aligned}
\alpha_{k+1} &= 2<a_k> - \alpha_k = \left(1-\frac{2}{N}\right)\alpha_k - \frac{2}{N}\beta_k, \\
\beta_{k+1} &= 2<a_k> + \beta_k = \left(1-\frac{2}{N}\right)\beta_k + 2\left(1-\frac{1}{N}\right)\alpha_k.
\end{aligned}
\tag{3.39}
$$

Эти рекуррентные соотношения надо решать с начальным условием, что для $k=0$ имеем:

$$
\alpha_0 = \beta_0 = 1/\sqrt{N}\,. \tag{3.40}
$$

Состояние $\left|\Psi_k\right\rangle$ является нормированным, поэтому действитель-

ные коэффициенты α_k и β_k для любого *k* подчиняются условию

$$\left(N-1\right)\alpha_k^2+\beta_k^2=1. \tag{3.41}$$

Сделаем подстановку

$$\alpha_k=\frac{1}{\sqrt{N-1}}\cos\theta_k,\quad \beta_k=\sin\theta_k \tag{3.42}$$

и выразим рекуррентные соотношения (3.39) через углы θ_k и θ_{k+1}:

$$\begin{aligned}\cos\theta_{k+1}&=\left(1-\frac{2}{N}\right)\cos\theta_k-\frac{2}{\sqrt{N}}\sqrt{1-\frac{1}{N}}\sin\theta_k\equiv\cos\left(\theta_k+2\theta\right),\\ \sin\theta_{k+1}&=\left(1-\frac{2}{N}\right)\sin\theta_k+\frac{2}{\sqrt{N}}\sqrt{1-\frac{1}{N}}\cos\theta_k\equiv\sin\left(\theta_k+2\theta\right),\end{aligned} \tag{3.43}$$

где

$$\cos 2\theta=1-\frac{2}{N},\quad \sin 2\theta=\frac{2}{\sqrt{N}}\sqrt{1-\frac{1}{N}}, \tag{3.44}$$

т.е.

$$\sin\theta=\frac{1}{\sqrt{N}}. \tag{3.45}$$

Из соотношений (3.43) следует, что углы θ_k образуют арифметическую прогрессию

$$\theta_{k+1}=\theta_k+2\theta. \tag{3.46}$$

При $k=0$ имеем $\alpha_0=\beta_0=\dfrac{1}{\sqrt{N}}$ (3.40). Тогда из (3.42) получаем

$$\begin{aligned}\cos\theta_0&=\sqrt{N-1}\alpha_0=\sqrt{1-1/N},\\ \sin\theta_0&=\beta_0=1/\sqrt{N}.\end{aligned}\qquad(3.47)$$

Из сопоставления с (3.45) видим, что

$$\theta=\theta_0\,.\qquad(3.48)$$

Следовательно, решение рекуррентных соотношений для величин θ_k имеет вид:

$$\theta_k=(2k+1)\theta,\quad k=0,1,2,\ldots\qquad(3.49)$$

Поэтому амплитуды

$$\alpha_k=\frac{1}{\sqrt{N-1}}\cos\left[(2k+1)\theta\right],\quad \beta_k=\sin\left[(2k+1)\theta\right]\qquad(3.50)$$

описываются тригонометрическими функциями, аргумент которых линейно растет с увеличением числа итераций. Наличие фактора $1/\sqrt{N-1}$ в коэффициенте α_k связано с тем, что $N-1$ состояний $|x\neq\omega\rangle$ имеют одинаковую амплитуду. При большой базе данных N начальный угол $\theta_0\approx\theta\approx1/\sqrt{N}$ маленький, и все амплитуды малы. Амплитуда β_k искомого состояния $|\omega\rangle$ возрастает с каждой итерацией и достигает максимального значения $\beta_k=1$ при условии $(2k+1)\theta=\pi/2$, т.е. на «шаге» с номером

$$k=\frac{\pi}{4}\theta-\frac{1}{2}\,,\qquad(3.51)$$

где $\sin\theta = \frac{1}{\sqrt{N}}$.

Наибольший интерес, конечно, представляет случай большой базы данных, когда $N \gg 1$. При этом число шагов, необходимое для достижения максимальной, т.е. близкой к единице, амплитуды искомого состояния, определяется выражением

$$k = \frac{\pi}{4}\sqrt{N} - \frac{1}{2} \sim \sqrt{N} \,. \qquad (3.52)$$

Таким образом, если повторить итерации ближайшее к величине (3.52) целое число раз, а потом измерить получившееся состояние, то можно с высокой и не зависящей от N вероятностью найти состояние $|\omega\rangle$.

Принципиальный результат состоит в том, что квантовый поиск требует числа шагов, которое пропорционально квадратному корню из размера базы.

Поскольку в процессе вычислений все амплитуды остаются действительными, всю процедуру квантового поиска можно непосредственно проиллюстрировать с помощью последовательности картинок, изображенных на рис. 3.3.

Они показывают поиск «квантовой иголки в квантовом стоге сена» из шести элементов. Изображены результаты преобразования амплитуд шести состояний $|x\rangle$.

Первый оператор $\hat{U}_\omega$ каждой итерации Гровера меняет знак амплитуды искомого состояния $|\omega\rangle$, в данном случае – четвертого слева. Второй оператор $\hat{U}_s$ осуществляет инверсию амплитуд относительно среднего значения. Здесь $N = 6$, поэтому из формулы (3.51) следует, что $k \simeq 1,4$. На рисунке отчетливо видно значительное возрастание амплитуды искомого состояния уже после двух итераций, т.е. после двукратного применения оператора Гровера.

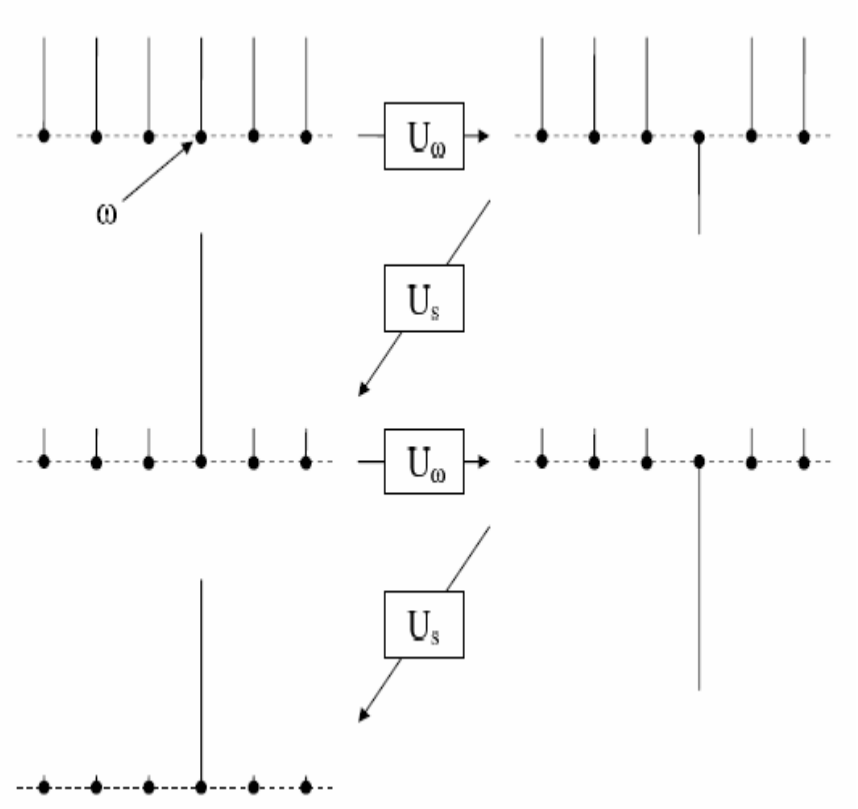


Рис. **3.3**

Квантовая схема алгоритма Гровера

Сконструируем квантовую схему, реализующую алгоритм квантового поиска Гровера. Для этого рассмотрим достаточно простой, но, тем не менее, вполне содержательный случай, когда база данных содержит четыре числа 0, 1, 2 и 3, которые в двоичном коде имеют вид x = 00, 01, 10 и 11. Этим числам отвечают четыре базовых состояния $|x\rangle$ двухкубитового регистра. К этому регистру добавляется еще один вспомогательный кубит $|y\rangle$.

Прежде всего, построим квантовую схему, описывающую действие оператора $\widehat{U}_{f_\omega}$ квантового «оракула» (3.14), т.е. $\widehat{U}_{f_\omega}|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$.

Если искомое число $\omega = 0$, т.е. $|\omega\rangle = |00\rangle$, то квантовая схема «оракула» имеет вид модифицированного элемента Тоффоли:

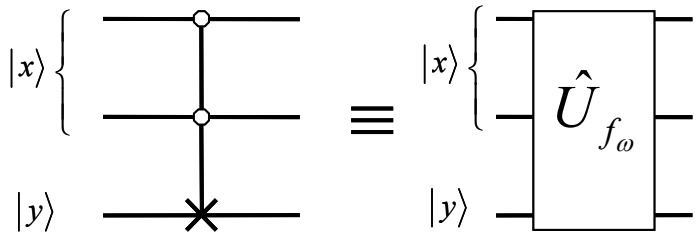


Рис. **3.4**

Действительно, если $x \neq 0$, т.е. $|x\rangle = |01\rangle, |10\rangle$ и $|11\rangle$, то состояние $|y\rangle$ вспомогательного кубита не меняется. Если $x = 0$, т.е. совпадает с искомым числом, то состояние двухкубитового регистра есть $|x\rangle = |00\rangle$, и состояние вспомогательного регистра проходит через операцию *NOT*:

$$|y = 0\rangle \to |1\rangle \equiv |0 \oplus 1\rangle,$$
$$|y = 1\rangle \to |0\rangle \equiv |1 \oplus 1\rangle.$$

Квантовые схемы «оракулов» для других значений искомого числа ω строятся аналогичным образом и показаны на рис. 3.5.

Схема (*a*) отвечает случаю $\omega = 1$, т.е. $|\omega\rangle = |01\rangle$. Управляемый (вспомогательный) кубит $|y\rangle$ проходит через операцию *NOT*, только если $|x\rangle = |01\rangle$.

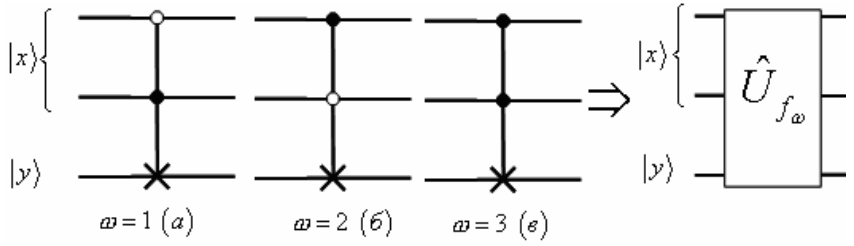


Рис. **3.5**

Схемы (*б*) и (*в*) отвечают, соответственно, значениям $\omega = 2$ и $\omega = 3$, т.е. базисным состояниям регистра данных $|10\rangle$ и $|11\rangle$. В дальнейшем каждая из этих схем изображается в виде блока («черного ящика»), как показано справа на рис. 3.4 и рис. 3.5.

На вход «оракула» подается состояние $|\Psi_0\rangle\frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$, которое описывается выражениями (3.21), (3.15) и приготавливается с помощью однокубитовых операций, показанных на рис. 3.6.

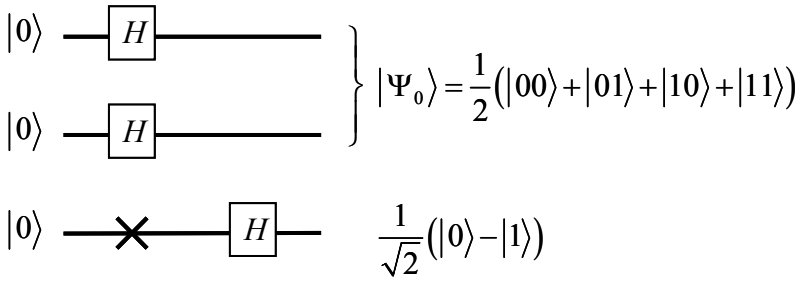


Рис. **3.6**

Теперь отдельно обсудим квантовую схему, реализующую оператор $\widehat{U}_s$ (3.23) инверсии относительно среднего. В общем случае *n*-кубитового регистра данных состояние $|s\rangle$ (3.21) получается из вектора $|00\ldots0\rangle$ применением оператора $H^{\otimes n}$ (см. формулу

(3.143)), т.е.

$$\left|s\right\rangle = 2^{-n/2}\sum_{x=0}^{2^n-1}\left|x\right\rangle = H^{\otimes n}\left|00\ldots0\right\rangle.$$

Подставляя это соотношение в (3.23) и учитывая, что $H^{+} = H = H^{-1}$, получаем следующее выражение для оператора $\widehat{U}_s$:

$$\widehat{U}_s = 2\left|s\right\rangle\left\langle s\right| - 1 = H^{\otimes n}\left(2\left|00\ldots0\right\rangle\left\langle 00\ldots0\right| - 1\right)H^{\otimes n}. \quad (3.53)$$

Стоящий в круглых скобках оператор

$$2\left|00...0\right\rangle\left\langle 00...0\right| - 1 \equiv 2\left|0\right\rangle\left\langle 0\right| - 1 \quad (3.54)$$

действует на базисные векторы $\left|x\right\rangle$ следующим образом:

$$\left|x = 0\right\rangle \to 2\left|0\right\rangle\left\langle 0\right|0\right\rangle - \left|0\right\rangle = \left|0\right\rangle,$$
$$\left|x \neq 0\right\rangle \to 2\left|0\right\rangle\left\langle 0\right|x\right\rangle - \left|x\right\rangle = -\left|x\right\rangle,$$

т.е. он меняет на противоположную фазу всех состояний, кроме $\left|0\right\rangle$. Другими словами, это оператор условного фазового сдвига. Наглядная интерпретация результата (3.53) достаточно проста. Как мы знаем, оператор $\widehat{U}_s$ осуществляет отражение относительно среднего. Операторы Адамара одинаковым образом поворачивают базисные векторы каждого кубита $\left\{\left|0\right\rangle, \left|1\right\rangle\right\} \to \left\{\frac{\left|0\right\rangle \pm \left|1\right\rangle}{\sqrt{2}}\right\}$. После такого поворота в гильбертовом пространстве операция инверсии относительно $\left|s\right\rangle$ становится преобразованием инверсии относительно $\left|0\right\rangle$.

В нашем случае двухкубитового регистра данных оператор (3.53) выглядит следующим образом:

$$\widehat{U}_s = H^{\otimes 2}\left(2\left|00\right\rangle\left\langle 00\right| - 1\right)H^{\otimes 2}. \qquad (3.55)$$

На рис. 3.7 показана квантовая схема, реализующая действие оператора $2\left|00\right\rangle\left\langle 00\right| - 1$ условного фазового сдвига, стоящего в круглых скобках в выражении (3.55).

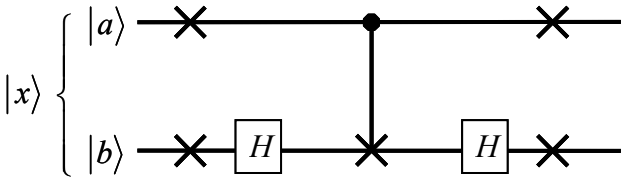


Рис. **3.7**

Чтобы убедиться в этом, посмотрим, как преобразуются базисные векторы $\left|x\right\rangle = \left|a\right\rangle\left|b\right\rangle$ двухкубитового регистра. Если на входе состояние $\left|1\right\rangle\left|b\right\rangle$, то операция *CNOT* на второй кубит не действует, так как после операции *NOT* над первым кубитом получается состояние $\left|0\right\rangle\left|b\right\rangle$. Поэтому второй кубит подвергается преобразованию $\sigma_1 HH\sigma_1 = 1$, т.е. не меняется. Итак, для любого *b* состояние $\left|1b\right\rangle$ не меняется.

Пусть теперь на входе состояние $\left|00\right\rangle$. Тогда последовательность преобразований выглядит так

$$\left|0\right\rangle\left|0\right\rangle \xrightarrow{NOT_1} \left|1\right\rangle\left|0\right\rangle \xrightarrow{NOT_2} \left|1\right\rangle\left|1\right\rangle \xrightarrow{H_2}$$

$$\xrightarrow{H_2} \left|1\right\rangle\frac{\left|0\right\rangle - \left|1\right\rangle}{\sqrt{2}} \xrightarrow{CNOT} \left|1\right\rangle\frac{\left|1\right\rangle - \left|0\right\rangle}{\sqrt{2}} \xrightarrow{H_2}$$

$$\xrightarrow{H_2} \left|1\right\rangle\frac{1}{\sqrt{2}}\left(\frac{\left|0\right\rangle - \left|1\right\rangle}{\sqrt{2}} - \frac{\left|0\right\rangle + \left|1\right\rangle}{\sqrt{2}}\right) =$$

$$= -\left|1\right\rangle\left|1\right\rangle \xrightarrow{NOT_2} -\left|1\right\rangle\left|0\right\rangle \xrightarrow{NOT_1} -\left|0\right\rangle\left|0\right\rangle.$$

Для аккуратности заметим, что индексы 1 и 2 показывают, на какой кубит действует операция, написанная над стрелкой. Итак, $|00\rangle \to -|00\rangle$.

Наконец, начальное состояние $|01\rangle$ преобразуется следующим образом:

$$|0\rangle|1\rangle \xrightarrow{NOT_1} |1\rangle|1\rangle \xrightarrow{NOT_2} |1\rangle|0\rangle \xrightarrow{H_2}$$

$$\xrightarrow{H_2} |1\rangle\frac{|0\rangle+|1\rangle}{\sqrt{2}} \xrightarrow{CNOT} |1\rangle\frac{|1\rangle+|0\rangle}{\sqrt{2}} \xrightarrow{H_2}$$

$$\xrightarrow{H_2} |1\rangle\frac{1}{\sqrt{2}}\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}+\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)=$$

$$=|1\rangle|0\rangle \xrightarrow{NOT_2} |1\rangle|1\rangle \xrightarrow{NOT_1} |0\rangle|1\rangle,$$

т.е. это состояние не меняется, как и все состояния вида $|1b\rangle$. В результате получаем, что фаза состояний $|01\rangle$, $|10\rangle$ и $|11\rangle$ поменялась на противоположную относительно фазы состояния $|00\rangle$.

Собирая все фрагменты (3.4) – (3.7) конструкции, получаем окончательный вид квантовой схемы, описывающей одну итерацию алгоритма Гровера, осуществляющего поиск в базе данных из 4-х элементов:

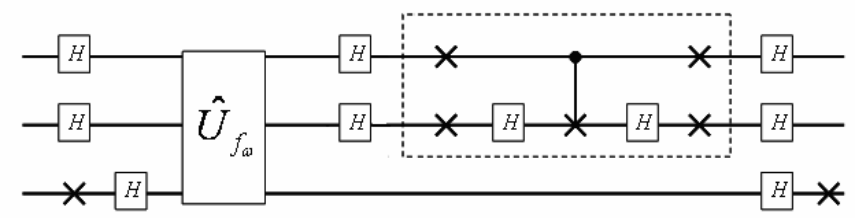


Рис. **3.8**

Для наглядности пунктирным прямоугольником выделен блок, описывающий оператор $2|00\rangle\langle 00|-1$ условного фазового сдвига, схема которого представлена на рис. 3.7. Этот блок взят в «обкладки» из оператора $H^{\otimes 2}$, чтобы получить преобразование (3.55) инверсии относительно среднего.

Операторы H и σ_1, стоящие справа на линии вспомогательного кубита, возвращают его в начальное состояние $|0\rangle$.

Квантовый поиск в базе данных из 4-х элементов представляет собой некоторый забавный специальный случай. Если $N=4$, то из общих формул (3.45) и (3.49) следует, что $\sin\theta = 1/\sqrt{N} = 1/2$, т.е. $\theta = \frac{\pi}{6}$, а $\theta_1 = 3\theta = \frac{\pi}{2}$. Тогда, согласно (3.50), амплитуда β_1 искомого состояния после первой итерации Гровера (k=1)

$$\beta_1 = \sin 3\theta = 1$$

оказывается максимально возможной, т.е. одна итерация Гровера с достоверностью дает искомое число.

В заключение отметим несколько важных моментов, связанных с задачей поиска. Можно показать, что алгоритм квантового поиска Гровера, который решает задачу с использованием только порядка $\sqrt{N}$ обращений к «оракулу», является оптимальным, и решить задачу за меньшее число шагов нельзя.

Абстрактная задача поиска относится к числу фундаментальных математических проблем. Это не только поиск в той или иной базе данных, но и определение, например, количества решений, так называемых, трудных задач, которые могут быть сформулированы как вопрос о существовании решения задачи поиска.

Квантовый алгоритм Гровера показывает, что процедуру поиска можно заметно ускорить по сравнению с расчетами на классическом компьютере.

Задачи

1. Вычислить число шагов, которое требуется, чтобы найти один элемент в неупорядоченной базе данных, содержащей N элементов.

Решение

Вероятность найти нужный элемент на первом шаге есть $W_1 = 1/N$. Вероятность найти на втором шаге есть произведение вероятности $1 - W_1$ отрицательного исхода первого шага и вероятности $1/(N-1)$ удачного исхода второго шага, т.е. $W_2 = (1–1/N)\ /(N-1) = 1/N$. Вероятность найти на третьем шаге есть

$$W_3 = (1–2/N)\ /\ (N-2) = 1/N,$$

где $(1–2/N)$ есть вероятность отрицательного исхода на двух первых шагах. И так далее. Тогда общая формула для вероятности найти искомый элемент ровно на S-ом шаге есть $W_S = 1/N$. Среднее число шагов есть

$$\langle S\rangle = \sum_{S=1}^{N} SW_S = \frac{N(N+1)}{2N} = \frac{N}{2} + \frac{1}{2} \approx \frac{N}{2} \qquad \text{при } N >> 1.$$

Если точно известно, что в базе данных есть искомый элемент, то последний N-й шаг делать не надо, и $\langle S\rangle$ надо уменьшить на величину $1/N$.

2. Дать «геометрическую» интерпретацию унитарного преобразования (3.20)

Решение

Пусть $|\omega\rangle$ — некоторый базисный вектор состояния n-кубитового регистра. Действие унитарного оператора

$$\hat{U}_\omega = 1 - 2|\omega\rangle\langle\omega|$$

на произвольное нормированное состояние $|\psi\rangle = \sum_{x=0}^{N-1} a_x |x\rangle$

системы, где $N = 2^n$, имеет вид

$$\hat{U}_\omega \left|\psi\right\rangle = \sum_{x\neq\omega} a_x \left|x\right\rangle - a_\omega \left|\omega\right\rangle \equiv \left|\Phi\right\rangle .$$

Представим состояние $\left|\psi\right\rangle$ в виде суммы

$$\left|\psi\right\rangle = \sum_{x\neq\omega} a_x \left|x\right\rangle - a_\omega \left|\omega\right\rangle = \sqrt{1-\left|a_\omega\right|^2}\left|\Omega\right\rangle + a_\omega \left|\omega\right\rangle ,$$

где кэт-вектор

$$\left|\Omega\right\rangle = \sum_{x\neq\omega} \frac{a_x}{\sqrt{1-\left|a_\omega\right|^2}} \left|x\right\rangle$$

нормирован на единицу и ортогонален вектору $\left|\omega\right\rangle$, т.е. $\left\langle\Omega\middle|\Omega\right\rangle = \left\langle\omega\middle|\omega\right\rangle = 1, \quad \left\langle\Omega\middle|\omega\right\rangle = 0$. Тогда для преобразованного состояния имеем

$$\left|\Phi\right\rangle = \hat{U}_\omega \left|\psi\right\rangle = \sqrt{1-\left|a_\omega\right|^2}\left|\Omega\right\rangle - a_\omega \left|\omega\right\rangle .$$

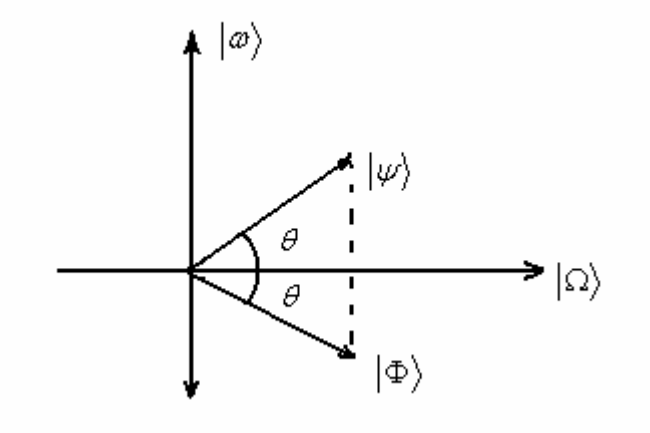
Без ущерба для общности можно считать, что коэффициент a_ω — действительный. Тогда

$$\left|\psi\right\rangle = \cos\theta \left|\Omega\right\rangle + \sin\theta \left|\omega\right\rangle ,$$

$$\left|\Phi\right\rangle = \cos\theta \left|\Omega\right\rangle - \sin\theta \left|\omega\right\rangle ,$$

где $\operatorname{tg}\theta = \dfrac{a_\omega}{\sqrt{1-a_\omega^2}}$. Представив $\left|\Omega\right\rangle$ и $\left|\omega\right\rangle$ как “орты” двумерной системы координат, изобразим $\left|\psi\right\rangle$ и $\left|\Phi\right\rangle$ как векторы, которые

показаны на следующем рисунке:



Таким образом, преобразование $\hat{U}_\omega$ представляет собой “отражение” $|\psi\rangle$ относительно $|\Omega\rangle$.

3.3. Квантовый алгоритм Шора

Важной вехой в становлении квантовой информатики явилось открытие в 1994 г. *Питером Шором* квантового алгоритма для эффективной факторизации больших чисел. Этот результат привлек внимание широкой научной общественности потому, что проблема факторизации, которая известна каждому, кто познакомился с началами арифметики, выступает как своего рода «жупел» для вычислительной математики. Считается, хотя это и не доказано, что для больших чисел эта задача является трудной с точки зрения теории вычислительной сложности. Немаловажную роль сыграл и тот факт, что именно трудность факторизации лежит в основе защищенности наиболее надежных на сегодняшний день методов криптографии. Возможность практического решения проблемы факторизации больших чисел выступает как демонстрация потенциальной мощи использования квантовых явлений для выполнения вычислений.

Изложение основного материала этого раздела предваряется

очень кратким качественным обзором некоторых вопросов, составляющих предмет формальной математической теории вычислительной сложности. Цель состоит в том, чтобы пояснить содержание таких понятий как «трудная задача» или «эффективный метод решения». Далее излагается дискретное квантовое преобразование Фурье (КПФ), которое играет ключевую роль в целом ряде квантовых алгоритмов, в том числе, в алгоритме Шора. Проводится сопоставление КПФ с классическим аналогом, так называемым быстрым преобразованием Фурье. Описывается квантовая схема, реализующая КПФ. Наконец, излагается идея алгоритма Шора.

В основе лежит тот факт, что проблема факторизации обладает важной структурой, которая позволяет свести процедуру построения решения к поиску периода длинной последовательности. Показывается, что квантовый алгоритм Шора эффективно решает эту задачу с экспоненциальным ускорением по сравнению с известными классическими алгоритмами.

Понятие вычислительной сложности

К понятию вычислительной сложности теория подходит, основываясь на том, какие ресурсы времени и памяти требуются для того или иного вычисления. Во главу угла ставится не столько сам факт существования или отсутствия алгоритма вычисления, сколько существование эффективного алгоритма. Это понятие можно формализовать (см. книгу 1), как это делается в теории вычислительной сложности, выделяя классы тех функций (или предикатов), вычисление которых возможно при задаваемых ограничениях на потребляемые ресурсы. Соответствующие совокупности называются классами сложности.

Такая характеристика функции как принадлежность к тому или иному классу сложности должна определять возможности ее вычисления, не связанные с конкретными реализациями алгоритмов.

Наиболее существенное различие между классами определяется ограничениями, которые накладываются на рост временных затрат, или объема памяти, или того и другого в зависимости от длины входного слова, т.е. от длины n двоичной строки, подаваемой на вход. Разграничение между эффективными и неэффективными

вычислениями задается функциями полиномиального роста[1].

Задача считается легкой или решаемой, если для ее решения существует алгоритм, требующий ресурсов, ограниченных функцией *poly*(*n*). В этом случае говорится, что есть эффективный алгоритм решения.

Рост быстрее любой степени принято называть экспоненциальным, хотя это может быть, например, функция типа $\exp\left[\left(\log n\right)^2\right] = n^{\log n}$, которая растет быстрее любого многочлена, но медленнее, скажем, экспоненты $\exp\left(n^{\alpha}\right)$ с $0 < \alpha < 1$. Задача считается трудной или нерешаемой, если любой возможный алгоритм требует экспоненциального ресурса. В этом случае считается, что нет эффективного алгоритма решения.

Разделение эффективных и неэффективных алгоритмов с помощью функций полиномиального роста не зависит от выбора модели вычислений. Это утверждение связано с так называемым тезисом Чёрча-Тьюринга, суть которого в несколько упрощенной форме сводится к тому, что различные модели вычислений отличаются только полиномиальным изменением числа операций. Поэтому принадлежность алгоритма полиномиальному или экспоненциальному классам не зависит от модели вычислений.

Мы не будем дальше погружаться в формальную математическую теорию вычислительной сложности. Главная цель предыдущего обсуждения состояла в том, чтобы пояснить, почему разграничение между эффективными и неэффективными вычислениями, т.е. между наиболее важными классами сложности, определяется полиномиальной либо экспоненциальной зависимостью ресурса от размера входных данных. Другими словами, вычислительная сложность определяется числом шагов (элементарных логических гейтов) *S*, которое необходимо, чтобы с помощью наилучшего из известных алгоритмов решить задачу, т.е. по информации, заданной на входе, получить результат на выходе. Пусть количество

---

[1] Функция $f(n)$ называется функцией *полиномиального роста*, если при достаточно больших *n* выполняется неравенство $f(n) \le n^{\alpha}$ с некоторой константой $\alpha > 0$. Такая функция обозначается как $f(n) \equiv poly(n)$.

информации, т.е. число битов, необходимое для ее хранения, есть n. Так, для числа M эта величина есть $n \simeq \log_2 M$. Считается, что задача поддается вычислению, если $S(n) = poly(n)$. Такая задача относится к классу сложности ***P*** (от слова *polynomial*). Существуют задачи, неразрешимые за полиномиальное время. Вспомним уже известную нам проблему поиска в неупорядоченной базе данных из 2^n элементов, когда число шагов любого классического алгоритма просто пропорционально размеру базы, т.е. зависит от n экспоненциально. Кстати, квантовый поиск тоже требует экспоненциального ресурса. Можно привести целый ряд примеров таких задач, для которых полиномиальные алгоритмы неизвестны, хотя в каждом конкретном случае доказательство того, что данная проблема неразрешима за полиномиальное время и требует экспоненциального ресурса, может отсутствовать.

Важным примером такой задачи, для которой не известен простой метод решения, является проблема факторизации, т.е. разложения большого числа на множители. Принято считать, что она не принадлежит классу ***P***. Примечательным свойством этой задачи и целого ряда других задач является то, что истинность того или иного предъявленного решения можно легко проверить за полиномиальное число шагов. Эти задачи принадлежат к классу сложности ***NP*** (от слов *nondeterministic polynomial)*. Пока остается нерешенной одна из фундаментальных проблем теории сложности – есть ли ***NP***-задачи, не принадлежащие к классу ***P***.

Наилучший известный классический алгоритм факторизации числа $M \gg 1$ – «решето числового поля» – требует экспоненциально большого числа шагов

$$S \sim \exp\left[\left(8/3\right)^{2/3} \left(\ln M\right)^{1/3} \left(\ln \ln M\right)^{2/3} \right]. \qquad (3.56)$$

Можно оценить, что для факторизации числа, содержащего, скажем, 130 десятичных знаков, потребуется порядка 10^{18} шагов. При быстродействии 10^{12} с^{-1} вычисление займет 12 дней. Кстати, в 1994 г. факторизацией 129-значного числа, известного как *RSA* 129, были заняты более полутора тысяч рабочих станций в течение 8

месяцев. Если увеличить число до 250 десятичных знаков, то при быстродействии 10^{12} с$^{-1}$ для его факторизации понадобится несколько тысячелетий. Эти оценки дают представление о том, что такое трудная задача.

Заметим, что практическая значимость этой теоретико-числовой задачи связана с тем, что сложность разложения на множители определяет защиту и секретность широко распространенных криптографических систем.

Например, известная криптографическая система с открытым ключом *RSA*, разработанная в 1979 г. *Роном Ривестом, Ади Шамиром* и *Леонардом Адлеманом*, использует следующую процедуру. Пусть большое число $c = p \cdot q$ есть произведение двух больших простых чисел *p* и *q*. Боб шифрует текст сообщения *T* с помощью некоторого нечетного числа *t*, которое является взаимно простым с числом $\varphi(c) = (p-1)(q-1)$, которое представляет собой так называемую функцию Эйлера. Для этого он вычисляет величину[1]

$$M(T) = T^t \pmod{c} \tag{3.57}$$

и посылает ее Алисе. Получив от Боба послание $M(T)$, Алиса расшифровывает его с помощью числа *m*, которое находит из условия

$$m \cdot t = 1 \pmod{\varphi(c)}. \tag{3.58}$$

Для дешифровки Алисе достаточно вычислить величину $(M(T))^m \pmod{c}$. Можно показать (см. задачу 1 в конце этого раздела), что эта величина в точности совпадает с текстом,

[1] Соотношение $a = b \pmod{c}$ эквивалентно равенству $a = k \cdot c + b$, где все буквы обозначают целые неотрицательные числа, и $b < c$.

который написал Боб, т.е.

$$\left(M(T)\right)^m \left(\mathrm{mod}\, c\right) = T\,. \tag{3.59}$$

В этой криптографической системе числа *c* и *t* являются открытым ключом и известны всем. Секретный ключ *m* можно найти, только зная простые делители числа *c*.

Квантовое преобразование Фурье

Пусть $f(x)$ есть функция битов, т.е. функция дискретной переменной *x*, которая принимает значение от 0 до $N-1$, где $N = 2^n$. Дискретное преобразование Фурье $\varphi(x)$ функции $f(x)$ определяется выражением

$$\varphi(x) = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \exp\left(2\pi i \frac{xy}{N}\right) f(y)\,. \tag{3.60}$$

Рассмотрим сначала классическую процедуру вычисления суммы (3.60). Если совокупность дискретных значений $\{f(0), f(1), \ldots, f(N-1)\}$ функции f и аналогичную совокупность значений $\{\varphi(0), \varphi(1), \ldots, \varphi(N-1)\}$ функции φ рассматривать как два вектор-столбца, то преобразование (3.60) означает, что искомая функция φ получается из f в результате действия унитарной[1] $N \times N$ матрицы $\widehat{F}$ с матричными элементами

$$F_{xy} = \frac{1}{\sqrt{N}} \exp\left(2\pi i \frac{xy}{N}\right). \tag{3.61}$$

Из определения (3.60) видно, что «бесхитростное» вычисление *N*

[1] Унитарность матрицы (3.61) доказывается в задаче 2 в конце этого раздела.

значений функции $\varphi(x)$ для каждой совокупности значений $f(y)$ потребует порядка N^2 операций.

В рассматриваемом нами случае, когда $N = 2^n$, существует классическая оптимизация процесса вычисления, которая сокращает трудоемкость до числа операций порядка $N \log_2 N = n2^n$. Такая процедура вычисления называется быстрым преобразованием Фурье.

Для этого вспомним, что x и y можно представить в виде n-разрядных разложений по степеням двойки:

$$\begin{aligned} x &= x_{n-1}2^{n-1} + x_{n-2}2^{n-2} + \cdots + x_1 2 + x_0 \\ y &= y_{n-1}2^{n-1} + y_{n-2}2^{n-2} + \cdots + y_1 2 + y_0, \end{aligned} \tag{3.62}$$

так что $x_i, y_i = 0,1$, а состоящие из нулей и единиц строки $\left(x_{n-1}x_{n-2}\cdots x_k \cdots x_1 x_0\right)$ и $\left(y_{n-1}y_{n-2}\cdots y_k \cdots y_1 y_0\right)$ являются n-разрядными двоичными записями чисел x и y соответственно.

При вычислении матричных элементов (3.61) в разложении произведения $x \cdot y$ по степеням двойки достаточно удержать только слагаемые, содержащие 2^k с $k \le n-1$, поскольку члены с более высокими степенями уже, очевидно, не влияют на величину $\exp\left(2\pi i xy/2^n\right)$, так как дают множители, равные единице. Тогда существенную для вычисления часть величины $xy/2^n$ можно представить в форме

$$\begin{aligned} &\frac{xy}{2^n} \to y_{n-1}\frac{x_0}{2} + y_{n-2}\left(\frac{x_1}{2} + \frac{x_0}{2^2}\right) + y_{n-3}\left(\frac{x_2}{2} + \frac{x_1}{2^2} + \frac{x_0}{2^3}\right) + \cdots + \\ &+ \cdots + y_1\left(\frac{x_{n-2}}{2} + \frac{x_{n-3}}{2^2} + \cdots \frac{x_1}{2^{n-2}} + \frac{x_0}{2^{n-1}}\right) + \\ &\quad + y_0\left(\frac{x_{n-1}}{2} + \cdots \frac{x_1}{2^{n-1}} + \frac{x_0}{2^n}\right) \equiv \\ &\equiv y_{n-1}\left(\bullet x_0\right) + y_{n-2}\left(\bullet x_1 x_0\right) + y_{n-3}\left(\bullet x_2 x_1 x_0\right) + \cdots + \\ &\quad + y_1\left(\bullet x_{n-2}x_{n-3}\cdots x_1 x_0\right) + y_0\left(\bullet x_{n-1}x_{n-2}\cdots x_0\right). \end{aligned} \tag{3.63}$$

Здесь на последнем шаге введено обозначение для двоичных дробей в виде множителей, написанных в скобках. Например,

$$\left(\bullet x_2 x_1 x_0\right) \equiv \frac{x_2}{2} + \frac{x_1}{2^2} + \frac{x_0}{2^3}. \qquad (3.64)$$

Подставляя разложение (3.63) в (3.61), получаем

$$F_{xy} = \frac{1}{\sqrt{N}} \prod_{k=0}^{n-1} \exp\left[2\pi i y_k \left(\bullet x_{n-k-1} \cdots x_0\right)\right]. \qquad (3.65)$$

Для вычисления функции $\varphi(x)$ надо, согласно (3.60), умножить $f(y)$ на F_{xy} и просуммировать по всем y. С помощью представления (3.65) для матрицы F_{xy} суммирование по y сводится к суммированию по двум возможным значениям $y_k = 0,1$ каждого двоичного разряда числа y. Поэтому число операций, которое требуется для вычисления $\varphi(x)$ для одного из N значений переменной x, определяется количеством сомножителей в произведении (3.65), т.е. порядка $n = \log_2 N$. Полное же вычисление функции $\varphi(x)$ потребует порядка $N \log_2 N = n2^n$ операций.

Перейдем теперь к квантовому преобразованию Фурье (КПФ). Этому преобразованию отвечает унитарный оператор, который действует на базисные векторы $|x\rangle$ состояний n-кубитового регистра по закону:

$$|x\rangle \xrightarrow{КПФ} |\Psi\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \exp\left(2\pi i \frac{xy}{N}\right) |y\rangle. \qquad (3.66)$$

Эта формула является квантовым аналогом выражения (3.60) в том смысле, что вместо вектор-столбцов $\varphi(x)$ и $f(y)$ стоят кэт-векторы $|\Psi\rangle$ и $|y\rangle$. Унитарность преобразования (3.66) совпадает с условием унитарности матрицы коэффициентов в разложении

(3.66), а она имеет тот же самый вид, что и матрица F_{xy} (3.61). Зная результат (3.66) преобразования для базисных векторов и используя свойство линейности оператора, не представляет труда написать КПФ для произвольного состояния.

Займемся преобразованием выражения (3.66) к виду, из которого легко понять, как построить квантовую схему, реализующую КПФ. В выражении (3.66) числа *x* и *y* считаем записанными в виде *n*-разрядных двоичных строк. Стоящая в показателе экспоненты величина $xy/2^n$ описывается формулой (3.63). Поскольку каждый базисный кэт-вектор $|y\rangle$ имеет вид $|y_{n-1}\dots y_1 y_0\rangle = |y_{n-1}\rangle|y_{n-2}\rangle\cdots|y_1\rangle|y_0\rangle$, суммирование по *y* сводится к суммированию по двум значениям $y_k = 0,1$ для каждого однокубитового состояния $|y_k\rangle$ вместе с фазовым множителем $\exp\left[2\pi i y_k\left(\bullet x_{n-k-1}\dots x_1 x_0\right)\right]$. Тогда цепочка преобразований выглядит следующим образом:

$$
\begin{aligned}
|\Psi\rangle &= 2^{-n/2}\sum_{y}\exp\left[2\pi i\sum_{k=0}^{n-1}y_k\left(\bullet x_{n-k-1}\cdots x_0\right)\right]|y_{n-1}y_{n-2}\dots y_0\rangle = \\
&= 2^{-n/2}\left(\sum_{y_{n-1}=0,1}\exp\left[2\pi i y_{n-1}\left(\bullet x_0\right)\right]|y_{n-1}\rangle\right)\times \\
&\times\left(\sum_{y_{n-2}=0,1}\exp\left[2\pi i y_{n-2}\left(\bullet x_1 x_0\right)\right]|y_{n-2}\rangle\right)\cdots \\
&\cdots\left(\sum_{y_0=0,1}\exp\left[2\pi i y_0\left(\bullet x_{n-1}\cdots x_0\right)\right]|y_0\rangle\right) = \\
&= 2^{-n/2}\left(|0\rangle + e^{2\pi i(\bullet x_0)}|1\rangle\right)\left(|0\rangle + e^{2\pi i(\bullet x_1 x_0)}|1\rangle\right)\cdots \\
&\cdots\left(|0\rangle + e^{2\pi i(\bullet x_{n-1}\cdots x_0)}|1\rangle\right).
\end{aligned}
\qquad (3.67)
$$

Получившееся состояние (3.67) имеет факторизованный вид.

Состояние каждого кубита является суперпозицией базисных состояний $|0\rangle$ и $|1\rangle$, а коэффициент при $|1\rangle$ представляет собой некоторый фазовый множитель. Можно сказать, что каждый кубит подвергается преобразованию сдвига фазы. При этом фазовые сдвиги зависят от значений двоичных дробей, которые определяются двоичными знаками числа *x*. Каждая такая дробь представляет сумму типа (3.64), так что результирующая фаза определяется не только значением данного кубита, но аддитивно зависит от других кубитов. Поэтому такие фазовые преобразования можно осуществить с помощью однокубитовых гейтов, а также двухкубитовых гейтов, которые описывают управляемые фазовые преобразования.

Напомним, что расположение однокубитовых кэт-векторов в тензорном произведении (3.67) соответствует убыванию двоичных разрядов слева направо. Количество же разрядов двоичных дробей, стоящих в фазах, напротив, возрастает слева направо. Поменяем местами кубиты – первый и последний, второй и предпоследний и т.д. Если число кубитов четное, то все обмены будут парными. При нечетном числе кубитов положение среднего кубита остается неизменным. Каждая перестановка представляет собой унитарное преобразование, которое реализуется с помощью трех гейтов CNOT (см. задачу 3 в конце раздела 2.5). Сделав такое преобразование состояния (3.67), получим

$$2^{-n/2}\left(|0\rangle + e^{2\pi i(\bullet x_{n-1}\cdots x_0)}|1\rangle\right)\left(|0\rangle + e^{2\pi i(\bullet x_{n-2}\cdots x_0)}|1\rangle\right)\cdots$$
$$\cdots\left(|0\rangle + e^{2\pi i(\bullet x_0)}|1\rangle\right). \qquad (3.68)$$

Теперь двоичные разряды кубитов и число разрядов в двоичных дробях, стоящих в фазах, упорядочены одинаковым образом – они убывают слева направо, что существенно упрощает понимание структуры квантовой схемы.

Каждая круглая скобка в (3.68) отвечает определенному двоичному разряду. Этот же разряд имеет первый знак в двоичной дроби, которая входит в фазовый множитель. Поэтому вклад в фазу первого слагаемого двоичной дроби зависит от значения данного бита

и определяется однокубитовым оператором Адамара. Действительно, если подействовать этим оператором на кубит $|x_k\rangle$, соответствующий *k*-му разряду, то получим

$$H|x_k\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{x_k}|1\rangle\right) = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i(\bullet x_k)}|1\rangle\right), \quad (3.69)$$

так как

$$(-1)^{x_k} = \exp(i\pi x_k) = \exp\left(2\pi i\frac{x_k}{2}\right) \equiv \exp\left[2\pi i(\bullet x_k)\right].$$

Вклады в фазу других слагаемых двоичной дроби зависят от значений битов в предшествующих разрядах. Они описываются двухкубитовыми операциями управляемых фазовых сдвигов:

$$Controlled\ P_d = |0\rangle_j \cdot_j \langle 0| \otimes \hat{I}_k + |1\rangle_j \cdot_j \langle 1| \otimes \hat{P}_d\,. \quad (3.70)$$

Управляющий кубит имеет индекс *j*, а управляемый кубит – индекс *k*, отвечающий более высокому разряду, чем *j*.

Однокубитовый унитарный оператор

$$\hat{P}_d \equiv \hat{P}\left(\pi/2^d\right) = |0\rangle_k \cdot {}_k\langle 0| + \exp\left(i\pi/2^d\right)|1\rangle_k \cdot {}_k\langle 1| \quad (3.71)$$

фазового сдвига $\pi/2^d$ действует на *k*-й кубит. Величина фазового сдвига зависит от «расстояния» $d = k - j$ между кубитами.

Чтобы получить, например, кэт-вектор, стоящий в первой круглой скобке выражения (3.68), надо на исходное состояние

$$|x_{n-1}\rangle|x_{n-2}\rangle\cdots|x_0\rangle$$

подействовать сначала оператором *H* на первый кубит, а потом применить последовательно операторы управляемых фазовых сдвигов на двухкубитовые состояния

$$|x_{n-1}\rangle|x_{n-2}\rangle, |x_{n-1}\rangle|x_{n-3}\rangle, \ldots, |x_{n-1}\rangle|x_0\rangle\,.$$

Тогда цепочка преобразований выглядит следующим образом:

$$|x_{n-1}\rangle|x_{n-2}\rangle\cdots|x_0\rangle \xrightarrow{H_{n-1}} \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i(\bullet x_{n-1})}|1\rangle\right)|x_{n-2}\rangle\cdots|x_0\rangle \longrightarrow$$

$$\xrightarrow{CP_1} \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i(\bullet x_{n-1}x_{n-2})}|1\rangle\right)|x_{n-2}\rangle|x_{n-3}\rangle\cdots|x_0\rangle \longrightarrow$$

$$\xrightarrow{CP_2} \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i(\bullet x_{n-1}x_{n-2}x_{n-3})}|1\rangle\right)|x_{n-2}\rangle\cdots|x_0\rangle \longrightarrow$$

$$\cdots \xrightarrow{CPn-1} \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i(\bullet x_{n-1}\cdots x_0)}|1\rangle\right)|x_{n-2}\rangle\cdots|x_0\rangle.$$

После завершения этой процедуры с первым кубитом аналогичные преобразования производятся со вторым кубитом, третьим и т.д. В результате получается состояние (3.68). Заключительным преобразованием надо вернуть переставленные кубиты на исходные места. Это делается с помощью того же самого преобразования обмена. На рис. 3.9 представлена квантовая схема, реализующая КПФ на трех кубитах.

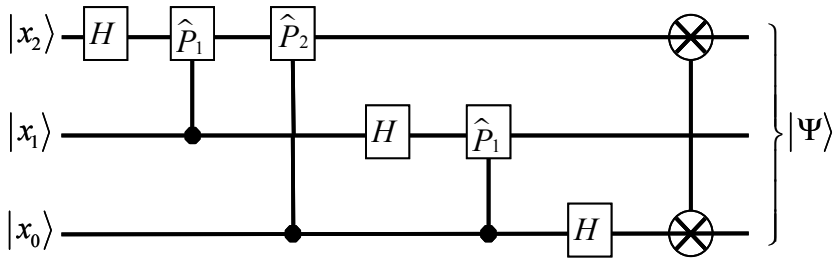


Рис. **3.9**

Последний элемент справа представляет преобразование обмена первого и третьего кубитов.

Оценим число операций, реализующих КПФ. Число однокубитовых операций H равно числу кубитов n. Число двухкубитовых

операций $Controlled\ P_d$ определяется числом пар среди *n* кубитов, поскольку каждый раз управляющие кубиты расположены в предыдущих разрядах двоичной записи числа *x*. Поэтому число двухкубитовых операций есть $C_n^2 = n(n-1)/2$. Эта величина определяет характер роста требуемого ресурса, который ведет себя полиномиальным образом как $n^2 = (\log_2 N)^2$.

Таким образом, КПФ дает очень сильное – экспоненциальное – ускорение вычислительной процедуры по сравнению с классическим быстрым преобразованием Фурье, которое, напомним, требует порядка $N \log_2 N$ операций. Отметим, что число операций для КПФ можно уменьшить до линейной зависимости от $n = \log_2 N$, если есть возможность снизить точность. Дело в том, что двухкубитовые гейты $Controlled\ P_d$ начинают давать экспоненциально малый вклад в фазовый сдвиг $\pi/2^d$, если «расстояние» *d* между управляющим и управляемым кубитами велико. Если опустить гейты, которые действуют на кубиты, разнесенные друг от друга более чем на *m* позиций, то каждое длинное слагаемое в (3.63) заменяется *m*-битовым приближением. Полная погрешность в $xy/2^n$ заведомо не больше чем $n/2^m$. Поэтому, если выбрать $m \geq \log n/\varepsilon$, то погрешность в величине $xy/2^n$ будет меньше ε. Итак, если сохранить только гейты, которые действуют на кубиты, разнесенные на *m* и менее позиций, то их число *nm* будет порядка $n \log n/\varepsilon$, а не n^2.

Квантовая схема, реализующая КПФ, была разработана *Д. Копперсмитом* в 1994 г. Заметим также, что преобразование Адамара принадлежит к некоторому классу квантовых преобразований Фурье.

Квантовый алгоритм поиска периода последовательности и задача факторизации

Задача факторизации может быть сведена к другой трудной проблеме – отысканию периода длинной последовательности. Пре-

имущества собственно квантовой составляющей алгоритма Шора как раз и проявляются при решении этой последней задачи.

Итак, для факторизации числа M выберем некоторое число $x < M$, которое является взаимно простым с M. Если это не так, то с помощью элементарного алгоритма Евклида находим общий делитель x и M и редуцируем задачу, так как один делитель числа M найден и можно искать делитель частного. Для данных M и x строим последовательность

$$f(a) = x^a \left(\mathrm{mod}\, M\right), \quad a = 0,1,2,\ldots \tag{3.72}$$

Можно убедиться, что эта последовательность

$$f(a) = 1, x, \ldots, x_{r-1}, 1, x, \ldots \tag{3.73}$$

является периодической функцией a с периодом r, где $r \neq 0$ есть минимальная степень, для которой

$$x^r = 1\left(\mathrm{mod}\, M\right). \tag{3.74}$$

Такое число r называется *порядком* числа x по модулю M.

Предположим, что с помощью какого-то алгоритма будет найден период r. Пусть этот период четный. Если r оказалось нечетным, то надо изменить x и повторить вычисления. Запишем соотношение (3.74) в виде

$$x^r - 1 = \left(x^{r/2} + 1\right)\left(x^{r/2} - 1\right) = 0\left(\mathrm{mod}\, M\right). \tag{3.75}$$

Отсюда следует, что либо один, либо другой сомножитель должен иметь с M общий делитель. Нахождение любого нетривиального делителя с помощью, например, алгоритма Евклида решает задачу. Если число M большое, то период r тоже оказывается достаточно большим. Задача определения периода длинной последовательности относится к тому же классу сложности, что и задача факторизации. Для нее не известен эффективный алгоритм решения.

Проиллюстрируем указанное свойство задачи факторизации на простом примере разложения на сомножители числа 21. В качестве x выберем число 5, взаимно простое с 21. Подсчитав вручную последовательность (3.72), получаем следующую таблицу:

A	0	1	2	3	4	5	6	7	8	9	10	…
$5^a \pmod{21}$	1	5	4	20	16	17	1	5	4	20	16	…

Из этой таблицы видно, что $5^6 \equiv 1 \pmod{21}$, т.е. период r в данном случае равен 6. Записывая далее соотношение (3.75), получаем

$$\left(5^3\right)^2 - 1 = \left(5^3 - 1\right)\left(5^3 + 1\right) = 124.126 = 0 \pmod{21}.$$

Осталось установить, что у числа 124 или 126 есть общий множитель с числом 21. Воспользовавшись алгоритмом Евклида, находим, что число 124 является взаимно простым с 21, а число 126 вместе с 21 делится на 3 и 7. Таким образом, разложение на множители имеет вид $21 = 3 \times 7$.

Теперь рассмотрим квантовый алгоритм поиска периода длинной последовательности $f(a), \quad a = 0,1,\ldots,2^n - 1$. Систему кубитов, каждый из которых первоначально находится в состоянии $|0\rangle$, образуют два квантовых регистра $|0;0\rangle \equiv |00\ldots0;00\ldots0\rangle$. О них можно говорить как о двух наборах квантовых переменных. В первом регистре n кубитов, с помощью которых записываются числа a. Второй регистр должен содержать число кубитов, достаточное для последующих вычислений. Применяя преобразование Адамара к каждому из кубитов первого регистра, получаем состояние

$$s^{-1/2} \sum_{a=0}^{s-1} |a;0\rangle, \quad s = 2^n, \tag{3.76}$$

которое является суперпозицией всех двоичных строк длины n для первого набора квантовых переменных.

Далее используется некоторая последовательность элементар-

ных квантовых гейтов, с помощью которой вычисляются значения функции $f(a)$ для каждого числа *a*, представленного в первом регистре, и результат записывается во второй регистр. Таким образом, унитарное преобразование, осуществляющее это квантовое вычисление, превращает каждое состояние $|a;0\rangle$ в состояние $|a;f(a)\rangle$. Примененная к суперпозиционному состоянию (3.76), эта операция дает состояние

$$s^{-1/2}\sum_{a=0}^{s-1}|a;f(a)\rangle. \qquad (3.77)$$

Мы вновь видим, как работает квантовый параллелизм, позволяющий за один шаг вычислить функцию $f(a)$ для экспоненциально большого числа 2^n значений переменной *a*. Отметим также, что состояние системы представляет собой сильно перепутанное состояние всех кубитов, в том числе перепутаны состояния двух регистров. В этой ситуации, как мы уже говорили, могут проявляться те или иные глобальные свойства функции $f(a)$.

Следующая ключевая операция состоит в применении квантового преобразования Фурье (КПФ) (3.66) к переменным первого набора. Для каждого члена суммы (3.77) это преобразование имеет вид

$$|a;f(a)\rangle \to s^{-1/2}\sum_{c=0}^{s-1}\exp\left[i\frac{2\pi a}{s}c\right]|c;f(a)\rangle. \qquad (3.78)$$

Тогда для суперпозиционного состояния (3.77) КПФ приводит к следующему состоянию системы на выходе:

$$s^{-1}\sum_{c=0}^{s-1}\sum_{a=0}^{s-1}\exp\left[i\frac{2\pi a}{s}c\right]|c;f(a)\rangle. \qquad (3.79)$$

На этом процесс квантового вычисления заканчивается.

Измерим состояние всех *n* кубитов первого регистра в вычислительном базисе $|0\rangle$ и $|1\rangle$. Такое измерение дает случайным образом какую-то строку $|c;\ldots\rangle$, представленную в состоянии (3.79). Пусть вероятность этого результата есть $W(c)$. Ключевым моментом является именно квантовое распределение вероятности получения того или иного результата. Если функция $f(a)$ имеет период *r*, то сумма по *a* в формуле (3.79) приводит к конструктивной интерференции большого числа коэффициентов в том случае, когда входящая в фазу величина c/s кратна обратному периоду $1/r$, т.е. $c/s = p/r$, где *p* – целое число. Действительно, в этом случае $\exp\left(i\frac{2\pi ac}{s}\right) = \exp\left(i2\pi a\frac{p}{r}\right) = 1$ для $a = r, 2r, 3r, \ldots$. Для всех других значений числа c/s, т.е. не кратных $1/r$, будет иметь место, в большей или меньшей степени, деструктивная интерференция. Это означает, что распределение вероятности $W(c)$ найти первый регистр в состоянии $|c\rangle$ будет иметь резкие пики вблизи значений

$$c = p\cdot\frac{s}{r} = 0,\ s/r,\ 2s/r,\ldots, \tag{3.80}$$

как это изображено на рис. 3.10.

Один описанный выше цикл работы с одним актом измерения дает случайное число $c = ps/r$, кратное обратному периоду $1/r$. Если *p* и *r* взаимно простые, то период *r* получается, если привести c/s к несократимой дроби. Для реализации такой благоприятной ситуации процедуру вычисления надо повторить несколько раз, порядка $\log_2\log_2 r < \log_2\log_2 M \sim \log_2 n$. Как уже отмечалось, квантовое преобразование Фурье требует порядка n^2 операций, а с учетом вычисления функции $f(a)$, полная сеть гейтов, необходимых для реализации алгоритма Шора, содержит порядка $300n^3$ логических элементов.

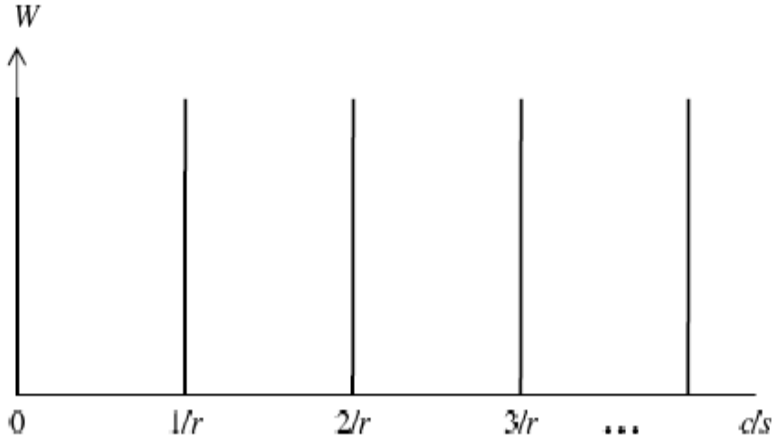


Рис. **3.10**

Таким образом, успешное решение задачи факторизации большого числа $M \sim 2^n$ может быть реализовано за *полиномиальное* число шагов с вероятностью, сколь угодно близкой к единице.

Задачи

1. Пусть $c=pq$, где p и q – простые числа, $\varphi(c) = (p-1)(q-1)$, а число t взаимно простое с $\varphi(c)$. Пусть далее $T^t=M(\mathrm{mod}\ c)$. Доказать, что имеет место равенство $M^m(\mathrm{mod}c)=T$, если $mt = 1(\mathrm{mod}\,\varphi(c))$.

Доказательство

Сначала покажем, что $\varphi(c)$ есть функция Эйлера, которая определяется как число положительных целых чисел, меньших c и взаимно простых с c. Действительно, $c = pq$, где p и q – простые числа. Поэтому делителями c являются все числа, кратные p, т.е. p, $2p$, …, $p(q–1)$, а также все числа, кратные q, т.е. q, $2q$, …, $q(p–1)$. Таким образом, число делителей c есть $q–1+p–1=q+p–2$. Остальные числа, которых $pq–1–(q+p–2) = (p–1)(q–1) \equiv \varphi(c)$ штук, будут

взаимно простые с c. Итак, $\varphi(c)$ есть функция Эйлера. Так как $T^t=M(\mathrm{mod}\ c)$, то интересующая нас величина имеет вид

$$M^m(\mathrm{mod}\ c)= T^{mt}(\mathrm{mod}\ c).$$

Из соотношений $mt=1(\mathrm{mod}\,\varphi(c))$ следует, что $mt=1+k\varphi(c)$, где k — целое число. Тогда

$$T^{mt}(\mathrm{mod}\ c) = T^{1+k\varphi(c)}(\mathrm{mod}\ c) = T(T^{\varphi(c)})^k\ (\mathrm{mod}\ c)\,.$$

Рассмотрим случай, когда T и c взаимно простые, т.е. T не делится на c. Поэтому надо вычислить величину $T^{\varphi(c)}$ (mod c). Для этого применим теорему Эйлера, которая гласит, что если T и c взаимно простые, то $T^{\varphi(c)}=1(\mathrm{mod}\ c)$, где $\varphi(c)$ – функция Эйлера. Очевидно, что $(T^{\varphi(c)})^k=1(\mathrm{mod}\ c)$. Таким образом, окончательно соотношение имеет вид $M^m(\mathrm{mod}\ c)=T$, что требовалось доказать.

Случай, когда T и c не являются взаимно простыми, предполагается для самостоятельной работы.

2. Доказать, что матрица дискретного преобразования Фурье

$$F_{xy} = \frac{1}{\sqrt{N}}\exp(2\pi i\frac{xy}{N}),$$

где x, y – целые неотрицательные числа, пробегающие значения от 0 до N–1, является унитарной.

Доказательство

Эрмитово сопряженная матрица имеет вид

$$(\hat{F}^+)_{xy} = F_{yx}^{\ *} = F_{xy}^{\ *} = \frac{1}{\sqrt{N}}\exp(-2\pi i\frac{xy}{N})\ .$$

Тогда для матричных элементов произведения матриц $\hat{F}\,\hat{F}^+$

получаем

$$(\hat{F}\ \hat{F}^{+})_{xy}=\sum_{z=0}^{N-1}\hat{F}_{xz}\ \hat{F}_{zy}^{*}=\sum_{z=0}^{N-1}\ \frac{1}{N}\exp(2\pi i\frac{x-y}{N}z)=$$

$$=\frac{1}{N}\frac{1-\exp(2\pi i(x-y))}{1-\exp(2\pi i\frac{(x-y)}{N})}=\delta_{xy}.$$

Действительно, если $x\neq y$, то $1\leq|x-y|\leq N-1$. Поэтому числитель равен нулю, а знаменатель отличен от нуля. Следовательно, матричные элементы при $x\neq y$ обращаются в нуль. Если $x = y$, то такие матричные элементы равны единице. Итак, имеем $\hat{F}\hat{F}^{+}=1$, т.е. матрица $\hat{F}$ является унитарной.

3.4. Корреляции ЭПР–Белла в квантовых коммуникационных схемах

Корреляции ЭПР – Белла

Рассмотрим корреляционные свойства перепутанных состояний двух квантовых систем. В историческом плане побудительной мотивацией тщательного анализа этих свойств послужил парадоксальный мысленный эксперимент, предложенный в 1935 г. Эйнштейном – Подольским – Розеном (ЭПР). В нем шла речь о системе двух частиц, которые находятся в состоянии, перепутанном по пространственным степеням свободы. При этом ни координата, ни импульс каждой частицы не определены, но координата центра инерции и разность импульсов, которым отвечают коммутирующие операторы, имеют определенные значения. Поэтому, измерив координату, например, второй частицы, мы достоверно можем предсказать координату первой. То же самое относится и к импульсам – измерение импульса одной частицы позволяет однозначно предсказать импульс другой частицы. Эти утверждения находятся в полном соответствии с квантово-механическим описанием перепутанных состояний. Свой вывод о том, что квантовые состояния в общем случае не могут быть полным описанием физи-

ческой системы, авторы делают, опираясь на такие понятия как «элемент физической реальности» и «локальность», которые были ими сформулированы в качестве необходимых атрибутов полной физической теории. Если частицы находятся достаточно далеко друг от друга, то взаимодействия между ними нет. Поэтому реальные свойства одной частицы не могут зависеть, по мнению авторов, от того, что происходит с ее удаленным партнером. В этом суть «локальности». Если можно, не возмущая систему, с достоверностью предсказать результат измерения некоторой физической величины, то эта характеристика является «элементом физической реальности». Оба эти понятия сейчас принято рассматривать под общим названием «локального реализма». В рассмотренном выше мысленном эксперименте ЭПР координата и импульс частицы, как считают авторы, обладают всеми признаками таких хорошо определенных характеристик состояния частицы, которые существуют независимо от наблюдения. Другими словами, они описывают свойства системы, которые существуют до измерения и независимо от него. Это противоречит квантовой механике, в которой такое описание принципиально невозможно. Данную ситуацию иногда называют «парадоксом ЭПР», хотя вся парадоксальность проистекает из того, что интуитивные классические представления применяются в области квантовых явлений. Экспериментальная проверка «локального реализма» была важна не только для понимания оснований квантовой механики, но и явилась, фактически, первым откровением в той физической реальности, которую мы называем квантовой информацией.

В оригинальной работе ЭПР речь шла о перепутывании состояний поступательного движения, достаточно трудных для тонких корреляционных измерений. В 1951 г. *Дэвид Бом* предложил рассматривать системы, перепутанные по спиновым состояниям двух частиц со спином 1/2. Эти системы существенно проще, а аргументация ЭПР легко переносится на спиновые состояния. Измеряя проекцию спина одной из частиц, можно с достоверностью предсказать значение проекции спина другой частицы, которая находится от нее достаточно далеко, так что взаимодействие отсутствует. Тогда указанная проекция является элементом реальности. Такое же утверждение справедливо и в отношении проекций на другие оси, что противоречит квантовой механике, так как состояний

с определенными проекциями спина на разные оси не существует.

В 1964 г. *Джон Белл* сформулировал утверждение, известное как *неравенство Белла*, которое является математическим выражением различия между предсказаниями результатов измерения коррелирующих величин, сделанными на основе квантовой механики и исходя из классических представлений, опирающихся на "локальный реализм". Существует много различных модификаций неравенств Белла. Мы рассмотрим одну из них, которая была предложена в 1969 г. *Д. Клаузером*, *М. Хорном*, *А. Шимони* и *Р. Хольтом* и лежит в основе многочисленных экспериментальных проверок.

Пусть имеется некоторый источник, генерирующий пары частиц, находящихся в том или ином состоянии. Одна из частиц попадет к Алисе, а другая – к Бобу. Каждый из них производит над своей частицей измерения некоторых физических характеристик, например, проекций спина на какие-то оси. Алиса случайным образом производит измерения, которые мы назовем F и G. Результатом измерения каждой из этих величин пусть будут числа ± 1. Подчеркнем, что в рамках классических представлений каждый из этих результатов есть элемент реальности, характеризующий данную частицу. Аналогично, Боб случайным образом производит какие-то другие измерения, J и K, результатом которых тоже могут быть числа ± 1. Считаем, что события измерения являются абсолютно удаленными и не могут влиять друг на друга.

Результаты измерений, которые мы будем обозначать теми же буквами – F и G у Алисы, J и K у Боба, зависят от исходного состояния пары частиц, но не зависят от процесса измерения. При многократном повторении процедуры можно говорить о вероятности $W(F, G, J, K)$ того, что перед измерением система находилась в состоянии с указанными значениями величин F, G, J и K, которые потом были обнаружены в результате измерений. Рассмотрим теперь величину

$$FJ + GJ + GK - FK \;=\; (F + G)J + (G - F)K\,, \qquad (3.81)$$

которая характеризует корреляционные свойства результатов измерений. Так как F, G, J и K принимают значения, равные ± 1, то

$$|FJ + GJ + GK - FK| = 2. \tag{3.82}$$

Поэтому для среднего значения величины (3.81) получаем

$$\begin{aligned}
&\left|< FJ + GJ + GK - FK >\right| = \left|< FJ > + < GJ > + < GK > - < FK >\right| = \\
&= \left| \sum_{F,G,J,K} W(F,G,J,K)(FJ + GJ + GK - FK) \right| \le \\
&\le \sum_{F,G,J,K} W(F,G,J,K)\left|FJ + GJ + GK - FK\right| = 2\sum W = 2.
\end{aligned}$$

Таким образом, имеем следующее обобщенное неравенство Белла (его называют неравенством КХШХ):

$$\left|< FJ > + < GJ > + < GK > - < FK >\right| \le 2, \tag{3.83}$$

в левой части которого стоит величина, характеризующая корреляционные свойства результатов измерений, проводимых Алисой и Бобом над состояниями пары частиц.

В качестве квантового объекта будем рассматривать ЭПР-пару, т.е. двухкубитовую систему, находящуюся в максимально перепутанном состоянии, полный набор которых записывается в виде четырех состояний Белла (2.162)–(2.163):

$$\begin{aligned}
\left|\Phi^{(\pm)}\right\rangle &= \frac{1}{\sqrt{2}}\left(\left|00\right\rangle \pm \left|11\right\rangle\right), \\
\left|\Psi^{(\pm)}\right\rangle &= \frac{1}{\sqrt{2}}\left(\left|01\right\rangle \pm \left|10\right\rangle\right).
\end{aligned} \tag{3.84}$$

Пусть квантовая система находится в состоянии $\left|\Psi^{(-)}\right\rangle$, а Алиса и Боб получают по одному кубиту этой ЭПР-пары.

Измерениям F и G, которые выполняет Алиса, отвечают эрмитовые операторы

$$\hat{F} = \sigma_3^{(1)}, \quad \hat{G} = \sigma_1^{(1)}, \tag{3.85}$$

действующие на первый кубит. Измерениям Боба соответствуют эрмитовые операторы

$$\hat{J} = -\frac{1}{\sqrt{2}}\left(\sigma_1^{(2)} + \sigma_3^{(2)}\right), \quad \hat{K} = \frac{1}{\sqrt{2}}\left(\sigma_3^{(2)} - \sigma_1^{(2)}\right), \tag{3.86}$$

действующие на второй кубит. Поскольку квадраты всех операторов, указанных в (3.85) и (3.86), равны единице, то собственные значения этих операторов равны ± 1. Вычисляя квантово-механические средние значения в состоянии $\left|\Psi^{(-)}\right\rangle$ тех же величин, что стоят слева в (3.83), получаем:

$$\left\langle \hat{F}\hat{J} \right\rangle = \left\langle \Psi^{(-)} \left| -\sigma_3^{(1)} \frac{\sigma_1^{(2)} + \sigma_3^{(2)}}{\sqrt{2}} \right| \Psi^{(-)} \right\rangle = \frac{1}{\sqrt{2}},$$

$$\left\langle \hat{G}\hat{J} \right\rangle = \left\langle \Psi^{(-)} \left| -\sigma_1^{(1)} \frac{\sigma_1^{(2)} + \sigma_3^{(2)}}{\sqrt{2}} \right| \Psi^{(-)} \right\rangle = \frac{1}{\sqrt{2}},$$

$$\left\langle \hat{G}\hat{K} \right\rangle = \left\langle \Psi^{(-)} \left| \sigma_1^{(1)} \frac{\sigma_3^{(2)} - \sigma_1^{(2)}}{\sqrt{2}} \right| \Psi^{(-)} \right\rangle = \frac{1}{\sqrt{2}},$$

$$\left\langle \hat{F}\hat{K} \right\rangle = \left\langle \Psi^{(-)} \left| \sigma_3^{(1)} \frac{\sigma_3^{(2)} - \sigma_1^{(2)}}{\sqrt{2}} \right| \Psi^{(-)} \right\rangle = -\frac{1}{\sqrt{2}}.$$

Тогда комбинация квантово-механических средних

$$\left\langle \hat{F}\hat{J} \right\rangle + \left\langle \hat{G}\hat{J} \right\rangle + \left\langle \hat{G}\hat{K} \right\rangle - \left\langle \hat{F}\hat{K} \right\rangle = 2\sqrt{2}, \tag{3.87}$$

характеризующая корреляционные свойства результатов измерений, заметно выходит за рамки классического неравенства (3.83).

Таким образом, уровень корреляций между подсистемами, находящимися в перепутанном квантовом состоянии, может превышать тот теоретический уровень корреляций, который определяется на основании любого физического закона, описывающего поведение частиц с помощью классических переменных, а не квантовых состояний.

Тот факт, что в квантовой механике возможна более высокая степень корреляции между подсистемами, недостижимая в классическом мире, проверен и подтвержден в целом ряде изящных экспериментов. Обратим внимание также, что в контексте поставленного Ричардом Фейнманом вопроса о моделировании физики на компьютерах мы видим в рассмотренной системе физическую реальность, поведение которой не может быть смоделировано, даже в принципе, ни на каком классическом компьютере.

Протокол квантовой плотной кодировки

Как уже неоднократно подчеркивалось, состояния Белла (3.84) являются максимально перепутанными состояниями двух кубитов. Измерение состояния любого кубита в базисе $|0\rangle$, $|1\rangle$ в каждом из четырех состояний Белла приводит к случайному результату, 0 или 1, с вероятностью 1/2. При этом каждый результат совместного измерения двух кубитов в том же базисе обладает максимальной степенью корреляции.

Поскольку проекция спина каждой из двух максимально перепутанных частиц на любую ось является совершенно случайной величиной, то квантовая информация, которую хранят два спиновых кубита, оказывается как бы спрятанной, если она закодирована с помощью состояний вычислительного базиса $|0\rangle$, $|1\rangle$. Эту ситуацию нельзя изменить путем перехода к любому другому базису однокубитовых состояний. Как было показано в разделе 2.4, перепутанное состояние нельзя факторизовать с помощью однокубитовых унитарных операций. Оно остается максимально перепутанным. Напомним, что в случае факторизованного двухкубитового состояния каждый кубит описывается некоторым кэт-вектором, т.е. спин частицы ориентирован вдоль какой-то оси. Измерение проекции спина на эту ось с достоверностью дает определенный резуль-

тат. Поэтому с помощью такого состояния можно хранить один кубит квантовой информации, а вся двухкубитовая система будет хранить два кубита квантовой информации, записанных в явном виде.

Вернемся к перепутанным состояниям Белла. В этом случае можно выделить два кубита квантовой информации, которые записаны в явном виде, но с помощью двухчастичных состояний. Такими кубитами являются кубит "четности" P и кубит "фазы" Σ. Определим два значения P как сонаправленность и противонаправленность двух спинов, которые имеют место в состояниях $\left|\Psi\right\rangle$ и $\left|\Phi\right\rangle$ соответственно. Формально это соответствует двум собственным значениям $P=\pm 1$ эрмитового оператора

$$\hat{P}=\sigma_3^{(1)}\sigma_3^{(2)}, \tag{3.88}$$

в котором верхние индексы 1 и 2 указывают, на какой кубит они действуют. Подействовав этим оператором на состояния (3.84), получаем

$$\begin{aligned}\hat{P}\left|\Phi^{(\pm)}\right\rangle &= \left|\Phi^{(\pm)}\right\rangle,\\ \hat{P}\left|\Psi^{(\pm)}\right\rangle &= -\left|\Psi^{(\pm)}\right\rangle.\end{aligned} \tag{3.89}$$

Два значения Σ кубита фазы соответствуют двум знакам "+" и "–", которые стоят между слагаемыми в выражениях (3.84). Они отвечают двум собственным значения $\Sigma=\pm 1$ эрмитового оператора

$$\hat{\Sigma}=\sigma_1^{(1)}\sigma_1^{(2)}. \tag{3.90}$$

Подействовав этим оператором на состояние (3.84), получаем

$$\begin{aligned}\hat{\Sigma}\left|\Phi^{(+)}\right\rangle &= \left|\Phi^{(+)}\right\rangle,\\ \hat{\Sigma}\left|\Psi^{(+)}\right\rangle &= \left|\Psi^{(+)}\right\rangle,\\ \hat{\Sigma}\left|\Phi^{(-)}\right\rangle &= -\left|\Phi^{(-)}\right\rangle,\\ \hat{\Sigma}\left|\Psi^{(-)}\right\rangle &= -\left|\Psi^{(-)}\right\rangle.\end{aligned} \tag{3.91}$$

Чтобы получить полную информацию о двухчастичном перепутанном состоянии, надо, очевидно, произвести совместное измерение состояния двух частиц, используя, например, полный базис состояний Белла. Но получить полную информацию, измеряя состояния кубитов по отдельности, невозможно. В то же время, можно произвольно манипулировать перепутанными состояниями, воздействуя только на одну из подсистем. Например, при применении операции $\sigma_3^{(1)}$ обращения относительной фазы (2.60) первого кубита происходит изменение кубита, закодированного в фазе перепутанного состояния:

$$\sigma_3^{(1)} \left|\Phi^{(\pm)}\right\rangle = \left|\Phi^{(\mp)}\right\rangle,$$
$$\sigma_3^{(1)} \left|\Psi^{(\pm)}\right\rangle = \left|\Psi^{(\mp)}\right\rangle. \qquad (3.92\textbf{а})$$

Если применить операцию $\sigma_1^{(1)}$ (2.56), которая инвертирует первый кубит, то в результате произойдет изменение кубита четности двухкубитовой системы:

$$\sigma_1^{(1)} \left|\Phi^{(\pm)}\right\rangle = \pm \left|\Psi^{(\pm)}\right\rangle. \qquad (3.92\textbf{б})$$

В общем случае любое локальное манипулирование одним из кубитов максимально перепутанного состояния позволяет получить какое-то другое максимально перепутанное состояние.

Указанное свойство имеет важные применения и лежит в основе так называемой *квантовой плотной кодировки*, предложенной *Чарльзом Беннетом* и *Стефаном Визнером* в 1992 г.

Суть этого протокола заключается в том, что его участники – Алиса и Боб – используют источник ЭПР-пар, находящихся, например, в перепутанном состоянии $\left|\Phi^{(+)}\right\rangle$, и получают по одной частице из этой пары. После этого у них появляется возможность переслать друг другу один кубит, передав при этом два бита информации.

Реализуется протокол следующим образом.

Пусть два бита информации кодируются с помощью состояний Белла следующим образом:

$$\begin{aligned} 00 &\leftrightarrow \left|\Phi^{(+)}\right\rangle \quad \Leftrightarrow \quad P=1, \quad \Sigma=1, \\ 01 &\leftrightarrow \left|\Phi^{(-)}\right\rangle \quad \Leftrightarrow \quad P=1, \quad \Sigma=-1, \\ 10 &\leftrightarrow \left|\Psi^{(+)}\right\rangle \quad \Leftrightarrow \quad P=-1, \quad \Sigma=1, \\ 11 &\leftrightarrow \left|\Psi^{(-)}\right\rangle \quad \Leftrightarrow \quad P=-1, \quad \Sigma=-1. \end{aligned} \tag{3.93}$$

Если Алиса хочет передать Бобу сообщение, содержащее два бита информации, то она локально манипулирует своим кубитом с помощью операций (3.92) и переводит общее для нее с Бобом состояние $\left|\Phi^{(+)}\right\rangle$ в любое из *четырех* состояний Белла, которые отвечают двухбитовым двоичным строкам, указанным в (3.93) слева. Потом она передает свой *один кубит* Бобу. Получив его, Боб производит совместное измерение состояния двух частиц в базисе состояний Белла и узнает, какое из них было создано Алисой. Тем самым, он получает *два бита* информации – бит четности и бит фазы, указанные в (3.93).

Отметим также, что помимо увеличения плотности канала такой протокол обеспечивает конфиденциальность передачи, так как злоумышленник, перехватывающий кубит Алисы, не сможет ничего узнать о передаваемом сообщении. Перехваченный кубит является одним из партнеров ЭПР-пары, и его состояние не содержит никакой информации. Оно описывается не вектором состояния, а матрицей плотности.

Квантовое распределение ключа

Одним и, наверное, единственным практическим успехом квантовой информатики на сегодняшний день стало появление квантовой криптографии. В настоящий момент существуют и коммерчески доступны устройства квантовой криптографии, созданные на описанном в данном разделе принципе.

Задача криптографии заключается в защите от прослушивания

сообщения при передаче его по незащищенному каналу. Решение заключается в том, что нужно предварительно обменяться секретными данными – ключом – и использовать его для передачи сообщения, применяя шифрование — некое математическое преобразование над самим сообщением и ключом. Доказано, что такой подход может обеспечить абсолютную надежность при условии, что размер ключа не меньше размера самого передаваемого сообщения[1]. Неудобство такого подхода вполне очевидно. Поэтому на практике применяется компромиссный метод, при котором ключ существенно меньше сообщения, но при этом характер используемых криптопреобразований таков, что не существует алгоритма, который позволил бы за приемлемое для взломщика время восстановить исходное сообщение из подслушанных им данных. Описанный практический подход в настоящий момент широко распространен и имеет множество успешных реализаций. Тем не менее, такой подход в корне порочен. Вся надежность алгоритмов криптопреобразований зиждется на том, что наилучший из *известных* алгоритмов гарантирует, что на взлом уйдет больше упомянутого приемлемого времени. Из этого следует, по крайней мере, две очевидные проблемы:

1). Если злоумышленнику известен улучшенный алгоритм, то данные, передаваемые с использованием существующей схемы криптографии, для него не являются секретными.

2). Если даже на сегодняшний день такой улучшенный алгоритм не известен и не доступны компьютеры, которые позволили бы взломать системы шифрования за приемлемое время, то нет гарантии того, что, сохранив само зашифрованное сообщение, злоумышленник не дождется той поры, когда или возникнут более мощные алгоритмы криптоанализа, или быстродействие компьютеров значительно возрастет. В мире существует большое количество информации, ценность которой за это время сохранится, и вопрос ее защиты не потеряет актуальности.

Для решения этих проблем был предложен метод, впервые сформулированный *Чарльзом Беннетом* и *Стефаном Визнером* в

[1] В этом случае можно воспользоваться простейшим алгоритмом: перед передачей сложить секретное сообщение с ключом побитно по модулю два.

1984 г., который называется *квантовым распределением ключа*[1]. Суть его в том, что для определения случайного секретного ключа для криптографии используются квантовые состояния.

Мы рассмотрим предложенный *Артуром Экертом* в 1991 г. протокол квантового распределения ключа с использованием ЭПР-пар. Предположим, что Алисе и Бобу нужно обменяться ключом для шифрования секретных сообщений. Для этого они используют источник частиц, находящихся в перепутанном состоянии. Для определенности будем говорить о парах частиц, находящихся в перепутанном по спинам состоянии Белла (2.164)

$$\left|\Psi^{(-)}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|\frac{1}{2}\right\rangle_1\left|-\frac{1}{2}\right\rangle_2 - \left|-\frac{1}{2}\right\rangle_1\left|\frac{1}{2}\right\rangle_2\right) \equiv \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right).$$

Алиса и Боб получают по одной частице из ЭПР-пары и измеряют проекции спина на одну из трех возможных для каждого из них осей. Эти оси, для простоты, лежат в плоскости $\{zy\}$ и отличаются углом поворота вокруг оси x общей системы координат. Для Алисы список углов включает

$$\varphi_1^{\text{а}} = 0, \quad \varphi_2^{\text{а}} = \frac{\pi}{2}, \quad \varphi_3^{\text{а}} = \frac{\pi}{4}, \tag{3.94}$$

а для Боба

$$\varphi_1^{\text{б}} = 0, \quad \varphi_2^{\text{б}} = -\frac{\pi}{4}, \quad \varphi_3^{\text{б}} = \frac{\pi}{4}. \tag{3.95}$$

Для каждого измерения Алиса и Боб выбирают направление оси случайным образом и независимо друг от друга. Как мы увидим, достаточно сложная процедура с выбором осей для измерений необходима для защиты от “подслушивания”.

[1] В англоязычной литературе встречается аббревиатура QKD – Quantum Key Distribution.

После того как серия измерений завершена, Алиса и Боб обмениваются информацией о том, на какие оси они производили измерения. После этого результаты измерений разделяются на две группы. В первую группу попадают результаты тех измерений, когда Алиса и Боб выбрали одинаковые оси, т.е. углы либо φ_1, либо φ_3. Во всех остальных случаях оси различаются, и результаты относятся ко второй группе. Для первой группы измерений в состоянии $\left|\Psi^{(-)}\right\rangle$ результаты должны быть строго антикоррелированы. В разделе 2.4 мы подробно обсудили свойства состояния $\left|\Psi^{(-)}\right\rangle$ и показали, что результаты измерений проекций спина каждой из частиц на любую ось являются противоположными – если одна проекция равна +1/2, то другая будет –1/2, и наоборот. Эти антикоррелированные результаты можно рассматривать как искомый секретный ключ. Нужно только убедиться, что во время передачи не имели место прослушивание или какое-то вмешательство в процесс передачи. Для этого используются результаты из второй группы, когда Алиса и Боб выбирали при измерении различные оси. На основе этих данных Алиса и Боб проверяют наличие корреляций ЭПР-Белла в данной группе результатов. Этот вопрос является основной целью данного раздела.

Коэффициент корреляции результатов измерений, отвечающих углу $\varphi_i^{\text{а}}$, выбранному Алисой, и углу $\varphi_j^{\text{б}}$, выбранному Бобом, определяется выражением:

$$E(\varphi_i^{\text{а}}, \varphi_j^{\text{б}}) = P_{++}(\varphi_i^{\text{а}}, \varphi_j^{\text{б}}) + P_{--}(\varphi_i^{\text{а}}, \varphi_j^{\text{б}}) - \\ - P_{+-}(\varphi_i^{\text{а}}, \varphi_j^{\text{б}}) - P_{-+}(\varphi_i^{\text{а}}, \varphi_j^{\text{б}}). \tag{3.96}$$

Он представляет собой сумму вероятностей одинаковых результатов измерений, когда обе проекции равны +1/2 или –1/2, из которых вычтена сумма вероятностей противоположных результатов, когда одна проекция равна +1/2, а другая –1/2.

Вычислим величины $P_{\pm\pm}(\varphi_i^{\text{а}}, \varphi_j^{\text{б}})$, которые представляют собой вероятности того, что та или иная комбинация результатов ±1/2

может быть получена Алисой или Бобом при измерении проекций спинов на оси, заданные углами $\varphi_i^{\text{а}}$ и $\varphi_j^{\text{б}}$. Измерение происходит для системы двух спинов, находящихся в состоянии $\left|\Psi^{(-)}\right\rangle$. Напомним, что, с физической точки зрения, это есть синглетное состояние с нулевым суммарным спином. Оно является скаляром и инвариантно относительно вращений. Оси, на которые измеряются проекции спинов, в общем случае не совпадают и образуют угол $\theta = \varphi_i^{\text{а}} - \varphi_j^{\text{б}}$. Заметим также, что они могут не совпадать с осью квантования *z*, выбранной для классификации одночастичных базисных состояний $\left|\pm 1/2\right\rangle$.

Физически, однако, понятно, что интересующие нас вероятности совпадения или несовпадения результатов измерений могут зависеть только от угла θ между осями измерительного базиса, а не от их ориентации относительно оси *z*, так как синглетное состояние $\left|\Psi^{(-)}\right\rangle$ не меняется при вращениях системы координат. Поэтому без ущерба для общности можно считать, что выбранная Бобом ось совпадает с осью квантования *z*, а ось его партнера Алисы образует с осью *z* угол θ.

Пусть θ=0, так что Алиса и Боб измеряют проекции спинов на одну и ту же ось. Поскольку в синглетном состоянии $\left|\Psi^{(-)}\right\rangle$ проекции спинов на любую ось противоположны, то вероятность получения совпадающих результатов есть

$$W_c = P_{\frac{1}{2}\frac{1}{2}}(\varphi_i^{\text{а}} = \varphi_j^{\text{б}}) + P_{-\frac{1}{2}-\frac{1}{2}}(\varphi_i^{\text{а}} = \varphi_j^{\text{б}}) = 0\,, \quad (3.97)$$

а вероятность получение разных результатов равна

$$W_a = P_{\frac{1}{2}-\frac{1}{2}}(\varphi_i^{\text{а}} = \varphi_j^{\text{б}}) + P_{-\frac{1}{2}\frac{1}{2}}(\varphi_i^{\text{а}} = \varphi_j^{\text{б}}) = 1 - W_c = 1\,. \quad (3.98)$$

Поэтому для первой группы измерений, когда выбирались одинаковые оси, имеет место полная антикорреляция результатов,

т.е.

$$E(\varphi_1^{\text{а}}, \varphi_1^{\text{б}}) = E(\varphi_3^{\text{а}}, \varphi_3^{\text{б}}) = -1\,. \qquad (3.99)$$

В случае произвольного угла θ можно совершить преобразование поворота первого спина, который находится у Алисы, на угол θ так, чтобы выбранная ею ось совпала с осью квантования. Это преобразование описывается унитарным оператором

$$\hat{R}(\theta) = \exp(i\frac{\theta}{2}\sigma_1^{(1)}) = \cos\frac{\theta}{2} + i\sin\frac{\theta}{2}\sigma_1^{(1)}\,. \qquad (3.100)$$

Здесь для простоты считается, что поворот происходит вокруг оси *x*. Поэтому в (3.100) вошла матрица Паули $\sigma_1^{(1)} \equiv \sigma_x$. Применяя это преобразовании к состоянию $\left|\Psi^{(-)}\right\rangle$, получаем

$$\begin{aligned}
&\hat{R}(\theta)\left|\Psi^{(-)}\right\rangle = \left(\cos\frac{\theta}{2} + i\sin\frac{\theta}{2}\sigma_1^{(1)}\right)\left|\Psi^{(-)}\right\rangle = \\
&= \cos\frac{\theta}{2}\left|\Psi^{(-)}\right\rangle + i\sin\frac{\theta}{2}\sigma_1^{(1)}\left|\Psi^{(-)}\right\rangle = \\
&= \cos\frac{\theta}{2}\left|\Psi^{(-)}\right\rangle - i\sin\frac{\theta}{2}\left|\Phi^{(-)}\right\rangle.
\end{aligned} \qquad (3.101)$$

Поскольку состояние $\left|\Psi^{(-)}\right\rangle$ дает 100 % антикорреляцию результатов, а состояние $\left|\Phi^{(-)}\right\rangle$, в которое входят однонаправленные спины, означает полную корреляцию результатов, то искомые вероятности имеют вид

$$\begin{aligned}
&W_c\left(\theta = \varphi_i^{\text{а}} - \varphi_j^{\text{б}}\right) = P_{\frac{1}{2}\frac{1}{2}}(\varphi_i^{\text{а}} - \varphi_j^{\text{б}}) + P_{-\frac{1}{2}-\frac{1}{2}}(\varphi_i^{\text{а}} - \varphi_j^{\text{б}}) = \sin^2\frac{\theta}{2} \\
&W_a\left(\theta = \varphi_i^{\text{а}} - \varphi_j^{\text{б}}\right) = P_{\frac{1}{2}-\frac{1}{2}}(\varphi_i^{\text{а}} - \varphi_j^{\text{б}}) + P_{-\frac{1}{2}\frac{1}{2}}(\varphi_i^{\text{а}} - \varphi_j^{\text{б}}) = \\
&= 1 - W_c = \cos^2\frac{\theta}{2}.
\end{aligned} \qquad (3.102)$$

Тогда коэффициент корреляции (3.96) равен

$$E(\varphi_i^{\text{а}}, \varphi_j^{\text{б}}) = \sin^2 \frac{\varphi_i^{\text{а}} - \varphi_j^{\text{б}}}{2} - \cos^2 \frac{\varphi_i^{\text{а}} - \varphi_j^{\text{б}}}{2} = -\cos\left(\varphi_i^{\text{а}} - \varphi_j^{\text{б}}\right). \quad (3.103)$$

Отсюда, в частности, для первой группы измерений, когда $\varphi_i^{\text{а}} = \varphi_j^{\text{б}}$, получаем соотношение (3.99), т.е. полную антикорреляцию результатов.

Для определения факта прослушивания можно вычислить величину

$$S = E(\varphi_1^{\text{а}}, \varphi_3^{\text{б}}) + E(\varphi_1^{\text{а}}, \varphi_2^{\text{б}}) + E(\varphi_2^{\text{а}}, \varphi_3^{\text{б}}) - E(\varphi_2^{\text{а}}, \varphi_2^{\text{б}}), \quad (3.104)$$

составленную из коэффициентов корреляции (3.103) результатов измерений из второй группы, когда Алиса и Боб использовали разные оси. Вычисляя коэффициенты (3.103) для пар углов из (3.94) и (3.95), получаем

$$S = -3\cos\frac{\pi}{4} - \sin\frac{\pi}{4} = -2\sqrt{2}. \quad (3.105)$$

Это есть предсказание квантовой механики. Факт прослушивания, если он имел место, приводит к разрушению квантовых корреляций, и величина $|S|$ становится существенно меньше. В выражение (3.104) входят результаты измерений проекций спина на две разные оси, которые выполняет Алиса (углы $\varphi_2^{\text{а}}$ и $\varphi_1^{\text{б}}$), и результаты аналогичных измерений, но на другие оси, проводимые Бобом (углы $\varphi_2^{\text{а}}$ и $\varphi_3^{\text{б}}$). Это соответствует той ситуации, которую мы обсуждали в связи с неравенством КХШХ (3.83). В случае полного отсутствия квантовых корреляций из этого неравенства следует, что $|S| \le 2$. В действительности ограничение оказывается даже более сильным.

Таким образом, факт “прослушивания” может быть установлен из анализа величины (3.104), которая характеризует степень квантовых корреляций ЭПР-Белла в перепутанном состоянии $\left|\Psi^{(-)}\right\rangle$.

Для практического применения гораздо больший интерес представляют ЭПР-пары фотонов, перепутанных по поляризационным состояниям.

Полученные выше результаты сохраняют свою форму, но в них надо сделать преобразование $\varphi \to 2\varphi$ углов. Это связано с тем, что фотон является векторным полем, которое преобразуется при поворотах системы координат по представлению момента 1 , а в полученных формулах использовано преобразование спина S=1/2.

С помощью поляризационных кубитов различные модификации протоколов квантового распределения ключа были реализованы экспериментально на значительные расстояния по волоконно-оптическим линиям связи. Недавно большой международный коллектив авторов сообщил об успешной экспериментальной реализации квантового протокола передачи ключа на расстояние 144 км между Канарскими островами Ла Пальма и Тенерифе. С помощью двух телескопов, т.е. по каналу связи в свободном пространстве, направлялись слабые когерентные лазерные импульсы. Передача секретного ключа происходила со скоростью 42 бит/с .

Квантовая телепортация

В этом разделе мы обсудим физическую интригу понятия *«квантовая телепортация».* Экспериментальная реализация в 1997 г. процесса квантовой телепортации является одной из принципиальных вех на пути становления всей области квантовой информатики. Этот эффект прочно входит в современный арсенал, как принято говорить, квантовых протоколов.

Теоретическая идея квантовой телепортации была сформулирована *Беннетом*, *Брассардом*, *Крэпо*, *Джозсой*, *Пэрэсом* и *Вуттером* в 1993 г. Они предложили процедуру передачи произвольного и неизвестного *a priori* квантового состояния от одной системы к другой удаленной квантовой системе.

Рис. 3.11 иллюстрирует схему процесса квантовой телепортации с участием традицинных персонажей коммуникационной схемы Алисы и Боба.

Следуя оригинальной работе, рассмотрим простейшую ситуацию, когда у Алисы есть одна частица, например, фотон, находящийся в некотором квантовом состоянии

$$\left|\Phi_1\right\rangle = a\left|v\right\rangle_1 + b\left|h\right\rangle_1 . \qquad (3.106)$$

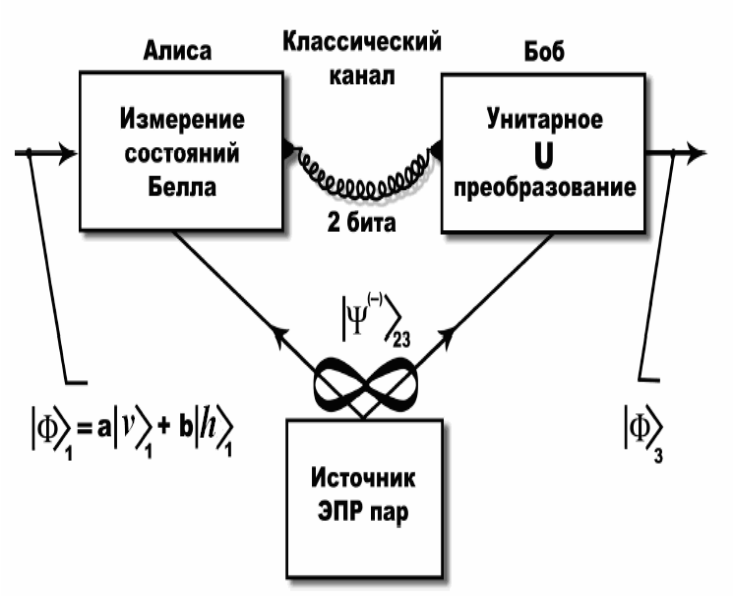


Рис. **3.11**

Здесь мы, имея в виду упомянутый выше эксперимент по квантовой телепортации, рассматриваем два ортогональных поляризационных состояния $|v\rangle$ и $|h\rangle$ фотона, которые являются базисными состояниями кубита. Поэтому $|\Phi_1\rangle$ описывает некоторое общего вида состояние этого кубита. Цель состоит в том, чтобы передать состояние (3.106) Бобу, не передавая ему, естественно, сам данный фотон. Никаких сведений об амплитудах a и b, кроме очевидного факта, что $|a|^2+|b|^2=1$, у Алисы нет. Более того, располагая только одной частицей, Алиса даже в принципе не может получить полную информацию о комплексных коэффициентах a и b. Это вытекает из самого статуса процедуры квантового измерения, которая представляет собой проектирование на то или иное состояние из полного набора базисных векторов. Случайный результат — кликнул или не кликнул детектор — одного акта измерения свидетельствует только о присутствии или отсутствии выбранного базисного состояния в измеряемом состоянии. А повторить измерение уже

нельзя, так как исходное состояние, вообще говоря, разрушается самим процессом первого измерения.

Оказывается, тем не менее, что состояние (3.106) можно передать Бобу. И в этом суть протокола *квантовой телепортации.* Для этого используется вспомогательная пара частиц 2 и 3, находящихся в перепутанном квантовом состоянии. Пусть источник таких ЭПР-пар (Эйнштейн – Подольский – Розен) дает состояние

$$\left|\Psi^{(-)}{}_{23}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|v\right\rangle_2\left|h\right\rangle_3 - \left|v\right\rangle_3\left|h\right\rangle_2\right). \qquad (3.107)$$

Одна из частиц этой пары, например 2, попадает к Алисе, а другая (3) направляется к Бобу. Из выражения (3.107) видно, что ни та, ни другая частица не имеют определенной поляризации. Другими словами, ни одна из частиц не несет информацию о поляризационном состоянии.

Состояние всей трехчастичной системы имеет вид

$$\begin{aligned}\left|\Psi_{123}\right\rangle &= \left|\Phi_1\right\rangle\left|\Psi^{(-)}{}_{23}\right\rangle = \\ &= \frac{1}{\sqrt{2}}\left(a\left|v\right\rangle_1 + b\left|h\right\rangle\right)\left(\left|v\right\rangle_2\left|h\right\rangle_3 - \left|v\right\rangle_3\left|h\right\rangle_2\right).\end{aligned} \qquad (3.108)$$

Разложим это состояние по полному ортонормированному набору состояний Белла

$$\begin{aligned}\left|\Psi^{(\mp)}{}_{12}\right\rangle &= \frac{1}{\sqrt{2}}\left(\left|v\right\rangle_1\left|h\right\rangle_2 \mp \left|h\right\rangle_1\left|v\right\rangle_2\right), \\ \left|\Phi^{(\mp)}{}_{12}\right\rangle &= \frac{1}{\sqrt{2}}\left(\left|v\right\rangle_1\left|v\right\rangle_2 \mp \left|h\right\rangle_1\left|h\right\rangle_2\right)\end{aligned} \qquad (3.109)$$

для пары частиц 1 и 2. Для этого достаточно перемножить все члены в правой части выражения (3.108), а получившиеся двухчастичные состояния $\left|v\right\rangle_1\left|v\right\rangle_2$, $\left|v\right\rangle_1\left|h\right\rangle_2$, $\left|h\right\rangle_1\left|v\right\rangle_2$, $\left|h\right\rangle_1\left|h\right\rangle_2$ выразить через состояния Белла (3.109).

В результате элементарного вычисления получаем

$$\begin{aligned}\left|\Psi_{123}\right\rangle = \frac{1}{2}\Big\{ &-\left(a\left|v\right\rangle_3 + b\left|h\right\rangle_3\right)\left|\Psi^{(-)}{}_{12}\right\rangle - \\ &-\left(a\left|v\right\rangle_3 - b\left|h\right\rangle_3\right)\left|\Psi^{(+)}{}_{12}\right\rangle + \\ &+\left(a\left|h\right\rangle_3 + b\left|v\right\rangle_3\right)\left|\Phi^{(-)}{}_{12}\right\rangle + \left(a\left|h\right\rangle_3 - b\left|v\right\rangle_3\right)\left|\Phi^{(+)}{}_{12}\right\rangle\Big\}.\end{aligned} \tag{3.110}$$

Напоминаем, что Алиса располагает двумя частицами. Одна из них (1) находится в состоянии $\left|\Phi_1\right\rangle$, которое подлежит телепортированию, а другая (2) является одним из партнеров вспомогательной ЭПР-пары. Алиса производит совместное измерение состояния этих двух частиц (1 и 2), используя базис состояний Белла (3.109). Если система детектирования позволяет спроектировать на любое из четырех состояний Белла, то, как видно из выражения (3.110), при любом результате измерения частица 3 будет находиться в состоянии, которое однозначно связано с передаваемым состоянием. Эти состояния суть те векторы, которые стоят в круглых скобках перед каждым состоянием Белла в выражении (3.110). Если, например, в результате измерения Алиса зарегистрировала состояние $\left|\Psi_{12}^{(-)}\right\rangle$, то состояние частицы 3, находящейся у Боба, в точности совпадает с исходным состоянием $\left|\Phi_1\right\rangle$. Если зарегистрировано состояние $\left|\Phi_{12}^{(-)}\right\rangle$, то состояние частицы 3 должно быть подвергнуто унитарному преобразованию σ_1. Тогда оно перейдет в исходное состояние, так как

$$\sigma_1\left(a\left|h\right\rangle_3 + b\left|v\right\rangle_3\right) = a\left|v\right\rangle_3 + b\left|h\right\rangle_3. \tag{3.111}$$

Напомним, что преобразование σ_1 является логическим гейтом *NOT*. В двух оставшихся случаях потребуются, как легко увидеть, однокубитные операции σ_3 и $\sigma_3\sigma_1$ соответственно.

Чтобы завершить протокол квантовой телепортации, Алиса передает Бобу через *классический* канал связи информацию о

результате измерения состояний Белла, а Боб производит соответствующее унитарное преобразование состояния частицы 3, которое в результате будет точно совпадать с исходным состоянием частицы 1. Поскольку Алиса случайным образом получает одно из четырех возможных состояний Белла, то сообщая Бобу полученный результат, она передает ему 2 бита классической информации.

Таким образом, мы видим, что концепция перепутывания квантовых состояний является ключевым элементом квантового канала передачи информации. Еще один принципиально новый момент, проявившийся в квантовой телепортации, состоит в том, что информация о квантовом состоянии может быть физически разложена на две составляющие – сугубо классическую и чисто квантовую, а потом восстановлена из них обратно. Квантовая составляющая «записана» в виде корреляций ЭПР-пары и сама по себе не содержит никакой информации о начальном квантовом состоянии, так же как и классическая составляющая. Однако после того как классическая и квантовая компоненты вновь объединяются, они полностью определяют исходное квантовое состояние.

Список используемой литературы (источники)

1. Китаев А.Ю. Квантовые вычисления: алгоритмы и исправления ошибок //УМН. 1997.–192с.

2. Китаев А., Шень А., Вялый М. Классические и квантовые вычисления. – М.: МЦНМО, ЧеРо, 1999. – 192с.

3. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация /Пер. с англ. – М.: Мир, 2006.–824с.

4. Квантовые вычисления: За и против. – Ижевск: Издательский дом «Удмуртский университет», 1999. – 212с.

5. Квантовый компьютер и квантовые вычисления. – Ижевск: Ижевская республиканская типография, 1999. – 288с.

Физические методы манипулирования квантовой информацией

Глава 4

ФИЗИЧЕСКИЕ МЕТОДЫ МАНИПУЛИРОВАНИЯ КВАНТОВОЙ ИНФОРМАЦИЕЙ

Содержание

Ионная ловушка Пауля. Модель Джейнса-Каммингса-Пауля. Двухкубитовый фазовый гейт. Гейт CNOT. Логические элементы на атомах в резонаторах. Экспериментальная реализация квантовой телепортации.

Данная глава ставит своей целью познакомить читателя с некоторыми физическими процессами и методами, которые используются для манипулирования квантовой информацией. Мы ограничились лишь схематическим описанием нескольких физических систем, поскольку их содержательное обсуждение требует далеко выходящего за рамки данной книги объема сведений из различных разделов современной физики.

4.1. Ионы в ловушке как управляемый квантовый регистр

В этом разделе на примере ионов в линейной ловушке мы рассмотрим вопрос о том, каким образом можно реализовать устройство, которое с помощью логических гейтов манипулирует квантовым регистром, состоящим из кубитов. В принципиальном плане такое логическое устройство является «кирпичиком», который нужен для построения квантового компьютера.

Ионная ловушка Пауля

Система, о которой идет речь, представляет собой цепочку ионов в линейной ловушке Пауля. Это, если угодно, искусственный одномерный кристалл, параметры которого можно варьировать в широких пределах. С одной стороны, ионы обладают богатой структурой внутренних состояний, что позволяет не только выбрать подходящий базис для кубита, но и иметь в распоряжении удобные атомные переходы для управления и считывания кубита, а также сильные переходы для лазерного охлаждения ионов. С дру-

гой стороны, наличие заряда существенно упрощает проблему пространственного удержания ионов в ловушке при соответствующем охлаждении.

Типичная температура ионов, которая требуется для их удержания, должна быть порядка 10^{-3} К. А вот для эффективного применения системы в качестве квантового регистра нужны температуры на два порядка ниже.

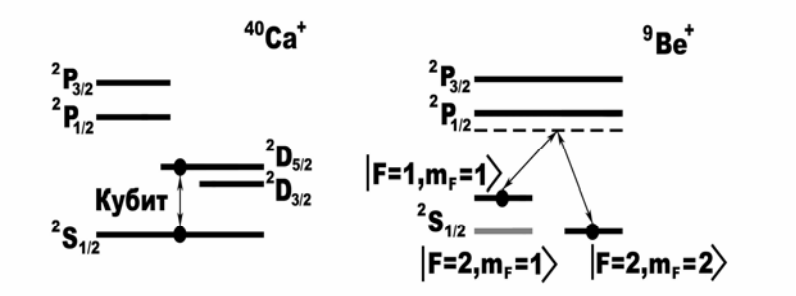


Рис. **4.1**

На рис. 4.1 показана для иллюстрации структура уровней ионов кальция и бериллия. Для ионов $^{40}\mathrm{Ca}^{+}$ базисом кубита могут быть основное состояние $\left|g\right\rangle = \left|{}^{2}S_{1/2}\right\rangle$ и метастабильное возбужденное состояние $\left|e\right\rangle = \left|{}^{2}D_{5/2}\right\rangle$ со временем жизни порядка одной секунды. Кубит показан двумя темными кружками.

Для лазерного охлаждения используется сильный переход ${}^{2}S_{1/2}$ — ${}^{2}P_{1/2}$ (с дополнительной подкачкой на переходе ${}^{2}D_{3/2}$ — ${}^{2}P_{1/2}$. В ионах $^{9}\mathrm{Be}^{+}$ кубитом являются два подуровня сверхтонкой структуры основного состояния. Для управления таким кубитом используется показанный стрелками двухфотонный рамановский переход через промежуточное ${}^{2}P_{1/2}$ состояние посредством двух лазерных пучков.

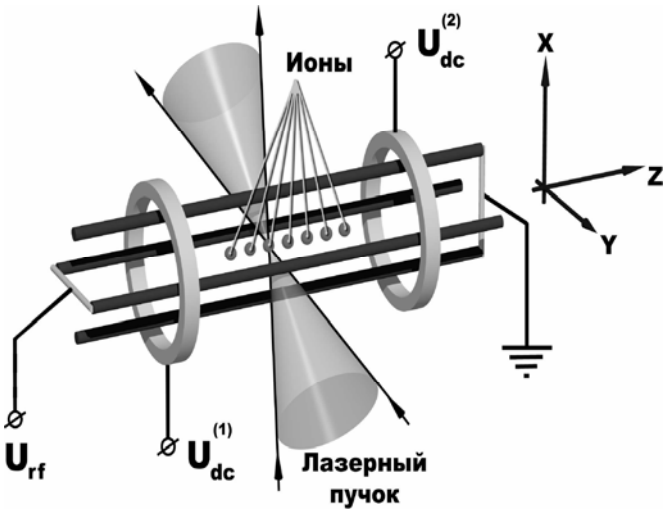


Рис. **4.2**

Один из вариантов линейной ловушки Пауля схематически показан на рис. 4.2. Четыре продольных стержня, к которым приложены постоянный и переменный высокочастотный потенциалы, создают поле с квадрупольной конфигурацией, которое обеспечивает динамическое удержание ионов в поперечном направлении, В направлении оси ловушки ионы удерживаются с помощью электростатического поля, создаваемого кольцевыми электродами. Поперечный линейный размер области конфайнмента гораздо меньше продольного, так что ионы совершают квазиодномерное движение вдоль оси z в поле, которое с хорошей степенью точности описывается потенциалом гармонического осциллятора. Частоты радиальных и продольных колебаний иона, ω_r и ω_z, зависят от конструкционных особенностей той или иной ловушки Пауля. Чтобы дать представление о масштабах этих величин, скажем, например, что в линейной ловушке для ионов кальция, которая работает в Инсбруке, типичные частоты составляют $\omega_r / 2\pi \simeq 1,2\,\text{МГц}$ и $\omega_z / 2\pi \simeq 200$ кГц. Энергия колебательного кванта $\hbar\omega_z$ отвечает температуре порядка 10^{-5} К. Если в ловушку помещены несколько

ионов, то в результате сильного кулоновского отталкивания, которое уравновешивается удерживающим потенциалом, ионы образуют одномерную цепочку. В упомянутой выше линейной ловушке в Инсбруке реализованы цепочки, содержащие несколько десятков ионов, расстояние между которыми составляет порядка 10 мкм. Эта последняя характеристика тоже очень важна, поскольку такие расстояния позволяют воздействовать лазерным излучением на внутренние состояния каждого иона отдельно, т.е. индивидуально управлять каждым кубитом.

Модель Джейнса-Каммингса-Пауля

Напомним некоторые простые сведения из квантовой теории одномерного гармонического осциллятора (см. главу 1). В матричной формулировке такая система описывается гамильтонианом

$$\hat{H}_0 = \hbar\omega(a^+ a + 1/2), \tag{4.1}$$

где $\omega_z \equiv \omega$ и означает частоту колебаний вдоль оси ловушки. Операторы уничтожения a и рождения a^+ подчиняются бозонным коммутационным соотношениям

$$[aa] = [a^+ a^+] = 0, \quad [aa^+] = 1. \tag{4.2}$$

Собственные состояния $|n\rangle$ гамильтониана

$$\hat{H}_0 |n\rangle = \varepsilon_n |n\rangle \tag{4.3}$$

отвечают собственным значениям энергии

$$\varepsilon_n = \hbar\omega(n + 1/2), \quad n = 0,1,2,\ldots \tag{4.4}$$

В рассматриваемой нами ситуации номер квантового состояния n, который принимает целочисленные значения, выступает как число «фононов» – колебательных возбуждений системы. Действие опе-

раторов a и a^+ на собственные энергетические состояния

$$a\left|n\right\rangle = \sqrt{n}\left|n-1\right\rangle, \quad a^+\left|n-1\right\rangle = \sqrt{n}\left|n\right\rangle \tag{4.5}$$

соответствует процессам поглощения или рождения одного элементарного возбуждения.

Ниже нам понадобится выражение для оператора координаты $\hat{z}$ через a и a^+, которое имеет вид

$$\hat{z} = \sqrt{\frac{\hbar}{2M\omega}}(a + a^+). \tag{4.6}$$

Входящая сюда величина $z_0 \equiv \sqrt{\hbar/M\omega}$, где M — масса частицы, является характерным масштабом длины для одномерного гармонического осциллятора. Например, она определяет ширину гауссовского волнового пакета

$$\psi_0(z) \sim \exp\left(-\frac{z^2}{2z_0^2}\right), \tag{4.7}$$

который описывает координатную волновую функцию основного состояния осциллятора.

Цепочка ионов в ловушке может колебаться как целое, без изменений расстояния между частицами. В дальнейшем мы ограничимся рассмотрением именно этого низкочастотного колебания центра инерции. К нему применимы все написанные выше соотношения. Надо только под M понимать массу всей цепочки, а не одного иона. Подчеркнем, что из-за большой массы иона ширина z_0 колебательного волнового пакета, по крайней мере, для не слишком больших n, значительно меньше расстояния между частицами.

Отметим также, что есть и другие, более высокочастотные моды возбуждений, когда расстояние между ионами в цепочке меняется. Такие моды называют «дышащими».

Теперь перейдем к вопросу о функционировании цепочки ионов в качестве логического элемента. Принципы такой схемы были сформулированы Цираком и Цоллером в 1995 г.

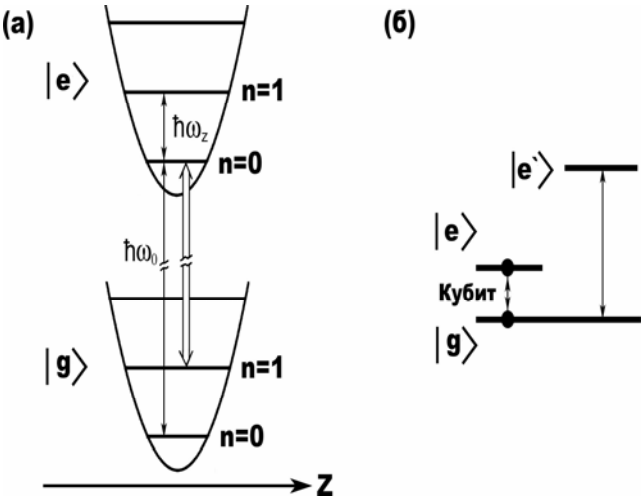


Рис. **4.3**

Рассмотрим систему, состоящую из двух ионов. Центр инерции этой системы совершает гармонические колебания вдоль оси z в удерживающем квадратичном потенциале ловушки с минимумом в точке $z = 0$. Пусть «дышащие» моды не возбуждаются, и расстояние l между ионами остается постоянным. Внутренние состояния каждого иона — основное $|g\rangle$ и возбужденное $|e\rangle$ — образуют кубит. Другими словами, мы имеем квантовый регистр, состоящий из двух кубитов, связь между которыми осуществляется за счет их общего синфазного колебания как целого. Для управления отдельным кубитом с координатой z_i используется поле

$$E = E_0 \sin kz_i e^{-i\omega_L t} + к.с. \qquad (4.8)$$

стоячей волны лазерного излучения с частотой $\omega_L = k_L c$, близкой к частоте ω_0 атомного перехода (рис. 4.3**а**). Обычно стоячая (вдоль оси *z*) волна образуется двумя лучами, пересекающимися под некоторым углом. Поэтому входящая в (4.8) величина *k* представляет собой проекцию волнового вектора $\vec{k}_L$ бегущей волны на ось *z*. Будем считать для определенности, что перемешивание внутренних состояний $|g\rangle$ и $|e\rangle$ происходит в результате электродипольного взаимодействия с локальной частотой Раби

$$\Omega(z_i) = \Omega_0 \sin kz_i, \tag{4.9}$$

где $\Omega_0 = dE_0/\hbar$, а *d* — дипольный матричный элемент перехода $|g\rangle \rightleftarrows |e\rangle$. Для простоты фаза стоячей волны выбрана таким образом, что частота (4.9) является действительной. В рамках резонансного приближения гамильтониан взаимодействия имеет вид

$$\hat{H}_{\text{int}} = \frac{\hbar\Omega(z_i)}{2}\left[|e\rangle\langle g| \cdot e^{-i(\omega_L-\omega_0)t} + |g\rangle\langle e| \cdot e^{i(\omega_L-\omega_0)t}\right]. \tag{4.10}$$

Отметим, что этот оператор действует не только на внутренние степени свободы иона, но и на «фононную» подсистему, так как величина z_i, т.е. координата отдельного кубита, зависит от оператора (4.6) координаты центра инерции системы двух ионов. Физический механизм перемешивания внутренних и поступательной степеней свободы обусловлен пространственной неоднородностью поля стоячей волны, т.е. зависимостью локальной частоты Раби (4.9) от положения иона. Градиент функции $\Omega(z_i)$ дает дополнительную силу, действующую на жестко связанную систему двух ионов, т.е. на ее центр инерции. Еще раз подчеркнем, что именно перемешивание внутренних и колебательной степеней свободы обеспечивает связь между кубитами.

Пусть поле стоячей волны приложено к первому иону. Тогда $z_1 = -l/2 + \hat{z}$, где *l* — фиксированное расстояние между ионами, а

$\hat{z}$ есть оператор координаты центра инерции, который выражается через операторы уничтожения и рождения «фонона» с помощью соотношения (4.6). Поскольку в узле градиент поля стоячей волны максимален, расположим волну так, чтобы узел поля был в точке $-l/2$, т.е. $\sin kl/2 = 0$, а $\cos kl/2 = 1$. Кроме того, рассмотрим, так называемый, режим Лэмба–Дике, когда характерная амплитуда колебаний

$$z_0 = \sqrt{\hbar/M\omega}$$

мала по сравнению с длиной волны $1/k$, т.е.

$$\eta \equiv kz_0 = \sqrt{\frac{\hbar k^2}{2M\omega}} \ll 1. \qquad (4.11)$$

Величина η называется параметром Лэмба–Дике. Режим Лэмба–Дике практически реализуется во многих экспериментах с ионами в ловушках. Он широко используется, например, для глубокого лазерного охлаждения ионов. Для полноты картины отметим, что величина, стоящая под знаком корня в (4.11), есть отношение частоты отдачи

$$\omega_{rec} \equiv \hbar k^2/2M$$

и частоты колебания ω.

Тогда частоту Раби $\Omega(z_1)$ можно записать в такой форме

$$\Omega(z_1) = \Omega_0 \sin k\left(-\frac{l}{2} + \hat{z}\right) = \Omega_0 \sin k\hat{z} \approx \Omega_0 k\hat{z} = \Omega_0 \eta\left(a + a^+\right). \qquad (4.12)$$

Здесь мы использовали условие $\cos kl/2 = 1$ и формулу (4.6), а также провели разложение с учетом неравенства (4.11). Это выражение надо подставить в оператор взаимодействия (4.10).

Если выбрать частоту ω_L лазерного поля так, что

$$\omega_L = \omega_0 - \omega, \tag{4.13}$$

то выполняется точное условие резонанса для переходов между состояниями $|g\rangle|n\rangle$ и $|e\rangle|n-1\rangle$, где кэт-векторы $|n\rangle$ и $|n-1\rangle$ описывают состояния фононной подсистемы. Один такой переход для $n = 1$ показан на рис. 4.3**а** двойной стрелкой. Последнее упрощение состоит в том, что в операторе взаимодействия (4.10) с учетом выражения (4.12) мы удерживаем только члены, отвечающие за резонансные переходы, т.е. в первом слагаемом оставляем оператор поглощения фонона a, а во втором – оператор рождения a^+. Переходя к представлению взаимодействия[1] с помощью гамильтониана $\hat{H}_0$ (4.1), получаем окончательное выражение для гамильтониана системы:

$$\hat{H} = \frac{\hbar\Omega_0}{2}\eta\left[|e\rangle\langle g|\cdot a + |g\rangle\langle e|\cdot a^+\right]. \tag{4.14}$$

Гамильтониан такого вида называют моделью Джейнса-Каммингса-Пауля. Это одна из самых популярных моделей, которая первоначально была сформулирована в квантовой оптике для описания взаимодействия двухуровневой системы с квантованным электромагнитным полем, когда операторы a и a^+ являются операторами уничтожения и рождения фотона одной резонансной моды поля (см. раздел 3.2). В нашем случае фотоны заменены «фононами».

---

[1] Полный гамильтониан системы есть $\hat{H}_0 + \hat{H}_{\text{int}}$, где $\hat{H}_0$ не зависит от времени. В представлении взаимодействия гамильтониан системы определяется выражением $\exp\left(i\frac{\hat{H}_0 t}{\hbar}\right)\hat{H}_{\text{int}}\exp\left(-i\frac{\hat{H}_0 t}{\hbar}\right)$.

Перейдем теперь к вопросу о том, как с помощью изложенных выше физических механизмов можно реализовать двухкубитовый гейт CNOT.

Ключевым моментом здесь является предложенная Цираком и Цоллером процедура, реализующая двухкубитовый фазовый гейт. Получение гейта CNOT из фазового гейта потребует нескольких дополнительных однокубитовых преобразований, которые мы рассмотрим в конце раздела.

Двухкубитовый фазовый гейт

Двухкубитовый фазовый гейт представляет собой преобразование «*управляемое* σ_3» и определяется следующим оператором (см. раздел 2.5):

$$|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes P(\pi). \tag{4.15}$$

Напомним, что операторы, стоящие в каждом из слагаемых слева, относятся к управляющему кубиту, а те, что справа — к управляемому кубиту. Оператор I описывает тождественное преобразование, а $P(\pi)$ имеет вид

$$P(\pi) = \sigma_3 = |0\rangle\langle 0| - |1\rangle\langle 1|. \tag{4.16}$$

Тогда двухкубитовое состояние $|\alpha\beta\rangle$ (α, β=0,1), в котором α относится к управляющему кубиту, а β — к управляемому, в результате действия фазового гейта преобразуется следующим образом:

$$\begin{gathered} |00\rangle, |01\rangle, |10\rangle \text{ не меняются,} \\ |11\rangle \to -|11\rangle. \end{gathered} \tag{4.17}$$

Базисные векторы состояний системы «два иона + фононы» будем

обозначать как $|\alpha\beta\rangle|n\rangle$, где $|\alpha\beta\rangle$ относится к двухкубитовой системе, а $|n\rangle$ описывает колебательную моду. Первый кубит (α) является управляющим, а второй (β) — управляемым. Состояние $|n\rangle$ колебательной системы обозначается целыми числами. В дальнейшем мы ограничимся только состояниями с $n = 0, 1$. Во избежание недоразумений, для возможных значений α и β будем использовать обозначения *g* и *e*. Для сопоставления с (4.15)–(4.17) следует использовать идентификацию $|g\rangle \equiv 0$, $|e\rangle \equiv 1$.

Сначала «фононная» подсистема приводится в состояние $n = 0$, т.е. охлаждается до основного колебательного уровня. Управляющий кубит $|\alpha\rangle$ подвергается воздействию импульса лазера, который создает стоячую волну. Кубит находится вблизи узла стоячей волны, так что взаимодействие описывается гамильтонианом (4.14). Длительность импульса выбирается равной $t = \pi / \Omega_0 \eta$, т.е. кубит подвергается воздействию π-импульса поля. Такой импульс (см. формулу (2.107)) переводит двухуровневую систему из нижнего состояния в верхнее (либо наоборот), умножая на фазовый множитель[1] (-*i*). В нашем случае речь идет о двух состояниях, которые соединены двойной стрелкой на рис. 4.3**а**. Поскольку сначала n = 0, есть только переход из верхнего состояния в нижнее.

Таким образом, в результате первой операции базисные состояния системы преобразуются следующим образом:

$$\begin{aligned} |g\beta\rangle|0\rangle &\to |g\beta\rangle|0\rangle, \\ |e\beta\rangle|0\rangle &\to (-i)|g\beta\rangle|1\rangle. \end{aligned} \qquad (4.18)$$

Состояние второго кубита, обозначенное свободным значком β, не меняется. Что касается первого кубита, то он оказывается в основ-

[1] Оператор эволюции (2.107) получен для гамильтониана, который отличается от (4.14) общим знаком. Поэтому для гамильтониана (4.14) фазовый множитель равен (-*i*), а не *i*, как в формуле (2.107)

ном состоянии $|g\rangle$, но при этом может измениться состояние колебательной моды, которая в общем случае переходит из начального состояния $|0\rangle$ в суперпозицию состояний $|0\rangle$ и $|1\rangle$. Действительно, если управляющий кубит α находится в состоянии $|\alpha\rangle = c_1|g\rangle + c_2|e\rangle$, то результатом взаимодействия с лазерным импульсом, как следует из (4.18), является преобразование

$$|\alpha\beta\rangle|0\rangle \to |g\beta\rangle\left(c_1|0\rangle - ic_2|1\rangle\right). \qquad (4.19)$$

С точки зрения манипулирования информацией, преобразование (4.19) означает, что квантовая информация кубита α перенесена в колебательную моду. Два колебательных состояния $|0\rangle$ и $|1\rangle$ тоже можно рассматривать как кубит. Другими словами, квантовая информация кубита α записана с помощью колебательного кубита.

Следующей операцией является воздействие еще одного импульса стоячей световой волны, но уже на управляемый кубит $|\beta\rangle$, который тоже располагается вблизи узла этого поля. При этом мы хотим, чтобы возбужденное состояние $|e\rangle$ рассматриваемого кубита не затрагивалось, а основное состояние $|g\rangle$ получило бы фазовый сдвиг π. С этой целью прикладывается световое поле, которое действует на смежном переходе $|g\rangle \rightleftarrows |e'\rangle$ между нижним состоянием кубита и каким-то возбужденным состоянием $|e'\rangle$, как показано на рис. 4.3**б**. Во всех остальных отношениях данное взаимодействие подобно тому, что было в случае первого импульса, и описывается гамильтонианом вида (4.14), в котором надо сделать замену $|e\rangle$ на $|e'\rangle$ и написать параметры Ω_0' и η'.

Длительность импульса выбирается равной $t' = 2\pi/\Omega_0'\eta'$. В качестве резонансной двухуровневой системы теперь выступают состояния $|g\rangle|1\rangle$ и $|e'\rangle|0\rangle$ второго иона, аналогичные тем, что соединены двойной стрелкой на рис. 4.3**а**, но с заменой $|e\rangle$ на $|e'\rangle$.

Поскольку 2π-импульс не изменяет состояние двухуровневой системы, а лишь сдвигает общую фазу на π, то начальное состояние $|g\rangle|1\rangle \to (-)|g\rangle|1\rangle$.

В результате второй операции состояния в правой части (4.18) преобразуются следующим образом:

$$\begin{aligned} &|g\beta\rangle|0\rangle \to |g\beta\rangle|0\rangle \quad (\text{здесь } \beta = g, e), \\ &-i|gg\rangle|1\rangle \to i|gg\rangle|1\rangle, \\ &-i|ge\rangle|1\rangle \to -i|ge\rangle|1\rangle. \end{aligned} \tag{4.20}$$

Это означает перепутывание второго кубита с колебательной модой. Поэтому квантовая информация, содержащаяся в колебательной моде, перераспределяется между «фононным» кубитом и кубитом β. Теперь вновь прикладывается π-импульс к контролирующему кубиту α. Тогда

$$\begin{aligned} &|g\beta\rangle|0\rangle \to |g\beta\rangle|0\rangle, \\ &i|gg\rangle|1\rangle \to (-i)(i)|eg\rangle|0\rangle = |eg\rangle|0\rangle, \\ &-i|ge\rangle|1\rangle \to (-i)(-i)|ee\rangle|0\rangle = -|ee\rangle|0\rangle. \end{aligned} \tag{4.21}$$

В результате трех операций (4.18), (4.20), (4.21) «фотонная» подсистема вернулась в исходное состояние $|0\rangle$, которое теперь можно просто опустить.

Что же касается базисных векторов двухкубитовой системы $|\alpha\beta\rangle$, то их преобразование имеет следующий вид:

$$\begin{aligned} &|gg\rangle, |ge\rangle, |eg\rangle \quad \text{не меняются}, \\ &|ee\rangle \to -|ee\rangle. \end{aligned} \tag{4.22}$$

С учетом идентификации $|g\rangle \equiv |0\rangle$, $|e\rangle \equiv |1\rangle$ легко видеть, что преобразование (4.22) совпадает с фазовым гейтом (4.17).

Гейт CNOT

Теперь заметим, что фазовый гейт (4.22) представляет собой CNOT-гейт, если управляемый кубит β записан в базисе повернутых состояний $|\pm\rangle = \frac{1}{\sqrt{2}}\left(|g\rangle \pm |e\rangle\right)$. Действительно, переходя к этому базису состояний управляемого кубита, из (4.22) получаем

$$\begin{aligned} |g\pm\rangle &\to |g\pm\rangle, \quad \text{т.е.} \quad |0\pm\rangle \to |0\pm\rangle, \\ |e\pm\rangle &\to |e\mp\rangle, \quad \text{т.е} \quad |1\pm\rangle \to |1\mp\rangle. \end{aligned} \tag{4.23}$$

Следовательно, управляемый кубит проходит через операцию *NOT*, $|+\rangle \to |-\rangle$ и $|-\rangle \to |+\rangle$, если управляющий кубит находится в состоянии $|1\rangle$. А это и есть, как мы знаем, CNOT-гейт. Справедливо и обратное утверждение. Так, пусть управляемый кубит $|\beta\rangle$ записан в базисе повернутых состояний $|\pm\rangle$. Тогда двухкубитовый фазовый гейт «*управляемое* σ_3» эквивалентен CNOT-гейту в базисе исходных состояний $|g\rangle$ и $|e\rangle$ управляемого кубита (см. задачу 5**б** в конце раздела 2.5)

Поэтому протокол CNOT-гейта в исходном базисе сводится к следующим операциям. Сначала совершается поворот базиса управляемого кубита β. Потом осуществляется двухкубитовый фазовый гейт, подробно описанный выше, и, наконец, управляемый кубит возвращается к исходному базису.

Поворот базиса представляет собой однокубитовый гейт типа преобразования Адамара. Его, как и другие однокубитовые гейты, можно реализовать с помощью импульса стоячей волны, расположенной так, что ион находится вблизи пучности поля. Из-за однородности поля вблизи пучности локальная частота Раби (4.9) в режиме Лэмба–Дике не содержит операторов колебательной моды, т.е. внутренние и поступательная степени свободы не перепутываются.

Тогда гамильтониан можно представить в форме

$$\hat{H}' = \frac{\hbar\Omega_0}{2}\left[\left|e\right\rangle\left\langle g\right|e^{-i\varphi} + \left|g\right\rangle\left\langle e\right|e^{i\varphi}\right]. \qquad (4.24)$$

Здесь мы ввели фазу φ стоячей волны. Поскольку оператор эволюции имеет вид $\exp\left(-i\hat{H}'t/\hbar\right)$, то варьируя φ и t, можно реализовать различные однокубитовые гейты. В качестве простого упражнения читателю предлагается проверить, что интересующее нас преобразование поворота базиса

$$\left|g\right\rangle \to \frac{1}{\sqrt{2}}\left(\left|g\right\rangle - \left|e\right\rangle\right), \quad \left|e\right\rangle \to \frac{1}{\sqrt{2}}\left(\left|g\right\rangle + \left|e\right\rangle\right) \qquad (4.25)$$

можно реализовать, если $\varphi = \pi/2$, а длительность импульса $t = \pi/2\Omega_0$. Возвращение же к исходному базису осуществляется с помощью импульса длительностью $3\pi/2\Omega_0$.

Изложенная принципиальная схема применима и к регистру с большим числом кубитов, а управляющий и управляемый кубиты могут достаточно далеко отстоять друг от друга. Передача квантовой информации между ними осуществляется с помощью общей для всей цепочки ионов колебательной моды, которая, тем самым, является квантовым регистром данных.

В заключение отметим, что квантовый логический элемент CNOT был впервые продемонстрирован экспериментально в 1995 г. в Национальном институте стандартов и технологий (NIST) в Боулдере с помощью одного иона $^9Be^+$ в ловушке. Управляющим кубитом были два колебательных состояния $\left|0\right\rangle$ и $\left|1\right\rangle$, а управляемым кубитом являлись внутренние состояния иона $\left|g\right\rangle$ и $\left|e\right\rangle$. Тем самым было показано, что возможно чтение из квантового регистра данных колебательного движения.

4.2. Логические элементы на атомах в резонаторах

В данном разделе мы вкратце обсудим еще одну физическую систему, с помощью которой были успешно продемонстрированы простые логические элементы, необходимые для манипулирования квантовой информацией.

Речь идет об атомах, взаимодействующих с квантованным электромагнитным полем в резонаторе. Физика таких систем является предметом квантовой электродинамики резонаторов (КЭР). Нынешний статус КЭР определяется впечатляющими успехами в создании высокодобротных резонаторов для полей как оптического, так и микроволнового диапазона. Ниже, для определенности, мы будем говорить об экспериментах с микроволновыми резонаторами, которые проводятся, например, в Гархинге (Германия) и в университете Эколь Нормаль в Париже.

Простейшей системой, позволяющей моделировать элементарные квантово-логические операции, является двухуровневый атом в резонаторе.

Представим себе резонатор объема V с одной модой квантованного электромагнитного поля. Оператор напряженности электрического поля имеет вид

$$\mathbf{E}(\mathbf{r})=\sqrt{\frac{2\pi\hbar\omega}{V}}\mathbf{e}u(\mathbf{r})(c+c^{+}), \qquad (4.26)$$

где $\mathbf{e}$ — вектор поляризации поля, ω — его частота, а c^{+} и c — операторы рождения и уничтожения фотона — элементарного возбуждения данной моды. Модовая функция $u(\mathbf{r})$ описывает пространственную структуру такого возбуждения резонатора. Она зависит от геометрии резонатора и в простейшем случае представляет собой стоячую (или бегущую) волну с некоторой огибающей в поперечном направлении.

Другой обязательный элемент экспериментов КЭР — нейтральный атом. Выберем какие-либо два его энергетических состояния, между которыми возможен переход, в качестве рабочих. Одно из них (с меньшей энергией) назовем основным и обозначим как $|g\rangle$,

а другое (с большей энергией) — возбужденным $|e\rangle$. Считаем, что с внешним полем атом взаимодействует дипольным образом, а частота резонатора ω точно совпадает с частотой ω_0 атомного рабочего перехода $|e\rangle \leftrightarrow |g\rangle$. Тогда в рамках резонансного приближения взаимодействие атома и поля описывается следующим гамильтонианом Джейнса–Каммингса:

$$\hat{H}_{\text{int}} = \hbar\Omega\left(c^{+}\sigma + c\sigma^{+}\right), \tag{4.27}$$

где величина $\Omega = d\sqrt{2\pi\omega/\hbar V u(\mathbf{r})}$ является параметром атомно-полевого взаимодействия. Ее называют вакуумной частотой Раби. Она зависит от величины d матричного элемента дипольного момента между основным и возбужденным состояниями и промодулирована по пространству с учетом модовой функции $u(\mathbf{r})$. Понижающий и повышающий операторы σ и σ^{+}

$$\sigma = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad \sigma^{+} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \tag{4.28}$$

в выражении (4.27) действуют в двухмерном векторном пространстве атомных состояний с базисом

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} \equiv |g\rangle \quad \begin{pmatrix} 1 \\ 0 \end{pmatrix} \equiv |e\rangle \tag{4.29}$$

по правилу

$$\begin{aligned} \sigma^{+}|g\rangle &= \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |e\rangle, \quad \text{т.е. } |e\rangle\langle g| \equiv \sigma^{+}, \\ \sigma|e\rangle &= \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |g\rangle, \quad \text{т.е. } |g\rangle\langle e| \equiv \sigma. \end{aligned} \tag{4.30}$$

Мы видим, что по своей структуре гамильтониан (4.27) аналогичен тому, который рассматривался в предыдущем разделе.

Основная проблема при реализации квантовой логики в рамках КЭР – это добиться доминирования взаимодействия вида (4.27) над неконтролируемыми процессами спонтанной релаксации атомов, затухания фотонов в резонаторах, теплового шума и других внешних воздействий, разрушающих квантовые логические элементы.

На сегодняшний день в этом направлении есть существенные достижения. Так, на основе сверхпроводящих материалов созданы резонаторы микроволнового диапазона, обладающие, как принято говорить, большим фактором добротности.

При низких температурах, порядка 1 К, время жизни фотона в них составляет от нескольких сотен микросекунд до нескольких миллисекунд. Это время гораздо больше времени взаимодействия поля и атома, пролетающего через резонатор с тепловой скоростью. Кроме того, при таких низких температурах тепловое воздействие пренебрежимо мало.

С другой стороны, в экспериментах по КЭР в микроволновой области чаще всего применяются так называемые ридберговские атомы. Это атомы, в которых валентный электрон находится в высоковозбужденном состоянии водородоподобного спектра с главным квантовым числом n порядка 50-60 или даже больше.

Поскольку расстояние электрона от ядра растет как n^2, то ридберговские атомы имеют большой дипольный момент и, тем самым, сильную связь с полем резонатора. Кроме того, ридберговские состояния имеют большое время жизни, достигающее 30 мс. Важно также и то, что разработаны методы надежного детектирования внутренних состояний ридберговских атомов.

Рис. 4.4 иллюстрирует схему, которая использовалась для демонстрации квантовых логических элементов в университете Эколь Нормаль (Париж). Атомы, испущенные источником, селектируются по скоростям, приготавливаются в одном из требуемых состояний – $|e\rangle$ или $|g\rangle$ – и направляются в сверхпроводящий резонатор, настроенный на частоту атомного перехода.

Отметим, что селекция по скоростям позволяет контролировать время пролета через резонатор, т.е. время взаимодействия.

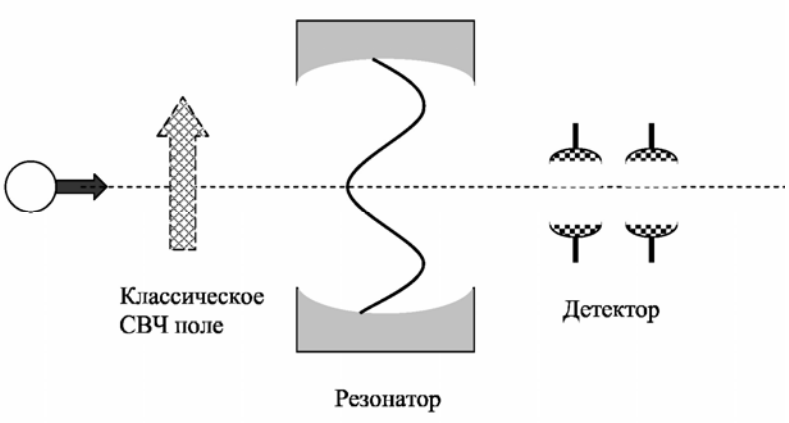


Рис. **4.4**

До входа в резонатор или после пролета через него атомы проходят через вспомогательные резонаторы, в которых импульс классического микроволнового поля может перемешивать уровни $|e\rangle$ и $|g\rangle$. Детектор, основанный на методе селективной ионизации в электрическом поле, позволяет подсчитывать число атомов в основном и возбужденном состоянии.

Самый простой, с точки зрения постановки задачи, эксперимент, выполненный в рамках указанной схемы, заключается в следующем. Пусть атом, который первоначально был в возбужденном состоянии $|e\rangle$, влетает в «пустой» резонатор, т.е. находящийся в вакуумном состоянии $|0\rangle$. В этом состоянии фотонов нет, так что оно удовлетворяет условию $c|0\rangle = 0$.

Внутри резонатора происходят процессы излучения и поглощения квантов возбуждения, которые описываются гамильтонианом (4.27). Излучение фотона сопровождается переходом атома в основное состояние $|g\rangle$, а поглощение фотона приводит к возбуждению атома.

Другими словами, атом и поле обмениваются возбуждением, а их состояния оказываются перепутанными. Вектор состояния такой системы имеет вид

$$\left|\Psi(t)\right\rangle = C_e(t)\left|e\right\rangle\left|0\right\rangle + C_g(t)\left|g\right\rangle\left|1\right\rangle, \tag{4.31}$$

где $\left|0\right\rangle$ и $\left|1\right\rangle$ — фоковские состояния поля с определенным числом (0 или 1) квантов. Коэффициенты $\left|C_e(t)\right|^2$ и $\left|C_g(t)\right|^2$ определяют вероятность найти атом в возбужденном и основном состояниях (а поле, соответственно, в вакуумном и однофотонном состояниях). Результирующие значения этих вероятностей после пролета атома через резонатор регистрируются селективным по атомным состояниям детектором. Уравнение Шрёдингера с гамильтонианом (4.27) для амплитуд C_g, C_e выглядит следующим образом:

$$\begin{cases} i\dfrac{dC_g}{dt} = \Omega C_e \\ i\dfrac{dC_e}{dt} = \Omega C_g. \end{cases} \tag{4.32}$$

Решение этой системы с начальным условием $C_e(0) = 1$, $C_g(0) = 0$

$$C_e(t) = \cos\Omega t, \quad C_g(t) = -i\sin\Omega t, \tag{4.33}$$

описывает так называемые вакуумные осцилляции Раби. Эти осцилляции можно наблюдать, варьируя, например, время взаимодействия, т.е. меняя скорость атомов. После того, как атом покинул резонатор, система «атом + поле» остается в перепутанном состоянии с постоянными коэффициентами. Рассматривая атом и поле как два кубита, можно сказать, что результатом обмена возбуждением является образование двухкубитовой ЭПР-пары. Реальный эксперимент хорошо согласуется с решением (4.33). При этом, конечно, амплитуды (4.33) содержат еще и затухающие множители из-за необратимых релаксационных процессов.

С помощью описанной схемы можно реализовать квантовую память в резонаторе. Пусть сначала атом в возбужденном состоянии попадает в пустой резонатор. Если время взаимодействия атома с полем таково, что $\Omega t = \pi/2$, то атом покидает резонатор в состоянии $|g\rangle$, оставив свое возбуждение в виде фотона в резонаторе. Если после некоторой задержки во времени T в резонатор влетает второй атом с той же скоростью, но в основном состоянии, то он поглощает этот фотон и покидает резонатор в состоянии $|e\rangle$. Заметим, кстати, что уменьшение вероятности найти второй атом в возбужденном состоянии при увеличении задержки T позволяет измерить время жизни фотона в резонаторе.

Следующий шаг состоит в том, что атом приготавливается в суперпозиционном состоянии $|\alpha\rangle = \frac{1}{\sqrt{2}}\left(|g\rangle + |e\rangle\right)$ с помощью $\pi/2$-импульса классического микроволнового поля, которое на рис. 4.4 показано слева от резонатора. Далее этот атом влетает в пустой резонатор и взаимодействует с ним в течение времени $t = \pi/2\Omega$. Согласно (4.27) и (4.33), компонента $|g\rangle$ атомного состояния никак не влияет на резонаторное поле, $|e\rangle$-компонента с амплитудой вероятности $(-i)$ приведет к излучению фотона и к переходу атома в основное состояние. В результате состояние системы преобразуется так:

$$|\alpha\rangle|0\rangle \to |g\rangle\frac{|0\rangle - i|1\rangle}{\sqrt{2}} \ . \qquad (4.34)$$

Атом оказывается в основном состоянии, а поле — в суперпозиции состояний $|0\rangle$ и $|1\rangle$. Квантовая информация кубита α оказывается записанной в полевом кубите. После некоторой задержки поле резонатора считывается вторым атомом, который приготовлен в состоянии $|g\rangle$ и взаимодействует с резонатором в течение того же самого промежутка времени. Очевидно, что такой атом никак не

влияет на вакуумную компоненту $|0\rangle$ поля, но в то же время он поглощает фотон из полевого состояния $|1\rangle$ и переходит в возбужденное состояние с амплитудой $(-i)$.

Тогда состояние всей системы, включающей два атома и поле, проходит через такую последовательность преобразований:

$$|g_2\rangle\frac{|g_1\rangle+|e_1\rangle}{\sqrt{2}}|0\rangle \to |g_2\rangle|g_1\rangle\frac{|0\rangle-i|1\rangle}{\sqrt{2}} \to \frac{|g_2\rangle-|e_2\rangle}{\sqrt{2}}|g_1\rangle|0\rangle. \quad (4.35)$$

Здесь для упрощения понимания мы снабдили состояния первого и второго атомов индексами 1 и 2. Поле вернулось в исходное состояние, а квантовая информация первого кубита оказалась записанной во втором кубите.

Аналогичная схема может быть использована для приготовления и манипулирования нелокальным перепутыванием между двумя атомами. Пусть первый атом, находящийся в состоянии $|e\rangle$, взаимодействует с первоначально пустым резонатором в течение времени $t = \pi/4\Omega$. При этом согласно (4.31) и (4.33) он перейдет в перепутанное с полем состояние вида

$$|e_1\rangle|0\rangle \to \frac{|e_1\rangle|0\rangle-i|g_1\rangle|1\rangle}{\sqrt{2}}. \quad (4.36)$$

Затем второй атом, приготовленный в состоянии $|g_2\rangle$, пролетает через резонатор за время $t = \pi/2\Omega$ и взаимодействует уже с равновероятной суперпозицией фотонных состояний, которая определяется правой частью формулы (4.36).

Не влияя на вакуумную компоненту $|0\rangle$ фотонного поля, второй атом с амплитудой вероятности $(-i)$ поглощает возбуждение поля, описываемое $|1\rangle$ — компонентой, т.е.

$$|g_2\rangle\frac{|e_1\rangle|0\rangle - i|g_1\rangle|1\rangle}{\sqrt{2}} \to \frac{|g_2\rangle|e_1\rangle - |e_2\rangle|g_1\rangle}{\sqrt{2}}|0\rangle. \qquad (4.37)$$

Таким образом, после описанных действий поле опять находится в вакуумном состоянии $|0\rangle$, а два атома образуют ЭПР-пару. Полученные здесь теоретические вероятности зарегистрировать двухатомные состояния $|g_2\rangle|e_1\rangle$ и $|e_2\rangle|g_1\rangle$ совпадают и равны 1/2. В упомянутом эксперименте французской группы из-за процессов, разрушающих когерентность, ЭПР-пары атомов возникали примерно с 60 %- ной вероятностью.

Интересно отметить, что аналогичным образом можно осуществить перепутывание двух макроскопических объектов.

Действительно, возьмем два пустых резонатора и атом, приготовленный в возбужденном состоянии $|e\rangle$. Пусть с первым резонатором атом взаимодействует в течение времени $t = \pi/4\Omega$, что приводит к перепутыванию состояний первого резонатора и атома

$$|e\rangle|0_1\rangle|0_2\rangle \to \frac{|e\rangle|0_1\rangle - i|g\rangle|1_1\rangle}{\sqrt{2}}|0_2\rangle, \qquad (4.38)$$

где индексы 1 и 2 относятся к первому и второму резонатору.

Если через второй резонатор атом пролетит за время $t = \pi/2\Omega$, то согласно результату (4.33) взаимодействие $|e\rangle$ — компоненты атомного состояния с вакуумной компонентой поля второго

резонатора приведет к суперпозиции вида

$$\frac{|e\rangle|0_1\rangle - i|g\rangle|1_1\rangle}{\sqrt{2}}|0_2\rangle \to \frac{-i}{\sqrt{2}}\left(|0_1\rangle|1_2\rangle + |1_1\rangle|0_2\rangle\right)|g\rangle, \qquad (4.39)$$

и мы опять получаем ЭПР-пару, но теперь уже макроскопических объектов – двух резонаторов с полем. Состояние этой ЭПР-пары написано в круглых скобках.

Резонансное взаимодействие между атомом и полем может также быть использовано для беспоглощательного детектирования фотона, находящегося в резонаторе.

Суть этого процесса состоит в том, что атом, находящийся в состоянии $|g\rangle$, пересекает резонатор за время

$$\Omega t = \pi .$$

Если при этом резонатор пуст, то никакого взаимодействия нет, и первоначальное состояние системы не меняется

$$|g\rangle|0\rangle \to |g\rangle|0\rangle .$$

Если же в резонаторе находится один фотон, то, как нетрудно установить из уравнений (4.32), система «атом + поле» испытывает фазовое преобразование

$$|g\rangle|1\rangle \to -|g\rangle|1\rangle ,$$

которое можно зафиксировать с помощью, так называемой, интерференции Рамзея.

В отличие от большинства детекторов фотонов в данном случае фотон не покидает резонатор, что является примером квантового неразрушающего измерения.

4.3. Экспериментальная реализация квантовой телепортации

Опишем теперь эксперимент по квантовой телепортации, выполненный в 1997 г. в Институте Экспериментальной физики в Инсбруке группой *А. Цайлингера*. В этом эксперименте была осуществлена телепортация поляризационного состояния единичного фотона при помощи вспомогательной пары фотонов в перепутанном поляризационном состоянии. Протокол квантовой телепортации был рассмотрен в разделе 3.4.

Не вдаваясь в многочисленные детали и тонкости, остановимся только на двух принципиальных элементах экспериментальной установки. Как мы видели, для реализации протокола квантовой телепортации нужен источник ЭПР-пар и анализатор состояний Белла.

В рассматриваемом эксперименте для получения перепутанных по поляризациям пар фотонов использовался процесс спонтанного параметрического рассеяния света в кристалле бета-бората бария, который обладает большой нелинейной восприимчивостью второго порядка. В результате такого процесса, который изображен на рис. 4.5**а**, падающий на кристалл фотон с частотой ультрафиолетового диапазона преобразуется в два фотона с меньшими, но близкими частотами. Поэтому в англоязычной литературе используется термин «даун-конверсия», т.е. буквально – преобразование (частоты) вниз.

Для того чтобы иметь перепутывание по поляризациям, использовалась определенная ориентация оптической оси кристалла относительно направления падающего излучения, при которой фотоны образовавшейся пары имеют две ортогональные поляризации. Импульсы этих фотонов ориентированы симметричным образом вблизи двух конических поверхностей, оси которых образуют некоторый угол. Поэтому излучение вдоль одного из конусов имеет, скажем, «вертикальную» поляризацию, а вдоль другого – «горизонтальную». Описанный процесс называют в литературе неколлинеарной даун-конверсией с синхронизмом типа II.

Теперь обратим внимание, что два фотона той пары, которые распространяются вдоль линий пересечения конических поверхностей, не обладают определенной поляризацией, а находятся в перепутанном поляризационном состоянии.

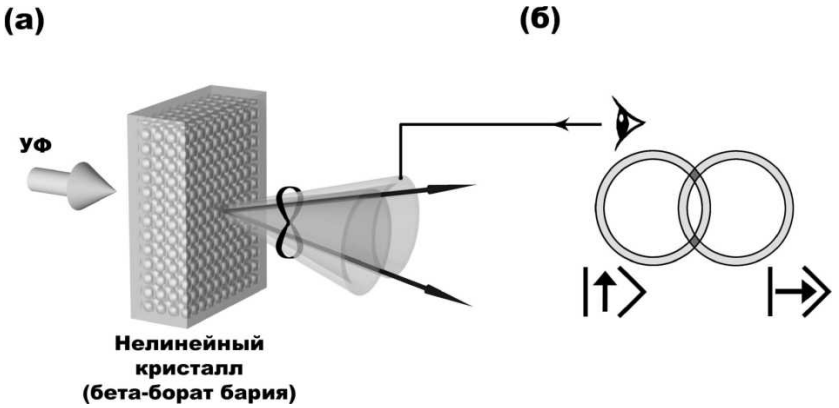


Рис. **4.5**

На проекции, показанной на рис. 4.5**б**, перепутанной паре отвечают зачерненные области. Так работает источник ЭПР-пар.

В качестве анализатора состояний Белла был использован простой оптический элемент – светоделитель, схематически представленный на рис. 4.6. Он представляет собой пластину, изготовленную из диэлектрического материала, которая с вероятностью 50 на 50 % пропускает или отражает свет. Принцип работы светоделителя как анализатора поляризационных состояний Белла состоит в следующем. Пусть, как показано на рис. 4.6, два фотона с ортогональными поляризациями попадают на светоделитель с разных сторон, т.е. в двух входных каналах системы. Если процессы отражения и похождения не меняют поляризацию, то для пары фотонов, которая покидает систему так, что в двух выходных каналах (справа и слева) есть по одному фотону, поляризация каждого из них не имеет определенного значения.

В разделе 2.4 мы показали, что такая пара оказывается в перепутанном поляризационном состоянии $\left|\Psi^{(-)}\right\rangle$. Антисимметричное состояние $\left|\Psi^{(-)}\right\rangle$ является единственным из полного набора двухкубитовых состояний Белла, которое реализуется, когда выходящие фотоны находятся с разных сторон от светоделителя.

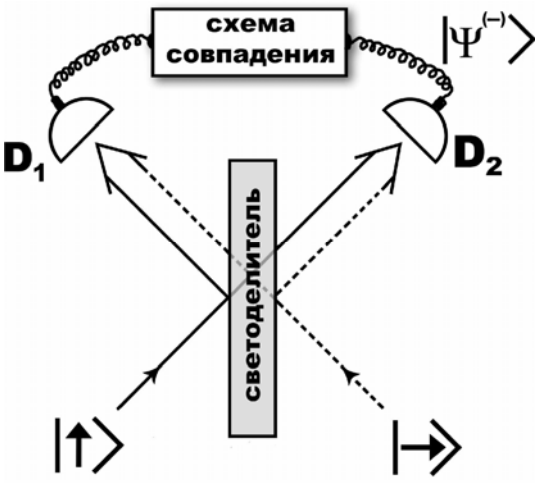


Рис. **4.6**

Два детектора D_1 и D_2 в выходных каналах регистрируют событие совпадения фотоотсчетов. Регистрация такого события означает, что пара фотонов находится в перепутанном состоянии $\left|\Psi^{(-)}\right\rangle$. Другими словами, происходит проектирование двухчастичного поляризационного состояния на состояние Белла $\left|\Psi^{(-)}\right\rangle$. Поскольку такое состояние является только одним из четырех возможных состояний Белла, то данная простейшая схема, использованная в рассматриваемом эксперименте, обеспечивала лишь частичный анализ перепутанных поляризационных состояний.

Для полноты картины скажем еще, что в качестве внешнего фотона, поляризационное состояние которого было объектом квантовой телепортации, брался один из партнеров другой ЭПР-пары, которая возникала в кристалле под действием того же светового импульса накачки.

В заключение хотелось бы обратить внимание, что даже весьма схематичное описание эксперимента, приведенное выше, показывает, как много разнообразных физических явлений вовлечено в реализацию протокола квантовой телепортации.

Список используемой литературы (источники)

1. Ландау Л.Д., Лифшиц Е.М. Квантовая механика. Нерелятивистская теория. — М.: Наука, 2006.
2. Давыдов А.С. Квантовая механика. — М.: Физматгиз, 1963.
3. Физика квантовой информации /Под ред. Д. Боумейстера, А. Экерта, А. Цайлингера. – М.: Постмаркет, 2002.–376с.
4. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация /Пер. с англ. – М.: Мир, 2006.–824с.
5. Яковлев В.П., Кондрашин М.П. Элементы квантовой информатики. – М.: МИФИ, 2004.–80с.

«…квантовая механика кажется новичку трудной и до некоторой степени таинственной дисциплиной. Тайна постепенно уменьшается по мере того, как разбирается все большее число примеров, но никогда не исчезает полностью ощущение, что у этого предмета есть что-то необычное.»

Р. Фейнман, А. Хибс [3, с.34]

«…Понимание того, как выполнять классические вычисления при условии обратимости, станет решающим шагом в понимании того, как использовать возможности квантовой механики для вычислений.»

М. Нильсен, И. Чанг [1, с.44]

«Материал, изложенный далее, в общем-то, отражает действительность. Однако надо признать, что он больше соответствует тому, как он был понят.»

С.Д. Кулик

Квантовая схемотехника

Г л а в а 5

КВАНТОВАЯ СХЕМОТЕХНИКА

Содержание

Квантовая механика для кибернетики. Амплитуда вероятности. Понятие схемы. Понятие однокубитовой схемы. Понятие двухкубитовой схемы. Понятие трех и более кубитовой схемы. Квантовая схема для алгоритма Дойча.

5.1. Квантовая механика для кибернетики

> «Если человек не шокирован квантовой теорией, он ее просто не понял.»
>
> *Н. Бор* [1, с.152]

> «…Принципы квантовой механики просты, но даже специалисты находят их противоречащими интуиции.»
>
> *М. Нильсен, И. Чанг* [1, с.20]

> «Постулаты квантовой механики были получены в результате долгого процесса проб и (по большей части) ошибок, который в значительной степени заключался в угадывании и нащупывании исходных положений теории. Не удивляйтесь, что мотивировки постулатов не всегда достаточно ясные; даже специалисты считают постулаты квантовой механики удивительными. Ознакомившись с несколькими следующими разделами, необходимо понять, как и когда следует применять эти постулаты.»
>
> *М. Нильсен, И. Чанг* [1, с.114]

Вернемся к основным положениям аппарата квантовой механики. С точки зрения кибернетики и квантовых вычислений, его можно рассматривать как формальную математическую структуру, заданную своими постулатами и правилами. Это позволит сформулировать далее важный набор *правил* и *свойств*, которые будут использоваться для анализа и синтеза простейших квантовых схем.

В основе *аппарата квантовой механики* лежат следующие постулаты.

Постулат **I**

С каждой изолированной физической системой связывается комплексное векторное пространство со скалярным произведением (т.е. гильбертово пространство), которое называется *пространством состояний* системы. Система полностью описывается *вектором состояний*, который представляет собой единичный вектор в пространстве состояний системы[1] [1, с.114-115] ■

Постулат **II**

Эволюция *замкнутой* квантовой системы описывается *унитарным преобразованием*. Другими словами, состояние $|\psi\rangle$ системы в момент времени t_1 связано с ее состоянием $|\psi'\rangle$ в момент времени $t_2=t_1+\tau$ посредством унитарного оператора U, который из-за однородности времени зависит только от интервала времени τ, т.е. $|\psi'\rangle = U(\tau)|\psi\rangle$ (см. и ср. с [1, с. 116]) ■

Постулат **IV**

Пространство состояний составной системы представляет собой тензорное произведение пространств состояний входящих в нее подсистем. Если эти подсистемы пронумерованы от 1 до n, и подсистема с номером i находится в состоянии $|\psi_i\rangle$, то состояние составной системы описывается вектором $|\psi_1\rangle\otimes|\psi_2\rangle\otimes\ldots\otimes|\psi_n\rangle$.
(см. и ср. с [1, с. 131]) ■

[1] Каждое возможное состояние системы описывается вектором (с единичной нормой), принадлежащим этому пространству. Поскольку гильбертово пространство является линейным многообразием, то для векторов состояний имеет место **принцип суперпозиции**.

Постулат **III**

Квантовые измерения описываются набором $\{M_{\boldsymbol{m}}\}$ *операторов измерения*. Это операторы, действующие в пространстве состояний системы, подлежащей измерению. Индекс обозначает результаты измерения, которые могут получиться в эксперименте. Если непосредственно перед этим квантовая система находилась в состоянии $|\psi\rangle$, то вероятность того, что в результате измерения будет получен результат $\boldsymbol{m}$, задается выражением

$$p(\boldsymbol{m}) = \langle\psi| M_m^\dagger M_m |\psi\rangle ,$$

а после измерения система будет находиться в состоянии

$$\frac{M_m |\psi\rangle}{\sqrt{\langle\psi| M_m^\dagger M_m |\psi\rangle}} .$$

Операторы измерения удовлетворяют *условию полноты*

$$\sum_m M_m^\dagger M_m = I .$$

Условие полноты означает, что сумма вероятностей различных исходов измерения равна единице:

$$1 = \sum_m p(m) = \sum_m \langle\psi| M_m^\dagger M_m |\psi\rangle$$

[1, с. 120] ■

Особо подчеркнем, что мы говорим здесь о квантовой механике не как о физической теории, а как о математической структуре, которая лежит в основе квантовых вычислений.

Сама по себе эта математическая структура не сообщает, каким физическим законам подчинена та или иная физическая система, каков смысл абстрактных векторов состояний и каким должно быть устройство пространства состояний. Не касаясь здесь также достаточно сложного вопроса о выборе и формулировке полноты набора постулатов абстрактного аппарата квантовой механики, заметим, что для конечномерных гильбертовых пространств, которые используются в квантовых вычислениях, изложенная математическая структура является совершенно корректной.

Прежде чем рассматривать постулаты, дадим следующее (не полное) определение *аппарата квантовой механики*, являющегося основой для квантовых вычислений.

*Определение 5.0**а***

Аппарат квантовой механики (АКМ) (см. и ср. [1, с.114]) — математическая конструкция для построения физических теорий (сам по себе АКМ не сообщает, каким физическим законам подчинена та или иная физическая система, однако он дает математические конструкции и понятия для формулировки этих законов).

ОТМЕТИМ. Аппарат квантовой механики был сформулирован, существует и применяется в следующих трех формах:

- матричная механика (*В. Гайзенберг*);
- волновая механика (*Э. Шрёдингер*);
- абстрактная векторная форма (*П.А.М. Дирак*).

Эти три формы эквивалентны в том смысле, что все они приводят к одинаковым *физическим результатам* и одна форма может быть преобразована в другую.

Первый постулат указывает место действия величин, описывающих квантово-механические процессы.

Эти величины действуют в абстрактном линейном *комплексном векторном пространстве* (КВП) со скалярным произведением.

Это гильбертово пространство и есть пространство состояний квантовой системы.

Рассмотрим следующий пример квантовой системы.

Пример 5.0**а**. Простейшая квантовая система [1, с.115].

В случае квантовых вычислений простейшей квантово-механической системой является кубит.

Для квантовых компьютеров кубит является наиболее распространенной такой системой. Для кубита характерно то, что его пространство состояний является **двумерным**. Если ввести базисные векторы $|0\rangle$ и $|1\rangle$, то произвольный вектор состояния $|\psi\rangle$ в гильбертовом пространстве (т.е. в абстрактном векторном пространство со скалярным произведением) есть

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle\,, \qquad (5.0\mathbf{а})$$

причем ***a*** и ***b*** — комплексные числа (КЧ). Совокупность пар КЧ образуют КВП. Из требований *Постулата* **I** следует, что *вектор состояния* $|\psi\rangle$ должен быть единичным вектором, т.е. $\langle\psi|\psi\rangle = 1$, что эквивалентно условию $|a|^2+|b|^2=1$. Отметим, что $\langle\varphi|\psi\rangle$ — скалярное произведение векторов $|\varphi\rangle$ и $|\psi\rangle$. Формально можно полагать, что для *кубита* его состояния $|0\rangle$ и $|1\rangle$ представляют значения 0 и 1, которые может принимать классический *бит* (или рассмотренный ранее в книге 1 ***RS*** триггер). Принципиальное отличие *кубита* от классического *бита* состоит в том, что *кубит* (как квантово-механическая система) может находиться помимо базисных состояний (т.е. $|0\rangle$ или $|1\rangle$) еще в состоянии так называемой суперпозиции, т.е. *кубит* может находиться в суперпозиции 2-х этих базисных состояний

$$|\psi\rangle = a_1\,|0\rangle + a_2\,|1\rangle\,, \qquad (5.0\mathbf{б})$$

где a_1 и a_2 — комплексные *амплитуды* для состояний $|0\rangle$ и $|1\rangle$ соответственно. Например, если кубит находится в суперпозиции $|\tilde{\psi}\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$, то амплитудами являются следующие числа: $a_1 = \frac{+1}{\sqrt{2}}$ и $a_2 = \frac{-1}{\sqrt{2}}$, так как эту суперпозицию можно представить в виде (5.0**б**) следующим образом: $|\tilde{\psi}\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$.

На этом закончим рассмотрение данного примера ■

По результатам рассмотрения предыдущего примера сформулируем следующие определения.

*Определение 5.0**б***

Амплитуда — в суперпозиционном состоянии, т.е. в линейной комбинации $\sum_i a_i |\psi_i\rangle$ каждое состояние $|\psi_i\rangle$ представлено с *амплитудой* a_i.

*Определение 5.0**в***

Условие нормировки [1, с.115] — условие $\langle\psi|\psi\rangle = 1$ называется *условием нормировки* для вектора состояния $|\psi\rangle$.

Таким образом, *Постулат* **I** позволяет понять, в каком состоянии может находиться одиночный (изолированный) *кубит* — квантовый триггер, т.е. элемент, из которого состоит квантовый регистр для квантового вычислителя.

Второй постулат позволяет понять, как одно состояние замкнутой квантовой системы связано с другим ее состоянием. В случае квантового вычислителя важно [1, с.116], что для одиночного *кубита* именно любой *унитарный оператор* можно в принципе реализовать в некоторой реальной системе. Замкнутость системы означает, что она никак не взаимодействует с другими системами.

Для представления преобразований (эволюции квантовой системы) имеются две формы — *операторная* (из теории линейных операторов) и *матричная* форма (из теории матриц). *Операторная* и *матричная* формы являются эквивалентными и могут применяться на равных правах, в том числе одновременно и порой смешиваться.

ВАЖНО. Формальный АКМ не конкретизирует вида оператора ***U***, который описывает динамику физической системы. Можно сказать, что он [1, с.116]: «… просто “гарантирует” надежное средство описания замкнутой квантово-механической системы».

Для *Постулата* **II** существует еще один эквивалентный вариант этого постулата. Приведем и его формулировку.

Постулат **II`**(еще один вариант) [1, с. 117]
Эволюция состояния замкнутой квантовой системы во времени описывается *уравнением Шрёдингера*:

$$i\hbar \frac{d|\psi\rangle}{dt} = H|\psi\rangle \quad \blacksquare \qquad (5.0\textbf{в})$$

В (5.0**в**) $\hbar$ — физическая постоянная Планка, которую часто включают в состав H [1, с. 117]); символ H — это вполне определенный для данной системы эрмитовый оператор, называемый *гамильтонианом* замкнутой системы. Оператор эволюции $\boldsymbol{U}$ однозначно определяется *гамильтонианом H.* Нахождение *H может оказаться сложной задачей, которая решается для каждой конкретной физической системы* [1, с. 117].

Рассмотрим следующий простой, но важный пример.

Пример 5.0б. Вычисление выходного вектора.

Кубит как квантовый объект характеризуется следующим вектором состояния в гильбертовом пространстве:

$$|\psi\rangle = a|0\rangle + b|1\rangle ,$$

где $\boldsymbol{a}$ и $\boldsymbol{b}$ — известные комплексные числа (амплитуды), причем выполнено условие $|a|^2+|b|^2=1$. Требуется определить выходной вектор состояния $|\psi'\rangle = A|0\rangle + B|1\rangle$ этого кубита после некоторого физического процесса, который описывается известным унитарным оператором $\boldsymbol{Z}$ (полагаем, что квантовая система замкнутая).

Решение

1). Из требований *Постулата* **II** следует, что эволюция *замкнутой* квантовой системы описывается *унитарным* преобразованием, что соответствует выражению в следующей операторной форме: $|\psi'\rangle = \boldsymbol{Z}|\psi\rangle$, где $\boldsymbol{Z}$ — унитарный оператор. В матричной форме это выглядит так же $|\psi'\rangle = \boldsymbol{Z}|\psi\rangle$, только теперь $\boldsymbol{Z}$ — это унитарная матрица, а векторы $|\psi'\rangle$ и $|\psi\rangle$ представлены как вектор-столбец $\begin{bmatrix} A \\ B \end{bmatrix}$ и $\begin{bmatrix} a \\ b \end{bmatrix}$ соответственно (отметим, что *гейту*, воздействующему на *кубит* так же, как и оператор $\boldsymbol{Z}$, соответствует та же самая унитарная матрица).

Требуется, зная вектор $|\psi\rangle = \frac{3}{5}|0\rangle + \frac{4}{5}|1\rangle$ и матрицу $\boldsymbol{Z}$, т.е.

$$|\psi\rangle = \begin{bmatrix} \frac{3}{5} \\ \frac{4}{5} \end{bmatrix}, \qquad \boldsymbol{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$$

найти выходной вектор $|\psi'\rangle$ (отметим, что $|3/5|^2 + |4/5|^2 = 1$).

2). Искомый вектор (согласно правилам линейной алгебры [9] и матричного исчисления [8]) находится известным способом путем умножения матрицы на вектор-столбец. Так как входной и выходной векторы связаны соотношением

$$Z \times |\psi\rangle = |\psi'\rangle \text{ , где } |\psi'\rangle = \begin{bmatrix} A \\ B \end{bmatrix},$$

то, зная $\boldsymbol{Z}$ и $|\psi\rangle$, вычислим выходной вектор $|\psi'\rangle = \begin{bmatrix} A \\ B \end{bmatrix}$ состояния квантовой системы:

$$Z \times |\psi\rangle =$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \times \begin{bmatrix} \frac{3}{5} \\ \frac{4}{5} \end{bmatrix} = \frac{1}{5}\begin{bmatrix} 1\cdot 3 + & 0\cdot 4 \\ 0\cdot 3 + (-1)\cdot 4 \end{bmatrix} = \frac{1}{5}\begin{bmatrix} 3 \\ -4 \end{bmatrix} = \begin{bmatrix} \frac{3}{5} \\ -\frac{4}{5} \end{bmatrix} = \begin{bmatrix} A \\ B \end{bmatrix},$$

т.е. $A = \frac{3}{5}$, $B = -\frac{4}{5}$ или $|\psi'\rangle = \begin{bmatrix} A \\ B \end{bmatrix} = \begin{bmatrix} \frac{3}{5} \\ -\frac{4}{5} \end{bmatrix} = \frac{1}{5}\begin{bmatrix} 3 \\ -4 \end{bmatrix}$.

Здесь и далее пунктирные линии используются для лучшего визуального восприятия векторов, матриц и действий над ними.

3). Проверим условие нормировки для вектора $|\psi'\rangle = \frac{3}{5}|0\rangle - \frac{4}{5}|1\rangle$

$$\left|\frac{3}{5}\right|^2 + \left|-\frac{4}{5}\right|^2 = \frac{9}{25} + \frac{16}{25} = \frac{25}{25} = 1,$$

т.е. условие нормировки выполняется.

На этом закончим рассмотрение данного примера ■

Таким образом, *Постулат* **II** предоставляет следующее очень важное правило для вычисления выходного вектора состояния, т.е. конечного состояния квантового объекта (в частности *кубита*), если известен входной вектор состояния, т.е. начальное состояние квантового объекта (*кубита*) и оператор (или *гейт*), выполняющий унитарное преобразование над состоянием этого *кубита*.

Правило 5.0**а**

Амплитуды вероятности (т.е. компоненты выходного) вектора состояния кубита (как замкнутой квантовой системы) после воздействия на этот кубит унитарного преобразования (*описываемого соответствующей унитарной матрицей*) *определяются путем* ***умножения*** *этой унитарной матрицы на вектор-столбец, составленный из амплитуд вероятностей (т.е. из компонентов входного) вектора состояния кубита до воздействия на него унитарным преобразованием* ■

Это правило кратко заключается в том, что выходной вектор получается простым умножением унитарной матрицы на входной вектор (само умножение выполняется по известным правилам умножения двух матриц). В частности это правило позволяет вычислить **амплитуды вероятностей** (в общем случае комплексные числа), являющиеся компонентами входного и выходного векторов при рассмотрении квантовых вычислений.

Далее это правило будет дополнено еще тремя правилами для вычисления как *амплитуд вероятностей*, так и самой *вероятности*, а также будут рассмотрены подробнее сами амплитуды вероятностей.

Третий постулат позволяет понять, что такое *измерение* состояния замкнутой квантовой системы, в том числе и *кубита*. Для более глубокого понимания квантовых вычислений необходимо иметь хотя бы некоторые основные важные представления об *измерении* в квантовой механике.

Рассмотрим следующий, хотя и простой, но важный пример измерения над одиночным кубитом, или другими словами, измерение кубита в *вычислительном базисе*.

Пример 5.0в. Измерение над одиночным кубитом [1, с.120-121].

Имеется одиночный кубит (т.е. квантовый регистр из 1-го кубита). Выполняется измерение в *вычислительном базисе* (измерение над одиночным кубитом с 2-мя возможными результатами, которые определяются 2-мя (***m***=2) операторами измерения M_0 и M_1).

Операторы измерения M_0 и M_1 определяются следующими соотношениями: $M_0 = |0\rangle\langle 0|$, $M_1 = |1\rangle\langle 1|$. Такие операторы называются *проекционными операторами* или *проекторами*.

Пусть измеряемое состояние кубита задается следующим вектором состояния: $|\psi\rangle = a|0\rangle + b|1\rangle$.

Требуется найти вероятность получения результата ***m***=0 и ***m***=1 в результате измерения описываемыми операторами M_0 и M_1. Требуется определить вектор состояния после измерения.

Решение

1). Заметим, что как оператор M_0, так и оператор M_1 является *эрмитовым* и $M_0^2 = M_0$, $M_1^2 = M_1$.

Поэтому (как требует *Постулат* **III**) выполнимо следующее условие полноты:

$$\sum_m M_m^\dagger M_m = M_0^\dagger M_0 + M_1^\dagger M_1 = M_0 + M_1 = I \ .$$

2). Вероятность получения результата ***m***=0 определяется (согласно *Постулату* **III**) следующей формулой:

$$p(\mathbf{0}) = \langle\psi|M_0^\dagger M_0|\psi\rangle = \langle\psi|M_0|\psi\rangle = |a|^2 .$$

Аналогично можно получить вероятность получения результата ***m***=1 по следующей формуле:

$$p(\mathbf{1}) = \langle\psi|M_1^\dagger M_1|\psi\rangle = \langle\psi|M_1|\psi\rangle = |b|^2 .$$

3). Вектор состояния после измерения определяется (согласно *Постулату* **III**) следующими формулами:

$$\frac{M_0|\psi\rangle}{\sqrt{\langle\psi|M_0^\dagger M_0|\psi\rangle}} = \frac{M_0|\psi\rangle}{\sqrt{|a|^2}} = \frac{M_0|\psi\rangle}{|a|} = \frac{a}{|a|}|0\rangle ,$$

$$\frac{M_1|\psi\rangle}{\sqrt{\langle\psi|M_1^\dagger M_1|\psi\rangle}} = \frac{M_1|\psi\rangle}{\sqrt{|b|^2}} = \frac{M_1|\psi\rangle}{|b|} = \frac{b}{|b|}|1\rangle \cdot$$

4). На этом закончим рассмотрение данного примера ■

Четвертый постулат позволяет понять, как следует поступать в случае составных квантовых систем (т.е. когда имеется более одного кубита). Этот постулат позволяет сформулировать следующее правило нахождения (вычисления) вектора состояния составной системы (квантового регистра), состоящей из нескольких подсистем (группы из ***n*** кубитов, т.е. квантовых триггеров), если известен вектор состояния для каждого из кубитов.

Правило 5.0**б**

Состояние составной системы описывается вектором $|\tilde{\psi}\rangle$, *который может быть вычислен путем* ***тензорного умножения*** *векторов состояния каждой из подсистем, входящих в составную систему. Если известны состояния подсистем (кубитов), пронумерованные от* 1 *до* ***n****, и подсистема (кубит) с номером* ***i*** *находится в состоянии* $|\psi_i\rangle$, *то состояние составной системы (квантового регистра) описывается вектором* $|\tilde{\psi}\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \ldots \otimes |\psi_n\rangle$ ■

Это правило заключается в том, что вектор состояния квантового регистра получается как ***тензорное*** произведение векторов состояний кубитов, входящих в этот квантовый регистр.

Сформулируем еще одно правило нахождения матрицы, действующую на регистр из ***n*** кубитов, если известны унитарные матрицы, действующие на отдельные кубиты.

Правило 5.0**в**

Унитарная матрица $\boldsymbol{M^{\{n\}}}$ *преобразования над квантовой системой из* ***n*** *кубитов (****n****>*1*) вычисляется путем* ***тензорного умножения*** *унитарных матриц* M_j, *связанных с преобразованием каждого j-го из этих кубитов, где* j=1,2,...,***n*** *(если над некоторым s-м кубитом не производится какого-либо преобразования, то это эквивалентно тождественному преобразованию с единичной унитарной матрицей* ***I****, т.е.* $M_s = \boldsymbol{I}$*):* $\boldsymbol{M^{\{n\}}} = M_1 \otimes M_2 \otimes \ldots \otimes M_n$ ■

Это правило кратко заключается в том, что итоговая унитарная матрица получается как ***тензорное*** произведение унитарных матриц преобразований кубитов, над которыми они выполняются.

Рассмотрим следующие простые, но важные примеры.

***Пример 5.0*г**. Вычисление вектора состояния системы 2-х кубитов.

Имеется система двух кубитов (т.е. квантовый регистр из 2-х кубитов). Каждый ***i***-й кубит имеет вектор состояния

$$|\psi_i\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle .$$

Требуется найти вектор состояния $|\tilde{\psi}\rangle$ системы этих двух кубитов (***n***=2), т.е. квантового регистра.

Решение

1). Применяя *Правило* 5.0**б**, получаем следующий вектор $|\tilde{\psi}\rangle$:

$$|\tilde{\psi}\rangle = |\psi_1\rangle \otimes |\psi_2\rangle =$$

$$= \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix} \otimes |\psi_2\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\cdot|\psi_2\rangle\\1\cdot|\psi_2\rangle\end{bmatrix} = \left(\frac{1}{\sqrt{2}}\right)^2 \begin{bmatrix}1\cdot\begin{bmatrix}1\\1\end{bmatrix}\\1\cdot\begin{bmatrix}1\\1\end{bmatrix}\end{bmatrix} = \frac{1}{2}\begin{bmatrix}1\\1\\1\\1\end{bmatrix} = \begin{bmatrix}0.5\\0.5\\0.5\\0.5\end{bmatrix}.$$

2). На этом закончим рассмотрение данного примера ■

***Пример 5.0*д**. Вычисление унитарной матрицы действующей на систему из 2-х кубитов.

Имеется система двух кубитов. Над каждым кубитом выполняется преобразование, заданное унитарной матрицей

$\boldsymbol{H} = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}$ (отметим, что существует *гейт* — элемент *Адамара*, у которого такая же унитарная матрица ***H***).

Требуется найти унитарную матрицу $\boldsymbol{H}^{\{2\}}$, действующую на систему этих двух кубитов (***n***=2).

Решение

1). Применяя *Правило* 5.0**в**, получаем следующую матрицу $\boldsymbol{H}^{\{2\}}$:

$$\boldsymbol{H}^{\{2\}} = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix} \otimes H = \frac{1}{\sqrt{2}}\begin{bmatrix}1\cdot H & 1\cdot H\\1\cdot H & (-1)\cdot H\end{bmatrix} = \frac{1}{\sqrt{2}}\left[\begin{array}{cc:cc}1 & 1 & 1 & 1\\1 & -1 & 1 & -1\\ \hdashline 1 & 1 & -1 & -1\\1 & -1 & -1 & 1\end{array}\right].$$

2). На этом закончим рассмотрение данного примера ■

Некоторые важные свойства унитарной матрицы

Для понимания квантовых вычислений важно знать свойства унитарной матрицы. Квантовая схемотехника напрямую связана с унитарными матрицами. Рассмотрим **еще раз** некоторые ее свойства, которые будем далее использовать.

Напомним, что унитарная матрица $\boldsymbol{M}$ по определению удовлетворяет следующим соотношениям:

$$MM^{\dagger} = M^{\dagger}M = I\,,$$

где $M^{\dagger} \equiv \left(M^{T}\right)^{*} = M^{T*}$ есть матрица **эрмитово** сопряженная матрице $\boldsymbol{M}$, а операция *эрмитового сопряженная* представляет собой транспонирование и комплексное сопряжение.

Полученные ранее из предыдущих разделов сведения об унитарных матрицах дают возможность сформулировать следующие два важных свойства унитарной матрицы.

Свойство 5.1

Если w, s, z, t — это действительные числа, то для унитарной матрицы $\boldsymbol{M} = \begin{bmatrix} w & s \\ z & t \end{bmatrix}$ справедливы следующие соотношения:

а)

$$\begin{cases} w^2 + z^2 = 1 \\ ws + zt = 0 \\ s^2 + t^2 = 1 \end{cases},$$

б)

$$\begin{cases} w^2 = t^2 \\ s^2 = z^2 \end{cases} \blacksquare$$

Предлагаем читателю (в качестве упражнения) убедиться в том, что $\boldsymbol{M}$ обладает этим свойством, а также посмотреть, как изменятся эти соотношения для комплексных значений w, s, z, t.

5.2. Амплитуда вероятности

«…мы и придумаем параметр *a*, который будем называть амплитудой вероятности, так как мы все равно не знаем, что это значит.»

Р. Фейнман [2, с.125]

«…В настоящее время представляется правильной любая общая закономерность, которую (как, например, свойства углового момента) мы в состоянии вывести непосредственно из принципа суперпозиции амплитуд вероятности. В то же время детали взаимодействий все еще ускользают от нас. Это наводит на мысль, что амплитуды вероятности будут существовать и в будущей теории, однако метод их вычисления может оказаться для нас весьма необычным...»

Р. Фейнман, А. Хибс [3, с.37]

«…гораздо более важным оказалось открытие того, что сложение вероятностей в природе происходит *не* по законам классической теории Лапласа. Квантовомеханические законы физического мира становятся очень близки к законам Лапласа лишь по мере того, как увеличивается размер объектов, участвующих в эксперименте. Поэтому обычная теория вероятностей вполне подходит для анализа поведения колеса рулетки, но не для рассмотрения отдельного электрона или фотона.»

Р. Фейнман, А. Хибс [3, с.13]

Теория вероятностей позволяет вычислять вероятности интересующих нас событий. Однако попытка ее применить для вычисления вероятностей состояний квантовых объектов оказывается порой безуспешной. Поэтому в квантовой механике выработаны специальные правила расчета вероятностей событий, происходящих с квантовыми объектами (системами). Одно из таких правил связано со следующим утверждением.

Утверждение 5.1

Вероятность любого события в идеальном эксперименте — т.е. эксперименте, где все определено настолько точно, насколько только это возможно, — равна квадрату некоторой величины ***a*** [2, с.132] (точнее квадрату модуля ***a***), которою мы называем *амплитудой вероятности*. Если это событие может происходить в нескольких взаимно исключающих вариантах, то [2, с.132] амплитуда вероятности ***a*** получается как сумма значений ***a*** для каждого из возможных вариантов (альтернатив) ■

Для того чтобы проиллюстрировать происхождение этого правила, обратимся к истории, а именно к специальным исследованиям и экспериментам. Рассмотрим следующий очень важный эксперимент, который, как мы увидим, непосредственно касается квантовых вычислений.

Пулемет *Р. Фейнмана* [2, с.118-120]

Пусть имеется (рис. 5.1) пулемет, стреляющий пулями через щель в бронированном щите 1, и есть еще 2-й бронированный щит (экран) с двумя отверстиями (щелями) с номерами 1 и 2, через которые могут пролетать эти пули (отверстия 1 и 2 подобраны специальным образом). За бронированным щитом 2 вдоль одной и той же линии расположен ряд (набор) пулеулавливателей (датчиков). В простейшем случае датчик может быть, например, в виде ящика с песком. В общем, может быть и один ящик. Полагаем, что все пули попадают обязательно в какой-то ящик. Число пуль, попавших в каждый ящик, можно подсчитать. Имеется разметка, указывающая местоположения датчиков на оси ***x***.

Этот эксперимент достаточно идеализирован. Во-первых, сам пулемет сильно дрожит (вибрирует) и качается, что приводит к тому, что пули летят не только в одном направлении. Возможно наличия рикошета от краев отверстий бронированного щита. Во-вторых, полагаем, что все пули имеют одинаковую скорость и энергию, а также что пули абсолютно не разрушаются. В ящик может попасть либо целая пуля, либо ничего не попадает. Самое главное, полагаем, что при выстреле одной пули в 2 разных ящика не может попасть по одной целой пуле (предполагается, что можно **различить** два последовательных выстрела).

Далее увидим, что свойство различимости очень важно.

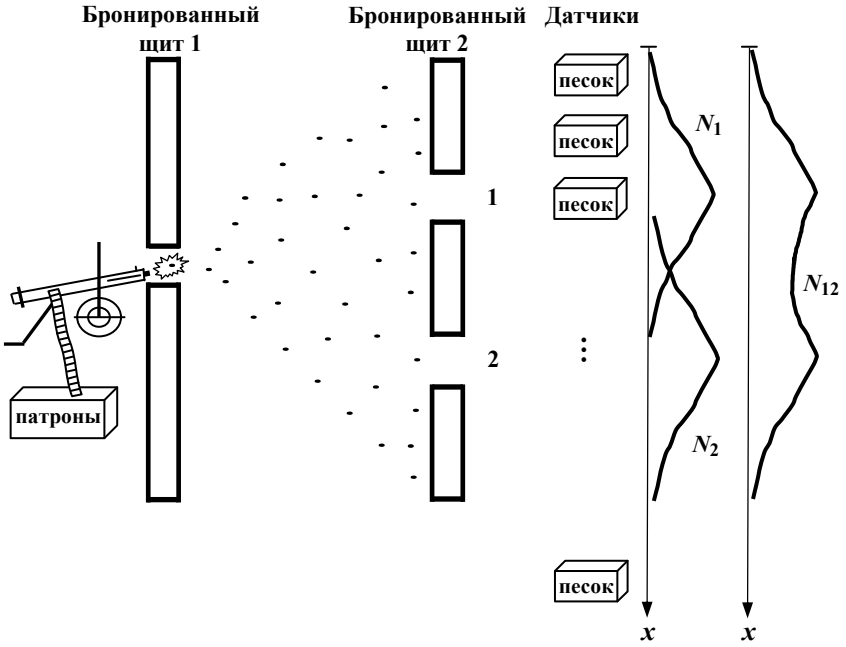


Рис. **5.1**

В эксперименте будем устанавливать ящик с песком (детектор) в разные места напротив 2-го бронированного щита так, чтобы менялась координата x (рис. 5.1), и будем считать, сколько пуль попадет в этот ящик за какой-нибудь период времени (например, за час). Если имеется набор ящиков (датчиков), то будем просто подсчитывать попавшие пули в разные ящики, установленные в разные координаты x. В итоге получим зависимости числа пуль N от x. В общем понятно, что если ящик стоит непосредственно за отверстием (щелью), то в него попадет много пуль, а если ящик стоит достаточно далеко от отверстия, то — мало, и чем дальше от отверстия будет стоять ящик, тем меньше попадет в него пуль и в итоге это число пуль уменьшиться до 0. Отверстия в бронированном щите 2 можно закрывать бронированной заслонкой.

Проведем три эксперимента. Первый эксперимент — открыто только одно отверстие 1. Второй эксперимент — открыто только одно отверстие 2. Третий эксперимент — открыты оба отверстия 1 и 2.

На рис. 5.1 показаны три кривые (т.е. зависимости числа пуль N от x). Эти кривые обозначены как N_1, N_2, N_{12} (нижние индексы у N показывают, какое отверстие было открыто). Если было открыто 1-е отверстие, то была получена кривая N_1; если было открыто 2-е отверстие — N_2; если открыты оба отверстия — N_{12}.

Анализируя все три кривые (рис. 5.1), можно сделать следующий простой, но очень важный вывод. Кривую N_{12} можно интерпретировать именно как сумму двух других кривых N_1, и N_2.

Утверждение 5.2
Число попаданий при двух открытых отверстиях представляет собой простую сумму числа попаданий через одно отверстие 1 и числа попаданий через одно отверстие 2 [2, с.120] ■

Для дальнейших рассуждений введем следующее определение интерференции.

Определение 5.1
Отсутствие интерференции [2, с.120] обозначает тот факт, что нужно просто сложить два числа.

Рассмотрим другой эксперимент с электронами, в некотором смысле аналогичный эксперименту с пулеметом.

Эксперимент с электронами [2, с.123-126; 3, с.13-24]

Пусть имеется (рис. 5.2) источник электронов S (отметим, что вместо электронов в эксперименте можно использовать свет). Из этого источника вылетают к экрану B электроны, имеющие одну и ту же энергию. В экране B есть два отверстия, обозначенных номерами 1 и 2 соответственно. Через эти два отверстия могут проходить электроны. Позади экрана B расположен в плоскости C детектор электронов. Если имеется только один детектор электронов, то его можно перемещать на расстояние x вдоль плоскости C (рис. 5.2). В случае установки многих детекторов электронов (каждый имеющий свою координату x) вместо одного можно наблюдать следующее. Два детектора никогда бы не срабатывали одновременно. Не было бы детектора, сработавшего только как бы «наполовину» (т.е. электрон попадает в детектор целиком либо ничего в детектор не попадает). Детектор регистрирует «*одиночный кор-*

пускулярный объект». Этот объект вылетает из источника ***S***, пролетает через какое-то отверстие в экране ***B*** и затем уже регистрируется детектором в точке ***x***. Результаты эксперимента представлены на рис. 5.3. В процессе эксперимента *измеряется* величина ***P***, при различных координатах ***x*** детектора, где ***P*** — вероятность того, что вылетевший из источника электрон попадет в точку с координатой ***x***. Схематично (в общих чертах) график функции вероятности ***P*** от ***x*** представлен на рис. 5.3 (кривая ***a***).

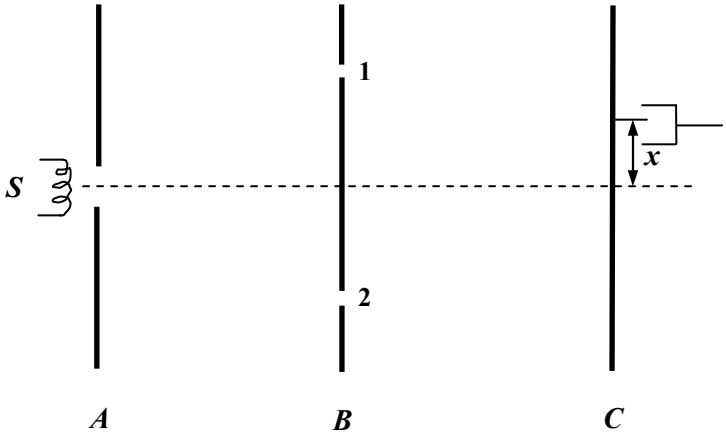


Рис. **5.2.** [**3**, с.14]

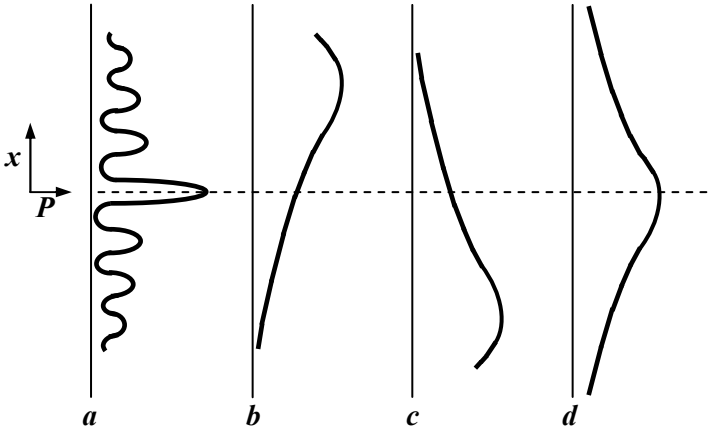


Рис .**5.3.** [**3**, с.15]

В эксперименте закрывали только одно отверстие 1 (рис. 5.2) и в результате получена кривая ***b*** на рис. 5.3 (вероятность $\boldsymbol{P_1}$). Затем закрывали только одно отверстие 2 (рис. 5.2) и в результате получена кривая ***c*** на рис. 5.3 (вероятность $\boldsymbol{P_2}$). При открытых обоих отверстиях получена кривая ***a*** на рис. 5.3. Это несколько неожиданный результат и он полностью не совпадает с результатом, аналогичным в эксперименте с пулями и двумя отверстиями. Кривая ***d*** есть сумма двух кривых ***b*** и ***c*** (но кривая ***a*** совсем не похожа на кривую ***d***). Эксперимент показывает, что $\boldsymbol{P \neq P_1 + P_2}$.

С электронами были проведены и более тонкие другие специальные эксперименты, суть которых состояла в следующем [3, с.18-24]. Исследователи выясняли влияние наблюдения на результаты эксперимента. Для этого (рис. 5.2) за отверстиями поместили источник света и стали наблюдать, через какое отверстие пройдет электрон. Так как электроны рассеивают свет, и само рассеивание происходит позади отверстия 2, то естественно можно понять, что электрон и прошел через именно это отверстие 2 (аналогичное справедливо и для другого отверстия 1). В эксперименте следили, через какое отверстие пролетает электрон и при этом (т.е. в то же время) определяли вероятность ***P*** (т.е. вероятность того, что электрон попадет в точку с координатой ***x***). Было установлено следующее неожиданное наблюдение. Если следят за электроном для установления отверстия, через которое он пролетел, то получается что $\boldsymbol{P = P_1 + P_2}$. А если не следят за электроном, то имеет место другой результат $\boldsymbol{P \neq P_1 + P_2}$ (далее увидим, что $\boldsymbol{P = |\varphi_1 + \varphi_2|^2}$). Наблюдение за электроном изменяет вероятность того, что электроны попадут в точку с координатой ***x***. Если начинают наблюдать за электроном, то кривая ***a*** (рис. 5.3) превращается в кривую ***d*** (рис. 5.3). Как отмечают *Р. Фейнман, А. Хибс* [3, с.20]: «Впервые это заметил Гейзенберг; он сформулировал свой принцип неопределенности, гласящий, что самосогласованность новой механики требует ограничения точности, с которой могут быть выполнены эксперименты. В нашем случае это означает, что любая попытка сконструировать прибор, определяющий то отверстие, через которое прошел электрон, и при этом настолько “деликатный”, чтобы не вызывать нарушения интерференционной картины, обречена на неудачу… Никаких исключений из принципа неопределенности до сих пор не обнаружено».

Для удобства дальнейшего изложения сформулируем принцип неопределенности по-другому и соответственно следующим образом (см. и ср. [3, с.21]):

«*Если в процессе выбора из нескольких путей эволюций удается проследить за каждым из них, то интерференция между ними становится невозможной*»■

Далее мы рассмотрим альтернативы подробно, а сейчас рассмотрим другой эксперимент уже с волнами.

Эксперимент с волнами [2, с.121-123; 3, с.16-17]

Отдельно отметим, что похожий эксперимент был проведен с волнами и двумя отверстиями. Этот эксперимент показывает хорошо известную в физике интерференцию волн. Аналогом вероятности $\boldsymbol{P(x)}$ в эксперименте с волнами является их интенсивность $\boldsymbol{I(x)}$. В точках с некоторыми координатами $\boldsymbol{x}$ часть волн именно в результате интерференции взаимопогашается (например, гребень от одной волны и впадина от другой волны в данной точке накладываются друг на друга). В результате получается набор различных максимумов и минимумов наподобие кривой, как на рис. 5.3 (кривая $\boldsymbol{a}$). Обычно принято [3, с.16], что *амплитуды* волн удобно представлять комплексными числами. В простейшем случае можно рассматривать волны на воде. Волнение воды характеризуется (см. [2, с.122-126]) высотой волны $\boldsymbol{h}$, а интенсивность волны $\boldsymbol{I}$ пропорциональна $\boldsymbol{h^2}$. Если открыты оба отверстия (т.е. 1 и 2), то в точке $\boldsymbol{x}$ наблюдается волна с высотой $\boldsymbol{h_{12}}$ и с интенсивностью $\boldsymbol{I_{12}}$. Если от отверстия 1 приходит в точку $\boldsymbol{x}$ бугор волны с положительной высотой $\boldsymbol{h_1}$ ($\boldsymbol{h_1}>0$) и с интенсивностью $\boldsymbol{I_1}$, а от отверстия 2 приходит впадина волны с отрицательной высотой $\boldsymbol{h_2}$ ($\boldsymbol{h_2}<0$) и с интенсивностью $\boldsymbol{I_2}$, то происходит компенсация именно одной высоты волны за счет другой. Интерференция между волнами вызывает ослабление интенсивности в одной точке и усиление интенсивности в другой точке. Наличие квадратов и приводит к следующим результатам [2, с.123]:

$$\boldsymbol{h_{12}= h_1+ h_2}, \tag{5.1}$$

но

$$\boldsymbol{I_{12} \neq I_1+ I_2} \text{ (интерференция)}; \tag{5.2}$$

$$\boldsymbol{I_{12}=(h_{12})^2; I_1=(h_1)^2; I_2=(h_2)^2}. \tag{5.3}$$

В эксперименте с волнами кривая изменения интенсивности $\boldsymbol{I_1}$ очень похожа на кривую $\boldsymbol{N_1}$, что и в эксперименте с пулями. Аналогично можно сказать и о кривых $\boldsymbol{I_2}$ и $\boldsymbol{N_2}$, полученных в двух разных экспериментах (с волнами и с пулями). Однако кривая $\boldsymbol{I_{12}}$ никак не похожа на кривую $\boldsymbol{N_{12}}$, но похожа на кривую ***a*** на рис. 5.3 в эксперименте с электронами.

Таким образом, можно сказать следующее [2, с.126]:

«…электроны попадают в детектор дискретными порциями, как если бы это были частицы, но вероятности попадания этих частиц определяются по тем же законам, по каким определяется интенсивность волнения воды. Именно в этом смысле можно говорить, что, с одной точки зрения, электрон ведет себя, как частица, а с другой — как волна».

В экспериментах с волнами и с пулями при сравнении результатов как бы взаимозаменялись $\boldsymbol{I}$ и $\boldsymbol{N}$. Тогда согласно *Р. Фейнману* [2, с.125]:

«…нам придется заменить h на что-то другое, совсем новое, — это никакая не высота, — в связи с чем мы и придумаем параметр a, который будем называть амплитудой вероятности, так как мы все равно не знаем, что это значит».

Теперь можно сформулировать утверждение о вероятности $\boldsymbol{P(x)}$ следующим образом [3, с.17] (полагая далее что φ — это и есть тот самый параметр a).

Утверждение 5.3

Вероятность $\boldsymbol{P(x)}$ представляет собой квадрат модуля некоторой комплексной величины $\varphi(x)$, которую мы назовем *амплитудой вероятности* попасть в точку $\boldsymbol{x}$ (если учитывается спин электрона, то это гиперкомплексная величина). Далее, $\varphi(x)$ равна сумме двух вкладов: амплитуды φ_1 попадания в точку $\boldsymbol{x}$ через отверстие 1 и амплитуды φ_2 попадания в ту же точку через отверстие 2 [3, с.17]■

ВАЖНО ПОМНИТЬ [3, с.17]. Специалисты вычисляют интенсивность (т.е. квадрат модуля амплитуды) волн, которые достигли бы датчика в точке $\boldsymbol{x}$, а затем интерпретируют эту интенсивность именно уже как вероятность события, что частица попадет в эту точку $\boldsymbol{x}$.

Таким образом, можно полагать, что [3, с. 17] существуют комплексные числа φ_1 и φ_2, причем такие, что выполнимы

следующие соотношения [3, с.17]:

$$\boldsymbol{P}=|\varphi|^2; \quad (5.4)$$

$$\varphi=\varphi_1+\varphi_2; \quad (5.5)$$

$$\boldsymbol{P}_1=|\varphi_1|^2; \quad (5.6)$$

$$\boldsymbol{P}_2=|\varphi_2|^2. \quad (5.7)$$

ОТМЕТИМ [3, с. 17]. Амплитуду вероятности на практике вычисляют следующим образом. Например амплитуду φ_1, как решение волнового уравнения, описывающего распространения волн от источника $\boldsymbol{S}$ до точки 1 и из точки 1 в точку $\boldsymbol{x}$.

Дадим следующее важное определение *интерференции*.

Определение 5.2

Интерференция [6, с.232, 261] — это специфическое квантово-механическое явление, связанное со сложением амплитуд вероятностей (т.е. возможна интерференция без волн; интерференция наблюдается для всех микрообъектов: фотонов, электронов и т.п.).

Вероятность в квантовой механике

В квантовой механике понятие вероятности $\boldsymbol{P}$ как таковой имеет обычный смысл. При неоднократном повторении опыта относительное число интересующих исходов составит приблизительно $\boldsymbol{P}$, где $\boldsymbol{P}$ — вероятности интересующего события. Т.е. никаких изменений самого понятия вероятности не делается, но зато существенно меняется сам способ вычисления этой вероятности. Полагают, что [3, с.25]: «*С физической точки зрения две траектории представляют собой независимые альтернативы; однако было бы ошибкой думать, что полная вероятность в этом случае есть сумма* P_1+P_2». Отметим, что две *траектории* — это два *канала эволюции*. Перед тем как окончательно ввести новые правила сложения вероятностей, уточним понятие «*альтернатива*». **Во-первых** — это концепция взаимоисключения, т.е. отверстия 1 и 2 есть [3, с.25] *несовместимые альтернативы* только в том случае, если одно из этих отверстий закрыто, или в том случае, если действует прибор, способный однозначно определить то отверстие, через которое именно и прошел электрон. **Во-вторых** — это концепция комбинирования или интерференции, т.е. [3, с.25] *интерференция* означает здесь то же, что и в оптике. Когда физически эквивалентные альтернативы невозможно различить никаким экспериментом, они обязательно *интерферируют*.

ВАЖНО ПОМНИТЬ. В случае, когда физически эквивалентные альтернативы невозможно различить никаким опытом (т.е. экспериментом), они обязательно *интерферируют*.

Сформулируем два очень важных определения, касающихся альтернатив.

Определение 5.3

Несовместимые альтернативы [3, с.25] — будем говорить, что отверстия 1 и 2 представляют собой *несовместимые альтернативы* в том случае,

если одно из этих отверстий закрыто;

или

если действует прибор, который может однозначно определить, через какое отверстие прошел электрон.

Определение 5.4

Интерферирующие альтернативы [3, с.25] — будем говорить, что по отношению к электрону отверстия 1 и 2 представляют собой *интерферирующие альтернативы* в том случае,

если открыты оба отверстия;

и

если не предпринимается попыток определить, через какое отверстие пролетел электрон

(именно в этом случае необходимо изменить правила получения вероятностей и выбрать их в виде (5.4) и (5.5)).

Важно уяснить следующее. Имеет место быть некоторая величина, которую в квантовой механике принято называть *амплитудой вероятности*. Эта амплитуда вероятности сопоставляется каждому возможному в природе способу осуществления события [3, с.31]. Полная амплитуда вероятности получается путем сложения амплитуд каждой альтернативы. При этом квадрат модуля амплитуды интерпретируется как вероятность соответствующего события. Наблюдение (измерение) прерывает развитие процесса еще до его завершения, что ведет [3, с.31-32] к необходимости изменить вид выражения для полной амплитуды.

Рассмотрим следующий простой, но очень важный пример с электронами и двумя отверстиями.

Пример 5.1. Присутствие 2-х видов альтернатив [3, с.26].

Пусть в некотором эксперименте с 2-мя отверстиями и электронами исследователя интересует вероятность попадания электрона в некоторую точку в пределах 1 см от центра экрана (под этой вероятностью можно понимать вероятность того, что сработавший детектор (датчик) находился в пределах 1 см от точки с координатой x=0, если сами датчики были расположены по всему экрану и один какой-то датчик из них наверняка сработал бы, при попадании электрона на экран). Для данного эксперимента характерно то, что существуют различные вероятности того, что электрон попадет в детектор (т.е. датчик зарегистрирует этот электрон) через 1-е или 2-е отверстие. В данном случае отверстия — это *интерферирующие альтернативы,* причем *детекторы* — это *несовместимые альтернативы*. При вычислении искомой вероятности следует поступать в следующей последовательности [3, с.26]:

1) складываем и получаем для фиксированного x сумму $\varphi_1 + \varphi_2$;
2) возводим эту сумму в квадрат (точнее вычисляем квадрат ее модуля);
3) полученные вероятности интегрируем по x от (–1) до 1.

Имея определенный опыт, можно понять какой вид альтернатив следует использовать ■

ОТМЕТИМ [3, с.34]. Амплитуда вероятности в квантовой механике определяется из решения уравнения Шрёдингера.

В теории вероятностей одним из ключевых элементов являются *совместные* и *несовместные* события, *зависимые* и *независимые* события, а также и *условная вероятность* некоторого события (это было рассмотрено в книге 1). *Теорема сложения вероятностей несовместных событий* и *Теорема умножения вероятностей событий* содержат эти элементы и позволяют вычислять вероятности интересующих событий. Однако, как отмечается в работе [6, с.260], эти события в теории вероятностей всегда подразумеваются *различимыми*. Оказалось, что в квантовой механике, как говорят специалисты [6, с.260]: «…*Не сама вероятность, а амплитуда вероятности (волновая функция) оказывается первичной величиной… С интерференцией амплитуд органически связан квантово-механический принцип суперпозиции состояний, отражающий специфику* «взаимоотношений» состояний микрообъекта».

Связь теории вероятностей и квантовой механики в глубинном понимании не столь очевидна и далеко не так проста. Приведем еще одну важную на наш взгляд цитату [6, с.263]: «…можно утверждать, что классическая физика по самому стилю своей философии (однозначность предсказаний в теориях динамического типа, подход к любому объекту как «набору» определенных «деталей», рассмотрения явления как последовательности определенных элементарных событий) тяготеет к метафизике».

В квантовой механике в отличие от теории вероятностей введены **несовместимые альтернативы** и **интерферирующие альтернативы**. Наряду с этим можно и будем говорить не об *интерферирующих* или *несовместных* альтернативах, а о различимых или неразличимых альтернативах, как в работе [6, с. 236-241] (иногда говорят о *частично* различимых альтернативах). Для этого введем следующие два определения.

Определение 5.5

Альтернативы различимы [6, с.237] — известно, какой из вариантов перехода реализуется в том или ином опыте. В данном случае вероятность перехода есть сумма вероятностей переходов, отвечающих разным альтернативам.

Определение 5.6

Альтернативы неразличимы [6, с.237] — неизвестно, какой из вариантов перехода реализуется в том или ином опыте. Существенно, что в этом случае *надо складывать не вероятности альтернативных переходов, а амплитуды вероятностей*.

ОТМЕТИМ [6, с.237]. Вариант неразличимых альтернатив специфичен именно для квантовой физики (механики). В классической физике этот вариант невозможен в принципе, поскольку всегда можно проследить за любым перемещением объекта.

В квантовой механике широко используется понятие *волновая функция*. Однако далее в основном будут использоваться только *амплитуды вероятностей.* Это связано с тем, что как считают специалисты [6, с.236]: «*…Амплитуда и волновая функция — это, строго говоря, одно и то же*».

Дадим следующее определение *амплитуды вероятности.*

Определение 5.7

Амплитуда вероятности [6, с.236] есть величина, квадрат модуля которой равен вероятности.

Опираясь на *Утверждения 5.1, 5.3* и на [3], сформулируем следующие три квантово-механических правила для случая неразличимых альтернатив. Эти правила позволяют вычислять вероятность перехода квантовой системы из одного состояния в другое при рассмотрении квантовых *вычислений* и квантовых *алгоритмов*.

Правило 5.1

Амплитуда вероятности перехода квантовой системы по траектории (т.е. по пути эволюции) из одного положения (состояния) в другое положение (состояние) равна ***произведению*** *амплитуд вероятностей всех процессов, связывающих между собой состояния, принадлежащие данной траектории* ■

Правило 5.2

Амплитуда вероятности перехода квантовой системы из начального положения (состояния) в конечное положение (состояние) равна ***сумме*** *амплитуд вероятностей переходов по всем возможным траекториям, связывающим эти положения (состояния)* ■

Правило 5.3

Вероятность перехода квантовой системы из начального положения (состояния) в конечное положение (состояние) равна ***квадрату модуля*** *амплитуды вероятности этого перехода* ■

Аналогичные правила для случая различимых альтернатив и для классических систем были представлены ранее, как *Правила* 1.1 и 1.2 . Предлагаем читателю вернуться к книге 1 и сравнить правила вычисления вероятности перехода *классической* системы из одного состояния в другое с правилами вычисления вероятности перехода *квантовой* системы. Можно заметить, что в квантовом случае наряду с *вероятностью*, как таковой, используется еще и *амплитуда вероятности.* При этом именно *амплитуда вероятности* играет

определяющую роль.

Для того чтобы уяснить и более глубоко понять саму суть вычислений некоторых «простых» вероятностей в квантовой механике, обратимся к наглядным и очень поучительным примерам, а именно к специальным исследованиям и экспериментам. Эти характерные примеры показывают, как надо вычислять вероятность в данном конкретном случае с точки зрения квантовой механики.

Будем обозначать *вероятность* перехода из состояния s в состояние f (см. [6, с.236]) как $w(s \to f)$, а *амплитуду вероятности* этого перехода как $\Psi(s \to f)$, причем $w(s \to f)=|\Psi(s \to f)|^2$. Пусть есть несколько вариантов перехода микрообъекта из s в f (т.е. есть несколько альтернатив), которым соответствуют следующие амплитуды вероятностей [6, с.237]:

$$\Psi_1(s \to f),\ \Psi_2(s \to f), \Psi_3(s \to f)\ ,\ \ldots, \Psi_i(s \to f)\ ,\ \ldots\ . \qquad (5.8)$$

В случае если альтернативы различимы, то справедливо следующее соотношение [6, с.237]:

$$\left|\psi\left(s \to f\right)\right|^2 = \sum_i \left|\psi_i\left(s \to f\right)\right|^2 . \qquad (5.9)$$

В случае если альтернативы неразличимы, то справедливо следующие соотношения [6, с.237]:

$$\psi\left(s \to f\right) = \sum_i \psi_i\left(s \to f\right) \qquad (5.10)$$

$$\left|\psi\left(s \to f\right)\right|^2 = \left|\sum_i \psi_i\left(s \to f\right)\right|^2 . \qquad (5.11)$$

ОТМЕТИМ. Специалисты полагают [6, с.241], что «*…Теорема сложения вероятностей работает, когда альтернативы полностью различимы. Она не работает в случае частичной различимости и тем более полной неразличимости. Во всех этих случаях наблюдается интерференция амплитуд вероятностей*».

ОТМЕТИМ [6, с.235, 236]. В эксперименте с электронами и щелями возникает *интерференция*, если опыт поставлен таким образом, что неизвестно, где именно пролетел электрон. Был сделан вывод, что [6, с.235]: «*Как только начинается контролирование процесса прохождения электронов через экран с щелями, интерференция исчезает*. Можно сказать, что наблюдение за поведением электронов в интерферометре *разрушает интерференцию*».

Пример 5.2. Применение *Правил* 5.1; 5.1; 5.3 [6, с.233-244].

Пусть в некотором эксперименте с 2-мя отверстиями (щелями ***A*** и ***B***), электронами и фотонами в интерферометре исследователя интересует вероятность перехода электрона из начального состояния *s* в конечное состояние *f*. Около щелей ***A*** и ***B*** находятся источник света **Ω** и фотоприемники ***a*** и ***b*** (рис. 5.4). Назначение этих 2-х фотоприемников состоит в том, чтобы регистрировать свет, который рассеется около щели.

Введем следующие обозначения [6, с.238-239]:

$\Psi_A(s \to f)$ — *амплитуда вероятности* перехода из *s* в *f* с прохождением электрона через щель ***A***;

$\Psi_B(s \to f)$ — *амплитуда вероятности* перехода из *s* в *f* с прохождением электрона через щель ***B***;

$\varphi(\Omega \to A \to a)$ — *амплитуда вероятности* перехода, соответствующая тому, что фотон, испущенный источником света **Ω** рассеялся на электроне, который прошел через щель ***A***, а затем этот фотон попал в фотоприемник ***a***;

$\varphi(\Omega \to A \to b)$ — *амплитуда вероятности* перехода, соответствующая тому, что фотон, испущенный источником света **Ω** рассеялся на электроне, который прошел через щель ***A***, а затем этот фотон попал в фотоприемник ***b***;

$\varphi(\Omega \to B \to a)$ — *амплитуда вероятности* перехода, соответствующая тому, что фотон, испущенный источником света **Ω** рассеялся на электроне, который прошел через щель ***B***, а затем этот фотон попал в фотоприемник ***a***;

$\varphi(\Omega \to B \to b)$ — *амплитуда вероятности* перехода, соответствующая тому, что фотон, испущенный источником света **Ω** рассеялся на электроне, который прошел через щель ***B***, а затем этот фотон попал в фотоприемник ***b***;

φ_1 — *амплитуда вероятности* фотону рассеяться в *ближний* к соответствующей щели фотоприемник;

φ_2 — *амплитуда вероятности* фотону рассеяться в *дальний* от соответствующей щели фотоприемник.

Может случиться так, что фотон, если рассеяние на электроне происходит, ни в один из приемников не попадет. Так вот такие электроны исследователя не интересуют. Экран – детектор ***D*** разделен по оси ***x*** (рис. 5.4) на небольшие отрезки.

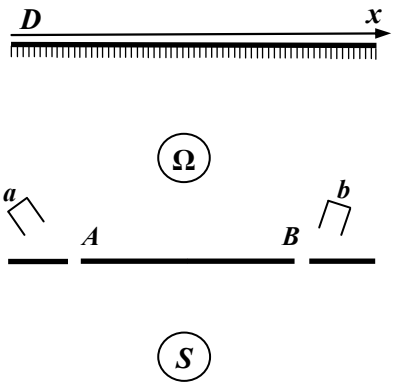


Рис. **5.4.** [**6**, с.234]

Тогда конечное состояние электрона — это состояние *f*, соответствующее регистрации электрона в пределах какого-то из этих отрезков.

Из соображений симметрии можно полагать, что справедливы следующие соотношения [6, с.239]:

$$\varphi(\boldsymbol{\Omega}\rightarrow \boldsymbol{A}\rightarrow \boldsymbol{a}) = \varphi(\boldsymbol{\Omega}\rightarrow \boldsymbol{B}\rightarrow \boldsymbol{b}) \equiv \varphi_1\,; \qquad (5.12)$$

$$\varphi(\boldsymbol{\Omega}\rightarrow \boldsymbol{A}\rightarrow \boldsymbol{b}) = \varphi(\boldsymbol{\Omega}\rightarrow \boldsymbol{B}\rightarrow \boldsymbol{a}) \equiv \varphi_2\,. \qquad (5.13)$$

Случай А (присутствие альтернатив).

Электрон совершает переход из *s* в *f* и одновременно фотон рассеивается в фотоприемнике ***a***. В этом случае имеются следующие 2 альтернативы (будем выделять две траектории):

1) электрон пролетел через щель ***A***, фотон рассеивается в *ближний* к ней фотоприемник (т.е. это будет ***a***);
2) электрон пролетел через щель ***B***, фотон рассеивается в *дальний* от нее фотоприемник (т.е. это будет ***a***).

Переходы в траекториях независимы. Зная $\Psi_A(s\rightarrow f)$ и φ_1 и применяя к ним *Правило* 5.1, получим, что

$$Д_1 = \Psi_A(s\rightarrow f)\cdot\varphi_1. \qquad (5.14)$$

Аналогично получаем, что

$$Д_2 = \Psi_B(s\rightarrow f)\cdot\varphi_2. \qquad (5.15)$$

Далее, поскольку неизвестна щель, через которую пролетит электрон, то альтернативы с амплитудами $Д_1$ и $Д_2$ — неразличимы.

Поэтому, зная $Д_1$ и $Д_2$ и применяя к ним Правило 5.2, получим, что

$$\Psi = Д_1 + Д_2 = \Psi_A(s \to f) \cdot \varphi_1 + \Psi_B(s \to f) \cdot \varphi_2, \qquad (5.16)$$

где Ψ — *амплитуда вероятности* того, что электрон попадет из s в состояние f, а фотон — в фотоприемник ***a***.

Случай Б (присутствие альтернатив).
Электрон совершает переход из s в f, и одновременно фотон рассеивается в фотоприемнике ***b***. В этом случае имеются следующие 2 альтернативы (т.е. две траектории):

1) электрон пролетел через щель ***A***, фотон рассеивается в *дальний* от нее фотоприемник (т.е. это будет ***b***);
2) электрон пролетел через щель ***B***, фотон рассеивается в *ближний* от нее фотоприемник (т.е. это будет ***b***).

Переходы в траекториях независимы. Зная $\Psi_A(s \to f)$ и φ_2 и применяя к ним *Правило* 5.1, получим, что

$$Ё_1 = \Psi_A(s \to f) \cdot \varphi_2. \qquad (5.17)$$

Аналогично получаем, что

$$Ё_2 = \Psi_B(s \to f) \cdot \varphi_1. \qquad (5.18)$$

Далее, поскольку неизвестна щель, через которую пролетит электрон, то альтернативы с амплитудами $Ё_1$ и $Ё_2$ — неразличимы. Поэтому, зная $Ё_1$ и $Ё_2$ и применяя к ним *Правило* 5.2, получим, что

$$\Phi = Ё_1 + Ё_2 = \Psi_A(s \to f) \cdot \varphi_2 + \Psi_B(s \to f) \cdot \varphi_1, \qquad (5.19)$$

где Φ — *амплитуда вероятности* того, что электрон попадет из s в состояние f, а фотон — в фотоприемник ***b***.

Случай В (применение *Правила* 5.3).

Получим $w(s \to f)$ — вероятность перехода $s \to f$ независимо от того, где зарегистрируют рассеянный электроном фотон (в фотоприемнике ***a*** или ***b***). В данном варианте имеется уже различимость того, куда попадет фотон (в ***a*** или ***b***). Поэтому применяем *Правило* 5.3 и *Теорему сложения вероятностей несовместных событий* и получаем следующее соотношение для искомой вероятности [6, с.240]:

$$w(s \to f) = |\Psi|^2 + |\Phi|^2 . \qquad (5.20)$$

Подставим (5.16) и (5.19) в (5.20) и получим следующее соотношение [6, с.240]:

$$w(s \to f) = | \Psi_A(s \to f) \cdot \varphi_1 + \Psi_B(s \to f) \cdot \varphi_2 |^2 + \\ + | \Psi_A(s \to f) \cdot \varphi_2 + \Psi_B(s \to f) \cdot \varphi_1 |^2 . \qquad (5.21)$$

Случай Г (полная НЕразличимость альтернатив).

Контроль прохождения электронов через щели отсутствует. Для этого допустим, что фотоны рассеиваются как в ближний, так и в дальний от щели фотоприемник с равной вероятностью 1/2. Тогда справедливы следующие соотношения [6, с.240]:

$$\varphi_1 = \varphi_2 = \varphi, \quad | \varphi |^2 = 1/2. \qquad (5.22)$$

Из (5.22) и (5.21) получим следующее соотношение [6, с.240]:

$$w(s \to f) = 2 \cdot | \varphi |^2 \cdot | \Psi_A(s \to f) + \Psi_B(s \to f) |^2 = \\ = | \Psi_A(s \to f) + \Psi_B(s \to f) |^2 . \qquad (5.23)$$

Случай Д (полная различимость альтернатив).

Контроль прохождения электронов через щели имеется. Для этого допустим, что фотоны рассеиваются только в ближний от щели фотоприемник, а в дальний — не могут. Тогда в этом случае справедливы следующие соотношения [6, с.240]:

$$\varphi_2 = 0, \quad | \varphi_1 |^2 = 1. \qquad (5.24)$$

Из (5.24), (5.20), (5.21) следует такое соотношение [6, с.241]:

$$w(s \to f) = | \Psi_A(s \to f) |^2 + | \Psi_B(s \to f) |^2 . \qquad (5.25)$$

Случай Е (частичная различимость альтернатив).

В эксперименте допускается и то, что [6, с.241]: «…возможен непрерывный набор ситуаций, когда вероятность фотону рассеяться в дальний фотоприемник отлична от нуля, но при этом меньше вероятности рассеяться в ближний фотоприемник». Эти все ситуации отражены в (5.21).

Управляя условием выполнения эксперимента, можно изменять отношение $|\varphi_2|^2 \big/ |\varphi_1|^2$. Если это отношение *увеличивается*, приближаясь к 1, то различимость альтернатив становится меньше, а если *уменьшается*, приближаясь к 0, то различимость альтернатив становится больше.

На этом закончим рассмотрение данного примера ■

Пример 5.3. Соединение 2-х элементов (см. и ср. [1, с.40-41; 7]).

Вернемся к ***Примеру 1.39*** (в книге 1) и к двум (рис. 5.5**в**,**г**) последовательно соединенным *квантовым* элементам $\sqrt{\boldsymbol{not}}$ и двум элементам *Адамара*, обозначаемые на *квантовых* схемах как $\boldsymbol{H}$.

Эти элементы $\boldsymbol{H}$ и $\sqrt{\boldsymbol{not}}$ (рис. 5.5**а,б**) преобразуют входной сигнал $\boldsymbol{A}$ (т.е. $|0\rangle$ или $|1\rangle$) в выходной сигнал $\boldsymbol{B}$ (т.е. $|0\rangle$ или $|1\rangle$) в соответствии со следующими амплитудами вероятности $\boldsymbol{a_{AB}}$:

$\boldsymbol{a_{00}}$ — амплитуда вероятности перехода из $|0\rangle$ в $|0\rangle$;

$\boldsymbol{a_{10}}$ — амплитуда вероятности перехода из $|0\rangle$ в $|1\rangle$;

$\boldsymbol{a_{01}}$ — амплитуда вероятности перехода из $|1\rangle$ в $|0\rangle$;

$\boldsymbol{a_{11}}$ — амплитуда вероятности перехода из $|1\rangle$ в $|1\rangle$.

Отметим, что эти амплитуды вероятности в общем случае есть комплексные числа $\boldsymbol{a_{AB}} = b_{AB} + \boldsymbol{i}d_{AB}$, а $\boldsymbol{i} = \sqrt{-1}$.

Требуется построить диаграмму переходов и найти вероятность того, что на выходе квантовой схемы (рис. 5.5**в**,**г**) будет $|1\rangle$, если на вход этой схемы подан $|0\rangle$.

Решение

1). Введем состояния системы $\boldsymbol{S_j}$, где $\boldsymbol{j}$ — число 0 для $|0\rangle$ или 1 для $|1\rangle$, причем начальное состояние (точка $\boldsymbol{O}$) есть $\boldsymbol{S_0}$, а конечное — $\boldsymbol{S_1}$ (т.е. точка $\boldsymbol{C}$).

2). Построим диаграмму, укажем амплитуды вероятности переходов (процессов) и выясним, какие траектории могут иметь место в данном случае (рис. 5.6).

Все амплитуды вероятности переходов известны, так как известны все квантовые элементы (т.е. это элементы *Адамара* или элементы $\sqrt{\boldsymbol{not}}$).

3). Требуется определить вероятность $P_{\mathbf{01}}$ — вероятность перехода системы ($O \to C$, см. рис. 5.6) из состояния $\boldsymbol{S_0}$ в $\boldsymbol{S_1}$ (точка $\boldsymbol{C}$).

4). Вычислим $P_{\mathbf{01}}$. Согласно диаграмме (см. рис. 5.6) из т. $\boldsymbol{O}$ в т. $\boldsymbol{C}$ можно перейти только по 2-м следующим траекториям:

траектория 1: $\{\boldsymbol{S_0}, \boldsymbol{S_1}, \boldsymbol{S_1}\}$; траектория 2: $\{\boldsymbol{S_0}, \boldsymbol{S_0}, \boldsymbol{S_1}\}$.

Применяем *Правило* 5.1 для вычисления $A_{\text{траектории1}}$ и $A_{\text{траектории2}}$, т.е. амплитуд вероятности перехода *квантовой* системы по каждой траектории.

Квантовые элементы *Адамара* и $\sqrt{not}$

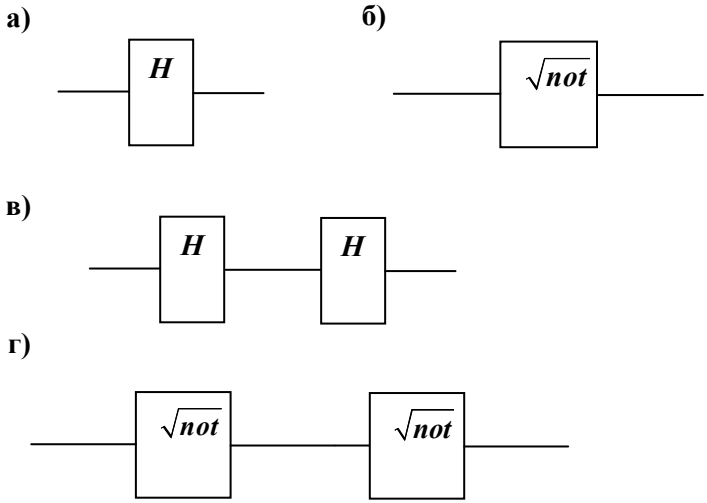


Рис. **5.5**

Диаграмма переходов для 2-х элементов

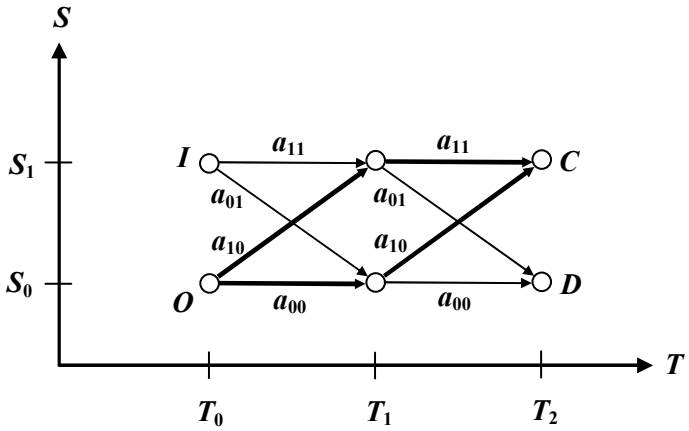


Рис. **5.6**

В данном случае эти амплитуды вероятности есть

$$A_{\text{траектории1}} = \boldsymbol{a_{10}a_{11}};\quad A_{\text{траектории2}} = \boldsymbol{a_{00}a_{10}}.$$

Применяем *Правило* 5.2 для вычисления A_{01} — амплитуды вероятности перехода системы из состояния $\boldsymbol{S_0}$ в состояние $\boldsymbol{S_1}$. В данном случае эта амплитуда вероятности есть

$$A_{01} = P\left(O \to C\right) = A_{\text{траектории1}} + A_{\text{траектории2}} = \boldsymbol{a_{10}a_{11}} + \boldsymbol{a_{00}a_{10}} \text{ или}$$

$$A_{01} = \boldsymbol{a_{10}a_{11}} + \boldsymbol{a_{00}a_{10}} = \boldsymbol{a_{10}}(\boldsymbol{a_{11}} + \boldsymbol{a_{00}}).$$

Применяем *Правило* 5.3 для вычисления вероятности P_{01} перехода системы из состояния $\boldsymbol{S_0}$ в состояние $\boldsymbol{S_1}$. В данном случае эта вероятность есть

$$P_{01} = |\, A_{01}\,|^2 = |\, \boldsymbol{a_{10}a_{11}} + \boldsymbol{a_{00}a_{10}}\,|^2.$$

5). Аналогично можно вычислить, что

$$A_{00} = P\left(O \to D\right) = \boldsymbol{a_{00}a_{00}} + \boldsymbol{a_{10}a_{01}} \quad \text{или}$$

$$P_{00} = |\, A_{00}\,|^2 = |\, \boldsymbol{a_{00}a_{00}} + \boldsymbol{a_{10}a_{01}}\,|^2.$$

А также, что

$$A_{10} = P\left(I \to D\right) = \boldsymbol{a_{01}a_{00}} + \boldsymbol{a_{11}a_{01}} \text{ и } P_{10} = |\, A_{10}\,|^2;$$

$$A_{11} = P\left(I \to C\right) = \boldsymbol{a_{11}a_{11}} + \boldsymbol{a_{01}a_{10}} \text{ и } P_{11} = |\, A_{11}\,|^2.$$

Получаем, что

$$P_{00} = |\boldsymbol{a_{00}a_{00}} + \boldsymbol{a_{10}a_{01}}|^2,\ P_{10} = |\, \boldsymbol{a_{01}a_{00}} + \boldsymbol{a_{11}a_{01}}|^2,\ P_{11} = |\boldsymbol{a_{11}a_{11}} + \boldsymbol{a_{01}a_{10}}|^2.$$

6). В случае элемента $\sqrt{\boldsymbol{not}} = \exp\left(i\pi/4\right)\cdot\sqrt{\boldsymbol{X}}$, зная амплитуды вероятностей $\boldsymbol{a_{AB}}$ [7]

$$\boldsymbol{a_{00}} = \boldsymbol{a_{11}} = \frac{i}{\sqrt{2}};\qquad \boldsymbol{a_{01}} = \boldsymbol{a_{10}} = \frac{1}{\sqrt{2}};$$

можно получить следующие соотношения:

$$P_{01} = |\, A_{01}\,|^2 = |\, \boldsymbol{a_{10}a_{11}} + \boldsymbol{a_{00}a_{10}}\,|^2 =$$

$$= \left|\frac{1}{\sqrt{2}}\frac{i}{\sqrt{2}} + \frac{1}{\sqrt{2}}\frac{i}{\sqrt{2}}\right|^2 = \left|\frac{i}{2} + \frac{i}{2}\right|^2 = |i|^2 = 1.$$

$$P_{10} = |\, A_{10}\,|^2 = |\, \boldsymbol{a_{01}a_{00}} + \boldsymbol{a_{11}a_{01}}\,|^2 =$$

$$= \left|\frac{1}{\sqrt{2}}\frac{i}{\sqrt{2}} + \frac{i}{\sqrt{2}}\frac{1}{\sqrt{2}}\right|^2 = \left|\frac{i}{2} + \frac{i}{2}\right|^2 = |i|^2 = 1.$$

$$P_{00}=|A_{00}|^2=|\boldsymbol{a}_{00}\boldsymbol{a}_{00}+\boldsymbol{a}_{10}\boldsymbol{a}_{01}|^2=$$
$$=\left|\frac{i}{\sqrt{2}}\frac{i}{\sqrt{2}}+\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}\right|^2=\left|\frac{i^2}{2}+\frac{1}{2}\right|^2=\left|-\frac{1}{2}+\frac{1}{2}\right|^2=0.$$

$$P_{11}=|A_{11}|^2=|\boldsymbol{a}_{11}\boldsymbol{a}_{11}+\boldsymbol{a}_{01}\boldsymbol{a}_{10}|^2=$$
$$=\left|\frac{i}{\sqrt{2}}\frac{i}{\sqrt{2}}+\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}\right|^2=\left|\frac{i^2}{2}+\frac{1}{2}\right|^2=\left|-\frac{1}{2}+\frac{1}{2}\right|^2=0.$$

В случае элемента *Адамара* $\boldsymbol{H}$, зная амплитуды вероятностей $\boldsymbol{a}_{AB}$ [1, с.40]:

$$\boldsymbol{a}_{00}=\boldsymbol{a}_{01}=\boldsymbol{a}_{10}=\frac{1}{\sqrt{2}};\quad \boldsymbol{a}_{11}=\frac{-1}{\sqrt{2}};$$

можно получить аналогичные следующие соотношения:

$$P_{01}=|A_{01}|^2=|\boldsymbol{a}_{10}\boldsymbol{a}_{11}+\boldsymbol{a}_{00}\boldsymbol{a}_{10}|^2=$$
$$=\left|\frac{1}{\sqrt{2}}\frac{(-1)}{\sqrt{2}}+\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}\right|^2=\left|\frac{(-1)}{2}+\frac{(+1)}{2}\right|^2=0.$$

$$P_{10}=|A_{10}|^2=|\boldsymbol{a}_{01}\boldsymbol{a}_{00}+\boldsymbol{a}_{11}\boldsymbol{a}_{01}|^2=$$
$$=\left|\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}+\frac{(-1)}{\sqrt{2}}\frac{1}{\sqrt{2}}\right|^2=\left|\frac{(+1)}{2}+\frac{(-1)}{2}\right|^2=0.$$

$$P_{00}=|A_{00}|^2=|\boldsymbol{a}_{00}\boldsymbol{a}_{00}+\boldsymbol{a}_{10}\boldsymbol{a}_{01}|^2=$$
$$=\left|\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}\right|^2=\left|\frac{1}{2}+\frac{1}{2}\right|^2=1.$$

$$P_{11}=|A_{11}|^2=\boldsymbol{a}_{11}\boldsymbol{a}_{11}+\boldsymbol{a}_{01}\boldsymbol{a}_{10}|^2=$$
$$=\left|\frac{(-1)}{\sqrt{2}}\frac{(-1)}{\sqrt{2}}+\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}\right|^2=\left|\frac{(+1)}{2}+\frac{(+1)}{2}\right|^2=1.$$

7). $P_{01}=1$ для $\sqrt{\boldsymbol{not}}$ и $P_{01}=0$ для $\boldsymbol{H}$. И тем самым задача решена■

Обсудим кратко рассмотренный выше ***Пример 5.3***.
В квантовых схемах полагают [1, с.238-239], что измерение можно представлять в них (выполнять или производить) только в конце всех вычислений. В данном случае имеет место полная НЕразличимость альтернатив, а значит применимы квантово-механические *Правила* 5.1, 5.2, 5.3 для квантовых схем (рис. 5.5**в**,**г**).

Иногда на практике для удобства рассмотрения можно изображать квантовые схемы и диаграмму переходов на одном рисунке одновременно, как показано для 1-го элемента $\sqrt{not}$ на рис. 5.7, а для 2-х последовательно соединенных элементов $\sqrt{not}$ — на рис. 5.8 в соответствии с известной работой [7]. На рис. 5.7, 5.8 символами **0** и **1** обозначены возможные состояния, поступающие на вход и выход элемента $\sqrt{not}$. Отметим, что возможны и другие обозначения, например, $|0\rangle$ и $|1\rangle$ соответственно.

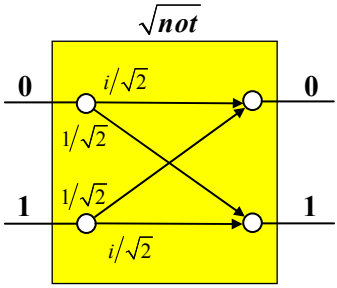


Рис. **5.7**

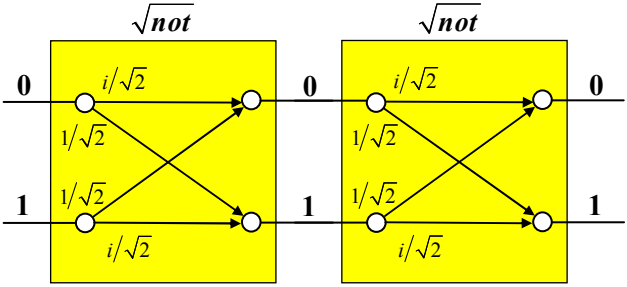


Рис. **5.8**

Схема (рис. 5.8) позволяет наглядно схематично представить возможные переходы из одного состояния в другое для квантовой схемы из двух квантовых элементов $\sqrt{\boldsymbol{not}}$.

В отличие от вероятностей в квантовых элементах именно амплитуды вероятностей могут при *сложении* взаимно компенсироваться (т.е. сокращаться).

Следует еще раз обратить внимание на то, что аналогичная схема (см. в книге 1, рис. 1.61**в**), построенная на классических вероятностных логических элементах НЕ (т.е. на элементах $\boldsymbol{R}$), эквивалентна одному элементу $\boldsymbol{R}$ (см. в книге 1, рис. 1.61**а**).

В случае же квантовых элементов такая же схема обладает уже другим свойством.

Два последовательно соединенных *квантовых* элемента $\sqrt{\boldsymbol{not}}$ уже не приводят к аналогичному эффекту как с элементом $\boldsymbol{R}$, несмотря на то, что для *квантового* элемента $\sqrt{\boldsymbol{not}}$ (как и для классического вероятностного элемента $\boldsymbol{R}$) выполняется следующее соотношение для вероятностей переходов:

$$|\boldsymbol{a}_{\mathbf{00}}|^2 = |\boldsymbol{a}_{\mathbf{01}}|^2 = |\boldsymbol{a}_{\mathbf{10}}|^2 = |\boldsymbol{a}_{\mathbf{11}}|^2 = 1/2.$$

Понять, почему так происходит, помогли именно *амплитуды вероятности* (в общем случае это есть комплексные числа) и диаграммная техника.

Два последовательно соединенных *квантовых* элемента $\sqrt{\boldsymbol{not}}$ преобразовали квантовую схему (рис. 5.8) в детерминированный логический элемент НЕ, так как для этого элемента, как показал расчет, выполненный выше, справедливы следующие соотношения:

$$P_{\mathbf{01}} = P_{\mathbf{10}} = 1, \quad P_{\mathbf{00}} = P_{\mathbf{11}} = 0,$$

что как раз и соответствует детерминированному логическому элементу НЕ. При последовательно соединенных 2-х *квантовых* элементах $\sqrt{\boldsymbol{not}}$ в итоговой квантовой схеме [7] случайность исчезает!!! В классической схеме (т.е. в комбинационной схеме на классических логических элементах) подобный эффект не возможен.

5.3. Квантовые схемы

«…В науке самые глубокие озарения часто приходят тогда, когда разрабатывается метод для исследования новой области Природы.»

М. Нильсен, И. Чанг [1, с.21]

Важнейшим понятием в квантовых вычислениях являются квантовые схемы. Опишем кратко язык квантовых схем. Пусть имеется некоторая простейшая квантовая схема, представленная на рис. 5.9.

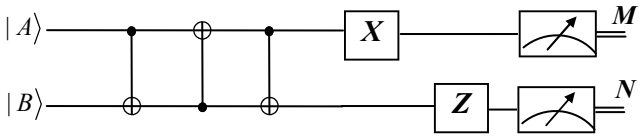


Рис. **5.9**

Схемы классических вычислителей, например комбинационные схемы, состоят из *входа* схемы, *выхода* схемы и логических *элементов*, а также из *проводов* (связей), соединяющих эти элементы между собой и с входом и выходом всей этой схемы.

В теории квантовых вычислений приняты следующие важные соглашения [1, с.45]. Квантовую схему необходимо читать именно слева направо. Горизонтальные линии на квантовой схеме — это «квантовые провода». На практике эти провода не всегда есть реальные физические провода (как, например, в комбинационных схемах), однако они могут соответствовать, например, течению *времени* или физической *частице*, которая перемещается из одной точки пространства в другую точку. В качестве такой частицы может быть фотон. Обычно принято, что исходное состояние всех кубитов (т.е. входное состояние квантовой схемы) — это одно из состояний вычислительного базиса. Часто таким вычислительным базисом является именно $|0\rangle$ и $|1\rangle$. В качестве входного состояния квантовой схемы обычно принимают то состояние, когда все кубиты находятся в $|0\rangle$. Если это соглашение не выдерживается, то желательно сообщать об этом тому, для кого предназначена та или иная квантовая схема. Полагают, что кубиты на квантовых схемах

расположены в начале квантовых проводов (т.е. горизонтальных линий, причем число этих линий совпадает с числом кубитов). На рис. 5.9 кубиты (всего их 2) обозначены как начала квантовых проводов (слева) и находятся соответственно — верхний кубит (**1**-я система) в состоянии $|A\rangle$, а нижний кубит (**2**-я система) в состоянии $|B\rangle$. Самый верхний провод (**1**-й кубит или **1**-я система) соответствует старшему двоичному разряду, а самый нижний (последний, т.е. ***n***-й кубит) — наименьшему двоичному разряду.

Можно обозначать преобразования ***H*** над *квантовой системой из* ***n*** *кубитов* как $\boldsymbol{H}^{\{n\}}$, так и $H^{\otimes n}$. В случае, когда в квантовой схеме используется много кубитов и соответственно квантовых проводов и гейтов, применяют специальное обозначение [1, с.59, 282, 289, 341, 567, 593], как показано на рис. 5.10, 5.11, 5.12.

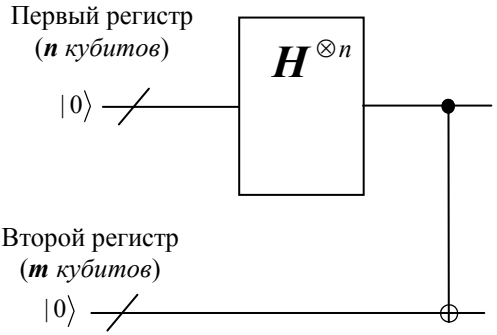


Рис. **5.10**

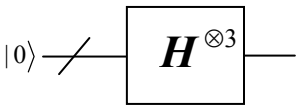


Рис. **5.11**

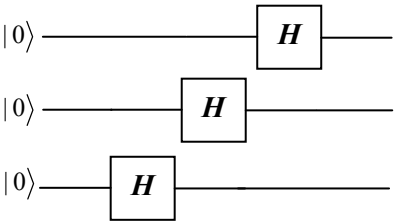


Рис. **5.12**

Квантовая схема на рис. 5.11 представляет то же самое, что квантовая схема на рис. 5.12. Эти две квантовые схемы эквивалентны.

Сами квантовые элементы (как и логические элементы в комбинационных схемах) имеют специальные обозначения, иногда очень похожие на классические логические элементы.

На практике в классических вычислителях могут применяться некоторые схемные решения, которые, как правило, отсутствуют в квантовых вычислителях.

Отметим следующие особенности квантовых схем [1, с.46].

Во-первых, в квантовых схемах (в отличие от классических схем) нет обратных связей.

Во-вторых, в квантовых схемах (в отличие от классических схем) не допускается соединение проводов в один провод, который содержит побитовое ИЛИ входов (т.е. монтажное ИЛИ). Такое соединение проводов соответствует *необратимой* операции, а в квантовых схемах используют именно обратимые операции.

В-третьих, в квантовых схемах (в отличие от классических схем) не допускается операция, результатом которой является несколько копий битов. Согласно квантовой механике сделать копию неизвестного квантового состояния вообще невозможно. Это несколько странно и необычно, поскольку в традиционных классических схемах вычислителя на логических элементах и триггерах копирование данных (например, из одного регистра в другой) это обычное дело и не вызывает каких-либо проблем на практике.

В-четвертых, для квантовых схем полагают [1, с.47, 238-239], что *измерение* можно представлять в них (выполнять или производить) только в конце всех вычислений, т.е. например так, как показано на рис. 5.9, где элементы в виде *измерителей* находятся в самом конце квантовых проводов. За самим измерителем начинается обычный провод, изображенный на рис. 5.9 двойной линией (т.е. провод в классическом смысле для представления (передачи) обычного классического бита $\boldsymbol{M}$ и $\boldsymbol{N}$). Можно полагать, что в схеме на концах квантовых проводов имеются измерители. С этой спе-

цифической особенностью тесно связаны следующие два очень важных принципа [1, с.238-239]:

Принцип отложенного измерения

Измерения всегда можно перенести в конец схемы; если на каком-то этапе работы схемы используются измерения, то в этом месте классические условные операции можно заменить квантовыми ■

Принцип неявного измерения

Без потери общности можно полагать, что все квантовые провода в схеме заканчиваются измерителями ■

Рассмотрим теперь подробнее квантовую схему на рис. 5.9. На этой схеме операции выполняются над 2-мя кубитами, один из которых (верхний или 1-й кубит) находится в состоянии $|A\rangle$, а нижний (или 2-й) кубит — в состоянии $|B\rangle$.

Входом схемы являются отдельные состояния кубитов $|A\rangle$, $|B\rangle$, (а также и состояние системы из 2-х кубитов).

Квантовая схема (см. рис. 5.9) заканчивается двумя *измерителями*, которые измеряют конечное состояние каждого из кубитов. В результате этих измерений становятся известными классические биты ***M*** и ***N*** с вероятностью в соответствии с амплитудами вероятностей этих конечных состояний кубитов.

Выходом схемы (см. рис. 5.9) являются новые состояния кубитов и новое состояние системы из 2-х кубитов. Измерение состояния этих кубитов дает с некоторой вероятностью два классических бита ***M*** и ***N***.

На схеме (см. рис. 5.9) последовательно один за одним изображены 5 квантовых элементов (гейтов), из которых 3 элемента — это гейты CNOT (2 включены одинаково, а 1 — наоборот), один — это гейт NOT, обозначенный как ***X*** и последний — это гейт элемент Паули ***Z***, обозначенный как ***Z***.

На схеме (см. рис. 5.9) элементы CNOT являются двухкубитовами (двухвходовыми) гейтами, а элементы ***X*** и ***Z*** — однокубитовыми (одновходовыми) гейтами.

Остановимся несколько подробнее на *состояниях* в квантовых схемах. При рассмотрении квантовых схем надо отчетливо себе представлять, что:

- каждый кубит имеет свое какое-то состояние;
- набор из нескольких (не из всех) кубитов имеет свое состояние;
- квантовый регистр (т.е. набор из всех кубитов) имеет также свое состояние.

Таким образом, с одной стороны, каждый кубит по отдельности характеризуется своим состоянием, и, с другой стороны, уже набор кубитов (как квантовая составная система) также характеризуется, но своим состоянием.

На вход квантовой схемы поступает как состояние каждого кубита по отдельности, так и состояние составной квантовой системы из этих кубитов, т.е. состояние всего квантового регистра в целом.

В результате применения гейтов к кубитам, их состояния (т.е. состояния кубитов) изменяются (или не изменяются), но во всяком случае становятся новыми, но не обязательно измененными.

В итоге и сам квантовый регистр (как составная квантовая система) приобретает новое, но не обязательно измененное состояние.

На выход квантовой схемы поступает как новое состояние каждого кубита по отдельности, так и новое состояние составной квантовой системы из этих кубитов, т.е. состояние всего квантового регистра в целом.

Выход квантовой схемы (т.е. состояние кубитов и всего квантового регистра) может быть измерен и тем самым получен ответ для той задачи, которую и решала эта квантовая схема.

Кубиты и квантовый регистр (согласно квантовой механике) могут быть как в **чистом** состоянии, так и в **смешанном** состоянии. Суперпозиция состояний кубита или суперпозиция состояний квантового регистра является чистым состоянием. В чистых состояниях выделяют базисные состояния, например для кубита — $|0\rangle$ и $|1\rangle$, а для квантового регистра из 2-х кубитов — $|00\rangle, |01\rangle, |10\rangle, |11\rangle$. Возможен случай, когда квантовый регистр находится в чистом состоянии, а отдельные кубиты (например, не все кубиты) — в смешанном состоянии. Отметим, что смешанное состояние описывается *матрицей плотности*. Среди чистых состояний составных систем выделяют **перепутанные** состояния ее

подсистем — очень важных для квантовых вычислений.

Для квантовых схем из содержания главы 2 следует, что при выбранном базисе для любого вектора состояния кубита $|\psi\rangle$ комплексные коэффициенты (т.е. амплитуды) a и b в суперпозиции $|\psi\rangle = a|0\rangle + b|1\rangle$ определяются однозначно.

На основании принципа суперпозиции произвольное состояние $|\varphi\rangle$ рассматриваемого ***n***-кубитового регистра имеет вид ($N=2^n-1$):

$$|\varphi\rangle = a_0|0...00\rangle + a_1|0...01\rangle + ... + a_N|1...11\rangle .$$

Для каждого из базисных состояний $|C_N C_{N-1}...C_0\rangle$, где C_m=0, 1 в этой суперпозиции состояние отдельного кубита описывается некоторым кэт-вектором и не зависит от состояний остальных кубитов. В общем случае вектор $|\varphi\rangle$ не может быть записан как произведение однокубитовых состояний, т.е. он не имеет факторизованного вида. Это означает, что квантовое состояние отдельного кубита не описывается каким-либо кэт-вектором. Такое состояние квантовой подсистемы (например, отдельного кубита) называется *смешанным* состоянием. Что касается всей системы (т.е. квантового регистра в целом), то говорят, что ее состояние является *перепутанным* состояниями отдельных кубитов.

> При рассмотрении квантовых схем будем полагать, что кубиты могут быть как в *чистом* состоянии, так и в *смешанном* (точнее в *перепутанном*) состоянии, а квантовый регистр (из этих кубитов) только в чистом состоянии.

Есть перепутанное состояния, которые нельзя превратить в факторизованное состояние с помощью одних только однокубитовых унитарных операций (это справедливо, например, для всех состояний Белла). Состояния Белла можно получить друг из друга с помощью однокубитовых гейтов. Только однокубитовыми гейтами нельзя «распутать» перепутанные состояния Белла. Если на факторизованное состояние подействовать однокубитовыми гейтами, то оно останется факторизованным. Состояния Белла остаются перепутанными в любом вычислительном базисе, однако есть много других состояний, перепутанных в одном базисе, но факторизующихся при переходе к другому базису.

Отметим, что под действием гейта CNOT факторизованное состояние $|a\rangle\otimes|b\rangle$ переходит в перепутанное двухкубитовое состояние.

С помощью гейта CNOT можно совершить и обратную операцию, т.е. факторизовать перепутанное состояние.

Точно так же, как и в классических вычислительных схемах необходимо было выбрать вычислительный базис (см. книгу 1), так и в квантовых схемах для выполнения вычислений необходимо выбрать некоторый вычислительный базис.

Сам выбор вычислительного базиса в некотором смысле произволен и не однозначен.

В квантовых вычислениях выбор вычислительного базиса связан с тем, что считать, например, двоичным нулем и двоичной единицей.

Так в качестве двоичного нуля может быть выбрано состояние квантового объекта, описываемое вектором

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix},$$

а в качестве двоичной единицы — состояние, описываемое вектором

$$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Вычислительным базисом могут быть также следующие состояния:

$$|\mathbf{0}\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix}, \quad |\mathbf{1}\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix}.$$

Вообще говоря, при решении некоторых задач (см. ***Пример 5.6***, ***5.7***, ***5.8*** и др.) не требуется вводить и тем более знать вычислительный базис.

Однако для того чтобы подчеркнуть значимость вычислительного базиса в квантовых вычислениях, в этих задачах он все-таки будет упоминаться, хотя и с оговорками.

По аналогии с комбинационными схемами будем также рассматривать следующие три типовые задачи, связанных уже с квантовыми схемами:

1) задача прямого анализа квантовой схемы;
2) задача обратного анализа квантовой схемы;
3) задача синтеза квантовой схемы.

Введем следующие три определения, непосредственно связанных с представленными выше типовыми задачами.

Определение 5.8
Задача прямого анализа квантовой схемы — по известному входному вектору $|\psi\rangle$ и заданной матрице $\boldsymbol{U}$, описывающей преобразование над $|\psi\rangle$, требуется найти выходной вектор $|\psi'\rangle$.

Определение 5.9
Задача обратного анализа квантовой схемы — по известному выходному вектору $|\psi'\rangle$ и заданной матрице $\boldsymbol{U}$, описывающей выполненное преобразование над входным вектором, требуется найти (восстановить) входной вектор $|\psi\rangle$.

Определение 5.10
Задача синтеза квантовой схемы — по известному входному вектору $|\psi\rangle$ и выходному вектору $|\psi'\rangle$ требуется найти (синтезировать) матрицу $\boldsymbol{U}$, описывающую необходимое преобразование над входным вектором $|\psi\rangle$, чтобы получить $|\psi'\rangle$.

Квантовые схемы, которые будем далее рассматривать, обязательно содержат набор *кубитов*, набор *гейтов*, набор квантовых *проводов* и могут содержать *измерители*, реальные физические провода (для классических битов), как в комбинационных схемах, и классические логические элементы.

5.4. Однокубитовые схемы

> «…в новаторской статье Шумахера … появился широко используемый теперь термин *кубит*, который возник в дискуссии Шумахера с Вуттерсом .»
>
> *М. Нильсен, И. Чанг* [1, с.735]

Однокубитовые схемы, которые будем далее рассматривать, содержат следующие компоненты:

- один кубит;
- набор одокубитовых гейтов;
- квантовый провод;
- измеритель (иногда на квантовых схемах не показывают).

Кубит, сфера Блоха и фаза

Для квантовой схемотехники важно научиться рассматривать сами кубиты как [1, с.33] «абстрактные математические объекты».

Определение 5.11

Кубит [1, с.224] — это вектор $|\psi\rangle = a|0\rangle + b|1\rangle$, параметризованный двумя комплексными числами, удовлетворяющими условию $|a|^2+|b|^2=1$.

В общем случае состояние кубита как квантового объекта — это [1, с.34] единичный вектор в двумерном комплексном векторном пространстве. Среди всех возможных состояний выделены два состояния $|0\rangle$ и $|1\rangle$, которые являются [1, с.34] **специальными** состояниями. Эти состояния $|0\rangle$ и $|1\rangle$ в теории квантовых вычислений называют [1, с.34] *состояниями вычислительного базиса*. Важно подчеркнуть, что эти два состояния образуют полный ортонормированный базис этого векторного пространства.

Состояние кубита в квантовых схемах является как входом для гейтов, так и их выходом, т.е. вектор исходного состояния кубита является входным вектором для однокубитового гейта, а вектор преобразованного состояния кубита является выходным вектором для этого гейта.

Само состояние кубита $|\psi\rangle = a|0\rangle + b|1\rangle$ можно записать в виде вектор-столбца (см. [1, с.93]):

$$|\psi\rangle \equiv \begin{bmatrix} a \\ b \end{bmatrix},$$

т.е.

$$a|0\rangle + b|1\rangle \equiv \begin{bmatrix} a \\ b \end{bmatrix}.$$

Базисные состояния $|0\rangle$ и $|1\rangle$ есть частный случай выражения $|\psi\rangle = a|0\rangle + b|1\rangle$. Действительно,

$$\text{если } b = 0, \quad a = 1, \quad \text{то } |\psi\rangle = |0\rangle;$$

$$\text{если } b = 1, \quad a = 0, \quad \text{то } |\psi\rangle = |1\rangle.$$

Кубит, который находится в состоянии $|\psi\rangle = a|0\rangle + b|1\rangle$, очень удобно представлять (рис. 5.13) как [1, с.33-37, 225] некоторую точку с координатами **(θ, φ)** на единичной сфере (сфере Блоха).

Причем амплитуды вероятностей a и b представляются для человека не знакомого с квантовой механикой очень *странным* образом, а именно следующим соотношением [1, с.35, 225]:

$$|\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right),$$

где **θ**, **φ**, **γ** — действительные числа, причем общий фазовый множитель $e^{i\gamma}$ можно **игнорировать**, так как [1, с.35] он «*не приводит к наблюдаемым эффектам*», т.е. можно полагать, что [1, с.225]:

$$a = \cos\frac{\theta}{2}; \qquad b = e^{i\varphi}\sin\frac{\theta}{2}.$$

Странность (но только на первый взгляд) этих формул для указанных амплитуд вероятностей состоит в том, что угол **θ** делится на 2, что никак не следует из школьного курса геометрии. Можно показать, что наличие множителя $\frac{1}{2}$ связано именно с тем, что *спин* есть $\frac{1}{2}$, т.е. с так называемым спинорным представлением группы вращений.

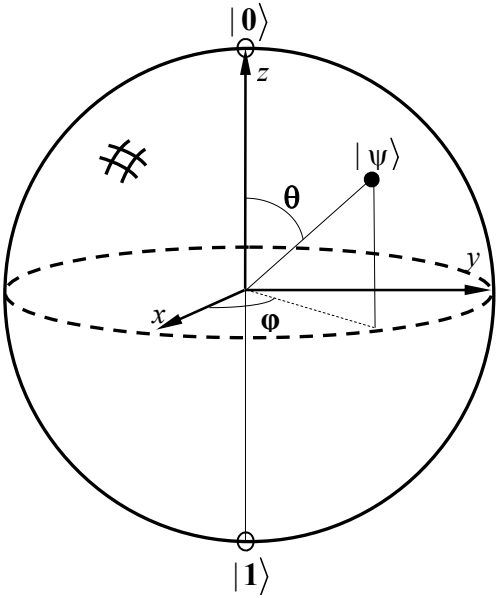


Рис. **5.13.** [1, с.36]

Два числа **θ** и **φ** на единичной сфере (см. рис. 5.13) в трехмерном пространстве определяют конкретную точку (состояние $|\psi\rangle$ кубита). На рис. 5.13 показаны следующие точки:

точка (в самом верху сферы), соответствующая состоянию, обозначенному как $|0\rangle$;

точка (в самом низу сферы), соответствующая состоянию, обозначенному как $|1\rangle$;

промежуточная точка с координатами (**θ**, **φ**), соответствующая некоторому состоянию кубита $|\psi\rangle = a|0\rangle + b|1\rangle$, где

$$a = \cos\frac{\theta}{2};$$

$$b = e^{i\varphi}\sin\frac{\theta}{2}.$$

Применение некоторого гейта к одиночному кубиту, находящемуся в состоянии $|\psi\rangle$ (с координатами (**θ**, **φ**) на сфере Блоха), может изменить его состояние с $|\psi\rangle$ на $|\psi'\rangle$ (и тем самым изменить его координаты с (**θ**, **φ**) на какие-то другие координаты). Действие гейта соответствует некоторому унитарному преобразованию, а в итоге некоторым вращениям на сфере Блоха.

Специалисты по квантовым вычислениям нас предупреждают [1, с.36]: «…Многие операции над одиночными кубитами, рассматриваемые далее в этой главе, изящно описываются с использованием сферы Блоха. Однако нужно иметь в виду, что возможности этого представления ограничены, так как не известно простого обобщения сферы Блоха на случай нескольких кубитов». По этой причине на этом и закончим рассмотрение сферы Блоха.

Измерение состояния кубита, находящегося в суперпозиции $|\psi\rangle = a|0\rangle + b|1\rangle$, изменяет состояние кубита.

В частности кубит может находиться в состоянии $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$, которое (см. [1, с.34]) иногда обозначают как $|+\rangle$. В результате измерения, как говорят специалисты [1, с.36], «… он коллапсирует из суперпозиции $|0\rangle$ и $|1\rangle$ в определенное состояние, соответствующее результату измерения. Например, если измерение $|+\rangle$ дает 0, то после измерения кубит останется в состоянии $|0\rangle$. Почему происходит этот коллапс — никто не знает».

Для понимания работы с кубитами в квантовых схемах важно знать следующее.

Если кубит находится в состоянии $|0\rangle$, то измерение этого состояния с вероятностью 1 покажет, что кубит находится в этом состоянии.

Аналогично, если кубит находится в состоянии $|1\rangle$, то измерение этого состояния также с вероятностью 1 покажет, что кубит находится в этом состоянии.

Это мало чем отличается от классического случая при измерении состояния логических элементов комбинационной схемы.

Однако, если кубит (как квантовый объект) уже находится в состоянии **суперпозиции**, например в состоянии $|\psi\rangle = a|0\rangle + b|1\rangle$, то измерение (в вычислительном базисе $|0\rangle$, $|1\rangle$) этого состояния с вероятностью

$|a|^2$ покажет результат ***m***=0, а кубит окажется в состоянии $|0\rangle$,

$|b|^2$ покажет результат ***m***=1, а кубит окажется в состоянии $|1\rangle$,

причем $|a|^2+|b|^2=1$.

Другими словами, можно полагать, что в результате измерения суперпозиционного состояния кубита с вероятностью $|a|^2$ у него наблюдается состояние $|0\rangle$, а с вероятностью $|b|^2$ — состояние $|1\rangle$.

В квантовых вычислениях не последнюю роль играет такая операция как измерение. Для измерения веден специальный графический символ в виде измерительного прибора, как на рис. 5.14.

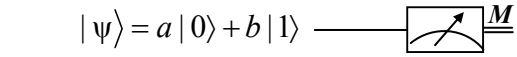


Рис. **5.14**

Можно полагать, что эта операция (на квантовой схеме ее обозначают специальным элементом — *измерителем*) преобразует состояние кубита $|\psi\rangle = a|0\rangle + b|1\rangle$, как говорят специалисты [1, с.46-47], «… в вероятностный классический бит M (изображаемый двойной линией, чтобы отличить его от кубита)… ». Этот *вероятностный классический бит* M имеет значение

0 с вероятностью $|a|^2$;

1 с вероятностью $|b|^2$.

На практике очень удобно представлять квантовые элементы (гейты) в *матричном* виде. Для этого (в качестве простого наглядного примера) определим некоторую матрицу X для представления гейта NOT (квантового элемента), являющегося аналогом классического логического элемента НЕ в комбинационных схемах, следующим образом [1, с.39]:

$$X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

где $X \equiv \sigma_1$, а σ_1 — матрица Паули.

На рис. 5.15 показано одно из возможных графических представлений квантового элемента NOT (гейта ***X***, обозначаемого исторически как *X* [1, с.40]).

Рис. **5.15**

Выходом квантовой схемы (см. рис. 5.15), состоящей только из одного гейта *X*, есть состояние $|\psi'\rangle$ того же кубита, чье состояние являлось входом этого гейта. На выходе гейта *X* будет состояние $|\psi'\rangle$, описываемое (см. [1, с.40]) следующим выражением:

$$|\psi'\rangle = X\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} b \\ a \end{bmatrix}.$$

По определению единичная матрица, соответствующая тождественному преобразованию над одним кубитом, есть

$$I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

На выходе гейта ***I*** будет состояние $|\psi'\rangle$, описываемое следующим выражением:

$$|\psi'\rangle = I\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix}.$$

Относительно унитарных матриц можно сделать два важных утверждения.

Утверждение 5.4
Существует бесконечно много унитарных матриц размера 2 × 2, а следовательно, бесконечно много однокубитовых элементов [1, с.42]■

Утверждение 5.5
Произвольная унитарная матрица U размера 2 × 2 может быть представлена в виде следующего произведения:

$$U = e^{i\alpha}\begin{bmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{bmatrix}\begin{bmatrix} \cos\left(\frac{\gamma}{2}\right) & -\sin\left(\frac{\gamma}{2}\right) \\ \sin\left(\frac{\gamma}{2}\right) & \cos\left(\frac{\gamma}{2}\right) \end{bmatrix}\begin{bmatrix} e^{-i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{bmatrix},$$

где $\boldsymbol{\alpha}$, $\boldsymbol{\beta}$, $\boldsymbol{\gamma}$, $\boldsymbol{\delta}$, — действительные числа (2-я матрица описывает обычное вращение, а 1-я и 3-я матрицы тоже описывают вращения, но в другой плоскости) [1, с.42]■

Таким образом, *Утверждение 5.4* дает представление о количестве унитарных матриц и однокубитовых гейтов. Оказывается, их очень много. Согласно *Утверждению 5.5* в квантовой схеме однокубитовый гейт может быть эквивалентно представлен как три идущих подряд однокубитовых гейта с унитарными матрицами, связанными с преобразованием вращений.

Фаза
Важно четко себе представлять, что же является *фазой* при выполнении квантовых вычислений. Этот термин достаточно часто используют в квантовой механике.

Различают [1, с.130-131] фазу, связанную с *общим фазовым множителем*, и *относительную фазу*. Введем ряд определений, которые приняты в квантовых вычислениях и соответственно будут далее полезны и для квантовой схемотехники.

Определение 5.12

Будем говорить, что состояние $e^{i\gamma}|\psi\rangle$ совпадает с состоянием $|\psi\rangle$ с точностью **до общего фазового множителя** $e^{i\gamma}$, где γ — действительное число (так как одинакова статистика измерений, которая предсказывается как для $e^{i\gamma}|\psi\rangle$, так и для $|\psi\rangle$) [1, с.130].

Имеется еще другой вид фазы, которую принято называть *относительной фазой*.

Для того чтобы понять относительную фазу, рассмотрим следующие два состояния

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, \qquad |\psi_2\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle.$$

Сравнивая для двух этих состояний $|\psi_1\rangle$ и $|\psi_2\rangle$ амплитуды у $|1\rangle$, можно заметить, что они отличаются только знаком (у одного знак *плюс*, а у другого знак *минус*). Абсолютная величина одна и та же, но знак разный. Эти состояния $|\psi_1\rangle$ и $|\psi_2\rangle$ совпадают с точностью до **сдвига фазы**, так как амплитуды при $|0\rangle$ одинаковы (при них *относительный фазовый множитель* есть **+1**), а амплитуды при $|1\rangle$ не одинаковы (эти амплитуды различаются *фазовым множителем,* который есть **–1**).

Важно понимать, что разница между *относительными фазами* и *общими фазовыми множителями* состоит в том, что в отличие от *общих фазовых множителей* именно *фазовые множители* бывают различными у разных амплитуд. От выбора базиса зависят относительные фазы, а не общие фазы.

Определение 5.13

Принято говорить, что две *амплитуды a* и *b* **различаются относительными фазами**, если существует такое действительное число γ, что $a = e^{i\gamma}b$ [1, с.130].

Определение 5.14

Принято говорить, что два *состояния* $|\psi_1\rangle$ и $|\psi_2\rangle$ **различаются относительными фазами** в некотором базисе, если все их амплитуды в этом базисе получаются одна из другой умножением на *фазовые множители* вида $e^{i\gamma}$, где γ — действительное число [1, с.130].

В табл. 5.1 приведены условные обозначения наиболее распространенных квантовых элементов (однокубитовых гейтов).

Амплитуды вероятностей a и b в общем случае есть комплексные числа вида

$$w + id,$$

где

$$i = \sqrt{-1} = \exp\left(i\pi/2\right),$$

$$\sqrt{i} = \exp\left(i\pi/4\right).$$

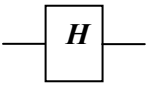
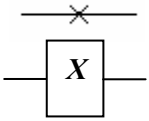
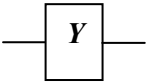
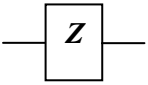
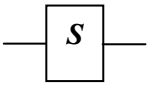
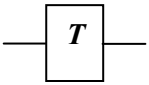
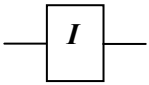
Вообще надо отметить, что однокубитовых гейтов может быть очень много, причем столько, сколько существует унитарных матриц размером 2×2.

Каждая унитарная матрица соответствует некоторому физическому процессу, отражающему преобразование вектора состояния кубита. Сама реализация на практике однокубитового гейта с заданной унитарной матрицей, вообще говоря, не такая простая задача (см. главу 2, главу 4).

Далее будет рассмотрен достаточно ограниченный набор однокубитовых гейтов, но который позволит получить основное представление об однокубитовых квантовых схемах.

Было выяснено, что для практического выполнения заданных квантовых вычислений достаточно уметь реализовывать только ограниченный (небольшой) набор однокубитовых квантовых элементов (гейтов), который можно назвать *универсальным*. Таким *универсальным* набором является набор из элемента *Адамара* H, сдвига фазы S [1, с.225], элемента $\pi/8$ — T. Эта *универсальность* понимается в том смысле, что с помощью этого набора можно [1, с.241] любой однокубитовый гейт (оператор) аппроксимировать с любой точностью.

Таблица 5.1. Однокубитовые гейты (см. [1, с.15-16,225; 10])

Наименование гейта	**Возможное условное обозначение**	**Выход гейта при входе** $a\,\|0\rangle + b\,\|1\rangle$	**Унитарная матрица гейта**
Элемент *Адамара*		$\frac{a+b}{\sqrt{2}}\|0\rangle + \frac{a-b}{\sqrt{2}}\|1\rangle$	$\boldsymbol{H}=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$
Элемент *Паули* $\boldsymbol{X}$		$b\,\|0\rangle + a\,\|1\rangle$	$\sigma_1=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$
Элемент *Паули* $\boldsymbol{Y}$		$-i\{b\,\|0\rangle - a\,\|1\rangle\}$	$\sigma_2=\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}$
Элемент *Паули* $\boldsymbol{Z}$		$a\,\|0\rangle - b\,\|1\rangle$	$\sigma_3=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$
Фазовый элемент		$a\,\|0\rangle + ib\,\|1\rangle$	$\boldsymbol{S}=\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}$
Элемент $\boldsymbol{\pi}/8$		$a\,\|0\rangle + e^{i\pi/4}\,b\,\|1\rangle$	$\boldsymbol{T}=\begin{bmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{bmatrix}$
Элемент *Тождественного преобразования*		$a\,\|0\rangle + b\,\|1\rangle$	$\boldsymbol{I}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$

ОТМЕТИМ (см. [1, с.225]). Можно заметить, что у гейта ***T*** несколько странное название — $\pi/8$. Это связано с общей фазой элемента и с матрицей, на диагонали которой стоят элементы именно $\exp(\pm i\,\pi/8)$ следующим образом:

$$\boldsymbol{T} = \exp(i\,\pi/8)\begin{bmatrix} \exp(-i\,\pi/8) & 0 \\ 0 & \exp(i\,\pi/8) \end{bmatrix}.$$

ВАЖНО [1, с.15, 40]. Строки и столбцы (см. табл. 5.1) унитарных матриц (унитарных преобразований) нумеруются слева направо и сверху вниз как 00…0, 00…1, …, 11…1; самый нижний провод соответствует самому младшему биту. Для любой унитарной матрицы U должно выполняться условие $U^{\dagger}U = I$, где $U^{\dagger}$ — эрмитово сопряженная матрица (т.е. по отношению к U она транспонирована и комплексно сопряженная), I — это единичная матрица. Для практики очень важен тот факт, что любая унитарная матрица описывает некоторый физически возможный квантовый элемент (гейт).

Рассмотрим следующие простые, но важные примеры.

Пример 5.4. Вычисление выхода одокубитового гейта.

На вход одокубитового гейта (см. табл. 5.1) поступает состояние кубита в виде суперпозиции $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$, причем выполнимо *условие нормировки* $|a|^2 + |b|^2 = 1$.

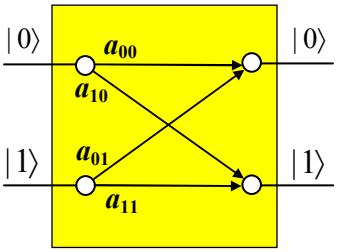
Требуется построить диаграмму переходов и найти выход $|\psi'\rangle$ каждого гейта из табл. 5.1, если на его вход поступило это состояние $|\psi\rangle$.

Решение

1). На рис. 5.16 приведен одокубитовый гейт (рис. 5.16**в**), его диаграмма переходов (рис. 5.16**а**) и унитарная матрица ***U*** для общего случая (рис. 5.16**б**). На вход этого гейта поступает вектор $|\psi\rangle$, а на его выход — вектор $|\psi'\rangle$. Каждый гейт из табл. 5.1 может быть представлен подобным образом. Так, аналогичное представление для гейта ***H*** показано на рис. 5.17.

Одокубитовый гейт ***U*** и его диаграмма переходов

а)



б)

$$U = \begin{bmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{bmatrix}$$

в)

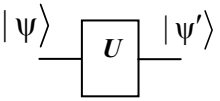
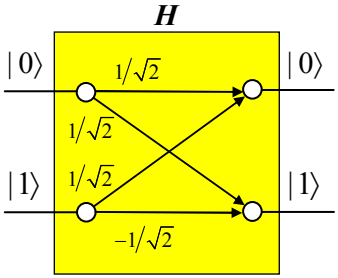


Рис. **5.16**

Одокубитовый гейт ***H*** и его диаграмма переходов

а)



б)

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

в)

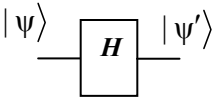


Рис. **5.17**

2). Зная входной вектор $|\psi\rangle$ и унитарную матрицу, применим *Правило* 5.0**а** и получим выходные векторы $|\psi'\rangle$ для каждого гейта из табл. 5.1.

Для гейта элемент *Адамара* ***H***

$$H\times|\psi\rangle=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\times\begin{bmatrix}a\\ b\end{bmatrix}=\frac{1}{\sqrt{2}}\begin{bmatrix}1\cdot a+ & 1\cdot b\\ 1\cdot a+(-1)\cdot b\end{bmatrix}=\begin{bmatrix}\dfrac{a+b}{\sqrt{2}}\\ \dfrac{a-b}{\sqrt{2}}\end{bmatrix}=|\psi'\rangle,$$

т.е. $|\psi'\rangle=|0\rangle\dfrac{a+b}{\sqrt{2}}+|1\rangle\dfrac{a-b}{\sqrt{2}}$.

ОТМЕТИМ. Символ $\times$ — это обычное умножение матриц или чисел, а символ $\otimes$ — это тензорное умножение.

Проверим условие нормировки для выходного вектора $|\psi'\rangle$

$$\left(\left|\frac{a+b}{\sqrt{2}}\right|\right)^2+\left(\left|\frac{a-b}{\sqrt{2}}\right|\right)^2=\frac{2\left(|a|^2+|b|^2\right)}{2}=\frac{2\cdot1}{2}=1,$$

т.е. условие нормировки выполняется (так как $|a|^2+|b|^2=1$).

Для гейта элемент *Паули* ***X***

$$X\times|\psi\rangle=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\times\begin{bmatrix}a\\ b\end{bmatrix}=\begin{bmatrix}0\cdot a+1\cdot b\\ 1\cdot a+0\cdot b\end{bmatrix}=\begin{bmatrix}b\\ a\end{bmatrix}=|\psi'\rangle,$$

т.е. $|\psi'\rangle=b\,|0\rangle+a\,|1\rangle$.

Проверим условие нормировки для выходного вектора $|\psi'\rangle$

$$|b|^2+|a|^2=|a|^2+|b|^2=1,$$

т.е. условие нормировки выполняется (так как $|a|^2+|b|^2=1$).

Для гейта элемент *Паули* ***Y***

$$Y\times|\psi\rangle=\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}\times\begin{bmatrix}a\\ b\end{bmatrix}=\begin{bmatrix}0\cdot a+(-i)\cdot b\\ i\cdot a+0\cdot b\end{bmatrix}=\begin{bmatrix}-ib\\ ia\end{bmatrix}=-i\begin{bmatrix}b\\ -a\end{bmatrix}=|\psi'\rangle,$$

т.е. $|\psi'\rangle=-i\{b\,|0\rangle-a\,|1\rangle\}$.

Проверим условие нормировки для выходного вектора $|\psi'\rangle$

$$\left(\left|-ib\right|\right)^2+\left(\left|ia\right|\right)^2=\left|a\right|^2+\left|b\right|^2=1,$$

т.е. условие нормировки выполняется (так как $\boldsymbol{i}^2=-1$ и $|a|^2+|b|^2=1$).

Для гейта элемент *Паули* ***Z***

$$Z\times|\psi\rangle=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\times\begin{bmatrix}a\\ b\end{bmatrix}=\begin{bmatrix}1\cdot a+0\cdot b\\ 0\cdot a+(-1)\cdot b\end{bmatrix}=\begin{bmatrix}a\\ -b\end{bmatrix}=|\psi'\rangle,$$

т.е. $|\psi'\rangle=a\,|0\rangle-b\,|1\rangle$.

Проверим условие нормировки для выходного вектора $|\psi'\rangle$

$$\left(\left|a\right|\right)^2+\left(\left|-b\right|\right)^2=\left|a\right|^2+\left|b\right|^2=1,$$

т.е. условие нормировки выполняется (так как $|a|^2+|b|^2=1$).

Для гейта фазовый элемент ***S***

$$S\times|\psi\rangle=\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}\times\begin{bmatrix}a\\ b\end{bmatrix}=\begin{bmatrix}1\cdot a+0\cdot b\\ 0\cdot a+i\cdot b\end{bmatrix}=\begin{bmatrix}a\\ ib\end{bmatrix}=|\psi'\rangle,$$

т.е. $|\psi'\rangle=a\,|0\rangle+ib\,|1\rangle$.

Проверим условие нормировки для выходного вектора $|\psi'\rangle$

$$\left(\left|a\right|\right)^2+\left(\left|ib\right|\right)^2=\left|a\right|^2+\left|b\right|^2=1,$$

т.е. условие нормировки выполняется (так как $\boldsymbol{i}^2=-1$ и $|a|^2+|b|^2=1$).

Для гейта элемент $\boldsymbol{\pi}/8$ — ***T***

$$T\times|\psi\rangle=\begin{bmatrix}1 & 0\\ 0 & \sqrt{i}\end{bmatrix}\times\begin{bmatrix}a\\ b\end{bmatrix}=\begin{bmatrix}1\cdot a+0\cdot b\\ 0\cdot a+\sqrt{i}\cdot b\end{bmatrix}=\begin{bmatrix}a\\ b\sqrt{i}\end{bmatrix}=|\psi'\rangle,$$

т.е. $|\psi'\rangle=a\,|0\rangle+b\sqrt{i}\,|1\rangle$.

Проверим условие нормировки для выходного вектора $|\psi'\rangle$

$$\left(\left|a\right|\right)^2+\left(\left|b\sqrt{i}\right|\right)^2=\left|a\right|^2+\left|b\right|^2=1,$$

т.е. условие нормировки выполняется (так как $|a|^2+|b|^2=1$).

Для гейта элемент *Тождественного преобразования* ***I***

$$I \times |\psi\rangle = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \times \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 1 \cdot a + 0 \cdot b \\ 0 \cdot a + 1 \cdot b \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix} = |\psi'\rangle,$$

т.е. $|\psi'\rangle = a|0\rangle + b|1\rangle$ или $|\psi'\rangle = |\psi\rangle$.

Проверим условие нормировки для выходного вектора $|\psi'\rangle$

$$|a|^2 + |b|^2 = 1,$$

т.е. условие нормировки выполняется (так как $|a|^2+|b|^2=1$).

Для одокубитового гейта ***U*** (общий случай)

$$U \times |\psi\rangle = \begin{bmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{bmatrix} \times \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} a_{00} \cdot a + a_{01} \cdot b \\ a_{10} \cdot a + a_{11} \cdot b \end{bmatrix} = |\psi'\rangle,$$

т.е. $|\psi'\rangle = \{a_{00} \cdot a + a_{01} \cdot b\}|0\rangle + \{a_{10} \cdot a + a_{11} \cdot b\}|1\rangle$.

Проверим условие нормировки для выходного вектора $|\psi'\rangle$

$$|a_{00}a + a_{01}b|^2 + |a_{10}a + a_{11}b|^2 = 1,$$

т.е. условие нормировки выполняется (так как $|a|^2+|b|^2=1$).

На этом закончим рассмотрение данного примера ■

Пример 5.5. Проверка унитарности для одокубитового гейта.

Имеются одокубитовые гейты (см. табл. 5.1) и матрицы, соответствующие преобразованиям, которые они выполняют.

Требуется проверить условие $U^\dagger U = I$ унитарности для матрицы каждого гейта из табл. 5.1. Отметим, что $U^\dagger = \left(U^T\right)^*$.

Решение

1). В соответствии с определением единичной матрицы ***I***, соответствующей размерности матрицы ***U*** для одокубитовых гейтов из табл. 5.1, эта матрица ***I*** (которую иногда обозначают и как **1**) может быть представлена следующим образом:

$$\mathbf{1} \equiv I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

2). Проверим условие $U^{\dagger}U = I$ унитарности для одокубитовых гейтов из табл. 5.1.

Для гейта элемент *Адамара* ***H***

$$H^{\dagger}H = \left(\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\right)^{\dagger} \times \left(\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\right) = \frac{1}{2}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} \times \begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} =$$

$$= \frac{1}{2}\begin{bmatrix}1+1 & 1-1\\ 1-1 & 1-(-1)\end{bmatrix} = \frac{1}{2}\begin{bmatrix}2 & 0\\ 0 & 2\end{bmatrix} = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} \equiv I,$$

т.е. свойство унитарности матрицы ***H*** выполняется.

Для гейта элемент *Паули* ***X***

$$X^{\dagger}X = \left(\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\right)^{\dagger} \times \left(\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\right) = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} \times \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} =$$

$$= \begin{bmatrix}0+1 & 0+0\\ 0+0 & 1+0\end{bmatrix} = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} \equiv I,$$

т.е. свойство унитарности матрицы ***X*** выполняется.

Для гейта элемент *Паули* ***Y***

$$Y^{\dagger}Y = \left(\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}\right)^{\dagger} \times \left(\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}\right) = \begin{bmatrix}0 & -i\\ i & 0\end{bmatrix} \times \begin{bmatrix}0 & -i\\ i & 0\end{bmatrix} =$$

$$= \begin{bmatrix}0-i^2 & 0+0\\ 0+0 & -i^2+0\end{bmatrix} = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} \equiv I,$$

т.е. свойство унитарности матрицы ***Y*** выполняется.

Для гейта элемент *Паули* ***Z***

$$Z^{\dagger}Z = \left(\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\right)^{\dagger} \times \left(\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\right) = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix} \times \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix} =$$

$$= \begin{bmatrix}1+0 & 0+0\\ 0+0 & 0+1\end{bmatrix} = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} \equiv I,$$

т.е. свойство унитарности матрицы ***Z*** выполняется.

Для гейта элемент *Паули* ***S***

$$S^{\dagger}S=\left(\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}\right)^{\dagger}\times\left(\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}\right)=\begin{bmatrix}1 & 0\\ 0 & -i\end{bmatrix}\times\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}=$$

$$=\begin{bmatrix}1+0 & 0+0\\ 0+0 & 0-i^2\end{bmatrix}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\equiv I,$$

т.е. свойство унитарности матрицы ***S*** выполняется.

Для гейта элемент $\boldsymbol{\pi}/8$ — ***T***

Поскольку $\sqrt{i}=\exp\left(i\pi/4\right)=\dfrac{1+i}{\sqrt{2}}$, то можно полагать, что выполнимы следующие соотношение для матрицы ***T***:

$$T=\begin{bmatrix}1 & 0\\ 0 & \dfrac{1}{\sqrt{2}}(1+i)\end{bmatrix},\ T^{T}=\begin{bmatrix}1 & 0\\ 0 & \dfrac{1}{\sqrt{2}}(1+i)\end{bmatrix},\ \left(T^{T}\right)^{*}=\begin{bmatrix}1 & 0\\ 0 & \dfrac{1}{\sqrt{2}}(1-i)\end{bmatrix}.$$

Тогда

$$T^{\dagger}T=\left(\begin{bmatrix}1 & 0\\ 0 & \dfrac{1}{\sqrt{2}}(1+i)\end{bmatrix}\right)^{\dagger}\times\left(\begin{bmatrix}1 & 0\\ 0 & \dfrac{1}{\sqrt{2}}(1+i)\end{bmatrix}\right)=$$

$$=\begin{bmatrix}1 & 0\\ 0 & \dfrac{1}{\sqrt{2}}(1-i)\end{bmatrix}\times\begin{bmatrix}1 & 0\\ 0 & \dfrac{1}{\sqrt{2}}(1+i)\end{bmatrix}=$$

$$=\begin{bmatrix}1+0 & 0+0\\ 0+0 & 0+\dfrac{1}{2}\left(1-i^2\right)\end{bmatrix}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\equiv I,$$

т.е. свойство унитарности матрицы ***T*** выполняется.

Для гейта элемент *Тождественного преобразования* ***I***

$$I^{\dagger}I=\left(\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\right)^{\dagger}\times\left(\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\right)=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\times\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}=$$

$$=\begin{bmatrix}1+0 & 0+0\\ 0+0 & 0+1\end{bmatrix}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\equiv I,$$

т.е. свойство унитарности матрицы ***I*** выполняется.

На этом закончим рассмотрение данного примера ■

Пример 5.6 (задача прямого анализа)

Известен входной вектор $|\psi\rangle=\begin{bmatrix}\frac{3}{5}\\ \frac{4}{5}\end{bmatrix}$ и квантовый одновходовой элемент с матрицей преобразования $\boldsymbol{M}=\frac{1}{5\sqrt{2}}\begin{bmatrix}5 & 5\\ 5 & -5\end{bmatrix}$.

Требуется определить выходной вектор $|\psi'\rangle=\begin{bmatrix}A\\ B\end{bmatrix}$ на выходе квантовой схемы, состоящей из этого одного квантового элемента:

$$\frac{1}{5}\begin{bmatrix}3\\ 4\end{bmatrix}\text{——}\boxed{\boldsymbol{M}=\frac{1}{5\sqrt{2}}\begin{bmatrix}5 & 5\\ 5 & -5\end{bmatrix}}\text{——}|\psi'\rangle.$$

Решение

1). В условиях задачи не указан явно вычислительный базис. Будем далее предполагать, что входной вектор $|\psi\rangle$, выходной вектор $|\psi'\rangle$ и матрица преобразования ***M*** соответствуют одному и тому же вычислительному базису, который для решения этой задачи знать не обязательно.

2). Проверим корректность исходных данных:

Условие нормировки для входного вектора $|\psi\rangle$

$$\left|\frac{3}{5}\right|^2+\left|\frac{4}{5}\right|^2=\frac{9}{25}+\frac{16}{25}=\frac{25}{25}=1$$

выполняется.

$$M^{\dagger}M=\left(\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\right)^{\dagger}\times\left(\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\right)=$$

$$=\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\times\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}=$$

$$=\frac{1}{2}\begin{bmatrix}1+1 & 1-1\\ 1-1 & 1-(-1)\end{bmatrix}=\frac{1}{2}\begin{bmatrix}2 & 0\\ 0 & 2\end{bmatrix}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\equiv I,$$

т.е. свойство унитарности матрицы ***M*** выполняется.

3). Так как входной и выходной векторы связаны соотношением

$$M\times|\psi\rangle=|\psi'\rangle=\begin{bmatrix}A\\ B\end{bmatrix},$$

то, зная ***M*** и $|\psi\rangle$, а также и применяя *Правило* 5.0**а**, вычислим выходной вектор $|\psi'\rangle=\begin{bmatrix}A\\ B\end{bmatrix}$ на выходе квантовой схемы:

$$M\times|\psi\rangle=$$

$$=\frac{1}{5\sqrt{2}}\begin{bmatrix}5 & 5\\ 5 & -5\end{bmatrix}\times\begin{bmatrix}\frac{3}{5}\\ \frac{4}{5}\end{bmatrix}=\frac{1}{5\sqrt{2}}\begin{bmatrix}3+4\\ 3-4\end{bmatrix}=\frac{1}{5\sqrt{2}}\begin{bmatrix}7\\ -1\end{bmatrix}=\begin{bmatrix}\frac{7}{5\sqrt{2}}\\ \frac{-1}{5\sqrt{2}}\end{bmatrix}=\begin{bmatrix}A\\ B\end{bmatrix},$$

т.е. $A=\frac{7}{5\sqrt{2}}$, $B=\frac{-1}{5\sqrt{2}}$ или $|\psi'\rangle=\begin{bmatrix}A\\ B\end{bmatrix}=\begin{bmatrix}\frac{7}{5\sqrt{2}}\\ \frac{-1}{5\sqrt{2}}\end{bmatrix}=\frac{1}{5\sqrt{2}}\begin{bmatrix}7\\ -1\end{bmatrix}$.

4). Проверим условие нормировки для выходного вектора $|\psi'\rangle$

$$\left|\frac{7}{5\sqrt{2}}\right|^2+\left|\frac{-1}{5\sqrt{2}}\right|^2=\frac{49}{50}+\frac{1}{50}=\frac{50}{50}=1,$$

т.е. условие нормировки выполняется.

5). Проверять, что найденный вектор $|\psi'\rangle$ действительно удовлетворяет условиям задачи:

$$M\times|\psi\rangle=|\psi'\rangle,$$

не требуется, так как это прямо следует из самого решения.

6). И тем самым задача решена■

Пример 5.7 (задача обратного анализа)

Известен выходной вектор $|\psi'\rangle=\begin{bmatrix}\frac{7}{5\sqrt{2}}\\ \frac{-1}{5\sqrt{2}}\end{bmatrix}$ и квантовый одновходовой элемент с матрицей преобразования $\boldsymbol{M}=\frac{1}{5\sqrt{2}}\begin{bmatrix}5 & 5\\ 5 & -5\end{bmatrix}$.

Требуется определить входной вектор $|\psi\rangle=\begin{bmatrix}A\\ B\end{bmatrix}$ на выходе квантовой схемы, состоящей из этого одного квантового элемента:

$$|\psi\rangle \longrightarrow \boxed{\boldsymbol{M}=\frac{1}{5\sqrt{2}}\begin{bmatrix}5 & 5\\ 5 & -5\end{bmatrix}} \longrightarrow \frac{1}{5\sqrt{2}}\begin{bmatrix}7\\ -1\end{bmatrix}.$$

Решение

1). В условиях задачи не указан явно вычислительный базис. Будем далее предполагать, что входной вектор $|\psi\rangle$, выходной вектор $|\psi'\rangle$ и матрица преобразования $\boldsymbol{M}$ соответствуют одному и

тому же вычислительному базису, который для решения этой задачи знать не обязательно.

2). Проверим корректность исходных данных.

Условие нормировки для выходного вектора $|\psi'\rangle$

$$\left|\frac{7}{5\sqrt{2}}\right|^2+\left|\frac{-1}{5\sqrt{2}}\right|^2=\frac{49}{50}+\frac{1}{50}=\frac{50}{50}=1$$

выполняется.

$$M^{\dagger}M=\left(\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\right)^{\dagger}\times\left(\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\right)=$$

$$=\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\times\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}=$$

$$=\frac{1}{2}\begin{bmatrix}1+1 & 1-1\\ 1-1 & 1-(-1)\end{bmatrix}=\frac{1}{2}\begin{bmatrix}2 & 0\\ 0 & 2\end{bmatrix}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\equiv I,$$

т.е. свойство унитарности матрицы ***M*** выполняется.

3). Так как входной и выходной векторы связаны соотношением

$$M\times|\psi\rangle=|\psi'\rangle,$$

то, зная ***M*** и $|\psi\rangle$, вычислим входной вектор $|\psi\rangle=\begin{bmatrix}A\\ B\end{bmatrix}$ на входе квантовой схемы:

$$M\times\begin{bmatrix}A\\ B\end{bmatrix}=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\times\begin{bmatrix}A\\ B\end{bmatrix}=\frac{1}{\sqrt{2}}\begin{bmatrix}A+B\\ A-B\end{bmatrix}=\frac{1}{\sqrt{2}}\begin{bmatrix}\frac{7}{5}\\ \frac{-1}{5}\end{bmatrix},$$

т.е.

$$\begin{cases} A+B=\dfrac{7}{5} \\ A-B=\dfrac{-1}{5} \end{cases}$$

или

$$2A=\frac{7}{5}-\frac{1}{5}=\frac{6}{5}\Rightarrow \quad A=\frac{3}{5}\Rightarrow \quad B=\frac{7}{5}-\frac{3}{5}=\frac{4}{5},$$

т.е.

$$|\psi\rangle=\begin{bmatrix}\dfrac{3}{5}\\ \dfrac{4}{5}\end{bmatrix}.$$

4). Проверим условие нормировки для входного вектора $|\psi\rangle$

$$\left|\frac{3}{5}\right|^2+\left|\frac{4}{5}\right|^2=\frac{9}{25}+\frac{16}{25}=\frac{25}{25}=1,$$

т.е. условие нормировки выполняется.

5). Проверим, что найденный вектор $|\psi\rangle$ действительно удовлетворяет условиям задачи:

$$M\times|\psi\rangle=|\psi'\rangle$$

или

$$M\times\begin{bmatrix}\dfrac{3}{5}\\ \dfrac{4}{5}\end{bmatrix}=\frac{1}{5\sqrt{2}}\begin{bmatrix}5 & 5\\ 5 & -5\end{bmatrix}\times\begin{bmatrix}\dfrac{3}{5}\\ \dfrac{4}{5}\end{bmatrix}=$$

$$= \frac{1}{5\sqrt{2}} \begin{bmatrix} 3+4 \\ 3-4 \end{bmatrix} = \frac{1}{5\sqrt{2}} \begin{bmatrix} 7 \\ -1 \end{bmatrix} = \begin{bmatrix} \frac{7}{5\sqrt{2}} \\ \frac{-1}{5\sqrt{2}} \end{bmatrix} = |\psi'\rangle,$$

т.е. найденное решение $|\psi\rangle = \begin{bmatrix} \frac{3}{5} \\ \frac{4}{5} \end{bmatrix}$ удовлетворяет условиям задачи.

6). И тем самым задача решена■

Пример 5.8 (задача синтеза квантовой схемы)

Известен $|\psi\rangle = \begin{bmatrix} \frac{3}{5} \\ \frac{4}{5} \end{bmatrix}$ — входной вектор и $|\psi'\rangle = \begin{bmatrix} \frac{7}{5\sqrt{2}} \\ \frac{-1}{5\sqrt{2}} \end{bmatrix}$ — выходной вектор на выходе квантовой схемы, состоящей из этого одного квантового элемента с матрицей преобразования $\boldsymbol{M} = \begin{bmatrix} w & s \\ z & t \end{bmatrix}$, причем w, s, z, t — это комплексные числа.

Требуется определить w, s, z, t, т.е. синтезировать унитарную матрицу $\boldsymbol{M}$ квантового элемента:

$$\frac{1}{5}\begin{bmatrix} 3 \\ 4 \end{bmatrix} \text{ ——— } \boxed{\boldsymbol{M}} \text{ ——— } \frac{1}{5\sqrt{2}}\begin{bmatrix} 7 \\ -1 \end{bmatrix},$$

т.е. достаточно найти хотя бы одно решение (т.е. одну матрицу $\boldsymbol{M}$).

Решение

1). В условиях задачи не указан явно вычислительный базис. Будем далее предполагать, что входной вектор $|\psi\rangle$, выходной вектор

$|\psi'\rangle$ и матрица преобразования $\boldsymbol{M}$ соответствуют одному и тому же вычислительному базису, который для решения этой задачи знать не обязательно.

2). Проверим корректность исходных данных.

Условие нормировки для входного вектора $|\psi\rangle$

$$\left|\frac{3}{5}\right|^2+\left|\frac{4}{5}\right|^2=\frac{9}{25}+\frac{16}{25}=\frac{25}{25}=1$$

выполняется.

Условие нормировки для выходного вектора $|\psi'\rangle$

$$\left|\frac{7}{5\sqrt{2}}\right|^2+\left|\frac{-1}{5\sqrt{2}}\right|^2=\frac{49}{50}+\frac{1}{50}=\frac{50}{50}=1$$

выполняется.

3). Будем сначала искать решение *w*, *s*, *z*, *t* в области действительных чисел. Если решение будет найдено, то оно и будет искомым.

Из преобразования $M\times|\psi\rangle=|\psi'\rangle$ следует:

$$\begin{cases}3w+4s=\dfrac{7}{\sqrt{2}}\\ 3z+4t=\dfrac{-1}{\sqrt{2}}\end{cases}.$$

Из Свойства 5.1**а** о свойстве унитарности $M^{\dagger}M=I$ следует:

$$\begin{cases}w^2+z^2=1\\ ws+zt=0\\ s^2+t^2=1\end{cases}.$$

Из Свойства 5.1**б** следует:

$$\begin{cases}w^2=t^2\\ s^2=z^2\end{cases}.$$

Таким образом, следует найти хотя бы одно решение следующей

системы уравнений:

$$\begin{cases} 3w+4s=\dfrac{7}{\sqrt{2}} \\ 3z+4t=\dfrac{-1}{\sqrt{2}} \\ \\ w^2+z^2=1 \\ ws+zt=0 \\ s^2+t^2=1 \\ w^2=t^2 \\ s^2=z^2 \end{cases}.$$

Возможны два случая:

случай **I**

$$\begin{cases} w=t \\ s=-z \end{cases},$$

случай **II**

$$\begin{cases} w=-t \\ s=z \end{cases}.$$

Рассмотрим *случай* **I**:

$$\begin{cases} 3w+4s=\dfrac{7}{\sqrt{2}} \\ -3s+4w=\dfrac{-1}{\sqrt{2}} \end{cases} \Rightarrow \begin{cases} 3w+4s=\dfrac{7}{\sqrt{2}} \\ 4w-3s=\dfrac{-1}{\sqrt{2}} \end{cases} \Rightarrow$$

$$\Rightarrow \left[\frac{3}{4}w+\frac{4}{3}w\right]+0=\frac{7}{4\sqrt{2}}-\frac{1}{3\sqrt{2}}=\frac{21-4}{12\sqrt{2}}=\frac{17}{12\sqrt{2}} \Rightarrow$$

$$\Rightarrow \left[\frac{9+16}{12}\right]w=\frac{17}{12\sqrt{2}} \Rightarrow \quad \frac{25}{12}w=\frac{17}{12\sqrt{2}} \Rightarrow \quad w=\frac{17}{25\sqrt{2}},$$

тогда

$$t = w, \quad w = \frac{17}{25\sqrt{2}} \Rightarrow s = \frac{7}{4\sqrt{2}} - \frac{3}{4}\frac{17}{25\sqrt{2}} = \frac{31}{25\sqrt{2}} \Rightarrow$$

$$\Rightarrow z = -s \Rightarrow s = \frac{-31}{25\sqrt{2}},$$

таким образом, искомая матрица $\boldsymbol{M}$ для *случая* **I** есть

$$\boldsymbol{M_1} = \begin{bmatrix} w & s \\ z & t \end{bmatrix} = \frac{1}{25\sqrt{2}} \begin{bmatrix} 17 & 31 \\ -31 & 17 \end{bmatrix}.$$

Рассмотрим *случай* **II**:

$$\begin{cases} 3w + 4s = \dfrac{7}{\sqrt{2}} \\ -4w + 3s = \dfrac{-1}{\sqrt{2}} \end{cases} \Rightarrow \begin{cases} w + \dfrac{4}{3}s = \dfrac{7}{3\sqrt{2}} \\ -w + \dfrac{3}{4}s = \dfrac{-1}{4\sqrt{2}} \end{cases} \Rightarrow$$

$$\Rightarrow 0 + \left[\frac{4}{3}s + \frac{3}{4}s\right] = \frac{7}{3\sqrt{2}} - \frac{1}{4\sqrt{2}} = \frac{28-3}{12\sqrt{2}} = \frac{25}{12\sqrt{2}} \Rightarrow$$

$$\Rightarrow \left[\frac{16+9}{12}\right]s = \frac{25}{12\sqrt{2}} \Rightarrow \quad \frac{25}{12}s = \frac{25}{12\sqrt{2}} \Rightarrow \quad s = \frac{1}{\sqrt{2}},$$

тогда

$$s = z, \quad z = \frac{1}{\sqrt{2}} \Rightarrow \ w = \frac{7}{3\sqrt{2}} - \frac{4}{3}\frac{1}{\sqrt{2}} = \frac{1}{\sqrt{2}} \Rightarrow \ w = -t \Rightarrow t = \frac{-1}{\sqrt{2}},$$

таким образом, искомая матрица $\boldsymbol{M}$ для *случая* **II** есть

$$\boldsymbol{M_2} = \begin{bmatrix} w & s \\ z & t \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

4). Проверим условие, что матрица $\boldsymbol{M_1}$ унитарна:

$$M_1^{\dagger} M_1 = \left(\frac{1}{25\sqrt{2}} \begin{bmatrix} 17 & 31 \\ -31 & 17 \end{bmatrix} \right)^{\dagger} \times \left(\frac{1}{25\sqrt{2}} \begin{bmatrix} 17 & 31 \\ -31 & 17 \end{bmatrix} \right) =$$

$$= \frac{1}{25\sqrt{2}} \frac{1}{25\sqrt{2}} \begin{bmatrix} 17 & -31 \\ 31 & 17 \end{bmatrix} \times \begin{bmatrix} 17 & 31 \\ -31 & 17 \end{bmatrix} =$$

$$= \frac{1}{1250} \begin{bmatrix} 289+961 & 1731-1731 \\ 1731-1731 & 961+289 \end{bmatrix} =$$

$$= \frac{1}{1250} \begin{bmatrix} 1250 & 0 \\ 0 & 1250 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \equiv I,$$

т.е. свойство унитарности матрицы $\boldsymbol{M_1}$ выполняется.

Проверим условие, что матрица $\boldsymbol{M_2}$ унитарна:

$$M_2^{\dagger} M_2 = \left(\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \right)^{\dagger} \times \left(\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \right) = \frac{1}{2} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \times \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} =$$

$$= \frac{1}{2} \begin{bmatrix} 1+1 & 1-1 \\ 1-1 & 1-(-1) \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \equiv I,$$

т.е. свойство унитарности матрицы $\boldsymbol{M_2}$ выполняется.

5). Проверим, что найденная (синтезированная) матрица $\boldsymbol{M_1}$ действительно удовлетворяет условиям задачи:

$$M_1 \times |\psi\rangle = |\psi'\rangle,$$

или

$$\frac{1}{25\sqrt{2}} \begin{bmatrix} 17 & 31 \\ -31 & 17 \end{bmatrix} \times \begin{bmatrix} \frac{3}{5} \\ \frac{4}{5} \end{bmatrix} = \begin{bmatrix} \frac{7}{5\sqrt{2}} \\ \frac{-1}{5\sqrt{2}} \end{bmatrix},$$

или

$$\frac{1}{25\sqrt{2}}\begin{bmatrix}17 & 31\\ -31 & 17\end{bmatrix}\times\begin{bmatrix}3\\ 4\end{bmatrix}\frac{1}{5}=\frac{1}{125\sqrt{2}}\begin{bmatrix}51+124\\ -93+68\end{bmatrix}=\frac{1}{125\sqrt{2}}\begin{bmatrix}175\\ -25\end{bmatrix}=$$

$$=\frac{25}{125\sqrt{2}}\begin{bmatrix}7\\ -1\end{bmatrix}=\frac{1}{5\sqrt{2}}\begin{bmatrix}7\\ -1\end{bmatrix}=\begin{bmatrix}\frac{7}{5\sqrt{2}}\\ \frac{-1}{5\sqrt{2}}\end{bmatrix}=|\psi'\rangle,$$

т.е. найденное решение $\boldsymbol{M_1}$ удовлетворяет условиям задачи.

Проверим, что найденная (синтезированная) матрица $\boldsymbol{M_2}$ действительно удовлетворяет условиям задачи:

$$M_2\times|\psi\rangle=|\psi'\rangle,$$

или

$$M_2\times\begin{bmatrix}\frac{3}{5}\\ \frac{4}{5}\end{bmatrix}=$$

$$=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\times\begin{bmatrix}\frac{3}{5}\\ \frac{4}{5}\end{bmatrix}=\frac{1}{5\sqrt{2}}\begin{bmatrix}3+4\\ 3-4\end{bmatrix}=\frac{1}{5\sqrt{2}}\begin{bmatrix}7\\ -1\end{bmatrix}=\begin{bmatrix}\frac{7}{5\sqrt{2}}\\ \frac{-1}{5\sqrt{2}}\end{bmatrix}=|\psi'\rangle,$$

т.е. найденное решение $\boldsymbol{M_2}$ удовлетворяет условиям задачи.
Таким образом, найдено два решения

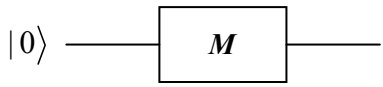
$$\boldsymbol{M_1}=\frac{1}{25\sqrt{2}}\begin{bmatrix}17 & 31\\ -31 & 17\end{bmatrix}\quad\text{и}\quad\boldsymbol{M_2}=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}.$$

6). И тем самым задача решена■

***Пример 5.9*а** (задача прямого анализа)

Известен вычислительный базис, т.е. $|0\rangle=\begin{bmatrix}1\\0\end{bmatrix}$, $|1\rangle=\begin{bmatrix}0\\1\end{bmatrix}$. Известен входной вектор $|\psi\rangle=|0\rangle$ и квантовый одновходовой элемент с матрицей преобразования $\boldsymbol{M}=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}$.

Требуется определить выходной вектор $|\psi'\rangle=\begin{bmatrix}A\\B\end{bmatrix}$ в вычислительном базисе на выходе квантовой схемы, состоящей из этого одного квантового элемента:



Решение

1). В условиях задачи указан явно вычислительный базис. Будем далее предполагать, что входной вектор $|\psi\rangle$, выходной вектор $|\psi'\rangle$ и матрица преобразования $\boldsymbol{M}$ соответствуют одному и тому же вычислительному базису.

2). Проверим корректность исходных данных.

Условие нормировки для входного вектора $|\psi\rangle$ $|1|^2+|0|^2=1+0=1$ выполняется.

$$M^{\dagger}M=\left(\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}\right)^{\dagger}\times\left(\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}\right)=$$

$$=\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}\times\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}=$$

$$=\frac{1}{2}\begin{bmatrix}1+1 & 1-1\\1-1 & 1-(-1)\end{bmatrix}=\frac{1}{2}\begin{bmatrix}2 & 0\\0 & 2\end{bmatrix}=\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}\equiv I,$$

т.е. свойство унитарности матрицы $\boldsymbol{M}$ выполняется.

3). Так как входной и выходной векторы связаны соотношением

$$M \times |\psi\rangle = |\psi'\rangle = \begin{bmatrix} A \\ B \end{bmatrix},$$

то, зная $\boldsymbol{M}$ и $|\psi\rangle$, вычислим выходной вектор $|\psi'\rangle = \begin{bmatrix} A \\ B \end{bmatrix}$ на выходе квантовой схемы:

$$M \times |\psi\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \times \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1+0 \\ 1-0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} A \\ B \end{bmatrix},$$

т.е. $A = \frac{1}{\sqrt{2}}$, $B = \frac{1}{\sqrt{2}}$ или $|\psi'\rangle = \begin{bmatrix} A \\ B \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}$.

4). Проверим условие нормировки для выходного вектора $|\psi'\rangle$

$$\left|\frac{1}{\sqrt{2}}\right|^2 + \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2} + \frac{1}{2} = \frac{2}{2} = 1,$$

т.е. условие нормировки выполняется.

5). Проверять, что найденный вектор $|\psi'\rangle$ действительно удовлетворяет условиям задачи:

$$M \times |\psi\rangle = |\psi'\rangle,$$

не требуется, так как это прямо следует из самого решения.

6). Представим выходной вектор $|\psi'\rangle$ в вычислительном базисе:

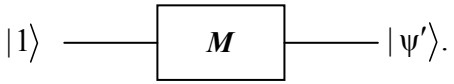
$$|\psi'\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1+0 \\ 0+1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle.$$

7). И тем самым задача решена■

***Пример 5.9*б** (задача прямого анализа)

Известен вычислительный базис, т.е. $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$. Известен входной вектор $|\psi\rangle = |1\rangle$ и квантовый одновходовой элемент с матрицей преобразования $\boldsymbol{M} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$.

Требуется определить выходной вектор $|\psi'\rangle = \begin{bmatrix} A \\ B \end{bmatrix}$ в вычислительном базисе на выходе квантовой схемы, состоящей из этого одного квантового элемента:



Решение

1). В условиях задачи указан явно вычислительный базис. Будем далее предполагать, что входной вектор $|\psi\rangle$, выходной вектор $|\psi'\rangle$ и матрица преобразования $\boldsymbol{M}$ соответствуют одному и тому же вычислительному базису.

2). Проверим корректность исходных данных.

Условие нормировки для входного вектора $|\psi\rangle$ $|0|^2 + |1|^2 = 0 + 1 = 1$ выполняется.

$$M^{\dagger}M = \left(\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \right)^{\dagger} \times \left(\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \right) =$$

$$= \frac{1}{\sqrt{2}} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \times \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} =$$

$$= \frac{1}{2} \begin{bmatrix} 1+1 & 1-1 \\ 1-1 & 1-(-1) \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \equiv I,$$

т.е. свойство унитарности матрицы $\boldsymbol{M}$ выполняется.

3). Так как входной и выходной векторы связаны соотношением

$$M \times |\psi\rangle = |\psi'\rangle = \begin{bmatrix} A \\ B \end{bmatrix},$$

то, зная $\boldsymbol{M}$ и $|\psi\rangle$, а также применяя *Правило* 5.0**а**, вычислим выходной вектор $|\psi'\rangle = \begin{bmatrix} A \\ B \end{bmatrix}$ на выходе квантовой схемы:

$$M \times |\psi\rangle =$$

$$= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \times \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 0+1 \\ 0-1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} A \\ B \end{bmatrix},$$

т.е. $A = \frac{1}{\sqrt{2}}$, $B = \frac{-1}{\sqrt{2}}$ или $|\psi'\rangle = \begin{bmatrix} A \\ B \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$.

4). Проверим условие нормировки для выходного вектора $|\psi'\rangle$

$$\left|\frac{1}{\sqrt{2}}\right|^2 + \left|\frac{-1}{\sqrt{2}}\right|^2 = \frac{1}{2} + \frac{1}{2} = \frac{2}{2} = 1,$$

т.е. условие нормировки выполняется.

5). Проверять, что найденный вектор $|\psi'\rangle$ действительно удовлетворяет условиям задачи:

$$M \times |\psi\rangle = |\psi'\rangle,$$

не требуется, так как это прямо следует из самого решения.

6). Представим выходной вектор $|\psi'\rangle$ в вычислительном базисе:

$$|\psi'\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1-0 \\ 0-1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \end{bmatrix} - \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle.$$

7). И тем самым задача решена■

***Пример 5.9*в** (задача прямого анализа)

Известен вычислительный базис, т.е. $|0\rangle=\begin{bmatrix}1\\0\end{bmatrix}$, $|1\rangle=\begin{bmatrix}0\\1\end{bmatrix}$. Известен входной вектор $|\psi\rangle=a|0\rangle+b|1\rangle$ (где $|a|^2+|b|^2=1$) и квантовый одновходовой элемент с матрицей преобразования $\boldsymbol{M}=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}$.

Требуется определить выходной вектор $|\psi'\rangle=\begin{bmatrix}A\\B\end{bmatrix}$ в вычислительном базисе на выходе квантовой схемы, состоящей из этого одного квантового элемента:

$$a|0\rangle+b|1\rangle \longrightarrow \boxed{\boldsymbol{M}} \longrightarrow |\psi'\rangle.$$

Решение

1). В условиях задачи указан явно вычислительный базис. Будем далее предполагать, что входной вектор $|\psi\rangle$, выходной вектор $|\psi'\rangle$ и матрица преобразования $\boldsymbol{M}$ соответствуют одному и тому же вычислительному базису.

2). Проверим корректность исходных данных.

Условие нормировки для входного вектора $|\psi\rangle$ выполняется (так как $|a|^2+|b|^2=1$).

$$M^{\dagger}M=\left(\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}\right)^{\dagger}\times\left(\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}\right)=$$

$$=\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}\times\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}=$$

$$=\frac{1}{2}\begin{bmatrix}1+1 & 1-1\\1-1 & 1-(-1)\end{bmatrix}=\frac{1}{2}\begin{bmatrix}2 & 0\\0 & 2\end{bmatrix}=\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}\equiv I,$$

т.е. свойство унитарности матрицы $\boldsymbol{M}$ выполняется.

3). Так как входной и выходной векторы связаны соотношением

$$M \times |\psi\rangle = |\psi'\rangle = \begin{bmatrix} A \\ B \end{bmatrix},$$

то, зная $\boldsymbol{M}$ и $|\psi\rangle = a|0\rangle + b|1\rangle = a\begin{bmatrix} 1 \\ 0 \end{bmatrix} + b\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix}$, вычислим выходной вектор $|\psi'\rangle = \begin{bmatrix} A \\ B \end{bmatrix}$ на выходе квантовой схемы:

$$M \times |\psi\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \times \begin{bmatrix} a \\ b \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} a+b \\ a-b \end{bmatrix} = \begin{bmatrix} \frac{a+b}{\sqrt{2}} \\ \frac{a-b}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} A \\ B \end{bmatrix},$$

т.е. $A = \frac{a-b}{\sqrt{2}}$, $B = \frac{a+b}{\sqrt{2}}$ или

$$|\psi'\rangle = \begin{bmatrix} A \\ B \end{bmatrix} = \begin{bmatrix} \frac{a+b}{\sqrt{2}} \\ \frac{a-b}{\sqrt{2}} \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} a+b \\ a-b \end{bmatrix}.$$

4). Проверим условие нормировки для выходного вектора $|\psi'\rangle$

$$\left(\frac{|a+b|}{\sqrt{2}}\right)^2 + \left(\frac{|a-b|}{\sqrt{2}}\right)^2 = 1, \text{ где } |a|^2 + |b|^2 = 1,$$

т.е. условие нормировки выполняется.

5). Проверять, что найденный вектор $|\psi'\rangle$ действительно удовлетворяет условиям задачи: $M \times |\psi\rangle = |\psi'\rangle$, не требуется, так как это прямо следует из самого решения.

6). Представим выходной вектор $|\psi'\rangle$ в вычислительном базисе:

$$|\psi'\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} a+b \\ a-b \end{bmatrix} = \frac{a+b}{\sqrt{2}}\begin{bmatrix} 1 \\ 0 \end{bmatrix} + \frac{a-b}{\sqrt{2}}\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{a+b}{\sqrt{2}}|0\rangle + \frac{a-b}{\sqrt{2}}|1\rangle.$$

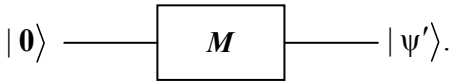
7). И тем самым задача решена■

***Пример 5.10*а** (задача прямого анализа)

Известен вычислительный базис, т.е. $|\mathbf{0}\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}$, $|\mathbf{1}\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}$.

Известен входной вектор $|\psi\rangle = |\mathbf{0}\rangle$ и квантовый одновходовой элемент с матрицей преобразования $\boldsymbol{M} = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}$.

Требуется определить выходной вектор $|\psi'\rangle = \begin{bmatrix}A\\B\end{bmatrix}$ в вычислительном базисе на выходе квантовой схемы, состоящей из этого одного квантового элемента:



Решение

1). В условиях задачи указан явно вычислительный базис. Будем далее предполагать, что входной вектор $|\psi\rangle$, выходной вектор $|\psi'\rangle$ и матрица преобразования $\boldsymbol{M}$ соответствуют одному и тому же вычислительному базису.

2). Проверим корректность исходных данных.

Условие нормировки для входного вектора $|\psi\rangle$ $\left|\frac{1}{\sqrt{2}}\right|^2 + \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2} + \frac{1}{2} = \frac{2}{2} = 1$ выполняется.

$$M^{\dagger}M = \left(\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}\right)^{\dagger} \times \left(\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}\right) =$$

$$= \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix} \times \begin{bmatrix}1 & 1\\1 & -1\end{bmatrix} =$$

$$= \frac{1}{2}\begin{bmatrix}1+1 & 1-1\\1-1 & 1-(-1)\end{bmatrix} = \frac{1}{2}\begin{bmatrix}2 & 0\\0 & 2\end{bmatrix} = \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix} \equiv I,$$

т.е. свойство унитарности матрицы $\boldsymbol{M}$ выполняется.

3). Так как входной и выходной векторы связаны соотношением

$$M \times |\psi\rangle = |\psi'\rangle = \begin{bmatrix} A \\ B \end{bmatrix},$$

то, зная $\boldsymbol{M}$ и $|\psi\rangle$, вычислим выходной вектор $|\psi'\rangle = \begin{bmatrix} A \\ B \end{bmatrix}$ на выходе квантовой схемы:

$$M \times |\psi\rangle = \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \times \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1+1 \\ 1-1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 2 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} A \\ B \end{bmatrix},$$

т.е. $A = 1$, $B = 0$ или $|\psi'\rangle = \begin{bmatrix} A \\ B \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$.

4). Проверим условие нормировки для выходного вектора $|\psi'\rangle$

$$|1|^2 + |0|^2 = 1 + 0 = 1,$$

т.е. условие нормировки выполняется.

5). Проверять, что найденный вектор $|\psi'\rangle$ действительно удовлетворяет условиям задачи:

$$M \times |\psi\rangle = |\psi'\rangle,$$

не требуется, так как это прямо следует из самого решения.

6). Представим выходной вектор $|\psi'\rangle$ в вычислительном базисе:

$$|\psi'\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1+1 \\ 1-1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 \\ 1 \end{bmatrix} + \frac{1}{2}\begin{bmatrix} 1 \\ -1 \end{bmatrix} =$$

$$= \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix} + \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{1}{\sqrt{2}}|\mathbf{0}\rangle + \frac{1}{\sqrt{2}}|\mathbf{1}\rangle.$$

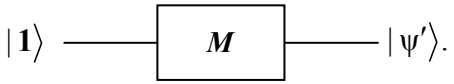
7). И тем самым задача решена■

Пример 5.10б (задача прямого анализа)

Известен вычислительный базис, т.е. $|\mathbf{0}\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}$, $|\mathbf{1}\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}$.

Известен входной вектор $|\psi\rangle = |\mathbf{1}\rangle$ и квантовый одновходовой элемент с матрицей преобразования $\boldsymbol{M} = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}$.

Требуется определить выходной вектор $|\psi'\rangle = \begin{bmatrix}A\\B\end{bmatrix}$ в вычислительном базисе на выходе квантовой схемы, состоящей из этого одного квантового элемента:



Решение

1). В условиях задачи указан явно вычислительный базис. Будем далее предполагать, что входной вектор $|\psi\rangle$, выходной вектор $|\psi'\rangle$ и матрица преобразования $\boldsymbol{M}$ соответствуют одному и тому же вычислительному базису.

2). Проверим корректность исходных данных.

Условие нормировки для входного вектора $|\psi\rangle$ $\left|\frac{1}{\sqrt{2}}\right|^2 + \left|\frac{-1}{\sqrt{2}}\right|^2 = \frac{1}{2}+\frac{1}{2} = \frac{2}{2} = 1$ выполняется.

$$M^{\dagger}M = \left(\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}\right)^{\dagger} \times \left(\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}\right) =$$

$$= \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix} \times \begin{bmatrix}1 & 1\\1 & -1\end{bmatrix} =$$

$$= \frac{1}{2}\begin{bmatrix}1+1 & 1-1\\1-1 & 1-(-1)\end{bmatrix} = \frac{1}{2}\begin{bmatrix}2 & 0\\0 & 2\end{bmatrix} = \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix} \equiv I,$$

т.е. свойство унитарности матрицы $\boldsymbol{M}$ выполняется.

3). Так как входной и выходной векторы связаны соотношением

$$M \times |\psi\rangle = |\psi'\rangle = \begin{bmatrix} A \\ B \end{bmatrix},$$

то, зная $\boldsymbol{M}$ и $|\psi\rangle$, вычислим выходной вектор $|\psi'\rangle = \begin{bmatrix} A \\ B \end{bmatrix}$ на выходе квантовой схемы:

$$M \times |\psi\rangle = \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \times \begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1-1 \\ 1+1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 0 \\ 2 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} A \\ B \end{bmatrix},$$

т.е. $A = 0$, $B = 1$ или $|\psi'\rangle = \begin{bmatrix} A \\ B \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$.

4). Проверим условие нормировки для выходного вектора $|\psi'\rangle$

$$|0|^2 + |1|^2 = 0 + 1 = 1,$$

т.е. условие нормировки выполняется.

5). Проверять, что найденный вектор $|\psi'\rangle$ действительно удовлетворяет условиям задачи:

$$M \times |\psi\rangle = |\psi'\rangle,$$

не требуется, так как это прямо следует из самого решения.

6). Представим выходной вектор $|\psi'\rangle$ в вычислительном базисе:

$$|\psi'\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1-(+1) \\ 1-(-1) \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 \\ 1 \end{bmatrix} - \frac{1}{2}\begin{bmatrix} 1 \\ -1 \end{bmatrix} =$$

$$= \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix} - \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{1}{\sqrt{2}}|\mathbf{0}\rangle - \frac{1}{\sqrt{2}}|\mathbf{1}\rangle.$$

7). И тем самым задача решена■

***Пример 5.10*в** (задача прямого анализа)

Известен вычислительный базис, т.е. $|\mathbf{0}\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}$, $|\mathbf{1}\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}$.

Известен входной вектор $|\psi\rangle = a|\mathbf{0}\rangle + b|\mathbf{1}\rangle$ (где $|a|^2+|b|^2=1$) и квантовый одновходовой элемент с матрицей преобразования $\boldsymbol{M} = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}$.

Требуется определить выходной вектор $|\psi'\rangle = \begin{bmatrix}A\\B\end{bmatrix}$ в вычислительном базисе на выходе квантовой схемы, состоящей из этого одного квантового элемента:

$$a|\mathbf{0}\rangle + b|\mathbf{1}\rangle \longrightarrow \boxed{\boldsymbol{M}} \longrightarrow |\psi'\rangle.$$

Решение

1). В условиях задачи указан явно вычислительный базис. Будем далее предполагать, что входной вектор $|\psi\rangle$, выходной вектор $|\psi'\rangle$ и матрица преобразования $\boldsymbol{M}$ соответствуют одному и тому же вычислительному базису.

2). Проверим корректность исходных данных.

Условие нормировки для входного вектора $|\psi\rangle$ выполняется (так как $|a|^2+|b|^2=1$).

$$M^{\dagger}M = \left(\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}\right)^{\dagger} \times \left(\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}\right) =$$

$$= \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix} \times \begin{bmatrix}1 & 1\\1 & -1\end{bmatrix} =$$

$$= \frac{1}{2}\begin{bmatrix}1+1 & 1-1\\1-1 & 1-(-1)\end{bmatrix} = \frac{1}{2}\begin{bmatrix}2 & 0\\0 & 2\end{bmatrix} = \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix} \equiv I,$$

т.е. свойство унитарности матрицы $\boldsymbol{M}$ выполняется.

3). Так как входной и выходной векторы связаны соотношением

$$M \times |\psi\rangle = |\psi'\rangle = \begin{bmatrix} A \\ B \end{bmatrix},$$

то, зная $\boldsymbol{M}$ и $|\psi\rangle$

$|\psi\rangle = a|\mathbf{0}\rangle + b|\mathbf{1}\rangle = a\frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix} + b\frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}a+b\\a-b\end{bmatrix}$, вычислим выходной вектор $|\psi'\rangle = \begin{bmatrix} A \\ B \end{bmatrix}$ на выходе квантовой схемы:

$$M \times |\psi\rangle =$$

$$= \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} \times \frac{1}{\sqrt{2}}\begin{bmatrix}a+b\\a-b\end{bmatrix} = \frac{1}{2}\begin{bmatrix}(a+b)+(a-b)\\(a+b)-(a-b)\end{bmatrix} = \begin{bmatrix}a\\b\end{bmatrix} = \begin{bmatrix}A\\B\end{bmatrix},$$

т.е. $A = a$, $B = b$ или

$$|\psi'\rangle = \begin{bmatrix} A \\ B \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix}.$$

4). Проверим условие нормировки для выходного вектора $|\psi'\rangle$

$$|a|^2 + |b|^2 = 1,$$

которое выполняется по условию задачи.

5). Проверять, что найденный вектор $|\psi'\rangle$ действительно удовлетворяет условиям задачи:

$$M \times |\psi\rangle = |\psi'\rangle,$$

не требуется, так как это прямо следует из самого решения.

6). Представим выходной вектор $|\psi'\rangle$ в вычислительном базисе:

$$|\psi'\rangle = \begin{bmatrix} a \\ b \end{bmatrix} = \frac{1}{2}\begin{bmatrix}2a\\2b\end{bmatrix} = \frac{1}{2}\begin{bmatrix}(a+b)+(a-b)\\(a+b)-(a-b)\end{bmatrix} =$$

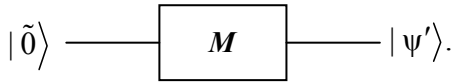
$$= \frac{a+b}{\sqrt{2}}\frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix} + \frac{a-b}{\sqrt{2}}\frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix} = \frac{a+b}{\sqrt{2}}|\mathbf{0}\rangle + \frac{a-b}{\sqrt{2}}|\mathbf{1}\rangle.$$

7). И тем самым задача решена■

***Пример 5.11*а** (задача прямого анализа)

Известен вычислительный базис, т.е. $|\tilde{0}\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$, $|\tilde{1}\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$. Известен входной вектор $|\psi\rangle = |\tilde{0}\rangle$ и квантовый одновходовой элемент с матрицей преобразования $\boldsymbol{M} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$.

Требуется определить выходной вектор $|\psi'\rangle = \begin{bmatrix} A \\ B \end{bmatrix}$ в вычислительном базисе на выходе квантовой схемы, состоящей из этого одного квантового элемента:



Решение

1). В условиях задачи указан явно вычислительный базис. Будем далее предполагать, что входной вектор $|\psi\rangle$, выходной вектор $|\psi'\rangle$ и матрица преобразования $\boldsymbol{M}$ соответствуют одному и тому же вычислительному базису.

2). Проверим корректность исходных данных.

Условие нормировки для входного вектора $|\psi\rangle$ $|0|^2 + |1|^2 = 0 + 1 = 1$ выполняется.

$$M^{\dagger}M = \left(\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\right)^{\dagger} \times \left(\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\right) =$$

$$= \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \times \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} =$$

$$= \frac{1}{2}\begin{bmatrix} 1+1 & 1-1 \\ 1-1 & 1-(-1) \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \equiv I,$$

т.е. свойство унитарности матрицы $\boldsymbol{M}$ выполняется.

3). Так как входной и выходной векторы связаны соотношением

$$M \times |\psi\rangle = |\psi'\rangle = \begin{bmatrix} A \\ B \end{bmatrix},$$

то, зная $\boldsymbol{M}$ и $|\psi\rangle$, а также применяя *Правило* 5.0**а**, вычислим выходной вектор $|\psi'\rangle = \begin{bmatrix} A \\ B \end{bmatrix}$ на выходе квантовой схемы:

$$M \times |\psi\rangle =$$

$$= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \times \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 0+1 \\ 0-1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} A \\ B \end{bmatrix},$$

т.е. $A = \frac{1}{\sqrt{2}}$, $B = \frac{-1}{\sqrt{2}}$ или $|\psi'\rangle = \begin{bmatrix} A \\ B \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$.

4). Проверим условие нормировки для выходного вектора $|\psi'\rangle$

$$\left|\frac{1}{\sqrt{2}}\right|^2 + \left|\frac{-1}{\sqrt{2}}\right|^2 = \frac{1}{2} + \frac{1}{2} = \frac{2}{2} = 1,$$

т.е. условие нормировки выполняется.

5). Проверять, что найденный вектор $|\psi'\rangle$ действительно удовлетворяет условиям задачи:

$$M \times |\psi\rangle = |\psi'\rangle,$$

не требуется, так как это прямо следует из самого решения.

6). Представим выходной вектор $|\psi'\rangle$ в вычислительном базисе:

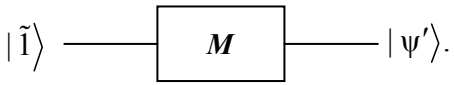
$$|\psi'\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1-0 \\ 0-1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \end{bmatrix} - \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} |\tilde{0}\rangle - \frac{1}{\sqrt{2}} |\tilde{1}\rangle.$$

7). И тем самым задача решена■

Пример 5.11б (задача прямого анализа)

Известен вычислительный базис, т.е. $|\tilde{0}\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$, $|\tilde{1}\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$. Известен входной вектор $|\psi\rangle = |\tilde{1}\rangle$ и квантовый одновходовой элемент с матрицей преобразования $\boldsymbol{M} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$.

Требуется определить выходной вектор $|\psi'\rangle = \begin{bmatrix} A \\ B \end{bmatrix}$ в вычислительном базисе на выходе квантовой схемы, состоящей из этого одного квантового элемента:



Решение

1). В условиях задачи указан явно вычислительный базис. Будем далее предполагать, что входной вектор $|\psi\rangle$, выходной вектор $|\psi'\rangle$ и матрица преобразования $\boldsymbol{M}$ соответствуют одному и тому же вычислительному базису.

2). Проверим корректность исходных данных.

Условие нормировки для входного вектора $|\psi\rangle$ $|1|^2 + |0|^2 = 1 + 0 = 1$ выполняется.

$$M^{\dagger} M = \left(\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \right)^{\dagger} \times \left(\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \right) =$$

$$= \frac{1}{\sqrt{2}} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \times \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} =$$

$$= \frac{1}{2} \begin{bmatrix} 1+1 & 1-1 \\ 1-1 & 1-(-1) \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \equiv I,$$

т.е. свойство унитарности матрицы $\boldsymbol{M}$ выполняется.

3). Так как входной и выходной векторы связаны соотношением

$$M \times |\psi\rangle = |\psi'\rangle = \begin{bmatrix} A \\ B \end{bmatrix},$$

то, зная $\boldsymbol{M}$ и $|\psi\rangle$, вычислим выходной вектор $|\psi'\rangle = \begin{bmatrix} A \\ B \end{bmatrix}$ на выходе квантовой схемы:

$$M \times |\psi\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \times \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1+0 \\ 1-0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} A \\ B \end{bmatrix},$$

т.е. $A = \frac{1}{\sqrt{2}}$, $B = \frac{1}{\sqrt{2}}$ или $|\psi'\rangle = \begin{bmatrix} A \\ B \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}$.

4). Проверим условие нормировки для выходного вектора $|\psi'\rangle$

$$\left|\frac{1}{\sqrt{2}}\right|^2 + \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2} + \frac{1}{2} = \frac{2}{2} = 1,$$

т.е. условие нормировки выполняется.

5). Проверять, что найденный вектор $|\psi'\rangle$ действительно удовлетворяет условиям задачи:

$$M \times |\psi\rangle = |\psi'\rangle,$$

не требуется, так как это прямо следует из самого решения.

6). Представим выходной вектор $|\psi'\rangle$ в вычислительном базисе:

$$|\psi'\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1+0 \\ 0+1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} |\tilde{0}\rangle + \frac{1}{\sqrt{2}} |\tilde{1}\rangle.$$

7). И тем самым задача решена■

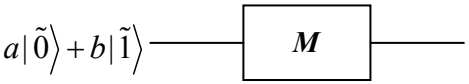
***Пример 5.11*в** (задача прямого анализа)

Известен вычислительный базис, т.е. $|\tilde{0}\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$, $|\tilde{1}\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$.

Известен входной вектор $|\psi\rangle = a|\tilde{0}\rangle + b|\tilde{1}\rangle$ (где $|a|^2+|b|^2=1$) и квантовый одновходовой элемент с матрицей преобразования

$$\boldsymbol{M} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

Требуется определить выходной вектор $|\psi'\rangle = \begin{bmatrix} A \\ B \end{bmatrix}$ в вычислительном базисе на выходе квантовой схемы, состоящей из этого одного квантового элемента:



Решение

1). В условиях задачи указан явно вычислительный базис. Будем далее предполагать, что входной вектор $|\psi\rangle$, выходной вектор $|\psi'\rangle$ и матрица преобразования $\boldsymbol{M}$ соответствуют одному и тому же вычислительному базису.

2). Проверим корректность исходных данных.

Условие нормировки для входного вектора $|\psi\rangle$ выполняется (так как $|a|^2+|b|^2=1$).

$$M^{\dagger}M = \left(\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\right)^{\dagger} \times \left(\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\right) =$$

$$= \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \times \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} =$$

$$= \frac{1}{2}\begin{bmatrix} 1+1 & 1-1 \\ 1-1 & 1-(-1) \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \equiv I,$$

т.е. свойство унитарности матрицы $\boldsymbol{M}$ выполняется.

3). Так как входной и выходной векторы связаны соотношением

$$M \times |\psi\rangle = |\psi'\rangle = \begin{bmatrix} A \\ B \end{bmatrix},$$

то, зная $\boldsymbol{M}$ и $|\psi\rangle = a|\tilde{0}\rangle + b|\tilde{1}\rangle = a\begin{bmatrix} 0 \\ 1 \end{bmatrix} + b\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} b \\ a \end{bmatrix}$, вычислим выходной вектор $|\psi'\rangle = \begin{bmatrix} A \\ B \end{bmatrix}$ на выходе квантовой схемы:

$$M \times |\psi\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \times \begin{bmatrix} b \\ a \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} b+a \\ b-a \end{bmatrix} = \begin{bmatrix} \frac{b+a}{\sqrt{2}} \\ \frac{b-a}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} A \\ B \end{bmatrix},$$

т.е. $A = \frac{b+a}{\sqrt{2}}$, $B = \frac{b-a}{\sqrt{2}}$ или

$$|\psi'\rangle = \begin{bmatrix} A \\ B \end{bmatrix} = \begin{bmatrix} \frac{b+a}{\sqrt{2}} \\ \frac{b-a}{\sqrt{2}} \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} b+a \\ b-a \end{bmatrix}.$$

4). Проверим условие нормировки для выходного вектора $|\psi'\rangle$

$$\left(\frac{|b+a|}{\sqrt{2}}\right)^2 + \left(\frac{|b-a|}{\sqrt{2}}\right)^2 = 1, \text{ где } |a|^2 + |b|^2 = 1,$$

т.е. условие нормировки выполняется.

5). Проверять, что найденный вектор $|\psi'\rangle$ действительно удовлетворяет условиям задачи: $M \times |\psi\rangle = |\psi'\rangle$, не требуется, так как это прямо следует из самого решения.

6). Представим выходной вектор $|\psi'\rangle$ в вычислительном базисе:

$$|\psi'\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} b+a \\ b-a \end{bmatrix} = \frac{b-a}{\sqrt{2}}\begin{bmatrix} 0 \\ 1 \end{bmatrix} + \frac{b+a}{\sqrt{2}}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{b-a}{\sqrt{2}}|\tilde{0}\rangle + \frac{b+a}{\sqrt{2}}|\tilde{1}\rangle.$$

7). И тем самым задача решена■

Пример 5.12 (задача синтеза квантовой схемы)

Известен вычислительный базис, т.е. $|\tilde{0}\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$, $|\tilde{1}\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$. Есть квантовая схема, состоящая из одного квантового элемента с матрицей преобразования $\boldsymbol{M} = \begin{bmatrix} w & s \\ z & t \end{bmatrix}$, причем w, s, z, t — это комплексные числа. Известно, какой выходной вектор $|\psi'\rangle$ должен быть на выходе, если на вход этой квантовой схемы подан соответствующий входной вектор $|\psi\rangle$. Входные и выходные векторы связаны с помощью матрицы $\boldsymbol{M}$ так $\boldsymbol{M}|\psi\rangle = |\psi'\rangle$ или более подробно следующим образом:

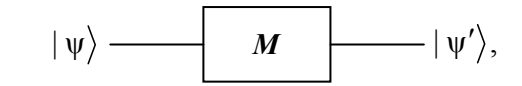
$$\boldsymbol{M}|\tilde{0}\rangle = \frac{1}{\sqrt{2}}|\tilde{0}\rangle + \frac{1}{\sqrt{2}}|\tilde{1}\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 0 \\ 1 \end{bmatrix} + \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} 0+1 \\ 1+0 \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix},$$

$$\boldsymbol{M}|\tilde{1}\rangle = \frac{1}{\sqrt{2}}|\tilde{0}\rangle - \frac{1}{\sqrt{2}}|\tilde{1}\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 0 \\ 1 \end{bmatrix} - \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} 0-1 \\ 1-0 \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} -1 \\ 1 \end{bmatrix},$$

или это же можно записать по-другому

$$\boldsymbol{M}|\tilde{0}\rangle = \begin{bmatrix} w & s \\ z & t \end{bmatrix} \times \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}, \quad \boldsymbol{M}|\tilde{1}\rangle = \begin{bmatrix} w & s \\ z & t \end{bmatrix} \times \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{-1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}.$$

Требуется определить w, s, z, t, т.е. синтезировать матрицу $\boldsymbol{M}$ квантового элемента:



т.е. достаточно найти хотя бы одно решение (т.е. одну матрицу $\boldsymbol{M}$).

Решение

1). В условиях задачи указан явно вычислительный базис. Будем далее предполагать, что входной вектор $|\psi\rangle$, выходной вектор $|\psi'\rangle$ и матрица преобразования $\boldsymbol{M}$ соответствуют одному и тому же вычислительному базису.

2). Так как по условию задачи

$$\boldsymbol{M}|\tilde{0}\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix},\ \boldsymbol{M}|\tilde{1}\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}-1\\1\end{bmatrix}$$

и выполнимы соотношения

$$\boldsymbol{M}|\tilde{0}\rangle = \begin{bmatrix}w & s\\ z & t\end{bmatrix}\times\begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}w\cdot 0 + s\cdot 1\\ z\cdot 0 + t\cdot 1\end{bmatrix} = \begin{bmatrix}s\\t\end{bmatrix} = \begin{bmatrix}\dfrac{1}{\sqrt{2}}\\[2mm] \dfrac{1}{\sqrt{2}}\end{bmatrix},$$

$$\boldsymbol{M}|\tilde{1}\rangle = \begin{bmatrix}w & s\\ z & t\end{bmatrix}\times\begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}w\cdot 1 + s\cdot 0\\ z\cdot 1 + t\cdot 0\end{bmatrix} = \begin{bmatrix}w\\z\end{bmatrix} = \begin{bmatrix}\dfrac{-1}{\sqrt{2}}\\[2mm] \dfrac{1}{\sqrt{2}}\end{bmatrix},$$

то можно сразу найти все элементы матрицы $\boldsymbol{M}$:

$$s = t = \frac{1}{\sqrt{2}} \quad \text{и} \quad w = -\frac{1}{\sqrt{2}},\ z = \frac{1}{\sqrt{2}}.$$

3). Проверим условие, что синтезированная матрица $\boldsymbol{M}$ унитарна:

$$M^{\dagger}M = \left(\frac{1}{\sqrt{2}}\begin{bmatrix}-1 & 1\\ 1 & 1\end{bmatrix}\right)^{\dagger}\times\left(\frac{1}{\sqrt{2}}\begin{bmatrix}-1 & 1\\ 1 & 1\end{bmatrix}\right) = \frac{1}{2}\begin{bmatrix}-1 & 1\\ 1 & 1\end{bmatrix}\times\begin{bmatrix}-1 & 1\\ 1 & 1\end{bmatrix} =$$

$$= \frac{1}{2}\begin{bmatrix}1+1 & 1-1\\ 1-1 & 1-(-1)\end{bmatrix} = \frac{1}{2}\begin{bmatrix}2 & 0\\ 0 & 2\end{bmatrix} = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} \equiv I,$$

т.е. свойство унитарности матрицы $\boldsymbol{M}$ выполняется.

4). Проверим, что найденная (синтезированная) матрица $\boldsymbol{M}$ действительно удовлетворяет условиям задачи:

$$M\times|\psi\rangle = |\psi'\rangle$$

или

$$|\tilde{0}\rangle \Rightarrow \boldsymbol{M}|\tilde{0}\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}-1 & 1\\ 1 & 1\end{bmatrix}\times\begin{bmatrix}0\\1\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}(-1)\cdot 0+1\cdot 1\\ 1\cdot 0+1\cdot 1\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix} =$$

$$= \frac{1}{\sqrt{2}}\begin{bmatrix}0+1\\1+0\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}0\\1\end{bmatrix} + \frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\end{bmatrix} = \frac{1}{\sqrt{2}}|\tilde{0}\rangle + \frac{1}{\sqrt{2}}|\tilde{1}\rangle,$$

$$|\tilde{1}\rangle \Rightarrow \boldsymbol{M}|\tilde{1}\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}-1 & 1\\ 1 & 1\end{bmatrix}\times\begin{bmatrix}1\\0\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}(-1)\cdot 1+1\cdot 0\\ 1\cdot 1+1\cdot 0\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}-1\\1\end{bmatrix} =$$

$$= \frac{1}{\sqrt{2}}\begin{bmatrix}0-1\\1-0\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}0\\1\end{bmatrix} - \frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\end{bmatrix} = \frac{1}{\sqrt{2}}|\tilde{0}\rangle - \frac{1}{\sqrt{2}}|\tilde{1}\rangle,$$

т.е. условия задачи выполнены. Аналогично для входного вектора

$$a|\tilde{0}\rangle + b|\tilde{1}\rangle \Rightarrow \text{ так как } a|\tilde{0}\rangle + b|\tilde{1}\rangle = a\begin{bmatrix}0\\1\end{bmatrix} + b\begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}0\\a\end{bmatrix} + \begin{bmatrix}b\\0\end{bmatrix} = \begin{bmatrix}b\\a\end{bmatrix},$$

то

$$\boldsymbol{M}\left\{a|\tilde{0}\rangle + b|\tilde{1}\rangle\right\} =$$

$$= \frac{1}{\sqrt{2}}\begin{bmatrix}-1 & 1\\ 1 & 1\end{bmatrix}\times\begin{bmatrix}b\\a\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}(-1)\cdot b+1\cdot a\\ 1\cdot b+1\cdot a\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}a-b\\a+b\end{bmatrix} =$$

$$= \frac{1}{\sqrt{2}}\begin{bmatrix}0\\a+b\end{bmatrix} + \frac{1}{\sqrt{2}}\begin{bmatrix}a-b\\0\end{bmatrix} =$$

$$= \frac{a+b}{\sqrt{2}}\begin{bmatrix}0\\1\end{bmatrix} + \frac{a-b}{\sqrt{2}}\begin{bmatrix}1\\0\end{bmatrix} = \frac{a+b}{\sqrt{2}}|\tilde{0}\rangle + \frac{a-b}{\sqrt{2}}|\tilde{1}\rangle.$$

Таким образом, найдено одно решение

$$\boldsymbol{M} = \frac{1}{\sqrt{2}}\begin{bmatrix}-1 & 1\\ 1 & 1\end{bmatrix}.$$

5). И тем самым задача решена■

Кратко обсудим разобранные выше примеры. В ***Примерах 5.9***, ***5.10***, ***5.11*** был выбран разный вычислительный базис (т.е. то, что считается ***нулем*** и ***единицей***) и одна и та же унитарная матрица. Каждый раз на вход квантовой схемы подавался либо ***нуль***, либо ***единица***, либо суперпозиция.

Выходной вектор $|\psi'\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ в ***Примерах 5.9*****а**, ***5.10*****а** совпадает (см. также табл. 5.1, элемент *Адамара* при ***a***=1 и ***b***=0), но отличается от выходного вектора $|\psi'\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$ в ***Примере 5.11*****а**.

Выходной вектор $|\psi'\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$ в ***Примерах 5.9*****б**, ***5.10*****б** совпадает (см. также табл. 5.1, элемент *Адамара* при ***a***=0 и ***b***=1), но отличается от выходного вектора $|\psi'\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ в ***Примере 5.11*****б**.

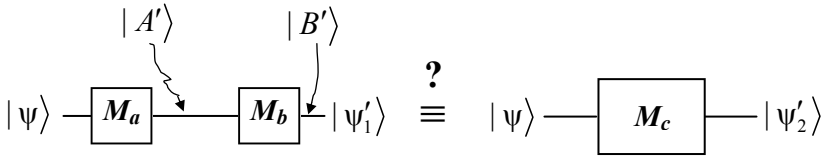
Выходной вектор $|\psi'\rangle = \frac{a+b}{\sqrt{2}}|0\rangle + \frac{a-b}{\sqrt{2}}|1\rangle$ в ***Примерах 5.9*****в**, ***5.10*****в** совпадает (см. также табл. 5.1, элемент *Адамара*), но отличается от выходного вектора $|\psi'\rangle = \frac{b-a}{\sqrt{2}}|0\rangle + \frac{b+a}{\sqrt{2}}|1\rangle$ в ***Примере 5.11***.

В ***Примере 5.12*** выполнен успешно синтез унитарной матрицы $\boldsymbol{M} = \frac{1}{\sqrt{2}}\begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix}$, которая в отличие от матрицы $\boldsymbol{M} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ обеспечивает для ***Примера 5.11*** такие же выходные векторы, как и в ***Примерах 5.9***, ***5.10***.

Рассмотрим еще один простой пример, который позволит далее сформулировать еще одно правило для квантовых схем.

Пример 5.13 (эквивалентные схемы на одном кубите)
Известна квантовая схема из 2-х последовательно соединенных однокубитовых гейтов с соответствующими унитарными матрицами $\boldsymbol{M_a}$ и $\boldsymbol{M_b}$.

Требуется определить один однокубитовый гейт, который эквивалентен этим двум последовательно соединенным однокубитовым гейтам. Другими словами, требуется определить унитарную матрицу $\boldsymbol{M_c}$ результирующего преобразования и установить, что следующие две квантовые схемы эквивалентны:



Решение

1). В условиях задачи не указан явно вычислительный базис. Будем далее предполагать, что входной вектор $|\psi\rangle$, выходные векторы $|\psi_1'\rangle$, $|\psi_2'\rangle$ и матрицы преобразования $\boldsymbol{M_a}$, $\boldsymbol{M_b}$ и $\boldsymbol{M_c}$ соответствуют одному и тому же вычислительному базису.

2). Эквивалентность двух схем понимается в том смысле, что при подаче одного и того же входного вектора $|\psi\rangle$ на вход каждой из этих схем на их выходе получается один и тот же выходной вектор, т.е. $|\psi_1'\rangle = |\psi_2'\rangle$, при этом матрица $\boldsymbol{M_c}$ результирующего преобразования является (как и матрицы $\boldsymbol{M_a}$ и $\boldsymbol{M_b}$) также унитарной. Специально отметим, что результирующее преобразование с матрицей $\boldsymbol{M_c}$ зависит, вообще говоря, от порядка, в котором выполняются операции с матрицами $\boldsymbol{M_a}$ и $\boldsymbol{M_b}$ (т.е. от порядка в котором выполняются гейты).

3). Так как из главы 2 следует, что результат произведения унитарных операторов есть унитарный оператор, а значит, результат умножения двух унитарных матриц $\boldsymbol{M_b} \times \boldsymbol{M_a} = \boldsymbol{M_c}$ есть унитарная матрица, то свойство унитарности матрицы $\boldsymbol{M_c}$ выполняется.

4). Пусть

$$\boldsymbol{M_a} = \begin{bmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{bmatrix},$$

$$\boldsymbol{M_b} = \begin{bmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \end{bmatrix},$$

тогда результирующая матрица $\boldsymbol{M_c}=\boldsymbol{M_b}\times\boldsymbol{M_a}$ (именно в таком порядке $\boldsymbol{M_b}$ на $\boldsymbol{M_a}$, хотя сами гейты в квантовой схеме идут в обратном: порядке сначала преобразование с матрицей $\boldsymbol{M_a}$, а затем преобразование с матрицей $\boldsymbol{M_b}$) есть

$$\begin{bmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \end{bmatrix} \times \begin{bmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{bmatrix} =$$

$$= \begin{bmatrix} b_{00}\cdot a_{00} + b_{01}\cdot a_{10} & b_{00}\cdot a_{01} + b_{01}\cdot a_{11} \\ b_{10}\cdot a_{00} + b_{11}\cdot a_{10} & b_{10}\cdot a_{01} + b_{11}\cdot a_{11} \end{bmatrix} = \begin{bmatrix} c_{00} & c_{01} \\ c_{10} & c_{11} \end{bmatrix} = \boldsymbol{M_c},$$

т.е.

$$c_{00} = b_{00}\cdot a_{00} + b_{01}\cdot a_{10}, \quad c_{01} = b_{00}\cdot a_{01} + b_{01}\cdot a_{11},$$

$$c_{10} = b_{10}\cdot a_{00} + b_{11}\cdot a_{10}, \quad c_{11} = b_{10}\cdot a_{01} + b_{11}\cdot a_{11}.$$

5). Пусть входной вектор есть $|\psi\rangle = \begin{bmatrix} V \\ W \end{bmatrix}$. Тогда при подаче этого вектора на вход первого гейта с матрицей $\boldsymbol{M_a}$ на его выходе будет следующий вектор $|A'\rangle$:

$$\begin{bmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{bmatrix} \times \begin{bmatrix} V \\ W \end{bmatrix} = \begin{bmatrix} a_{00}\cdot V + a_{01}\cdot W \\ a_{10}\cdot V + a_{11}\cdot W \end{bmatrix} = |A'\rangle.$$

6). Далее (для квантовой схемы из двух гейтов) при подаче уже этого вектора $|A'\rangle$ на вход второго гейта с матрицей $\boldsymbol{M_b}$ на его выходе будет вектор $|B'\rangle$, который определяется следующим образом:

$$\begin{bmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \end{bmatrix} \times |A'\rangle = \begin{bmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \end{bmatrix} \times \begin{bmatrix} a_{00} \cdot V + a_{01} \cdot W \\ a_{10} \cdot V + a_{11} \cdot W \end{bmatrix} =$$

$$= \begin{bmatrix} b_{00}\left[a_{00} \cdot V + a_{01} \cdot W\right] + b_{01}\left[a_{10} \cdot V + a_{11} \cdot W\right] \\ b_{10}\left[a_{00} \cdot V + a_{01} \cdot W\right] + b_{11}\left[a_{10} \cdot V + a_{11} \cdot W\right] \end{bmatrix} =$$

$$= \begin{bmatrix} V\left[b_{00}a_{00} \cdot + b_{01} \cdot a_{10}\right] + W\left[b_{00} \cdot a_{01} + b_{01} \cdot a_{11}\right] \\ V\left[b_{10} \cdot a_{00} + b_{11} \cdot a_{10}\right] + W\left[b_{10} \cdot a_{01} + b_{11} \cdot a_{11}\right] \end{bmatrix} = |B'\rangle = |\psi_1'\rangle,$$

который и есть результирующий выходной вектор $|\psi_1'\rangle$ всей квантовой схемы из двух последовательно соединенных гейтов, т.е. $|\psi_1'\rangle = |B'\rangle$.

7). Далее при подаче вектора $|\psi\rangle = \begin{bmatrix} V \\ W \end{bmatrix}$ на вход другой квантовой схемы из одного гейта с матрицей $\boldsymbol{M_c}$ на его выходе будет следующий вектор $|\psi_2'\rangle$:

$$\boldsymbol{M_c} \times |\psi\rangle = \begin{bmatrix} c_{00} & c_{01} \\ c_{10} & c_{11} \end{bmatrix} \times \begin{bmatrix} V \\ W \end{bmatrix} = \begin{bmatrix} c_{00} \cdot V + c_{01} \cdot W \\ c_{10} \cdot V + c_{11} \cdot W \end{bmatrix} =$$

$$= \begin{bmatrix} V\left[b_{00}a_{00} \cdot + b_{01} \cdot a_{10}\right] + W\left[b_{00} \cdot a_{01} + b_{01} \cdot a_{11}\right] \\ V\left[b_{10} \cdot a_{00} + b_{11} \cdot a_{10}\right] + W\left[b_{10} \cdot a_{01} + b_{11} \cdot a_{11}\right] \end{bmatrix} = |\psi_2'\rangle.$$

Сравнение векторов $|\psi_1'\rangle$ и $|\psi_2'\rangle$ показывает, что они идентичны, а значит и сами схемы эквивалентны.

8). И тем самым задача решена■

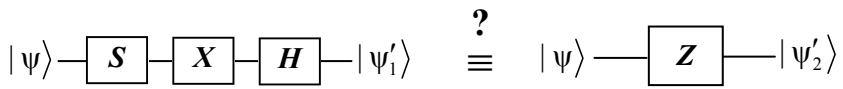
Из ***Примера 5.13*** и главы 2 следует, что результат произведения унитарных операторов есть унитарный оператор, а значит последовательное применение нескольких однокубитовых гейтов эквивалентно некоторому результирующему однокубитовому гейту (квантовому элементу).

Для рассмотрения далее очередных примеров сформулируем следующее важное правило.

> Правило 5.4(**1**)
> *Последовательное применение нескольких **одно**кубитовых гейтов, расположенных в заданном порядке, эквивалентно некоторому результирующему **одно**кубитовому гейту. Унитарная матрица этого результирующего преобразования получается как результат последовательного (в **инверсном** (т.е. обратном) порядке по отношению к порядку следования гейтов) перемножения унитарных матриц этих гейтов* ■

На практике важно уметь упрощать квантовые схемы. Один из возможных способов упрощения квантовой схемы — это замена одной ее части (или даже целиком ее) другой эквивалентной квантовой схемой. Для этого необходимо заменять группу гейтов в квантовой схеме на один или несколько других гейтов, которые реализуют то же самое унитарное преобразование. Следующий пример показывает, как это можно делать.

Пример 5.14**а** (тождества и эквивалентные схемы)
Пусть ***H***, ***X***, ***Y***, ***Z***, ***S***, ***T***, ***I*** — это обозначения матриц гейтов, представленных в табл. 5.1. Запись, например, вида ***HXS*** означает перемножение этих матриц, а сами три гейта последовательно один за другим соединены в обратном порядке, т.е. сначала ***S***, а затем ***X*** и ***H***. Проверить тождество $\boldsymbol{HXS} \equiv \boldsymbol{Z}$ означает, что необходимо выяснить эквивалентность следующих двух квантовых схем:



Знак минус перед обозначением матрицы гейта (например, $-\boldsymbol{Y}$) означает, что все элементы этой матрицы умножаются на (–1).

Последовательность нескольких стоящих подряд одинаковых матриц (гейтов) будем обозначать с помощью показателя степени, например, $\boldsymbol{HHXH}$ как $\boldsymbol{H^2XH}$, или $\boldsymbol{ZZ}$ как $\boldsymbol{Z^2}$, или $\boldsymbol{TTTT}$ как $\boldsymbol{T^4}$ и т.п. ($\boldsymbol{H^2}$ и $\boldsymbol{H^{\otimes 2}}$ — это разные обозначения, см. рис. 5.10, 5.11). Отметим, что порядок в последовательности записи матриц (гейтов) очень существенен. Например, $\boldsymbol{HXH}$ и $\boldsymbol{HHX}$ приводят к разному конечному результату, т.е. к разным выходным векторам, поскольку эти последовательности гейтов имеют разные матрицы результирующих преобразований (это является следствием того, что рассматриваемые матрицы подчиняются некоммутативной алгебре).

Требуется выяснить справедливость следующих тождеств:

для 4-х гейтов

$$\boldsymbol{T^4 \equiv Z},$$

для 3-х гейтов [1, с.228]

$$\boldsymbol{HXH \equiv Z},$$
$$\boldsymbol{HYH \equiv -Y},$$
$$\boldsymbol{HZH \equiv X},$$

для 2-х гейтов [1, с.116,225]

$$\boldsymbol{H^2 \equiv I},$$
$$\boldsymbol{I^2 \equiv I},$$
$$\boldsymbol{S^2 \equiv Z},$$
$$\boldsymbol{T^2 \equiv S}.$$

Решение

1). В условиях задачи не указан явно вычислительный базис. Будем далее предполагать, что входной вектор $|\psi\rangle$, выходные векторы $|\psi_1'\rangle$, $|\psi_2'\rangle$ и необходимые матрицы преобразования гейтов соответствуют одному и тому же вычислительному базису.

2). Применяя *Правило* 5.4(**1**) и учтя, что

$$\boldsymbol{i} = \sqrt{-1}\ ,$$

$$\text{а } \sqrt{i} = \exp\left(i\pi/4\right) = \frac{1+i}{\sqrt{2}}\ ,$$

проверим следующие требуемые тождества:

тождество $\boldsymbol{H^2 \equiv I}$

$$H^2 = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \times \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \times \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} =$$

$$= \frac{1}{2}\begin{bmatrix} 1+1 & 1-1 \\ 1-1 & 1-(-1) \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \equiv I,$$

тождество $\boldsymbol{I^2 \equiv I}$

$$I^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1+0 & 0+0 \\ 0+0 & 0+1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \equiv I,$$

тождество $\boldsymbol{S^2 \equiv Z}$

$$S^2 = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \times \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} = \begin{bmatrix} 1+0 & 0+0 \\ 0+0 & 0+i^2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \equiv Z,$$

тождество $\boldsymbol{T^2 \equiv S}$

$$T^2 = \begin{bmatrix} 1 & 0 \\ 0 & \frac{1}{\sqrt{2}}(1+i) \end{bmatrix} \times \begin{bmatrix} 1 & 0 \\ 0 & \frac{1}{\sqrt{2}}(1+i) \end{bmatrix} =$$

$$= \begin{bmatrix} 1+0 & 0+0 \\ 0+0 & 0+\frac{1}{2}(1+i)^2 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & \frac{1}{2}(1+2i+i^2) \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \equiv S,$$

тождество $\boldsymbol{T^4 \equiv Z}$

поскольку справедливы $\boldsymbol{T^2 \equiv S}$ и $\boldsymbol{S^2 \equiv Z}$, то

$$T^4 = \boldsymbol{T^2}\ T^2 = \boldsymbol{S}\ T^2 = \boldsymbol{S}\ \boldsymbol{S} = S^2 \equiv Z,$$

тождество $\boldsymbol{HXH \equiv Z}$

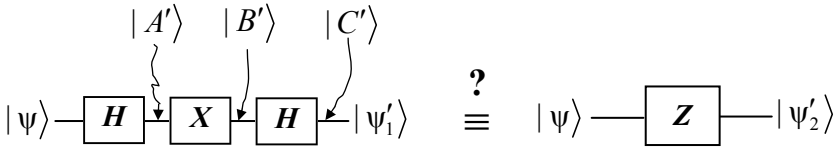
$$XH = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \times \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} =$$

$$= \frac{1}{\sqrt{2}} \begin{bmatrix} 0+1 & 0-1 \\ 1+0 & 1+0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} = \boldsymbol{M},$$

$$\boldsymbol{HXH} = H\boldsymbol{M} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \times \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1+1 & -1+1 \\ 1-1 & -1-1 \end{bmatrix} =$$

$$= \frac{1}{2} \begin{bmatrix} 2 & 0 \\ 0 & -2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \equiv Z,$$

еще один способ проверки (по входу и выходу)



пусть $|\psi\rangle = a|0\rangle + b|1\rangle$, тогда (см. табл. 5.1)

$$|A'\rangle = \frac{a+b}{\sqrt{2}}|0\rangle + \frac{a-b}{\sqrt{2}}|1\rangle = A|0\rangle + B|1\rangle,$$

$$|B'\rangle = B|0\rangle + A|1\rangle = \frac{a-b}{\sqrt{2}}|0\rangle + \frac{a+b}{\sqrt{2}}|1\rangle = E|0\rangle + W|1\rangle,$$

$$|C'\rangle = \frac{E+W}{\sqrt{2}}|0\rangle + \frac{E-W}{\sqrt{2}}|1\rangle =$$

$$= \frac{\frac{a-b}{\sqrt{2}} + \frac{a+b}{\sqrt{2}}}{\sqrt{2}}|0\rangle + \frac{\frac{a-b}{\sqrt{2}} + \frac{a+b}{\sqrt{2}}}{\sqrt{2}}|1\rangle = a|0\rangle - b|1\rangle,$$

$$|\psi'_1\rangle \equiv |C'\rangle = a|0\rangle - b|1\rangle,$$

$$|\psi'_2\rangle = a|0\rangle - b|1\rangle,$$

и сравнивая $|\psi'_1\rangle$ и $|\psi'_2\rangle$, получаем, что $|\psi'_1\rangle = |\psi'_2\rangle$,

тождество $\boldsymbol{HYH} \equiv -\boldsymbol{Y}$

$$YH = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \times \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} =$$

$$= \frac{1}{\sqrt{2}} \begin{bmatrix} 0-i & 0+i \\ i+0 & i-0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} -i & i \\ i & i \end{bmatrix} = \boldsymbol{M},$$

$$H\boldsymbol{YH} = H\boldsymbol{M} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \times \frac{1}{\sqrt{2}} \begin{bmatrix} -i & i \\ i & i \end{bmatrix} = \frac{1}{2} \begin{bmatrix} -i+i & 2i \\ -i-i & i-i \end{bmatrix} =$$

$$= \frac{1}{2} \begin{bmatrix} 0 & 2i \\ -2i & 0 \end{bmatrix} = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix} = -\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \equiv -Y,$$

тождество $\boldsymbol{HZH} \equiv \boldsymbol{X}$

$$ZH = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \times \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} =$$

$$= \frac{1}{\sqrt{2}} \begin{bmatrix} 1+0 & 1+0 \\ 0-1 & 0+1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} = \boldsymbol{M},$$

$$H\boldsymbol{ZH} = H\boldsymbol{M} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \times \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1-1 & 1+1 \\ 1+1 & 1-1 \end{bmatrix} =$$

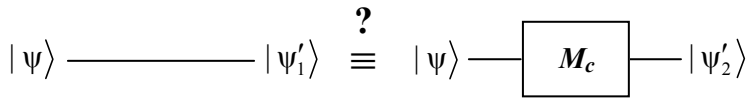
$$= \frac{1}{2} \begin{bmatrix} 0 & 2 \\ 2 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \equiv X,$$

3). И тем самым задача решена■

Перейдем к рассмотрению еще одного несколько необычного примера для однокубитовых схем.

***Пример 5.14*б** (эквивалентность 2-х схем на одном кубите)
Известна квантовая схема из кубита и только одного провода без каких-либо последовательно соединенных однокубитовых гейтов.

Требуется определить один однокубитовый гейт, который эквивалентен этому одному проводу. Другими словами, требуется определить унитарную матрицу $\boldsymbol{M_c}$ результирующего преобразования и установить, что следующие две квантовые схемы эквивалентны:



Решение

1). В условиях задачи не указан явно вычислительный базис. Будем далее предполагать, что входной вектор $|\psi\rangle$, выходные векторы $|\psi_1'\rangle$, $|\psi_2'\rangle$ и необходимые матрицы преобразования гейтов соответствуют одному и тому же вычислительному базису.

2). Преобразование, которое выполняет квантовый провод, состоит в том, что не изменяется состояния кубита, что фактически равносильно (см. *Правило* 5.0**в**) тождественному преобразованию $\boldsymbol{I}$ с соответствующей унитарной матрицей

$$I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

а значит $|\psi\rangle = \boldsymbol{I}|\psi\rangle$ или $|\psi_1'\rangle = |\psi\rangle$.

3). Учтя, что для эквивалентных схем обязательно должно выполняться $|\psi_1'\rangle = |\psi_2'\rangle$ при одинаковом входном векторе $|\psi\rangle$, а значит $|\psi_2'\rangle = |\psi\rangle$, получаем окончательно, что $\boldsymbol{M_c} = \boldsymbol{I}$ или

$$\boldsymbol{M_c} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

4). И тем самым задача решена■

На этом закончим рассмотрение однокубитовых схем и прейдем к алгоритму Дойча и к двухкубитовым квантовым схемам.

5.5. Однокубитовая схема алгоритма Дойча

Рассмотрим пример одного из вариантов [7, с.53] первого квантового алгоритма, предложенного в 1985 г. *Д. Дойчем* (см. раздел 3.1). Можно полагать [7, с.54], что с этого алгоритма и началась фактически область исследования квантовых вычислений.

Алгоритм решает следующую задачу для булевой функции f, отображающей {0, 1} в себя.

Существуют только 4 функции [7, с.53]:

постоянные

$$f_1(0)=f_1(1)=0;$$

$$f_2(0)=f_2(1)=1;$$

биекции (или другое название — *сбалансированные*)

$$f_3(0)=0,\ f_3(1)=1;$$

$$f_4(0)=1,\ f_4(1)=0.$$

Имеется возможность вычислить значение функции только один раз. Случайно выбирается одна из 4 функций, но не известно, какая именно.

Ставится задача определить, что это за отобранная функция, т.е. является ли она биекций (само значение этой функции интереса не представляет, и это значение определять не требуется).

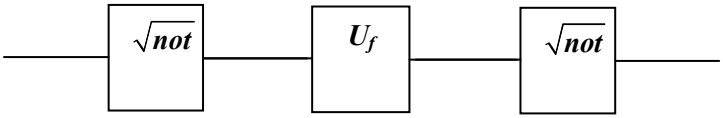
Заметим, что в классическом случае для определения такого глобального свойства функции f требуется вычислить как значение $f(1)$, так и значение $f(0)$, что, как очевидно, потребует дважды вычислять значение этой функции.

С помощью квантовых вычислений при решении этой задачи уже потребуется только **однократное** вычисление значения этой функции (т.е. используется только 1 гейт $\boldsymbol{U}_f$, вычисляющий f).

Квантовая схема, решающая эту задачу (см. [7]), представлена на рис. 5.18**а**, а диаграмма переходов (см. и ср. с [7]) с амплитудами вероятностей показана на рис. 5.18**б**. Отметим (см. рис. 5.18**б**), что для $\boldsymbol{U}_f$ амплитуды вероятности переходов из **1** в **0** , а также из **0** в **1** не показаны, поскольку они равны нулю.

Квантовая схема и диаграмма для алгоритма Дойча

а)



б)

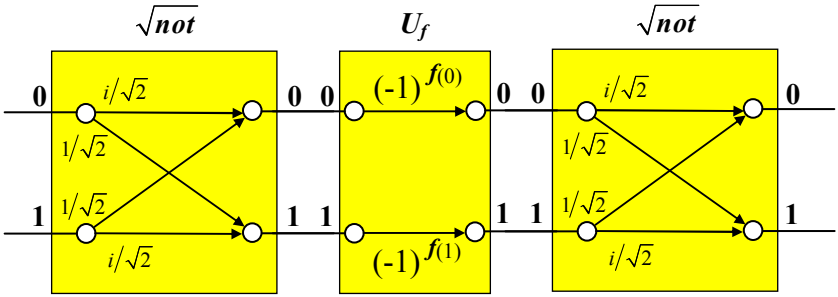


Рис. **5.18**

Квантовый элемент $\boldsymbol{U_f}$ — гейт, вычисляющий, значение функции $f(x)$ только один раз, а точнее (см. [7]) амплитуда вероятности на пути x (на траектории, соответствующей x) умножается на специально подобранный фазовый множитель $\exp\left(\boldsymbol{i}\cdot\pi\cdot f\left(x\right)\right)$, где $\boldsymbol{i}=\sqrt{-1}=\exp\left(i\pi/2\right)$, $\exp\left(i\pi\right)=\cos\left(\pi\right)+i\sin\left(\pi\right)=\cos\left(\pi\right)=-1$, т.е.

на $(-1)^{f(0)}$ (на траектории для 0 в $\boldsymbol{U_f}$);

на $(-1)^{f(1)}$ (на траектории для 1 в $\boldsymbol{U_f}$).

Перейдем к вычислениям.

1). Вычислим вероятность $P_{\mathbf{00}}$ — выхода **0** на входе **0**. Согласно диаграмме (см. рис. 5.18**б**) из **0** в **0** можно прийти только по следующим 2-м траекториям:

траектория 1: { **0** в **0**, **0** в **0**, **0** в **0** };

траектория 2: { **0** в **1**, **1** в **1**, **1** в **0** }.

Применяем *Правило* 5.1 для вычисления $A_{\text{траектории1}}$ и $A_{\text{траектории2}}$, т.е. амплитуд вероятности перехода *квантовой* системы по каждой траектории.

В данном случае эти амплитуды вероятности есть

$$A_{\text{траектории1}}=\left(i/\sqrt{2}\right)\cdot(-1)^{f(0)}\cdot\left(i/\sqrt{2}\right)=-\frac{1}{2}\cdot(-1)^{f(0)};$$

$$A_{\text{траектории2}}=\left(1/\sqrt{2}\right)\cdot(-1)^{f(1)}\cdot\left(1/\sqrt{2}\right)=+\frac{1}{2}\cdot(-1)^{f(1)}.$$

Применяем *Правило* 5.2 для вычисления $A_{\mathbf{00}}$ — амплитуды вероятности перехода системы из **0** в **0**. В данном случае эта амплитуда вероятность есть

$$A_{\mathbf{00}}=A_{\text{траектории1}}+A_{\text{траектории2}}=-\frac{1}{2}\cdot(-1)^{f(0)}+\frac{1}{2}\cdot(-1)^{f(1)}$$

или

$$A_{\mathbf{00}}=\frac{1}{2}\left\{(-1)^{f(1)}-(-1)^{f(0)}\right\}.$$

Применяем *Правило* 5.3 для вычисления вероятности $P_{\mathbf{00}}$ перехода системы из **0** в **0**. В данном случае эта вероятность есть

$$P_{\mathbf{00}}=|A_{\mathbf{00}}|^2=\left|\frac{1}{2}\left\{(-1)^{f(1)}-(-1)^{f(0)}\right\}\right|^2.$$

2). Заметим следующую важную закономерность. Для этого выпишем все возможные значения вероятности $P_{\mathbf{00}}$ при 4 различных возможных вариантах рассматриваемой функции:

для постоянной функции

при $f_1(0)=f_1(1)=0$ значение $P_{\mathbf{00}}=0$;

при $f_2(0)=f_2(1)=1$ значение $P_{\mathbf{00}}=0$;

для НЕ*постоянной функции*

при $f_3(0)=0$, $f_3(1)=1$ значение $P_{\mathbf{00}}=1$;

при $f_4(0)=1$, $f_4(1)=0$ значение $P_{\mathbf{00}}=1$.

3). Вычислим другие 3 оставшиеся вероятности

P_{10} — выхода **0** на входе **1**;
P_{01} — выхода **1** на входе **0**;
P_{11} — выхода **1** на входе **1**.

Согласно той же диаграмме (см. рис. 5.18**б**) из **1** в **0**, или из **0** в **1**, или из **1** в **1** можно также прийти только по 2-м соответствующим траекториям.

Применяем *Правило* 5.1 и *Правило* 5.2, вычислим

$$A_{10} = \frac{i}{2}\left\{(-1)^{f(0)} + (-1)^{f(1)}\right\};$$

$$A_{01} = \frac{i}{2}\left\{(-1)^{f(0)} + (-1)^{f(1)}\right\};$$

$$A_{11} = \frac{1}{2}\left\{(-1)^{f(0)} - (-1)^{f(1)}\right\}.$$

Применяем *Правило* 5.3, вычислим

$$P_{10} = |A_{10}|^2 = \left|\frac{i}{2}\left\{(-1)^{f(0)} + (-1)^{f(1)}\right\}\right|^2;$$

$$P_{01} = |A_{01}|^2 = \left|\frac{i}{2}\left\{(-1)^{f(0)} + (-1)^{f(1)}\right\}\right|^2;$$

$$P_{11} = |A_{11}|^2 = \left|\frac{1}{2}\left\{(-1)^{f(0)} - (-1)^{f(1)}\right\}\right|^2.$$

Заметим следующую аналогичную закономерность:

для постоянной функции

$$P_{10}=1;\ \ P_{01}=1;\ P_{11}=0;$$

для НЕ*постоянной функции*

$$P_{10}=0;\ P_{01}=0;\ P_{11}=1.$$

4). Таким образом, подав на вход схемы (см. рис. 5.18**а**), например **нуль**, т.е. $|0\rangle$, на ее выходе для <u>постоянной</u> функции с вероятностью $P_{01}=1$ будет **единица**, т.е. $|1\rangle$, а для <u>НЕпостоянной</u> функции будет **нуль**, т.е. $|0\rangle$ с вероятностью $P_{00}=1$.

5). И тем самым задача решена■

5.6. Двухкубитовые схемы

> «Современное понимание квантовой механики похоже на представления начинающего шахматиста. Правила известны более 70 лет, и у нас есть несколько остроумных приемов, пригодных в некоторых ситуациях, но мы пока не можем похвастаться мастерством.»
>
> *М. Нильсен* [5]

Двухкубитовые схемы, которые будем далее рассматривать, содержат следующие компоненты:

- два кубита;
- набор однокубитовых гейтов;
- набор двухкубитовых гейтов;
- квантовые провода;
- специальные графические символы на квантовых проводах;
- измеритель (иногда на квантовых схемах не показывают).

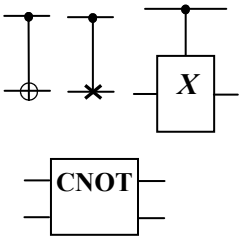
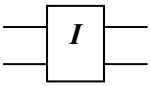
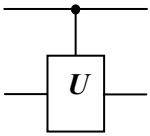
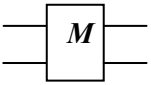
В табл. 5.2 приведены условные обозначения наиболее распространенных квантовых элементов (двухкубитовых гейтов).

На рис. 5.19 приведены дополнительные соглашения, связанные с возможными обозначениями 2-кубитовых гейтов.

Так на рис. 5.19**а**, **г** черная точка (у квантового провода верхнего кубита) заменена на светлую точку (светлый кружок).

На рис. 5.19**а** изображен гейт, реализующий несколько измененную операцию CNOT. Верхняя линия отвечает по-прежнему управляющему кубиту, а нижняя — управляемому кубиту. Светлый кружок и крест, расположенные на этих линиях и соединенные вертикальной прямой, и есть измененная операция CNOT. Светлый кружок стоит на линии управляющего кубита, а крест, изображающий операцию **НЕ** (NOT), расположен на линии управляемого кубита. Измененная операция CNOT заключается в том, что состояния $|0\rangle$ и $|1\rangle$ управляющего кубита поменялись своими функциями. Теперь управляемый кубит подвергается операции **НЕ** в том случае, когда управляющий кубит находится в состоянии $|0\rangle$.

Таблица 5.2. Двухкубитовые гейты (см. [1, с.16,46,229-230; 11])

Наименование гейта	**Возможное условное обозначение**	**Унитарная матрица гейта**
Элемент CNOT (*управляемый* NOT)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \mathbf{0} & \mathbf{1} \\ 0 & 0 & \mathbf{1} & \mathbf{0} \end{bmatrix}$
Элемент *Тождественного преобразования*		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
Элемент *Управляемое* ***U*** (***CU***)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \boldsymbol{w} & \boldsymbol{s} \\ 0 & 0 & \boldsymbol{z} & \boldsymbol{t} \end{bmatrix}$, $U = \begin{bmatrix} w & s \\ z & t \end{bmatrix}$
Элемент *Общего вида*		$\begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{bmatrix}$

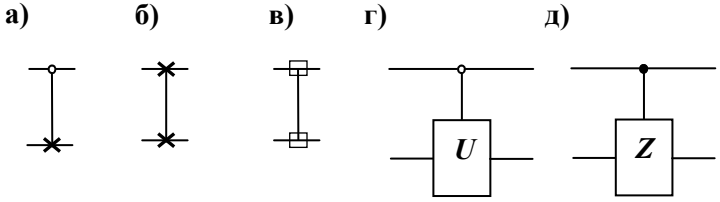


Рис. **5.19**

На рис. 5.19**г** изображен гейт, реализующий несколько измененную операцию *Управляемое* ***U*** из табл. 5.2. Смысл введенных изменений тот же, что и для элемента на рис. 5.19**а** (нижний, т.е. управляемый кубит подвергается операции **НЕ** в том случае, когда управляющий кубит (т.е. верхний) находится в состоянии $|0\rangle$).

Черная точка (для гейтов из табл. 5.2) означает, что управляемый кубит (в данном случае он изображен как нижний кубит) подвергается операции, когда управляющий кубит (в данном случае он изображен как верхний кубит) находится в состоянии $|1\rangle$.

Светлый кружок (для гейта $\widetilde{CNOT}$ на рис. 5.19**а**, для гейта $\widetilde{CU}$ на рис. 5.19**г**) означает, что управляемый кубит (в данном случае он изображен как нижний кубит) подвергается операции **НЕ** (см. рис. 5.19**а**) или операции ***U*** (см. рис. 5.19**г**), когда управляющий кубит (в данном случае он изображен как верхний кубит) находится в состоянии $|0\rangle$.

На рис. 5.19**б** изображен гейт [1, с.45], реализующий операцию обмена состояний двух кубитов.

На рис. 5.19**в** представлено специальное изображение гейта, реализующего операцию *Управляемое* ***Z*** (рис. 5.19**д**).

Гейты [1, с.16] на рис. 5.19**в** и 5.19**д** полностью эквивалентны и обозначают одно и то же.

Управляемое ***Z*** называется управляемым фазовым сдвигом.

В табл. 5.2 (в последней строке) приведен квантовый элемент (2-кубитовый гейт) в самом общем виде со своей унитарной матрицей $\boldsymbol{M}$, где ее элементы есть некоторые комплексные числа.

Ниже приведены следующие унитарные матрицы для гейтов, представленных на рис. 5.19:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$ — *Обмен* [1, с.16];

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \mathbf{1} & \mathbf{0} \\ 0 & 0 & \mathbf{0} & \mathbf{-1} \end{bmatrix}$$ — *Управляемый* $\boldsymbol{Z}$ [1, с.16];

$$\begin{bmatrix} \mathbf{0} & \mathbf{1} & 0 & 0 \\ \mathbf{1} & \mathbf{0} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$ — *Управляемый* $\boldsymbol{X}$ на рис. 5.19**а** (см. раздел 2.5);

$$\begin{bmatrix} \boldsymbol{w} & \boldsymbol{s} & 0 & 0 \\ \boldsymbol{z} & \boldsymbol{t} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$ — *Управляемый* $\boldsymbol{U}$ на рис. 5.19**г**, где $U = \begin{bmatrix} w & s \\ z & t \end{bmatrix}$.

Перейдем к подробному рассмотрению наиболее простых примеров двухкубитовых квантовых схем.

Пример 5.15**а**. Вычисление вектора состояния 2-х кубитов.

Имеется система двух кубитов (т.е. квантовый регистр из 2-х кубитов на квантовой схеме). Каждый ***k***-й кубит (***k***=1, 2) может иметь один из двух векторов состояний

$$|\psi_k\rangle = \{|0\rangle,\ \ |1\rangle\},$$

где $|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}$, $|1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$.

Требуется найти вектор состояния $|\tilde{\psi}\rangle$ системы этих двух кубитов (***n***=2), т.е. квантового регистра (ср. с ***Примером 5.0*****г**).

Решение

1). Пусть $|\psi_1\rangle = |0\rangle$ и $|\psi_2\rangle = |0\rangle$. Нумерацию квантовых систем (кубитов) примем, как в условии примера, и будем полагать, что верхний кубит на схеме имеет номер **1**, а нижний — **2**.

Применяя *Правило* 5.0**б**, получаем следующий вектор $|\tilde{\psi}\rangle$:

$$|\tilde{\psi}\rangle = |00\rangle = |\psi_1\rangle \otimes |\psi_2\rangle =$$

$$= \begin{bmatrix}1\\0\end{bmatrix} \otimes |\psi_2\rangle = \begin{bmatrix}1\cdot|\psi_2\rangle\\0\cdot|\psi_2\rangle\end{bmatrix} = \begin{bmatrix}1\cdot\begin{bmatrix}1\\0\end{bmatrix}\\0\cdot\begin{bmatrix}1\\0\end{bmatrix}\end{bmatrix} = \begin{bmatrix}1\\0\\0\\0\end{bmatrix}.$$

2). Пусть 1-й кубит имеет вектор состояния $|\psi_1\rangle = |0\rangle$.

Пусть 2-й кубит имеет вектор состояния $|\psi_2\rangle = |1\rangle$.

Применяя *Правило* 5.0**б**, получаем следующий вектор $|\tilde{\psi}\rangle$:

$$|\tilde{\psi}\rangle = |01\rangle = |\psi_1\rangle \otimes |\psi_2\rangle =$$

$$= \begin{bmatrix}1\\0\end{bmatrix} \otimes |\psi_2\rangle = \begin{bmatrix}1\cdot|\psi_2\rangle\\0\cdot|\psi_2\rangle\end{bmatrix} = \begin{bmatrix}1\cdot\begin{bmatrix}0\\1\end{bmatrix}\\0\cdot\begin{bmatrix}0\\1\end{bmatrix}\end{bmatrix} = \begin{bmatrix}0\\1\\0\\0\end{bmatrix}.$$

3). Пусть 1-й кубит имеет вектор состояния $|\psi_1\rangle = |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$.

Пусть 2-й кубит имеет вектор состояния $|\psi_2\rangle = |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$.

Применяя *Правило* 5.0**б**, получаем следующий вектор $|\tilde{\psi}\rangle$:

$$|\tilde{\psi}\rangle = |10\rangle = |\psi_1\rangle \otimes |\psi_2\rangle =$$

$$= \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes |\psi_2\rangle = \begin{bmatrix} 0 \cdot |\psi_2\rangle \\ 1 \cdot |\psi_2\rangle \end{bmatrix} = \begin{bmatrix} 0 \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} \\ 1 \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}.$$

4). Пусть 1-й кубит имеет вектор состояния $|\psi_1\rangle = |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$.

Пусть 2-й кубит имеет вектор состояния $|\psi_2\rangle = |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$.

Применяя *Правило* 5.0**б**, получаем следующий вектор $|\tilde{\psi}\rangle$:

$$|\tilde{\psi}\rangle = |11\rangle = |\psi_1\rangle \otimes |\psi_2\rangle =$$

$$= \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes |\psi_2\rangle = \begin{bmatrix} 0 \cdot |\psi_2\rangle \\ 1 \cdot |\psi_2\rangle \end{bmatrix} = \begin{bmatrix} 0 \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix} \\ 1 \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}.$$

5). На этом закончим рассмотрение данного примера ■

***Пример 5.15*б**. Вычисление вектора состояния 2-х кубитов.

Имеется система двух кубитов (т.е. квантовый регистр из 2-х кубитов на квантовой схеме). Каждый ***k***-й кубит (***k***=1, 2) может иметь один из двух векторов состояний

$$|\psi_k\rangle = \left\{ |\tilde{0}\rangle,\ \ |\tilde{1}\rangle \right\},$$

где $|\tilde{0}\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}$, $|\tilde{1}\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}$.

Требуется найти вектор состояния $|\tilde{\psi}\rangle$ системы этих двух кубитов (***n***=2), т.е. квантового регистра (ср. с ***Примером 5.0*г**).

Решение

1). Пусть $|\psi_1\rangle = |\tilde{0}\rangle$ и $|\psi_2\rangle = |\tilde{0}\rangle$. Нумерацию квантовых систем (кубитов) примем, как в условии примера, и будем полагать, что верхний кубит на схеме имеет номер **1**, а нижний — **2**.

Применяя *Правило* 5.0**б**, получаем следующий вектор $|\tilde{\psi}\rangle$:

$$|\tilde{\psi}\rangle = |\tilde{0}\tilde{0}\rangle = |\psi_1\rangle \otimes |\psi_2\rangle =$$

$$= \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix} \otimes |\psi_2\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\cdot|\psi_2\rangle\\1\cdot|\psi_2\rangle\end{bmatrix} = \left(\frac{1}{\sqrt{2}}\right)^2 \begin{bmatrix}1\cdot\begin{bmatrix}1\\1\end{bmatrix}\\1\cdot\begin{bmatrix}1\\1\end{bmatrix}\end{bmatrix} = \frac{1}{2}\begin{bmatrix}1\\1\\1\\1\end{bmatrix} = \begin{bmatrix}0.5\\0.5\\0.5\\0.5\end{bmatrix}.$$

2). Пусть 1-й кубит имеет вектор состояния $|\psi_1\rangle = |\tilde{0}\rangle$.

Пусть 2-й кубит имеет вектор состояния $|\psi_2\rangle = |\tilde{1}\rangle$.

Применяя *Правило* 5.0**б**, получаем следующий вектор $|\tilde{\psi}\rangle$:

$$|\tilde{\psi}\rangle = |\tilde{0}\tilde{1}\rangle = |\psi_1\rangle \otimes |\psi_2\rangle =$$

$$= \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix} \otimes |\psi_2\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\cdot|\psi_2\rangle\\1\cdot|\psi_2\rangle\end{bmatrix} = \left(\frac{1}{\sqrt{2}}\right)^2 \begin{bmatrix}1\cdot\begin{bmatrix}1\\-1\end{bmatrix}\\1\cdot\begin{bmatrix}1\\-1\end{bmatrix}\end{bmatrix} = \frac{1}{2}\begin{bmatrix}1\\-1\\1\\-1\end{bmatrix}.$$

3). Пусть 1-й кубит имеет вектор состояния $|\psi_1\rangle = |\tilde{1}\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}$.

Пусть 2-й кубит имеет вектор состояния $|\psi_2\rangle = |\tilde{0}\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}$.

Применяя *Правило* 5.0**б**, получаем следующий вектор $|\tilde{\psi}\rangle$:

$$|\tilde{\psi}\rangle = |\tilde{1}\tilde{0}\rangle = |\psi_1\rangle \otimes |\psi_2\rangle =$$

$$= \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix} \otimes |\psi_2\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\cdot|\psi_2\rangle\\-1\cdot|\psi_2\rangle\end{bmatrix} = \left(\frac{1}{\sqrt{2}}\right)^2 \begin{bmatrix}1\cdot\begin{bmatrix}1\\1\end{bmatrix}\\-1\cdot\begin{bmatrix}1\\1\end{bmatrix}\end{bmatrix} = \frac{1}{2}\begin{bmatrix}1\\1\\-1\\-1\end{bmatrix}.$$

4). Пусть 1-й кубит имеет вектор состояния $|\psi_1\rangle = |\tilde{1}\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}$.

Пусть 2-й кубит имеет вектор состояния $|\psi_2\rangle = |\tilde{1}\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}$.

Применяя *Правило* 5.0**б**, получаем следующий вектор $|\tilde{\psi}\rangle$:

$$|\tilde{\psi}\rangle = |\tilde{1}\tilde{1}\rangle = |\psi_1\rangle \otimes |\psi_2\rangle =$$

$$= \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix} \otimes |\psi_2\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\cdot|\psi_2\rangle\\-1\cdot|\psi_2\rangle\end{bmatrix} = \left(\frac{1}{\sqrt{2}}\right)^2 \begin{bmatrix}1\cdot\begin{bmatrix}1\\-1\end{bmatrix}\\-1\cdot\begin{bmatrix}1\\-1\end{bmatrix}\end{bmatrix} = \frac{1}{2}\begin{bmatrix}1\\-1\\-1\\1\end{bmatrix}.$$

5). На этом закончим рассмотрение данного примера ■

***Пример 5.15*в** (задача синтеза квантовой схемы)

Известен вычислительный базис, т.е.

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix},$$

$$|00\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, |01\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, |10\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}, |11\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}.$$

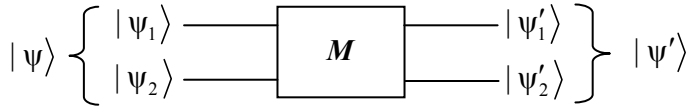
Есть квантовая схема из 2-х кубитов (***k***-й кубит (***k***=1, 2) имеет состояние $|\psi_k\rangle$) и 1-го гейта с матрицей преобразования

$$\boldsymbol{M} = \begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{bmatrix},$$

причем a_{ij} — это комплексные числа (***i***=0, 1, 2, 3; ***j***=0, 1, 2, 3). Известно, какой выходной вектор $|\psi'\rangle$ должен быть на выходе, если на вход этой квантовой схемы подан соответствующий входной вектор $|\psi\rangle$. Входные и выходные векторы связаны с помощью матрицы ***M*** так: $\boldsymbol{M}|\psi\rangle = |\psi'\rangle$ — или более подробно следующим образом:

$$\boldsymbol{M}|00\rangle = |00\rangle, \quad \boldsymbol{M}|01\rangle = |01\rangle, \quad \boldsymbol{M}|10\rangle = |11\rangle, \quad \boldsymbol{M}|11\rangle = |10\rangle.$$

Требуется определить a_{ij}, т.е. синтезировать <u>унитарную</u> матрицу ***M*** квантового элемента (гейта):



т.е. достаточно найти хотя бы одно решение (т.е. одну матрицу ***M***).

Решение

1). В условиях задачи указан явно вычислительный базис. Будем далее предполагать, что входной вектор $|\psi\rangle$ и $|\psi_1\rangle$, $|\psi_2\rangle$,

выходной вектор $|\psi'\rangle$ и $|\psi'_1\rangle$, $|\psi'_2\rangle$ и матрица преобразования $\boldsymbol{M}$ соответствуют одному и тому же вычислительному базису.

2). Так как по условию задачи $\boldsymbol{M}|00\rangle = |00\rangle$, то это же самое можно записать по-другому, например следующим образом:

для ($\boldsymbol{i}$=0) самой верхней строки

$$\boldsymbol{M}|\tilde{0}\tilde{0}\rangle = \begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{bmatrix} \times \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \Rightarrow$$

$$\Rightarrow a_{00} = 1,$$

для ($\boldsymbol{i}$=1) следующей строки

$$\boldsymbol{M}|00\rangle = |00\rangle \Rightarrow a_{10} = 0,$$

для ($\boldsymbol{i}$=2) следующей строки

$$\boldsymbol{M}|00\rangle = |00\rangle \Rightarrow a_{20} = 0,$$

для ($\boldsymbol{i}$=3) самой нижней строки

$$\boldsymbol{M}|00\rangle = |00\rangle \Rightarrow a_{30} = 0.$$

Таким образом, получаем, что $a_{00} = 1$, $a_{10} = a_{20} = a_{30} = 0$.

Аналогичный результат (для всех строк) можно получить (как и для вектора $|00\rangle$), используя три других вектора

$$|01\rangle,$$
$$|10\rangle,$$
$$|11\rangle.$$

Далее для вектора $|01\rangle$ получаем, что $\boldsymbol{M}|01\rangle = |01\rangle \Rightarrow$

$$\Rightarrow a_{11} = 1,\ \ a_{01} = a_{21} = a_{31} = 0.$$

Далее для вектора $|10\rangle$ получаем, что $\boldsymbol{M}|10\rangle = |11\rangle \Rightarrow$

$$\Rightarrow a_{32} = 1,\ \ a_{02} = a_{12} = a_{22} = 0.$$

Далее для вектора $|11\rangle$ получаем, что $\boldsymbol{M}|11\rangle = |10\rangle \Rightarrow$

$$a_{23} = 1,\ \ a_{03} = a_{13} = a_{33} = 0.$$

Т.е. в итоге получили, что

$$a_{00} = a_{11} = a_{23} = a_{32} = 1,$$

$$a_{10} = a_{20} = a_{30} = a_{01} = a_{21} = a_{31} = a_{02} = a_{12} = a_{22} = a_{03} = a_{13} = a_{33} = 0.$$

Таким образом, найдена следующая матрица:

$$\boldsymbol{M} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix},$$

которая в точности совпадает с матрицей для квантового элемента CNOT.

3). Проверим, что синтезированная матрица ***M*** унитарна:

$$M^{\dagger}M = \left(\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}\right)^{\dagger} \times \left(\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}\right) =$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \times \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} =$$

$$= \begin{bmatrix} 1+0 & 0 & 0 & 0 \\ 0 & 1+0 & 0 & 0 \\ 0 & 0 & 1+0 & 0 \\ 0 & 0 & 0 & 1+0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \equiv I,$$

т.е. свойство унитарности матрицы ***M*** выполняется.

ОТМЕТИМ. Матрицу ***I*** иногда обозначают и как **1**, т.е. она может быть представлена следующим образом:

$$\mathbf{1} \equiv I \equiv \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

4). Проверим, что найденная (синтезированная) матрица $\boldsymbol{M}$ действительно удовлетворяет условиям задачи:

$$M \times |\psi\rangle = |\psi'\rangle$$

или

$$\boldsymbol{M}|00\rangle = |00\rangle \Rightarrow \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \times \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1+0 \\ 0+0 \\ 0+0 \\ 0+0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = |00\rangle ,$$

$$\boldsymbol{M}|01\rangle = |01\rangle \Rightarrow \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \times \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0+0 \\ 1+0 \\ 0+0 \\ 0+0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = |01\rangle ,$$

$$\boldsymbol{M}|10\rangle = |11\rangle \Rightarrow \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \times \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0+0 \\ 0+0 \\ 0+0 \\ 1+0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = |11\rangle ,$$

$$\boldsymbol{M}|11\rangle = |10\rangle \Rightarrow \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \times \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0+0 \\ 0+0 \\ 0+1 \\ 0+0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = |10\rangle ,$$

т.е. все условия задачи для найденной матрицы $\boldsymbol{M}$ выполнены.

5). И тем самым задача решена■

***Пример 5.15*г** (задача синтеза квантовой схемы)

Известен вычислительный базис, т.е.

$$|\tilde{0}\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix},\ |\tilde{1}\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix},$$

$$|\tilde{0}\tilde{0}\rangle = \frac{1}{2}\begin{bmatrix}1\\1\\1\\1\end{bmatrix},\ |\tilde{0}\tilde{1}\rangle = \frac{1}{2}\begin{bmatrix}1\\-1\\1\\-1\end{bmatrix},\ |\tilde{1}\tilde{0}\rangle = \frac{1}{2}\begin{bmatrix}1\\1\\-1\\-1\end{bmatrix},\ |\tilde{1}\tilde{1}\rangle = \frac{1}{2}\begin{bmatrix}1\\-1\\-1\\1\end{bmatrix}.$$

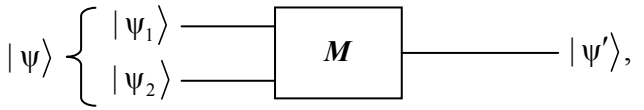
Есть квантовая схема из 2-х кубитов (***k***-й кубит имеет состояние $|\psi_k\rangle$) и 1-го квантового элемента с матрицей преобразования

$$\boldsymbol{M} = \begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{bmatrix},$$

причем a_{ij} — это комплексные числа (***i***=0,1,2,3; ***j***=0,1,2,3). Известно, какой выходной вектор $|\psi'\rangle$ должен быть на выходе, если на вход этой квантовой схемы подан соответствующий входной вектор $|\psi\rangle$. Входные и выходные векторы связаны с помощью матрицы ***M*** так: $\boldsymbol{M}|\psi\rangle = |\psi'\rangle$ — или более подробно следующим образом:

$$\boldsymbol{M}|\tilde{0}\tilde{0}\rangle = |\tilde{0}\tilde{0}\rangle,\ \boldsymbol{M}|\tilde{0}\tilde{1}\rangle = |\tilde{0}\tilde{1}\rangle,\ \boldsymbol{M}|\tilde{1}\tilde{0}\rangle = |\tilde{1}\tilde{1}\rangle,\ \boldsymbol{M}|\tilde{1}\tilde{1}\rangle = |\tilde{1}\tilde{0}\rangle.$$

Требуется определить a_{ij}, т.е. синтезировать <u>унитарную</u> матрицу ***M*** квантового элемента:



т.е. достаточно найти хотя бы одно решение (т.е. одну матрицу ***M***).

Решение

1). В условиях задачи указан явно вычислительный базис. Будем далее предполагать, что входные векторы $|\psi\rangle$ и $|\psi_1\rangle$, $|\psi_2\rangle$, выходной вектор $|\psi'\rangle$ и матрица преобразования $\boldsymbol{M}$ соответствуют одному и тому же вычислительному базису.

2). Так как по условию задачи $\boldsymbol{M}|\tilde{0}\tilde{0}\rangle = |\tilde{0}\tilde{0}\rangle$, то это же самое записать по-другому, например следующим образом:

для ($\boldsymbol{i}$=0) самой верхней строки

$$\boldsymbol{M}|\tilde{0}\tilde{0}\rangle = \begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{bmatrix} \times \frac{1}{2}\begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} \Rightarrow$$

$$\Rightarrow a_{00}+a_{01}+a_{02}+a_{03}=1,$$

для ($\boldsymbol{i}$=1) следующей строки

$$\boldsymbol{M}|\tilde{0}\tilde{0}\rangle = |\tilde{0}\tilde{0}\rangle \Rightarrow a_{10}+a_{11}+a_{12}+a_{13}=1,$$

для ($\boldsymbol{i}$=2) следующей строки

$$\boldsymbol{M}|\tilde{0}\tilde{0}\rangle = |\tilde{0}\tilde{0}\rangle \Rightarrow a_{20}+a_{21}+a_{22}+a_{23}=1,$$

для ($\boldsymbol{i}$=3) самой нижней строки

$$\boldsymbol{M}|\tilde{0}\tilde{0}\rangle = |\tilde{0}\tilde{0}\rangle \Rightarrow a_{30}+a_{31}+a_{32}+a_{33}=1.$$

Аналогичный результат (для всех строк) можно получить (как и для вектора $|\tilde{0}\tilde{0}\rangle$), используя три других вектора:

$$|\tilde{0}\tilde{1}\rangle,\ |\tilde{1}\tilde{0}\rangle,\ |\tilde{1}\tilde{1}\rangle.$$

Таким образом (для (i=0) самой верхней строки) получаем, что

$$\boldsymbol{M}|\tilde{0}\tilde{0}\rangle = |\tilde{0}\tilde{0}\rangle \Rightarrow\ a_{00}+a_{01}+a_{02}+a_{03}=1,$$

$$\boldsymbol{M}|\tilde{0}\tilde{1}\rangle = |\tilde{0}\tilde{1}\rangle \Rightarrow\ a_{00}-a_{01}+a_{02}-a_{03}=1,$$

$$\boldsymbol{M}|\tilde{1}\tilde{0}\rangle = |\tilde{1}\tilde{1}\rangle \Rightarrow\ a_{00}+a_{01}-a_{02}-a_{03}=1,$$

$$\boldsymbol{M}|\tilde{1}\tilde{1}\rangle = |\tilde{1}\tilde{0}\rangle \Rightarrow\ a_{00}-a_{01}-a_{02}+a_{03}=1.$$

Решая систему уравнений

$$\begin{cases} a_{00}+a_{01}+a_{02}+a_{03}=1 \\ a_{00}-a_{01}+a_{02}-a_{03}=1 \\ a_{00}+a_{01}-a_{02}-a_{03}=1 \\ a_{00}-a_{01}-a_{02}+a_{03}=1 \end{cases},$$

можно получить, что $a_{00}=1,\ a_{01}=a_{02}=a_{03}=0$.

Аналогично можно получить и затем решить еще 3 другие похожие системы уравнений:

$$\begin{cases} a_{10}+a_{11}+a_{12}+a_{13}=1 \\ a_{10}-a_{11}+a_{12}-a_{13}=-1 \\ a_{10}+a_{11}-a_{12}-a_{13}=-1 \\ a_{10}-a_{11}-a_{12}+a_{13}=1 \end{cases},$$

$$\begin{cases} a_{20}+a_{21}+a_{22}+a_{23}=1 \\ a_{20}-a_{21}+a_{22}-a_{23}=1 \\ a_{20}+a_{21}-a_{22}-a_{23}=-1 \\ a_{20}-a_{21}-a_{22}+a_{23}=-1 \end{cases},$$

$$\begin{cases} a_{30}+a_{31}+a_{32}+a_{33}=1 \\ a_{30}-a_{31}+a_{32}-a_{33}=-1 \\ a_{30}+a_{31}-a_{32}-a_{33}=1 \\ a_{30}-a_{31}-a_{32}+a_{33}=-1 \end{cases},$$

т.е. в итоге можно получить, что

$$a_{13}=a_{22}=a_{31}=1,\ a_{10}=a_{11}=a_{12}=a_{20}=a_{21}=a_{23}=a_{30}=a_{32}=a_{33}=0.$$

Таким образом, найдена матрица

$$\boldsymbol{M} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

3). Проверим, что синтезированная матрица $\boldsymbol{M}$ унитарна:

$$M^{\dagger}M = \left(\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \right)^{\dagger} \times \left(\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \right) =$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \times \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} =$$

$$= \begin{bmatrix} 1+0 & 0 & 0 & 0 \\ 0 & 1+0 & 0 & 0 \\ 0 & 0 & 1+0 & 0 \\ 0 & 0 & 0 & 1+0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \equiv I,$$

т.е. свойство унитарности матрицы $\boldsymbol{M}$ выполняется.

4). Проверим, что найденная (синтезированная) матрица $\boldsymbol{M}$ действительно удовлетворяет условиям задачи:

$$M \times |\psi\rangle = |\psi'\rangle$$

или

$$\boldsymbol{M}|\tilde{0}\tilde{0}\rangle = |\tilde{0}\tilde{0}\rangle \Rightarrow \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \times \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1+0 \\ 1+0 \\ 1+0 \\ 1+0 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = |\tilde{0}\tilde{0}\rangle,$$

$$\boldsymbol{M}|\tilde{0}\tilde{1}\rangle = |\tilde{0}\tilde{1}\rangle \Rightarrow \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \times \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1+0 \\ 0-1 \\ 1+0 \\ 0-1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \end{bmatrix} = |\tilde{0}\tilde{1}\rangle,$$

$$\boldsymbol{M}|\tilde{1}\tilde{0}\rangle = |\tilde{1}\tilde{1}\rangle \Rightarrow \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \times \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ -1 \\ -1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1+0 \\ 0-1 \\ 0-1 \\ 1+0 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ -1 \\ 1 \end{bmatrix} = |\tilde{1}\tilde{1}\rangle,$$

$$\boldsymbol{M}|\tilde{1}\tilde{1}\rangle = |\tilde{1}\tilde{0}\rangle \Rightarrow \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \times \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ -1 \\ 1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1+0 \\ 1+0 \\ 0-1 \\ 0-1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ -1 \\ -1 \end{bmatrix} = |\tilde{1}\tilde{0}\rangle,$$

т.е. все условия задачи для найденной матрицы $\boldsymbol{M}$ выполнены.

5). И тем самым задача решена■

Кратко обсудим разобранные выше примеры. В ***Примерах 5.15*а**, **б** вычисляются векторы состояния $|\tilde{\psi}\rangle$ системы двух кубитов (***n***=2), т.е. квантового регистра (по аналогии с рассмотренным ранее ***Примером 5.0*г**). Полученные векторы являются базисными векторами. Далее эти полученные векторы используются в ***Примерах 5.15*в**, **г** уже для представления различных вычислительных базисов.

В ***Примере 5.15*в** найдена унитарная матрица, соответствующая унитарному преобразованию для квантового элемента — гейта CNOT. Действительно, сравнивая матрицу из табл. 5.2 (для гейта CNOT) и матрицу

$$\boldsymbol{M} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix},$$

полученную (в ***Примере 5.15*в**) в результате синтеза, можно заметить, что эти матрицы идентичны.

Важно отметить, что унитарные матрицы, полученные (для разных базисных векторов и соответственно для разных вычислительных базисов) в ***Примерах 5.15*в**, **г**, не совпадают.

Действительно, сравнивая матрицу из ***Примера 5.15*в**

$$\boldsymbol{M} = \begin{bmatrix} \mathbf{1} & 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1} \\ 0 & 0 & \mathbf{1} & 0 \end{bmatrix}$$

и матрицу из ***Примера 5.15*г**

$$\boldsymbol{M} = \begin{bmatrix} \mathbf{1} & 0 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1} \\ 0 & 0 & \mathbf{1} & 0 \\ 0 & \mathbf{1} & 0 & 0 \end{bmatrix},$$

можно заметить, что эти матрицы **не** идентичны.

Теперь вернемся к ***Примеру 5.0д*** и рассмотрим вычисление унитарной матрицы для квантовых схем из 2-х кубитов (рис. 5.20).

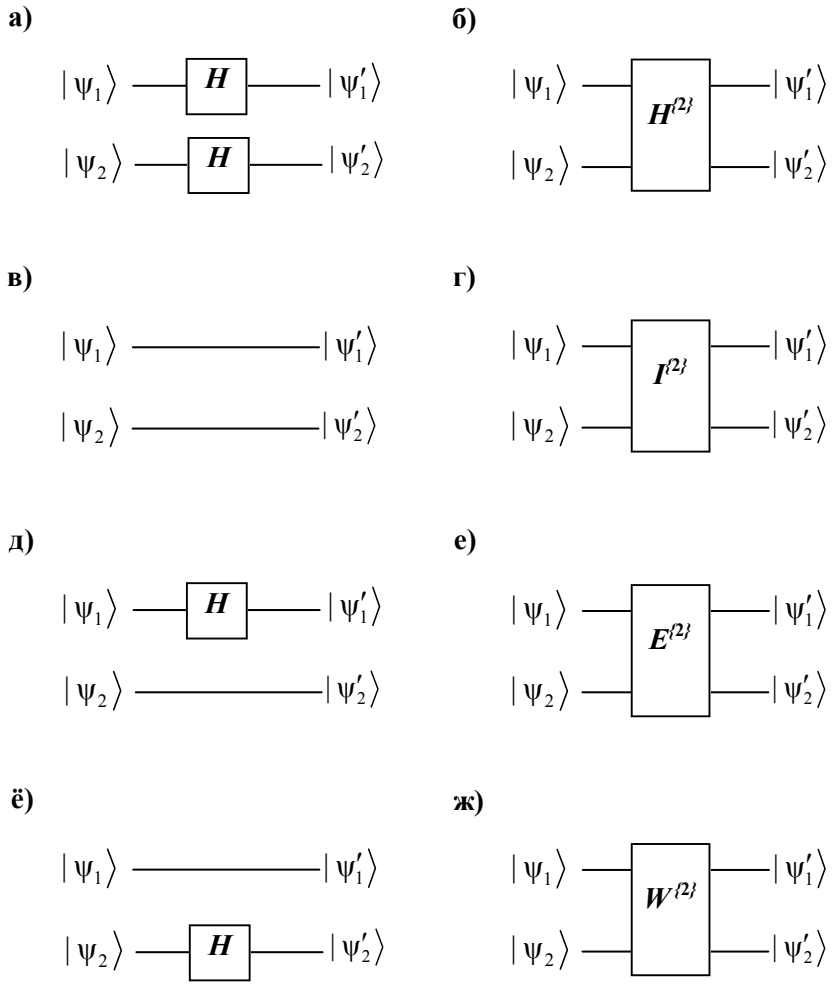


Рис. **5.20**

***Пример 5.16*г** (задача на вычисление унитарной матрицы)

Известны следующие унитарные матрицы $\boldsymbol{H}$ и $\boldsymbol{I}$:

$$\boldsymbol{H}=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix},\quad \boldsymbol{I}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}.$$

Имеется система двух кубитов. Над кубитом выполняется преобразование, характеризующееся известной унитарной матрицей (т.е. известен гейт и его унитарная матрица).

Требуется найти результирующую унитарную матрицу $\boldsymbol{H}^{\{2\}}$, $\boldsymbol{I}^{\{2\}}$, $\boldsymbol{E}^{\{2\}}$, $\boldsymbol{W}^{\{2\}}$ для каждой системы на рис. 5.20 этих двух кубитов ($\boldsymbol{n}$=2).

Решение

1). В условиях задачи не указан явно вычислительный базис. Будем далее предполагать, что входные векторы $|\psi_1\rangle$, $|\psi_2\rangle$, выходные векторы $|\psi_1'\rangle$, $|\psi_2'\rangle$ и матрицы преобразования $\boldsymbol{H}$ и $\boldsymbol{I}$ соответствуют одному и тому же вычислительному базису.

2). Нумерацию квантовых систем (кубитов) примем, как показано на рис. 5.20, т.е. верхний кубит имеет номер **1**, а нижний — **2**. Применяя ранее введенное *Правило* 5.0**в**, получим следующие унитарные матрицы:

для схемы на рис. 5.20**а**

$$\boldsymbol{H}^{\{2\}}=H\otimes H=\frac{1}{\sqrt{2}}\begin{bmatrix}1\cdot H & 1\cdot H\\ 1\cdot H & (-1)\cdot H\end{bmatrix}=\frac{1}{2}\left[\begin{array}{cc:cc}1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ \hdashline 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\end{array}\right],$$

для схемы на рис. 5.20**в** (см. ***Пример 5.14*б**)

$$\boldsymbol{I}^{\{2\}}=I\otimes I=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\otimes I=\begin{bmatrix}1\cdot I & 0\cdot I\\ 0\cdot I & 1\cdot I\end{bmatrix}=\left[\begin{array}{cc:cc}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ \hdashline 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\end{array}\right],$$

для схемы на рис. 5.20**д** (см. ***Пример 5.14б***)

$$\boldsymbol{E}^{\{2\}} = H \otimes I = \frac{1}{\sqrt{2}}\begin{bmatrix} 1\cdot I & 1\cdot I \\ 1\cdot I & (-1)\cdot I \end{bmatrix} = \frac{1}{\sqrt{2}}\left[\begin{array}{cc:cc} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ \hdashline 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{array}\right],$$

для схемы на рис. 5.20**ё** (см. ***Пример 5.14б***)

$$\boldsymbol{W}^{\{2\}} = I \otimes H = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes H = \begin{bmatrix} 1\cdot H & 0\cdot H \\ 0\cdot H & 1\cdot H \end{bmatrix} = \frac{1}{\sqrt{2}}\left[\begin{array}{cc:cc} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ \hdashline 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{array}\right].$$

3). Таким образом, установлено следующее, что:

схема на рис. 5.20**а** эквивалентна схеме на рис. 5.20**б**;

схема на рис. 5.20**в** эквивалентна схеме на рис. 5.20**г**;

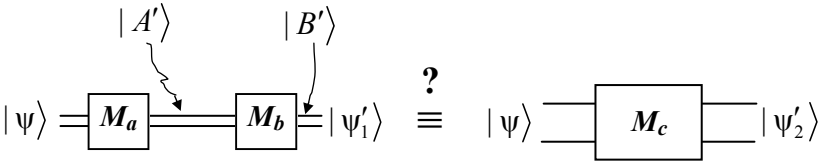
схема на рис. 5.20**д** эквивалентна схеме на рис. 5.20**е**;

схема на рис. 5.20**ё** эквивалентна схеме на рис. 5.20**ж**.

4). И тем самым задача решена■

Пример 5.17 (эквивалентные схемы на двух кубитах)
Известна квантовая схема из 2-х последовательно соединенных двухкубитовых гейтов с соответствующими унитарными матрицами $\boldsymbol{M_a}$ и $\boldsymbol{M_b}$.

Требуется определить один двухкубитовый гейт, который эквивалентен этим двум последовательно соединенным двухкубитовым гейтам. Другими словами, требуется определить унитарную матрицу $\boldsymbol{M_c}$ результирующего преобразования и установить, что следующие две квантовые схемы эквивалентны:



Решение

1). В условиях задачи не указан явно вычислительный базис. Будем далее предполагать, что входной вектор $|\psi\rangle$, выходные векторы $|\psi_1'\rangle$, $|\psi_2'\rangle$ и матрицы преобразования $\boldsymbol{M_a}$, $\boldsymbol{M_b}$ и $\boldsymbol{M_c}$ соответствуют одному и тому же вычислительному базису.

2). Эквивалентность двух схем понимается в том смысле, что при подаче одного и того же входного вектора $|\psi\rangle$ на вход каждой из этих схем на их выходе получается один и тот же выходной вектор, т.е. $|\psi_1'\rangle = |\psi_2'\rangle$, при этом матрица $\boldsymbol{M_c}$ результирующего преобразования является (как и матрицы $\boldsymbol{M_a}$ и $\boldsymbol{M_b}$) также унитарной. Специально еще раз отметим, что результирующее преобразование с матрицей $\boldsymbol{M_c}$ зависит, вообще говоря, от порядка, в котором выполняются операции с матрицами $\boldsymbol{M_a}$ и $\boldsymbol{M_b}$ (т.е. от порядка, в котором выполняются гейты).

3). Так как из главы 2 следует, что результат произведения унитарных операторов есть унитарный оператор, значит, результат умножения двух унитарных матриц $\boldsymbol{M_b} \times \boldsymbol{M_a} = \boldsymbol{M_c}$ есть унитарная матрица, т.е. свойство унитарности матрицы $\boldsymbol{M_c}$ выполняется.

4). Пусть

$$\boldsymbol{M_a} = \begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{bmatrix}, \quad \boldsymbol{M_b} = \begin{bmatrix} b_{00} & b_{01} & b_{02} & b_{03} \\ b_{10} & b_{11} & b_{12} & b_{13} \\ b_{20} & b_{21} & b_{22} & b_{23} \\ b_{30} & b_{31} & b_{32} & b_{33} \end{bmatrix},$$

тогда результирующая матрица $\boldsymbol{M_c}=\boldsymbol{M_b}\times\boldsymbol{M_a}$ (именно в таком порядке — $\boldsymbol{M_b}$ на $\boldsymbol{M_a}$, хотя сами гейты в квантовой схеме идут в обратном порядке — сначала преобразование с матрицей $\boldsymbol{M_a}$, а затем преобразование с матрицей $\boldsymbol{M_b}$) есть

$$\begin{bmatrix} b_{00} & b_{01} & b_{02} & b_{03} \\ b_{10} & b_{11} & b_{12} & b_{13} \\ b_{20} & b_{21} & b_{22} & b_{23} \\ b_{30} & b_{31} & b_{32} & b_{33} \end{bmatrix} \times \begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{bmatrix} =$$

$$= \begin{bmatrix} c_{00} & c_{01} & c_{02} & c_{03} \\ c_{10} & c_{11} & c_{12} & c_{13} \\ c_{20} & c_{21} & c_{22} & c_{23} \\ c_{30} & c_{31} & c_{32} & c_{33} \end{bmatrix} = \boldsymbol{M_c},$$

где

$$c_{00} = b_{00}a_{00} + b_{01}a_{10} + b_{02}a_{20} + b_{03}a_{30},$$

$$c_{01} = b_{00}a_{01} + b_{01}a_{11} + b_{02}a_{21} + b_{03}a_{31},$$

$$c_{02} = b_{00}a_{02} + b_{01}a_{12} + b_{02}a_{22} + b_{03}a_{32}$$

$$c_{03} = b_{00}a_{03} + b_{01}a_{13} + b_{02}a_{23} + b_{03}a_{33},$$

……………………………………………..

$$c_{ij} = b_{i0}a_{0j} + b_{i1}a_{1j} + b_{i2}a_{2j} + b_{i3}a_{3j},$$

……………………………………………..

$$c_{33} = b_{30}a_{03} + b_{31}a_{13} + b_{32}a_{23} + b_{33}a_{33}.$$

5). Пусть входной вектор есть $|\psi\rangle = \begin{bmatrix} V \\ W \\ Q \\ K \end{bmatrix}$. Тогда при подаче этого вектора на вход первого гейта с матрицей $\boldsymbol{M_a}$ на его выходе будет следующий вектор $|A'\rangle$:

$$\begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{bmatrix} \times \begin{bmatrix} V \\ W \\ Q \\ K \end{bmatrix} = \begin{bmatrix} a_{00}V + a_{01}W + a_{02}Q + a_{03}K \\ a_{10}V + a_{11}W + a_{12}Q + a_{13}K \\ a_{20}V + a_{21}W + a_{22}Q + a_{23}K \\ a_{30}V + a_{31}W + a_{32}Q + a_{33}K \end{bmatrix} = |A'\rangle .$$

6). Далее (для квантовой схемы из двух гейтов) при подаче уже этого вектора $|A'\rangle$ на вход второго гейта с матрицей $\boldsymbol{M_b}$ на его выходе будет вектор $|B'\rangle$, который определяется следующим образом:

$$\begin{bmatrix} b_{00} & b_{01} & b_{02} & b_{03} \\ b_{10} & b_{11} & b_{12} & b_{13} \\ b_{20} & b_{21} & b_{22} & b_{23} \\ b_{30} & b_{31} & b_{32} & b_{33} \end{bmatrix} \times |A'\rangle =$$

$$= \begin{bmatrix} b_{00} & b_{01} & b_{02} & b_{03} \\ b_{10} & b_{11} & b_{12} & b_{13} \\ b_{20} & b_{21} & b_{22} & b_{23} \\ b_{30} & b_{31} & b_{32} & b_{33} \end{bmatrix} \times \begin{bmatrix} a_{00}V + a_{01}W + a_{02}Q + a_{03}K \\ a_{10}V + a_{11}W + a_{12}Q + a_{13}K \\ a_{20}V + a_{21}W + a_{22}Q + a_{23}K \\ a_{30}V + a_{31}W + a_{32}Q + a_{33}K \end{bmatrix} =$$

$$= \begin{bmatrix} e_0 \\ e_1 \\ e_2 \\ e_3 \end{bmatrix} = |B'\rangle = |\psi_1'\rangle ,$$

где

$$\begin{aligned} e_0 = {} & b_{00}\{a_{00}V + a_{01}W + a_{02}Q + a_{03}K\} + \\ & + b_{01}\{a_{10}V + a_{11}W + a_{12}Q + a_{13}K\} + \\ & + b_{02}\{a_{20}V + a_{21}W + a_{22}Q + a_{23}K\} + \\ & + b_{03}\{a_{30}V + a_{31}W + a_{32}Q + a_{33}K\}, \end{aligned}$$

e_1, e_2, e_3 вычисляются аналогично, как и e_0.

Таким образом, результирующий выходной вектор $|\psi_1'\rangle$ всей квантовой схемы из двух последовательно соединенных гейтов есть $|\psi_1'\rangle = |B'\rangle$.

7). Далее при подаче вектора $|\psi\rangle = \begin{bmatrix} V \\ W \\ Q \\ K \end{bmatrix}$ на вход другой квантовой схемы из одного гейта с матрицей $\boldsymbol{M_c}$ на его выходе будет следующий вектор $|\psi_2'\rangle$:

$$\boldsymbol{M_c} \times |\psi\rangle =$$

$$= \begin{bmatrix} c_{00} & c_{01} & c_{02} & c_{03} \\ c_{10} & c_{11} & c_{12} & c_{13} \\ c_{20} & c_{21} & c_{22} & c_{23} \\ c_{30} & c_{31} & c_{32} & c_{33} \end{bmatrix} \times \begin{bmatrix} V \\ W \\ Q \\ K \end{bmatrix} = \begin{bmatrix} c_{00}\boldsymbol{V} + c_{01}\boldsymbol{W} + c_{02}\boldsymbol{Q} + c_{03}\boldsymbol{K} \\ c_{10}V + c_{11}W + c_{12}Q + c_{13}K \\ c_{20}V + c_{21}W + c_{22}Q + c_{23}K \\ c_{30}V + c_{31}W + c_{32}Q + c_{33}K \end{bmatrix} =$$

$$= \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{bmatrix} = |\psi'_2\rangle,$$

где $c_{ij} = b_{i0}a_{0j} + b_{i1}a_{1j} + b_{i2}a_{2j} + b_{i3}a_{3j}$, а i=0, 1, 2, 3; j=0, 1, 2, 3.

8). Сравним первые (самые верхние строки) компонент e_0 и x_0 векторов $|\psi'_1\rangle$, $|\psi'_2\rangle$ и покажем, что они равны.

Так как для вектора $|\psi'_1\rangle$ справедливо соотношение

$$\begin{aligned} e_0 &= b_{00}\{a_{00}V + a_{01}W + a_{02}Q + a_{03}K\} + \\ &+ b_{01}\{a_{10}V + a_{11}W + a_{12}Q + a_{13}K\} + \\ &+ b_{02}\{a_{20}V + a_{21}W + a_{22}Q + a_{23}K\} + \\ &+ b_{03}\{a_{30}V + a_{31}W + a_{32}Q + a_{33}K\} = \\ &= \{b_{00}a_{00} + b_{01}a_{10} + b_{02}a_{20} + b_{03}a_{30}\}V + \\ &+ \{b_{00}a_{01} + b_{01}a_{11} + b_{02}a_{21} + b_{03}a_{31}\}W + \\ &+ \{b_{00}a_{02} + b_{01}a_{12} + b_{02}a_{22} + b_{03}a_{32}\}Q + \\ &+ \{b_{00}a_{03} + b_{01}a_{13} + b_{02}a_{23} + b_{03}a_{33}\}K, \end{aligned}$$

для вектора $|\psi'_2\rangle$ справедливо соотношение

$$\begin{aligned} x_0 &= c_{00}\boldsymbol{V} + c_{01}\boldsymbol{W} + c_{02}\boldsymbol{Q} + c_{03}\boldsymbol{K} = \\ &= \{b_{00}a_{00} + b_{01}a_{10} + b_{02}a_{20} + b_{03}a_{30}\}V + \\ &+ \{b_{00}a_{01} + b_{01}a_{11} + b_{02}a_{21} + b_{03}a_{31}\}W + \\ &+ \{b_{00}a_{02} + b_{01}a_{12} + b_{02}a_{22} + b_{03}a_{32}\}Q + \\ &+ \{b_{00}a_{03} + b_{01}a_{13} + b_{02}a_{23} + b_{03}a_{33}\}K, \end{aligned}$$

то $e_0 = x_0$.

Сравнение всех остальных компонент e_1, e_2, e_3 и x_1, x_2, x_3 для векторов $|\psi'_1\rangle$ и $|\psi'_2\rangle$ показывает, что они идентичны, а значит и сами схемы эквивалентны.

9). Есть еще один способ вывода результирующей матрицы.
Как хорошо известно [8, с.18], умножение сцепленных матриц *ассоциативно* (т.е. обладает сочетательным свойством). В данном случае используемые $\boldsymbol{M_a}$, $\boldsymbol{M_b}$ и $\boldsymbol{M_c}$ — квадратные матрицы размерностью 4×4. Вектор $|\psi\rangle = \begin{bmatrix} V \\ W \\ Q \\ K \end{bmatrix}$ — это тоже матрица, но уже размерностью 4×1. Тогда

$$|A'\rangle = \boldsymbol{M_a}\times|\psi\rangle,$$

$$|B'\rangle = \boldsymbol{M_b}\times|A'\rangle$$

или

$$|B'\rangle = \boldsymbol{M_b}\times|A'\rangle = \boldsymbol{M_b}\times\{\boldsymbol{M_a}\times|\psi\rangle\} = |\psi_1'\rangle.$$

Введем следующее обозначение: $\boldsymbol{M}=\boldsymbol{M_b}\times\boldsymbol{M_a}$.

Воспользуемся теперь свойством, что умножение матриц *ассоциативно*, и окончательно получим следующее соотношение (изменив расположение фигурных скобок):

$$|\psi_1'\rangle = \boldsymbol{M_b}\times|A'\rangle = \boldsymbol{M_b}\times\left\{\ \boldsymbol{M_a}\times|\psi\rangle\ \right\} =$$

$$= \left\{\ \boldsymbol{M_b}\times\boldsymbol{M_a}\ \right\}\times|\psi\rangle = \boldsymbol{M}\times|\psi\rangle.$$

Таким образом, если в качестве матрицы $\boldsymbol{M_c}$ взять матрицу $\boldsymbol{M}$, то выходные векторы $|\psi_1'\rangle$ и $|\psi_2'\rangle$ будут идентичны, так как

$$\boldsymbol{M_c}\times|\psi\rangle = |\psi_2'\rangle.$$

10). И тем самым задача решена■

Из ***Примера 5.17*** и главы 2 следует, что результат произведения унитарных операторов есть унитарный оператор, а значит последовательное применение нескольких двухкубитовых гейтов эквивалентно некоторому результирующему двухкубитовому гейту (квантовому элементу).

Для рассмотрения далее очередных примеров сформулируем следующее важное правило.

Правило 5.4(**2**)

Последовательное применение нескольких ***двух****кубитовых гейтов (расположенных в заданном порядке) эквивалентно некоторому результирующему* ***двух****кубитовому гейту. Унитарная матрица этого результирующего преобразования получается как результат последовательного (в* ***инверсном*** *(т.е. обратном) порядке по отношению к порядку следования гейтов) перемножения унитарных матриц этих гейтов* ■

На практике порой требуется упрощать квантовые схемы на двух кубитах. Один из возможных способов упрощения квантовой схемы — это замена одной ее части (или даже целиком ее) другой эквивалентной квантовой схемой. Для этого необходимо заменять группу гейтов в квантовой схеме на один или несколько других гейтов, которые реализуют то же самое унитарное преобразование. Следующий пример показывает, как это можно делать.

Пример 5.18 (схема обмена на двух кубитах)

Известна квантовая схема из 3-х последовательно соединенных двухкубитовых гейтов CNOT с соответствующими унитарными матрицами $\boldsymbol{M_a}$ и $\boldsymbol{M_b}$.

Требуется определить один двухкубитовый гейт, который эквивалентен этим трем последовательно соединенным двухкубитовым гейтам.

Другими словами, требуется определить унитарную матрицу $\boldsymbol{M_c}$ (рис. 5.21**б**) результирующего преобразования и установить, что

следующие две квантовые схемы (рис. 5.21**а**) эквивалентны:

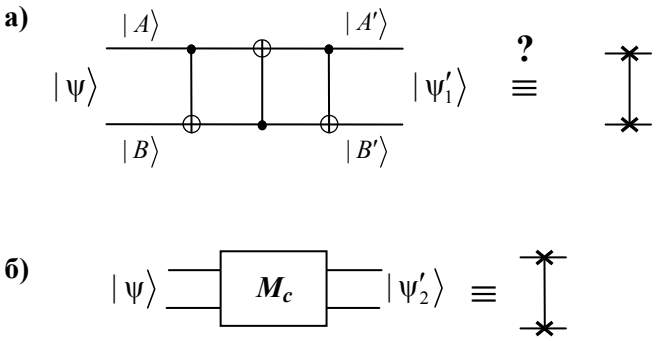


Рис. **5.21**

Решение

1). В условиях задачи не указан явно вычислительный базис. Будем далее предполагать, что входные векторы $|\psi\rangle$ и $|A\rangle$, $|B\rangle$, выходные векторы $|\psi_1'\rangle$, $|\psi_2'\rangle$ и $|A'\rangle$, $|B'\rangle$, а также и матрицы преобразования $\boldsymbol{M_a}$, $\boldsymbol{M_b}$ и $\boldsymbol{M_c}$ соответствуют одному и тому же вычислительному базису

2). Эквивалентность двух схем понимается в том смысле, что матрица $\boldsymbol{M_c}$ (гейта обмена) эквивалентна матрице $\boldsymbol{E_c}$ результирующего преобразования трех гейтов CNOT (два гейта имеют матрицу $\boldsymbol{M_a}$, а один гейт CNOT, включенный наоборот, имеет матрицу $\boldsymbol{M_b}$). Специально еще раз отметим, что результирующее преобразование с матрицей $\boldsymbol{M_c}$ зависит, вообще говоря, от порядка, в котором выполняются операции с матрицами $\boldsymbol{M_a}$ и $\boldsymbol{M_b}$ (т.е. от порядка, в котором выполняются гейты).

3). Таким образом, применяя *Правило* 5.4(**2**), необходимо сначала вычислить матрицу $\boldsymbol{E_c}$, где

$$\boldsymbol{E_c}=\boldsymbol{M_a}\times\boldsymbol{M_b}\times\boldsymbol{M_a},$$

и затем сравнить $\boldsymbol{E_c}$ с матрицей $\boldsymbol{M_c}$. Если $\boldsymbol{E_c} \equiv \boldsymbol{M_c}$, то схемы эквивалентны.

4). Матрица (табл. 5.2) для гейта CNOT есть

$$\boldsymbol{M_a} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix},$$

матрица (см. далее ***Пример 5.23***) для гейта CNOT, включенного наоборот, есть

$$\boldsymbol{M_b} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix},$$

матрица для гейта обмена была приведена ранее и есть

$$\boldsymbol{M_c} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

5). Тогда для $\boldsymbol{E_c}=\boldsymbol{M_a}\times\boldsymbol{M_b}\times\boldsymbol{M_a}$ имеем

$$\boldsymbol{E_{00}} = \boldsymbol{M_b}\times\boldsymbol{M_a} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \times \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} =$$

$$= \begin{bmatrix} 1+0 & 0+0 & 0+0 & 0+0 \\ 0+0 & 0+0 & 1+0 & 0+0 \\ 0+0 & 0+0 & 0+0 & 1+0 \\ 0+0 & 1+0 & 0+0 & 0+0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix},$$

тогда окончательно получаем следующее выражение:

$$\boldsymbol{E}_c=\boldsymbol{M}_a\times\boldsymbol{E}_{00}=\left[\begin{array}{cccc}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{array}\right]\times\left[\begin{array}{cccc}1&0&0&0\\0&0&1&0\\0&0&0&1\\0&1&0&0\end{array}\right]=$$

$$=\begin{bmatrix}1+0&0+0&0+0&0+0\\0+0&0+0&1+0&0+0\\0+0&1+0&0+0&0+0\\0+0&0+0&0+0&1+0\end{bmatrix}=\begin{bmatrix}1&0&0&0\\0&0&1&0\\0&1&0&0\\0&0&0&1\end{bmatrix}.$$

6). Таким образом, если сравнить матрицу $\boldsymbol{E}_c$ с матрицей $\boldsymbol{M}_c$, то легко заметить, что эти две матрицы идентичны, т.е.

$$\boldsymbol{E}_c \equiv \boldsymbol{M}_c.$$

7). Отметим следующее.

В ***Примере 5.15г*** для нахождения унитарной матрицы, удовлетворяющей условиям для гейта CNOT

$$\boldsymbol{M}_a|00\rangle=|00\rangle,\ \boldsymbol{M}_a|01\rangle=|01\rangle,\ \boldsymbol{M}_a|10\rangle=|11\rangle,\ \boldsymbol{M}_a|11\rangle=|10\rangle,$$

была составлена и затем решена система уравнений. В результате была найдена требуемая матрица $\boldsymbol{M}_a$. Аналогичным образом для гейта CNOT, уже включенного наоборот, была найдена унитарная матрица $\boldsymbol{M}_b$, удовлетворяющая условиям

$$\boldsymbol{M}_b|00\rangle=|00\rangle,\ \boldsymbol{M}_b|01\rangle=|11\rangle,\ \boldsymbol{M}_b|10\rangle=|10\rangle,\ \boldsymbol{M}_b|11\rangle=|01\rangle.$$

8). И тем самым задача решена■

Пример 5.19 (факторизация вектора)

Известен вектор состояния $|\tilde{\psi}\rangle = \begin{bmatrix} V \\ W \\ Q \\ K \end{bmatrix}$ для двухкубитовой схемы.

Требуется разложить этот вектор на 2 множителя (вектора), т.е. факторизовать его.

Решение

1). Эта задача является обратной по отношению к задаче из ***Примеров 5.15*****а**, **б**.

2). Опираясь на квантовую механику, отметим следующее. Если кубит находится в *чистом* состоянии, то он имеет вектор состояния $|\psi\rangle$, а если кубит находится в *смешанном* состоянии, то он не описывается вектором состояния. Если оба кубита находятся в чистом состоянии (т.е. каждый из них имеет свой вектор состояния $|\psi_1\rangle$, $|\psi_2\rangle$), то соответственно существует $|\tilde{\psi}\rangle$ — вектор состояния квантового регистра (как квантовой системы из 2-х кубитов). Причем $|\tilde{\psi}\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$. Однако, если известно, что квантовый регистр находится в чистом состоянии (т.е. имеет некоторый вектор состояния), то это еще **не означает**, что сами кубиты по отдельности (как подсистемы составной квантовой системы в виде квантового регистра) имеют свои векторы состояния (например, оба кубита находятся в смешанном состоянии, а квантовый регистр — в чистом состоянии).

3). Предположим, что оба кубита находятся в чистом состоянии.

Тогда состояние 1-го кубита есть

$$|\psi_1\rangle = a|0\rangle + b|1\rangle \text{ (где } |a|^2 + |b|^2 = 1),$$

а состояние 2-го кубита есть

$$|\psi_2\rangle = c|0\rangle + d|1\rangle \text{ (где } |c|^2 + |d|^2 = 1)$$

и должно выполняться следующее соотношение:

$$|\tilde{\psi}\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \,.$$

4). Выберем некоторый вычислительный базис, например

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix},$$

тогда

$$|\psi_1\rangle = a|0\rangle + b|1\rangle = a\begin{bmatrix} 1 \\ 0 \end{bmatrix} + b\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix},$$

$$|\psi_2\rangle = c|0\rangle + d|1\rangle = c\begin{bmatrix} 1 \\ 0 \end{bmatrix} + d\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} c \\ d \end{bmatrix},$$

$$|\tilde{\psi}\rangle = |\psi_1\rangle \otimes |\psi_2\rangle = \begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} a\begin{bmatrix} c \\ d \end{bmatrix} \\ b\begin{bmatrix} c \\ d \end{bmatrix} \end{bmatrix} = \begin{bmatrix} ac \\ ad \\ bc \\ bd \end{bmatrix} = \begin{bmatrix} V \\ W \\ Q \\ K \end{bmatrix},$$

т.е., найдя решение следующей системы уравнений:

$$\begin{cases} ac = V \\ ad = W \\ bc = Q \\ bd = K \end{cases},$$

можно определить и сами векторы состояний $|\psi_1\rangle$, $|\psi_2\rangle$, конечно, в том случае, если решение этой системы уравнений существует (*a, b, c, d* — это комплексные числа).

5). И тем самым задача решена■

Из ***Примера 5.19*** и *Правила* 5.0**б** следует:

- состояние составной системы (квантового регистра) описывается вектором $|\tilde{\psi}\rangle$, который может быть вычислен путем **тензорного умножения** векторов состояния каждой из систем (кубитов), входящих в составную систему, т.е. $|\tilde{\psi}\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \ldots \otimes |\psi_n\rangle$;
- для того чтобы найти все векторы $|\psi_i\rangle$, зная вектор $|\tilde{\psi}\rangle$, необходимо решить обратную задачу, т.е. факторизовать вектор состояния, если это возможно; один из возможных способов решения этой обратной задачи заключается в том, что необходимо **составить некоторую систему уравнений**, а затем попытаться ее решить; если решение существует и оно найдено, то задача факторизации считается решенной.

Сформулируем следующее важное правило.

Правило 5.5

Вектор состояния $|\psi_i\rangle$ *для каждого* ***i****–го кубита (****i*** *изменяется от* 1 *до* ***n****) из квантового регистра может быть найден (при условии, что этот вектор существует) путем факторизации* $|\tilde{\psi}\rangle$ *— вектора состояния квантового регистра (для этого необходимо решить* ***обратную задачу*** *по отношению к задаче нахождения вектора* $|\tilde{\psi}\rangle$ *по совокупности* ***n*** *векторов* $|\psi_i\rangle$ *)* ■

Данное правило позволяет для конкретного вектора состояния квантовой составной системы (в данном случае квантового регистра, состоящего из кубитов) найти векторы состояний самих подсистем (т.е. векторы состояний кубитов), входящих в эту составную систему, или убедиться в их отсутствии. Важно понять, что квантовый регистр (находящийся в чистом состоянии) имеет вектор состояния, при этом кубиты, входящие в этот регистр, могут каждый по отдельности иногда не иметь вектора состояния (хотя вектор состояния квантового регистра существует). Следующий пример показывает, как можно применять это правило.

Пример 5.20 (факторизация конкретного вектора)

Известен вектор состояния $|\tilde{\psi}\rangle = \frac{1}{2}\begin{bmatrix} -1 \\ 1 \\ 1 \\ -1 \end{bmatrix}$ для двухкубитовой схемы.

Требуется разложить этот вектор на 2 множителя (вектора), т.е. факторизовать его.

Решение

1). Сначала будем искать решение среди действительных чисел (действительных амплитуд). Если решение среди действительных чисел не будет найдено, то будем искать решение среди комплексных чисел.

2). Применим *Правило* 5.5, опираясь на ***Пример 5.19***. Учтя, что $|a|^2+|b|^2=1$ и $|c|^2+|d|^2=1$, составим и решим следующую систему уравнений:

$$|\tilde{\psi}\rangle = |\psi_1\rangle \otimes |\psi_2\rangle = \begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} a\begin{bmatrix} c \\ d \end{bmatrix} \\ b\begin{bmatrix} c \\ d \end{bmatrix} \end{bmatrix} = \begin{bmatrix} ac \\ ad \\ bc \\ bd \end{bmatrix} = \frac{1}{2}\begin{bmatrix} -1 \\ 1 \\ 1 \\ -1 \end{bmatrix}$$

или

$$\begin{cases} 2ac = -1 \\ 2ad = 1 \\ 2bc = 1 \\ 2bd = -1 \end{cases},$$

из этой системы следует (для действительных амплитуд), что

$$\begin{cases} a^2c^2 = \frac{1}{4} \\ a^2d^2 = \frac{1}{4} \end{cases} \Rightarrow a^2\left(c^2+d^2\right) = \frac{1}{2} \Rightarrow a^2 \cdot 1 = \frac{1}{2} \Rightarrow a = \pm\frac{1}{\sqrt{2}},$$

$$\begin{cases} b^2c^2=\dfrac{1}{4} \\ b^2d^2=\dfrac{1}{4} \end{cases} \Rightarrow\ b^2\left(c^2+d^2\right)=\frac{1}{2} \Rightarrow\quad b^2\cdot 1=\frac{1}{2} \Rightarrow\quad b=\pm\frac{1}{\sqrt{2}}.$$

Аналогично можно получить, что

$$\begin{cases} a^2c^2=\dfrac{1}{4} \\ b^2c^2=\dfrac{1}{4} \end{cases} \Rightarrow\ c^2\left(a^2+b^2\right)=\frac{1}{2} \Rightarrow\quad c^2\cdot 1=\frac{1}{2} \Rightarrow\quad c=\pm\frac{1}{\sqrt{2}},$$

$$\begin{cases} a^2d^2=\dfrac{1}{4} \\ b^2d^2=\dfrac{1}{4} \end{cases} \Rightarrow\ d^2\left(a^2+b^2\right)=\frac{1}{2} \Rightarrow\quad d^2\cdot 1=\frac{1}{2} \Rightarrow\quad d=\pm\frac{1}{\sqrt{2}}.$$

3). Таким образом, получены два решения:

первое решение

$$|\psi_1^I\rangle=a|0\rangle+b|1\rangle=+\frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix},\ |\psi_2^I\rangle=c|0\rangle+d|1\rangle=+\frac{1}{\sqrt{2}}\begin{bmatrix}-1\\1\end{bmatrix},$$

второе решение

$$|\psi_1^{II}\rangle=a|0\rangle+b|1\rangle=-\frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix},\ |\psi_2^{II}\rangle=c|0\rangle+d|1\rangle=-\frac{1}{\sqrt{2}}\begin{bmatrix}-1\\1\end{bmatrix}.$$

4). Отметим, что $|\psi_1^I\rangle=(-1)|\psi_1^{II}\rangle$, $|\psi_2^I\rangle=(-1)|\psi_2^{II}\rangle$, а $\exp(i\pi)=-1$. Для $|\psi\rangle$, амплитуд вероятностей a и b справедливо следующее соотношение:

$$|\psi\rangle=e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle+e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right),$$

где $\boldsymbol{\theta}$, $\boldsymbol{\varphi}$, $\boldsymbol{\gamma}$ — действительные числа, причем множитель $e^{i\gamma}$ в общем-то можно **игнорировать**, так как [1, с.35] он «*не приводит к наблюдаемым эффектам*».

5). И тем самым задача решена■

Комментарий к задачам о факторизации двухкубитового состояния

Пусть задан кэт-вектор $\left|\tilde{\Psi}\right\rangle$ чистого двухкубитового состояния. Как обычно, его можно представить в разных формах:

$$\left|\tilde{\Psi}\right\rangle = V\left|00\right\rangle + W\left|01\right\rangle + Q\left|10\right\rangle + K\left|11\right\rangle \equiv \begin{bmatrix} V \\ W \\ Q \\ K \end{bmatrix}. \qquad \text{(К1)}$$

Единственное ограничение, накладываемое на комплексные амплитуды *V, W, Q, K,* есть условие нормировки

$$\left|V\right|^2 + \left|W\right|^2 + \left|Q\right|^2 + \left|K\right|^2 = 1. \qquad \text{(К2)}$$

Нас интересует, можно ли $\left|\tilde{\Psi}\right\rangle$ представить в факторизованном виде как тензорное произведение

$$\left|\tilde{\Psi}\right\rangle = \left|\Psi_1\right\rangle \otimes \left|\Psi_2\right\rangle \qquad \text{(К3)}$$

однокубитовых кэт-векторов $\left|\Psi_1\right\rangle$ и $\left|\Psi_2\right\rangle$?

Сформулируем необходимые и достаточные условия, накладываемые на *V, W, Q, K* (помимо условия нормировки (К2)), при которых это возможно. Для этого вычислим матрицу плотности одной из подсистем (для определенности, первого кубита). Согласно результатам последнего раздела главы 1, матрица плотности $\hat{\rho}_1$ первой подсистемы определяется следующим выражением:

$$\hat{\rho}_1 = Sp_2\left|\tilde{\Psi}\right\rangle\left\langle\tilde{\Psi}\right|, \qquad \text{(К4)}$$

где символом Sp_2 обозначена операция вычисления следа оператора $\left|\tilde{\Psi}\right\rangle\left\langle\tilde{\Psi}\right|$, который представляет собой матрицу плотности чистого состояния (К1) двухкубитовой системы, по квантовым числам второго кубита.

Подставляя в (К4) выражение (К1), получаем (индексами 1 и 2 для удобства отмечены бра- и кэт-векторы 1-го и 2-го кубитов)

$$\begin{aligned}
&\hat{\rho}_1 = Sp_2\left(V^*{}_1\langle 0|_2\langle 0| + W^*{}_1\langle 0|_2\langle 1| + Q^*{}_1\langle 1|_2\langle 0| + K^*{}_1\langle 1|_2\langle 1|\right)\times \\
&\times\left(V|0\rangle_1|0\rangle_2 + W|0\rangle_1|1\rangle_2 + Q|1\rangle_1|0\rangle_2 + K|1\rangle_1|1\rangle_2\right) = \\
&= (|V|^2 + |W|^2)|0\rangle_1{}_1\langle 0| + (VQ^* + WK^*)|0\rangle_1{}_1\langle 1| + (V^*Q + W^*K)|1\rangle_1{}_1\langle 0| + \\
&+ (|Q|^2 + |K|^2)|1\rangle_1{}_1\langle 1|.
\end{aligned} \tag{К5}$$

В последних двух строчках индекс 1, конечно, можно опустить, коль скоро здесь остались только операторы, относящиеся к 1-му кубиту. Операторное выражение (К5) означает, что матрица оператора $\hat{\rho}_1$, т.е. матрица плотности первого кубита в базисе $|0\rangle$ и $|1\rangle$, имеет вид

$$\hat{\rho}_1 = \begin{bmatrix} |V|^2 + |W|^2 & VQ^* + WK^* \\ V^*Q + W^*K & |Q|^2 + |K|^2 \end{bmatrix}. \tag{К6}$$

Она, очевидно, удовлетворяет всем необходимым требованиям, а именно

$$\hat{\rho}^{\dagger}{}_1 = \hat{\rho}_1 \ ,$$

т.е. это эрмитовая матрица,

$$Sp\,\hat{\rho}_1 = |V|^2 + |W|^2 + |Q|^2 + |K|^2 = 1,$$

и удовлетворяет условию нормировки, как это видно из (К2).

Теперь сформулируем условие возможности факторизации состояния $\left|\tilde{\Psi}\right\rangle$ в (К1).

Факторизация означает, что не только вся система, но и каждая из подсистем, в том числе и первый кубит, находится в чистом состоянии.

Необходимым и достаточным условием того, что подсистема находится в чистом состоянии, является равенство

$$\hat{\rho}_1^2 = \hat{\rho}_1, \qquad (К7)$$

т.е. квадрат матрицы плотности совпадает с самой матрицей плотности. Если состояние является смешанным, то

$$\hat{\rho}_1^2 \neq \hat{\rho}_1 \text{ и } Sp\,\hat{\rho}_1^2 < 1.$$

Подставляя выражение (К6) в (К7), получаем 4 комплексных условия на коэффициенты *V, W, Q, K*.

Для иллюстрации можно убедиться, что в ***Примере 5.20***, когда

$$V = -1/2,\ W = 1/2,\ Q = 1/2,\ K = -1/2,$$

имеем

$$\hat{\rho}_1 = \frac{1}{2}\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} = \frac{1}{2}\left\{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} - \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\right\} = \frac{1}{2}\left(\boldsymbol{I} - \sigma_1\right),$$

а

$$\boldsymbol{I}^2 = \sigma_1^2 = \boldsymbol{I}, \quad \sigma_1 = \boldsymbol{X},$$

так что

$$\hat{\rho}^2 = \frac{1}{4}\left(\boldsymbol{I} - \sigma_1\right)^2 = \frac{1}{4}\left(\boldsymbol{I}^2 - 2\sigma_1 + \sigma_1^2\right) = \frac{1}{2}\left(\boldsymbol{I} - \sigma_1\right) = \hat{\rho}_1,$$

т.е. состояние первого кубита является чистым, и вектор системы можно факторизовать!

Пример 5.21 (построение унитарной матрицы в общем случае)
Известны требования к унитарной матрице $\boldsymbol{M}$ размером 4×4 в виде

$$\boldsymbol{M}|d_{00}\rangle=|A\rangle,\ \boldsymbol{M}|d_{01}\rangle=|B\rangle,\ \boldsymbol{M}|d_{10}\rangle=|C\rangle,\ \boldsymbol{M}|d_{11}\rangle=|D\rangle,$$

где $|d_{00}\rangle$, $|d_{01}\rangle$, $|d_{10}\rangle$, $|d_{11}\rangle$ — это вычислительный базис 2-х кубитов (базисные векторы), а $|A\rangle$, $|B\rangle$, $|C\rangle$, $|D\rangle$ — векторы, являющиеся результатом преобразования базисных векторов.

Требуется определить унитарную матрицу $\boldsymbol{M}$.

Решение

1). Пусть $\boldsymbol{E}$ имеет представление

$$\boldsymbol{E}=\begin{bmatrix} e_{00} & e_{01} & e_{02} & e_{03} \\ e_{10} & e_{11} & e_{12} & e_{13} \\ e_{20} & e_{21} & e_{22} & e_{23} \\ e_{30} & e_{31} & e_{32} & e_{33} \end{bmatrix}.$$

2). Для конкретного вычислительного базиса будем искать решение, т.е. элементы некоторой матрицы $\boldsymbol{E}$, как решение следующей системы уравнений:

$$\begin{cases} \boldsymbol{E}|d_{00}\rangle=|A\rangle \\ \boldsymbol{E}|d_{01}\rangle=|B\rangle \\ \boldsymbol{E}|d_{10}\rangle=|C\rangle \\ \boldsymbol{E}|d_{11}\rangle=|D\rangle \end{cases}.$$

Если решение этой системы уравнений не существует (e_{ik}, — комплексные числа и элементы матрицы $\boldsymbol{E}$), то не существует и самой матрицы $\boldsymbol{M}$.

3). Для найденной матрицы $\boldsymbol{E}$ необходимо проверить свойство унитарности, т.е. $\boldsymbol{E}\boldsymbol{E}^{\dagger}=\boldsymbol{E}^{\dagger}\boldsymbol{E}=I$. Если $\boldsymbol{E}$ унитарна, то она есть искомая матрица, т.е. $\boldsymbol{M}=\boldsymbol{E}$.

4). И тем самым задача решена■

Из ***Примеров 5.8***, ***5.15*****в**, **г** и *Правила* 5.0**а** следует:

- амплитуды вероятности (т.е. компоненты выходного) вектора состояния кубита после воздействия на этот кубит унитарного преобразования (описываемого соответствующей унитарной матрицей) определяются путем **умножения** этой унитарной матрицы на вектор-столбец, составленный из амплитуд вероятностей (компонентов входного) вектора состояния кубита, до воздействия на него унитарным преобразованием;
- для того чтобы найти все элементы унитарной матрицы, соответствующей преобразованию над кубитом (или кубитами), необходимо решить обратную задачу; один из возможных способов решения этой обратной задачи заключается в том, что необходимо составить некоторую систему уравнений, а затем попытаться ее решить; если решение существует и оно найдено, то искомая матрица считается найденной.

Для рассмотрения далее очередных примеров сформулируем следующее важное правило.

Правило 5.6

*Унитарная матрица **M** может быть найдена (при условии, что она существует) путем определения ее элементов по совокупности требований к ней — т.е. по набору входных и выходных векторов, которые связаны между собой с помощью этой матрицы **M** (для этого необходимо решить **обратную задачу** по отношению к задаче нахождения выходного вектора $|\tilde{\psi}\rangle$ по входному вектору $|\psi\rangle$ и унитарной матрице **M**)* ■

Данное правило позволяет для конкретного набора входных и выходных векторов, которые связаны между собой с помощью неизвестной унитарной матрицы ***M***, найти эту матрицу или убедиться в ее отсутствии.

В общем случае такая матрица может быть не единственной или не существовать совсем.

Следующий пример показывает, как можно применять это правило.

Пример 5.22 (построение конкретной унитарной матрицы)
Известны требования к унитарной матрице $\boldsymbol{M}$ размером 4×4 в виде

$$\boldsymbol{M}|00\rangle=|00\rangle,\ \ \boldsymbol{M}|01\rangle=|01\rangle,\ \ \boldsymbol{M}|10\rangle=|11\rangle,\ \ \boldsymbol{M}|11\rangle=|10\rangle,$$

где $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$ — это вычислительный базис 2-х кубитов (базисные векторы), а $|0\rangle=\begin{bmatrix}1\\0\end{bmatrix}$, $|1\rangle=\begin{bmatrix}0\\1\end{bmatrix}$.

Требуется определить унитарную матрицу $\boldsymbol{M}$.

Решение

1). Пусть $\boldsymbol{E}$ имеет представление

$$\boldsymbol{E}=\begin{bmatrix}e_{00}&e_{01}&e_{02}&e_{03}\\e_{10}&e_{11}&e_{12}&e_{13}\\e_{20}&e_{21}&e_{22}&e_{23}\\e_{30}&e_{31}&e_{32}&e_{33}\end{bmatrix}.$$

2). Применим *Правило* 5.6 и будем искать решение, т.е. элементы некоторой матрицы $\boldsymbol{E}$, как решение следующей системы уравнений:

$$\begin{cases}\boldsymbol{E}|00\rangle=|00\rangle\\\boldsymbol{E}|01\rangle=|01\rangle\\\boldsymbol{E}|10\rangle=|11\rangle\\\boldsymbol{E}|11\rangle=|10\rangle\end{cases}.$$

Если решение этой системы уравнений не существует (e_{ik} — комплексные числа и элементы матрицы $\boldsymbol{E}$), то не существует и самой матрицы $\boldsymbol{M}$.

3). Далее решение полностью соответствует решению задачи из ***Примера 5.15*****в**.

4). И тем самым задача решена■

Пример 5.23 (построение конкретной унитарной матрицы)
Известны требования к унитарной матрице $\boldsymbol{M}$ размером 4×4 в виде

$$\boldsymbol{M}|00\rangle=|00\rangle,\quad \boldsymbol{M}|01\rangle=|11\rangle,\quad \boldsymbol{M}|10\rangle=|10\rangle,\quad \boldsymbol{M}|11\rangle=|01\rangle,$$

где $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$ — это вычислительный базис 2-х кубитов (базисные векторы), а $|0\rangle=\begin{bmatrix}1\\0\end{bmatrix}$, $|1\rangle=\begin{bmatrix}0\\1\end{bmatrix}$.

Требуется определить унитарную матрицу $\boldsymbol{M}$.

Решение

1). Пусть $\boldsymbol{E}$ имеет представление

$$\boldsymbol{E}=\begin{bmatrix}e_{00} & e_{01} & e_{02} & e_{03}\\ e_{10} & e_{11} & e_{12} & e_{13}\\ e_{20} & e_{21} & e_{22} & e_{23}\\ e_{30} & e_{31} & e_{32} & e_{33}\end{bmatrix}.$$

2). Применим *Правило* 5.6 и будем искать решение, т.е. элементы некоторой матрицы $\boldsymbol{E}$, как решение следующей системы уравнений:

$$\begin{cases}\boldsymbol{E}|00\rangle=|00\rangle\\ \boldsymbol{E}|01\rangle=|11\rangle\\ \boldsymbol{E}|10\rangle=|10\rangle\\ \boldsymbol{E}|11\rangle=|01\rangle\end{cases}.$$

Если решение этой системы уравнений не существует (e_{ik}, — комплексные числа и элементы матрицы $\boldsymbol{E}$), то не существует и самой матрицы $\boldsymbol{M}$.

3). Так как

$$|0\rangle=\begin{bmatrix}1\\0\end{bmatrix},\quad |1\rangle=\begin{bmatrix}0\\1\end{bmatrix},$$

то из ***Примера 5.15*****а** следует, что базисные векторы

$$|00\rangle,\ |01\rangle,\ |10\rangle,\ |11\rangle$$

могут быть представлены как

$$|00\rangle=\begin{bmatrix}1\\0\\0\\0\end{bmatrix},\ |01\rangle=\begin{bmatrix}0\\1\\0\\0\end{bmatrix},\ |10\rangle=\begin{bmatrix}0\\0\\1\\0\end{bmatrix},\ |11\rangle=\begin{bmatrix}0\\0\\0\\1\end{bmatrix},$$

а сама система уравнений может быть записана следующим образом:

$$\begin{cases}\boldsymbol{E}\times\begin{bmatrix}1\\0\\0\\0\end{bmatrix}=\begin{bmatrix}1\\0\\0\\0\end{bmatrix}\\ \boldsymbol{E}\times\begin{bmatrix}0\\1\\0\\0\end{bmatrix}=\begin{bmatrix}0\\0\\0\\1\end{bmatrix}\\ \boldsymbol{E}\times\begin{bmatrix}0\\0\\1\\0\end{bmatrix}=\begin{bmatrix}0\\0\\1\\0\end{bmatrix}\\ \boldsymbol{E}\times\begin{bmatrix}0\\0\\0\\1\end{bmatrix}=\begin{bmatrix}0\\1\\0\\0\end{bmatrix}\end{cases}\Rightarrow\quad\begin{cases}\begin{bmatrix}e_{00}\\e_{10}\\e_{20}\\e_{30}\end{bmatrix}=\begin{bmatrix}1\\0\\0\\0\end{bmatrix}\\ \begin{bmatrix}e_{01}\\e_{11}\\e_{21}\\e_{31}\end{bmatrix}=\begin{bmatrix}0\\0\\0\\1\end{bmatrix}\\ \begin{bmatrix}e_{02}\\e_{12}\\e_{22}\\e_{32}\end{bmatrix}=\begin{bmatrix}0\\0\\1\\0\end{bmatrix}\\ \begin{bmatrix}e_{03}\\e_{13}\\e_{23}\\e_{33}\end{bmatrix}=\begin{bmatrix}0\\1\\0\\0\end{bmatrix}\end{cases}$$

4). Таким образом, найдено следующее решение для матрицы $\boldsymbol{E}$:

$$\boldsymbol{E}=\begin{bmatrix}1&0&0&0\\0&0&0&1\\0&0&1&0\\0&1&0&0\end{bmatrix}.$$

5). Для найденной матрицы $\boldsymbol{E}$ проверим свойство унитарности, т.е. $\boldsymbol{E}\boldsymbol{E}^{\dagger}=\boldsymbol{E}^{\dagger}\boldsymbol{E}=I$.

$$E^{\dagger}E=\left(\begin{bmatrix}1&0&0&0\\0&0&0&1\\0&0&1&0\\0&1&0&0\end{bmatrix}^{\dagger}\right)\times\left(\begin{bmatrix}1&0&0&0\\0&0&0&1\\0&0&1&0\\0&1&0&0\end{bmatrix}\right)=$$

$$=\begin{bmatrix}1&0&0&0\\0&0&0&1\\0&0&1&0\\0&1&0&0\end{bmatrix}\times\begin{bmatrix}1&0&0&0\\0&0&0&1\\0&0&1&0\\0&1&0&0\end{bmatrix}=$$

$$=\begin{bmatrix}1+0&0&0&0\\0&1+0&0&0\\0&0&1+0&0\\0&0&0&1+0\end{bmatrix}=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix}\equiv I,$$

т.е. свойство унитарности матрицы $\boldsymbol{E}$ выполняется. Так как $\boldsymbol{E}$ унитарна, то она есть искомая матрица, т.е. $\boldsymbol{M}=\boldsymbol{E}$. Отметим, что матрица из ***Примера 5.15*г** совпадает с $\boldsymbol{M}$.

6). И тем самым задача решена■

Комментарий к задачам синтеза унитарного (двухкубитового) преобразования

Задача в общем виде может быть поставлена так. Заданы состояния, которые получаются под действием некоторого двухкубитового гейта из базисных состояний двухкубитового регистра, поданных на вход квантовой схемы. Надо построить унитарный оператор (матрицу) этого преобразования.

Чтобы задача была корректной, векторы выходных состояний должны удовлетворять определенным условиям. В противном случае унитарного оператора просто может не существовать.

Суть в том, что унитарное преобразование сохраняет все скалярные произведения. Поэтому оно переводит полный ортонормированный набор состояний в какой-то другой полный ортонормированный набор. Следовательно, заданные на выходе состояния должны образовывать полный ортонормированный базис. Если это так, то задача нахождения матрицы преобразования решается в общем виде с помощью одной простой формулы. Конечно, это легко делается в гильбертовом пространстве любой размерности, но мы, для определенности, ограничимся четырехмерным гильбертовым пространством двухкубитового регистра.

Пусть $|a_i\rangle$, где $i = 0, 1, 2, 3$, есть некоторый полный ортонормированный базис, т.е.

$$\begin{aligned} &\langle a_i | a_j \rangle = \delta_{ij}, \\ &\sum_{i=0}^{3} |a_i\rangle\langle a_i| = 1. \end{aligned} \qquad \text{(К8)}$$

Под действием унитарного преобразования $\hat{M}$ эти состояния преобразуются следующим образом:

$$\hat{M}|a_i\rangle = |A_i\rangle, \qquad \text{(К9)}$$

где набор состояний $|A_i\rangle$ (i = 0, 1, 2, 3), в силу унитарности $\hat{M}$, удовлетворяет условиям

$$\begin{aligned} &\langle A_i | A_j \rangle = \delta_{ij}, \\ &\sum_{i=0}^{3} |A_i\rangle\langle A_i| = 1. \end{aligned} \qquad \text{(К10)}$$

В правой части (К9) вектор $|A_i\rangle$ разложим по старому полному базису $\{|a_i\rangle\}$, т.е.

$$|A_i\rangle = \sum_j M_{ji} |a_j\rangle. \qquad \text{(К11)}$$

Следовательно, с одной стороны,

$$M_{ji} = \langle a_j | A_i \rangle, \qquad \text{(К12)}$$

а с другой стороны, из (К9) следует, что

$$M_{ji} = \langle a_j | A_i \rangle = \langle a_j | \hat{M} | a_i \rangle. \qquad \text{(К13)}$$

Таким образом, M_{ji} искомого оператора в старом базисе имеют вид

$$M_{ji} = \langle a_j | A_i \rangle, \quad i, j = 0, 1, 2, 3. \qquad \text{(К14)}$$

Для иллюстрации рассмотрим ***Пример 5.23***, где

$$\begin{aligned} |a_0\rangle &\equiv |00\rangle, \\ |a_1\rangle &\equiv |01\rangle, \\ |a_2\rangle &\equiv |10\rangle, \\ |a_3\rangle &\equiv |11\rangle. \end{aligned}$$

По условию задачи матрица $\hat{M}$ осуществляет следующие преобразование базисных векторов:

$$|a_0\rangle \to |00\rangle \equiv |A_0\rangle,$$

$$|a_1\rangle \to |11\rangle \equiv |A_1\rangle,$$

$$|a_2\rangle \to |10\rangle \equiv |A_2\rangle,$$

$$|a_3\rangle \to |01\rangle \equiv |A_3\rangle.$$

Нетрудно видеть, что

$$M_{ji} = \langle a_j | A_i \rangle, \quad i,j = 0, 1, 2, 3;$$

а матрица $\hat{M}$ имеет вид

$$\hat{M} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix},$$

и нет необходимости проверять полноту и ортогональность набора состояний

$$\{|A_i\rangle\},$$

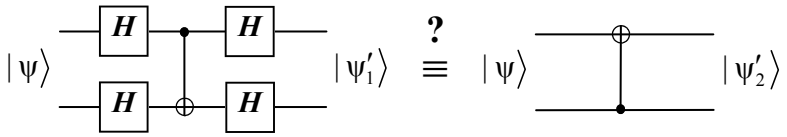
так как он отличается от исходного набора

$$\{|a_i\rangle\}$$

просто перестановкой двух базисных векторов.

Пример 5.24 (эквивалентные схемы на двух кубитах)
Известна квантовая схема [1, с.231] из последовательно соединенных гейтов с соответствующими известными унитарными матрицами $\boldsymbol{H}$ (для гейта *Адамара*) и $\boldsymbol{M_a}$ (для гейта CNOT). Известна также матрица $\boldsymbol{M_c}$ для гейта CNOT, включенного наоборот.

Требуется определить один двухкубитовый гейт, который эквивалентен этим последовательно соединенным гейтам. Другими словами, требуется определить унитарную матрицу $\boldsymbol{E}$ результирующего преобразования и установить, что следующие две квантовые схемы эквивалентны (т.е. $\boldsymbol{E} \equiv \boldsymbol{M_c}$):



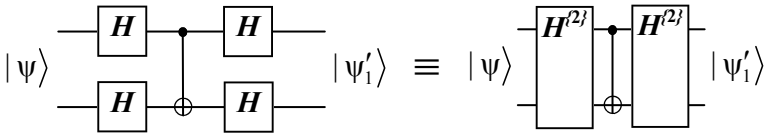
Решение

1). В условиях задачи не указан явно вычислительный базис. Будем далее предполагать, что входной вектор $|\psi\rangle$, выходные векторы $|\psi_1'\rangle$, $|\psi_2'\rangle$ и матрицы преобразования $\boldsymbol{H}$, $\boldsymbol{M_a}$ и $\boldsymbol{M_c}$ соответствуют одному и тому же вычислительному базису.

2). Будем искать решение, т.е. элементы некоторой матрицы $\boldsymbol{E}$, применяя *Правило* 5.0**в** и *Правило* 5.4(**2**).

3). Таким образом, применяя *Правило* 5.0**в** (опираясь также на ***Пример 5.16*****г**, рис. 5.20**а**, **б**), получим следующую матрицу $\boldsymbol{H^{\{2\}}}$ и две эквивалентные схемы:

$$\boldsymbol{H^{\{2\}}} = H \otimes H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1\cdot H & 1\cdot H \\ 1\cdot H & (-1)\cdot H \end{bmatrix} = \frac{1}{2}\left[\begin{array}{cc:cc} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ \hdashline 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{array}\right],$$



4). Из ***Примера 5.23*** известна $\boldsymbol{M_c}$ (для гейта CNOT, включенного наоборот). Матрица (табл. 5.2) для гейта CNOT также известна. Таким образом, известны следующие унитарные матрицы:

$$\boldsymbol{H}^{\{2\}}=\frac{1}{2}\begin{bmatrix}1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\end{bmatrix},$$

$$\boldsymbol{M_c}=\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0\end{bmatrix},\qquad \boldsymbol{M_a}=\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}.$$

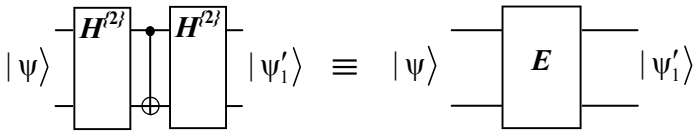
5). Далее, применяя *Правило* 5.4(**2**) (опираясь на ***Пример 5.18***), получим следующую матрицу $\boldsymbol{E}=\boldsymbol{H}^{\{2\}}\times\boldsymbol{M_a}\times\boldsymbol{H}^{\{2\}}$ и две эквивалентные схемы:

$$\boldsymbol{A}=\boldsymbol{M_a}\times\boldsymbol{H}^{\{2\}}=\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}\times\frac{1}{2}\begin{bmatrix}1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\end{bmatrix}=$$

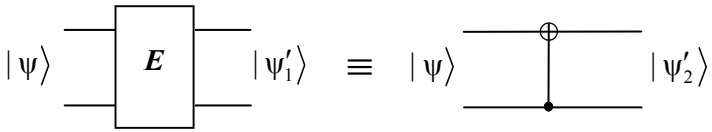
$$=\frac{1}{2}\begin{bmatrix}1+0 & 1+0 & 1+0 & 1+0\\ 1+0 & 0-1 & 1+0 & 0-1\\ 1+0 & 0-1 & 0-1 & 1+0\\ 1+0 & 1+0 & 0-1 & 0-1\end{bmatrix}=\frac{1}{2}\begin{bmatrix}1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & -1 & -1 & 1\\ 1 & 1 & -1 & -1\end{bmatrix},$$

$$\boldsymbol{E}=\boldsymbol{H}^{\{2\}}\times\boldsymbol{A}=\frac{1}{2}\begin{bmatrix}1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\end{bmatrix}\times\frac{1}{2}\begin{bmatrix}1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & -1 & -1 & 1\\ 1 & 1 & -1 & -1\end{bmatrix}=$$

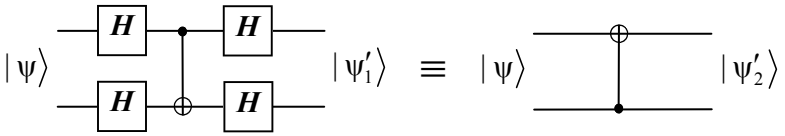
$$= \frac{1}{4}\begin{bmatrix} 4 & 2-2 & 2-2 & 2-2 \\ 2-2 & 2-2 & 2-2 & 4 \\ 2-2 & 2-2 & 4 & 2-2 \\ 2-2 & 4 & 2-2 & 2-2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$



6). Далее, сравнивая матрицу $\boldsymbol{E}$ с матрицей $\boldsymbol{M_c}$, устанавливаем, что они эквивалентны, т.е. $\boldsymbol{E} \equiv \boldsymbol{M_c}$, а значит и эквивалентны следующие две схемы:



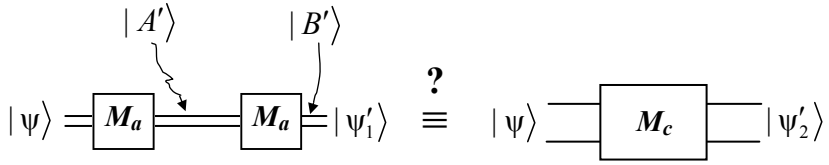
7). Так как $\boldsymbol{E}=\boldsymbol{H}^{\{2\}} \times \boldsymbol{M_a} \times \boldsymbol{H}^{\{2\}}$ и $\boldsymbol{E} \equiv \boldsymbol{M_c}$, то эквивалентны и исходные следующие две квантовые схемы:



8). И тем самым задача решена■

Пример 5.25 (эквивалентная схема на двух кубитах для 2-х CNOT) Известна квантовая схема из 2-х последовательно соединенных двухкубитовых гейтов CNOT (унитарная матрица $\boldsymbol{M_a}$ для CNOT известна).

Требуется определить один двухкубитовый гейт, который эквивалентен этим двум последовательно соединенным двухкубитовым гейтам CNOT. Другими словами, требуется определить унитарную матрицу $\boldsymbol{E_c}$ результирующего преобразования и установить, что следующие две квантовые схемы эквивалентны (где $\boldsymbol{M_c}= \boldsymbol{I}^{\{2\}}$):



Решение

1). В условиях задачи не указан явно вычислительный базис. Будем далее предполагать, что входной вектор $|\psi\rangle$, выходные векторы $|\psi'_1\rangle$, $|\psi'_2\rangle$ и матрицы преобразования $\boldsymbol{M_a}$, $\boldsymbol{E_c}$ и $\boldsymbol{M_c}$ соответствуют одному и тому же вычислительному базису.

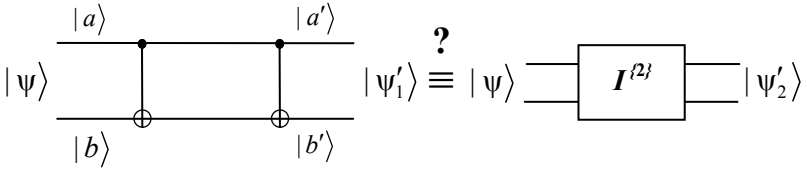
2). Эквивалентность двух схем понимается в том смысле, что при подаче одного и того же входного вектора $|\psi\rangle$ на вход каждой из этих схем на их выходе получается один и тот же выходной вектор, т.е. $|\psi'_1\rangle = |\psi'_2\rangle$, при этом матрица $\boldsymbol{M_c}$ результирующего преобразования является (как и матрица $\boldsymbol{M_a}$) также унитарной. Специально еще раз отметим, что результирующее преобразование с матрицей $\boldsymbol{M_c}$ зависит, вообще говоря, от порядка, в котором выполняются операции с матрицами (т.е. от порядка, в котором выполняются гейты).

3). Таким образом, применяя *Правило* 5.4(**2**), необходимо сначала вычислить матрицу $\boldsymbol{E_c}$, где

$$\boldsymbol{E_c} = \boldsymbol{M_a} \times \boldsymbol{M_a},$$

и затем сравнить $\boldsymbol{E_c}$ с *единичной* матрицей $\boldsymbol{I}^{\{2\}}$. Если $\boldsymbol{E_c}=\boldsymbol{I}^{\{2\}}$, то схемы эквивалентны.

4). Представим исходные квантовые схемы в следующем более (см. рис. 5.20**в**, **г**) конкретном виде:



5). Так как (см. ***Пример 5.16*****г** и табл. 5.2) матрица $\boldsymbol{I}^{\{2\}}$ и матрица для гейта CNOT есть

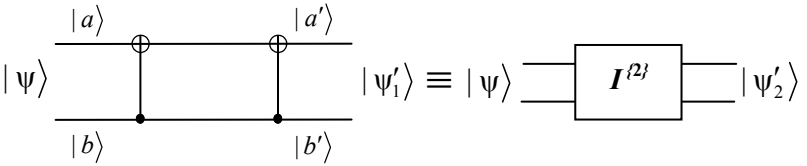
$$\boldsymbol{I}^{\{2\}} = I \otimes I = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \boldsymbol{M_a} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix},$$

то

$$\boldsymbol{E_c} = \boldsymbol{M_a} \times \boldsymbol{M_a} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \times \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} =$$

$$= \begin{bmatrix} 1\cdot 1+0 & 0 & 0 & 0 \\ 0 & 1\cdot 1+0 & 0 & 0 \\ 0 & 0 & 1\cdot 1+0 & 0 \\ 0 & 0 & 0 & 1\cdot 1+0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \boldsymbol{I}^{\{2\}}.$$

6). Отметим, что следующие квантовые схемы тоже эквивалентны:



7). И тем самым задача решена■

Еще раз напомним, что при рассмотрении квантовых схем будем полагать:

кубиты могут быть

- как в *чистом* состоянии,
- так и в *смешанном* (точнее в *перепутанном*) состоянии,

а квантовый регистр (из этих кубитов) только в чистом состоянии.

Из квантовой механики, из содержания главы 2 и раздела 5.3 следует, что:

- при выбранном базисе для любого вектора состояния кубита $|\psi\rangle$ комплексные коэффициенты (т.е. амплитуды) a и b в суперпозиции $|\psi\rangle = a|0\rangle + b|1\rangle$ определяются однозначно;
- базисное состояние ***n***-кубитового регистра можно выбрать в виде $|C_N C_{N-1}...C_0\rangle = |C_N\rangle|C_{N-1}\rangle...|C_0\rangle$, где C_m=0, 1; так, что состояние каждого кубита описывается некоторым вектором состояния и не зависит от состояний остальных кубитов;
- на основании принципа суперпозиции произвольное состояние $|Rg\rangle$ ***n***-кубитового регистра имеет следующий вид ($N=2^n-1$):

  $$|Rg\rangle = a_0|0...00\rangle + a_1|0...01\rangle + ... + a_N|1...11\rangle .$$

  Для такого состояния, вообще говоря, вектор состояния квантового регистра не может быть записан как произведение однокубитовых векторов состояний (т.е. этот вектор не имеет факторизованного вида), что означает — квантовое состояние отдельного кубита оказывается *перепутанным* с состояниями других кубитов и не описывается каким-либо кэт-вектором (такое состояние кубита называется *смешанным* состоянием).

Для рассмотрения далее очередных примеров сформулируем следующее важное правило.

Правило 5.7

Пока существует $|\psi_i\rangle$ *— вектор состояния каждого* ***i****–го кубита из квантового регистра, где* ***i*** *изменяется от* 1 *до* ***n*** *(т.е. пока этот кубит находится в* ***чистом*** *состоянии), его дальнейшую «судьбу» после применения очередного гейта можно отслеживать как по его текущему вектору* $|\psi_i\rangle$*, так и по текущему вектору квантового регистра* $|Rg\rangle$.

После того как ***i****–й кубит перешел в* ***смешанное*** *состояние (т.е. у него теперь нет вектора* $|\psi_i\rangle$*), то его дальнейшую «судьбу» после применения очередного гейта следует отслеживать по текущему вектору квантового регистра* $|Rg\rangle$.

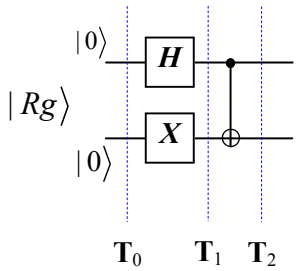
После того как ***i****–й кубит вновь перейдет в* ***чистое*** *состояние (т.е. у него опять есть вектор* $|\psi_i\rangle$*), то его дальнейшую «судьбу» после применения очередного гейта опять можно отслеживать как по его текущему вектору* $|\psi_i\rangle$*, так и по текущему вектору квантового регистра* $|Rg\rangle$ ■

Данное правило позволяет в конкретной ситуации прослеживать «судьбу» кубита, т.е. выполнять над ним преобразования с помощью гейтов и анализировать результат этого преобразования. Основной смысл этого правила состоит в том, что, несмотря на то, в каком состоянии находится отдельный кубит (в смешанном или чистом), следует продолжать применять к нему необходимые гейты (в соответствии с квантовой схемой), а текущий результат контролировать в зависимости от состояния кубита, т.е. либо только по вектору $|Rg\rangle$, либо по $|Rg\rangle$ и вектору состояния кубитов.

Следующий пример показывает, как можно применять это правило.

Пример 5.26 (два кубита в смешанном состоянии на выходе) Имеется следующая исходная двухкубитовая квантовая схема **Ы** (унитарная матрица $\boldsymbol{M}_1$ для гейта $\boldsymbol{H}$, унитарная матрица $\boldsymbol{M}_2$ для гейта $\boldsymbol{X}$ и унитарная матрица $\boldsymbol{M}_3$ для CNOT — известны):

Схема Ы



$$\boldsymbol{M}_1=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix},\quad \boldsymbol{M}_2=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix},$$

$$\boldsymbol{M}_3=\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}$$

Проведем подробное исследование этой квантовой схемы.

1). В исходной квантовой схеме имеются два кубита (верхний кубит с номером **1**, а нижний кубит с номером **2**). Первый кубит находится в базисном состоянии, т.е. $|\psi_1\rangle=|0\rangle$. Второй кубит также находится в базисном состоянии, т.е. $|\psi_2\rangle=|0\rangle$. На эти два кубита действует квантовая схема, содержащая гейт $\boldsymbol{H}$, гейт $\boldsymbol{X}$ и гейт CNOT, причем гейт включен так, что первый (верхний) кубит является *управляющим*, а второй (нижний) кубит — *управляемым* (т.е. верхний кубит управляет нижним кубитом).

2). Будем далее предполагать, что входной вектор $|Rg\rangle$, промежуточные векторы состояний, выходной вектор $|Rg'\rangle$ и все матрицы преобразования соответствуют одному и тому же вычислительному базису:

$$|0\rangle=\begin{bmatrix}1\\ 0\end{bmatrix},\quad |1\rangle=\begin{bmatrix}0\\ 1\end{bmatrix}.$$

3). Применим *Правило* 5.0**б**, результат ***Примера 5.15*****а** и получим следующие векторы вычислительного базиса:

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \quad |01\rangle = |0\rangle \otimes |1\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix},$$

$$|10\rangle = |1\rangle \otimes |0\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \quad |11\rangle = |1\rangle \otimes |1\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}.$$

Таким образом, исходное состояние квантового регистра есть

$$|Rg\rangle = |\psi_1\rangle \otimes |\psi_2\rangle = |0\rangle \otimes |0\rangle = |00\rangle = |0\rangle \otimes |0\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}.$$

4). Определим состояния кубитов $|\psi_1\rangle$, $|\psi_2\rangle$ и состояние самого квантового регистра $|Rg^{x}\rangle$, где $\boldsymbol{x}$=0, 1, 2, …, в различные моменты времени $\mathbf{T}_x$, отмеченные на схеме **Ы** как $\mathbf{T}_0$, $\mathbf{T}_1$ и $\mathbf{T}_2$.

В момент $\mathbf{T}_0$

$$|\psi_1\rangle = |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |\psi_2\rangle = |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix},$$

$$|Rg^{\mathbf{0}}\rangle = |00\rangle = |0\rangle \otimes |0\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix},$$

т.е. кубиты и квантовый регистр находятся в *чистом* состоянии.

В момент $\mathbf{T}_1$

$$|\psi_1\rangle = \boldsymbol{M}_1\ |0\rangle = \boldsymbol{H}\ |0\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\times\begin{bmatrix}1\\ 0\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\ 1\end{bmatrix},$$

$$|\psi_2\rangle = \boldsymbol{M}_2\ |0\rangle = \boldsymbol{X}\ |0\rangle = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\times\begin{bmatrix}1\\ 0\end{bmatrix} = \begin{bmatrix}0\\ 1\end{bmatrix} = |1\rangle,$$

$$|Rg^{\mathbf{1}}\rangle = |\psi_1\rangle\otimes|\psi_2\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\ 1\end{bmatrix}\otimes\begin{bmatrix}0\\ 1\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\cdot\begin{bmatrix}0\\ 1\end{bmatrix}\\ 1\cdot\begin{bmatrix}0\\ 1\end{bmatrix}\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}0\\ 1\\ 0\\ 1\end{bmatrix},$$

т.е. кубиты и квантовый регистр находятся в *чистом* состоянии.

В момент $\mathbf{T}_2$

$$|\psi_1\rangle = \mathbf{?}$$

$$|\psi_2\rangle = \mathbf{?}$$

$$|Rg^{\mathbf{2}}\rangle = \boldsymbol{M}_3\times|Rg^{\mathbf{1}}\rangle =$$

$$= \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}\times\frac{1}{\sqrt{2}}\begin{bmatrix}0\\ 1\\ 0\\ 1\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}0\\ 1\\ 1\\ 0\end{bmatrix}.$$

Применим *Правило* 5.5, опираясь на ***Пример 5.19***. Учтя, что

$$|a|^{\mathbf{2}}+|b|^{\mathbf{2}}=1$$

и

$$|c|^{\mathbf{2}}+|d|^{\mathbf{2}}=1,$$

составим и решим следующую систему уравнений:

$$|\tilde{\psi}\rangle = |\psi_1\rangle \otimes |\psi_2\rangle = \begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} c \\ d \end{bmatrix} =$$

$$= \begin{bmatrix} a\begin{bmatrix} c \\ d \end{bmatrix} \\ b\begin{bmatrix} c \\ d \end{bmatrix} \end{bmatrix} = \begin{bmatrix} ac \\ ad \\ bc \\ bd \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = |Rg^2\rangle$$

или

$$\begin{cases} \sqrt{2}ac = 0 \\ \sqrt{2}ad = 1 \\ \sqrt{2}bc = 1 \\ \sqrt{2}bd = 0 \end{cases}, \qquad (*)$$

Далее, поскольку для комплексных z и w справедливо, что

$$|zw| = |z|\,|w|,$$

то

$|ac|^2 = |a|^2\,|c|^2 = 0$; $\quad |ad|^2 = |a|^2\,|d|^2 = 0.5$;

$|bc|^2 = |b|^2\,|c|^2 = 0.5$; $\quad |bd|^2 = |b|^2\,|d|^2 = 0$;

или либо $|a|^2 = 0$, либо $|c|^2 = 0$, при этом $|ad|^2 = 0.5$ и $|bc|^2 = 0.5$.

Далее,

если $|a|^2 = 0$, то $|ad|^2 \neq 0.5$ (противоречие);

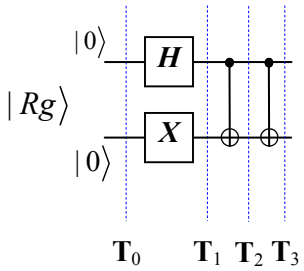
если $|c|^2 = 0$, то $|bc|^2 \neq 0.5$ (противоречие).

Таким образом, получается, что составленная система уравнений (*) не имеет решения в комплексных числах, а значит, выходной вектор $|Rg^2\rangle$ квантового регистра не факторизуем,

т.е. кубиты находятся в *смешанном* состоянии (у них нет векторов состояния), а сам квантовый регистр находится в *чистом* состоянии, так как у него есть вектор состояния.

5). Дополним исходную квантовую схему **Ы** еще одним гейтом CNOT, как показано на следующей схеме **Ю**:

Схема Ю



6). Определим состояния кубитов $|\psi_1\rangle$, $|\psi_2\rangle$ и состояние самого квантового регистра $|Rg^x\rangle$, где x=0, 1, 2, …, в различные моменты времени, отмеченные на схеме **Ю** как $\mathbf{T}_0$, $\mathbf{T}_1$, $\mathbf{T}_2$ и $\mathbf{T}_3$.

В моменты $\mathbf{T}_0$, $\mathbf{T}_1$ и $\mathbf{T}_2$ расчет этих состояний полностью совпадает с расчетом, выполненным ранее для схемы **Ы**.

В момент $\mathbf{T}_3$

$$|\psi_1\rangle = ?$$

$$|\psi_2\rangle = ?$$

$$|Rg^3\rangle = M_3 \times |Rg^2\rangle =$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \times \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}.$$

Применим *Правило* 5.5, опираясь на ***Пример 5.19***. Учтя, что

$$|a|^2+|b|^2=1$$

и

$$|c|^2+|d|^2=1,$$

составим и решим следующую систему уравнений:

$$|\tilde{\psi}\rangle = |\psi_1\rangle \otimes |\psi_2\rangle =$$

$$= \begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} a\begin{bmatrix} c \\ d \end{bmatrix} \\ b\begin{bmatrix} c \\ d \end{bmatrix} \end{bmatrix} = \begin{bmatrix} ac \\ ad \\ bc \\ bd \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} = |Rg^3\rangle$$

или

$$\begin{cases} \sqrt{2}ac = 0 \\ \sqrt{2}ad = 1 \\ \sqrt{2}bc = 0 \\ \sqrt{2}bd = 1 \end{cases}. \qquad (**)$$

Далее, решая эту систему уравнений (**) аналогично, как в ***Примере 5.20***, (получим одно из возможных) следующее ее решение:

$$a = \frac{1}{\sqrt{2}}, \quad b = \frac{1}{\sqrt{2}}, \quad c = 0, \quad d = 1$$

или

$$|\psi_1\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \quad |\psi_2\rangle = |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

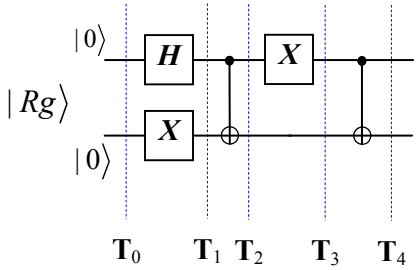
и

$$|Rg^3\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix},$$

т.е. кубиты и квантовый регистр находятся в *чистом* состоянии. Отметим (см. схему **Ю**), что справедливо $(CNOT)^2 = I$.

7). Дополним исходную квантовую схему **Ы** еще одним гейтом ***X*** и гейтом CNOT, как показано на следующей схеме **Я**:

Схема Я



8). Определим состояния кубитов $|\psi_1\rangle$, $|\psi_2\rangle$ и состояние самого квантового регистра $|Rg^x\rangle$, где x=0, 1, 2, …, в различные моменты времени, отмеченные на схеме **Я** как $\mathbf{T}_0$, $\mathbf{T}_1$, $\mathbf{T}_2$ и $\mathbf{T}_3$, $\mathbf{T}_4$.

В моменты $\mathbf{T}_0$, $\mathbf{T}_1$, $\mathbf{T}_2$ расчет этих состояний совпадает с расчетом, выполненным ранее для схемы **Ы**.

В момент $\mathbf{T}_3$

$$|\psi_1\rangle = \mathbf{?}$$

$$|\psi_2\rangle = \mathbf{?}$$

Кубиты находятся в смешанном состоянии, поэтому применим *Правило* 5.0**в**, *Правило* 5.7 и вычислим вектор состояния квантового регистра $|Rg^3\rangle$ по его состоянию $|Rg^2\rangle$ и матрице $X \otimes I$ следующим образом:

$$|Rg^3\rangle = \{X \otimes I\} \times |Rg^2\rangle = \left\{ \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \otimes I \right\} \times |Rg^2\rangle =$$

$$= \begin{bmatrix} 0 \cdot I & 1 \cdot I \\ 1 \cdot I & 0 \cdot I \end{bmatrix} \times |Rg^2\rangle = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \times \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}.$$

Применим *Правило* 5.5, опираясь на ***Пример 5.19***. Учтя, что

$$|a|^2+|b|^2=1 \quad \text{и} \quad |c|^2+|d|^2=1,$$

составим и решим следующую систему уравнений:

$$|\tilde{\psi}\rangle = |\psi_1\rangle \otimes |\psi_2\rangle = \begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} c \\ d \end{bmatrix} =$$

$$= \begin{bmatrix} a\begin{bmatrix} c \\ d \end{bmatrix} \\ b\begin{bmatrix} c \\ d \end{bmatrix} \end{bmatrix} = \begin{bmatrix} ac \\ ad \\ bc \\ bd \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = |Rg^3\rangle$$

или

$$\begin{cases} \sqrt{2}ac = 1 \\ \sqrt{2}ad = 0 \\ \sqrt{2}bc = 0 \\ \sqrt{2}bd = 1 \end{cases}. \qquad (***)$$

Далее, поскольку для комплексных z и w справедливо, что

$$|zw|=|z|\,|w|,$$

то

$$|ac|^2=|a|^2\,|c|^2=0.5; \qquad |ad|^2=|a|^2\,|d|^2=0;$$

$$|bc|^2=|b|^2\,|c|^2=0; \qquad |bd|^2=|b|^2\,|d|^2=0.5;$$

или либо $|a|^2=0$, либо $|d|^2=0$, при этом $|ac|^2=0.5$ и $|bd|^2=0.5$.

Далее,

если $|a|^2=0$, то $|ac|^2\neq 0.5$ (противоречие);

если $|d|^2=0$, то $|bd|^2\neq 0.5$ (противоречие).

Таким образом, получается, что составленная система уравнений (***) не имеет решения в комплексных числах, а значит, выходной вектор $|Rg^3\rangle$ квантового регистра не факторизуем, т.е. кубиты находятся в *смешанном* состоянии (у них нет векторов состояния), а сам квантовый регистр находится в *чистом* состоянии, так как у него есть вектор состояния.

В момент $\mathbf{T}_4$

$$|\psi_1\rangle = ?$$

$$|\psi_2\rangle = ?$$

Кубиты находятся в смешанном состоянии, поэтому применим *Правило* 5.7 и вычислим вектор состояния квантового регистра $|Rg^4\rangle$ по состоянию $|Rg^3\rangle$ и матрице $\boldsymbol{M}_3$ следующим образом:

$$|Rg^4\rangle = \boldsymbol{M}_3 \times |Rg^3\rangle =$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \times \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}.$$

Применим *Правило* 5.5, опираясь на ***Пример 5.19***. Учтя, что

$$|a|^2+|b|^2 = 1$$

и

$$|c|^2+|d|^2=1,$$

составим и решим следующую систему уравнений:

$$|\tilde{\psi}\rangle = |\psi_1\rangle \otimes |\psi_2\rangle =$$

$$= \begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} a \begin{bmatrix} c \\ d \end{bmatrix} \\ b \begin{bmatrix} c \\ d \end{bmatrix} \end{bmatrix} = \begin{bmatrix} ac \\ ad \\ bc \\ bd \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} = |Rg^4\rangle$$

или

$$\begin{cases} \sqrt{2}ac = 1 \\ \sqrt{2}ad = 0 \\ \sqrt{2}bc = 1 \\ \sqrt{2}bd = 0 \end{cases}. \qquad (****)$$

Далее, решая эту систему уравнений (****) аналогично, как в ***Примере 5.20***, (получим одно из возможных) следующее ее решение:

$$a = \frac{1}{\sqrt{2}}, \quad b = \frac{1}{\sqrt{2}},$$

$$c = 1, \quad d = 0$$

или

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}, \quad |\psi_2\rangle = |0\rangle = \begin{bmatrix}1\\0\end{bmatrix}$$

и

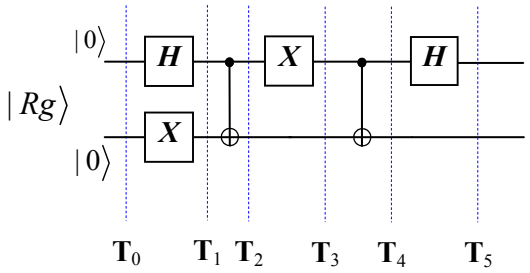
$$|Rg^4\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\1\\0\end{bmatrix},$$

т.е. кубиты и квантовый регистр находятся в *чистом* состоянии, так как каждый кубит и сам квантовый регистр имеют каждый свой вектор состояния.

Таким образом, повторное применение в квантовой схеме гейта CNOT позволило распутать ранее полученное с помощью другого уже гейта CNOT *запутанное* состояние двух кубитов.

9). Теперь дополним квантовую схему **Я** еще одним гейтом ***H***, как показано на следующей схеме **Э**:

Схема Э



10). Определим состояния кубитов $|\psi_1\rangle$, $|\psi_2\rangle$ и состояние самого квантового регистра $|Rg^x\rangle$, где x=0, 1, 2, …, в различные моменты времени, отмеченные на схеме **Э** как $\mathbf{T}_0$, $\mathbf{T}_1$, $\mathbf{T}_2$, $\mathbf{T}_3$, $\mathbf{T}_4$, $\mathbf{T}_5$. В моменты $\mathbf{T}_0$, $\mathbf{T}_1$, $\mathbf{T}_2$, $\mathbf{T}_3$, $\mathbf{T}_4$, $\mathbf{T}_5$ расчет этих состояний полностью совпадает с расчетом, выполненным ранее для схемы **Я**.

В момент $\mathbf{T}_5$

$$|\psi_1\rangle = \boldsymbol{M}_1 \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix} = \boldsymbol{H}\frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix} =$$

$$= \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} \times \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix} = \frac{1}{2}\begin{bmatrix}1+1\\1-1\end{bmatrix} = \frac{1}{2}\begin{bmatrix}2\\0\end{bmatrix} = \begin{bmatrix}1\\0\end{bmatrix} = |0\rangle,$$

$$|\psi_2\rangle = I|0\rangle = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} \times \begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}1\\0\end{bmatrix} = |0\rangle,$$

$$|Rg^5\rangle = |\psi_1\rangle \otimes |\psi_2\rangle = \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}1\cdot\begin{bmatrix}1\\0\end{bmatrix}\\ 0\cdot\begin{bmatrix}1\\0\end{bmatrix}\end{bmatrix} = \begin{bmatrix}1\\0\\0\\0\end{bmatrix},$$

т.е. кубиты и квантовый регистр находятся в *чистом* состоянии.

11). Заметим, что, подав на вход квантовой схемы **Э** $|0\rangle$ и $|0\rangle$, на выходе получаются те же состояния кубитов $|0\rangle$ и $|0\rangle$, при этом состояние квантового регистра, что на входе квантовой схемы и что и на ее выходе, одно и то же и есть

$$|Rg^{\mathbf{5}}\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}.$$

Это наталкивает на мысль, что квантовая схема **Э**, наверно, эквивалентна тождественному преобразованию с единичной матрицей. Проверим это следующим образом:

вычислим матрицу результирующего преобразования

$$\boldsymbol{M}_{00} = \{H \otimes I\} \times \boldsymbol{M}_3 \times \{X \otimes I\} \times \boldsymbol{M}_3 \times \{H \otimes X\},$$

где

$$H \otimes X = \frac{1}{\sqrt{2}} \begin{bmatrix} X & X \\ X & -X \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{bmatrix},$$

$$X \otimes I = \begin{bmatrix} 0 & I \\ I & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix},$$

$$H \otimes I = \frac{1}{\sqrt{2}} \begin{bmatrix} I & I \\ I & -I \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix},$$

тогда

$$v = \boldsymbol{M}_3 \times \{H \otimes X\} =$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \times \frac{1}{\sqrt{2}} \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix},$$

$$y = \{X \otimes I\} \times v =$$

$$= \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \times \frac{1}{\sqrt{2}} \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix},$$

$$z = \boldsymbol{M}_3 \times y =$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \times \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix},$$

$$\boldsymbol{M}_{00} = \{H \otimes I\} \times z =$$

$$= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \times \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix},$$

т.е. получилась не совсем единичная матрица (так как один и тот же результат можно получить разными матрицами).

12). На этом закончим рассмотрение данного примера ■

Прежде чем рассмотреть очередное правило для квантовой схемотехники, вернемся вновь к унитарной матрице гейта, реализующего некоторое унитарное преобразование.

В унитарных матрицах, которые мы рассматриваем, строки и столбцы нумеруются слева направо и сверху вниз, а сама нумерация представляется как

$$00\ldots0,\ 00\ldots1,\ \ldots,\ 11\ldots1,$$

причем самый нижний провод на квантовой схеме соответствует именно самому младшему биту.

На рис. 5.22, 5.23 представлены следующие матрицы:

$$\begin{bmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{bmatrix}, \quad \begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{bmatrix}.$$

На рис. 5.22 представлена в общем виде унитарная матрица для однокубитового гейта, а на рис. 5.23 — для двухкубитового гейта.

Состояния $|\mathbf{0}\rangle$, $|\mathbf{1}\rangle$ (для однокубитовых схем) или $|\mathbf{00}\rangle$, $|\mathbf{01}\rangle$, $|\mathbf{10}\rangle$, $|\mathbf{11}\rangle$ (для двухкубитовых схем) являются базисными состояниями и к тому же они, как правило, являются и *вычислительным базисом*. На рис. 5.22, 5.23 столбцы соответствуют базисным векторам на выходе гейта. Например, если на вход однокубитового гейта поступил вектор $|\psi\rangle$, который есть базисный вектор $|\mathbf{1}\rangle$, т.е. $|\psi\rangle = |\mathbf{1}\rangle$ (рис. 5.22), то на выходе этого гейта будет выходной вектор $|\psi'\rangle$ из базисных векторов с амплитудами в соответствующем столбце, т.е. $|\psi'\rangle = a_{01}|\mathbf{0}\rangle + a_{11}|\mathbf{1}\rangle$. Аналогичное справедливо и для двухкубитового гейта. Например, если на вход двухкубитового гейта поступил базисный вектор $|\psi\rangle = |\mathbf{01}\rangle$ (рис. 5.23), то на выходе этого гейта будет выходной вектор $|\psi'\rangle$ из базисных векторов с амплитудами в соответствующем столбце, т.е.

$$|\psi'\rangle = a_{01}|\mathbf{00}\rangle + a_{11}|\mathbf{01}\rangle + a_{21}|\mathbf{10}\rangle + a_{31}|\mathbf{11}\rangle.$$

Унитарная матрица для однокубитового гейта

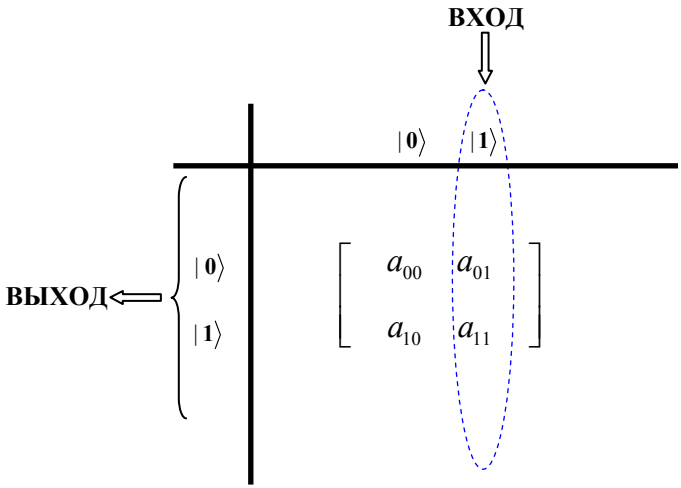


Рис. **5.22**

Унитарная матрица для двухкубитового гейта

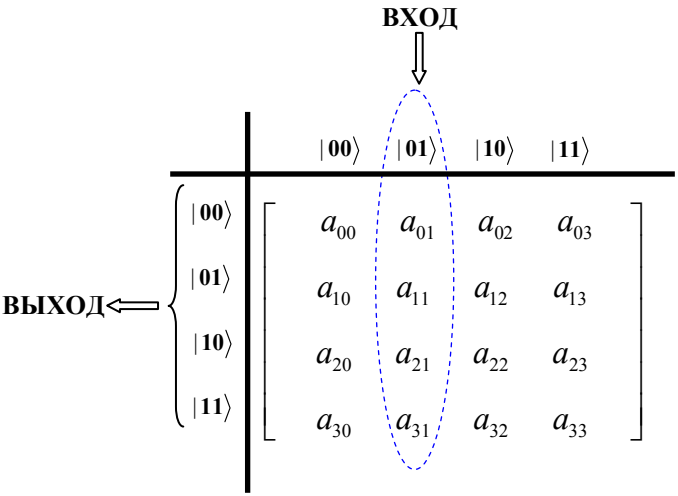


Рис. **5.23**

Из квантовой механики, из работы *П. Шора* [12, с. 211], из содержания главы 2 и данного раздела следует, что:

- тождественное преобразование с единичной унитарной матрицей $\boldsymbol{I}^{\{n\}}$ не изменяет вектора $|\psi_i\rangle$ состояния ***i***–го кубита или квантового регистра $|Rg\rangle$;
- если применяется гейт (с унитарной матрицей ***M***) к двум кубитам большого вектора состояния квантового регистра $|Rg\rangle$ (предполагается, что квантовая схема состоит более чем из двух кубитов), то для каждого базисного вектора следует применять преобразование этого гейта, изменяющее состояние только этих двух кубитов согласно матрице ***M*** и не затрагивающее состояния других кубитов квантового регистра (это полностью соответствует умножению полного вектора состояния $|Rg\rangle$, на тензорное произведение матрицы ***M*** этого гейта, действующего на два кубита, и единичных матриц ***I*** оставшихся кубитов).

Для многокубитовых схем (т.е. квантовых схем с числом кубитов больше двух) сформулируем следующее важное правило.

Правило 5.8

Если в многокубитовой схеме (т.е. в квантовой схеме, в которой число кубитов квантового регистра больше двух) применяется двухкубитовый гейт (с унитарной матрицей ***M***) к состояниям двух кубитов (предполагается, что квантовый регистр находится в состоянии $|Rg\rangle$), то для каждого базисного вектора следует применять преобразование этого гейта, изменяющее состояние только этих двух кубитов согласно матрице ***M*** и не затрагивающее состояния других кубитов в этом базисном состоянии ■

Данное правило позволяет относительно быстро вычислять новый вектор состояния квантового регистра.

Следующий сокращенный пример показывает, как можно применять это правило.

Пример 5.27 (три кубита и состояние квантового регистра [12])
Имеется некоторая трехкубитовая квантовая схема. Унитарная матрица ***M*** для двухкубитового гейта известна:

$$\boldsymbol{M} = \frac{1}{\sqrt{2}} \begin{bmatrix} \sqrt{2} & 0 & 0 & 0 \\ 0 & \sqrt{2} & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}.$$

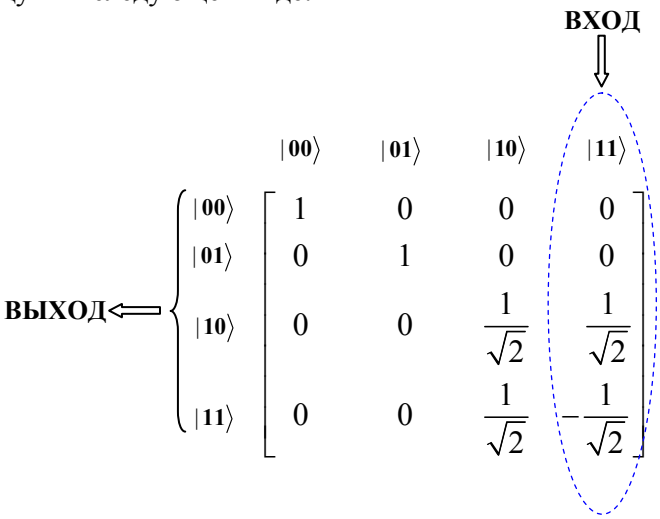
Известен также исходный вектор состояния квантового регистра

$$|Rg\rangle = |110\rangle.$$

Требуется определить состояние квантового регистра $|Rg'\rangle$ на выходе квантовой схемы, т.е. после применения этого двухкубитового гейта с унитарной матрицей ***M*** к первым двум кубитам.

Решение

1). Применим *Правило* 5.8, а для этого представим унитарную матрицу ***M*** в следующем виде:



2). На основании принципа суперпозиции произвольное состояние $|Rg\rangle$ рассматриваемого n-кубитового регистра при $N=2^n-1$ имеет вид ($n=3$, $N=7$):

$$|Rg\rangle = a_0|0...00\rangle + a_1|0...01\rangle + ... + a_N|1...11\rangle$$

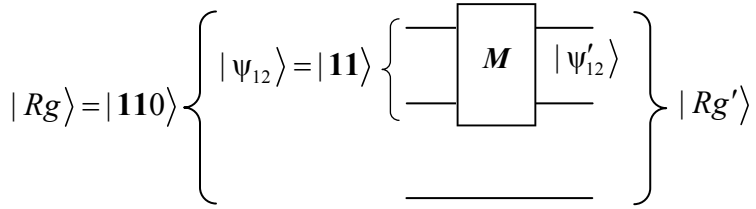
или

$$|Rg\rangle = a_0|000\rangle + a_1|001\rangle + a_2|010\rangle + a_3|011\rangle + \\ = a_4|100\rangle + a_5|101\rangle + a_6|110\rangle + a_7|111\rangle .$$

В данном случае $|Rg\rangle = |110\rangle$, т.е. имеем следующие амплитуды для входного состояния квантового регистра:

$$a_0=a_1=a_2=a_3=a_4=a_5=a_7=0, \quad a_6=1.$$

3). По условию задачи квантовая схема содержит 3 кубита, 1 двухкубитовый гейт, действующий на 2 первых кубита, а исходное состояние квантового регистра есть $|Rg\rangle = |\mathbf{110}\rangle$. Тогда квантовая схема может быть представлена следующим образом:



4). Так как $|Rg\rangle = |\mathbf{110}\rangle$, то $|\psi_{12}\rangle = |\mathbf{11}\rangle$, т.е. два первых кубита находятся в состоянии $|\mathbf{11}\rangle$, тогда согласно матрице $\boldsymbol{M}$ на вход гейта поступает состояние $|\mathbf{11}\rangle$, а его выход образует состояние

$$|\psi'_{12}\rangle = 0|\mathbf{00}\rangle + 0|\mathbf{01}\rangle + \frac{1}{\sqrt{2}}|\mathbf{10}\rangle - \frac{1}{\sqrt{2}}|\mathbf{11}\rangle = \frac{1}{\sqrt{2}}|\mathbf{10}\rangle - \frac{1}{\sqrt{2}}|\mathbf{11}\rangle ,$$

а значит $|Rg'\rangle = \frac{1}{\sqrt{2}}|\mathbf{100}\rangle - \frac{1}{\sqrt{2}}|\mathbf{110}\rangle$,

т.е. состояние 3-го кубита не меняется.

5). И тем самым задача решена■

На этом закончим рассмотрение примеров.

5.7. Двухкубитовая схема алгоритма Дойча

> «По сути, разработка многих квантовых алгоритмов сводится к хитроумному выбору функции и окончательного преобразования, позволяющих эффективно определять полезную глобальную информацию о функции — информацию, которую нельзя быстро получить на классическом компьютере.»
>
> *М. Нильсен, И. Чанг* [1, с.58]

Рассмотрим очень важный пример одного из *упрощенных* и *усовершенствованных* вариантов [1, с.56-58] квантового алгоритма *Д. Дойча* для двух кубитов. Именно этот вариант легко может быть масштабирован на большее число кубитов (т.е. на многоразрядную логическую функцию *f*).

Алгоритм решает следующую задачу для булевой функции *f*, отображающей {0, 1} в себя.

Существуют только следующие 4 функции [7, с.53]:

постоянные

$$f_1(0)=f_1(1)=0;$$

$$f_2(0)=f_2(1)=1;$$

сбалансированные

$$f_3(0)=0,\ f_3(1)=1;$$

$$f_4(0)=1,\ f_4(1)=0.$$

Под *сбалансированной* функцией f понимается [1, с.58] такая функция, которая для одной половины всех возможных своих аргументов принимает значение 1 и принимает значение 0 для другой половины своих аргументов.

Имеется возможность вычислить значение функции только один раз. Случайно выбирается одна из 4 функций, но не известно, какая именно.

Ставится задача определить, что это за отобранная функция, т.е. является ли она *сбалансированной* или *постоянной.*

Специально еще раз отметим, что в классическом случае для определения такого глобального свойства функции f требуется вычислить как значение $f(1)$, так и значение $f(0)$, что как, очевидно, потребует дважды вычислять значение этой функции.

Данная задача допускает следующую простую [13, с.131] интерпретацию с монетой.

В подлинной монете на одной стороне изображена *решка*, а на другой стороне — *орел*. В фальшивой монете на каждой стороне изображен *орел.* Для того чтобы определить подлинность монеты, необходимо посмотреть на монету дважды, т.е. один раз с одной стороны, а второй раз — с другой стороны. Таким образом, в классическом случае необходимо выполнить измерение дважды.

С помощью квантовых вычислений при решении этой задачи уже потребуется только **однократное** вычисление значения функции (т.е. в схеме используется только 1 гейт $\boldsymbol{U}_f$, вычисляющий f).

Теория алгоритма Дойча и его обобщения изложены в разделе 3.1

Квантовая схема, решающая эту задачу (см. [1, с.56-58; 13, с.132; 14, с.147]), представлена на рис. 5.24. На этой схеме показаны два однокубитовых регистра. Первый (верхний) кубит является регистром данных $\boldsymbol{x}$ для аргумента функции $f(\boldsymbol{x})$, а второй (нижний) кубит является регистром значений $\boldsymbol{y}$, т.е. результат $(\boldsymbol{y} \oplus f(\boldsymbol{x}))$ для гейта $\boldsymbol{U}_f$.

Квантовая схема для алгоритма Дойча на 2-х кубитах

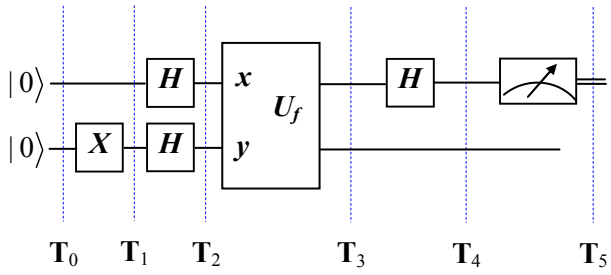


Рис. **5.24**

Проведем подробное исследование (см. рис. 5.24) этой квантовой схемы.

1). В исходной квантовой схеме имеются два кубита (верхний кубит с номером **1**, а нижний кубит с номером **2**).

Первый кубит находится в базисном состоянии, т.е. $|\psi_1\rangle = |0\rangle$. Второй кубит также находится в базисном состоянии, т.е. $|\psi_2\rangle = |0\rangle$. На эти два кубита действует квантовая схема, содержащая три гейта ***H***, гейт ***X*** и гейт $\boldsymbol{U_f}$, а также измерительный элемент для измерения состояния первого кубита. В данной квантовой схеме каждый кубит является однокубитовым регистром, при этом оба этих кубита (т.е. регистра) представляют *квантовую систему* из двух кубитов (регистров), которую будем называть *составным* регистром, а состояние этого *составного* регистра будем обозначать как $|Rg\rangle$, причем входной вектор и есть исходное состояние *составного* регистра, а выходной вектор есть конечное состояние *составного* регистра.

2). Будем далее предполагать, что входной вектор $|Rg\rangle$, промежуточные векторы состояний, выходной вектор $|Rg'\rangle$ и все матрицы преобразования соответствуют одному и тому же вычислительному базису:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

3). Применим *Правило* 5.0**б**, результат ***Примера 5.15*****а** и получим следующие векторы вычислительного базиса:

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \quad |01\rangle = |0\rangle \otimes |1\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix},$$

$$|10\rangle = |1\rangle \otimes |0\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \quad |11\rangle = |1\rangle \otimes |1\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}.$$

Таким образом, исходное состояние $|Rg\rangle$ *составного* регистра есть

$$|Rg\rangle = |\psi_1\rangle \otimes |\psi_2\rangle = |0\rangle \otimes |0\rangle = |00\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}.$$

4). Определим состояния кубитов $|\psi_1^{\,m}\rangle$, $|\psi_2^{\,m}\rangle$ и состояние самого *составного* регистра $|Rg^{m}\rangle$, где m=0, 1, 2, …, в различные моменты времени $\mathbf{T}_m$, отмеченные на схеме (рис. 5.24) как $\mathbf{T}_0$, $\mathbf{T}_1$, $\mathbf{T}_2$, $\mathbf{T}_3$, $\mathbf{T}_4$, $\mathbf{T}_5$. В моменты $\mathbf{T}_0$, $\mathbf{T}_1$, $\mathbf{T}_2$ эти состояния одинаковы и не зависят от различных унитарных матриц гейта $\boldsymbol{U}_f$.

В момент $\mathbf{T}_0$

$$|\psi_1^{\,0}\rangle = |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |\psi_2^{\,0}\rangle = |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix},$$

$$|Rg^{0}\rangle = |00\rangle = |0\rangle \otimes |0\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix},$$

т.е. кубиты и квантовый регистр находятся в *чистом* состоянии.

В момент $\mathbf{T}_1$

$$|\psi_1^{\,1}\rangle = |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |\psi_2^{\,1}\rangle = \boldsymbol{X}|0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \times \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle,$$

$$|Rg^{1}\rangle = |\psi_1^{\,1}\rangle \otimes |\psi_2^{\,1}\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix} \\ 0 \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix},$$

т.е. кубиты и квантовый регистр находятся в *чистом* состоянии.

В момент $\mathbf{T}_2$

$$|\psi_1^{\,2}\rangle = \boldsymbol{H}\,|0\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\times\begin{bmatrix}1\\ 0\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\ 1\end{bmatrix},$$

$$|\psi_2^{\,2}\rangle = \boldsymbol{H}\,|1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\times\begin{bmatrix}0\\ 1\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\ -1\end{bmatrix},$$

$$|Rg^{\boldsymbol{2}}\rangle = |\psi_1^{\,2}\rangle\otimes|\psi_2^{\,2}\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\ 1\end{bmatrix}\otimes\frac{1}{\sqrt{2}}\begin{bmatrix}1\\ -1\end{bmatrix} = \frac{1}{2}\begin{bmatrix}1\cdot\begin{bmatrix}1\\ -1\end{bmatrix}\\ 1\cdot\begin{bmatrix}1\\ -1\end{bmatrix}\end{bmatrix} = \frac{1}{2}\begin{bmatrix}1\\ -1\\ 1\\ -1\end{bmatrix},$$

т.е. кубиты и квантовый регистр находятся в *чистом* состоянии.

5). Для того чтобы определить состояния кубитов $|\psi_1^{\,\boldsymbol{m}}\rangle$, $|\psi_2^{\,\boldsymbol{m}}\rangle$ и состояние *составного* квантового регистра $|Rg^{\boldsymbol{m}}\rangle$, где $\boldsymbol{m}$=3, 4, 5, т.е. в различные моменты времени, отмеченные на квантовой схеме (рис. 5.24) как $\mathbf{T}_3$, $\mathbf{T}_4$, $\mathbf{T}_5$, получим конкретный вид 4-х унитарных матриц $\boldsymbol{M}_1$, $\boldsymbol{M}_2$, $\boldsymbol{M}_3$, $\boldsymbol{M}_4$ гейта $\boldsymbol{U}_f$ соответственно для каждой булевой функции $f_1(\boldsymbol{x})$, $f_2(\boldsymbol{x})$, $f_3(\boldsymbol{x})$, $f_4(\boldsymbol{x})$.

В ***Примере 5.22*** (***Примере 5.15*****в**) с использованием *Правила* 5.6 найдена (для $f_3(0)=0$, $f_3(1)=1$) следующая матрица:

$$\boldsymbol{M}_3 = \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix},$$

которая в точности совпадает с матрицей для квантового элемента CNOT и является матрицей для гейта $\boldsymbol{U}_f$ с $f_3(\boldsymbol{x})$.

Поступая аналогичным образом и применяя *Правило* 5.6 с учетом $f_1(0)=f_1(1)=0$ и требований к матрице $\boldsymbol{M_1}$

$$\boldsymbol{M}|00\rangle=|00\rangle,\ \ \boldsymbol{M}|01\rangle=|01\rangle,\ \ \boldsymbol{M}|10\rangle=|10\rangle,\ \ \boldsymbol{M}|11\rangle=|11\rangle,$$

может быть найдена следующая матрица:

$$\boldsymbol{M_1}=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix},$$

которая в точности совпадает с матрицей $\boldsymbol{I}$ для тождественного преобразования и является матрицей для гейта $\boldsymbol{U}_f$ с $f_1(\boldsymbol{x})$.

Поступая аналогичным образом и применяя *Правило* 5.6 с учетом $f_2(0)=f_2(1)=1$ и требований к матрице $\boldsymbol{M_2}$

$$\boldsymbol{M}|00\rangle=|01\rangle,\ \ \boldsymbol{M}|01\rangle=|00\rangle,\ \ \boldsymbol{M}|10\rangle=|11\rangle,\ \ \boldsymbol{M}|11\rangle=|10\rangle,$$

может быть найдена следующая матрица:

$$\boldsymbol{M_2}=\begin{bmatrix}0&1&0&0\\1&0&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}=\begin{bmatrix}1&0\\0&1\end{bmatrix}\otimes\begin{bmatrix}0&1\\1&0\end{bmatrix}=\boldsymbol{I}\otimes\boldsymbol{X},$$

которая является матрицей $\boldsymbol{M_2}$ для гейта $\boldsymbol{U}_f$ с $f_2(\boldsymbol{x})$.

Поступая аналогичным образом и применяя *Правило* 5.6 с учетом $f_4(0)=1$, $f_4(1)=0$ и требований к матрице $\boldsymbol{M_4}$

$$\boldsymbol{M}|00\rangle=|01\rangle,\ \ \boldsymbol{M}|01\rangle=|00\rangle,\ \ \boldsymbol{M}|10\rangle=|10\rangle,\ \ \boldsymbol{M}|11\rangle=|11\rangle,$$

может быть найдена следующая матрица:

$$\boldsymbol{M_4} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \boldsymbol{M_3} \times \boldsymbol{M_2},$$

которая является матрицей $\boldsymbol{M_4}$ для гейта $\boldsymbol{U_f}$ с $f_4(\boldsymbol{x})$.

6). Продолжим определять состояния кубитов $|\psi_1^{\boldsymbol{m}}\rangle$, $|\psi_2^{\boldsymbol{m}}\rangle$ и состояние самого *составного* регистра $|Rg^{\boldsymbol{m}}\rangle$, где $\boldsymbol{m}$=3, 4, 5 в различные моменты времени, отмеченные на схеме (рис. 5.24) как $\mathbf{T}_3$, $\mathbf{T}_4$, $\mathbf{T}_5$. В моменты $\mathbf{T}_0$, $\mathbf{T}_1$, $\mathbf{T}_2$ эти состояния одинаковы и не зависят от различных унитарных матриц гейта $\boldsymbol{U_f}$.

В момент $\mathbf{T}_3$ (матрица $\boldsymbol{M_1}$)

$$|\psi_1^{\,3}\rangle = ?$$

$$|\psi_2^{\,3}\rangle = ?$$

$$|Rg^{3}\rangle = \boldsymbol{M_1} \times |Rg^{2}\rangle =$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \times \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1+0 \\ -1+0 \\ 1+0 \\ -1+0 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \end{bmatrix},$$

применим *Правило* 5.5, получим разложение вектора $|Rg^{3}\rangle$

$$|Rg^{3}\rangle = |\psi_1^{\,3}\rangle \otimes |\psi_2^{\,3}\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \otimes \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix},$$

$$|\psi_1{}^3\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix},$$
$$|\psi_2{}^3\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}.$$

В момент $\mathbf{T}_3$ (матрица $\boldsymbol{M_2}$)

$$|\psi_1{}^3\rangle = ?$$

$$|\psi_2{}^3\rangle = ?$$

$$|Rg^3\rangle = \boldsymbol{M_2} \times |Rg^2\rangle =$$
$$= \begin{bmatrix}0&1&0&0\\1&0&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix} \times \frac{1}{2}\begin{bmatrix}1\\-1\\1\\-1\end{bmatrix} = \frac{1}{2}\begin{bmatrix}-1+0\\1+0\\-1+0\\1+0\end{bmatrix} = \frac{1}{2}\begin{bmatrix}-1\\1\\-1\\1\end{bmatrix},$$

применим *Правило* 5.5, получим разложение вектора $|Rg^3\rangle$

$$|Rg^3\rangle = |\psi_1{}^3\rangle \otimes |\psi_2{}^3\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix} \otimes \frac{1}{\sqrt{2}}\begin{bmatrix}-1\\1\end{bmatrix},$$
$$|\psi_1{}^3\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix},$$
$$|\psi_2{}^3\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}-1\\1\end{bmatrix}.$$

В момент $\mathbf{T}_3$ (матрица $\boldsymbol{M_3}$)

$$|\psi_1{}^3\rangle = ?$$

$$|\psi_2{}^3\rangle = ?$$

$$|Rg^3\rangle = \boldsymbol{M_3} \times |Rg^2\rangle =$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \times \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1+0 \\ -1+0 \\ -1+0 \\ 1+0 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ -1 \\ 1 \end{bmatrix},$$

применим *Правило* 5.5, получим разложение вектора $|Rg^3\rangle$

$$|Rg^3\rangle = |\psi_1{}^3\rangle \otimes |\psi_2{}^3\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} \otimes \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix},$$

$$|\psi_1{}^3\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix},$$

$$|\psi_2{}^3\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}.$$

В момент $\mathbf{T}_3$ (матрица $\boldsymbol{M_4}$)

$$|\psi_1{}^3\rangle = ?$$

$$|\psi_2{}^3\rangle = ?$$

$$|Rg^3\rangle = \boldsymbol{M_4} \times |Rg^2\rangle =$$

$$= \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \times \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} -1+0 \\ 1+0 \\ 1+0 \\ -1+0 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} -1 \\ 1 \\ 1 \\ -1 \end{bmatrix},$$

применим *Правило* 5.5, получим разложение вектора $|Rg^3\rangle$

$$|Rg^3\rangle = |\psi_1{}^3\rangle \otimes |\psi_2{}^3\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix} \otimes \frac{1}{\sqrt{2}}\begin{bmatrix}-1\\1\end{bmatrix},$$

$$|\psi_1{}^3\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix},$$

$$|\psi_2{}^3\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}-1\\1\end{bmatrix}.$$

В момент $\mathbf{T}_4$ (матрица $\boldsymbol{M_1}$)

$$|\psi_1{}^4\rangle = \boldsymbol{H}\,|\psi_1{}^3\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix} \times \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix} = \frac{1}{2}\begin{bmatrix}1+1\\1-1\end{bmatrix} = \begin{bmatrix}1\\0\end{bmatrix} = |0\rangle,$$

$$|\psi_2{}^4\rangle = |\psi_2{}^3\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix},$$

$$|Rg^4\rangle = |\psi_1{}^4\rangle \otimes |\psi_2{}^4\rangle = \begin{bmatrix}1\\0\end{bmatrix} \otimes \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\\0\\0\end{bmatrix}.$$

В момент $\mathbf{T}_4$ (матрица $\boldsymbol{M_2}$)

$$|\psi_1{}^4\rangle = \boldsymbol{H}\,|\psi_1{}^3\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix} \times \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix} = \frac{1}{2}\begin{bmatrix}1+1\\1-1\end{bmatrix} = \begin{bmatrix}1\\0\end{bmatrix} = |0\rangle,$$

$$|\psi_2{}^4\rangle = |\psi_2{}^3\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}-1\\1\end{bmatrix},$$

$$|Rg^4\rangle = |\psi_1{}^4\rangle \otimes |\psi_2{}^4\rangle = \begin{bmatrix}1\\0\end{bmatrix} \otimes \frac{1}{\sqrt{2}}\begin{bmatrix}-1\\1\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}-1\\1\\0\\0\end{bmatrix}.$$

В момент $\mathbf{T}_4$ (матрица $\boldsymbol{M_3}$)

$$|\psi_1^{\,4}\rangle = \boldsymbol{H}\,|\psi_1^{\,3}\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\times\frac{1}{\sqrt{2}}\begin{bmatrix}1\\ -1\end{bmatrix} = \frac{1}{2}\begin{bmatrix}1-1\\ 1+1\end{bmatrix} = \begin{bmatrix}0\\ 1\end{bmatrix} = |1\rangle,$$

$$|\psi_2^{\,4}\rangle = |\psi_2^{\,3}\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\ -1\end{bmatrix},$$

$$|Rg^{4}\rangle = |\psi_1^{\,4}\rangle\otimes|\psi_2^{\,4}\rangle = \begin{bmatrix}0\\ 1\end{bmatrix}\otimes\frac{1}{\sqrt{2}}\begin{bmatrix}1\\ -1\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}0\\ 0\\ 1\\ -1\end{bmatrix}.$$

В момент $\mathbf{T}_4$ (матрица $\boldsymbol{M_4}$)

$$|\psi_1^{\,4}\rangle = \boldsymbol{H}\,|\psi_1^{\,3}\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\times\frac{1}{\sqrt{2}}\begin{bmatrix}1\\ -1\end{bmatrix} = \frac{1}{2}\begin{bmatrix}1-1\\ 1+1\end{bmatrix} = \begin{bmatrix}0\\ 1\end{bmatrix} = |1\rangle,$$

$$|\psi_2^{\,4}\rangle = |\psi_2^{\,3}\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}-1\\ 1\end{bmatrix},$$

$$|Rg^{4}\rangle = |\psi_1^{\,4}\rangle\otimes|\psi_2^{\,4}\rangle = \begin{bmatrix}0\\ 1\end{bmatrix}\otimes\frac{1}{\sqrt{2}}\begin{bmatrix}-1\\ 1\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}0\\ 0\\ -1\\ 1\end{bmatrix}.$$

В момент $\mathbf{T}_5$ (матрица $\boldsymbol{M_1}$ или $\boldsymbol{M_2}$)
с вероятностью 1 измерение покажет
для 1-го кубита состояние $|0\rangle$.

В момент $\mathbf{T}_5$ (матрица $\boldsymbol{M_3}$ или $\boldsymbol{M_4}$)
с вероятностью 1 измерение покажет
для 1-го кубита состояние $|1\rangle$.

Отметим, что само измерение, вообще говоря, влияет на состояние кубита.

6). Сведем полученные результаты в следующую табл. 5.3.

Таблица 5.3. Состояния кубитов в алгоритме *Д. Дойча*

Функция	Момент времени		
	$\mathbf{T}_4$		$\mathbf{T}_5$
	1-й кубит	2-й кубит	1-й кубит
f_1	$\|0\rangle$	$+\left\{\frac{1}{\sqrt{2}}\|0\rangle-\frac{1}{\sqrt{2}}\|1\rangle\right\}$	С вероятностью 1 (после измерения) кубит будет обнаружен в состоянии $\|0\rangle$
f_2	$\|0\rangle$	$-\left\{\frac{1}{\sqrt{2}}\|0\rangle-\frac{1}{\sqrt{2}}\|1\rangle\right\}$	
f_3	$\|1\rangle$	$+\left\{\frac{1}{\sqrt{2}}\|0\rangle-\frac{1}{\sqrt{2}}\|1\rangle\right\}$	С вероятностью 1 (после измерения) кубит будет обнаружен в состоянии $\|1\rangle$
f_4	$\|1\rangle$	$-\left\{\frac{1}{\sqrt{2}}\|0\rangle-\frac{1}{\sqrt{2}}\|1\rangle\right\}$	

Эта таблица позволяет уже получить окончательное решающее правило.

7). Таким образом, для определения свойства функции можно предложить следующее решающее правило:

- если измерение состояния 1-го (верхнего) кубита (т.е. регистра данных) показало, что состояние этого кубита $|0\rangle$, то функция $f(\boldsymbol{x})$ является постоянной;
- если измерение состояния 1-го (верхнего) кубита (т.е. регистра данных) показало, что состояние этого кубита $|1\rangle$, то функция $f(\boldsymbol{x})$ является сбалансированной.

8). И тем самым задача решена ■

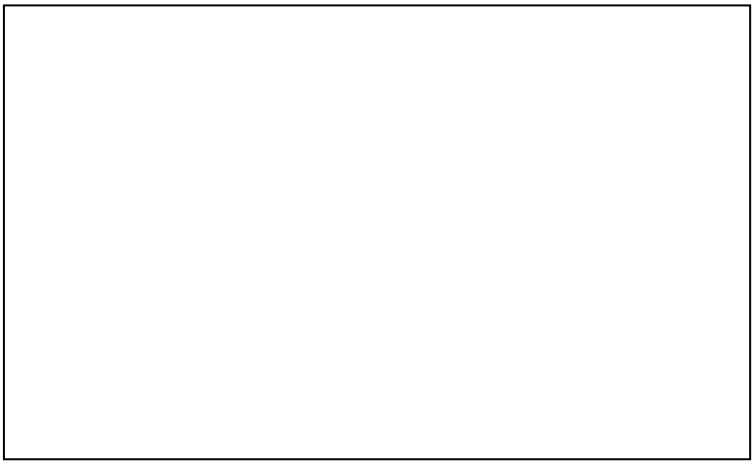
Краткие методические замечания для квантового алгоритма *Д. Дойча* на двух кубитах

Наиболее существенное замечание связано с гейтом $\boldsymbol{U}_f$, реализующим вычисление одной из 4-х, но нам не известной функции $f(\boldsymbol{x})$. Обычно предполагают (см. [1, с.55-57; 14, с.146]), что $\boldsymbol{U}_f$ — некоторый «*черный ящик*», или другое его название *оракул*, содержимое которого нам по какой-то причине недоступно. Оракул может выдавать значение функции для любого допустимого значения на его входе. В каком-то смысле оракул может быть представлен как некоторая программа для ЭВМ. Эту программу можно запускать на ЭВМ и вычислять значения функции (но какая из 4-х функций $f_1(\boldsymbol{x})$, $f_2(\boldsymbol{x})$, $f_3(\boldsymbol{x})$ или $f_4(\boldsymbol{x})$ реализована в этой программе, нам не известно). Исходный текст этой программы или то, как она работает, нам также не известны (не доступны). Причины этого могут быть разные, например **юридические** (существующие нормативные документы не всегда разрешают восстанавливать исходный текст программы путем *дизассемблирования* исполняемого кода) или **технические** (исходный текст сложен и очень запутан, и нет механического способа [14, с.150] узнать, какая в ней реализована функция быстрее, чем запустить эту программу на ЭВМ достаточное число раз и по результатам работы этой программы сделать вывод о реализованной в ней функции).

Действительно, ниже представлен следующий исходный текст программы **fun1** на языке Си:

```
Int fun1(x)
  int x;
 {
     double otvet;
           x=0;        /вычисление функции/
           otvet=x
     return(otvet);
 }
```

Программисту достаточно одного беглого взгляда на этот текст программы, чтобы сразу понять, что эта программа при любых исходных значениях выдает на выход только 0, т.е. в программе реализована именно функция $f_1(\boldsymbol{x})$. Однако следующий исходный текст не столь очевиден:



Даже очень опытный программист будет испытывать затруднение в интерпретации этого вырожденного исходного текста, представленного пустым множеством символов (чистый, белый лист бумаги). Этот исходный текст есть модифицированная программа **VACUUM** [15] на специальном языке программирования. Знание о том, что делает эта программа, доступна создателю [15] программы, а не нам (поэтому для нас она представляется как «*черный ящик*»).

Можно отметить, что эта программа на специальном языке программирования, реализует именно функцию $f_2(\boldsymbol{x})$. Для того чтобы на практике определить, какую функцию реализует программа, необходимо достаточное число раз (т.е. 2 раза) запустить ее на ЭВМ, зафиксировать выдаваемые ею результаты и по ним уже сделать вывод о реализованной в программе функции.

В заключение необходимо отметить, что рассматриваемый алгоритм *Д. Дойча* был успешно реализован (см. работу [13]) на практике экспериментальным путем на молекуле хлороформа при использовании ЯМР.

5.8. Трех- и более кубитовые схемы

> «…состояние составной системы, не представимое в виде произведения состояний входящих в эту систему компонент, является *запутанным*. По причинам, которые до конца не ясны, запутанные состояния играют ключевую роль в квантовых вычислениях и обработке квантовой информации.»
>
> *М. Нильсен, И. Чанг* [1, с.133]

Многокубитовые (т.е. трех- и более кубитовые) схемы, которые будем далее рассматривать, содержат следующие компоненты:

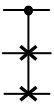
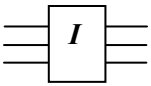
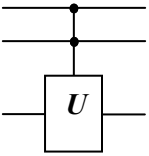
- три или более кубита;
- набор одно- , двухкубитовых гейтов;
- набор трехкубитовых гейтов;
- квантовые провода;
- специальные графические символы на квантовых проводах;
- измеритель (иногда на квантовых схемах не показывают).

В табл. 5.4 приведены условные обозначения наиболее распространенных квантовых элементов (трехкубитовых гейтов).

Черная точка (для гейтов из табл. 5.4) означает то же самое, что и для двухкубитовых гейтов (эти точки обозначают управляющие кубиты). Управляемый кубит (в данном случае он изображен как самый нижний кубит) подвергается операции, когда управляющие кубиты (в данном случае они изображены как два самых верхних кубита и обозначены этими черными точками) находятся оба в состоянии $|1\rangle$. В элементе *Фредкина* черная точка (на линии управляющего кубита) означает, что выполняется управляемый обмен между двумя самыми нижними кубитами, когда самый верхний кубит находится в состоянии $|1\rangle$.

Аналогично, как и для двухкубитовых гейтов, можно ввести обозначение в виде светлого кружка (вместо черного), означающее, что управляемый кубит (т.е. самый нижний кубит) подвергается операции, например, **НЕ** (в элементе *Тоффоли*) или операции $\boldsymbol{U}$ (в элементе $C^2\boldsymbol{U}$), когда управляющие кубиты (т.е. два самых верхних кубита) находится в состоянии $|0\rangle$).

Таблица 5.4. Трехкубитовые гейты (см. [1, с.16-17] и др.)

Наименование гейта	**Возможное условное обозначение**	**Унитарная матрица гейта**
Элемент *Тоффоли*		$\begin{bmatrix} \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} \\ 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 \end{bmatrix}$
Элемент *Фредкина*		$\begin{bmatrix} \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 \\ 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} \end{bmatrix}$
Элемент *Тождественного преобразования*		$\begin{bmatrix} \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} \end{bmatrix}$
Элемент $C^2\boldsymbol{U}$		$\begin{bmatrix} \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \boldsymbol{A} & \boldsymbol{B} \\ 0 & 0 & 0 & 0 & 0 & 0 & \boldsymbol{C} & \boldsymbol{D} \end{bmatrix}$, $U = \begin{bmatrix} \boldsymbol{A} & \boldsymbol{B} \\ \boldsymbol{C} & \boldsymbol{D} \end{bmatrix}$

В главе 2 было рассмотрено очень важное теоретическое положение. Все двухкубитовые гейты (операции) могут быть представлены (построены) с помощью **только** однокубитовых гейтов (преобразований) и двухкубитовых гейтов CNOT. Было показано, что трехкубитовые гейты (и многокубитовые) могут быть также представлены (построены) с помощью **только** однокубитовых преобразований и фундаментального гейта CNOT. Опираясь на это, можно сформулировать следующее важное правило для многокубитовых квантовых схем.

Правило 5.9

Любую многокубитовую схему (т.е. в квантовую схему, в которой число кубитов квантового регистра больше двух) можно синтезировать, используя **только** 2 типа гейтов — однокубитовые гейты и двухкубитовые гейты CNOT ■

Для многокубитовых схем (т.е. квантовых схем с числом кубитов больше двух) сформулируем еще аналогично *Правилу* 5.8 следующее важное правило.

Правило 5.10

Если в многокубитовой схеме (т.е. в квантовой схеме, в которой число кубитов квантового регистра больше двух) применяется n-й кубитовый гейт, где $n>2$ (с унитарной матрицей M) к состояниям n кубитов (предполагается, что квантовый регистр имеет состояние $|Rg\rangle$), то для каждого базисного вектора следует применять преобразование этого гейта, изменяющее состояние только этих n кубитов согласно матрице M и не затрагивающее состояния других кубитов в этом базисном состоянии ■

Данное правило позволяет относительно быстро вычислять новый вектор состояния квантового регистра.

Сокращенные примеры (рассмотренные ниже) кратко покажут, как можно применять некоторые введенные правила.

Воспользовавшись результатами глав 2, 3, можно выполнять прямой анализ, обратный анализ и синтез квантовых схем, содержащих многокубитовые гейты. Соответствующие некоторые примеры и необходимые приемы были разобраны ранее.

В случае трех- и более кубитовых схем следует поступать аналогично, как в случае меньшего числа кубитов.

Так, если требуется решить задачу прямого анализа для квантовой схемы с числом кубитов больше 2, можно поступить, например, следующим образом. Вычислить (опираясь на *Правило* 5.0**в**, *Правила* 5.4(**1**), 5.4(**2**)) матрицу результирующего преобразования (если она не известна из условия задачи) и затем, применяя необходимым образом *Правила* 5.0 **а**, **б** и с учетом *Правила* 5.7, 5.8, 5,10 уже вычислить выходной вектор квантового регистра (и если есть возможность, то вычислить векторы состояний отдельных кубитов). В отличие от квантовых схем с малым числом кубитов задача обратного анализа для квантовой многокубитовой схемы с числом кубитов больше 2 представляет уже некоторую трудность в ее решении, но при этом известно как надо ее решать.

Для решения обратной задачи можно поступать аналогично, как это было сделано при решении подобных задач с малым числом кубитов. Для этого надо знать унитарную матрицу результирующего преобразования для данной квантовой схемы. Зная эту матрицу и выходной вектор квантового регистра, необходимо составить соответствующую этим данным систему уравнений и затем попытаться решить ее. Если решение найдено, то входной вектор будет известен. Затем надо факторизовать его и попытаться найти векторы состояний отдельных кубитов. Если отдельные векторы кубитов существуют, то состояния этих кубитов есть чистое состояние, а если векторы отдельных кубитов не существуют, то это будет означать, что состояния этих кубитов есть смешанное состояние.

Для решения задачи синтеза можно поступать так же, как при решении задач с малым числом кубитов. Эта задача в общем виде пока далека от своего окончательного решения, так как представляет серьезную проблему в области квантовых вычислений.

Многокубитовая схема алгоритма Дойча была достаточно подробно рассмотрена в главе 3 и поэтому далее она не обсуждается. Далее остановимся на примерах, опирающихся на унитарные матрицы и матричное исчисление.

Пример 5.28 (построение конкретной унитарной матрицы)
Известны требования к унитарной матрице $\boldsymbol{M}$ размером 8×8 в виде

$$\boldsymbol{M}|000\rangle = |000\rangle,\ \boldsymbol{M}|001\rangle = |001\rangle,$$
$$\boldsymbol{M}|010\rangle = |010\rangle,\ \boldsymbol{M}|011\rangle = |011\rangle,$$
$$\boldsymbol{M}|100\rangle = a|100\rangle + c|101\rangle,\ \boldsymbol{M}|101\rangle = b|100\rangle + d|101\rangle,$$
$$\boldsymbol{M}|110\rangle = a|110\rangle + c|111\rangle,\ \boldsymbol{M}|111\rangle = b|110\rangle + d|111\rangle,$$

где $|000\rangle$, $|001\rangle$, $|010\rangle$, $|011\rangle$, $|100\rangle$, $|101\rangle$, $|110\rangle$, $|111\rangle$ — это вычислительный базис 3-х кубитов (базисные векторы), а

$$|0\rangle = \begin{bmatrix}1\\0\end{bmatrix},\quad |1\rangle = \begin{bmatrix}0\\1\end{bmatrix},\quad V = \begin{bmatrix}a & b\\ c & d\end{bmatrix},\quad V^{\dagger}V = I\,.$$

Требуется определить унитарную матрицу $\boldsymbol{M}$.

Решение

1). Пусть $\boldsymbol{E}$ имеет представление

$$\boldsymbol{E} = (e_{ik}),$$

где $\boldsymbol{i}$ =0, 2, …, 7; $\boldsymbol{k}$ =0, 2, …, 7.

2). Применим *Правило* 5.6 и будем искать решение, т.е. элементы некоторой матрицы $\boldsymbol{E}$ как решение следующей системы из 8 уравнений:

$$\begin{cases}
\boldsymbol{E}|000\rangle = |000\rangle,\\
\boldsymbol{E}|001\rangle = |001\rangle,\\
\boldsymbol{E}|010\rangle = |010\rangle,\\
\boldsymbol{E}|011\rangle = |011\rangle,\\
\boldsymbol{E}|100\rangle = a|100\rangle + c|101\rangle,\\
\boldsymbol{E}|101\rangle = b|100\rangle + d|101\rangle,\\
\boldsymbol{E}|110\rangle = a|110\rangle + c|111\rangle,\\
\boldsymbol{E}|111\rangle = b|110\rangle + d|111\rangle.
\end{cases}$$

Если решение этой системы уравнений не существует (e_{ik}, — комплексные числа и элементы матрицы $\boldsymbol{E}$), то не существует и самой матрицы $\boldsymbol{M}$. Отметим, что если подматрица V унитарна, то решение существует (см. ранее сделанный комментарий к задачам синтеза унитарного преобразования).

3). Так как

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix},$$

то, опираясь на ***Пример 5.15*а,** по аналогии следует, что базисные векторы

$$|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle$$

могут быть представлены в виде

$$|000\rangle = |0\rangle \otimes |0\rangle \otimes |0\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, |001\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, |010\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, |011\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix},$$

$$|100\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, |101\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, |110\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}, |111\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix},$$

а сама система уравнений может быть записана следующим образом:

$$\begin{cases} \begin{bmatrix} e_{00} \\ e_{10} \\ e_{20} \\ e_{30} \\ e_{40} \\ e_{50} \\ e_{60} \\ e_{70} \end{bmatrix} = \begin{bmatrix} \mathbf{1} \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} e_{01} \\ e_{11} \\ e_{21} \\ e_{31} \\ e_{41} \\ e_{51} \\ e_{61} \\ e_{71} \end{bmatrix} = \begin{bmatrix} 0 \\ \mathbf{1} \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} e_{02} \\ e_{12} \\ e_{22} \\ e_{32} \\ e_{42} \\ e_{52} \\ e_{62} \\ e_{72} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \mathbf{1} \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} e_{03} \\ e_{13} \\ e_{23} \\ e_{33} \\ e_{43} \\ e_{53} \\ e_{63} \\ e_{73} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \mathbf{1} \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \\ \begin{bmatrix} e_{04} \\ e_{14} \\ e_{24} \\ e_{34} \\ e_{44} \\ e_{54} \\ e_{64} \\ e_{74} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ \boldsymbol{a} \\ \boldsymbol{c} \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} e_{05} \\ e_{15} \\ e_{25} \\ e_{35} \\ e_{45} \\ e_{55} \\ e_{65} \\ e_{75} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ \boldsymbol{b} \\ \boldsymbol{d} \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} e_{06} \\ e_{16} \\ e_{26} \\ e_{36} \\ e_{46} \\ e_{56} \\ e_{66} \\ e_{76} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ \boldsymbol{a} \\ \boldsymbol{c} \end{bmatrix}, \begin{bmatrix} e_{07} \\ e_{17} \\ e_{27} \\ e_{37} \\ e_{47} \\ e_{57} \\ e_{67} \\ e_{77} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ \boldsymbol{b} \\ \boldsymbol{d} \end{bmatrix}. \end{cases}$$

4). Таким образом, найдено следующее решение для матрицы $\boldsymbol{E}$:

$$\boldsymbol{E} = \begin{bmatrix} \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \boldsymbol{a} & \boldsymbol{b} & 0 & 0 \\ 0 & 0 & 0 & 0 & \boldsymbol{c} & \boldsymbol{d} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \boldsymbol{a} & \boldsymbol{b} \\ 0 & 0 & 0 & 0 & 0 & 0 & \boldsymbol{c} & \boldsymbol{d} \end{bmatrix}.$$

5). Для найденной матрицы $\boldsymbol{E}$ проверим свойство унитарности, т.е. $\boldsymbol{E}\boldsymbol{E}^{\dagger} = \boldsymbol{E}^{\dagger}\boldsymbol{E} = I$.

$$E^{\dagger}E =$$

$$= \left\{ \begin{bmatrix} \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \boldsymbol{a} & \boldsymbol{b} & 0 & 0 \\ 0 & 0 & 0 & 0 & \boldsymbol{c} & \boldsymbol{d} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \boldsymbol{a} & \boldsymbol{b} \\ 0 & 0 & 0 & 0 & 0 & 0 & \boldsymbol{c} & \boldsymbol{d} \end{bmatrix} \right\}^{\dagger} \times \begin{bmatrix} \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \boldsymbol{a} & \boldsymbol{b} & 0 & 0 \\ 0 & 0 & 0 & 0 & \boldsymbol{c} & \boldsymbol{d} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \boldsymbol{a} & \boldsymbol{b} \\ 0 & 0 & 0 & 0 & 0 & 0 & \boldsymbol{c} & \boldsymbol{d} \end{bmatrix} =$$

$$= \left[\begin{array}{cccc|cccc} \mathbf{1} & & \mathbf{0} & & & & & \\ & \mathbf{1} & & & & & & \\ \mathbf{0} & & \mathbf{1} & & & & & \\ & & & \mathbf{1} & & & & \\ \hline & & & & a^{*} & c^{*} & & \\ & \mathbf{0} & & & b^{*} & d^{*} & & \mathbf{0} \\ & & & & & & a^{*} & c^{*} \\ & & & & & & b^{*} & d^{*} \end{array}\right] \times \left[\begin{array}{cccc|cccc} \mathbf{1} & & \mathbf{0} & & & & & \\ & \mathbf{1} & & & & & & \\ \mathbf{0} & & \mathbf{1} & & & & & \\ & & & \mathbf{1} & & & & \\ \hline & & & & a & b & & \\ & \mathbf{0} & & & c & d & & \mathbf{0} \\ & & & & & & a & b \\ & & & & & & c & d \end{array}\right] =$$

$$= \left[\begin{array}{cccc|cccc} \mathbf{1} & & \mathbf{0} & & & & & \\ & \mathbf{1} & & & & & & \\ \mathbf{0} & & \mathbf{1} & & & & & \\ & & & \mathbf{1} & & & & \\ \hline & & & & \mathbf{1} & 0 & & \\ & \mathbf{0} & & & 0 & \mathbf{1} & & \mathbf{0} \\ & & & & & & \mathbf{1} & 0 \\ & & & & & & 0 & \mathbf{1} \end{array}\right] \equiv I,$$

т.е. свойство унитарности матрицы $\boldsymbol{E}$ выполняется. Так как $\boldsymbol{E}$ унитарна, то она есть искомая матрица, т.е. $\boldsymbol{M}=\boldsymbol{E}$.

6). И тем самым задача решена■

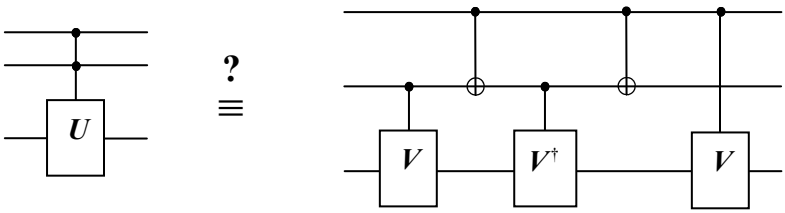
Пример 5.29 (представление 3-кубитового гейта)
Вернемся к главе 2 и рассмотрим (табл. 5.4) 3-кубитовый элемент $C^2(\boldsymbol{U})$ с известной унитарной матрицей $\boldsymbol{M_0}$ размером 8×8 в виде

$$\boldsymbol{M_0}=\left[\begin{array}{cccc:cccc}
\mathbf{1} & & \mathbf{0} & & & & & \\
 & \mathbf{1} & & & & & \mathbf{0} & \\
\mathbf{0} & & \mathbf{1} & & & & & \\
 & & & \mathbf{1} & & & & \\
\hdashline
 & & & & \mathbf{1} & 0 & & \mathbf{0} \\
 & \mathbf{0} & & & 0 & \mathbf{1} & & \\
 & & & & & & w & s \\
 & & & & \mathbf{0} & & z & t
\end{array}\right],$$

где $V^{\mathbf{2}}=U$, $U=\begin{bmatrix} w & s \\ z & t \end{bmatrix}$, $V=\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, U и V — унитарные матрицы с комплексными элементами, где

$$w=a^{\mathbf{2}}+cb;\ \ s=ab+bd;\ \ z=ac+cd;\ \ t=cb+d^{\mathbf{2}}.$$

Требуется установить, что следующие две квантовые схемы эквивалентны:



Решение

1). В условиях задачи не указан явно вычислительный базис. Будем далее предполагать, что входные векторы, выходные векторы, а также и все используемые матрицы преобразования соответствуют одному и тому же вычислительному базису.

2). Эквивалентность двух схем понимается в том смысле, что матрица $\boldsymbol{M_0}$ (гейта $C^2\boldsymbol{U}$) эквивалентна матрице $\boldsymbol{E_c}$ результирующего преобразования пяти гейтов (два гейта имеют матрицу $\boldsymbol{V}$, один гейт матрицу $\boldsymbol{V}^\dagger$ и два гейт CNOT — матрицу $\boldsymbol{M_b}$). Специально еще раз отметим, что результирующее преобразование с матрицей $\boldsymbol{E_c}$ зависит, вообще говоря, от порядка, в котором выполняются операции с матрицами (т.е. от порядка, в котором выполняются гейты).

3). Таким образом, применяя *Правило* 5.0**в** и учитывая *Правило* 5.4(**2**), необходимо сначала найти матрицы $\boldsymbol{M}_1$, $\boldsymbol{M}_2$, $\boldsymbol{M}_3$, $\boldsymbol{M}_4$ для системы из 3-х кубитов и вычислить матрицу $\boldsymbol{E_c}$, где

$$\boldsymbol{E_c}=\boldsymbol{M}_4\times\boldsymbol{M}_2\times\boldsymbol{M}_3\times\boldsymbol{M}_2\times\boldsymbol{M}_1,$$

и затем уже сравнить $\boldsymbol{E_c}$ с матрицей $\boldsymbol{M_0}$. Если $\boldsymbol{E_c}\equiv\boldsymbol{M_0}$, то схемы эквивалентны.

4). Матрица (табл. 5.2) для гейта CNOT есть

$$\boldsymbol{M_b}=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix},$$

матрица для гейта CNOT, с учетом третьего кубита, есть

$$\boldsymbol{M}_2=\boldsymbol{M_b}\otimes\boldsymbol{I}=\boldsymbol{M_b}\otimes\begin{bmatrix}1&0\\0&1\end{bmatrix}=\left[\begin{array}{cc:cc}\mathbf{1}&\mathbf{0}&\mathbf{0}&\\&\mathbf{1}&&\\\mathbf{0}&&\mathbf{1}&\\&&&\mathbf{1}\\\hdashline\multicolumn{2}{c:}{\multirow{2}{*}{$\mathbf{0}$}}&\mathbf{0}&\mathbf{1}\ \ 0\\&&0&\mathbf{1}\\\multicolumn{2}{c:}{}&\mathbf{1}\ \ 0&\\\multicolumn{2}{c:}{}&0\ \ \mathbf{1}&\mathbf{0}\end{array}\right],$$

матрица $\boldsymbol{M}_4$ (см. ***Пример 5.28***) для последнего 2-кубитового гейта в квантовой схеме (с учетом еще одного кубита, который на схеме показан как кубит в середине, т.е. второй кубит) есть

$$\boldsymbol{M}_4=\begin{bmatrix} \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \boldsymbol{a} & \boldsymbol{b} & 0 & 0 \\ 0 & 0 & 0 & 0 & \boldsymbol{c} & \boldsymbol{d} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \boldsymbol{a} & \boldsymbol{b} \\ 0 & 0 & 0 & 0 & 0 & 0 & \boldsymbol{c} & \boldsymbol{d} \end{bmatrix},$$

аналогично, как и для $\boldsymbol{M}_4$, могут быть найдены матрица $\boldsymbol{M}_1$ для гейта с $\boldsymbol{V}$ и матрица $\boldsymbol{M}_3$ для гейта с $\boldsymbol{V}^{\dagger}$, которые представлены следующим образом:

$$\boldsymbol{M}_1=\left[\begin{array}{cccc|cccc} \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & a & b & 0 & 0 & 0 & 0 \\ 0 & 0 & c & d & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & a & b \\ 0 & 0 & 0 & 0 & 0 & 0 & c & d \end{array}\right],$$

$$\boldsymbol{M}_3=\left[\begin{array}{cccc|cccc} \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & a^* & c^* & 0 & 0 & 0 & 0 \\ 0 & 0 & b^* & d^* & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & a^* & c^* \\ 0 & 0 & 0 & 0 & 0 & 0 & b^* & d^* \end{array}\right].$$

5). Тогда для $\boldsymbol{E_c}=\boldsymbol{M}_4\times\boldsymbol{M}_2\times\boldsymbol{M}_3\times\boldsymbol{M}_2\times\boldsymbol{M}_1$ имеем

$$\boldsymbol{E_{00}}=\boldsymbol{M}_2\times\boldsymbol{M}_1=\left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & & & & \\ 0 & 1 & a & b & & & & \\ 0 & 0 & c & d & & & & \\ 0 & 0 & 0 & 1 & & & & \\ \hline & & & & 0 & a & b & \\ & & & & 1 & c & d & \\ & & & & 0 & 0 & 0 & 1 \\ & & & & 0 & 0 & 1 & 0 \end{array}\right],$$

$$\boldsymbol{E_{000}}=\boldsymbol{M}_3\times\boldsymbol{E_{00}}=\left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & & & & \\ 0 & 1 & a & b & & & & \\ 0 & 0 & c & d & & & & \\ 0 & 0 & 0 & 1 & & & & \\ \hline & & & & 0 & a & b & \\ & & & & 1 & c & d & \\ & & & & a^* & c^* & 0 & 0 \\ & & & & b^* & d^* & 0 & 1 \end{array}\right],$$

$$\boldsymbol{E_{0000}}=\boldsymbol{M}_2\times\boldsymbol{E_{000}}=\left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & & & & \\ 0 & 1 & a & b & & & & \\ 0 & 0 & c & d & & & & \\ 0 & 0 & 0 & 1 & & & & \\ \hline & & & & 0 & a & b & \\ & & & & 1 & c & d & \\ & & & & a^* & c^* & 0 & 0 \\ & & & & b^* & d^* & 0 & 1 \end{array}\right],$$

и окончательно получаем следующее выражение:

$$\boldsymbol{E_c} = \boldsymbol{M}_4 \times \boldsymbol{E}_{0000} = \left[\begin{array}{cccc|cc} \mathbf{1} & & \mathbf{0} & & & \\ & \mathbf{1} & & & \multicolumn{2}{c}{\multirow{2}{*}{$\mathbf{0}$}} \\ \mathbf{0} & & \mathbf{1} & & & \\ & & & \mathbf{1} & & \\ \hline & & & & \mathbf{1} & \\ \multicolumn{2}{c|}{\multirow{2}{*}{$\mathbf{0}$}} & & & \mathbf{0} & \\ & & & & \mathbf{0} & w \quad s \\ & & & & & z \quad t \end{array}\right].$$

6). Таким образом, если сравнить матрицу $\boldsymbol{E_c}$ с матрицей $\boldsymbol{M_0}$, то легко заметить, то эти две матрицы идентичны, т.е.

$$\boldsymbol{E_c} \equiv \boldsymbol{M_0}.$$

7). Отметим следующее.

Для нахождения унитарной матрицы $\boldsymbol{M}_4$ с учетом еще одного кубита для 2-кубитовых гейтов была составлена и затем решена система уравнений. Для нахождения $\boldsymbol{M}_1$ или $\boldsymbol{M}_3$ можно поступить по-другому:

$$\boldsymbol{M}_1 = \boldsymbol{I} \otimes \boldsymbol{M_u} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes \left[\begin{array}{cc|cc} \mathbf{1} & & \multicolumn{2}{c}{\multirow{2}{*}{$\mathbf{0}$}} \\ & \mathbf{1} & & \\ \hline \multicolumn{2}{c|}{\multirow{2}{*}{$\mathbf{0}$}} & a & b \\ & & c & d \end{array}\right],$$

$$\boldsymbol{M}_3 = \boldsymbol{I} \otimes \boldsymbol{M_u}^{\dagger} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes \left[\begin{array}{cc|cc} \mathbf{1} & & \multicolumn{2}{c}{\multirow{2}{*}{$\mathbf{0}$}} \\ & \mathbf{1} & & \\ \hline \multicolumn{2}{c|}{\multirow{2}{*}{$\mathbf{0}$}} & a^* & c^* \\ & & b^* & d^* \end{array}\right],$$

где $\boldsymbol{M_u}$ взята из табл. 5.2 для элемента *Управляемое U*.

8). И тем самым задача решена■

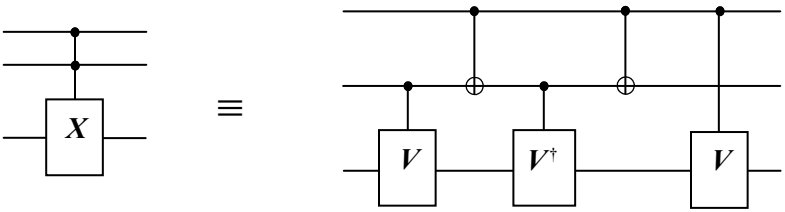
Пример 5.30 (представление 3-кубитового гейта)
Представить элемент *Тоффоли* как квантовую схему, состоящую только из двухкубитовых гейтов.

Решение

1). Можно заметить, что элемент *Тоффоли* (табл. 5.4) — это частный случай 3-кубитового элемента $C^2\boldsymbol{U}$ с известной унитарной матрицей, где $\boldsymbol{U}=\boldsymbol{X}$, а элемент $\boldsymbol{X}$ (см. табл. 5.1) имеет следующую матрицу:

$$\boldsymbol{X}=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}.$$

2). Тогда (см. ***Пример 5.29***) согласно полученному ранее результату следующие две квантовые схемы эквивалентны:



$\boldsymbol{V}^2=U$ или $\boldsymbol{V}^2=\boldsymbol{X}$ или $V=\sqrt{\boldsymbol{X}}=\sqrt{\sigma_1}$.

3). В главе 2 было рассмотрено, как вычислять корень квадратный из $\boldsymbol{X}$ (т.е. из матриц Паули). В итоге можно получить и требуемую матрицу $\boldsymbol{V}$:

$$\boldsymbol{V}=\frac{1-i}{2}\begin{bmatrix}1 & i\\ i & 1\end{bmatrix},$$

$$\boldsymbol{i}=\sqrt{-1}=\exp\left(i\pi/2\right).$$

4). И тем самым задача решена■

На этом завершим такое подробное рассмотрение элементов квантовой схемотехники.

Задачи

a) Докажите (см. [1, с.594]), что $\boldsymbol{ZSXZ} \equiv -\boldsymbol{SX}$.

b) Докажите, что $\boldsymbol{XXX} \equiv \boldsymbol{X}$.

c) Докажите (см. [16, с.8-10]), что $\boldsymbol{Y} \equiv \boldsymbol{i}\{\boldsymbol{XZ}\}$, где $\boldsymbol{i} = \sqrt{-1}$.

d) Докажите (см. [1, с.226]), что $\boldsymbol{XYX} \equiv -\boldsymbol{Y}$.

e) Докажите, что $\boldsymbol{HI} \equiv \boldsymbol{IH} \equiv \boldsymbol{H}$, где $\boldsymbol{I}$ — единичная матрица.

f) Докажите, что для любой квадратной матрицы $\boldsymbol{M}$ с комплексными элементами справедливо $\boldsymbol{MI} \equiv \boldsymbol{IM} \equiv \boldsymbol{M}$, где $\boldsymbol{I}$ — единичная матрица подходящих размеров.

g) Докажите, что $\boldsymbol{XHH} \equiv \boldsymbol{HHX} \equiv \boldsymbol{X}$.

h) Докажите (см. [1, с.590]), что $\boldsymbol{HZ} \equiv \boldsymbol{XH}$.

i) Докажите, что $\boldsymbol{HZH} \equiv \boldsymbol{HHX}$.

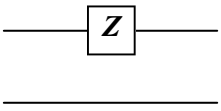
j) Докажите (см. [1, с.225]), что $\boldsymbol{H} \equiv \frac{1}{\sqrt{2}}\{\boldsymbol{X}+\boldsymbol{Z}\}$.

k) Упростите квантовую схему, представленную выражением $\boldsymbol{YY}$ (или, иными словами, чему тождественно выражение $\boldsymbol{YY} \equiv ?$).

l) Покажите, что $\boldsymbol{XHH}$ и $\boldsymbol{HXH}$ приводят, в общем-то, к разному конечному результату, т.е. к разным выходным векторам (при одних и тех же векторах на входе), поскольку эти последовательности умножения матриц соответствуют гейтам, имеющим разные матрицы результирующих преобразований.

m) Есть два кубита, и каждый из них находится в *смешанном* состоянии (т.е. состояние всей системы является *перепутанным* состоянием 2-х кубитов). Известен вектор состояния квантового регистра из этих двух кубитов. К первому кубиту применили гейт $\boldsymbol{X}$. Как изменится вектор состояния квантового регистра?

n) Проверьте, действительно ли квантовая схема **Э** из ***Примера 5.26*** эквивалентна следующей квантовой схеме:



o) Известен[1] вычислительный базис $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$. Известен входной вектор $|\psi\rangle = \frac{1}{5}\begin{bmatrix} 3 \\ 4 \end{bmatrix}$ и квантовая схема в виде одновходового элемента с матрицей преобразования $\boldsymbol{H} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$. Требуется определить $|\psi'\rangle = \begin{bmatrix} A \\ B \end{bmatrix}$ — выходной вектор в этом вычислительном базисе на выходе этой схемы.

p) Известен вычислительный базис $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$. Известен входной вектор $|\psi\rangle = \frac{1}{17}\begin{bmatrix} 15 \\ 8 \end{bmatrix}$ и квантовая схема в виде одновходового элемента с матрицей преобразования $\boldsymbol{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. Требуется определить $|\psi'\rangle = \begin{bmatrix} A \\ B \end{bmatrix}$ — выходной вектор в этом вычислительном базисе на выходе этой схемы.

[1] Эти и им подобные задачи были получены с помощью программного генератора задач, который разработал аспирант МИФИ *К.И. Ткаченко.*

Список используемой литературы (источники)

1. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация.–М.: Мир, 2006.–824с.–(Nielsen M.A., Chuang I.L. Quantum Computation and Quantum Information.–M.: Cambridge University Press, 2000.–704p.).

2. Фейнман Р. Характер физических законов /Пер. с англ.–2-е изд. испр.–М.:Наука, 1987.–160с.

3. Фейнман Р., Хибс А. Квантовая механика и интегралы по траекториям.–М.:Мир, 1968.–383с.

4. Фейнман Р. Моделирование физики на компьютерах //Квантовый компьютер и квантовые вычисления /Пер. с англ. под ред. В.А. Садовничего .–Ижевск: Ред. журн. Регуляр. и хаотич. динам., 1999.–Т.2.–С.96–124.

5. Нильсен М. Правила для сложного квантового мира // В мире науки. – 2003. –№3(март).–(http://www.sciam.ru/2003/3/inform.shtml).

6. Тарасов Л.В. Закономерности окружающего мира. В 3 кн. Кн.3: Эволюция естественно-научного знания.–М.:ФИЗМАТЛИТ, 2004.–440с.

7. Дойч Д., Экерт А., Лупачини Р. Машины, логика и квантовая физика //*Математическое* просвещение, 2001. – Сер.3. – Вып.5. – С.47–60).–(http://files.school-collection.edu.ru/dlrstore/d62fb03e-a780-11dc-945c-d34917fee0be/index.html).– (Deutcsh D., Ekert A., Lupacchini R. Machines, Logic and Quantum Physics //arXiv:math.HO/9911150, v.1, 19 Nov., 1999.–(http://quantum3000.narod.ru/papers/edu/deutcsh_machines.zip).

8. Гантмахер Ф.Р. Теория матриц. –М.:Наука, 1966.–576с.

9. Гельфанд И. М. Лекции по линейной алгебре.–М.:Наука,1966.–280с.

10. Риффель Э., Полак В. Основы квантовых вычислений //Квантовые компьютеры и квантовые вычисления, 2000. – Том 1. – №1. – С.4–57.–(http://ics.org.ru/rus?menu=mi_pubs&abstract=247).

11. Кулик С.Д. Квантовая программа, квантовая база данных и квантовый компьютер //Научная сессия МИФИ-2007. Сборник научных трудов в 17 т. Т.12:Информатика и процессы управления. Компьютерные системы и технологии.–М.: МИФИ, 2007.–Т.12.–С.101-103.

12. Шор П. Полиномиальные по времени алгоритмы разложения числа на простые множители и нахождения дискретного логарифма для квантового компьютера //Квантовый компьютер и квантовые вычисления /Пер. с англ. под ред. В.А. Садовничего . –Ижевск: Ред. журн. Регуляр. и хаотич. динам., 1999. – Т2. – С.200–247. – (Shor P. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer //SIAM Jour. Comp., 1997, v.26, №5, pp.1484-1509).

13. Чанг И., Вандерсипен Л., Жу К., Леюнг Д., Ллойд С. Экспериментальная реализация квантового алгоритма //Квантовые вычисления: за и против. Квантовый компьютер и квантовые вычисления. Том 1 /Пер. с англ. под ред. В.А. Садовничего .–Ижевск: Ред. журн. Регуляр. и хаотич. ди-

нам., Издательский дом Удмуртский университет, 1999.–С.130–140.
14. Физика квантовой информации /Под ред. Д. Боумейстера, А. Экерта, А. Цайлингера /Пер. с англ.–.М.: Постмаркет, 2002.–376с.
15. Кулик С.Д. Свидетельство на программу Российской Федерации №2000610470 "Самая маленькая в мире не классическая программа ВАКУУМ для ЭВМ" (VACUUM) /С.Д. Кулик (Россия).–Заявка №2000610307; Заяв. 04.04.2000;Зарегистр. 02.06.2000. Бюл. №3(32),с.170–172.– (РОСПАТЕНТ).
16. Яковлев В.П., Кондрашин М.П. Элементы квантовой информатики.–М.: МИФИ, 2004.–80с.

Список рекомендуемых источников для самостоятельной работы

1. Яковлев В.П., Кондрашин М.П. Элементы квантовой информатики.–М.: МИФИ, 2004.–80с.
2. Nielsen M.A., Chuang I.L. Quantum Computation and Quantum Information.–M.: Cambridge University Press, 2000.–704p.–(Нильсен М., Чанг И. Квантовые вычисления и квантовая информация.–М.: Мир, 2006.–824с.).
3. Колмогоров А.Н. Основные понятия теории вероятностей.–М.:ФАЗИС, 1998.–142с.
4. Феллер В. Введение в теорию вероятностей и ее приложения. В 2 т.–М.:Мир, 1984.
5. Вентцель Е.С. Теория вероятностей.–М.:Высшая школа, 2001.–576с.
6. Квантовые вычисления: за и против. Квантовый компьютер и квантовые вычисления. Том 1 /Пер. с англ. под ред. В.А. Садовничего.–Ижевск: Ред. журн. Регуляр. и хаотич. динам., Издательский дом Удмуртский университет, 1999.–212с.
7. Квантовый компьютер и квантовые вычисления /Пер. с англ. под ред. В.А. Садовничего.–Ижевск: Ред. журн. Регуляр. и хаотич. динам., 1999.–Т.2.–288с.
8. Квантовые компьютеры и квантовые вычисления (международный научный журнал), 2000. – Том 1. – №1. – 116с. – (http://ics.org.ru/rus?menu=mi_publish&issue=3&vol=1&number=1&year=2000).
9. Ландау Л.Д., Лифшиц Е.М. Квантовая механика. Краткий курс теоретической физики. Книга 2.– М.:Наука, 1972.–368с.
10. Фейнман Р. Характер физических законов /Пер. с англ. – 2-е изд. испр.—М.:Наука, 1987.–160с.

11. Мигдал А.Б. Квантовая физика для больших и маленьких.–М.:Наука, 1989.–144с.
12. Фейнман Р. Квантовомеханические компьютеры //Квантовый компьютер и квантовые вычисления /Пер. с англ. под ред. В.А. Садовничего. – Ижевск: Ред. журн. Регуляр. и хаотич. динам., 1999.–Т.2.–С.125–156.
13. Фейнман Р., Хибс А. Квантовая механика и интегралы по траекториям.—М.:Мир, 1968.–383с.
14. Тарасов Л.В. Закономерности окружающего мира. В 3 кн. Кн.3: Эволюция естественно-научного знания.–М.:ФИЗМАТЛИТ, 2004.–440с.
15. Физика квантовой информации /Под ред. Д. Боумейстера, А. Экерта, А. Цайлингера /Пер. с англ.–М.: Постмаркет, 2002.–376с.

СПИСОК СОКРАЩЕНИЙ

АКМ — *аппарат квантовой механики*;

ГХЦ — *Гринбергер-Хорн-Цейлингер*;

ДС — *дуальное соответствие*;

к.с. — *комплексное сопряжение*;
КЧ — *комплексные числа*;
КВП — *комплексное векторное пространство*;
КПФ — *квантовое преобразование Фурье*;
КЭР — *квантовая электродинамика резонаторов*;

МИФИ — *Московский Инженерно-Физический Институт*;

см. — *смотри*;
см — *сантиметр*;

т. — *точка*;

ЭВМ — *электронно-вычислительная машина*;
ЭПР — *А.Эйнштейн, Б. Подольский, Н. Розен*;

ЯМР — *ядерный магнитный резонанс*.

Сергей Дмитриевич Кулик
Александр Викторович Берков
Валерий Петрович Яковлев

ВВЕДЕНИЕ В ТЕОРИЮ КВАНТОВЫХ ВЫЧИСЛЕНИЙ
(методы квантовой механики в кибернетике)
Книга 2

Учебное пособие

Редактор *Е.Е. Шумакова*
Оригинал-макет подготовил *С.Д. Кулик*

Подписано в печать 06.11.2008. Формат 60x84 1/16
Печ. л. 33,25. Уч.-изд.л 33,25. Тираж 150 экз.
Изд. № 1/1а Заказ №

Московский инженерно-физический институт
(государственный университет),
115409, Москва, Каширское ш., 31.

Типография издательства "Тровант",
г. Троицк Московской области