Май 1999 г. *Том 169, № 5*

УСПЕХИ ФИЗИЧЕСКИХ НАУК

ОБЗОРЫ АКТУАЛЬНЫХ ПРОБЛЕМ

Квантовая информация

С.Я. Килин

Новое направление физики — квантовая информация — возникло на стыке квантовой механики, оптики, теории информации и программирования, дискретной математики, лазерной физики и спектроскопии и включает в себя вопросы квантовых вычислений, квантовых компьютеров, квантовой телепортации и квантовой криптографии, проблемы декогеренции и спектроскопии одиночных молекул и примесных центров. Сообщается о некоторых новых результатах в этой быстро развивающейся области исследований.

PACS number: **03.67.–a**

Содержание

1. **Введение (507).**
2. **Шрёдингер и его знаменитая работа 1935 г. (508).**
   2.1. Суперпозиция, парадокс шрёдингеровского кота. 2.2. Перепутанные (entangled) состояния. 2.3. Невозможность клонирования квантовых состояний.
3. **Квантовая телепортация (512).**
4. **Квантовая криптография (514).**
5. **Квантовые вычисления и компьютеры (516).**
   5.1. Обратимые и необратимые классические процессоры. 5.2. Квантовые компьютеры.
6. **Проблема декогеренции (522).**
   6.1. Релаксация как неунитарная эволюция состояния. Конструирование квантовых резервуаров. 6.2. Релаксация как квантовый стохастический процесс. Чистота условных состояний. 6.3. Коррекция ошибок с помощью обратной связи.

7. Заключение (525).

Список литературы (525).

1. Введение

Развитие квантовой оптики конца XX века стремительно заставляет нас — не только ученых, работающих в области квантовой физики, но и людей далеких от этой области — переосмыслить основополагающие утверждения квантовой теории, сформулированные в период ее создания. Связано это с тем, что весьма абстрактные идеи, лежащие в основе квантовой физики, казавшиеся недавно уделом внимания только единиц, оказывается, затрагивают практически всех благодаря новым технологическим возможностям, прежде всего в области оптических взаимодействий. Квантовые компьютеры, квантовая телепортация, квантовая криптография, возможность наблюдения отдельных атомов, ионов, молекул, в том числе биологически важных и манипулирования ими — все это объекты и явления, относящиеся к квантовому миру, который очень непросто воспринимается при оперировании понятиями из окружающего нас классического мира макроскопической физики и требует для своего описания адекватного языка — языка квантовой механики и квантовой теории поля.

Квантовая механика, основные идеи которой первыми сформулировали Нильс Бор (1885–1962 гг.), Эрвин Шрёдингер (1887–1961 гг.) и Вернер Гейзенберг (1901–1976 гг.), помимо аппарата, позволяющего рассчитывать энергетические состояния атомов и молекул и вычислять матричные элементы переходов между ними, незамедлительно востребованного практической физикой, содержала "идейную", философскую часть, обычно относимую к основаниям квантовой механики и остававшуюся практически невостребованной до недавнего времени. Именно эта часть квантовой механики объясняет необычность квантового мира. Наиболее полно и четко, порой специально доводя утверждения до парадоксальности, изложил эту часть квантовой теории Эрвин Шрёдингер в своей знаменитой работе 1935 г. [1], которую он сам не знал, как классифицировать: как "... реферат или генеральную исповедь" ("Referat oder Generalbeichte?"). В ней, употребляя современный термин, обсуждается одна из проблем квантовой информации — что мы можем узнать о состояниях объектов квантового мира и что происходит с объектами в процессе получения этого знания. Потребовалось больше полувека для того, чтобы глубина осознанного Шрёдингером стала необходимой при интерпретации экспериментов, направленных на практические приложения.

В настоящей работе речь пойдет о нескольких таких экспериментах. Здесь прежде всего эксперименты по квантовой телепортации, квантовой криптографии и, наконец, квантовым компьютерам, выгоды от реализации которых настолько привлекательны, насколько и

С.Я. Килин. Институт физики им. Б.И. Степанова
Национальной академии наук Беларуси,
220602 Минск, просп. Франциска Скарины 70, Беларусь
Тел. (017) 284-26-13
Факс (017) 284-08-79
E-mail: kilin@ifanbel.bas-net.by

Статья поступила 18 июня 1998 г.

сложны пути их создания. Часть работы посвящается одиночным объектам вещества в квантовой оптике и методам их регистрации, т.е. тем объектам, которые, в частности, могут служить в качестве элементной базы для квантовых компьютеров. В заключении рассмотрены способы решения одной из проблем, стоящей на пути реализации квантовых вычислений, проблемы декогеренции. Но в начале — о языке квантовой оптики и о положениях квантовой теории, знание которых необходимо для понимания всего последующего.

2. Шрёдингер и его знаменитая работа 1935 г.

29 ноября 1935 г. в журнале *Die Naturwissenschaften* выходит работа Э. Шрёдингера "*Современное состояние квантовой механики*" [1]. Статья написана во время его вынужденного нахождения в Оксфорде (рис. 1), уже после получения в 1933 г. Нобелевской премии по физике (совместно с П. Дираком). Как отмечает сам Шрёдингер, статья была инициирована дискуссией, которая началась с работы Альберта Эйнштейна, Бориса Подольского и Натана Розена "*Может ли квантовомеханическое описание реальности быть полным?*" [2], вышедшей 15 мая того же 1935 г., и была продолжена в одноименной статье Нильсом Бором [3].

Несмотря на довольно абстрактный и сложный для восприятия стиль изложения, значение работы [1] было быстро осознано русскими учеными, о чем свидетельствует немедленный перевод этой статьи на русский язык в 1936 г. в *Успехах химии* [1]. (Для сравнения, англоязычный перевод появился только в 1980 г. [1].)

В работе Шрёдингер анализирует "подводные камни" в описании квантовомеханических процессов измерения и формулирует четыре основных положения, которые сводятся к тому, что состояния объектов квантового мира обладают следующими свойствами:

1. *Суперпозиции*. Состояния описываются линейной суперпозицией базисных состояний.

2. *Интерференции*. Результат измерений зависит от относительных фаз амплитуд в этой суперпозиции.

3. *Entanglement* ("*перепутывания*", "*взаимосопряженности*", "*сцепленности*"). Полное знание о состоянии всей системы не соответствует такому же полному знанию о состоянии ее частей.

4. *Неклонируемости и неопределенности*. Неизвестное квантовое состояние невозможно клонировать, а также наблюдать без его возмущения.

Поясним кратко каждое из них. Но прежде отметим, что третье и четвертое из этих положений еще недавно были малоизвестны в широких физических кругах и обсуждались разве что при исследованиях парадокса Эйнштейна – Подольского – Розена (ЭПР) и связанных с ним неравенств Белла.

2.1. Суперпозиция, парадокс шрёдингеровского кота

Квантовый объект, в отличие от классического, изначально статистический. Однако вероятностный характер квантового объекта не сводится к классически воспринимаемой неопределенности, связанной, например, с неполнотой знания об объекте. Для описания квантового объекта используется понятие *состояние*. Говоря, что объект находится в определенном состоянии, подразумевают, что можно представить к рассмотрению список, каталог (в терминах Шрёдингера), или, что то же самое, волновую функцию, вектор состояния, или матрицу плотности, которые содержат информацию о возможных результатах измерений над этим объектом. Поскольку результаты измерений над объектом, приготавливаемом в одном и том же состоянии, в общем случае меняются от измерения к измерению, вектор состояния должен давать и дает статистическую информацию (функции распределения) результатов ансамбля тех или иных измерений.

Рис. 1. Эрвин Шрёдингер родился в Вене. Там же он и учился сначала в гимназии, затем в университете, который окончил в 1910 г. Посвятив себя теоретической физике, Шрёдингер вскоре стал профессором в Бреславле (ныне Вроцлав), потом в Цюрихе, где до него работал Эйнштейн. Именно в Цюрихе были сделаны работы Шрёдингера, приведшие к открытию основного уравнения нерелятивистской квантовой механики — волнового уравнения, которое теперь называют его именем. Создание квантовой механики было отмечено Нобелевской премией 1933 г., которую Шрёдингер разделил с Дираком. В 1927 г. Шрёдингер был приглашен на кафедру теоретической физики в Берлин, кафедру, которую до него занимал Планк. С приходом к власти Гитлера Шрёдингер покинул фашистскую Германию и принял приглашение в Оксфорд. В 1936 г. он ненадолго вернулся в Австрию, заняв кафедру в Граце; однако после аншлюса вынужден был снова покинуть свою страну. На этот раз Шрёдингер переехал в Ирландию, в Институт фундаментальных исследований в Дублине. В 1947 г. он, наконец, вернулся на родину. Но его здоровье уже было подорвано, и после продолжительной болезни он скончался в Вене (фотография и биографический комментарий из антологии *Жизнь науки* (составитель С.П. Капица) (М.: Наука, 1973)).

Простым примером служит вектор состояния системы, обладающей двумя ортогональными состояниями $|1\rangle$ и $|2\rangle$, например, энергетическими. Состояние такого объекта описывается вектором состояния (волновой функцией)

$$|\Psi\rangle = \alpha|1\rangle + \beta|2\rangle\,, \qquad (1)$$

где α и β — комплексные числа, т.е. общее состояние есть линейная суперпозиция, а квадраты модулей комплексных амплитуд α и β равны вероятностям обнаружить систему в соответствующих состояниях ($|\alpha|^2 + |\beta|^2 = 1$). При измерении когерентная суперпозиция (1) разрушается и редуцируется к новому состоянию, которое определяется типом измерения. Так, при попытке обнаружения системы в состоянии $|2\rangle$ возмущение измерительного прибора приведет к тому, что в момент измерения произойдет редукция (проецирование)

$$|\Psi\rangle \Rightarrow |2\rangle\langle 2|\Psi\rangle \Rightarrow |2\rangle\,, \tag{2}$$

в результате которой система после измерения окажется в состоянии $|2\rangle$, а исходное состояние перестанет существовать[1].

Суперпозиционные состояния следует отличать от смеси состояний, которая описывается матрицей плотности

$$\rho_{\text{mix}} = |\alpha|^2|1\rangle\langle 1| + |\beta|^2|2\rangle\langle 2| \tag{3}$$

и которая по сути является классическим состоянием, так как в смешанном состоянии (3) система может быть обнаружена или в состоянии $|1\rangle$, или в состоянии $|2\rangle$, тогда как в суперпозиционном состоянии (1) система может быть обнаружена в двух состояниях *одновременно*. Это принципиальное отличие суперпозиционного состояния проявляется в дополнительных интерференционных членах в его матрице плотности:

$$\rho = |\Psi\rangle\langle\Psi| = |\alpha|^2|1\rangle\langle 1| + |\beta|^2|2\rangle\langle 2| + \alpha\beta^*|1\rangle\langle 2| + \alpha^*\beta|2\rangle\langle 1|\,. \tag{4}$$

Из (4), в частности, следует, что получение ненулевого результата при измерении физической величины, оператор которой имеет только недиагональные матричные элементы (к примеру, электронный дипольный момент атома), возможно только в том случае, когда система одновременно находится в нескольких состояниях, например, в $|1\rangle$ и $|2\rangle$.

Чтобы обратить внимание на необычный характер суперпозиционных состояний, Шрёдингер приводит пример, который возмущает наше обыденное восприятие мира. Предположим, следуя Шрёдингеру, что в стальном ящике находится флакон с ядом, который может быть разбит посредством механизма, запускающегося при распаде одного радиоактивного атома. Находящийся внутри ящика первоначально живой кот в результате распада одного атома может стать мертвым. Однако точно так же, как и состояние радиоактивного атома есть квантовая суперпозиция распавшегося и не распавшегося состояний, состояние шрёдингеровского кота есть суперпозиция состояний живого $|\uparrow\rangle$ и не живого $|\downarrow\rangle$: $|\Psi\rangle = L|\uparrow\rangle + D|\downarrow\rangle$. Поскольку в системах микроскопических, таких как атомы и молекулы, наблюдение квантовых суперпозиций обычное явление, а в макросистемах квантовые суперпозиционные состояния или состояния шрёдингеровского кота не наблюдаемы, очевидно, есть причина, приводящая к разрушению таких состояний. Природа такого разрушения — декогеренции — будет рассмотрена ниже. Здесь же отметим, что проблема сохранения суперпозиционных состояний типа шрёдингеровского кота для мезоскопических систем — актуальная задача, с решением которой можно будет говорить о многих приложениях квантовой информации.

Пример суперпозиционного состояния, который нам понадобится в дальнейшем, представляет однофотонный пучок света с заданным волновым вектором, или же состояние одного фотона: $|1_{\text{фотон}}\rangle$. Поскольку электромагнитное излучение поляризовано, то состояние излучения с заданным волновым вектором можно моделировать как состояние двух квантовых гармонических осцилляторов, каждый из которых соответствует одной из взаимно-ортогональных поляризаций (рис. 2). Обозначая собственные состояния осциллятора с вертикальной поляризацией, как $|n\rangle_{\updownarrow}$, а состояния с горизонтальной поляризацией, как $|m\rangle_{\leftrightarrow}$, можно ввести два базисных вектора

$$|1\rangle_{\updownarrow}|0\rangle_{\leftrightarrow} = |\updownarrow\rangle\,, \qquad |0\rangle_{\updownarrow}|1\rangle_{\leftrightarrow} = |\leftrightarrow\rangle$$

и разложить по ним любое однофотонное состояние:

$$|1_{\text{фотон}}\rangle = a|\updownarrow\rangle + \beta|\leftrightarrow\rangle\,. \tag{5}$$

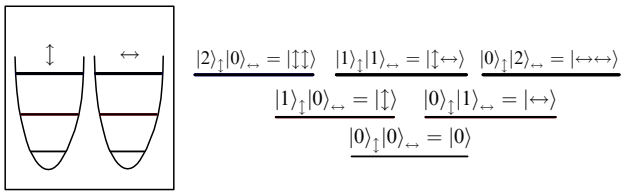


Рис. 2. Световой пучок с заданным волновым вектором эквивалентен двум гармоническим осцилляторам, соответствующим двум ортогонально поляризованным колебаниям электромагнитного поля. Однофотонное состояние этого пучка определяется суперпозицией двух энергетически вырожденных состояний поляризованных фотонов $|\updownarrow\rangle$ и $|\leftrightarrow\rangle$. Двухфотонное состояние этого пучка в общем случае есть суперпозиция трех энергетически вырожденных состояний, два из которых — пары тождественно поляризованных фотонов $|\updownarrow\updownarrow\rangle$ и $|\leftrightarrow\leftrightarrow\rangle$, а одно — пара ортогонально поляризованных фотонов $|\updownarrow\leftrightarrow\rangle$.

Отметим относительный характер понятия суперпозиционного состояния. Состояние (5) с $\alpha = \beta = 1/\sqrt{2}$ является суперпозиционным в базисе горизонтальных и вертикальных поляризаций, т.е. при измерениях, проводимых с поляризаторами, ориентированными в таких направлениях. Однако, если это состояние $(|\updownarrow\rangle + |\leftrightarrow\rangle)/\sqrt{2}$ выступает в качестве одного из пары базисных

$$|\nearrow\rangle = \frac{|\updownarrow\rangle + |\leftrightarrow\rangle}{\sqrt{2}}\,, \quad |\searrow\rangle = \frac{|\updownarrow\rangle - |\leftrightarrow\rangle}{\sqrt{2}}\,, \tag{6}$$

что соответствует измерениям с поляризаторами, ориентированными под 45° и 135°, то, очевидно, о нем нельзя

[1] Отметим, что процесс измерения — взаимодействие с макроскопическим измерительным прибором — является принципиально необратимым процессом, в результате которого состояние измеряемого объекта меняется (претерпевает редукцию). Редукция, как и другой физический процесс, имеет свои характерные времена, присущие конкретному измерению. Однако, в силу его краткосрочности, вопрос о внутренней динамике процесса редукции, т.е. возможности "увидеть его воочию", обычно не рассматривается, хотя для ряда измерений, например в квантовой томографии сверхкоротких импульсов, он, несомненно, представляет интерес.

говорить как о суперпозиционном. То есть понятие суперпозиционного состояния используется исключительно совместно с конкретным базисом, определяемым набором измерений, применяемых к квантовому объекту. В этом смысле любое чистое квантовое состояние — суперпозиционное, поскольку оно является таковым для всех базисов за исключением тех, где оно выступает в качестве базисного.

2.2. Перепутанные (entangled) состояния

Наряду с суперпозиционными состояниями, Шрёдингер вводит в рассмотрение и так называемые перепутанные состояния (entangled states), которые необходимы для описания состояния совокупной системы, образованной из нескольких частей, возможно, и пространственно разделенных, делокализованных. Примером таких состояний может служить состояние поля и излучившего его атома (рис. 3) или состояние квантовой системы, образованной двумя однофотонными пучками с различающимися волновыми векторами (рис. 4). Любое состояние такой фотонной пары представимо в виде суперпозиции четырех возможных поляризационных базисных состояний:

$$|1_1 + 1_2\rangle = C_{\updownarrow\updownarrow}|\updownarrow\rangle_1|\updownarrow\rangle_2 + C_{\leftrightarrow\leftrightarrow}|\leftrightarrow\rangle_1|\leftrightarrow\rangle_2 + C_{\updownarrow\leftrightarrow}|\updownarrow\rangle_1|\leftrightarrow\rangle_2 + C_{\leftrightarrow\updownarrow}|\leftrightarrow\rangle_1|\updownarrow\rangle_2 . \quad (7)$$

Рис. 3. Перепутанные состояния можно представить себе на примере составной системы — двухуровневый атом и поле. Предположим, что атом пролетает область взаимодействия с полем, например, полем резонатора. После короткого времени взаимодействия атом и поле оказываются пространственно разнесенными. Однако состояние общей системы оказывается взаимозависимым, перепутанным, так как состояние, в котором находится поле, жестко зависит от состояний атома: $|\Psi\rangle = |\text{атом}\rangle_1|\text{поле}\rangle_1 + |\text{атом}\rangle_2|\text{поле}\rangle_2$. Причем время жизни такого перепутанного состояния может быть много больше времени взаимодействия.

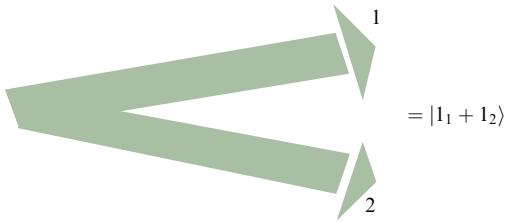


Рис. 4. Два однофотонных пучка, образующих фотонные пары, находящиеся в сцепленных состояниях.

В общем случае каждый фотон из одного пучка связан с фотоном из другого, поскольку общее состояние не выражается в виде произведения волновых функций двух фотонов. Причем эта связь гораздо более жесткая, чем можно было представить в случае классической корреляции. Это хорошо демонстрируют фотонные пары, находящиеся в состояниях Белла [4], который ввел их в 1964 г. для рассмотрения парадокса ЭПР. Состояния

$$|\Phi^+\rangle = \frac{|\updownarrow\rangle_1|\updownarrow\rangle_2 + |\leftrightarrow\rangle_1|\leftrightarrow\rangle_2}{\sqrt{2}} , \quad (8а)$$

$$|\Phi^-\rangle = \frac{|\updownarrow\rangle_1|\updownarrow\rangle_2 - |\leftrightarrow\rangle_1|\leftrightarrow\rangle_2}{\sqrt{2}} , \quad (8б)$$

$$|\Psi^+\rangle = \frac{|\updownarrow\rangle_1|\leftrightarrow\rangle_2 + |\leftrightarrow\rangle_1|\updownarrow\rangle_2}{\sqrt{2}} , \quad (8в)$$

$$|\Psi^-\rangle = \frac{|\updownarrow\rangle_1|\leftrightarrow\rangle_2 - |\leftrightarrow\rangle_1|\updownarrow\rangle_2}{\sqrt{2}} , \quad (8г)$$

представляют базисные состояния Белла. Каждое из этих перепутанных состояний обладает замечательным свойством: как только каким-нибудь измерением один из фотонов проецируется на состояние с определенной поляризацией, так поляризация фотона из другого пучка становится также определенной. Например, для состояний $|\Psi^{\pm}\rangle$ при обнаружении одного из фотонов с поляризацией $\leftrightarrow$ поляризация другого оказывается противоположной $\updownarrow$. Как измерение, производимое над одной частицей, может мгновенно влиять на состояние другой, которая может быть удаленной на произвольное расстояние? Эйнштейн среди других замечательных физиков просто не принимал это по его определению, "действие призраков на расстоянии". В настоящее время такие свойства перепутанных состояний продемонстрированы в ряде экспериментов [5, 6].

Кроме того, перепутанные состояния демонстрируют еще одно парадоксальное, на первый взгляд, свойство, отмеченное Шрёдингером в [1], где он пишет о том, что полное знание о состоянии всей системы еще не предполагает такого же полного знания о состоянии ее частей. Действительно, если мы желаем узнать состояние одной из частиц в любой из пар (8), нам следует усреднить матрицу плотности чистого, а следовательно, максимально определенного состояния, например,

$$|\Psi^-\rangle = \frac{|\updownarrow\rangle_1|\leftrightarrow\rangle_2 - |\leftrightarrow\rangle_1|\updownarrow\rangle_2}{\sqrt{2}} ,$$

по состояниям другой частицы, например второй. В результате получающаяся матрица плотности первой частицы

$$\rho^{(1)} = \mathrm{Sp}_2\left(|\Psi^-\rangle\langle\Psi^-|\right) = \underbrace{\left(|\updownarrow\rangle_{11}\langle\updownarrow| + |\leftrightarrow\rangle_{11}\langle\leftrightarrow|\right)/2}_{\text{смесь}} \quad (9)$$

говорит о том, что состояние первой частицы смешанное, т.е. не являющееся максимально определенным.

2.2.1. Как генерировать перепутанные состояния? Перепутанные пары фотонов можно получить экспериментально при каскадных распадах в атомных системах [7] и в параметрических процессах при резонансной флуоресценции, где фотоны ω_1 и ω_2, рожденные при рассеянии двух фотонов накачки $2\omega_0 \to \omega_1 + \omega_2$, находятся в перепутанных состояниях. Теоретическое предсказание квантовой коррелированности таких фотонов [8] наблюдалось экспериментально в [9]. Эксперимент [10] продемонстрировал также возможность генерации перепутанных состояний массивных частиц — атомов. Наибольшее распространение в настоящее время получили источники на основе спонтанного параметрического распада

в кристаллах с квадратичной нелинейностью, когда ультрафиолетовый фотон накачки распадается на два красных фотона с приблизительно равной энергией [11, 12]. При этом выполняется закон сохранения энергии и импульса: $\hbar\omega_\mathrm{p} = \hbar\omega_\mathrm{s} + \hbar\omega_\mathrm{i}$, $\hbar\mathbf{k}_\mathrm{p} = \hbar\mathbf{k}_\mathrm{s} + \hbar\mathbf{k}_\mathrm{i}$, где $\hbar\omega_j$ и $\hbar\mathbf{k}_j$ $(j = \mathrm{p}, \mathrm{s}, \mathrm{i})$ — соответственно энергии и импульсы исходного (p) и двух дочерних фотонов, обычно называемых "сигнальным" (s) и холостым (i). Использование квадратичных кристаллов с фазовым синхронизмом II типа (рис. 5) позволяет легко получить поляризационно перепутанные состояния в направлениях 1 и 2, определяемых пересечениями конусов синхронизма для обыкновенных и необыкновенных фотонов (рис. 5б). Именно в этих направлениях создаются [13] состояния Белла (8).

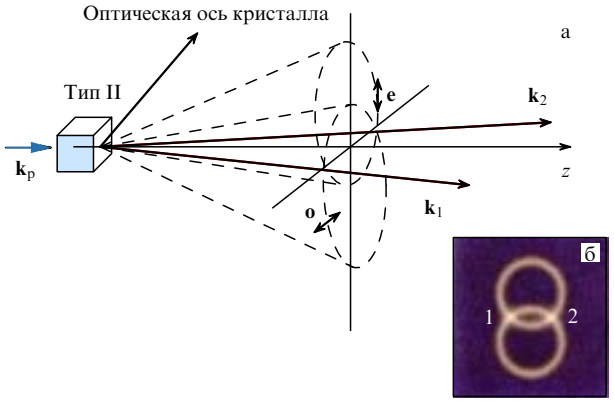


Рис. 5. (а) Сохранение импульса внутри кристалла, известное как "фазовый синхронизм", достигается благодаря двулучепреломлению кристалла, позволяющего компенсировать дисперсию в кристалле. В результате сигнальные и холостые фотоны создают радугу цветных конусов, в которых сопряженные фотоны излучаются в противоположные стороны от пучка накачки. В случае фазового синхронизма типа I сигнальные и холостые фотоны имеют одинаковую линейную поляризацию, перпендикулярную поляризации фотонов накачки, и их конусы концентричны с пучком накачки. В случае фазового синхронизма типа II сопряженные пары образуются из обычно-(o) и необычно-(e)поляризованных фотонов. В этом случае конусы сигнальных и холостых фотонов имеют различные оси. В случае одноосных кристаллов с отрицательной дисперсией, таких как BBO, ось конуса необычно поляризованных фотонов расположена между осью кристалла и пучком накачки, а ось конуса обычно поляризованных фотонов расположена дальше от пучка накачки (при этом все оси и пучок накачки лежат в одной плоскости). (б) Приведено схематическое изображение, которое получается при фотографировании излучения, испускаемого нелинейным кристаллом при параметрическом распаде, перпендикулярно направлению накачки. Цифрами 1 и 2 обозначены направления, в которых создаются поляризационно-коррелированные пары фотонов. В этих направлениях поляризация не определена; все, что мы знаем, — это то, что поляризации должны быть различны.

2.2.2. Как измерить (спроецировать) перепутанные состояния? Возможность отличить одно из белловских состояний от других обеспечивается их различными симметриями. Из четырех состояний (8) первые три обладают бозонной симметрией, поскольку их волновая функция не меняет знак при перестановке частиц 1 и 2. Последнее состояние (8г) фермионное: при перестановке 1 и 2 знак волновой функции изменяется. Эта выделенность состояния $|\Psi^-\rangle = (|\updownarrow\rangle_1|\leftrightarrow\rangle_2 - |\leftrightarrow\rangle_1|\updownarrow\rangle_2)/\sqrt{2}$ проявляется и в результатах интерференции интенсивностей пучков 1 и 2 (рис. 6). Два детектора в этой схеме сработают только в случае, если генерируемые кристаллом перепутанные фотонные пары находятся в поляризационно-фермионном состоянии $|\Psi^-\rangle$. Это является отражением известного факта из двухчастичной интерференции на делителе пучка [14]: две частицы покидают делитель в одном пучке для пространственно-симметричной волновой функции и в разных для пространственно-антисимметричных состояний. Фотоны — бозонные частицы, поэтому пространственная часть волновой функции поляризационно-фермионного состояния $|\Psi^-\rangle$ для сохранения общей симметрии должна быть антисимметричной. Измерение, выделяющее фермионное состояние из четырех возможных состояний (8), относится к так называемым измерениям состояний Белла (ИСБ).

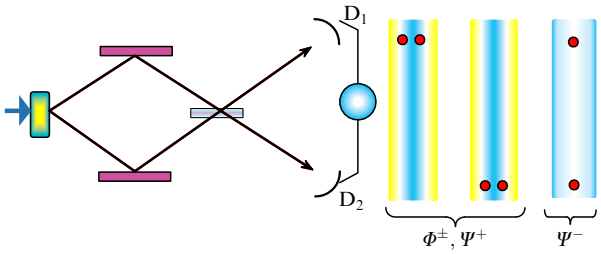


Рис. 6. Схема по наблюдению интерференции интенсивностей. Перепутанные поляризационные пучки, излучаемые кристаллом, смешиваются на полупрозрачном (50 %) зеркале и регистрируются двумя детекторами, отсчеты которых анализируются на совпадения. Существуют две возможности для фотона из любого пучка попасть в один из детекторов — либо отразившись от полупрозрачного зеркала, либо пройдя через него. При вычислении вероятности фотоотсчета складываются квантовомеханические амплитуды этих двух возможностей. При унитарном преобразовании на поляризационно-нечувствительном зеркале имеет значение только пространственная часть волновой функции фотонов. Фотоны — бозонные частицы, поэтому ясно, что пространственная часть волновой функции является симметричной для бозонных поляризационных состояний $|\Phi^\pm\rangle, |\Psi^+\rangle$ и антисимметричной для фермионного состояния $|\Psi^-\rangle$. Из двухчастичной интерференции на делителе пучка известно, что две частицы покидают делитель в одном пучке для пространственно-симметричной волновой функции, и в разных для пространственно-антисимметричных состояний. Следовательно, совпадение отсчетов двух детекторов проецирует состояние фотонной пары на фермионное состояние $|\Psi^-\rangle$.

2.3. Невозможность клонирования квантовых состояний

Факт разрушения квантового состояния в результате воздействий, производимых измеряющей аппаратурой, позволяет говорить о квантовом состоянии как об очень "чутком", ускользающем от попыток получить о нем информацию объекте. Известное соотношение неопределенностей есть одно из проявлений такой лабильности. Другим ярким проявлением является теорема о невозможности клонировать отдельный квантовый объект [15]. Под клонированием понимается создание точной копии исходного объекта при сохранении его в том состоянии, в каком он был до операции клонирования и которое изначально неизвестно.

Предположим, что мы обладаем устройством для клонирования фотонов. Его действие сводится к воспроизводству фотонов с сохранением их свойств (состояний). Если речь идет о поляризационных состояниях, то эффект описывается преобразованием

$$|\mathrm{R_I}\rangle|\updownarrow\rangle \Rightarrow |\mathrm{R_{FV}}\rangle|\updownarrow\updownarrow\rangle\,,$$
$$|\mathrm{R_I}\rangle|\leftrightarrow\rangle \Rightarrow |\mathrm{R_{FH}}\rangle|\leftrightarrow\leftrightarrow\rangle\,,$$

где $|\mathrm{R_I}\rangle$ — начальное состояние устройства для клонирования, $|\mathrm{R_{FV}}\rangle$, $|\mathrm{R_{FH}}\rangle$ — конечные его состояния при попытке клонирования вертикально и горизонтально поляризованных фотонов. То есть вместо одного фотона с заданной поляризацией появляются два с такой же поляризацией (см. рис. 2). Однако, если мы попытаемся клонировать фотон с поляризацией, отличной от вертикальной и горизонтальной, например, $\alpha|\updownarrow\rangle + \beta|\leftrightarrow\rangle$, то такое устройство совершит преобразование

$$|\mathrm{R_I}\rangle\left(\alpha|\updownarrow\rangle + \beta|\leftrightarrow\rangle\right) \Rightarrow \alpha|\mathrm{R_{FV}}\rangle|\updownarrow\updownarrow\rangle + \beta|\mathrm{R_{FH}}\rangle|\leftrightarrow\leftrightarrow\rangle\,. \quad (10)$$

Преобразованное состояние даже в условиях равенства $|\mathrm{R_{FV}}\rangle$ и $|\mathrm{R_{FH}}\rangle$ не соответствует двум фотонам, поляризованным под углом $\varphi = \arctan\beta/\alpha$. Действительно, рождение *одного* фотона, поляризованного под углом $\varphi = \arctan\beta/\alpha$, т.е. в состоянии $\alpha|\updownarrow\rangle + \beta|\leftrightarrow\rangle$, достигается однократным применением оператора рождения $\hat{b}^+_\varphi = \alpha\hat{a}^+_\mathrm{V} + \beta\hat{a}^+_\mathrm{H}$ к вакууму, где $\hat{a}^+_\mathrm{V}$, $\hat{a}^+_\mathrm{H}$ — операторы рождения вертикально и горизонтально поляризованных фотонов, соответствующих левому и правому гармоническому осциллятору на рис. 2. *Два* фотона с такой поляризацией получаются двукратным действием оператора $\hat{b}^+_\varphi = \alpha\hat{a}^+_\mathrm{V} + \beta\hat{a}^+_\mathrm{H}$ на вакуум:

$$\frac{(\hat{b}^+_\varphi)^2}{\sqrt{2}}|0\rangle = \alpha^2|\updownarrow\updownarrow\rangle + \beta^2|\leftrightarrow\leftrightarrow\rangle + \sqrt{2}\alpha\beta|\updownarrow\leftrightarrow\rangle\,. \quad (11)$$

Состояние (11) ни при каких отличных от нуля значениях α и β не совпадает с полевой частью состояния (10), т.е. клонирование одного фотона в состоянии с произвольной изначально неизвестной поляризацией невозможно. Этот пример доказывает невозможность в общем случае клонирования произвольного квантового объекта.

3. Квантовая телепортация

Нормальное (эволюционное) течение исследований в области измерения, трансформации и передачи информации в квантовом мире было взорвано экспериментальной реализацией в конце 1997 г. Антоном Цайлингером и его сотрудниками [16] старой мечты фантастов о телепортации — исчезновении объекта в одном месте и возникновении в другом, пространственно удаленном. Хотя предложение о *квантовой телепортации* — возможности переноса квантового состояния одного объекта на другой, было сделано Чарлзом Беннетом с коллегами еще в 1993 г. [17], именно эксперимент [16] и последовавший за ним эксперимент [18] привлекли к себе широкое внимание научной (и не только) общественности.

Классически понимаемая телепортация состоит в максимальном тестировании объекта телепортации и затем в передаче этих свойств с последующим восстановлением объекта. Однако проецирование и разрушение измеряемого объекта при измерении запрещают эту процедуру в квантовом мире. Существует иной метод передачи квантового состояния одного объекта на другой. Кратко схема передачи неизвестного состояния $|\psi\rangle$ от Алисы к Бобу (традиционные персонажи в объяснении особенностей передачи квантовой информации) состоит в следующем: *Алиса имеет у себя частицу в некотором неизвестном ей состоянии* $|\psi\rangle$. *Производя операцию телепортации, Алиса разрушает состояние* $|\psi\rangle$ *в своем местоположении, но при этом частица у Боба переходит в это* ($|\psi\rangle$) *квантовое состояние. Ни Боб, ни Алиса не получают информацию о состоянии* $|\psi\rangle$, *а Боб даже не знает, что на его частицу телепортировано некоторое состояние. Чтобы сообщить Бобу об акте телепортации, Алиса должна воспользоваться классическим каналом информации.*

Ключевую роль в данной схеме играют фотонные пары, находящиеся в перепутанных состояниях. Именно с их помощью осуществляется квантовый канал информации между Алисой и Бобом. Предположим, что частица 1 (фотон), которую Алиса хочет телепортировать, находится первоначально в поляризационном состоянии $|\psi\rangle_1 = \alpha|\updownarrow\rangle_1 + \beta|\leftrightarrow\rangle_1$ (рис. 7). Алиса связана с Бобом с помощью пар фотонов, посылаемых ЭПР-источником и находящихся в перепутанных состояниях

$$|\Psi^-\rangle_{23} = \frac{|\updownarrow\rangle_2|\leftrightarrow\rangle_3 - |\leftrightarrow\rangle_2|\updownarrow\rangle_3}{\sqrt{2}}\,. \quad (12)$$

Фотоны 2 посылаются Алисе, а фотоны 3 — Бобу. Совместное состояние фотонов 1 и 2, встречающихся на станции Алисы, есть произведение состояний $|\Psi\rangle_1$ и $|\Psi^-\rangle_{23}$:

$$\begin{aligned}|\Psi\rangle_1|\Psi^-\rangle_{23} = {}& |\Psi^-\rangle_{12}\frac{\alpha|\leftrightarrow\rangle_3 + \beta|\updownarrow\rangle_3}{2} + \\ & + |\Psi^+\rangle_{12}\frac{-\alpha|\leftrightarrow\rangle_3 + \beta|\updownarrow\rangle_3}{2} + \\ & + |\Phi^+\rangle_{12}\frac{-\beta|\leftrightarrow\rangle_3 + \alpha|\updownarrow\rangle_3}{2} + \\ & + |\Phi^-\rangle_{12}\frac{\beta|\leftrightarrow\rangle_3 + \alpha|\updownarrow\rangle_3}{2}\,. \end{aligned} \quad (13)$$

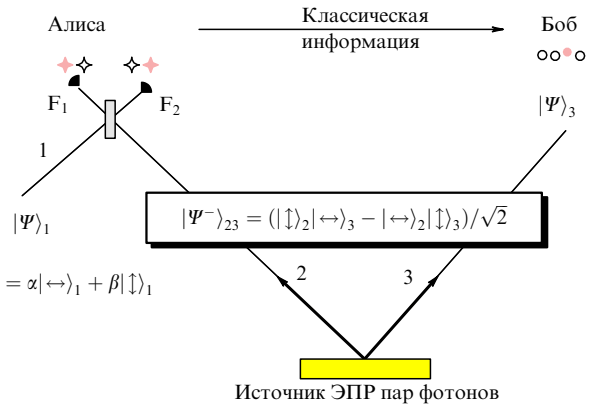


Рис. 7. Принципиальная схема телепортации. Алиса хочет передать состояния частицы 1 частице, находящейся на станции Боба. Алиса и Боб получают фотоны 2 и 3, образующие ЭПР пару в перепутанном состоянии $|\Psi^-\rangle_{23}$. Алиса, выполняя измерения белловских состояний частиц 1 и 2, осуществляет проецирование также и частицы 3, находящейся у Боба. В одном случае из четырех два детектора $\mathrm{F_1}$ и $\mathrm{F_2}$ сработают одновременно, давая Алисе знать, что одновременно состояние частицы 3 стало таким, как начальное состояние фотона 1, т.е. произошла телепортация состояния $|\Psi\rangle_1$. Воспользовавшись классическим каналом, Алиса может сообщить об этом Бобу. Кроме того, при использовании классического канала и дополнительного унитарного преобразования, выполняемого Бобом, можно получать состояния $|\Psi\rangle_1$ на стороне Боба со стопроцентной вероятностью после каждого белловского измерения, выполненного Алисой.

Из волновой функции (13) для трех частиц, две из которых у Алисы, а одна у Боба, следует, что если Алиса спроецирует частицы 1 и 2 на состояние $|\Psi^-\rangle_{12}$, то состояние частицы 3 на стороне Боба мгновенно редуцируется к состоянию первой частицы $|\Psi\rangle_3 = \alpha|\leftrightarrow\rangle_3 + \beta|\updownarrow\rangle_3$. То есть производя измерения белловских состояний, образующихся при смешении на зеркале фотонов 1 и 2, и регистрируя совпадения фотоотсчетов детекторов F_1 и F_2 (рис. 7), Алиса тем самым осуществляет мгновенную редукцию состояния фотона 3 к первоначальному состоянию фотона 1, другими словами, производит телепортацию! Некоторые особенности квантовой телепортации требуют специального упоминания.

1. Процедура телепортации не нарушает теорему о неклонируемости отдельного квантового объекта. В момент произведения Алисой измерения состояний Белла фотон 1 становится компонентой поляризационно перепутанной пары фотонов 1 и 2, т.е. теряет свою индивидуальность. Начальное его состояние $|\Psi\rangle_1$ разрушается.

2. Перенос квантовой информации от фотона 1 к фотону 3 может осуществляться на произвольные расстояния. Технически сейчас осуществимо поддержание поляризационной перепутанности фотонов на расстояниях более 10 км.

3. В момент измерения Алиса знает о факте телепортации, а Боб не знает: телепортация не предполагает передачу информации о факте ее осуществления. Более того, Алиса может и не знать конкретно, какое состояние фотона 1 она передает.

4. Для информирования Боба о факте передачи состояния на фотон 3 требуется классический канал информации.

5. Если Алиса проводит полное измерение состояний Белла, идентифицируя помимо фермионного и три бозонных состояния, каждое из которых возникает с вероятностью 25 %, то Боб, получая по классическому каналу от Алисы эту информацию, может правильно выбранным преобразованием перевести состояние фотона 3 в начальное состояние фотона 1 при любом результате измерений Алисы. Если этого не делать, а ограничиться проецированием на фермионное состояние, то телепортация будет успешно осуществляться в среднем один раз из четырех попыток, как это и было продемонстрировано в работе [16].

На рисунке 8 приведена схема эксперимента [16]. Источником фотонных пар 2–3, связывающих Алису и Боба, был нелинейный кристалл, возбуждаемый УФ фемтосекундными импульсами, преобразуемыми при параметрическом распаде по II типу в фотоны 2 и 3. Отраженная часть накачки использовалась для создания фотона 1 для телепортирования. Измерение состояний Белла фотонов 1 и 2 производилось при смешении их на зеркале с последующей регистрацией детекторами F_1 и F_2. Для анализа поляризационных свойств фотона на стороне Боба использовалось поляризационное зеркало с последующими двумя детекторами D_1 и D_2.

Экспериментальное доказательство телепортации состояло в регистрации совпадений отсчетов детекторов F_1 и F_2, фиксирующих момент телепортации, и одного из детекторов на стороне Боба, настроенных на регистрацию различным образом поляризованных фотонов (трехпортовые совпадения). Выбирая в качестве телепортируемого фотон 1 с поляризацией 45° и

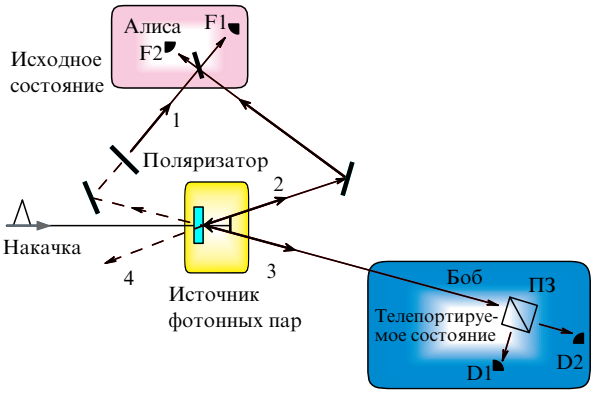


Рис. 8. Схема эксперимента [16] по квантовой телепортации. Источником вспомогательных фотонных пар, связывающих Алису и Боба, был нелинейный кристалл, возбуждаемый УФ фемтосекундными импульсами, преобразуемыми при параметрическом распаде по II типу в фотоны 2 и 3. Отраженная часть накачки использовалась для создания при обратном проходе фотона 1 для телепортирования и фотона 4 для временной привязки. Измерение состояний Белла фотонов 1 и 2 производилось при смешении их на зеркале с последующей регистрацией детекторами F_1 и F_2. Для анализа поляризационных свойств фотона на стороне Боба использовалось поляризационное зеркало с последующими двумя детекторами D_1 и D_2.

настраивая поляризационное зеркало на селекцию поляризации −45° (детектор D_1) и +45° (детектор D_2), следует ожидать, что при совпадении отсчетов F_1 и F_2 фотон 3 должен иметь поляризацию +45°, т.е. детектор D_2 должен дать отсчет, а детектор D_1 — нет. Если рассматривать вероятности тройных совпадений ($D_1F_1F_2$) и ($D_2F_1F_2$) как функции задержки между фотонами 1 и 2, реализуемой перемещением зеркала, переотражающего импульсы накачки, то должен наблюдаться провал до нуля для совпадений ($D_1F_1F_2$) и отсутствие какой-либо зависимости для совпадений ($D_2F_1F_2$). Постоянный уровень вероятности тройных совпадений вне области телепортации там, где фотоны 1 и 2 попадают на детекторы F_1 и F_2 независимо друг от друга, составляет $50\,\% \times 50\,\% = 25\,\%$ (50 % от вероятности совпадений фотонов 1 и 2, и 50 % от вероятности фотону 3, не имеющему в этом случае определенной поляризации, попасть на D_1 или D_2). Экспериментальные результаты, полученные в [16], подтвердили это как для телепортации фотона 1 с поляризацией 45° (рис. 9а, б), так и для фотона 1, имеющего поляризацию −45° (рис. 9в, г). Телепортация была также проведена для фотонов, находящихся в суперпозиции этих поляризационных состояний: 0°, 90° и для циркулярно поляризованных фотонов.

Реализация квантовой телепортации состояний приоткрывает новые возможности в решении проблемы передачи легко разрушаемых суперпозиционных состояний на большие расстояния без потери ими когерентности, что является камнем преткновения для создания квантовых компьютеров. Кроме этого проблема телепортации, несомненно, затрагивает ряд вопросов принципиального характера, в частности, обмена квантовой информацией в сложных пространственно разнесенных молекулярных структурах, в том числе биологических.

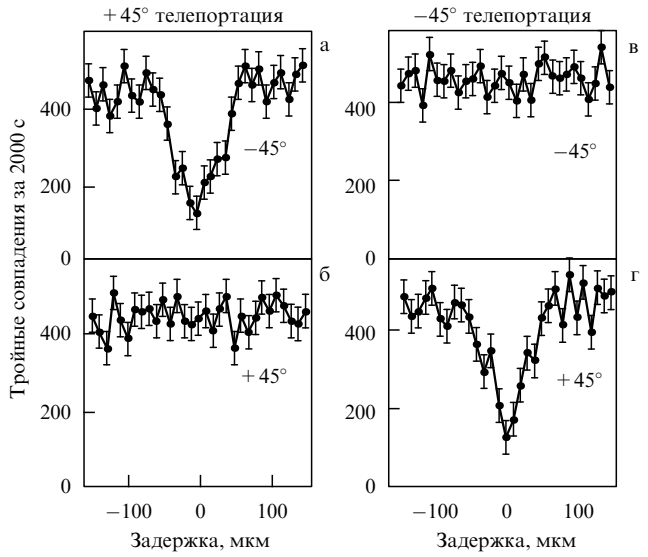


Рис. 9. Скорость совпадения отсчетов тройных совпадений $D_1F_1F_2(-45°)$ и $D_2F_1F_2(+45°)$ как функция задержки между фотонами 1 и 2, реализуемой перемещением зеркала, переотражающего импульсы накачки. Телепортирование фотона 1, поляризованного при +45° (а и б) или −45° (в и г).

Значение работы [16] и последовавших за ней экспериментов[2] [18] состоит еще и в том, что после них обсуждения информационного аспекта квантовой механики окончательно перешли с уровня "мысленных экспериментов" в разряд "практически значимых". Кроме того, эксперименты по телепортации еще раз продемонстрировали, что "классическая" трактовка квантовой механики, опирающаяся на понятия "состояния", "суперпозиция состояний", "редукция", не дававшая ранее сбоя в предсказании *результатов экспериментов*, была состоятельной и в этот раз. Точно так же, как любое квантовомеханическое измерение фиксирует реализацию одной из возможностей, которые возникают из начально приготовленного состояния, измерение на стороне Алисы фиксирует возможность для Боба получить фотон 3 в исходном состоянии фотона 1, которая является только одной из возможностей, предоставляемых начальным состоянием трех фотонов, два из которых (2 и 3) первоначально находились в перепутанном состоянии, генерируемым общим источником. При этом, однако, не следует забывать, что возможности в квантовой механике для произвольных начальных состояний не описываются положительно определенными вероятностями (или плотностями вероятностей), т.е. их описание не сводится к классической теории вероятностей. Конечно, для отдельных экспериментов, измерений и состояний можно подыскать альтернативную интерпретацию, основанную на классических вероятностях, однако можно ли это сделать в общем случае, пока неизвестно. Современное состояние этого вопроса изложено в [19].

[2] Когда настоящая статья находилась на рассмотрении в редакции, появились две экспериментальные работы, в которых были реализованы безусловная квантовая телепортация при использовании сжатых двухмодовых оптических полей (Furusawa A, Sörensen J L, Braunstein S L, Fuchs C A, Kimble H J, Polzik E S *Science* **282** 706 (1998)) и полная квантовая телепортация магнитных состояний ядра водорода на состояния ядра хлора в пределах одной молекулы трихлорэтилена (Nielsen M A, Knill E, Laflamme R, http: // xxx.lanl.gov/archive/quant-ph/ 9811020).

4. Квантовая криптография

Одним из направлений квантовой информации, наиболее продвинутых в область практических приложений, является квантовая криптография. Задача криптографии состоит в передаче информации между двумя сторонами (Алисой и Бобом) так, чтобы попытка перехватить передачу или узнать секретный код была обречена на неудачу. Современными методами классической криптографии эта задача *почти* решается, например, в рамках "симметричной" криптосистемы, опирающейся на создание секретного кода.

В этой системе Алиса и Боб, и только они, имеют секретный код — последовательность случайных чисел, например, десятичных:

$$K = \{12793\ 41169\ 42357\ldots\}.$$

По заданному правилу каждой букве алфавита ставится в соответствие десятичное число и Алиса, желающая переслать Бобу послание, заменяет в послании каждую букву соответствующей ей цифрой. Сама по себе эта процедура не имеет защиты и легко дешифруется. Получающаяся последовательность чисел

$$P = \{73997\ 68279\ 65867\ldots\},$$

послание, затем шифруется — к каждому числу послания прибавляется число из кода и получающиеся цифры в разряде единиц представляют собой криптограмму

$$C = \{85680\ 09338\ 07114\ldots\},$$

которую можно пересылать по открытому каналу (телефону и пр.). Боб, получив криптограмму и зная код K, расшифровывает ее, получая послание C. Отметим, что последовательности K, P и C, приведенные выше, взяты из реального послания, которое посылал Че Гевара из Боливии Ф. Кастро на Кубу в 1967 г. [20].

В 1949 г. С. Шеннон, опираясь на разработанную им теорию информации, доказал теорему, что данная криптосистема является абсолютно секретной, если секретный код *истинно случайный* и он используется только один раз [21]. Однако на практике реализация данной системы наталкивается на серьезные трудности. Одна из них — создание и передача большого секретного кода, необходимого каждый раз, когда посылается новое сообщение. Избежать этой сложности можно было бы при наличии физического канала, секретность которого обеспечивалась бы физическими законами. Именно такой канал и представляет квантовая физика.

Квантовая криптография опирается так же, как и квантовая телепортация, на невозможность клонирования отдельного квантового объекта. Если в качестве передатчика секретного кода выступают состояния отдельных частиц, то при попытке зарегистрировать эти состояния внешним наблюдателем они разрушаются. Факт попытки перехвата можно обнаружить, используя определенное соглашение (протокол) между Алисой и Бобом.

Один из таких протоколов связан с кодировкой поляризационных состояний фотонов в двух альтерна-

тивных базисах[3], не ортогональных друг другу [22]. Передача секретного кода осуществляется в несколько этапов (рис. 10).

№	Действия								Секретность
1	A → B	1	0	0	1	0	0	1	1	секретно
		↕	/	↔	\	↔	↔	↕	↕	квант. канал
2	B измеряет	+	+	×	×	+	×	×	+	открытый канал
		↕	↕	/	\	↔	/	/	↕	секретно
3	A → B: тип изм. A → B: верно	√			√	√			√	открытый канал
4	A и B создают код	↕			\	↔			↕	секретно
		1			1	0			1	

Рис. 10. Последовательность действий для квантовой криптографии при использовании кодировки поляризационных состояний.

1. Предварительно Алиса и Боб договариваются о кодировке (фотоны с поляризацией 0° и 45° кодируют число 0, фотоны с поляризацией 90° и 135° — единицу). Затем Алиса случайным образом меняет поляризацию фотонов, посылаемых по квантовому каналу Бобу.
2. Боб измеряет поляризацию получаемых фотонов, случайным образом меняя ориентацию анализатора для распознавания поляризации 0° и 90°(+) или 45° и 135°(×). Как сказано выше, согласно теории информации Шенона, рассматриваемая криптосистема будет секретной только в случае, если используемый код случайный. Именно случайности кода и добиваются Алиса и Боб, случайно меняя поляризаторы.
3. По открытому каналу Боб сообщает Алисе, какой тип измерения он выполнял для каждого фотона, а Алиса подтверждает, верно или нет он выбрал его.
4. Оставляя из всей последовательности только верно выбранные измерения, Алиса и Боб создают секретный код.

Внешний наблюдатель, пытаясь узнать секретный код, обязательно должен пытаться считывать информацию из квантового канала. Но при этом он вызовет несовпадения в кодах, которые получат Алиса и Боб, так как измерения внешнего наблюдателя необратимым образом разрушают поляризационные состояния фотонов, передаваемых по квантовому каналу. Делая проверку совпадений по случайной выборке, Алиса и Боб обнаружат превышение уровня ошибок по сравнению с уровнем ошибок, генерируемых детекторами. Тем самым будет установлен факт попытки нарушения секретности.

[3] Каждая из цифр кодируется двумя поляризациями для достижения гарантии секретности. Если использовать только один базис, то остается только квантовый канал для передачи кода от Алисы к Бобу. Но в этом случае, даже если Алиса и передаст случайный код, у Боба не будет возможности проверить истинный он или испорченный попытками перехвата.

Другим протоколом, который может использоваться при передаче квантового кода, является *фазовая модуляция* с интерферометрическим детектированием [23], основанным на интерференции одного фотона с самим собой в интерферометре, образованном двумя интерферометрами Маха – Цандера (рис. 11). Фотон, посылаемый Алисой, в зависимости от его пути попадает в детектор на стороне Боба в один из трех разделенных временных интервалов. Первый соответствует пути "короткое плечо интерферометра А – короткое плечо интерферометра Б". В средний попадают фотоны по двум неразличимым путям: "короткое плечо интерферометра А – длинное плечо интерферометра Б" и "длинное плечо интерферометра А – короткое плечо интерферометра Б". В последний интервал собираются фотоны, проходящие путь "длинное плечо интерферометра А – длинное плечо интерферометра Б".

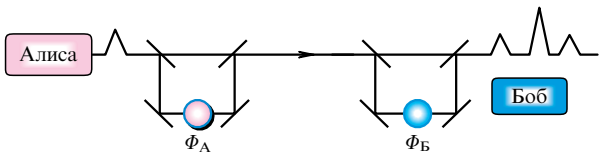


Рис. 11. Схема квантовой криптографии на основе фазовой модуляции с интерферометрическим детектированием.

Вследствие неразличимости путей в среднем интервале должна наблюдаться интерференция, зависящая от разности фаз $\Phi_А$ и $\Phi_Б$ модуляторов, которыми управляют Алиса и Боб. Действительно, вероятность того, что Боб зарегистрирует в центральном окне фотон, равна

$$P_В \propto \cos^2\left(\frac{\Phi_А - \Phi_Б}{2}\right).$$

Следовательно, если Алиса и Боб будут использовать фазы $(\Phi_А,\ \Phi_Б) = (0,3\pi/2)$ для своих 0-битов и $(\Phi_А,\ \Phi_Б) = (\pi/2,\pi)$ для 1-битов, они будут иметь интерферометрический аналог кодировки поляризационных состояний, описанный выше.

В настоящее время для реализации квантового канала в схеме квантовой криптографии наиболее подходящей средой является оптическое волокно, свойства которого позволяют передавать криптограммы на расстояния до 100 км. Использование волокна накладывает ограничения на возможность работы с поляризационной кодировкой, поскольку оптоволокно обладает ощутимыми флуктуациями двулучепреломления. В силу этого для квантовой криптографии используется фазовая модуляция с интерферометрическим детектированием. Для экспериментальной квантовой криптографии необходимо соблюсти некоторые требования: малость потерь в канале (оптоволокно обладает низкими потерями в ИК диапазоне для длин волн 1,3 мкм (0,3 дБ/км) и 1,55 мкм); использование для регистрации фотодетекторов, работающих в режиме счета одиночных фотонов (для выбранной длины волны 1,3 мкм существующие лавинные фотодиоды (Ge или InGaAs) при соответствующей подготовке [23] могут быть использованы для этих целей); невозможность использования усилителей (из теоремы о невозможности клонирования состояний квантовых систем следует, что при передаче по кванто-

вому каналу использование усилителя оказывает такое же разрушающее воздействие, как и попытка перехвата сообщения). В настоящее время реализованы две квантовые криптографические установки [23] и [24]. В [24] сообщается о передаче квантового кода по стандартному оптическому волокну (Swiss Telecom), проложенному по дну Женевского озера на расстояние 23 км. Длина кода, переданного за 11 часов, составила 20 кбит; скорость ошибок составила 1 %, причем эти ошибки генерировались, в основном, германиевым фотодиодом.

Мы провели выше рассмотрение только одного протокола для классической и квантовой криптографии. Существует множество других протоколов. Один из них RSA — наиболее популярная криптосистема с открытой передачей кода. Названа по имени трех создателей R. Rivest, A. Shamir, L. Adelman [25] и основана на использовании двух секретных кодов: одного для шифрования, другого для дешифрования. В этом протоколе в качестве вспомогательного кода, который можно передавать по открытым каналам, используются произведения больших простых чисел (больше 200 знаков). Секретность метода связана со сложностью задачи факторизации больших чисел, решение которой с привлечением современных математических методов и физических устройств не может быть получено за разумные времена для таких длин чисел. Попытка решить математическую часть проблемы привела недавно к разработке быстрой процедуры, реализуемой физически в так называемых квантовых компьютерах, устройствах, для создания которых требуется консолидация достижений во многих областях физики: квантовой оптики, физики твердого тела, лазерной физики, спектроскопии.

5. Квантовые вычисления и компьютеры

5.1. Обратимые и необратимые классические процессоры

Изложению основных принципов квантовых вычислений и квантовых компьютеров предпошлем описание некоторых аспектов действия обычных — классических — компьютеров, не претендуя на полноту описания, а ставя целью наглядность перехода к обсуждению особенностей квантовых вычислений.

Классические компьютеры, как устройства для вычислений, должны оперировать с числами. Простейшее устройство, способное представлять числа, — это устройство, которое имеет два устойчивых состояния. Так, проводники с током могут находиться в двух состояниях: когда нет тока, соответствующих значению 0, а когда есть, — 1. Использование таких устройств для проведения действий над числами возможно благодаря двоичной записи чисел. Для примера, натуральное число 9 в двоичной системе запишется, как $1001 = (1 \times 2^3) + (0 \times 2^2) + (0 \times 2^1) + (1 \times 2^0)$, а сложение чисел выполняется согласно таблице

$$0 + 0 = 0,$$
$$0 + 1 = 1,$$
$$1 + 0 = 1,$$
$$1 + 1 = 0 \text{ (1 в следующем разряде, " в уме").}$$

В настоящее время придумано множество различных устройств, осуществляющих такую операцию сложения. Для наглядности приведем вариант механического устройства для сложения (рис. 12). Данное устройство состоит из заслонок (вентилей) и каналов, соединяющих их. По каналам могут двигаться под действием силы тяжести шарики, переводящие при этом движении заслонки в одно из двух возможных положений: Т-состоянию заслонки приписывается значение 0, а повернутому, λ-состоянию, — значение 1. В состав устройства входят два типа заслонок: заслонки A и C, обозначенные серой штриховкой и выполняющие функцию записи состояния канала, в котором они расположены, а также заслонки B, обозначенные черным цветом и выполняющие функцию логических вентилей (gates) сложения двух битов. Действительно, каждый вентиль B имеет один подводящий канал (слева) и два отводящих (справа), из которых нижний соответствует биту переноса в следующий разряд, а верхний предназна-

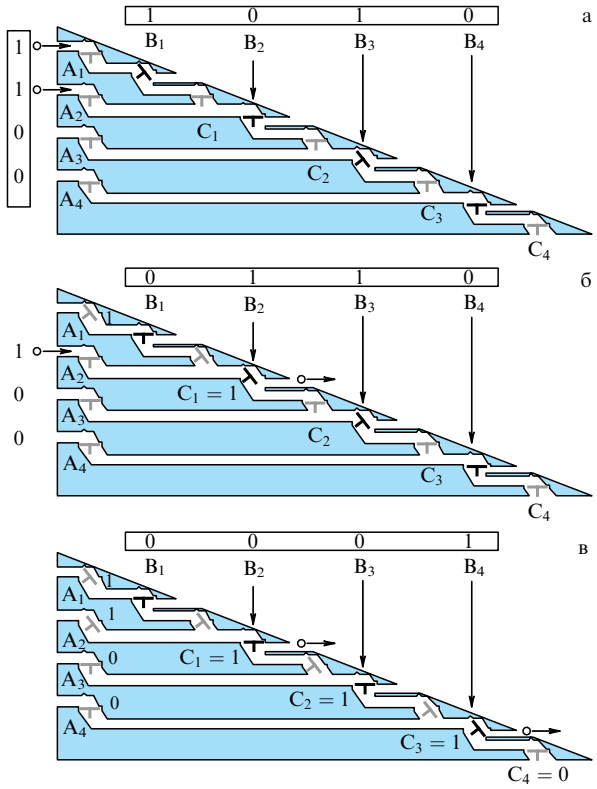


Рис. 12. Механическая схема суммирующего процессора на шариках. Данное устройство состоит из заслонок (вентилей) и каналов, соединяющих их. По каналам могут двигаться под действием силы тяжести шарики, переводящие при этом движении заслонки в одно из двух возможных положений. Т-состоянию заслонки приписывается значение 0, а повернутому, λ-состоянию, — значение 1. В состав устройства входят два типа заслонок: заслонки A и C, обозначенные серой штриховкой и выполняющие функцию записи состояния канала, в котором они расположены, а также заслонки B, обозначенные черным цветом и выполняющие функцию логических вентилей (gates) сложения двух битов. (а) Исходное состояние процессора: на состояниях заслонок (B_4, B_3, B_2, B_1), "записано" число 5 = 101; на входе в устройство с помощью шариков "приготовлено" другое число: 3 = 11. (б) Состояние суммирующего процессора после действия шарика из первого разряда: на регистре $\{A_i\}$"записалось" число 1, а на регистре $\{B_i\}$ — число 110 (5 + 1). (в) Конечное состояние суммирующего процессора после действия шарика из второго разряда: на регистре $\{A_i\}$ записано исходное число 11, регистр $\{B_i\}$ переведен в состояние, соответствующее сумме 101 + 11 = 1000 (5 + 3 = 8).

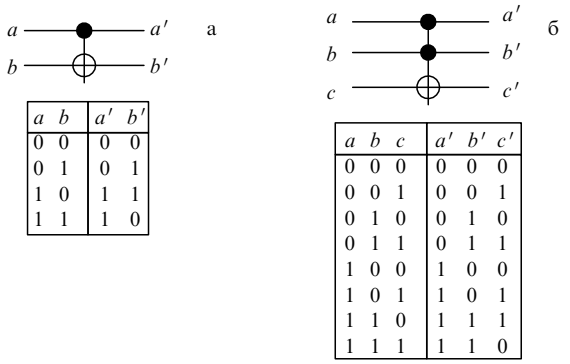
чен для сброса шариков. Если считать, что наличие шарика на входе в вентиль B соответствует 1, а его отсутствие — 0, то данный логический блок осуществляет свое действие согласно табл. 1.

Таблица 1

Начальное состояние входа в вентиль B (наличие шарика — 1, его отсутствие — 0)	Начальное состояние заслонки B ($T = 0, \lambda = 1$)	Конечное состояние заслонки B	Конечное состояние нижнего канала выхода (канала бита переноса)
0	0	0	0
0	1	1	0
1	0	1	0
1	1	0	1

Это действие эквивалентно операции сложения двух битов, если под первым складываемым битом понимать состояние входа B, а под вторым слагаемым — начальное состояние заслонки B, конечное состояние которой и есть результат сложения совместно с конечным состоянием канала бита переноса. Объединяя такие логические вентили в сеть путем присоединения канала переноса к каналу входа логического вентиля следующего разряда, получим процессор для суммирования чисел любой разрядности (рис. 12а – в).

Следует отметить важное обстоятельство действия такого процессора. Этот процессор будет выполнять операцию сложения даже и без наличия заслонок A и C. В этом случае действие сумматора будет необратимым, так как преобразование "*два входа → один выход*" (начальное состояние входа в вентиль B, начальное состояние заслонки B → конечное состояние заслонки B) не позволяет различить по конечному состоянию выхода, что было на входе (ср. вторую и третью строчки в таблице) и, следовательно, обратить операцию. Однако в 1973 г. Чарльз Беннет [26] показал, что все логические операции для построения компьютера (а их всего $4^2 = 16$ для логических вентилей "*два входа → один выход*") могут быть сделаны обратимыми. В случае операции суммирования для обратимости следует сохранить состояния исходного бита, т.е. использовать преобразования типа $(a, b) \to (a' = a, b' = a + b)$, где штрих обозначает конечные состояния входа и выхода. В 1980 г. Том Тоффоли нашел [27], как можно описать обратимыми вычисления, используя традиционный язык булевских логических вентилей, подобных И (AND), ИЛИ (OR) и т.д., но обладающих свойствами обратимости. Одним из таких логических вентилей, который, как оказалось впоследствии, очень важен для квантовых вычислений, является логический вентиль, выполняющий операцию контролируемого НЕ (обратимого XOR): бит b (бит цели) изменяет свое состояние тогда и только тогда, когда состояние бита источника a соответствует 1, при этом состояние бита источника не меняется (рис. 13а). Тоффоли показал также, что можно построить любой обратимый процессор, используя только один логический вентиль — универсальный трехбитовый вентиль Тоффоли (рис. 13б). В этом логическом блоке состояние бита цели (c) меняется тогда и только тогда, когда оба неизменяемых бита источников (a и b) имеют значение 1. Для демонстрации обратимого классического сумматора обратимся опять к рис. 12. Добавляя в рассмотрение состояние заслонок A и C, цель которых записывать состояние входов A_i и битов переноса C_i в каждом разряде, получаем обратимый сумматор. Действительно, если перевернуть относительно горизонтальной оси это устройство (рис. 12в) и последовательно "запустить" шарики, попавшие в каналы сброса, то конечное состояние устройства после прохождения шариков будет совпадать с начальным.



a	b	a'	b'
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

Рис. 13. (а) Графическое представление и *таблица истинности* для элементарного логического вентиля (блока) контролируемого НЕ: бит b (бит цели) изменяет свое состояние тогда и только тогда, когда состояние бита источника a соответствует 1, при этом состояние бита источника не меняется. Каждая горизонтальная линия представляет собой состояние одного бита, изменяющегося во времени слева направо. Символы на двух линиях, соединенных вертикальной линией, означают совместное действие двух вентилей на эти биты. Очевидно, что *таблица истинности* для этого логического вентиля, называемого также ИСКЛЮЧАЮЩЕЕ ИЛИ (XOR), соответствует таблице сложения двух битов, если в последней не учитывать бита переноса. (б) Графическое представление и *таблица истинности* для трехбитового логического вентиля Тоффоли, являющегося *универсальным* для построения обратимой булевской логики. Его действие сводится к изменению состояния бита цели c при условии, что оба неизменяемых бита источников (a и b) имеют значение 1. Каждая горизонтальная линия представляет собой состояние одного бита, изменяющегося во времени слева направо. Символы на трех линиях, соединенных вертикальной линией, означают совместное действие трех вентилей на эти биты.

Действие такого обратимого суммирующего процессора эквивалентно представляется логической схемой — сетью (рис. 14), демонстрирующей развитие во времени состояний битов, входящих в состав процессора. От подобной обратимой логической сети состояний битов до понятия квантового процессора — один шаг. И сделан он был в восьмидесятые годы Р. Фейнманом [28, 29], который осознал, что вместо классических состояний битов для построения обратимых сетей для вычислений можно использовать состояния квантовых систем, как объектов, подчиняющихся обратимой гамильтоновой динамике. Это время можно считать началом истории развития квантовых компьютеров.

5.2. Квантовые компьютеры

Квантовые компьютеры — физические устройства, выполняющие логические операции над квантовыми состояниями путем унитарных преобразований, не нарушающих квантовые суперпозиции в процессе вычислений. Очень схематично работа квантового компьютера может быть представлена как последовательность трех операций:

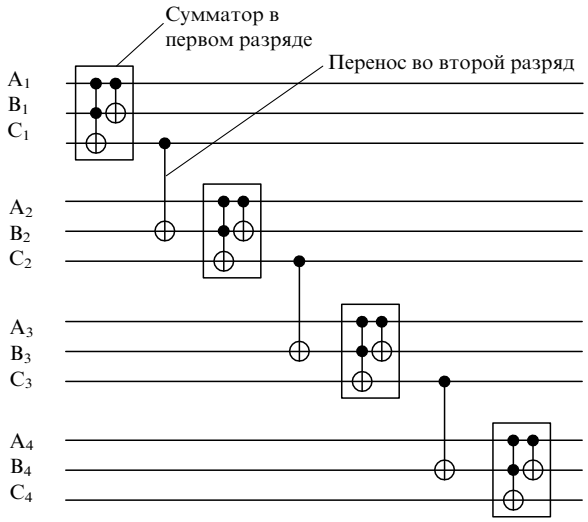


Рис. 14. Логическая схема обратимого сумматора, механическая схема которого представлена на рис. 12. Горизонтальные линии соответствуют состояниям битов разрядов двух складываемых чисел (A_4, A_3, A_2, A_1) и (B_4, B_3, B_2, B_1), а также битов переносов в следующие разряды (C_4, C_3, C_2, C_1). Поразрядно *суммирующие блоки* представляют операцию, которую может производить шарик, попадающий на заслонки B_i в механической схеме: заслонка B_i изменяет свое состояние при условии, что в канале A_i присутствует шарик; если к тому же состояние заслонки B_i до взаимодействия с шариком равно 1, то шарик переходит в следующий разряд по каналу переноса, меняя состояние заслонки C_i, которая исходно имела состояние 0. *Блоки переноса* в последующие разряды осуществляют операцию контролируемого НЕ путем изменения состояния заслонки B_{i+1} шариком, попавшим на вход $i+1$-го суммирующего вентиля из канала бита переноса C_i.

1) запись (приготовление) начального состояния;

2) вычисление (унитарные преобразования начальных состояний);

3) вывод результата (измерение, проецирование конечного состояния).

1) Как продемонстрировано выше, обычный числовой компьютер оперирует с битами — булевскими переменными, принимающими значения 0 и 1 — и на любом этапе вычислений компьютер имеет определенные значения в каждом бите, используемом для вычислений. Причем эти значения можно измерить. На первом этапе вычислений необходимо записать исходные данные в регистр — набор битов, каждый из которых должен иметь определенные значения (0 или 1).

Квантовый компьютер оперирует с состояниями. Простейшей системой, выполняющей функцию, аналогичную битам в классических компьютерах, является система с двумя возможными состояниями. Для обозначения состояния такой квантовой двухуровневой системы предложен специальный термин: *q-бит* (*qubit*) — квантовый бит информации — состояние квантовой системы с двумя возможными базовыми состояниями $|0\rangle$ и $|1\rangle$. Общее состояние такой системы есть суперпозиция

$$|q\rangle = c_0|0\rangle + c_1|1\rangle\,,$$

— нечто большее, чем булевское 0 или 1; q-бит — это квантовая суперпозиция двух чисел: нуля и единицы! Физическими системами, реализующими q-биты, могут быть любые объекты, имеющие два квантовых состояния: поляризационные состояния фотонов, электронные состояния изолированных атомов или ионов, спиновые состояния ядер, нижние состояния в квантовых точках и др.

Уже первая операция всех (классических и квантовых) вычислений — приготовление начального состояния регистра — демонстрирует возможные преимущества квантовых операций с q-битами. При наборе начального числа на классическом регистре, состоящем из w битов, нам потребуется w операций — на каждом бите установить значения 0 или 1. При этом будет записано только одно число длиной w. При совершении w унитарных операций с каждым q-битом в квантовом регистре — устройстве, состоящем, например, из w квантовых точек (рис. 15) — мы приготовим когерентную суперпозицию всех $Q = 2^w$ состояний общей системы квантового регистра. Тем самым мы приготовим вместо одного числа сразу 2^w возможных значений регистра — когерентную

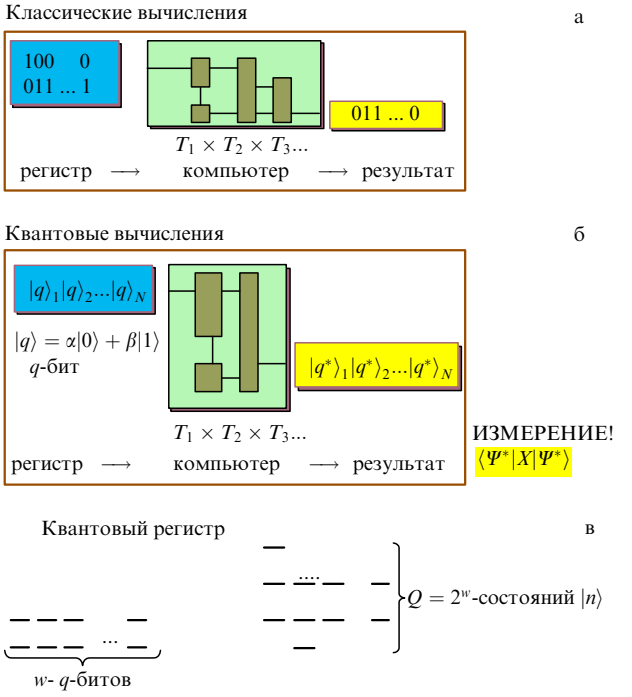


Рис. 15. Квантовые компьютеры — физические устройства, выполняющие логические операции над квантовыми состояниями путем унитарных преобразований, не нарушающих квантовые суперпозиции в процессе вычислений. Схематично работа квантового компьютера (б) может быть представлена как последовательность трех операций: запись (приготовление) начального состояния; вычисление (унитарные преобразования начальных состояний); вывод результата (измерение, проецирование конечного состояния). В отличие от обычного числового компьютера (а), оперирующего с битами — булевскими переменными, принимающими значения 0 и 1, квантовый компьютер оперирует с q-*битами* (*qubit*) — квантовыми битами информации — состояниями квантовой системы с двумя возможными базовыми состояниями $|0\rangle$ и $|1\rangle$. Физическими системами, реализующими q-биты, могут быть любые объекты, имеющие два квантовых состояния: поляризационные состояния фотонов, электронные состояния изолированных атомов или ионов, спиновые состояния ядер, нижние состояния в квантовых точках и др. Вывод результата квантового вычисления является вероятностным — требуется несколько измерений, чтобы извлечь информацию о конечном состоянии квантового компьютера. (в) Квантовый регистр образуют состояния нескольких q-битов. При количестве q-битов в регистре число состояний экспоненциально больше: $Q = 2^w$.

суперпозицию всех возможных для данного регистра чисел. Естественно, это свойство может быть использовано для квантовых параллельных вычислений.

2) Применяя к приготовленным состояниям унитарные преобразования, выполняющие те или иные логические операции, можно реализовать собственно квантовый процессор. Роль соединений (проводов) в обычных компьютерах играют q-биты, а роль логических блоков (вентилей), на которые разбивается весь процесс вычислений как в классическом, так и квантовом процессоре, — унитарные преобразования. Такая концепция квантового процессора и квантовых логических вентилей была предложена в 1989 г. Д. Дейчем, который также нашел универсальный логический блок (аналогичный вентилю Тоффоли в обратимых классических процессорах), с помощью которого можно выполнить любые квантовые вычисления [30]. Недавно было показано, что одно- и двухбитных блоков достаточно для получения всего необходимого набора преобразований [31–34]. Среди таких логических блоков — операция отрицания НЕ (квантовый аналог заслонок A и C в схеме классического сумматора)

$$\widehat{T}_{\mathrm{NOT}} = |0\rangle\langle 1| + |1\rangle\langle 0|\,, \tag{14}$$

действующая на одиночный q-бит и меняющая его состояние:

$$\widehat{T}_{\mathrm{NOT}}|0\rangle = |1\rangle\,, \qquad \widehat{T}_{\mathrm{NOT}}|1\rangle = |0\rangle\,,$$

и операция УСЛОВНОЕ НЕ (квантовый аналог логического вентиля B в схеме, рассмотренной выше)

$$\widehat{T}_{\mathrm{XOR}} = |0\rangle_{11}\langle 0|\widehat{I}_2 + |1\rangle_{11}\langle 1|\widehat{T}_{2\mathrm{NOT}}\,, \tag{15}$$

применяемая к двум q-битам, первый из которых не меняет состояния под действием $\widehat{T}_{\mathrm{XOR}}$, а второй меняет, но в зависимости от состояния первого q-бита. Например,

$$\widehat{T}_{\mathrm{XOR}}\big(\alpha|0\rangle_1 + \beta|1\rangle_1\big)|0\rangle_2 = \alpha|0\rangle_1|0\rangle_2 + \beta|1\rangle_1|1\rangle_2\,, \tag{16}$$

т.е. операция $\widehat{T}_{\mathrm{XOR}}$ трансформирует суперпозиционные состояния в перепутанные и обратно. Квантовый аналог логического вентиля Тоффоли (УСЛОВНОЕ–УСЛОВНОЕ НЕ) (рис. 13б) действует на состояния трех q-битов согласно соотношению

$$\widehat{T}_{\mathrm{Toffoli}}\big(\alpha|0\rangle_1 + \beta|1\rangle_1\big)\big(\gamma|0\rangle_2 + \delta|1\rangle_2\big)\big(\mu|0\rangle_3 + \nu|1\rangle_3\big) =$$

$$= \Big(\alpha|1\rangle_1\big(\gamma|0\rangle_2 + \delta|1\rangle_2\big) + \beta\gamma|0\rangle_1|0\rangle_2\Big)\big(\mu|0\rangle_3 + \nu|1\rangle_3\big) +$$

$$+ \beta\delta|1\rangle_1|1\rangle_2\big(\mu|1\rangle_3 + \nu|0\rangle_3\big)\,. \tag{17}$$

Квантовые логические блоки, объединенные вместе и в определенной последовательности действующие на состояния q-битов, образуют квантовую сеть. Если в качестве примера обратиться к схеме обратимого суммирующего процессора (см. рис. 12) и предположить, что вместо заслонок стоят двухуровневые системы, взаимодействия между которыми соответствуют унитарным преобразованиям (15)–(17), то образованная сеть (см. рис. 14) будет представлять собой простейшую квантовую сеть — сумматор.

3) Операция вывода результата вычисления для классического компьютера ничем не отличается от любой другой операции во время вычислений. Вычисления могут быть остановлены в любом месте, промежуточные результаты прочитаны и вычисления продолжены. В квантовом компьютере это не так. Конечным результатом квантовых вычислений является состояние квантового регистра после совершенных унитарных преобразований, представляющее собой когерентную суперпозицию всех возможных для данного регистра состояний. Очевидно, что мы не можем получить все амплитуды вероятностей C_j в разложении этого суперпозиционного состояния. Все, что мы можем получить от этого одиночного квантового объекта, что доступно нам согласно квантовой теории — квадратичные формы $\sum_{i,j} C_i C_j^* R_{ij}$, соответствующие измерению среднего значения некой физической величины, которой соответствует оператор R. Причем очевидно, что конечный результат квантовых вычислений будет флуктуировать от вычисления к вычислению. Однако даже в таких условиях квантовых неопределенностей квантовые компьютеры могут дать существенное ускорение вычислений некоторых математических задач.

5.2.1. Квантовые компьютеры и математические проблемы. Когда Р. Фейнман впервые обратил внимание на возможность построения процессора, работающего по квантовомеханическим принципам [29], не было понятно, в решении каких математических проблем такой компьютер может дать преимущество по сравнению с обычными процессорами? Первый реалистичный пример был найден в 1994 г. П. Шором [35] — задача факторизации большого n-значного числа. В качестве пояснения: задача вычисления произведения двух простых чисел, скажем 521 и 809, не вызывает никаких затруднений. Однако обратная задача: нахождение простых сомножителей числа 421489, потребует определенного времени. Известно, что это время (при использовании известных теперь классических алгоритмов) растет с ростом длины n факторизуемого числа, как $\exp(n^{1/3})$. Достижение Шора состоит в том, что он нашел алгоритм, основанный на особенности квантовых вычислений, уменьшающий рост этого времени до полиномиального (n^2). Отметим, что задача факторизации относится к классу математических задач, в которых решение сводится к поиску среди экспоненциально большого класса кандидатов.

Алгоритм решения задачи факторизации опирается на сводимость ее к нахождению периода вспомогательной функции. Такой функцией является остаток от деления степенно́й функции a^x на целое число N:

$$f_N(x) = a^x \bmod N\,.$$

Например, при $a = 11$, $N = 15$ значения функции $f_N(x)$ при $x = 0, 1, 2, 3$ равны соответственно 1, 11, 1, 11, т.е. период функции $11^x \bmod 15$ равен 2. Далее процедура нахождения простых делителей в этом примере сводится к следующим операциям $11 \pm 1 = 10, 12$; $15 - 10 = 5$; $15 - 12 = 3$.

Шор показал, что процедура нахождения периода функции с помощью квантовых вычислений значительно ускоряется. Последовательно должны выполняться следующие операции (рис. 16):

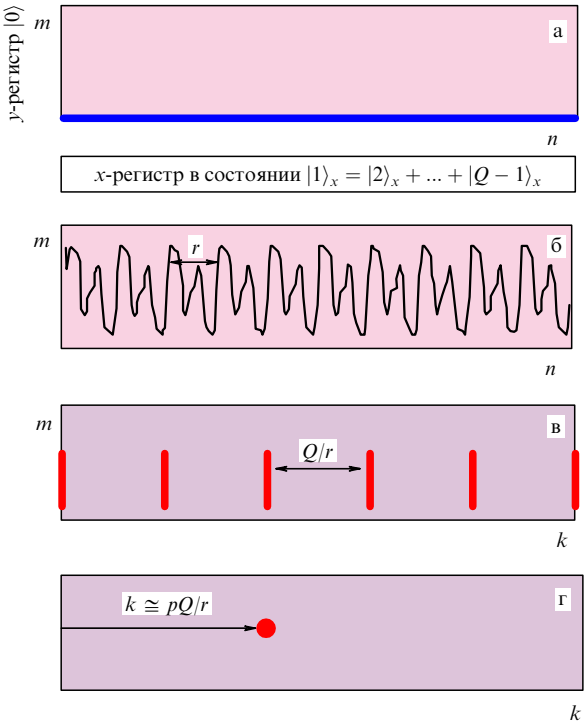


Рис. 16. Процедура нахождения периода периодической функции с помощью квантовых вычислений. (а) Приготовление независимых состояний двух регистров: x и y. По оси абсцисс отложены номера n базисных состояний $|n\rangle_x$ в x-регистре, по оси ординат — номера m состояний $|m\rangle_y$ в y-регистре. Линия на плоскости отмечает номера состояний в двух регистрах, участвующих в образовании исходного состояния. (б) Изображение перепутанного состояния двух регистров (18), в котором номера связанных состояний y- и x-регистров образуют дискретную периодическую функцию $m(n)$ с периодом r. (в) Изображение того же состояния, но в измененном дискретным преобразованием Фурье (19) базисе x-регистра. В силу периодичности рассматриваемой функции в новом базисе задействованными в перепутанном состоянии оказываются только состояния с номерами k, локализованными вблизи значений Q/r. (г) В силу такой локализации достаточно нескольких измерений состояний x-регистра, чтобы определить искомый период r.

(A) Приготовление двух регистров: одного — для записи аргументов (x-регистр), второго — для значений периодической функции, например целочисленной функции $f_N(x) = a^x \bmod N$. Пусть в x-регистре количество q-битов w, тогда такой регистр содержит $Q = 2^w$ возможных состояний, которые мы будем обозначать, как $|n\rangle_x$ (см. рис. 16). Количество q-битов может быть экспоненциально меньше периода r функции $f_N(x)$. y-регистр содержит такое же количество битов; базовые состояния этого регистра будем обозначать, как $|m\rangle_y$. Первоначально находившийся в "невозбужденном", основном состоянии x-регистр переводится поворотом каждого q-бита на 45° в состояние однородной суперпозиции:

$$\frac{1}{\sqrt{Q}}\left(|0\rangle_x + |1\rangle_x + |2\rangle_x + |3\rangle_x + \ldots + |Q-1\rangle_x\right)|0\rangle_y .$$

Далее, путем *однократного* применения правильно подобранного унитарного преобразования U_f переводим это состояние в перепутанное состояние двух регистров:

$$\frac{1}{\sqrt{Q}}\left(|0\rangle_x|f_N(0)\rangle_y + |1\rangle_x|f_N(1)\rangle_y + |2\rangle_x|f_N(2)\rangle_y + \right.$$
$$\left. + |3\rangle_x|f_N(3)\rangle_y + \ldots + |Q-1\rangle_x|f_N(Q-1)\rangle_y\right) . \qquad (18)$$

Это состояние схематически изображено как некая периодическая функция на рис. 16б, причем каждой точке на графике соответствует пара целочисленных значений $(n, m = f_N(n))$, обозначающих слагаемое $|n\rangle_x|f_N(n)\rangle_y$ в сумме (18); значение n откладывается по оси абсцисс, значение m — по оси ординат.

(B) Следующая операция — **дискретное преобразование Фурье** над состояниями x-регистра. Соответствующее унитарное преобразование (преобразование базиса)

$$T_{\mathrm{FT}} = \frac{1}{Q}\sum_{n=0}^{Q-1}\sum_{k=0}^{Q-1}\exp\left(\frac{2\pi i k n}{Q}\right)|k\rangle_{xx}\langle n| , \qquad (19)$$

примененное к состоянию (18) приводит к новому состоянию обоих регистров:

$$\sum_{k=0}^{Q-1}\sum_{m=0}^{r}\Delta_{km}|k\rangle_x|f_N(m)\rangle_y , \qquad (20)$$

где амплитуда, соответствующая каждому состоянию в x-регистре

$$\Delta_{km} = \sum_{l=0}^{G_m}\exp\frac{2\pi i k(lr+m)}{Q} = \exp\frac{2\pi i k m}{Q}\times$$
$$\times\frac{\exp(2\pi i k r G_m/Q) - 1}{\exp(2\pi i k r/Q) - 1} , \qquad (21)$$

имеет максимум при $k = pQ/r$ (рис. 16в). Очевидно, предполагается, что общее число состояний Q не кратно периоду r. В формуле (21)

$$G_m = \left[\frac{Q}{r}\right] + \theta(Q \bmod r - m) ,$$

т.е. G_m равно или числу периодов r, укладывающихся в общем числе состояний Q, или на единицу больше, в зависимости от того больше или нет остаток от деления Q на r, чем номер m.

(C) Результатом **измерения** (одного или нескольких) состояния x-регистра будут значения приблизительно кратные отношению Q/r в силу локализации амплитуд Δ_{km} вблизи этих значений (рис. 16в). Тем самым определяется значение периода r.

Отметим, что использование фурье-стробирования для нахождения неизвестного периода аналогично дифракции рентгеновских лучей или нейтронов для измерения периода решетки. Однако, если аппроксимировать задачу о факторизации 200-значного числа на задачу дифракции, то нам потребовалось бы иметь кристалл с периодом 10^{200} А размером грани 10^{400} А при использовании излучения 1 А, что, естественно, вряд ли возможно.

Математические проблемы, решение которых сводится к поиску решения среди экспоненциально большого числа кандидатов, не ограничиваются задачей о факторизации. Недавно была предложена еще одна задача, решение которой ускоряется при использовании квантовых вычислений, — поиск среди элементов базы данных, каждый из которых на запрос может давать ответ (ДА/НЕТ) [36]. Однако другие подобные задачи до сих пор ждут своего решения. К таким задачам относятся комбинаторные, среди которых выделяется проблема коммивояжера [37]: найти кратчайший путь между n точками с известными расстояниями между парами, проходящий через каждую точку один раз. К

задачам типа коммивояжера относится задача доставки продуктов питания в магазины, подвода электроэнергии потребителям, построения кольцевых линий электропередач и др. Поиск алгоритмов решения таких задач, основанных на возможностях квантовых вычислений, — одна из важнейших проблем теории квантовой информации. Другой, такой же важной проблемой, является коррекция ошибок, генерируемых при вычислениях. Причем, в силу очень чувствительного характера квантовых состояний к внешним возмущениям, коррекции ошибок следует уделять значительно большее внимание, чем при классических вычислениях [38, 39].

5.2.2. Квантовые компьютеры и физические проблемы. Проблемы создания квантового компьютера в настоящий период времени — это прежде всего физические проблемы. Основная из них — быстрый распад суперпозиционных состояний и превращение их в смесь. Этот процесс называется *декогеренцией*, и выяснение природы его объясняет парадокс шрёдингеровского кота (см. раздел 6). Декогеренция накладывает основное требование на физические элементы, предполагаемые к использованию в квантовых компьютерах: время сохранения когерентности состояний должно быть больше времени вычисления. Отсюда следуют два способа избежать распада когерентности: найти квантовую систему, максимально изолированную от окружения, или увеличивать время когерентности искусственно.

Пути поиска хорошо изолированных квантовых систем можно суммировать, как это представлено в табл. 2. Изоляция полевых квантовых систем — мод поля — возможна в высокодобротных микрорезонаторах оптического [40] и микроволнового [41] диапазонов, в которых при миллиметровых размерах резонаторов достигаются параметры, обеспечивающие время сохранения суперпозиционных оптических состояний от секунд до микросекунд при изменении числа фотонов в моде от единиц до 100 [42] для микроволнового диапазона. Другим, перспективным методом полевой изоляции, является использование поверхностных мод типа "мод шепчущих галерей" на поверхности микросфер из синтетического кремния [43], где возможно достижение добротности порядка $10^9 - 10^{10}$, что соответствует времени затухания мод 1 – 0,1 мкс [44]. Принципиально новым методом изоляции является использование трехмерных периодических диэлектрических структур — фотонных кристаллов [45, 46], идеально "запирающих" фотоны определенной полосы частот внутри кристалла. Локализация фотонов в фотонных кристаллах настолько велика, что при взаимодействии с ними отдельного атома должно наблюдаться явление замораживания спонтанного распада и безинверсная генерация когерентного монохроматического субпуассоновского излучения [47, 48]. Предложено несколько материалов — кандидатов для фотонных кристаллов. Наиболее перспективным из них на настоящее время является синтетический опал [49, 50].

Таблица 2. Локализация одиночных квантовых систем

Поле	Вещество
Микрорезонаторы: *оптические* [40]; *микроволновые* [41, 42]	***Пучки*** ***Ловушки для ионов***: *Paul trap* [51]; *end-cap* [52, 53]; *квадрупольные кольцевые* [54] ***Лазерные ловушки*** [57, 58]
Резонаторы мод "шепчущих галерей" [43, 44] ***Фотонные кристаллы*** [45 – 50]	***Естественно изолированные системы***: *молекулы в аморфном и поликристаллическом окружении* [60, 61]; *примеси в кристаллах* [62]; *молекулы в биоструктурах* [63 – 65] (*метод исследования: спектроскопия одиночных молекул* [66 – 68]) ***Квантовые точки*** [69] ***Ядерные спины молекул*** [70 – 72]

Изоляция отдельных массивных частиц: атомов, молекул, ионов исторически начиналась с одномерной изоляции в пучках (табл. 2). Среди других методов изоляции (локализации):

1. Квадрупольные ловушки для ионов, так называемые ловушки Пауля [51] различных конфигураций, позволяющих удерживать один ион (концевая квадрупольная ловушка, *endcap trap* [52], приспособленная для облучения лазерными пучками [53]) или несколько (кольцевые квадрупольные ловушки [54]). Последние, кстати, рассматриваются как возможный кандидат для создания квантового регистра [55]. Отметим успешную демонстрационную реализацию двух-q-битового квантового логического вентиля, реализованного на охлажденном ионе бериллия [56].

2. Оптические ловушки для нейтральных атомов [57, 58]. Наблюдение бозе-эйнштейновского конденсата [59] заставляет думать и об этом возможном объекте для квантовых вычислений.

3. Методы матричной изоляции молекул в поликристаллических и аморфных средах [60], гелях [61], а также примесных центров в кристаллах [62] и молекул в пространственно-организованных биоструктурах: ДНК [63], белках [64], фотосинтетических антенных комплексах [65]. Значительный прогресс в исследовании отдельных изолированных молекулярных систем обеспечивается быстрым развитием эксперимента и теории спектроскопии одиночных молекул [66 – 68].

4. Квантовые точки [69].

5. Весьма перспективный объект для проведения квантовых вычислений — ядерные спины молекул, которые в силу экранирования оказываются сильно изолированными от влияния окружения. Времена сохранения когерентной суперпозиции могут достигать секунд и более. При этом, используя большое число молекул, например, в растворе, можно оперировать квантовыми регистрами с числом состояний 2^n, где n — число спинов в одной молекуле, а не число молекул в растворе [70]. Созданные природой объекты — молекулы, по-видимому, могут рассматриваться как отдельный, уже существующий, элементарный квантовый компьютер. Есть первые экспериментальные реализации логических блоков с помощью ЯМР на трех ядерных спинах (протонный и углеродные спины трихлорэтилена) [71]. В [72] сообщено о демонстрации на ядерных спинах трихлорметана (хлороформа) первого квантового алгоритма, позволяющего выполнить за одно действие процедуру, аналогичную идентификации за одну попытку изображения на каждой стороне одной монеты: орел, решка или две

стороны одинаковы [4]. Следует отметить принципиальное отличие выполнения квантовых вычислений на распределенных в объеме и изолированных от окружения квантовых объектах. Оно сродни отличию экспериментов на ансамбле объектов и ансамбля экспериментов на одном объекте.

Из других физических проблем, связанных с реализацией идеи квантовых вычислений, следует выделить поиск конкретных процессов, выполняющих логические операции. Одиночные ионы, взаимодействующие с микроволновыми полями в резонаторах [73, 74], колебательное движение иона как целого в ловушках [55, 56] позволяют выполнять операции XOR. Перспективным является метод динамического управления квантовомеханическим процессом туннелирования с помощью лазерного излучения [75].

При использовании полевых объектов в качестве логических элементов, а не только передатчика, важны методы измерения квантовых состояний оптических полей, позволяющие регистрировать сложные суперпозиции. Примером такого метода является квантовая томография [76] и различные методы квантовых неразрушающих измерений [77]. В тех устройствах, где необходимо использовать полевые состояния с заданным числом фотонов, например, соединения узлов квантовой информационной сети, требуется решить целый блок проблем генерации субпуассоновского излучения [78], среди которых выделяется поиск практически реализуемых методов генерации, основанных как на унитарных [79], так и на неунитарных (проекционных) [80–85], преобразованиях.

Если по тем или иным причинам не удается добиться желаемой изоляции объекта, и ошибки, вносимые взаимодействием с окружением, нарушают квантовую когерентность, можно воспользоваться активными методами коррекции квантовых ошибок, среди которых метод, основанный на увеличении числа каналов, по которым передается информация, с последующей коррекцией на основе того или иного протокола [38, 39]; метод организации взаимодействия с окружением [86–90]; методы, основанные на использовании обратной связи [91–94] или пассивные [95]. Все они направлены на решение проблемы декогеренции, так ярко отмеченной Шрёдингером в известном примере с состоянием кота [1].

6. Проблема декогеренции

Процесс декогеренции, проявляющийся в быстром превращении чистого состояния в смесь при взаимодействии квантовой системы с окружающей средой, обладает некоторыми общими закономерностями, не зависящими от особенностей взаимодействия. Выбирая в качестве изолированного объекта гармонический осциллятор, который может моделировать многочисленные физические объекты, например, поле в резонаторе или колебания иона в ловушке, а в качестве начального его состояния — суперпозицию двух когерентных состояний, которые определяются одним комплексным параметром — средней амплитудой колебаний, мы получаем в рассмотрение наглядный пример состояния типа шрёдингеровского кота (рис. 17). Физическая наглядность достигается использованием функции квазивероятности Вигнера

$$W(\beta)=\frac{1}{\pi^2}\int \mathrm{d}^2\xi\,\mathrm{Sp}\left\{\widehat{\rho}\,\exp\left[\xi(\widehat{a}^{+}-\beta^{*})-\xi^{*}(\widehat{a}-\beta)\right]\right\}, \tag{22}$$

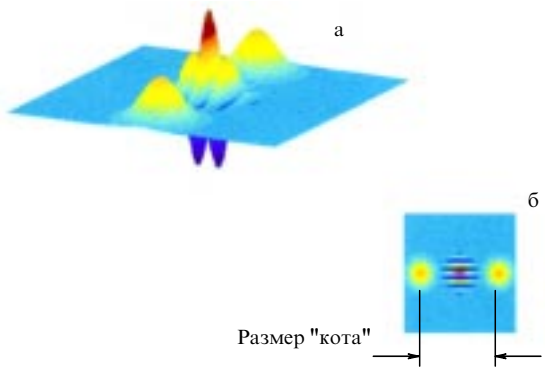


Рис. 17. (а) Функция Вигнера суперпозиции, образованной двумя когерентными состояниями, отличающимися по фазе на π. Каждый из двух пиков соответствует одному из когерентных состояний $|\alpha\rangle$ или $|-\alpha\rangle$. Расстояние между пиками определяет макроскопичность состояния (размер шрёдингеровского кота, см. на рис. (б), где приведено изображение проекции функции Вигнера). Отличительной особенностью функции Вигнера состояния $|\alpha\rangle+\exp(\mathrm{i}\theta)|-\alpha\rangle$ является интерференционная часть в центре фазовой плоскости. Отрицательные значения свидетельствуют о квантовом характере состояния.

графическое представление которой содержит информацию о всей волновой функции объекта: фотона, фонона или другой квантовой системы, моделируемой гармоническим осциллятором, поскольку эта функция для классических состояний равна плотности совместной вероятности "координата(x) – импульс(p)" ($\beta=x+\mathrm{i}p$). В частности, для состояния

$$|\psi_{+}\rangle=N\left(|\alpha\rangle+\exp\mathrm{i}\theta|-\alpha\rangle\right),$$
$$N^{-2}=2\left[1+\cos\theta\exp(-2|\alpha|^2)\right] \tag{23}$$

функция Вигнера $W(\beta)$ имеет два максимума, локализованных в точках $\beta=\pm\alpha$ и отмечающих преимущественную вероятность обнаружить при измерении систему в состоянии $|\alpha\rangle$ или $|-\alpha\rangle$. Кроме того, имеется интерференционная структура при $\beta=0$, которая при некоторых аргументах принимает отрицательные значения. Эта структура возникает вследствие квантовых интерференционных членов $|\alpha\rangle\langle-\alpha|\exp(-\mathrm{i}\theta)+|-\alpha\rangle\langle\alpha|\exp\mathrm{i}\theta$ в матрице плотности состояния (23), и именно ее наличие указывает на неклассический характер состояния.

[4] В известной игре в фанты в руке у партнера монета и Вам предлагается определить, имеет ли данная монета две стороны разные (орел и решка) или они одинаковые. Очевидно, сделав два взгляда на разные стороны монеты, вы дадите ответ. Но можно ли дать правильный ответ, взглянув только один раз? Моделируя эту ситуацию на спиновых состояниях ядер молекулы хлороформа, авторы работы [72] дали ответ за один "прогон" квантового процессора. При этом спиновые состояния ядер водорода использовались в качестве аналога индикатора, на какую сторону монеты сделан взгляд (спин вверх или вниз), а состояния спина ядра углерода — для индикации результата наблюдения.

Будучи подверженным релаксации, например, вследствие выхода фотонов из резонатора со скоростью γ, состояние гармонического осциллятора меняется своеобразно: интерференционная часть исчезает первой, и суперпозиционное состояние превращается в смесь, которая затем релаксирует к вакуумному состоянию (рис. 18). Причем скорость исчезновения интерференционных членов $t_{\text{decoh}}^{-1} = 2\gamma|\alpha|^2$ тем больше, чем больше "размер" состояния (22), определяемый амплитудой α. Эта особенность процесса релаксации, отмеченная впервые Цуреком [86], объясняет, почему суперпозиционные состояния, легко наблюдаемые в микромире, при переходе в макромир становятся труднодоступными, почему трудно наблюдать суперпозицию живого и неживого кота. Однако сам по себе этот факт еще не дает ключей к решению проблемы избавления от декогеренции. Для этого надо исследовать детали релаксационного процесса.

6.1. Релаксация как неунитарная эволюция состояния. Конструирование квантовых резервуаров

Любой тип релаксации предполагает, что квантовая система взаимодействует с резервуаром — объектом, содержащим большое число степеней свободы и обладающим плотным и широким энергетическим спектром. Это обеспечивает направленный перенос возмущений от системы к резервуару. Стандартная модель резервуара — совокупность большого числа гармонических осцилляторов с распределенными собственными частотами ω_i и операторами рождения и уничтожения b_i^+, b_i. В процессе взаимодействия первоначально независимые состояния системы и резервуара становятся перепутанными, при этом исходное суперпозиционное состояние системы теряет свою индивидуальность как член более общей системы и превращается в смесь. Особенности этого перехода зависят от вида взаимодействия "система – резервуар". Предположим, что квантовая система, выделенный осциллятор, взаимодействует с бассейном посредством гамильтониана

$$H_{\text{int}} = A(a, a^+)\Gamma^+ + A^+(a, a^+)\Gamma\,, \tag{24}$$

где $A(a, a^+)$ — функция, в общем случае нелинейная, операторов рождения и уничтожения выделенного осциллятора, $\Gamma = \hbar\sum_i g_i b_i$ — линейная по операторам бассейна функция. Гамильтониан (24), хотя и не универсальный, описывает множество физических ситуаций. Прежде всего для линейного взаимодействия $A(a, a^+) = a$, и затухание описывается уравнением

$$\dot\rho = \frac{\gamma}{2}(2a\rho a^+ - a^+a\rho - \rho a^+a) \tag{25}$$

для матрицы плотности осциллятора a, усредненной по начальному вакуумному состоянию резервуара. Константа $\gamma = \pi\rho(\omega)|g(\omega)|^2$ есть скорость затухания энергии, $\rho(\omega)$ — плотность состояний бассейна. Решение уравнения (25) дает значение матрицы плотности в каждый момент времени, предсказывая возможные результаты измерений над осциллятором a. Например, начальная суперпозиция $|\psi_+\rangle = N(|\alpha\rangle + \exp\mathrm{i}\theta|-\alpha\rangle)$ эволюционирует, согласно (25), как

$$\begin{aligned}\rho(t) = {}& \frac{1}{2}\left(|\alpha_t\rangle\langle\alpha_t| + |-\alpha_t\rangle\langle-\alpha_t|\right) + \\ & + \frac{1}{2}\exp\left\{-2|\alpha|^2\left[1-\exp(-\gamma t)\right]\right\}\times \\ & \times\left[\exp\mathrm{i}\theta|-\alpha_t\rangle\langle\alpha_t| + \exp(-\mathrm{i}\theta)|\alpha_t\rangle\langle-\alpha_t|\right],\end{aligned} \tag{26}$$

медленно уменьшая амплитуду $\alpha_t = \alpha\exp(-\gamma t/2)$ и быстро, со скоростью $t_{\text{decoh}}^{-1} = 2\gamma|\alpha|^2$, превращаясь из чистого состояния в смесь.

В общем случае, когда взаимодействие "осциллятор a – резервуар" является нелинейным, релаксация происходит согласно кинетическому уравнению

$$\dot\rho = \frac{\gamma}{2}\left([A, \rho A^+] + [A\rho, A^+]\right), \tag{27}$$

из которого, а также из гамильтониана (24) следует, что релаксация осциллятора a будет происходить своеобразно, в сильной степени завися от вида взаимодействия $A(a, a^+)$: если оператор связи $A(a, a^+)$ обладает собственными состояниями $|\Psi\rangle_A$, то именно эти состояния, не возмущаясь в результате взаимодействия с бассейном, образуют так называемый "направляющий базис" [86], определяющий специфику релаксационной эволюции. Следовательно, имеется возможность, используя различные виды оператора связи $A(a, a^+)$, создавать различные "направляющие базисы" и тем самым изменять процесс релаксации, и более того, получать различные стационарные состояния в результате релаксации. Некоторые известные примеры такого "конструирования квантовых резервуаров" собраны в табл. 3.

Заметим, что выбирая в качестве динамической системы не гармонический осциллятор, а N двухуровне-

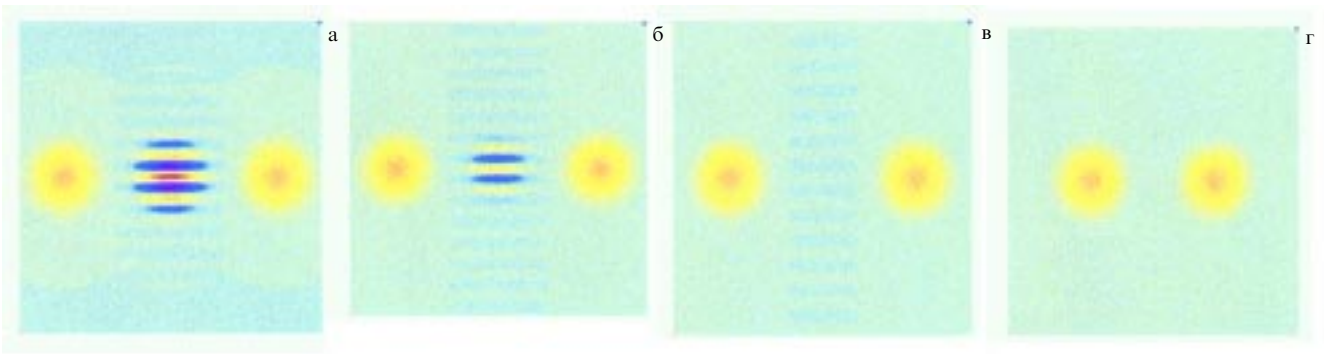


Рис. 18. Эволюция функции Вигнера затухающего квантового гармонического осциллятора, первоначально находившегося в состоянии $|\alpha\rangle + \exp(\mathrm{i}\theta)|-\alpha\rangle$, при $t = 0$ (а), $1/16\gamma$ (б), $1/4\gamma$ (в), $1/\gamma$ (г); $\alpha = 2$ (вид сверху). Явление декогеренции состоит в быстром исчезновении интерференционной части функции Вигнера в процессе релаксации.

Таблица 3. Различные формы связи система – резервуар для конструирования квантовых резервуаров

Форма связи	"Направляющий базис"	Стационарное состояние	Литература
$A = a + a^+ \sim x$	Собственные состояния координаты	Вакуум	[86]
$A = a^2$	Четные и нечетные когерентные состояния	Вакуум	[87]
$A = (a+\alpha)(a-\alpha)$	Четные и нечетные когерентные состояния	Четные и нечетные когерентные состояния	[88 – 90]
$A = a^+a$	Фоковские состояния	Вакуум	[90]
$A = a(a^+a - n)$	Фоковские состояния	Фоковские состояния	[90]
$A = \exp(\mathrm{i}\pi a^+a)a$	Суперпозиционные состояния Юрке – Столера	Вакуум	[91 – 93]

вых систем, моделирующих квантовый регистр, можно найти подпространство для состояний регистра, которое полностью расцеплено от состояний резервуара и, следовательно, не возмущаемо резервуаром. Для некоторых особых случаев взаимодействий подобное рассмотрение уже выполнено [95]. С другой стороны, имеющаяся жесткая связь между состояниями одного двухуровневого атома и состояниями бассейна, например, поля излучения, позволяет, изменяя состояния бассейна, изменять динамику атома. Так, выбор в качестве начального состояния бассейна одной моды (резонансной) в состоянии Юрке – Столера $|\alpha\rangle + \mathrm{i}|-\alpha\rangle$, а всех остальных — в вакуумном, приводит, в силу перепутанности совместных состояний, к эффекту *квантовой неустойчивости* — экспоненциальному росту переходного дипольного момента атома [96] вместо обычных осцилляций Раби.

6.2. Релаксация как квантовый стохастический процесс. Чистота условных состояний

Релаксацию осциллятора a можно рассматривать и как результат усреднения возможных квантовых случайных процессов, создаваемых актами передачи квантов от осциллятора a к осцилляторам резервуара. Каждый акт такой передачи, например, вылет фотона из резонатора, сопровождается мгновенным изменением состояния осциллятора a — редукцией. Отсутствие передачи квантов в промежутках между актами редукции, происходящими в случайные моменты времени, не означает отсутствия изменения состояния осциллятора a — с увеличением времени ожидания следующего отсчета увеличивается и вероятность того, что осциллятор a не возбужден, следовательно, в эти промежутки времени его амплитуда должна уменьшаться. Такая последовательность чередующихся актов редукции и промежутков неунитарной эволюции представляет собой основной объект исследований для теории непрерывных квантовых измерений или квантовых скачков [97 – 99]. Применительно к затуханию с линейной связью эта последовательность случайных событий описывается *условным* вектором состояния осциллятора a после передачи *точно* n квантов в резервуар в моменты времени $t_1, t_2, \ldots, t_n$ в интервале $[0, t)$:

$$|\psi_{\mathrm{cond}}(t)\rangle = \gamma^n S(t, t_n) a S(t_n, t_{n-1}) a \ldots a S(t_1, 0)|\psi(0)\rangle\,, \quad (28)$$

где $S(t_i, t_{i-1}) = \exp\{-\gamma a^+ a (t_i - t_{i-1})/2\}$ — неунитарный оператор эволюции между двумя последовательными актами редукции при t_{i-1} и t_i. Испускание квантов в моменты времени $\{t_i\}$ производит редукцию состояния, изымая один квант. Если $|\psi(0)\rangle = |\psi_+\rangle$, то это действие

$$a\big[|\alpha\rangle \pm \exp(\mathrm{i}\theta)|-\alpha\rangle\big] = \alpha\big[|\alpha\rangle \mp \exp(\mathrm{i}\theta)|-\alpha\rangle\big]\,, \quad (29)$$

приводит к изменению относительной фазы θ на π, но состояние остается чистым суперпозиционным. Неунитарная эволюция $S(t_i, t_{i-1})$ между отсчетами уменьшает экспоненциально амплитуду α. В результате условное состояние

$$|\psi_{\mathrm{cond}}(t)\rangle = N(\gamma\alpha)^n\big[|\alpha\exp(-\gamma t/2)\rangle + (-1)^n \exp(\mathrm{i}\theta)|-\alpha\exp(-\gamma t/2)\rangle\big] \quad (30)$$

остается во время всего периода эволюции *чистым*, сохраняя свою когерентность! Сохранение чистоты условного состояния в процессах релаксации не противоречит вышесказанному о декогеренции матрицы плотности: усреднение условной матрицы плотности $|\psi_{\mathrm{cond}}(t)\rangle\langle\psi_{\mathrm{cond}}(t)|$ по случайным реализациям отсчетов немедленно приводит к результату (26), что следует понимать как частичную потерю информации о состоянии системы. Очевидно также и то, что для стирания квантовых интерференционных членов достаточно первого отсчета, среднее время ожидания которого как раз совпадает со временем декогеренции $t_{\mathrm{deconh}} = 1/2\gamma|\alpha|^2$.

6.3. Коррекция ошибок с помощью обратной связи

Другой урок, который следует из рассмотрения релаксации как квантового стохастического процесса, состоит в том, что процесс декогеренции, хотя и является очень серьезным препятствием на пути использования преимуществ квантовой информации, но все же не непреодолимым. Для исправления ошибок и неопределенностей, которые вносит окружение при взаимодействии с квантовым объектом, не надо знать сложное состояние окружения. Достаточно контролировать времена передачи квантов от объекта к окружению и унитарным преобразованием возвращать состояние системы к прежнему после каждого из актов редукции [91 – 93].

Для суперпозиции когерентных состояний Юрке – Столера $|\alpha\rangle + \mathrm{i}|-\alpha\rangle$ этот протокол коррекции ошибок должен реализовываться путем поворота фазы амплитуды осциллятора a на 180° [91]. В этом случае последовательность событий, определяющих квантовый стохастический процесс, будет состоять из чередующихся неунитарной эволюции (отсутствие отсчетов), редукции и следующей за ней операции изменения фазы:

$$|\psi_{\mathrm{cond}}(t)\rangle = \gamma^n S(t, t_n)\exp(\mathrm{i}\pi a^+a)a S(t_n, t_{n-1})\times \times \exp(\mathrm{i}\pi a^+a)a \ldots \exp(\mathrm{i}\pi a^+a)a S(t_1, 0)|\psi_+\rangle\,. \quad (31)$$

Коррекция, осуществляемая посредством обратного воздействия на осциллятор a (рис. 19), приводит к тому, что не только условное, но и безусловное его состояние, получаемое при усреднении по случайным отсчетам,

остаются чистыми суперпозициями:

$$|\psi(t)\rangle = \frac{1}{\sqrt{2}}\left[\left|\alpha\exp(-\gamma t/2)\right\rangle + \mathrm{i}\left|-\alpha\exp(-\gamma t/2)\right\rangle\right]. \quad (32)$$

Единственное проявление релаксации в этом случае — экспоненциальное уменьшение амплитуды (энергетическая релаксация).

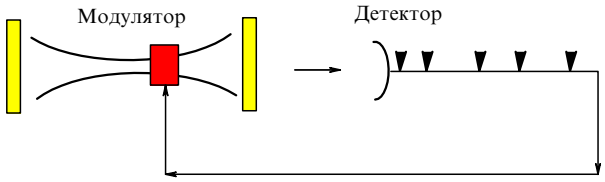


Рис. 19. Замедление процесса декогеренции с помощью коррекции ошибок на основе обратной связи. Первоначально возбужденное в состояние Юрке–Столера внутрирезонаторное поле непрерывно детектируется высокоэффективным детектором, сигнал от каждого отсчета которого передается по линии обратной связи на фазовый модулятор, изменяющий фазу поля на π. Повторяя эту последовательность далее, мы сохраняем суперпозиционное состояние внутри резонатора до тех пор, пока в резонаторе есть фотоны.

Отметим, что матрица плотности состояния (32) удовлетворяет уравнению типа (27)

$$\dot{\rho} = \frac{\gamma}{2}\left(\left[A_\pi, \rho A_\pi^+\right] + \left[A_\pi\rho, A_\pi^+\right]\right), \quad (33)$$

где нелинейные операторы связи $A_\pi = \exp(\mathrm{i}\pi a^+ a)a$, и $A_\pi^+ = a^+\exp(-\mathrm{i}\pi a^+ a)$ — частный случай обобщенных операторов рождения и уничтожения $A_\varphi = \exp(\mathrm{i}\varphi a^+ a)a$, $A_\varphi^+ = a^+\exp(-\mathrm{i}\varphi a^+ a)$, собственные состояния которых — обобщенные когерентные состояния, обладают необычными квантовыми свойствами [92].

Экспериментальная реализация предложенной схемы исправления декогеренции очевидна [93] (рис. 19). Для этого первоначально возбужденное в состояние Юрке–Столера внутрирезонаторное поле непрерывно детектируется высокоэффективным детектором, сигнал от каждого отсчета которого передается по линии обратной связи на фазовый модулятор, изменяющий фазу поля на π. Повторяя эту последовательность далее, мы сохраняем суперпозиционное состояние внутри резонатора до тех пор, пока в резонаторе есть фотоны.

Принцип замедления декогеренции на основе квантовой обратной связи является универсальным, и его использование обосновано там, где возможен непрерывный контроль за потерями (локальные узлы квантовых вычислений). В настоящее время, помимо работ [91–93], имеется ряд предложений в этом направлении [94]. В тех случаях, когда контроль затруднен, например, при передаче по квантовым каналам, следует использовать методы коррекции квантовых ошибок, опирающиеся на дублирование используемых для передачи q-битов [38, 39].

7. Заключение

Развитие области квантовой информации происходит необычайно быстро. "Научная гонка" за достижениями, приближающими реализацию преимуществ квантовых информационных технологий, вовлекла в себя, объединила и взаимно обогатила ранее стоявшие несколько отстраненно друг от друга такие области, как дискретная математика и квантовая механика, программирование и квантовая оптика. Кроме того, она придала практическую значимость исследованиям, ранее казавшимся весьма далекими от возможных практических приложений — исследованиям одиночных квантовых объектов: отдельных атомов и ионов в высокодобротных резонаторах и ловушках, отдельных молекул и примесных центров в полимерных и кристаллических матрицах. Все это вызывает развитие принципиально новых подходов, методов и материалов, уследить за которыми даже по новым публикациям в приоритетных научных изданиях вряд ли возможно. Весьма полезны при этом электронные публикации и препринты, доступные в сети Internet раньше их журнальных вариантов [100].

В заключение хотелось бы отметить, что несмотря на "громкие имена" и относительно большой промежуток времени, отделяющий нас от основополагающей работы Шрёдингера [1], настоящая история развития квантовой информации, затрагивающая практические интересы общества, только начинается. Неоценимый вклад в развитие этого направления внес Б.Б. Кадомцев, трагическое известие о смерти которого пришло, когда настоящая статья была на рассмотрении в редакции. Б.Б. Кадомцев считал, что информационные аспекты квантовой теории должны быть подвергнуты детальным исследованиям. Его последняя монография [101] посвящена проблемам квантовой теории информации.

Благодарности. Автор выражает благодарность Белорусскому республиканскому Фонду фундаментальных исследований за поддержку работ в области квантовой информации и его председателю А.С. Рубанову за предложение написать этот обзор; В.С. Буракову за любезное предложение выступить на семинаре Белорусского физического общества, выступление на котором частично нашло отражение в данной работе; П.А. Апанасевичу, Д.Б. Хорошко, В.Н. Шатохину, А.П. Низовцеву, Т.М. Маевской, Д.С. Могилевцеву, Т.Б. Карлович, В.А. Запорожченко за сотрудничество, а также H. Walther, P. Berman, M. Raymer, G. Bjork, C. von Borczyskowski за плодотворные обсуждения. С благодарностью отмечается частичная финансовая поддержка Национального научного фонда США (грант NSF-9414515 "Спектроскопия одиночных молекул"), Фонда Фольксваген (грант 1/72 171 "Двухуровневые системы в спектроскопии одиночных молекул"), INTAS (грант 96 167 "Генерация одиночных фотонов и синтез квантовых состояний"), Национального научного совета США (Twinning programm "Квантовая томография и другие реконструктивные методы измерений в квантовой оптике").

Список литературы

1. Schrödinger E *Naturwissenschaften* **23** 807, 823, 844 (1935) [Перевод на русск.: *Успехи химии* **5** 390 (1936); [перевод на англ.: *Proc. Am. Philos. Soc.* **124** 323 (1980)]
2. Einstein A, Podolsky B, Rosen N *Phys. Rev.* **45** 777 (1935)
3. Bohr N *Phys. Rev.* **48** 696 (1935)
4. Bell J S *Physics* **1** 195 (1964)
5. Clauser J F, Shimony A *Rep. Prog. Phys.* **41** 1881 (1978)
6. Greenberger D M, Horne M A Zeilinger A *Phys. Today* **46** (8) 22 (1993)
7. Aspect A, Grangier P, Roger G *Phys. Rev. Lett.* **47** 460 (1981)
8. Apanasevich P A, Kilin S Ya *Phys. Lett. A* **62** 83 (1977); *J. Phys. B* **12** L83 (1979)

9. Aspect A et al. *Phys. Rev. Lett.* **45** 617 (1980)
10. Hagley E et al. *Phys. Rev. Lett.* **79** 1 (1997)
11. Зельдович Б Я, Клышко Д Н *Письма в ЖЭТФ* **9** 69 (1969)
12. Burnham D C, Weinberg D L *Phys. Rev. Lett.* **25** 84 (1970)
13. Kwiat P G et al. *Phys. Rev. Lett.* **75** 4337 (1995)
14. Фейнман Р, Лейтон Р, Сэндс М *Фейнмановские лекции по физике* Т. 8, Гл. 2 (М.: Мир, 1978) с. 30
15. Wootters W K, Zurek W H *Nature* (London) **299** 802 (1982)
16. Bouwmeester D, Pan J-W, Mattle K, Eibl M, Weinfurtner H, Zeilinger A *Nature* (London) **390** 575 (1997)
17. Bennett C H et al. *Phys. Rev. Lett.* **70** 1895 (1993)
18. Boschi D et al. *Phys. Rev. Lett.* **80** 1121 (1998)
19. Клышко Д Н *УФН* **168** 975 (1998)
20. Bennett C H, Brassard G, Ekert A K *Scientific Am.* **267** 26 (1992)
21. Shannon C E *Bell Syst. Tech. J.* **28** 657 (1949)
22. Bennett C H *Phys. Rev. Lett.* **68** 3121 (1992)
23. Hughes R J et al. *Contemp. Phys.* **38** 149 (1995)
24. Muller A, Zbinden H, Gisin N *Europhys. Lett.* **33** 335 (1996); **33** 586 (1997)
25. Rivest R, Shamir A, Adleman L "On digital signatures and public-key cryptosystems" MIT Laboratory for Computer Science Technical Report MIT/LCS/TR-212 (1979)
26. Bennett C H *IBM J. Res. Dev.* **17** 525 (1973)
27. Toffoli T, in *Automata, Languages and Programming* (Eds J W de Bakker, J van Leeuwen) (New York: Springer, 1980) p. 632
28. Feynman R P *Int. J. Theor. Phys.* **21** 467 (1982)
29. Feynman R P *Found. Phys.* **16** 507 (1986) [Впервые опубл. в *Opt. News* **11** (February 1985); перевод на русск. *УФН* **149** 671 (1986)]
30. Deutsch D *Proc. R. Soc. London Ser. A* **425** 73 (1989)
31. Schumacher B *Phys. Rev. A* **51** 2738 (1995)
32. DiVincenzo D *Phys. Rev. A* **51** 1015 (1995)
33. Barenco A et al. *Phys. Rev. Lett.* **74** 4073 (1995)
34. Sleator T, Weifurtner H *Phys. Rev. Lett.* **74** 4087 (1995)
35. P W Shor, in *Proc. of the 35th Ann. Symp. of the Foundations of Computer Sci.* (Ed S Goldwasser) (Los Alamitos, CA: IEEE Computer Society, 1994) p. 124
36. Grover L K *Phys. Rev. Lett.* **79** 4709 (1997)
37. Оре О *Теория графов* (М.: Наука, 1968)
38. Shor P W *Phys. Rev. A* **52** R2493 (1995)
39. Ekert A, Macchiavello C *Phys. Rev. Lett.* **77** 2585 (1995)
40. Kimble H J, in *Cavity Quantum Electrodynamics* (Ed P Berman) (New York: Academic Press, 1994) p. 203
41. Raithel G et al., in *Cavity Quantum Electrodynamics* (Ed P Berman) (New York: Academic Press, 1994) p. 57
42. Davidovich L et al. *Phys. Rev. A* **53** 1295 (1996)
43. Braginsky V B, Gorodetsky M L, Ilchenko V S *Phys. Lett. A* **137** 393 (1989)
44. Collet L et al. *Europhys. Lett.* **23** 327 (1993)
45. John S *Phys. Rev. Lett.* **58** 2486 (1987)
46. Yablonovich E *Phys. Rev. Lett.* **58** 2059 (1987)
47. Kilin S Ya, Mogilevtsev D S *Laser Phys.* **2** 153 (1992)
48. Килин С Я, Могилевцев Д С *Опт. Спектроск.* **74** 974 (1993)
49. Bogomolov V N et al. *Phys. Rev. E* **55** 7619 (1997)
50. Romanov S G, Johnson N P, De La Rue D M *Appl. Phys. Lett.* **70** 2091 (1997)
51. Fischer E *Z. Phys.* **156** 1 (1959)
52. Scharma C A et al. *Opt. Commum.* **101** 32 (1993)
53. Hoffges J T et al. *J. Mod. Opt.* **44** 1999 (1997)
54. Birkl G, Kassner S, Walther H *Nature* (London) **357** 310 (1992)
55. Cirac J, Zoller P *Phys. Rev. Lett.* **74** 4091 (1995)
56. Monroe C et al. *Phys. Rev. Lett.***75** 4714 (1995)
57. Миногин В Г, Летохов В С *Давление лазерного излучения на атомы* (М.: Наука, 1986)
58. D J Wineland, C E Wieman, S J Smith (Eds) *Atomic Physics* 14 (New York: AIP, 1994)
59. Anderson M A et al. *Science* **269** 198 (1995)
60. T Basché, W E Moerner, M Orrit, U P Wild (Eds) *Single-Molecule Optical Detection, Imaging and Spectroscopy* (Weinheim: VCH, 1996)
61. Dickson R M et al. *Science* **274** 966 (1996)
62. Gruber A et al. *Science* **276** 2012 (1997)
63. Wennmalm S, Edman L, Rigler R *Proc. Natl. Acad. Sci. USA* **94** 10641 (1997)
64. Dickson R M et al. *Nature* (London) **388** 355 (1996)
65. Tietz C et al. *J. Chem Phys.* (1999) (in print)
66. Pirotta M et al. *Spectroscopy Europe* **9/4** 16 (1997)
67. Kilin S Ya et al. *Phys. Rev. B* **56** 24 (1997)
68. Kilin S Ya et al. *Phys. Rev. A* **57** 1400 (1998)
69. Ekert A, Jozsa R *Rev. Mod. Phys.* **68** 733 (1996)
70. Gershenfeld N, Chuang I *Science* **275** 350 (1997)
71. Laflamme R et al. Квантовые вычисления и криптография в Лос-Аламосе — http://qso.lanl.gov/qc/ (March 1998)
72. Chuang I L et al. *Nature* (London) **393** 143 (1998)
73. Turchette Q A et al. *Phys. Rev. Lett.* **75** 4710 (1995)
74. Kilin S Ya, Krinitskaya T B *J. Opt. Soc. Am. B* **8** 2289 (1991); *Phys. Rev. A* **48** 3870 (1993)
75. Kilin S Ya, Berman P, Maevskaya T M *Phys. Rev. Lett.* **76** 3297 (1996)
76. Leonardt U et al. *Opt. Commun.* **127** 144 (1996)
77. Braginskii V B, Khalili F Ya *Quantum Measurements* (New York: Cambridge Univ. Press, 1992)
78. Rarity J G, Tapster P R, in *Quantum Optics of Confined Systems* (NATO ASI Series. Ser. E, No 314, Eds M Ducloy, D Bloch) (Dordrecht: Kluwer Acad. Publ., 1996) p. 47
79. Kilin S Ya, Horoshko D B *Phys. Rev. Lett.* **74** 5206 (1995)
80. Голубев Ю М, Соколов И В *ЖЭТФ* **87** 408 (1984)
81. Yamamoto Y, Imoto N, Machida S *Phys. Rev. A* **33** 3243 (1986)
82. Фофанов Я А *Квантовая электрон.* **12** 2593 (1989)
83. Хорошко Д Б, Килин С Я *ЖЭТФ* **106** 1278 (1994); *Опт. Спектроск.* **82** 913 (1997)
84. Yamamoto Y et al. *Prog. Opt.* **28** 88 (1990)
85. Jann A, Ben-Aryeh Y *J. Opt. Soc. Am.* **14** 11 (1997)
86. Zurek W H *Phys. Today* **44** (10) 36 (1991); *Phys. Rev. D* **24** 1516 (1981); *Phys. Rev. D* **26** 1862 (1982)
87. Gerry C, Hach E E *Phys. Lett. A* **174** 185 (1993)
88. Garraway B R, Knight V *Phys. Rev. A* **49** 1266 (1994); **50** 2548 (1994)
89. Filho M R L,Vogel W *Phys. Rev. Lett.* **76** 608 (1996)
90. Poyatos J F, Cirac J I, Zoller P *Phys. Rev. Lett.* **77** 4728 (1996)
91. Horoshko D B Kilin S Ya *Phys. Rev. Lett.* **78** 840 (1997)
92. Kilin S Ya, Horoshko D B, Shatokhin V N *Acta Phys. Pol. A* **93** 97 (1998)
93. Kilin S Ya, Horoshko D B *J. Mod. Opt.* **44** 2043 (1997); *Opt. Express* **2** 347 (1998)
94. Vitali D, Tombesi P, Milburn G J *Phys. Rev. Lett.* **79** 2442 (1997)
95. Zanardi P, Rasetti M *Phys. Rev. Lett.* **79** 3306 (1997)
96. Kilin S Ya, Shatokhin V N *Phys. Rev. Lett.* **76** 1051 (1996); *ЖЭТФ* **111** 1174 (1997); *Опт. Спектроск.* **82** 972 (1997)
97. Davies E B *Quantum Theory of Open Systems* (New York: Academic Press, 1976)
98. Килин С Я *Квантовая оптика. Поля и их детектирование* (Мн.: Навука і тэхніка, 1990)
99. Холево А С *Изв. вузов. Математика* (8) 3 (1982)
100. Квантовые вычисления и криптография в Лос-Аламосе — http://qso.lanl.gov/qc/;
квантовые вычисления и криптография в Оксфорде — http://eve.physics.ox.ac.uk/QChome.html;
Лаборатория теоретических и квантовых вычислений, Университет Монреаля — http://www.iro.umontreal.ca/labs/theorique/index_en.html;
квантовые вычисления в IBM — http://www.research.ibm.com/xw-quantuminfo;
введение в квантовые вычисления http://chem-phys.weizmann.ac.il//~schmuel/comp/comp.html;
квантовые вычисления в Австралийском национальном университете — http://aerodec.anu.edu,au/~qc/index.html;
квантовая информация — http://vesta.physics.ucla.edu/~smolin;
архив по квантовым вычислениям — http:/feynman.stanford.edu/qcomp/;
препринты по квантовой информации в архиве Лос-Аламоса — http://xxx.lanl.gov/archive/quant-ph/;
препринты по квантовой информации в архиве ICTP Триесте: — http:/www.ictp.trieste.it/indexes/preprints.html;
квантовая оптика — http:/master.bas-net.by/
101. Кадомцев Б Б *Динамика и информация* (М.: Ред. журн. "Успехи физических наук", 1997)

Quantum information

S.Ya. Kilin
B I Stepanov Institute of Physics,
National Academy of Sciences of Belarus, prosp. Frantsiska Scariny 70,
220602 Minsk, Belarus
Tel. (375-17) 284-26 13
Fax (375-17) 284-08 79
E-mail: kilin@ifanbel.bas-net.by

A new research direction known as quantum information is a multidisciplinary subject which involves quantum mechanics, optics, information theory, programming, discrete mathematics, laser physics and spectroscopy, and depends heavily on contributions from such areas as quantum computing, quantum teleportation and quantum cryptography, decoherence studies, and single-molecule and impurity spectroscopy. Some new results achieved in this rapidly growing field are discussed.

PACS number: **03.67.–a**

Bibliography — 101 references

Received 18 June 1998

Май 1999 г. ***Том 169, № 5***

УСПЕХИ ФИЗИЧЕСКИХ НАУК

НОВЫЕ КНИГИ ПО ФИЗИКЕ И СМЕЖНЫМ НАУКАМ

Капица П.Л. ***Научные труды. Наука и современное общество*** (Отв. ред. А.С. Боровик-Романов, Ред.-сост. П.Е. Рубинин) (М.: Наука, 1998) 539 с. Проект РФФИ 97-06-87016.

В книгу Петра Леонидовича Капицы включены статьи, речи, выступления 1913 – 1982 гг., посвященные роли и значению науки и ученого в современном мире, глобальным научным проблемам, вопросам организации науки, творческому воспитанию молодых ученых, истории науки. Значительная часть материалов из архива ученого публикуется впервые. В виде приложения приводится наиболее полное собрание физических задач П.Л. Капицы. Для широкого круга читателей, интересующихся путями развития науки.

Горшков А.С. ***Избранные труды*** (Составитель К.И. Воляк) (М., 1998) 360 с.

Сборник посвящен 70-летию со дня рождения ученого-радиофизика Анатолия Савельевича Горшкова. В собрание трудов вошли основные работы, опубликованные в отечественной и зарубежной научной периодике. Сборник завершается очерками биографии и научной деятельности А.С. Горшкова. Книга представляет интерес для специалистов-радиофизиков и научных работников смежных специальностей, преподавателей вузов, а также студентов старших курсов и аспирантов.

Гладков С.О. ***Физика пористых структур*** (М.: Наука, 1997) 175 с. Библ.: 146 назв.

В монографии дается систематическое изложение основ теоретического и экспериментального исследования важнейших физических характеристик пористых структур. Описано нестандартное поведение отдельных физических параметров, к которым относится, например, поле электрического пробоя пористого вещества и тангенс диэлектрических потерь. Подробно изложен метод вычисления коэффициента теплопроводности пористых диэлектриков при помощи принципа неравновесности. Предлагаемый подход может быть применен к исследованию свойств таких, казалось бы, "безнадежных" веществ, как целлюлоза, композиты и композиционные материалы.

Вараксин А.Н. ***Взаимодействие и миграция точечных структурных дефектов в диэлектриках на основе щелочно-галоидных кристаллов (компьютерное моделирование)*** (Екатеринбург: Изд. УрО РАН, 1997) 128 с. Библ.: 176 назв.

Рассмотрены процессы образования, взаимодействия и миграции точечных структурных дефектов в твердых телах на основе щелочно-галоидных кристаллов (ЩГК) (номинально чистые, слаболегированные и смешанные ЩГК) с помощью математических компьютерных моделей, использующие следующие методы: молекулярной статики, молекулярной динамики, Монте-Карло, сокращенные методы моделирования. Проведены расчеты энергий образования, взаимодействия и миграции структурных дефектов, электропроводности слаболегированных и смешанных ЩГК, проанализированы механизмы элементарных диффузионных скачков. Наряду с компьютерными моделями использованы аналитические методы (феноменологические и микроскопические). Прослежены закономерности формирования макроскопических характеристик дефектных кристаллов исходя из характеристик элементарного диффузионного скачка. Для специалистов в области физики дефектных кристаллов и вычислительной физики твердого тела, студентов и аспирантов физических специальностей.

Симметрии и законы сохранения уравнений математической физики (Под ред. А.М. Виноградова, И.С. Красильщика) (М.: Факториал, 1997) 464 с. Библ.: 157 назв. Проект РФФИ 95-01-02825.