Квантовая информатика и квантовый компьютер

Учебное пособие

Д.А.Кронберг, Ю.И.Ожигов, А.Ю.Чернявский
МГУ имени М.В.Ломоносова, факультет ВМК

Пособие предназначено для самостоятельной работы студентов, слушающих курс «Квантовые вычисления» или любой другой курс по основам квантовой информатики. Проработка данного пособия означает освоение основами квантовой информатики, что дает возможность дальнейшей специализации в этом направлении, включая поступление в аспирантуру. Работа с данным пособием заключается в самостоятельном решении предлагаемых в конце задач с использованием сведений, изложенных в регулярном курсе. В случае необходимости в качестве источника теоретических сведений можно вместо курса можно также использовать пособие [65]. Все теоретические сведения, формально необходимые для решения задач, кратко излагаются в данном пособии. При решении задач можно, в случае необходимости, пользоваться указанной литературой как вспомогательным средством, но только если задача упорно не поддается решению, или для самоконтроля - после получения решения. Самая важная часть работы состоит именно в попытках найти самостоятельное решение всех предлагаемых задач. Решать их надо последовательно, используя помещенные подсказки. После решения всего списка задач можно сдавать экзамен по дисциплине квантовая информатика на кафедре и начинать научные исследования в данной области.

Оглавление

Глава 1

Квантовые процессы

В данном разделе описывается формализм квантовой физики с кубитовой точки зрения, так что студент, знакомый с основами квантовой теории, сможет переписать любую ее часть на этом языке. Обычно в литературе по физике используется традиционные обозначения из теории функций, например, волновую функцию записывают как $\Psi(x)$, что вызывает коллизию со значением волновой функции в конкретной точке x, и потому для него используется интегральное представление $\int \Psi(y)\delta_x(y)\ dy$. Эти традиционные обозначения удобны для ручных вычислений, при которых разрешение таких коллизий не создает проблемы для человека. Однако для компьютерного моделирования необходима большая степень формализации основных понятий. Более того, формализм должен быть приспособлен к тому, что мы будем работать только с конечными числами даже если в используемых нами формулах можно подставлять бесконечные величины. Особенно это касается квантовой электродинамики, для которой здесь предлагается формальная система обозначений кубитового типа.

1.1 Основные положения одночастичной квантовой механики

Главный постулат квантовой механики состоит в том, что вся динамика любой системы определяется ее волновой функцией, которая является комплексной функцией от координат все частиц, составляющих эту систему:

$$\Psi(t, r_1, r_2, \ldots, r_n).$$

Здесь r_j есть координаты частицы j (имеются в виду не только пространственные координаты частиц, но и их спиновые координаты). Эта волновая функция должна рассматриваться как вектор в гильбертовом пространстве состояний n частичной системы. Значения этой функции называются амплитудами, соответствующими пребыванию частицы в данный момент времени t в таком состоянии, при котором для каждого $j = 1, 2, \ldots, n$ частица j имеет координаты r_j. Такая трактовка состояния в виде вектора сразу ведет к нетривиальному следствию: любая линейная комбинация состояний снова является некоторым возможным физическим состоянием данной системы. Таким образом, множество состояний обладает свойством линейности, и это означает, что любое уравнение, которому подчиняется вектор Ψ, должно быть линейным. Этот принцип называется принципом суперпозиции, и из него вытекает существование особого процесса, называемого интерференцией амплитуд, который не имеет прямого аналога в классической физике (не считая волновую физику, где интерференция проявляется как коллективный эффект, к чему мы вернемся).

Интерференцию амплитуд проще всего

продемонстрировать, применяя матрицы. Представим себе, что мы выбрали базис в гильбертовом пространстве состояний, и представляем всякий вектор Ψ в виде некоего столбца координат этого вектора в данном базисе. Тогда из принципа суперпозиции вытекает, что состояние в следующий момент времени $t+\delta t$ можно найти, применив к состоянию в момент времени t некий линейный оператор U, называемый оператором унитарной эволюции (дальше мы увидим, что он должен быть не только линейным, но и унитарным). Этот факт можно выразить на языке матричного умножения так:

$$\begin{pmatrix} u_{1,1} & u_{1,2} & \dots & u_{1,n} \\ u_{2,1} & u_{2,2} & \dots & u_{2,n} \\ \dots & \dots & \dots & \dots \\ u_{n,1} & u_{n,2} & \dots & u_{n,n} \end{pmatrix} \begin{pmatrix} \psi_1(t) \\ \psi_2(t) \\ \dots \\ \psi_n(t) \end{pmatrix} = \begin{pmatrix} \psi_1(t+\delta t) \\ \psi_2(t+\delta t) \\ \dots \\ \psi_n(t+\delta t) \end{pmatrix} \tag{1.1}$$

То есть любая амлитуда $\psi_j(t+\delta t)$ может быть найдена по формуле

$$\psi_j(t+\delta t) = \sum_{i=1}^{n} \psi_i(t) u_{j,i}. \tag{1.2}$$

Формула (1.2) означает, что для нахождения амплитуды в некоторой точке в следующий момент времени надо просуммировать все амплитуды во всех точках в предыдущий момент, предварительно умножив их на соответствующие амплитуды перехода из этих точек в исходную. Значит, движение квантовой частицы можно представлять себе как движение некоей среды, где амплитуда в любой точке складывается из вкладов, которые вносят в эту точку движения этой частицы из всех других точек. При этом каждый вклад берется с комплексным весом, соответствующим описанному переходу из точки в точку. Это представление квантовой частицы в виде среды порождает аналогию квантовой физики с гидродинамикой.

А теперь рассмотрим два последовательных перехода, которые осуществляются с помощью того же оператора эволюции U: от момента t до момента $t + 2\delta t$. Тогда у нас получится: $\Psi(t + 2\delta t) = U^2\Psi(t)$. Выписав подробнее, мы получим $\psi_j(t + 2\delta t) = \sum_{i,k} \psi_i(t)u_{i,k}u_{k,j}$. Это означает, что квантовая частица может двигаться, вообще говоря, вдоль произвольной траектории, а не только по прямой, и ее амплитуда в любой точке есть результат суммирования амплитуд по всем путям, ведущим из каждой точки в данную. При этом вклад в сумму каждого пути получается умножением элементов матрицы эволюции U, соответствующих всем последовательным частям этого пути (мы представляем путь в виде ломаной и части - это ее звенья). Таким образом, амплитуда считается как сумма по всем путям, а вдоль каждого пути это - произведение амплитуд переходов по всем его последовательным частям.

Это правило справедливо везде, в том числе и в квантовой электродинамике где процессы описываются диаграммами. Оно в точности соответствует формуле для полной вероятности сложного события в теории вероятностей, с той лишь разницей, что в теории вероятности величины вещественные и неотрицательные, а у нас здесь - комплексные. Такая аналогия наводит на мысль о возможности статистической интерпретации квантовой теории, а также на возможность отказа от комплексных чисел при ее описании, - мы также вернемся к этим идеям позже.

Классическим величинам в квантовой теории соответствуют операторы. Величине координаты x соответствует оператор умножения на эту координату: $x : \ f(x) \longrightarrow xf(x)$, вектору $\bar{r} = (x, y, z)$ - оператор

$\bar{r} \ : \quad f(x, y, z) \ \longrightarrow \ (xf(x, y, z), yf(x, y, z), zf(x, y, z))$, импульсу p_x вдоль координатной оси x - оператор

импульса $p_x = \frac{h}{i}\frac{\partial}{\partial x}$, полному импульсу $\bar{p}$ - оператор $\bar{p} = \frac{h}{i}(\frac{\partial}{\partial x}, \frac{\partial}{\partial y}, \frac{\partial}{\partial z})$, энергии - оператор энергии $\frac{p^2}{2m} + V(x)$, где V - потенциальная энергия частицы. Оператор энергии называется гамильтонианом. При этом мы принимаем обычные правила перехода к векторым величинам, например оператор квадрата модуля координаты действует как $|r|^2 : \ f(x,y,z) \longrightarrow (x^2+y^2+z^2)f(x,y,z)$, оператор квадрата импульса - как $p^2 : \ f \longrightarrow -h^2\Delta f$ (то есть квадрат трактуется нами как скалярный квадрат), моменту импульса $\bar{r} \times \bar{p}$ - оператор момента, координаты которого получаются по правилу взятия векторного произведения из координат его сомножителей - операторов, и т.д.

Преобразование Фурье от волновой функции называется импульсным представлением волновой функции:

$$\Phi(p) = \int\limits_R e^{-\frac{ipx}{h}}\Psi(x)dx, \tag{1.3}$$

где обратный оператор выглядит так:

$$\Phi(x) = \frac{1}{2\pi h}\int\limits_R e^{\frac{ipx}{h}}\Phi(p)dp.$$

Полный переход к импульсному представлению и обратно в трехмерном пространстве имеет вид

$$\begin{aligned}\Phi(p) &= \int\limits_{R^3} e^{-\frac{ip\cdot R}{h}}\Psi(R)d^3R,\\ \Psi(R) &= \frac{1}{(2\pi h)^3}\int\limits_{R^3} e^{\frac{ip\cdot R}{h}}\Phi(p)d^3p,\end{aligned}$$

При этом если волновая функция зависит от 3 переменных, можно переходить к ее импульсному представлению по каждой из координат независимоо от других, например, можно рассмотреть функцию

вида $\Phi(x, p_y, z)$, или $\Phi(p_x, y, p_z)$, и т.д. Подчеркнем, что волновая функция не меняется при переходе к ее импульсному представлению - она представляет собой тот же самый вектор в гильбертовом пространстве состояний. Импульсное представление есть просто запись этого вектора в другом базисе, в котором базисные векторы - это не дельта функции, как при координатном представлении, а функции вида $exp(ipR)$. Мы могли бы выбрать какой-либо иной базис, например, соответствующий собственным векторам эрмитова оператора суммы $R + p$ импульс плюс координата, и завести соответствующее представление волновых функций, если это необходимо. Таким образом, все манипуляции, связанные с переходом к импульсному представлению, есть простая операция изменения базиса. Использование таких переходов есть часть стандартного формализма, и из этого следует важный для дальнейшего вывод: трудности с записью тех или иных взаимодействий в разных базисах свидетельствуют о серьезных проблемах.

Важнейшим правилом квантовой механики является правило Борна, которое гласит, что квадрат модуля волновой функции есть плотность вероятности обнаружения частицы в точке x:

$$p(x) = |\Psi(x)|^2 \tag{1.4}$$

Это правило инвариантно относительно базиса пространства состояний в том смысле, что плотность вероятности обнаружить импульс частицы равным p есть квадрат модуля импульсного представления волновой функции.

Правило Борна является сутью квантовой теории. Оно утверждает, что с ее помощью мы можем предсказать только вероятности наступления того или иного события но не сами эти события, как в классической физике. Использование математического понятия

вероятности автоматически предполагает существование так называемого пространства элементарных исходов, каждый из которых определяет уже не вероятность, а точное наступление события. Идеология копенгагенской квантовой теории предполагает, что нам принципиально не доступно пространство элементарных исходов. Этот запрет на доступ к элементарным исходам обычно формулируют как отсутствие скрытых параметров. Этот идеологический постулат[1] имеет смысл только в рамках классического математического аппарата, лежащего в основе квантовой теории. В дальнейшем мы рассмотрим конструктивную трактовку вероятности в квантовой теории, при которой элементарные исходы принадлежат административной части модели. В настоящее время появились эксперименты, связанные с квантовой нелокальностью, точное рассмотрение которых требует явных манипуляций с элементарными исходами.

Динамика волновой функции в стандартном формализме зависит от степени изолированности рассматриваемой системы, причем не существует точного определения изолированности. В случае изолированной системы динамика описывается уравнением Шредингера, в случае контакта с окружением - измерениями волновой функции. Измерение в данном базисе пространства волновых функций есть случайная величина, принимающая значения из векторов этого базиса с плотностью вероятности, задаваемой правилом Борна. Окружение всегда считается классической системой, подчиняющейся законам классической физики, и измерение системы дает вероятностное распределение ее состояний, подчиняющееся правилу Борна. Уравнение

[1]Другим постулатом того же статуса является представление о тождественности элементарных частиц одного типа.

Шредингера имеет вид

$$ih\frac{\partial\Psi}{\partial t} = H\Psi \tag{1.5}$$

где H есть оператор энергии частицы (или системы частиц). В простейшем случае частицы в потенциальном поле оператор энергии выписан выше. В более сложных случаях (несколько частиц, наличие векторного потенциала электромагнитного поля) оператор энергии получается из выражения для классической энергии с помощью замены всех физических величин на соответствующие им квантовые операторы. В частности, из уравнения Шредингера вытекает, что в случае постоянства потенциальной энергии во времени, общее решение уравнения Шредингера дается выражением

$$\Psi(x,t) = exp\left(-\frac{i}{h}Ht\right)\Psi(x,0) \tag{1.6}$$

Экспонента от оператора определяется как соответствующий ряд, составленый из операторов. Это же выражение можно использовать и для непостоянных гамильтонианов, только экспоненту надо тогда трактовать как так называемую хронологическую экспоненту.

По существу, мы описали весь стандартный формализм квантовой теории. Из этих основных положений вытекают некоторые другие (например, касающиеся измерений и возможностей выбора базисов), которые мы рассмотрим в кубитовом формализме. Все выводы копенгагенской квантовой теории получаются из этих основных положений с помощью разного рода эвристик и аналогий с классической физикой; математический аппарат стандартной квантовой теории исчерпывается изложенным в этом параграфе.

1.1.1 Кубитовый формализм

А сейчас займемся важным моментом перехода от волновой функции к конечному вектору. Эта процедура называется переходом к кубитовому представлению волновой функции. Собственно кубиты в данном случае играют декоративную роль, а сейчас важна процедура дискретизации волновой функции. Дискретизация волновых функций имеет глубокий смысл, так как она связана с наличием возможного зерна в конфигурационном пространстве. Если мы предположим, что конфигурационное пространство не является делимым до бесконечности, а в нем существует наименьшая ненулевая длина $d > 0$, то у нас получится, что вместо непрерывной волновой функции надо рассматривать ее дискретное приближение, которое на самом деле будет уже не приближением, а точным выражением, то есть приближением надо будет считать как раз непрерывный вариант волновой функции. Существование такой дискретизации пространства косвенно вытекает из расходимости рядов в квантовой электродинамике (см. ниже), а также из свойств волновых функций даже одной частицы при уменьшении зерна пространственного разрешения (это мы рассмотрим в параграфе, посвященном фейнмановским интегралам по траекториям). Но главное, для чего на самом деле нужно дискретное представление - это конструктивизация квантовой теории. Необходимость рассматривать и работать именно с приближениями координат частиц, а не с их вещественными "точными" значениями, ведет нас к кубитовому формализму.

Зерно пространственного-временного разрешения $d = (d_x, d_t)$ может и не быть абсолютной величиной, а зависеть от рассматриваемого процесса. Оно фактически

определяет степень несовершенства методов классической математики, которыми мы поневоле будем пользоваться, даже при построении алгоритмов. Это зерно есть граница применимости одного такого аналитического метода, на одном шаге конструктивного приближения реального процесса (см. секцию "Конструктивный математический анализ").

Пусть у нас имеется одна частица, координаты которой принимают значения из некоторого конфигурационного пространства R (для одномерной частицы это вещественные числа, но в данном случае структура R нам не очень важна). Разобъем R на конечное число сегментов $D_1, D_2, \ldots, D_m$ и рассмотрим приближение функции Ψ ступенчатой функцией $|\Psi\rangle$, которая принимает на сегменте D_j некоторое значение $\lambda_j \in C$. Пусть $|j\rangle$ обозначает характеристическую функцию сегмента D_j. Тогда мы можем записать формальное равенство

$$|\Psi\rangle = \sum_{j=1}^{m} \lambda_j |j\rangle \tag{1.7}$$

Рассмотрим линейное пространство, порожденное функциями $|j\rangle$. Если ввести скалярное произведение функций по стандартному правилу $(g, f) = \int \bar{f}(x) g(x) dx$, у нас получится, что $|j\rangle$ образуют ортогональный базис этого пространства. Если мы нормируем их (это можно сделать, фиксировав λ_j и подбирая нужные D_j), то этот базис будет ортонормированным. Тогда равенство (1.7) будет являться разложением вектора $|\Psi\rangle$ по ортонормированному базису, состоящему из векторов $|j\rangle$. Представление волновой функции в виде (1.7) является корректным, в отличие от двусмысленного выражения $\Psi(x)$, поскольку в последнем выражении переменная x является свободной, и потому неясно, что выражает запись $\Psi(x)$ - функцию Ψ или ее значение в конкретной

точке x. Подобные тонкости не важны в классической математике, так как при аналитических вычислениях свободную переменную всегда можно связать логическим квантором, но в конструктивной математике они важны. При построении алгоритма мы должны четко различать саму функцию, включающую все свои значения, как в (1.7) и ее конкретное значение в фиксированной точке.

Теперь мы можем установить соответствие квантового формализма и линейной алгебры. Будем через $|a\rangle$ понимать запись вектора a в конечномерном гильбертовом пространстве состояний в виде столбца его координат в выбранном заранее базисе. Тогда действие линейного оператора A на данный вектор выразится как результат матричного умножения $A|a\rangle$, где под A понимается матрица A в данном базисе. Договоримся также считать, что $\langle a|$ есть вектор - строка, полученная из $|a\rangle$ транспонированем и комплексным сопряжением элементов. Эта операция - транспонирование и комплексное сопряжение - называется просто сопряжением, когда речь идет о матрицах. Будем также сливать две рядом стоящие вертикальные черты в обозначениях. Тогда скалярное произведение векторов a и b запишется как $\langle a|b\rangle$. Запись $\langle a|A|b\rangle$ можно толковать вдояко: либо как $\langle a|(A|b\rangle)$, либо как $(\langle a|A^*)|b\rangle$. Но если матрица A самосопряженная, то есть $A = A^*$, двойственность исчезает, и мы можем использовать выписанное выражение без скобок. Самосопряженные матрицы еще называют эрмитовыми. Матрицы вида $\exp(iH)$, где H - эрмитова, называются унитарными. Приведением к диагональному виду легко доказывается, что матрица U унитарна тогда и только тогда, когда $U^{-1} = U^*$, или, что то же самое, когда матрица U сохраняет все расстояния в гильбертовом пространстве.

Можно определить измерение состояния $|\Psi\rangle$ в

ортонормированном базисе $|\phi_1\rangle, |\phi_2\rangle, \ldots, |\phi_N\rangle$ как случайную величину, принимающую значения $|\phi_j\rangle$ с вероятностями $|\langle\phi_j|\Psi\rangle|^2$. Это есть переформулировка борновского правила. Таким образом, измерение задает случайный процесс, который называется коллапсом волновой функции: при этом процессе происходит переход от состояния $|\Psi\rangle$ к одному из состояний $|\phi_j\rangle$, причем для каждого $j = 1, 2, \ldots, N$ нам известна исключительно вероятность перехода в это состояние, и больше ничего. В этом и состоит суть стандартной или копенгагенской квантовой теории. Она является полной в том смысле, что попытка ее изменить, например, ввести, помимо волновой функции $|\Psi\rangle$ еще и некоторые другие параметры, определяющие состояние (так называемые скрытые параметры) неизменно приводит к отказу от использования стандартного аппарата вообще, и при отсутствии альтернативного аппарата такая попытка превращается в ничто.

Копенгагенская квантовая механика обладает всей гибкостью, необходимой для полной физической теории одной - двух частиц. Например, любой физической величине ставится в соответствие эрмитов оператор A, такой что классические значения этой величины являются собственными числами этого оператора. Измерение этой величины есть измерение состояния рассматриваемой системы в базисе собственных векторов оператора A. Если у двух операторов общий набор собственных функций (это то же самое, что их коммутативность), то это означает, что данные величины могут быть измерены одновременно (с одинаково высокой точностью). Примером может служить энергия частицы и проекция оператора момента импульса на одну из координатных осей (чаще выбирают z). Если же операторы не имеют общей системы собственных функций, то соответствующие им величины не могут

быть измерены одновременно. Например, координата и импульс вдоль этой же оси не могут быть измерены одновременно. Действительно, нетрудно проверить, что если мы выбираем сегменты D_j как последовательные отрезки равной длины, то с точностью до коэффициента матрица оператора координаты x будет иметь вид

$$\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 2 & \dots & 0 \\ 0 & 0 & 3 & \dots \\ \dots & \dots & \dots & \dots \end{pmatrix} \tag{1.8}$$

в то время как матрица оператора импульса для той же координатной оси имеет вид

$$DFT \begin{pmatrix} -h^2\ 1^2/2m & 0 & \dots & 0 \\ 0 & -h^2\ 2^2/2m & \dots & 0 \\ 0 & 0 & -h^2\ 3^2/2m & \dots \\ \dots & \dots & \dots & \dots \end{pmatrix} DFT^{-1} \tag{1.9}$$

где DFT обозначает дискретное преобразование Фурье (см. Приложение - QFT). Числа $1, 2, \dots$ взяты здесь для примера. Это просто числовые значения координаты или импульса в двоичном представлении. Действительно, первое утверждение вытекает из определений непосредственно, а для доказательства второго заметим, что преобразование Фурье переводит дифференцирование в умножение на мнимую единицу и аргумент результата преобразования Фурье. Это свойство здесь и использовано для того, чтобы диагонализовать матрицу, соответствующую оператору импульса. Эта матрица будет диагональной в базисе, который получается преобразованием Фурье из исходного, так что у операторов координаты и импульса действитебно нет общих собственных векторов. Разумеется, если рассмотреть, например, координату x и оператор импульса вдоль другой оси, например, p_y, то у таких

операторов будет общая система собственных векторов, и их можно измерить одновременно.

Одновременное измерение здесь трактуется как измерение обоих величин с одинаковой точностью. То есть возможность сколь угодно точно знать одновременно значения и одной и другой величины. Если же отказаться от требования абсолютной точности, то, конечно, измерить можно любые две величины. При этом, если одна из них приняла определенное значение (то есть наш вектор состояния совпал с собственным вектором соответствующего этой величине оператора), то другая, вообще говоря, будет иметь некоторое вероятностное распределение значений в соответствии с правилом Борна. Рассмотрим, для примера, двумерное гильбертово пространство, в котором измеряется «координата», а затем «импульс» частицы. Я заключаю название физических величин в кавычки для того, чтобы подчеркнуть, что рассматриваются не настоящая координата или импульс, а их самые грубые приближения, вытекающие из того, что частица может занимать только два пространственных положения, а не континуальный набор, как в стандартных курсах по физике. Поскольку при измерении «координаты» мы попадаем в одно из двух состояний $|1\rangle, |2\rangle$, а преобразование Фурье в двумерном случае имеет матрицу Адамара (с точностью до фазового сдвига

$$\begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix}$$

то вероятность получить каждый из возможных значений "импульса" 1 или 2, будет равен 1/2. "Импульс частицы" при условии, что эта частица способна занимать только два пространственных положения: $|0\rangle$ или $|1\rangle$, означает, что эта частица либо совершает прыжок из одного положения в другое, либо стоит на месте. Физическая

интуиция дает нам верное понимание этого понятия в такой необычной ситуации. Как видим, можно приписать понятию импульса частицы совершенно определенное понимание, пусть и не сводящееся к одному числу, но тем не менее строгое и корректное в том смысле, что с этим пониманием можно работать дальше. Мы сделали это, опираясь на кубитовый формализм, то есть на специальный математический прием.[2] Кубитовый формализм, как мы видим, более надежен, чем стандартный формализм волновых функций. Он обладает большими выразительными возможностями, так как позволяет трактовать операторы как конкретные эрмитовы матрицы, и таким образом, явно использовать алгебраические приемы. Кубитовая техника более требовательна, чем традиционная аналитическая, так как она явно содержит некое зерно разрешения конфигурационного пространства. Любой изъян формализма, который можно легко скрыть, используя аналитичекую технику, становится явным при использовании техники кубитов, в чем мы убедимся далее на примере квантовой электродинамики. Кроме того, предположение о наличии зерна пространственного разрешения гораздо ближе к реальности, чем предположение о бесконечной делимости пространства. Ввиду этого, я буду в дальнейшем стараться применять именно кубитовую запись квантовых объектов, не оговаривая этого специально. Рассмотренная нами ситуация вообще типична в том смысле, что самым коротким путем к численному результату является простая манипуляция с математическим объектом;

[2]Я предлагая читателю рассмотреть возможности применения для такой задачи эвристику стандартного математического анализа (то есть того, что принято понимать под физической интуицией), когда скорость рассматривается как предел $\Delta s/\Delta t$, и т.д.

все то, что понимают под физической интуицией, обязательно должно сводиться к такой манипуляции. Самостоятельное существование некой физической интуиции, не оформленной как такая манипуляция, есть верный признак отсталости используемой математики.

Итак копенгагенская квантовая механика обладает полным арсеналом для рассмотрения одной или двух частиц, так как две частицы можно свести к одной, выбирая в качестве начала системы координат их общий центр масс. Однако в более сложных задачах она не применима. Трудности начинаются уже в формально одночастичных задачах, но содержащих измерения, см. Пример 2 из 2.4.2. Физически измерение означает взаимодейтсвие рассматриваемой частицы с окружением, состоящим из очень болшого числа частиц, и потому проявляющего классические свойства. То есть фактически, задача об измерении не является уже одночастичной задачей. Это проявляется в виде так называемой декогерентности, то есть распаде квантового состояния при контакте его с окружающими частицами, не входящими в рассматриваемый ансамбль.

1.1.2 Тензорные произведения

Мы подошли к ядру гильбертова формализма квантовой механики - описанию многочастичных систем с помощью тензорных произведений пространств состояний. Эта конструкция символизирует всю мощь классической математики, поскольку дает возможность предсказать явление, которое уже невозможно строго описать с помощью стандартного подхода: существование запутанных квантовых состояний. Мы должны тщательно изучить формализм тензорных произведений так как он является основой дальнейшего изучения квантовых

компьютеров.

Ключевой элемент стандартного формализма многочастичной квантовой механики - взятие тензорного произведения пространств состояний отдельных частиц. Состояние ансамбля нескольких частиц в квантовой теории не сводится к набору их квантовых состояний, а принадлежит тензорному произведению пространств состояний отдельных частиц, составляющих данный ансамбль. В этом состоит фундаментальное отличие квантовой теории от классической. Пусть $\mathcal{H}_1, \mathcal{H}_2, \ldots, \mathcal{H}_n$ - пространства квантовых состояний частиц $1, 2, \ldots, n$ соответственно. Тогда квантовые состояние ансамбля данных частиц составляют тензорное произведение $\mathcal{H} = \mathcal{H}_1 \bigotimes \mathcal{H}_2 \bigotimes \ldots \bigotimes \mathcal{H}_n$, которое мы сейчас определим. Пусть $b_1^j, b_2^j, \ldots, b_{k_j}^j$ есть некоторый базис пространства $\mathcal{H}_j$, $j = 1, 2, \ldots, n$. Тогда базисом пространства $\mathcal{H}$, по определению, будет набор всех формальных произведений вида

$$b_{i_1}^1 \bigotimes b_{i_2}^2 \bigotimes \ldots \bigotimes b_{i_n}^n,$$

где знак тензорного произведения часто опускается. Например, если у нас только два пространства, и оба представляют собой состояния кубитов - первого и второго, то в их произведении базис будет таким: $|0\rangle|0\rangle, |0\rangle|1\rangle, |1\rangle|0\rangle, |1\rangle|1\rangle$. Часто в дираковских обозначениях $\rangle|$ также опускается и пишут просто $|00\rangle$ и т.д. Теперь мы можем отождествить волновую функцию вида $\Psi(r_1, r_2, \ldots, r_n)$ с вектором в тензорном пространстве $\mathcal{H} = \mathcal{H}_1 \bigotimes \mathcal{H}_2 \bigotimes \ldots \bigotimes \mathcal{H}_n$ где всевозможные значения r_1 принадлежат базису $\mathcal{H}_1$, и т.д. Если у нас есть состояния $|\psi_j\rangle \in \mathcal{H}_j$ $j = 1, 2, \ldots, n$, то их тензорное произведение $|\psi_1\rangle \bigotimes |\psi_2\rangle \bigotimes \ldots \bigotimes |\psi_n\rangle$ определяется так. Надо разложить каждое состояние по базису, и перемножить эти записи, считая что знак тензорного произведения $\bigotimes$ обладает всеми свойствами произведения, кроме

коммутативности, то есть дистрибутивен по отношению к сложению, и допускает вынесение числового множителя. Такое произведение состояний принадлежит тензорному произведению пространств.

Если $A^j : \mathcal{H}_j \longrightarrow \mathcal{H}_j$ есть линейные операторы, мы определим их тензорное произведение $A = A^1 \bigotimes A^2 \bigotimes \ldots \bigotimes A^n$ так. Сначала определим этот оператор естественным образом на базисных векторах

$$\mathcal{H}: \; A(b^1_{i_1} \bigotimes b^2_{i_2} \bigotimes \ldots \bigotimes b^n_{i_n}) =$$

$$= A^1(b^1_{i_1}) \bigotimes A^2(b^2_{i_2}) \bigotimes \ldots \bigotimes A^n(b^n_{i_n}),$$

а затем распространим этот оператор по линейности на все пространство $\mathcal{H}$.

Не всякий вектор из $\mathcal{H}$ имеет вид тензорного произведения векторов из отдельных пространств. Например, в случае двух кубитов вектор $|00\rangle + |11\rangle$ представить в таком виде невозможно. Такие состояние называются запутанными, в знак того, что их нельзя свести к комбинации (произведению) отдельных состояний. Именно наличие запутанных состояний делает квантовую физику многих частиц принципиально более сложной, чем классическая, где нет такого понятия как запутанность. С другой стороны, запутанность не имела бы никакого особого смысла, если бы мы представляли частицу как точечную, то есть классически. Таким образом, запутанность есть удивительное, чисто квантовое явление. В главе 6 мы увидим, что оно приводит к макроскопическим следствиям. Таким образом, квантовую механику нельзя свести к поправкам к классической. Она одна дает нам ключ к пониманию наблюдаемой картины мира.

Если мы работаем с обычной записью волновых функций $\Psi(r_1, \ldots, r_n)$, тензорное произведение надо

трактовать как обычное произведение $\psi_1(r_1)\psi_2(r_2)\dots\psi_n(r_n)$. Смысл математического определения, данного нами состоит в том, что оно действует в кубитовом формализме, который полностью адекватен квантовой теории, поскольку включает в себя зерно пространственного разрешения: мы используем это зерно для выбора базиса $b_1^j, \dots$ для каждой частицы. Например, мы можем считать, что b_1^1 означает нахождение первой частицы в точке 1, b_2^1 - нахождение ее в точке 2 и т.д. При этом зерна для разных частиц могут, вообще говоря, иметь разный размер. Также и частица сама по себе может быть целым ансамблем, состоящим из более мелких частиц, так что ее пространство тоже получается как тензорное произведение, и т.д.

1.2 Унитарная динамика и измерения

Самой фундаментальной особенностью квантовой теории является двойственное описание динамики любого объекта, которая подразделяется на два совершенно особых типа: унитарная динамика и измерения. Эта особенность настолько фундаментальна, что, по видимому, должна быть в той или иной форме сохранена для любого нового подхода к вычислениям на базе квантовой теории.

Рассмотрим эти два вида динамики отдельно.

Унитарная динамика. Считается, что возможные состояния $|\Psi\rangle$ квантовой системы образуют некое гильбертово пространство состояний $\mathcal{H}$, так что изменение любого состояния во времени при переходе от момента t_0 к моменту t_1 задается унитарным оператором

$$U_{t_0,t_1} : \mathcal{H} \longrightarrow \mathcal{H} \tag{1.10}$$

Можно еще детализировать это утверждение, сказав, что этот оператор имеет вид $U = exp(-\frac{i}{h}H(t_1 - t_0))$, где H называется гамильтонианом данной системы, и равен оператору ее полной энергии (зависящей от самой этой системы и от внешних потенциалов), что является просто переформулировкой того обстоятельства, что эволюция конкретного состояния $|\Psi(t)\rangle$ определяется уравнением Шредингера. Принципиальным в этой аксиоме квантовой теории является то, что если бы мы взяли вместо $|\Psi\rangle$ любое другое состояние $|\Psi_1\rangle$ в пространстве $\mathcal{H}$ и поставили бы его в те же самые условия, что и $|\Psi\rangle$, то мы бы получили результат применения того же самого оператора U_{t_0,t_1}.

Как это утверждение можно проверить ? Для этого есть единственный путь: надо брать всевозможные состояния $|\Psi\rangle$ в качестве начальных состояний и подвергать их действию тех же самых потенциалов, чтобы посмотреть на результат их эволюции. После этого надо каким то образом сравнить результаты их эволюций, то есть состояния вида $U_{t_0,t_1}|\Psi\rangle$, чтобы сделать вывод о том, насколько эта аксиома верна.

Но для этого совершенно необходимо сравнивать между собой квантовые состояния. Оказывается этого нельзя сделать только с помощью унитарной эволюции. Для этого необходим совершенно другой вид эволюции квантовых систем, называемый измерением. Таким образом, даже само определение унитарности эволюции ровным счетом ничего не означает до тех пор, пока мы не применили к нашей системе измерение. Этот принципиальный факт говорит о том, что **не существует чисто квантовой механики, которая бы не опиралась бы на классическую механику, описывающую процесс измерения.**

Измерения. Зафиксируем некоторый базис

$\{|\psi_1\rangle, \ldots, |\psi_n\rangle\}$ в пространстве $\mathcal{H}$, о котором будем считать, что он ортонормирован. Тогда измерением в этом базисе называется случайная величина, принимающая значения $|\psi_j\rangle$ с вероятностями $|\langle\psi_j|\Psi\rangle|^2$. Это и есть правило Борна вычисления квантовых вероятностей, которое в стандартном формализме принимается как аксиома. Нет никакого иного способа извлечь информацию о квантовом состоянии, кроме как подвергнуть его процедуре измерения. Единственный выбор при этом заключается в выборе базиса $|\bar{\psi}_j\rangle$ - он зависит от экспериментальной установки, на которой проводится измерение. Чаще всего выбирают измерение каких-либо дополнительных величин, например, координаты (и тогда говорят о координатном базисе в пространстве состояний), либо импульса (и тогда говорят об импульсном базисе в пространстве состояний). Измерить же одновременно и координату и импульс невозможно в том смысле, что не существует ортонормированного базиса, объединяющего векторы из двух различных ортонормированных базисов одного пространства.

Физически измерение означает контакт изучаемой системы с некоторым классическим объектом, состоящим из множества частиц. так что унитарный характер квантовой динамики при таком процессе совершенно теряется и от него остаются только вероятности. Поскольку измерение есть единственная возможность что-то узнать про состояние квантовой системы, для того, чтобы пользоваться квантовой теорией, абсолютно необходима классическая физика.

Из этих двух постулатов квантовой теории можно сделать очень серьезное заключение. Утверждение об унитарности квантовой эволюции касается не одной отдельно взятой эволюции, а огромного числа однотипных

экспериментов, при которых только после статистической обработки их результатов будут видны такие свойства как линейность, сохранение норм векторов и т.д. При этом для обработки даже единичного эксперимента (одной эволюции) необходимо привлекать принципиально многочастичные системы, к которым мы уже не сможем применять квантовой механики, а будем вынеждены пользоваться механикой классической, чтобы определить, какой же исход измерения в действительности произошел: $|\psi_{j_1}\rangle$ или $|\psi_{j_2}\rangle$. Если мы по каким-либо причинам не можем обеспечить идентичности условий экспериментов (включая совпадающую настройку аппаратуры для разных экспериментов, и вообще возможность пользоваться макроскопическими приборами для измерения), утверждения о квантовом характере эволюции теряют всякий смысл.

Таким образом, квантовая теория для самого своего существования требует наличия многочастичных систем и возможности непосредственно вовлекать их в эксперимент. При этом мы должны иметь много частиц (макроскопический прибор) одновременно для измерения состония, а также много частиц для выбора их в качестве измеряемой квантовой системы, чье состояние $|\Psi\rangle$ мы изучаем. Сколько времени займет процедура измерения ? Если предположить, что частицы одного типа идентичны, можно произвести одновременно очень много экспериментов (как это и делается в статистической квантовой теории). Можно напрямую проверить аксиому о идентичности элементарных частиц, имеющих одинаковый тип. Для этого надо произвести множество последовательных экспериментов над одной и той же частицей. Современные приборы, такие как сканирующий туннельный микроскоп, позволяют адресоваться непосредственно к индивидуальным атомам,

поэтому для постановки такого рода экспериментов нет принципиальных трудностей, кроме времени.

1.2.1 Абстрактная модель квантового компьютера

Теперь мы опишем абстрактную модель квантового компьютера, которая может уже использоваться для подсчета его сложности, то есть времени T_{qua}.

Эта модель состоит из двух частей: классической и квантовой. Классическая часть состоит из регистров, в которых указаны номера элементарных унитраных операций из некоторого списка $U_1, U_2, \ldots$ простых 1-2 или 3 кубитных унитарных операторов, и указателей, то есть стрелок, которые указывают, к каким кубитам надлежит применить данный оператор. Кроме этого, классическая часть содерит два особых регистра: регистр конца вычисления и регистр вопроса к оракулу.

Квантовая часть компьютера - это лента, в ячейках которой стоят кубиты. Потенциально лента не ограничена в том смысле, что к ней при необходимости можно всегда добавлять новые кубиты, инициализированные состоянием $|0\rangle$. Если лента содержит n кубит, то ее квантовые состояния заполняют 2^n мерное гильбертово пространство состояний. Общий вид состояния квантовой части компьютера таков:

$$|\Psi\rangle = \sum_{j=0}^{N-1} \lambda_j |j\rangle \tag{1.11}$$

где $N = 2^n$, а коэффициенты λ_j есть комплексные числа, называемые амплитудами соответствующих состояний $|j\rangle$. Таким образом, мы всегда можем счиать, что эволюция состояния квантовой ленты происходит в конечномерном

пространстве состояний, размерность которого N нам недоступна, хотя число кубитов n есть вполне доступная величина. Мы видим, что (1.11) совпадает с тем, что мы мы назвали кубитовым представлением волновой функции. Поэтому квантовый компьютер выражает стандартную форму многочастичного гильбертова формализма.

Квантовый алгоритм - это классический алгоритм, задающий изменение во времени состояния классической части компьютера. Вычисление на квантовом компьютере - это последовательность унитарных преобразований над состоянием квантовой части, которая задается состоянием классической части компьютера. То есть на каждом шаге j над состоянием $|\Psi_j\rangle$ выполняется преобразование вида

$$U \bigotimes V \bigotimes W \bigotimes \dots \tag{1.12}$$

где данные элементарные операторы $U, V, W \dots$ коды которых стоят в регистрах классической части выполняются над теми кубитами, на которые указывают стрелки, выходящие из соответствующего регистра.

Таким образом, чисто классический закон изменения управляющей классической части квантового компьютера индуцирует квантовую унитарную эволюцию его квантовой части вида

$$|\Psi(t)\rangle = \sum_{j=0}^{N-1} \lambda_j(t)|j\rangle$$

то есть сводится к изменению во времени амплитуд базисных квантовых состояний.

Мы дали определение вычисления без оракула, или абсолютного квантового вычисления. По аналогии с классическим случаем, можно ввести понятие квантового вычисления с оракулом. Предположим, что нам задан

некоторый унитарный оператор $U : H_1 \longrightarrow H_2$, где H_1 - m и k кубитное гильбертово пространство состояний. Заведем на ленте определенное место: набор кубит (регистр) из m кубит, и специальный регистр в классической части, называемый регистром вопроса (query). Условимся что если регистр вопроса содержит 0, вычисления происходят в обычном порядке. Если же регистр вопроса содержит 1, мы вместо обычного унитарного преобразования, индуцируемого классической частью компьютера, совершаем обращение к оракулу, которое заключается в том, что применяется оператор $I \bigotimes U$, где U применяется к выделенному нами m кубитному регистру, а идентичное преобразование - ко всем прочим. Нетрудно понять, что это определение является непосредственным распространением понятия вычисления с оракулом на квантовый случай.

Конкретизируем понятие квантового оракула на случай обычной функции вида

$$f : \{0,1\}^m \longrightarrow \{0,1\}^k$$

Заведем на квантовой ленте m и k кубитные регистры, назвав первый регистром вопроса, а второй - регистром ответа. Пусть a и b - кортежи из нулей и единиц, содержащиеся в этих регистрах. Введем унитарное преобразование, определенное таким его действием на базисных векторах:

$$Qu_f|a,b\rangle \longrightarrow |a, b \bigoplus f(a)\rangle \tag{1.13}$$

где $\bigoplus$ означает побитовое сложение по модулю 2. Такой оператор является просто перестановкой базисных векторов, и потому он линейно продолжается до унитарного оператора во всем пространстве квантовых состояний. Он инволютивен, то есть $Qu_f^2 = I$. В

Приложении описано, как с помощью этого приема построить быстрый квантовый алгоритм перебора.

1.3 Роль запутанности

Как мы знаем, запутанное состояние двух квантовых систем S_1 и S_2, это состояние, которое невозможно представить в виде $|\Psi_{S_1}\rangle \bigotimes |\Psi_{S_2}\rangle$. Это в точности соответствует, в обычной аналитической записи невозможности представления волновой функции всей системы в виде произведения волновых функций ее частей S_1 и S_2. Можно ввести меру такой запутанности различными путями. Например, с использованием относительной матрицы плотности ρ_{S_1}. Определим меру запутанности как квантовую энтропию $H = tr(\rho_{S_1} \ln\ \rho_{S_1})$, которая равна тому же выражению, взятому для S_2. Такая мера запутанности часто применяется в теории квантовой информации.

Нетрудно понять, что квантовая эволюция любой системы, которая может быть представлена как эволюция незапутанного состояния (то есть тензорного произведения одночастичных состояний) может быть моделирована на классическом компьютере в режиме реального времени, то есть с сложностью, равной физическому времени. Из этого вытекает, что реализация быстрых квантовых алгоритмов на незапутанных состояниях невозможна, то есть квантовый компьютер построен как раз на запутанных состояниях, и без них он свелся бы просто к собственной классической части.

Но было бы ошибочно отождествить множество всех запутанных состояний с состояниями, имеющими максимальную энтропию запутанности H. Возможность получения многочастичных запутанных состояний

даже с максимальной степенью запутанности совсем не означает, что мы создали квантовый компьютер. В качестве примера рассмотрим два класса запутанных квантовых состояний, которые реально детектируются в экспериментах на ионах в ловушке Пауля. Это GHZ и W состояния, имеющие вид

$$\begin{aligned} GHZ: &\quad \lambda_1|11\ldots1\rangle + \lambda_2|22\ldots2\rangle + \ldots + \lambda_k|kk\ldots k\rangle, \\ W: &\quad \lambda_1|100\ldots0\rangle + \lambda_2|010\ldots0\rangle + \ldots + \lambda_k|00\ldots1\rangle. \end{aligned} \tag{1.14}$$

Мы видим, что для хранения таких состояний в памяти компьютера достаточно выделить порядка n ячеек памяти, где n - число кубитов. Это означает, что любые вычисления с такими состояниями можно воспроизводить на классических компьютерах, и имея только такие квантвоые состояния невозможно реализовать быстрые квантовые алгоритмы.

В действительности, состояния типа GHZ и W можно свести к одночастичным состояниям. Рассмотрим сначала состояние GHZ. Его аналогом для $n = 2$ является так называемое шмидтовское состояние двух частиц, то есть состояние двух частиц вида

$$\sum_j \lambda_j |\psi_j^1\rangle \bigotimes |\psi_j^2\rangle \tag{1.15}$$

где $\{|\psi_j^1\}$ и $\{|\psi_j^2\}$ есть ортонормированные базисы в пространствах состояний первой и второй частиц соответственно. Состояние (1.15 характеризуется N числами, где N есть размерность гильбертовых пространств состояний одной частицы. Таким образом, для хранения такого двухчастицного состояния необходим тот же объем памяти, что и для хранения состояния одной частицы.

Состояние GHZ есть форма шмидтовского состояния для нескольких частиц. Такое состояние означает следующее. У нас реально имеется только одна частица, но она состоит из нескольких частей, ведущих себя просто как одно целое. Рассмотрим GHZ состояние при $k = 2$: $|\Psi\rangle = |00\rangle + |11\rangle$. Будем трактовать 0 и 1 как положения одной частицы в двух различных фиксированных точках. Тогда измерение в стандартном базисе одной из частиц повлечет нахождение обеих частиц в одной и той же точке. Если же мы захотим измерить импульс частицы, нам придется применить к соответствующему кубиту преобразование квантовое преобразование Фурье, что в случае одного кубита есть с точностью до условного поворота фазы, оператор Адамара. Применив к обоим кубитам такой оператор мы перейдем в базис, в котором значениями кубитов будут импульсы соответствующей частицы. Простой подсчет показывает, что результат будет тот же: $|00\rangle + |11\rangle$. Это означает, что и импульс у обеих частиц будет одним и тем же при измерении его у любой из них. Это и объясняет то, что такое состояние есть состояние по-существу, одной частицы. Для детектирования такого состояния достаточно проверить интерференционные свойства объекта, состоящего из нескольких частей, например, интерференцию молекулы водорода на двух щелях. Наличие интерференционной картины и будет означать запутанность GHZ типа. Таким образом, данный тип запутанности является достаточно широко распространенным. Более интересно детектирование такого типа запутанности на больших расстояниях. Для ионов в ловушках Пауля оно составляет несколько миллиметров, для фотонов - до нескольких километров.

Не зависимо от числа точек конфигурационного пространства (лишь бы оно было не меньше двух)

справедливы следующие утверждения:

1) Всякое квантовое состояние двух частиц можно представить в виде шмидтовского разложения.

2) Существуют состояния трех частиц, которые нельзя представить в виде шмидтовского разложения.

Простейший пример, для случая 3 кубитов, дает состояние $|100\rangle + |010\rangle + |001\rangle$, или его аналог с разными амплитыдами, что и является простейшим примером состояния типа W (и универсальным в смысле сводимости с применением одночастичных унитарных операторов, запутываний отдельных кубитов с анциллами и измерений, т.н. LOCC- сводимости).

Теперь обратимся к общему виду состояния W типа. Это состояние не может быть сведено к GHZ состоянию никакими LOCC - операциями. Однако его можно трактовать как одночастичное состояние, если рассматривать каждый кубит как элемент конфигурационного пространства. Напомним, что при кубитовом представлении волновой функции мы договаривались кодировать кубитами точки конфигурационного пространства в том смысле, что каждый следующий кубит был уточнением в два раза положения точки конфигурационного пространства. А теперь мы временно примем иное соглашение: каждый кубит будем отождествлять именно с точкой конфигурационного пространства, взятой с предельной возможной точностью. Это соглашение будет совершенно иным. Но тогда, скажем, базисное состояние $|100\rangle$ будет означать нахождение частицы в точке 1 (а точки 2 и 3 свободны), состояние $|010\rangle$ означает нахождение частицы в точке 2 (а точки 1 и 3 свободны), и т.д. Тогда состояние GHZ типа вида (1.14) будет соответствовать волновой функции одной частицы вида $\sum_{j=1}^{k} \lambda_j |j\rangle$.

Запутанные состояния играют центральную роль в квантовой теории многих частиц. Например, без них не возможно дать описание химических реакций.

1.3.1 Моделирование квантовых систем

Теперь обратимся к задаче квантового моделирования физических систем. Это как раз и есть та задача, которую имел в виду Р.Фейнман, выдвигая идею квантового компьютера. Состояние многочастичной системы может быть описано набором чисел, выражающих значение физических величин, таких как массы, координаты, скорости, время и т.д. Эти числа (в отличие от амплитуд) вещественные. Более того, при надлежащем ограничении области рассмотрения и разрешимости измеряющего прибора можно считать, что все они представляются в виде $\frac{l}{2^n}$, где n разумной величины число. Тогда базисное состояние рассматриваемой многочастичной системы можно представить как базисный же вектор в пространстве состояний квантовой памяти из n кубит. Соответственно, линейной комбинации базисных состояний изучаемой системы будет отвечать состояние квантового компьютера с точно такими же амплитудами. Кубиты нашего квантового компьютера для моделируемой системы носят виртуальный характер, т.е. мы не можем приписать им никакого естественного физического смысла. Однако в нашем квантовом компьютере, который будет моделировать изучаемую систему, это реальные, "физические" кубиты. Такой подход к описанию физических систем можно назвать "кубитовым". Мы увидим, что такой подход к описанию физики принципиально более эффективен, чем традиционный "битовый" подход, используемый при численном моделировании многочастичных

процессов на классических компьютерах. Для этого попробуем решить на квантовом компьютере уравнение Шредингера. Здесь снова ключевую роль будет играть быстрое преобразование Фурье, но использоваться будет немного иное его свойство, чем раньше. Это свойство состоит в том, что преобразование Фурье переводит операцию дифференцирования в операцию умножения на независимую переменную с мнимым коэффициентом. Таким образом, если применить его к волновой функции, получится, что оператор двойного дифференцирования, входящий в Гамильтониан, превратится для Фурье-образа волновой функции в оператор умножения на квадрат независимой переменной этого Фурье-образа с неким коэффициентом, а эта переменная есть не что иное как импульс. Эта идея, хорошо известная физикам, вручную решающим волновое уравнение, великолепно работает и для квантового компьютера. Надо лишь убедиться, что квантовое преобразование Фурье обладает аналогичным свойством, связанным с операцией дифференцирования (для нашего квантового симулятора роль дифференцирования будет играть соответствующая конечная разность). Это следует из того, что QFT является приближением оператора настоящего преобразования Фурье при переходе к кубитовому представлению волновой функции.

Нашей целью будет получение состояния нашего квантового компьютера, соответствующего состоянию изучаемой системы в некоторый момент времени t. Нам нужно с помощью рабочих преобразований приблизить действие оператора эволюции $e^{-iHt/h}$ на волновую функцию ψ_0, где $H = H_p + H_x$, $H_p = \frac{p^2}{2m}$, $H_x = V(x)$, $p = \frac{h}{i}\frac{\partial}{\partial x}$ и потенциал $V(x)$ есть вещественная функция. Для простоты возьмем время t равным единице. Реализовать на квантовом компьютере действие H_x просто. Поскольку

матрица этого оператора (а значит и e^{iH_x}) диагональна, для этого надо всего лишь изменить фазы в зависимости от вида базисных состояний, - а это делается примерно так же, как инверсия нулевого состояния в алгоритме Гровера. Однако со вторым слагаемым Гамильтониана это не пройдет. Трудность заключается в том, что оператор H_p не будет диагональным в выбранном нами "координатном" базисе. Однако мы уже знаем, как свести дело к простому диагональному случаю: надо перейти к импульсному базису, иными словами, совершить преобразование Фурье - а это у нас очень хорошо получается. Для этого выберем маленький интервал времени Δt представим приближенно наш эволюционный оператор через формулу Троттера:

$$e^{-iH} \approx (e^{-iH_x \Delta t}\ e^{-iH_p \Delta t})^{1/\Delta t}. \qquad (1.16)$$

В справедливости этой формулы легко убедиться, раскладывая экспоненту в ряд. Мы выбрали "координатный" базис, так что H_x имеет диагональный вид. Применяя квантовое преобразование Фурье: $\mathrm{QFT}: \ f \longrightarrow \int_{-\infty}^{+\infty} e^{-ipx} f(x)\ dx$ и его свойство переводить дифференцирование $\partial/\partial x$ в умножение на ip, мы можем представить действие импульсной части оператора как $e^{-iH_p} = \mathrm{FT}^{-1}\ e^{-ip^2\Delta t/2m}\ \mathrm{FT}$, где средний оператор имеет диагональный вид. Теперь последовательные применения QFT и фазового сдвига на $-p^2/2m$ при реализации последовательности (1.16) дают требуемое приближение.

Примененное в данном методе преобразование Фурье осуществляется по каждой из координат отдельно, и если у нас несколько частиц - то по каждой из координат каждой частицы отдельно. Некоторую совершенно техническую проблему представляет реализация на квантовом компьютере унитарного оператора e^{-iH_x}, соответствующего потенциальной энергии. Если потенциальная энергия просто равна p, то реализация

такого диагонального оператора может быть сделана, если мы просто совершаем последовательные повороты фазы вида $|0\rangle \longrightarrow |0\rangle$, $|1\rangle \longrightarrow e^{i\phi}|1\rangle$, в зависимости от места очередного кубита в регистре, содержащем значение координаты. В случае произвольного вида потенциальной энергии, мы будем предполагать, что ее можно разложить в ряд Тейлора с коэффициентами, которые определяются с помощь достаточно быстрого алгоритма. Например, если этот потенциал получается как сумма кулоновских потенциалов от n разных частиц, то такой алгоритм будет иметь сложность линейную в зависимости от числа n при условии, что координаты частиц также выдаются некоторым фиксированным алгоритмом (который можно рассматривать как оракул). Тогда оператор e^{-ihH_x} можно представить в виде схемы квантовых вентилей (quantum gate array) размера, линейно зависящего от n.

Сложность данного метода в зависимости от времени t реальной физической системы будет $O(t^2)$. Это непосредственно вытекает из того, что точность формулы Троттера имеет второй порядок, поскольку она вытекает из тейлоровского разложения экспоненты до первого члена. Можно понизить сложность до знеачения $O(t^{1+\epsilon})$ для любого $\epsilon > 0$, если вместо формулы Троттера использовать тейлоровское разложение более высоких порядков (см. [65]). Итак, на квантовом компьютере можно моделировать унитарные эволюции - решения уравнения Шредингера почти в реальном времени, и с памятью, пропорциональной размеру рассматриваемой системы.[3] В то время как на обычном компьютере это потребовало бы экспоненциальных ресурсов. Однако в квантовом компьютере мы получаем лишь квантовое состояние, являющееся кубитовым приближением

[3]Предсказывать состояния системы в момент t за меньшее время $t' < t$ можно только в специальных случаях, см., например, [32].

реального, в то время как классическое вычисление дает нам значение амплитуд как таковых.

Заметим также, совершенно аналогично можно производить моделирование унитарной квантовой динамики системы движущихся заряженных частиц в нереляривистском приближении, с учетом электромагнитного поля с векторным потенциалом A. Для этого надо заменить оператор импульса p любой частицы на $p - \frac{e}{c}A$, где e ее заряд, c - скорость света. Проследив вышеизложенные рассуждения, мы увидим, что это никак не отразится на конечном результате. Отметим, что это не является рассмотрением квантовой электродинамики, а лишь нерелятивистским приближением, для которого можно учесть эффекты поля, вводя указанную поправку в гимильтониан. То есть здесь мы считаем поле классическим, что по определению означает, что его можно включить в гамильтониан в виде потенциальной энергии или добавки к ней, или в виде указанной добавки к импульсу.

Глава 2

Задачи

1). Доказать, что пространство квантовых состоний с естественным скалярным произведением (что это?) является гильбертовым (доказать линейность скалярного произведения, неравенство треугольника).

2). Как определить скалярное произведение в случае непрерывных функций $|\Psi\rangle$? Доказать, что это определение переходит в естественное на конечномерном гильбертовом пространстве.

3). Экспонента от матрицы A: $exp(A)$ определяется как сумма ряда Маклорена для экспоненты (что это такое?).

а) Показать, что равенство $exp(A+B) = exp(A)exp(B)$ имеет место для коммутирующих матриц A и B (что это такое?) и может нарушаться для некоммутирующих.

б). Показать, что производную матричной функции $exp(A\ t)$ можно найти по обычному правилу $(exp(A\ t))' = A\ exp(A\ t)$.

3). Эрмитов линейный оператор H определяется формулой $(Hf, g) = (f, Hg)$ для любых векторов пространства состояний. Унитарный оператор U по определению есть линейный оператор, сохраняющий длины всех векторов. Доказать, что а) для любого

эрмитова оператора H оператор $exp(iH)$ является унитарным, б) для любого унитарного оператора U существует эрмитов оператор H, такой что $U = exp(iH)$. (Указание: 1) воспользоваться теоремой о приведении к диагональному виду, 2) использовать определение матричной экспоненты).

4). Почему запись $\langle\psi|H|\phi\rangle$ является корректной только в случае эрмитовости оператора H?

5). В квантовой механике измеряемым величинам соответствуют эрмитовы операторы, которые строятся по аналогии с обычными величинами в классической механике. Если некоторое состояние $|\Psi\rangle$ является собственным для оператора A, то говорят, что величина, соответствующая оператору A принимает в состоянии $|\Psi\rangle$ определенное значение, равное соответствующему собственному числу A. Какие из следующих операторов будут эрмитовыми:

а) оператор градиента (что это такое?),

б) оператор импульса $p = \frac{h}{i}\nabla$ где $h \approx 10^{-27}$эрг сек - постоянная Планка,

в) оператор координаты $x:\ \psi(x) \longrightarrow x\psi(x)$?

г) оператор кинетической энергии (выписать его)?

д) оператор потенциальной энергии (выписать его для частицы в кулоновском поле точечного заряда)?

6). По аналогии с задачей 5) построить квантово механические операторы: кинетической энергии, трехмерного набора координат r, момента импульса. Какие их этих операторов будут эрмитовыми?

7). Как определить диагональный вид операторов над непрерывными функциями? (Указание: перейти к кубитовому представлению конфигурационного пространства). Какие из операторов задач 5) и 6) имеют диагональный вид?

8). Найти собственные значения и собственные векторы

операторов Паули

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

и привести их к диагональному виду. Являются ли эти операторы эрмитовыми? унитарными? Получить коммутационные соотношения вида $[A, B] = C$ где A, B - матрицы Паули. Найти экспоненты от этих операторов.

9). Оператор H в уравнении Шредингера называется Гамильтонианом и является оператором энергии.

а). Написать его явный вид для одномерной частицы. (Указание: использовать результаты задач 5) и 6), а также классическую формулу для полной энергии $E = p^2/2m + V$ где p- импульс, V - потенциальная энергия.

б). Написать его явный вид для трехмерной частицы.

в). Написать его явный вид для системы, состоящей из электрона и протона (атом водорода без учета спинов).

г). Написать его явный вид для системы, состоящей из двух протонов и двух электронов (молекула водорода без учета спинов).

10). Стационарное уравнение Шредингера имеет вид задачи на нахождене собственных значений и собственных векторов Гамильтониана. Сформулировать ее в виде задачи поиска решений некоторого уравнения (Указание: это уравнение имеет вид $H|\Psi\rangle_j = {}_j|\Psi\rangle_j$. E_j называются энергетическими уровнями, $|\Psi\rangle_j$ - соответствующими стационарными состояниями. Считается, что стационраные состояния - это такие, в которых система не излучает фотонов.)

11). Решить стационарную задачу для

а) свободной частицы (это частица в нулевом потенциале).

б) одномерной частицы в бесконечно глубокой потенциальной яме.

в) трехмерной свободной частицы

г)*** трехмерной заряженной частицы массой m и зарядом e в кулоновском потенциале точечного неподвижного заряда (Это - трудная задача. Указание: какой физический объект является прообразом для данной идеализации? Решение можно найти в любой книге по квантовой механике, а также в википедии).

д)** можно ли применять идеальную модель из пункта г), если кулоновское поле создается другой частицей с тем же зарядом, но массой $M \approx 2000m$? Дать грубую оценку точности нахождения энергий такой двухчастичной системы при применении идеальной модели пункта г).

12). Написать уравнение для поиска собственых векторов и значений оператора импульса.

а) Решить эту задачу для свободной частицы (Указание: волна де Бройля $exp(i\bar{p}\bar{r}/h)$. Использовать задачу 5)).

б) Как выглядит решение задачи Коши для уравнения Шредингера в случае свободной частицы с определенным начальным импульсом? (Указание: будет ли определенной также и ее энергия? Использовать результат задачи 11а)).

13). Сформулировать задачу Коши для уравнения Шредингера. Как решать эту задачу, если есть формула для общего решения уравнения Шредингера?

14). Предположим, что стационарная задача для уравнения Шредингера решена. Написать выражение для общего решения задачи Коши для уравнения Шредингера.

15). Написать формулу для нахождения общего решения уравнения Шредингера (Указание: предположить, что Гамильтониан - это просто число, а затем использовать понятие матричной экспоненты и результат решения задачи 3б). В каком случае удобно пользоваться найденной формулой? Можно ли применять

ее, если потенциал V зависит от времени? Как надо понимать экспоненту для того, чтобы эту формулу можно было применять в случае нестационарного потенциала?*** (Это - трудная задача. Указание: использовать понятие хронологической экспоненты (см. [?]).

16). Найти собственные состояния (векторы) и собственные числа оператора координаты. Рассмотреть случай одной частицы и n частиц. (Указание: решить задачу сначала в кубитовой форме. Затем перейти к непрерывному случаю, используя дельта функции Дирака.) Как выглядит разложение произвольного состояния в ряд по собственным функциям оператора координаты? Собственные вектора оператора координаты составляют так называемый координатный базис гильбертова пространства состояний.

17). Как выглядит преобразование Фурье в непрерывном случае? В дискретном? Написать оператор Фурье в кубитовой форме (Указание: Используя кубитовое приближение волновой функции $|\Psi\rangle$, написать, во что кубитовое преобразование Фурье переводит собственный вектор оператора координаты из задачи 16)). Кубитовое преобразование Фурье называется квантовым преобразованием Фурье (Quantum Fourier Tranform - QFT). Выписать, во что обратное квантовое преобразование Фурье переводит произвольный базисный вектор. Выписать матрицу прямого и обратного квантового преобразования Фурье.

18). Собственные функции оператора импульса образуют так называемый импульсный базис пространства состояний. Используя результат задачи 12), написать выражение для оператора перехода от координатного базиса к импульсному и обратного оператора. Будет ли этот оператор унитарным? Эрмитовым? Каково короткое название этого оператора?

(Указание: Рассмотреть кубитовый и непрерывный случаи. Использовать результат задачи 17)).

19). Как выглядит QFT и обратное ему в случае одного кубита?

20). Найти базис пространства состояний, в котором матрица оператора импульса диагональна. (Указание: использовать преобразование Фурье. Решить задачу двумя способами: а) с использованием задачи 18) и б) с использованием того факта, что непрерывное преобразование Фурье переводит дифференцирование в умножение на аргумент и мнимую единицу (см. [**?**]), и того, что QFT является дискретной версией преобразования Фурье).

21). Найти базис пространства состояний, в которой оператор кинетической энергии диагонален. (Указание: использовать задачу 20).

Рассмотрим систему 2 кубитов. Измерение каждого из них может дать 0 или 1. Поэтому у системы есть 4 классических состояния: 00, 01, 10 и 11. Аналогичные им базовые квантовые состояния:

$$|00\rangle, |01\rangle, |10\rangle, |11\rangle.$$

И наконец, общее квантовое состояние системы имеет вид

$$|\Psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle.$$

Теперь $|a|^2$ — вероятность получить в результате измерения $|00\rangle$, и т.д. Отметим, что $|a|^2+|b|^2+|c|^2+|d|^2 = 1$ как полная вероятность.

Если мы измерим только первый кубит квантовой системы, находящейся в состоянии $|\Psi\rangle$, у нас получится:

1) с вероятностью $p_0 = |a|^2+|b|^2$ первый кубит перейдет в состояние $|0\rangle$ а второй - в состояние

$$\frac{1}{\sqrt{|a|^2 + |b|^2}}(a|0\rangle + b|1\rangle),$$

2) с вероятностью $p_1 = |c|^2 + |d|^2$ первый кубит перейдет в состояние $|1\rangle$ а второй - в состояние

$$\frac{1}{\sqrt{|c|^2 + |d|^2}}(c|0\rangle + d|1\rangle).$$

В первом случае измерение даст состояние

$$|\Psi_0\rangle = |0\rangle \bigotimes \frac{1}{\sqrt{|a|^2 + |b|^2}}(a|0\rangle + b|1\rangle),$$

во втором - состояние

$$|\Psi_1\rangle = |1\rangle \bigotimes \frac{1}{\sqrt{|c|^2 + |d|^2}}(c|0\rangle + d|1\rangle)$$

Мы снова видим, что результат такого измерения невозможно записать как вектор в гильбертовом пространстве состояний. Такое состояние, в котором участвует наше незнание о том, какой же результат получится на первом кубите, называют смешанным состоянием. В нашем случае такое смешанное состояние называют проекцией исходного состояния $|\Psi\rangle$ на второй кубит, и записывают в виде матрицы плотности вида $\rho_2 = p_0\rho_{\Psi_0} + p_1\rho_{\Psi_1}$ где матрица плотности состояния $|\psi\rangle$ определяется как $|\psi\rangle\langle\psi|$.

Рассмотрим следующую ситуацию. У нас имеется состояние $\mathcal{A}$, про которое мы знаем, что для каждого $j = 1, 2, \ldots, k$ с вероятностью p_j оно является состоянием $|\Psi\rangle_j$ для некоторого фиксированного списка состояний $\{|\Psi\rangle_j \ , \ j = 1, 2, \ldots, k\}$. Такое состояние можно представить себе как случайную величину, принимающую значения $|\Psi\rangle_j$ с вероятностями p_j. Таким образом, $\mathcal{A}$ не является элементом гильбертова пространства состояний. Такое состояние называют смешанным, в отличие от чистых состояний - элементов гильбертова пространства.

Имея смешанное состояние, мы, в действительности, имеем некоторое чистое состояние, просто мы не знаем, какое именно, и смешанность состояния можно трактовать как меру нашего незнания. Матрица плотности смешанного состояния $\mathcal{A}$ по определению равна

$$\sum_j p_j \rho_{\Psi_j}.$$

Матрицы плотности были впервые введены в квантовую механику Л.Д.Ландау (позже также Дж. фон Нейманом). Их роль состоит в том, что все выводы квантовой теории можно сформулировать только на языке матриц плотностей.

22). Написать общий вид матрицы плотности $\rho_\Psi = |\Psi\rangle\langle\Psi|$ состояния $|\Psi\rangle$ n кубитов. Какой смысл имеют диаготальные элементы этой матрицы?

23). Пусть состояние $|\Psi(t)\rangle$ зависит от времени, и является решением уравнения Шредингера. Написать уравнение, которому подчиняется его матрица плотности $\rho_\Psi(t)$. (Указание: доказать, что формула дифференцирования произведения распространяются на матрицы и использовать ее для получения уравнения на матрицу плотности.)

24). Верно ли, что если два (смешанных) состояния имеют одинаковые матрицы плотности, то мы не можем никакими экспериментами отличить их друг от друга? Под экспериментом понимается выдача экспериментатору реальной системы, находящейся в заданном состоянии, и последующие действия экспериментатора над данной системой. (Указание: дать различные уточнения этой общей формулировки, и рассмотреть унитарные эволюции - решения уравнения Шредингера, и измерения.)

25). Доказать, что общий фазовый множитель $exp(i\phi)$ для всех элементов квантовой суперпозиции не имеет

физического смысла. (Использовать результат задачи 24).

26). Есть ли физический смысл в прибавлении константы к потенциальной энергии? Что эта операция означает на уровне матричной записи уравнения Шредингера?

27). Рассмотрим N- мерное гильбертово пространство состояний. Как записать базисное состояние $|j\rangle$ из этого пространства, где $j \in \{0, 1, \ldots, N-1\}$ в виде столбца координат? Как записать в матричной форме объект $\langle j|$? (Указание: надо, чтобы выражение $\langle j|k\rangle$ обозначало бы скалярное произведение состояний $|j\rangle$ и $|k\rangle$; надо применить определение скалярного произведениия - см. задачи 1 и 2). Как записать в дираковских обозначениях матрицу плотности чистого состояния $|\Psi\rangle$?

28). Верно ли, что матрица плотности всегда является эрмитовой? Каков канонический (диагональный) вид матрицы плотности чистого состояния? Смешанного состояния? Привести алгоритм, распознающий чистоту состояния по заданной его матрице плотности.

29). Чему равен след матрицы плотности? Обосновать ответ. (Указание: использовать правило Борна и аксиомы вероятности).

30). Доказать формулу $trace\ |\Psi\rangle\langle\Phi| = \langle\Phi|\Psi\rangle$.

31). Наблюдаемой называется любой эрмитов оператор H. Как определить понятие среднее $\langle H\rangle_\Psi$ значения наблюдаемой H в состоянии $|\Psi\rangle$? (Указание: использовать набор собственных чисел).

32). Доказать формулу $\langle H\rangle = trace\ (\rho_\Psi H) = trace\ (H\rho_\Psi)$. (Указание: использовать задачу 31). Как вычислить среднее значение наблюдаемой в смешанном состоянии?

33). Верно ли, что по матрице плотности смешанного состояния однозначно восстанавливаются его чистые компоненты? Обосновать ответ. Какое условие надо

наложить на чистые компоненты, чтобы их можно было восстановить однозначно? (Указание: использовать теорему о приведении любой эрмитовой матрицы к каноническому виду).

Рассморим два пространства A и B, и зафиксируем в них ортонормированные базисы $a_1, a_2, \ldots, a_N$ и $b_1, b_2, \ldots, b_M$. Тензорным произведением этих пространств $A \bigotimes B$ называется линейная оболочка формальных выражений $a_i \bigotimes b_j$, $i = 1, 2, \ldots, N$, $j = 1, 2, \ldots, M$, которые считаются ортонормированным базисом в тензорном произведении. Условимся, что знак $\bigotimes$ обладает свойствами ассоциативности, и по отношению к сложению дистрибутивностью. Тогда тензорным произведением состояний $\bar{a} \in A$ и $\bar{b} \in B$ называется $\bar{a} \bigotimes \bar{b} \in A \bigotimes B$. Такое состояние называется не запутанным.

Тензорным произведением операторов A и B называется оператор $A \bigotimes B$, действующий на базисные вектора по правилу: $A \bigotimes B a_i \bigotimes b_j = A(a_i) \bigotimes B(b_j)$. Эти определения естественно переносятся на случай нескольких пространств.

При использовании дираковских обозначений знак тензорного произведения часто опускается.

34). Существуют ли запутанные состояния? Обосновать ответ.

35). Пусть $|\Psi\rangle$ - состояние 2 кубитов. Написать его общий вид. Написать, как будет выглядеть матрица плотности ρ_1 смешанного состояния первого кубита после измерения второго. Доказать, что ρ_1 является матрицей плотности чистого состояния тогда и только тогда, когда состояние $|\Psi\rangle$ было не запутанным.

36). Оператор называется не запутывающим, если он переводит не запутанные состояния двух кубитной системы в не запутанные. Верно ли, что любой не запутывающий оператор для 2 кубитов является

тензорным произведением?

36). Оператор CNOT (control not) действует так: $|x\ y\rangle \longrightarrow |x\ x \bigoplus y\rangle$, $x, y \in \{0, 1\}$, $\bigoplus$ есть сложение по модулю 2. Будет ли этот оператор запутывающим? Будет ли он тензорным произведением? Написать его матрицу. Аналогичные вопросы про оператор Тоффоли на трех кубитах:

$|x\ y\ z\rangle \longrightarrow |x\ y\ z \bigoplus xy\rangle$.

36). Пусть $|\Psi\rangle$ - не запутанное состояние двух кубитов, один из которых находится в распоряжении Алисы, а другой - у Боба. Может ли Боб без обмена информацией с Алисой определить, какие дейтсвия (унитарные операции и измерения) она делает над своим кубитом? Изменится ли вывод, если у Алисы и Боба есть еще дополнительные кубиты (которыми они не могут обмениваться), которые они могут запутывать с основными?

37). Пусть A и B заданы матрицами. Написать короткую формулу для вычисления элементов матрицы их тензорного произведения. Обобщить эту формулу на случай многих кубитов.

38). Написать матрицу оператора Адамара H : $|0\rangle \longrightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|1\rangle \longrightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

39)*. Оператор Уолша Адамара W есть n - я тензорная степень H (что это такое и почему это понятие корректно?). Выписать короткую формулу для элементов матрицы W. (Указание: Используем задачи 37) и 38) и рассмотрим элемент w_{ij}. Написать разложение чисел i и j в двоичной системе счисления и наложить их друг на друга а потом посчитать сколько раз единица придется на единицу.)

40). Эксперимент над состоянием с некоторой матрицей плотности есть последовательность шагов, каждый из которых заключается в том, что экспериментатор получает новую систему, находящуюся в данном

состоянии, а затем проводит над ней (и нулевыми анциллами) некоторые операции - унитарные и измерения. После этого можно статистически обработать данные, полученные на всех шагах. Можно ли ограничиться только однократной выдачей данного состояния - на первом шаге? Иными словами, будет ли такая ограниченная формулировка эквивалентна первоначальной? Обосновать ответ.

41). Существует ли унитарный оператор U, такой что для любого состояния $|\Psi\rangle$ $U|\Psi\rangle \bigotimes |0\rangle = |\Psi\rangle \bigotimes |\Psi\rangle$? (теорема о запрете клонирования квантовых состояний). Применить результат к задаче 40).

Упрощённая схема вычисления на квантовом компьютере выглядит так: берется система кубитов, на которой записывается начальное состояние. Затем состояние системы или её подсистем изменяется посредством базовых квантовых операций. В конце измеряется значение, и это результат работы компьютера.

Оказывается, что для построения любого вычисления достаточно двух базовых операций. Квантовая система дает результат, только с некоторой вероятностью являющийся правильным. Но за счет небольшого увеличения операций в алгоритме можно сколь угодно приблизить вероятность получения правильного результата к единице.

С помощью базовых квантовых операций можно симулировать работу обычных логических элементов, из которых сделаны обычные компьютеры. Поэтому любую задачу, которая решена сейчас, квантовый компьютер решит, и за такое же время. Следовательно, новая схема вычислений будет не слабее нынешней.

Чем же квантовый компьютер лучше классического? Квантовый компьютер способен получать решения некоторых типов задач (переборного типа) значительно

быстрее, чем любой классический компьютер. Это и называется квантовым ускорением.

42). Отражением вдоль вектора $|a\rangle$ называется отображение, действие которого на базисных векторах задается формулой

$$I_a : \ |b\rangle \longrightarrow \begin{cases} |b\rangle, & if \ \langle b|a\rangle = 0, \\ -|a\rangle, & if \ |b\rangle = |a\rangle. \end{cases}$$

Доказать, что это отображение унитарно. Построить его матрицу. Что оно означает геометрически?

43). Пусть $|\bar{0}\rangle$ - базисный вектор вида $|00\ldots0\rangle$, $|\tilde{0}\rangle = W|\bar{0}\rangle$. Написать разложение $|\tilde{0}\rangle$ по стандартному базису. Как выразить $I_{\tilde{0}}$ через $I_{\bar{0}}$ и W?

44)**. Реализовать на квантовом компьютере оператор $I_{\bar{0}}$. (Указание: сканировать кубиты аргумента слева направо, одновременно с нулевой анциллой, нужной для сбора мусора, а результат выявления хотя бы одной единицы накапливать в специальном кубите, который после сканирования использовать для изменения знака. После этого сделать все операторы в сканировании в обратном порядке.)

45). Пусть $f : \ \{0,1\}^n \longrightarrow \{0,1\}$ - n- местная булевская функция. Квантовый оракул, соответствующий ей, действует на базисные векторы так: $Qu_f \ : \ |x,y\rangle \ \longrightarrow \ |x, y \bigoplus f(x)\rangle$ (явно указаны только разряды аргумента и значения функции. Пусть f задана в виде классической схемы из функциональных элементов. Построить квантовый алгоритм, реализующий Qu_f, а также $I_{x_{tar}}$. Сколько вызовов f необходимо для этого? Можно ли обойтись одним?

46). Пусть x_{tar} - единственный корень уравнения $f(x) = 1$, L_2^R - вещественная линейная оболочка (что это такое?) векторов $|\tilde{0}\rangle$ и $|x_{tar}\rangle$. Доказать, что L_2^R есть инвариант отражений $I_{x_{tar}}$ и $I_{\tilde{0}}$.

47). Каков геометрический смысл оператора Гровера $G = -I_{x_{tar}} I_{\tilde{0}}$? (Указание: рассмотреть действие G на L_2^R и его ортогональном дополнении (что это?).

48). Пусть уравнение $f(x) = 1$ имеет не один, а l корней. Какой геометрический смысл тогда будет иметь ограничение G на L_2^R ?

49). Найти натуральное t, такое что $G^t|\tilde{0}\rangle$ максимально близко к $|x_{tar}\rangle$. Если для этого значения t измерить состояние $G^t|\tilde{0}\rangle$, с какой вероятностью получится $|x_{tar}\rangle$? Как ответ зависит от числа корней l?

50). Построить алгоритм для нахождения какого-либо корня уравнения $f(x) = 1$ на квантовом компьютере. Если известно общее число корней, то какова будет его сложность?

51). Решить задачу 50) в случае неизвестного числа всех корней.

52)***. Доказать, что помещенная ниже квантовая схема реализует QFT^{-1}.

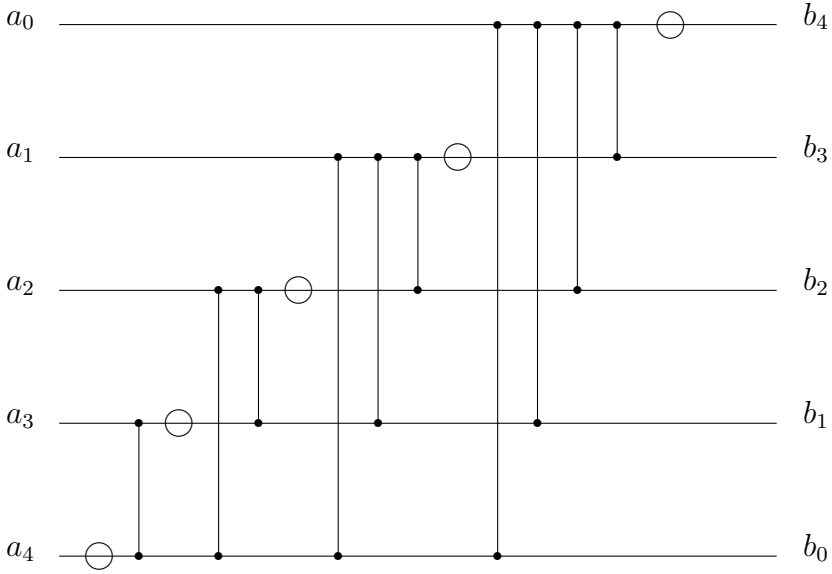

Рисунок 1. Квантовая схема для QFT^{-1}.

Кружки обозначают оператор Адамара, двухкубитные операторы имеют вид:

$$U_{k,j} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\pi/2^{k-j}} \end{pmatrix}, \; k > j. \qquad (2.1)$$

Указание: Зафиксировать два произвольных базисных состояния $a = \sum_j a_j 2^j$ и $b = \sum_k b_k 2^k$ и рассмотреть, с какой амплитудой a переходит в b (это есть соответствующий элемент матрицы оператора, о котором надо доказать, что он равен QFT^{-1} - см. определение

обратного квантового преобразования Фурье из задачи 17).) Амплитуда есть комплексное число, у котрого есть модуль и фаза. Проследить процесс изменения текущего вектора состояния квантового вычисления - слева направо в показанной схеме. При встрече с оператором Адамара меняется модуль амплитуды (а при двухкубитных?) - выписать его результирующее изменение и убедиться, что оно такое, какое надо. После этого посчитать фазу амплитуды. Для этого зафиксировать два значения $j > k$ и определить вклад двухкубитного оператора между j и k кубитами. Обратить внимание на обратный порядок a_j и b_k на входе и выходе. Использовать, то, что a_j переходит в b_{n-j+1} только в результате определенного оператора Адамара. Просуммировать все вклады в фазу и убедиться, что они дают то, что требуется оператором QFT^{-1}. При необходимости использовать пособие ([65]) а также первоисточник ([40]).

53). Дана схема квантовых вентилей, реализующая унитарный оператор U. Построить схему, реализующую оператор $U_{seq}|\Psi, a\rangle = (U^a|\psi\rangle|a\rangle$, где a- один кубит (оператор условного применения, типа CNOT). Указание: расширить набор элементарный вентилей, включив в него условные вентили типа CNOT для всех использующихся вентилей.

54)**. В условиях задачи 53) реализовать U_{seq} для a- произвольное число кубитов. Какова сложность этого квантового алгоритма?

55). Пусть a- n-кубитный регистр, а собственные числа U имеют вид $exp(2\pi i w_k)$ где w_k имеют вид $k/2^n$, k - натуральное. Показать, что применение оператора

$$Rev_U = QFT_2\ U_{seq}$$

где последний оператор применяется к анцилле, к начальному состоянию вида $|\psi, \tilde{0}\rangle$ и последующее

измерение анциллы даст одно из чисел w_k. (Указание: вычислить результат применения оператора.) Этот алгоритм принадлежит Абрамсу и Ллойду. В частном случае, когда U есть умножение на натуральное число, его использовал Шор.

56)***. Показать, что процедура из задачи 55) способна дать приближение с точностью до $s/2^n$ одного из w_k с вероятностью $1 - 1/s$, даже если w_k не имеют указанного в задаче 55) вида. (Указание: оценить вероятность ошибки, если цель состоит в получении приближения с точностью $s/2^n$ для натурального s. Можно воспользоваться пособием ([?]).)

57)***. Пусть q - натуральное число, такое что $2^{n-1} < q < 2^n$, $x^r = 1\ (mod(q))$ (r - мультипликативный период x по модулю q), оператор U_x действует на n кубитное базисное состояние как $U_x|y\rangle = |yx\ mod(q)\rangle$ если $y < q$ и $U_x|y\rangle = |y\rangle$ если $y = q, q+1, \ldots, 2^n - 1$. Доказать, что применение Rev_{U_x} к состоянию из задачи 55) и последующее измерение анциллы позволяет вычислить r. (Указание: использовать результат задачи 56). Какова сложность данного алгоритма?

58)***. Показать, что сложость алгоритма из задачи 57) можно радикально уменьшить, если сделать реализацию $U_{x\ seq}$ экономным образом, используя последовательное умножение вида x^{2^d}, $d = 0, 1, 2, \ldots$.

Из результатов задач 56)-58) вытекает квантовый алгоритм П.Шора факторизации произвольного целого числа q. Для этого надо уметь находить мультипликативные периоды случайно выбранных чисел по модулю q; сложность этого алгоритма $O(log\ q)^2\ log^3(log\ q)$ не намного превышает сложность простого умножения целых чисел $(log^2\ q)$. Алгоритм Шора является самым быстрым из известных квантовых алгоритмов. К сожалению, до сих пор не доказано, что не

существует столь же быстрого классического алгоритма. Самый быстрый из известных классических алгоритмов требует времени $O(q^{1/3})$.

59). Используя результат задачи 52), доказать, что приближенное преобразование Фурье можно реализовать за время $O(n)$ где n - число кубитов. (Указание: отбросить двухкубитные вентили с большим значением $|j-k|$ и оценить возникающую при этом ошибку.)

60). Доказать формулу Троттера $exp(A+B) \approx (exp(\frac{1}{m}A)exp(\frac{1}{m}B))^m$ для эрмитовых матриц A и B (важна ли здесь эрмитовость?). Оценить ошибку этой формулы. (Указание: применить разложение в ряд экспоненты).

61). Вывести более точное выражене для $exp(A+B)$ чем формула Троттера.

62)***. Доказать, что на квантовом компьютере можно получить состояние из $O(n)$ кубит, служащее кубитовым приближением точного решения $\Psi(t,r)$ уравнения Шредингера для квантовой системы из n реальных частиц за время $O(t^2)$, при условии, что потенциалы взаимодействия между частицами имеют простой алгоритм вычисления (схему из функциональных элементов). Указание: используя результаты задач 18), 20) и 52), представить гамильтониан в виде суммы кинетической и потенциальной энергий и применить к возникающим экспонентым формулу Троттера. Затем примерить результаты задач 18) и 20) к импульсной части. Использовать также имеющиеся схемы вычисления потенциалов.

Было показано, что не для всякого алгоритма возможно «квантовое ускорение». Более того, возможность получения квантового ускорения для произвольного классического алгоритма является большой редкостью ([30])

Применение идей квантовой механики уже открыли

новую эпоху в области криптографии, так как методы Квантовая криптография|квантовой криптографии открывают новые возможности в области передачи сообщений. Прототипы систем подобного рода находятся на стадии разработки

2.1 Физические реализации квантовых компьютеров

Построение квантового компьютера в виде реального физического прибора является фундаментальной задачей физики 21 века. В настоящее время построены только ограниченные его варианты (в пределах 10 кубит). Вопрос о том, до какой степени возможно масштабирование такого устройства, является предметом новой интенсивно развивающейся области - многочастичной квантовой механики. Центральным здесь является вопрос о природе декогерентности (точнее, о коллапсе волновой функции), который пока остается открытым. Различные трактовки этого процесса можно найти в списке литературы. Приведем пример реализации операции CNOT на зарядовых состояниях электрона в квантовых точках.

Один кубит можно представить в виде электрона в двух ямном потенциале, так что $|0\rangle$ означает нахождение его в левой яме, а $|1\rangle$ - в правой. Это называется кубит на зарядовых состояниях. Общий вид квантового состояния такого электрона:

$$|\Psi\rangle = \lambda_0|0\rangle + \lambda_1|1\rangle.$$

Зависимость его от времени есть зависимость от времени амплитуд λ_0, λ_1; она задается уравнением Шредингера вида

$$ih\frac{\partial\Psi}{\partial t}\Psi = H\Psi,$$

где гамильтониан H имеет в силу одинакового вида ям и эрмитовости вид

$$\begin{pmatrix} a & -a \\ -a & a \end{pmatrix}$$

для некоторой константы a, так что вектор

$$|\tilde{0}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

есть собственный вектор этого гамильтониана с собственным значением 0 (так называемое основное состояние), а

$$|\tilde{1}\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

- собственный вектор со значением $2a$ (первое возбужденное состояние). Никаких других собственных состояний (с определенным значением энергии) здесь нет, так как наша задача двумерная. Поскольку каждое состояние $|\Psi\rangle$ переходит за время t в состояние

$$\lambda_0 \exp(0t)|\tilde{0}\rangle + \lambda_1 \exp(-2at/h)|\tilde{1}\rangle,$$

то для реализации операции NOT (перехода $|0\rangle - > |1\rangle$ и наоборот) достаточно просто подождать время $t = \pi h/2a$. То есть гейт NOT дается просто естественной квантовой эволюцией нашего кубита при условии, что внешний потенциал задает двух ямную структуру; это делается с помощью технологии квантовых точек.

Для реализации CNOT надо расположить два кубита (то есть две пары ям) перпендикулярно друг другу, и в каждой из них расположить по отдельному электрону. Тогда константа a для первой (управляемой) пары ям будет зависеть от того, в каком состоянии находится электрон во второй (управляющей) паре ям: если ближе к первой, a будет больше, если дальше - меньше. Поэтому

состояние электрона во второй паре определяет время совершения NOT в первой яме, что позволяет снова выбрать нужную длительность времени для производства операции CNOT.

Эта схема очень приблизительная и идеализирована; реальные схемы сложнее и их реализация представляет вызов экспериментальной физике.

Литература

[1] G. Adenier, A. Yu. Khrennikov. Is the Fair Sampling Assumption supported by EPR Experiments?, J. Phys. B 40 No 1 (2007) 131-141

[2] V.Akulin et al, Description of quantum entanglement with nilpotent polynimials: extensive characterization of entanglement and canonical forms, Proceedings of SPIE, 2006, vol. 6264, pp. 02-1 - 02-11.

[3] V.Akulin et al, Quantum computers and computing, 2006, vol. 6 N1, pp. 107-125.

[4] V. Aho, J. E. Hopcroft, and J. D. Ullman. The Design and Analysis of. Computer Algorithms. Addison-Wesley, 1974.

[5] K.Arakelov, Y.Ozhigov, Association of two-atom molecules. Simulation via Quantum state selection, accepted for publication on Vestnik of MGU, Computational mathematics and cybernetics, issue 2009.

[6] Experimental Realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A New Violation of Bell's Inequalities, A. Aspect, P. Grangier, and G. Roger, Physical Review Letters, Vol. 49, Iss. 2, pp.91-94 (1982) doi:10.1103/PhysRevLett.49.91

[7] P.Benioff, Quantum mechanical hamiltonian models of Turing machines, J. Stat. Phys. 29, 1982, 515-546.

[8] C.H. Bennett, E. Bernstein, G. Brassard and U.V. Vazirani, "Strengths and weaknesses of quantum computing" SIAM J. on Computing, Vol. 26, No. 5, pp. 1510–1523, 1997.

[9] G. Birkhoff, J. von Neumann, The Logic of Quantum Mechanics, «Annals of Mathematics», 37 (1936), p. 823—843.

[10] C.H.Bennett, G.Brassard, C.Crepeau, U.M.Maurer, Generalized privacy amplification, IEEE Trans. Inform. Teory, 41, 1915, 1995.

[11] R.Blatt et al, Ion trap quantum computing with Ca+ ions, Quantum Information Processing, vol.3, 1-5, pp. 61-73, 2004.

[12] D.V.Blohintsev, Principal topics of quantum theory, 1977, Moscow, Nauka (Phys-math. lit.).

[13] M. Boyer, M., G. Brassard, P. Hyer, and A. Tapp, "Tight bounds on quantum searching", Proc. 4th Workshop on Physics and Computation, pp. 36–43, 1996.

[14] Bravyi S.B., Kitaev A.Yu. Fermionic Quantum Computation, Ann. Phys. - 2002.- v.298, N.1. - p.210-226

[15] L. E. J. Brouer. Intuitionism and formalism. Amer. Math. Soc. Bull., 20:81–96, 1913.

[16] Durr, C., Hoyer, P., A Quantum Algorithm for finding the Minimum, Proc.Roy.Soc.Lond. A455 (1999) 2165-2172

[17] R.Feynman, The theory of fundamental processes, Caltex, W.A.Benjamin, Inc., NY, 1961.

[18] R.Feynman, Simulating physics with computers, J. Theoret. hys., 1982, 21, pp. 467-488.

[19] R.Feynman, D.Hibbs, Quantum mechanics and path integrals, 1984, Moscow, Nauka (Phys-math. lit.).

[20] M.Genovese, Research on hidden variable theories: A review of recent progress, Physics Reports, 413, 2005, pp.319-396

[21] L.Grover, A fast quantum mechanical algorithm for database search, Proceedings, 28th Annual ACM Symposium on the Theory of Computing (STOC), May 1996, pages 212-219. Proceedings, Melville, NY, 2006, vol. 810, electronic version: xxx.lanl.gov, quant-ph/0610052.

[22] M.A.Horne, A.Zeilinger, Speakable and Unspeakable in Quantum Mechanics, Invited book review, Amer.J.Phys., 42,630 (1989).

[23] A.Khrennikov, Prequantum Classical Statistical Field Theory: Complex Representation, Hamilton-Schr?dinger Equation, and Interpretation of Stationary States, Foundations of Physics letters, vol. 19, N4, pp. 299-319

[24] Kleene, S. C. and Vesley, R. E., 1965, The Foundations of Intuitionistic Mathematics, Especially in Relation to Recursive Functions, North-Holland, Amsterdam.

[25] D.E.Knuth, The art of computer programming, Addison-Wesley, 1997

[26] P.Kurakin, G.Malinetskii, H.Bloom, Dialogue model of quantum dynamics, Proccedings of SPIE, vol. 6264, 2005, Quantum Informatics - 2005 (ed. Y.Ozhigov)

[27] A.A.Markov, About the continuity of constructive functions, Uspehi Mat. Nauk (rus), 1954, 9, N 3 (61), pp. 226-229.

[28] Yu.I.Ozhigov, A.Yu.Ozhigov, Algorithmic container for physics, AIP Conference Proceedings, vol. 962 (Quantum Theory, Reconsideration of Foundations) pp. 168-174

[29] Y.Ozhigov, Amplitude quanta in multi particle system simulation, Russian Microelectronics, 2006, vol. 35, 1, 53-65.

[30] Y.Ozhigov, Lower bounds of a quantum search for an extreme point, Proc.Roy.Soc.Lond. A455 (1999) 2165-2172

[31] Y.I.Ozhigov.Quantum Computers Speed Up Classical with Probability Zero, Chaos Solitons Fractals 10 (1999) 1707-1714

[32] Y.Ozhigov, How behavior of systems with sparse spectrum can be predicted on a quantum computer, Pis'ma v JETP, vol. 76, 11, pp. 799-804.

[33] Y.Ozhigov, Dynamical diffusion as the approximation of one quantum particle dynamics, lanl e-print, quant-ph/0702237

[34] Y.Ozhigov, Quantum recognition of eigenvalues, structure of devices and thermodynamic properties. ZhETF, 2003, vol. 123, iss. 2, pp. 384-398.

[35] Y.I.Ozhigov, Easy control on fermionic quantum computations, NATO Science Series, 2005, vol. 189, pp. 27-32.

[36] A.Ozhigov, K.Arakelov, Y.Ozhigov, Principles of the numerical simulation of many body quantum dynamics, Quantum computers and computing, 2006, vol. 6 N1, pp. 137-148.

[37] Y.Ozhigov, L.Fedichkin, Quantum Computer with Fixed Interaction is Universal, JETP Lett. 77, 328-330 (2003)

[38] R. Penrose, The road to the reality, NY 2006.

[39] J. Shenfield, Mathematical Logic, Nauka, Moscow (1975).

[40] P.Shor, Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, SIAM J.Sci.Statist.Comput. 26 (1997) 1484-1512

[41] J.L. Andrade E Silva, J. Loshak, Fields, Particles, Quanta. Moscow, Science, 1972.

[42] G.S.Tseitin, Algorithmic operators in the constructive metric spaces, Doklady Academii Nauk USSR (rus), 1959, 128, N 1, pp.49-52.

[43] J.A. Wheeler and W.H. Zurek, Quantum Theory and Measurement, Princeton UP, 1983

[44] Wolfram, S. Twenty Problems in the Theory of Cellular Automata. Physica Scripta T9, 170-183, 1985.

[45] C. Zalka: Grover's quantum searching algorithm is optimal. Phys. Rev. A 60 (1999) 2746–2751.

[46] V. Zarnitsyna , J.Huang , F.Zhang , Y.Chien , D.Leckband , C.Zhu , Memory in receptor ligand-mediated cell adhesion, Proc Natl Acad Sci U S A. 2007 Nov 8.

[47] W.Zurek, Probabilities from entanglement, Born's rule from invariance, Phys. Rev. A 71, 052105 (2005)

[48] Н.Боголюбов, Б.Ширков, Введение в теорию квантованных полей, М.,Наука, 1974.

[49] Валиев К.А., Квантовые компьютеры: смена парадигмы вычислений, Вестн. МГУ,сер.15:Выч.мат.и киберн. 2005, N.2. стр .3-16.

[50] Валиев К.А., Квантовые компьютеры и квантовые вычисления, УФН, 175 1 (2005), стр. 3-39

[51] Валиев К.А., Кокин А.А. Квантовые компьютеры: надежды и реальность, Москва-Ижевск, РХД, 2000.

[52] П. Витаньи, М. Ли, Колмогоровская сложность: двадцать лет спустя, УМН, 1988, 43:6(264), 129–166

[53] Владимиров В.С. Уравнения математической физики. М.: Наука, 1981.

[54] П.Дирак, Математические основы теории относительности, М., Мир, 1982.

[55] В.М.Дубовик, частное сообщение

[56] В.П.Кудря, частное сообщение.

[57] Б. А. Кушнер. Лекции по конструктивному математическому анализу. — М.: Наука, 1973.

[58] Л.Д.Ландау, Е.М.Лифшиц, Квантовая механика. Нерелятивистская теория, Москва, Наука, 1974.

[59] Л.Д.Ландау, Е.М.Лифшиц, Гидродинамика, М.Наука, 1988.

[60] А.Н.Мальцев, Алгоритмы и рекурсивные функции, М., Наука, 1986.

[61] Менский М. Б. Концепция сознания в контексте квантовой механики, УФН 175 413 (2005)

[62] С.Н.Молотков, Квантовая криптография и теоремы В.А.Котельникова об одноразовых ключах и об отсчетах, УФН, 2006, т. 176, 7, стр. 777-788

[63] Новиков П. С. Конструктивная математическая логика с точки зрения классической. М.: Наука. 1977

[64] Новосадов Б.К. Методы решения уравнений квантовой химии: Основы теории молекулярных орбиталей. Наука, Москва, 1988, 184 с.

[65] Ю.И.Ожигов, Квантовые вычисления, учебное пособие, Изд-во ВМК МГУ, 2003.

[66] Д.Роджерс, Алгоритмы и рекурсивные функции, М., Мир, 1970.

[67] А.Н.Тихонов, Методы решения некорректных задач, 1986, М.Наука, см. также ДАН СССР, 1963, т. 151, N3, стр. 501-504.

[68] Р. Темам, Уравнение Навье-Стокса. Теория и численный анализ, М.Мир, 1981.

[69] Успенский В.А., Что такое нестандартный анализ? М.Наука, 1987.

[70] Успенский В.А. Лекции о вычислимых функциях, Москва, Наука, 1960

[71] А.Ю.Хренников, Квантовая теория информации, М., Физматлит, 2008.