# Квантовые вычисления (курс лекций)

Ю.И.Ожигов

*Московский Государственный Университет им. М.В.Ломоносова, Факультет вычислительной математики и кибернетики, Московский центр фундаментальной и прикладной математики, Физико-технологический институт РАН им. К.А.Валиева, e-mail: ozhigov@cs.msu.ru*

**Ключевые слова:** Квантовый компьютер, квантовый алгоритм, декогерентность, квантовое моделирование, запутанные состояния, квантовое дальнодействие

# Аннотация

Этот курс лекций уже несколько лет читается в Московском Государственном Университете им. М.В.Ломоносова; его модифицированная версия 2021 года предполагается также к чтению также в Жедженьском университете (Ханьчжоу). Курс посвящен новому типу вычислений, основанных на квантовой механике. Квантовые вычисления принципиально отличаются от классических тем, что они происходят в пространстве так называемых квантовых состояний, а не в обычных бинарных строках. Физическая реалиация квантовых вычислений - устройство, называемое квантовым компьютером, частично уже создано, и его технология продолжает интенсивно развиваться. Квантовые вычисления являются реальным процессом, в котором математическое описание неразрывно связано с квантовой физикой. В частности, квантовая механика сложных систем, образцом которых является квантовый компьютер, в настоящее время только создается, поэтому квантовые вычисления являются фундаментальным направлением в большей мере, чем прикладным. Поэтому в курсе - в целом математическом, большое внимание уделяется физической реализации этого нового типа вычислений. Рассматриваются разные формы квантовых вычисленииий: гейтовая модель Фейнмана, фермионные и адиабатические вычисления. Описывается класс задач, в которых квантовые вычисления не просто эффективнее классических, но и не могут быть ими заменены. Это важнейшие задачи описания сложных процессов на предсказательном уровне. В частности, с использованием феномена квантовой нелокальности, открытого в конце 20 века. Даются также оценки предельной возможности квантовых вычислений - нижние оценки квантовой сложности. Курс рассчитан на студентов физико-математических и естественно-научных специальностей. а также всех интересующихся данным предметом. Требуется знакомство с основами линейной алгебры и математического анализа в объеме первых двух курсов университета.

# Содержание

# Введение

Естествознание изучает закономерности, которым подчиняются сценарии реального мира. Там, где нет закономерностей, царит хаос. Классическая механика родилась из хаоса средневекового описания мира, но натолкнулась на хаос микромира в начале 20 века, из чего возникла квантовая механика, давшая нам микроэлектронику и IT технологии. Дальнейший прогресс связан со сложными сценариями, прежде всего - биологическими. В их описании в настоящее время господствуют представления классической физики, и также пока царит хаос. Геометрический рост биологических баз данных типа Protein Data Bank и требование все более мощных компьютеров для всего лишь внешней, неглубокой обработки накапливаемой информации, не сопровождается видимым прогрессом ни в медицине, ни в фундаментальной биологии, с момента открытия двойной спирали ДНК в 1953 году. Наведение порядка в хаотической области, которую представляет современная биология, требует введение точной теории микромира, то есть квантовых методов. Этой цели и служит квантовый компьютер.

Путь к построению полной теории микромира, включающей сложные системы и процессы, очень труден и мы пока находимся, по существу, в его начале (см. рисунок 1).

Однако все шаги, предпринятые с 1982 года, когда впервые была обнародована идея квантового компьютера (см. [1], [2]), были шагами в верном направлении. В данном курсе мы проследим эти шаги с математической точки зрения.

Квантовые вычисления есть математическое обеспечение квантового компьютера. Для понимания места этого предмета мы должны дать представление о самом квантовом компьютере и о необходимости его создания.

Физика квантового компьютера есть, по-существу, квантовая физика сложных систем, которая отличается от квантовой теории простых систем, так называемой копенгагенской теории. Отличие - в новых, более жестких ограничениях на математический аппарат бесконечно малых, а также и тем, что для сложных систем вычисления играют совершенно особую роль, которой не было в старой, копенгагенской теории. Название этого проекта возникло в далеких временах конца 20 века, когда мы представляли его конечный продукт как некую вычислительную машину, стоящую на рабочем столе, или в лаборатории, и способную вычислять какие-то вещи быстрее, чем классические суперкомпьютеры.

Последние 30 лет показали наивность такого представления. В действительности мы хотим не вычислять что-то абстрактное, мы хотим управлять сложными естественными процессами, что нужно для нашего выживания. И это управление должно вестись на квантовом уровне, потому что ход сложного процесса определяется в микромире, где господствуют законы квантовой физики.

Сами вычисления нужны лишь для того, чтобы управлять. Для этого надо хорошо знать, к чему приведет тот или иной ход в управлении, то есть надо уметь предсказывать поведение управляемой системы (наноустройство, живая клетка или организм), причем делать это в режиме реального времени, то есть быстрее, чем управляемая система сама откликнется на наше управление. Вот эту роль и должен

Рис. 1: Квантовая механика и сложные процессы

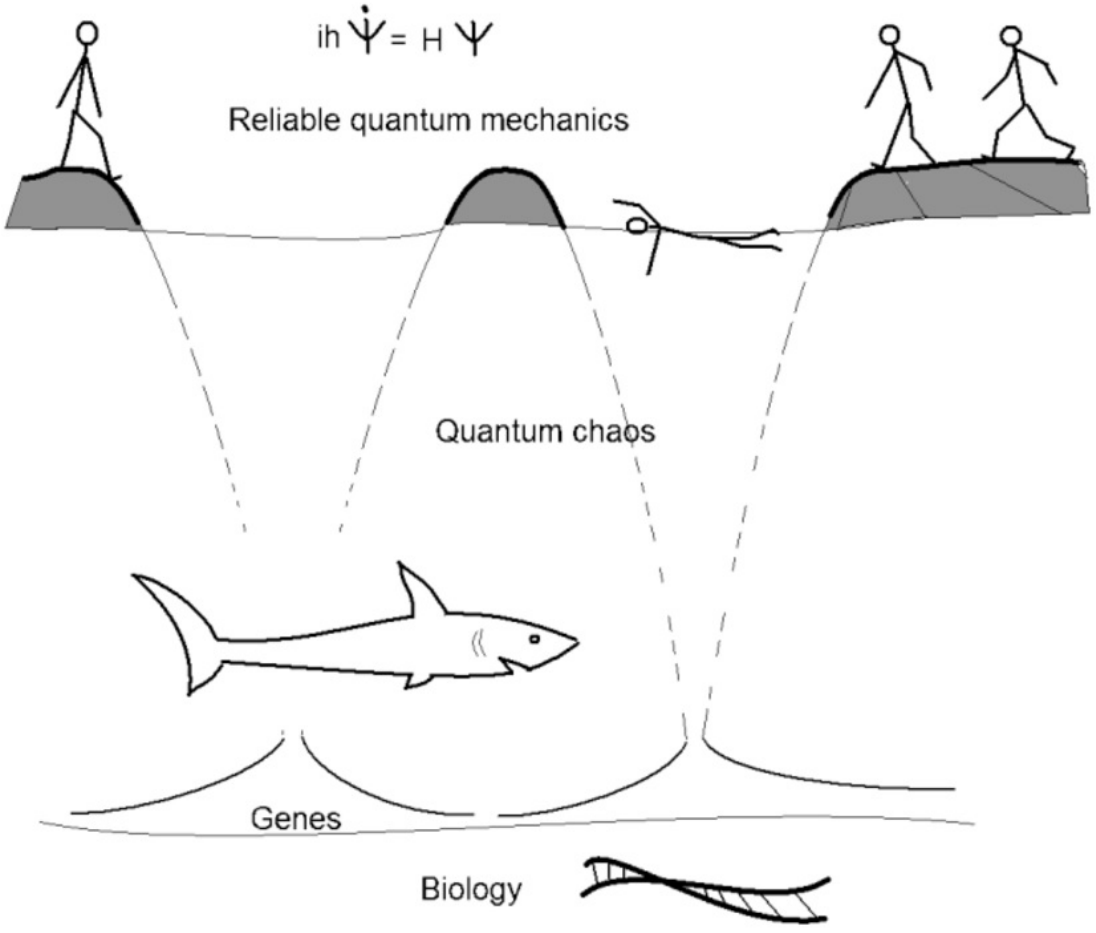
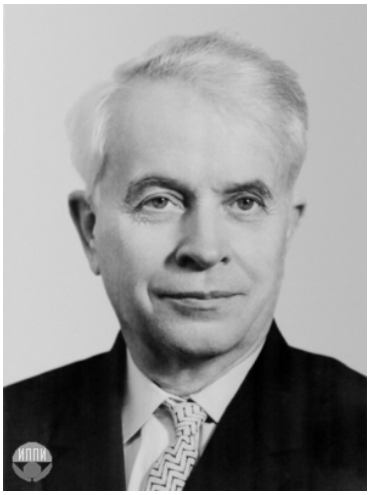


Рис. 2: Андрей Андреевич Марков - младший, основатель конструктивной математики



сыграть квантовый компьютер, как бы он ни выглядел.

Первый шаг на пути создания этого устройства уже сделали наши предшественники - основатели квантовой механики. Этот грандиозный шаг в познании мира привел к появлению компьютеров как таковых. Разумеется, можно отсчитывать историю вычислений от механических арифмометров времен Буля; исторически это имеет основания, но все же компьютер - это микроэлектронное устройство - набор микросхем на кремниево-германиевых гетероструктурах. И принцип работы таких устройств основан на квантовом представлении о состоянии электронов в твердом теле, то есть на квантовой механике.

Вся современная микроэлектроника - достижение квантовой теории. Причем здесь она применяется для управления огромными ансамблями идентичных частиц - бозонов, как фотоны, или фермионов, как электроны. Методы математического анализа работают для таких ансамблей очень хорошо, что и является причиной успеха на этом этапе, охватывающем почти весь 20 век. Мы умеем хорошо управлять такими микроэлектронными системами.

Сегодня нужно научиться управлять более сложными системами биологической природы. Здесь речь идет об отдельных атомах, обладающих индивидуальностью. Отдельные звенья ДНК уже нельзя объединить в ансамбли тождественных частиц, как атомы гелия-4 в жидком состоянии, или как электроны в полупроводящем слое гетероструктуры. Вот этот этап и обозначается термином "квантовый компьютер", и его нам только предстоит пройти. Речь здесь идет об управлении живым, что радикально отличает задачи настоящего времени от прошлых эпох. Роль аналитических методов прошлого сегодня переходит к компьютерам, и идеология Computer Science становится главной в физике сложных процессов. Следовательно, квантовые вычисления становятся математической формой управления этими процессами.

Квантовый компьютер есть метод проникновения в глубины микромира, в ту область, где и сама квантовая теория должна быть преобразована и приспособлена к огромной сложности живой материи. Проект его создания обширный и многообразный, его невозможно охватить в одном лекционном курсе.

В данном лекционном курсе представлена только одна его сторона - математическая, причем с пристрастной точки зрения автора, который сам занимается этой темой. Слушатель может найти описание иных сторон этого проекта в постоянно растущей литературе и обращаясь к архиву http:arxiv.org, раздел quant-ph. Математическая сторона квантового компьютера очень важна, так как здесь аналитический аппарат, привычный физикам 20 века, не является вполне адекватным реальности. Это было ярко продемонстрировано в 90-х годах на примере так называемых быстрых квантовых алгоритмов, основные примеры которых мы подробно рассмотрим.

Развитие проекта квантового компьютера способно оказать серьезное воздействие на ход развития естествознания уже в ближайшие десятилетия, поэтому многие работы по нему не публикуются, а их результаты сразу используются в сфере информационных технологий. Это относится к квантовой криптографии - части проекта, которая оперирует с одним или двумя кубитами или с прецизионными квантовыми приборами; оба эти направления широко применяются в практике. Здесь мы коснемся этих направлений только очень кратко. Нашим предметом будут квантовые вычисления и их связь с важнейшими общенаучными задачами.

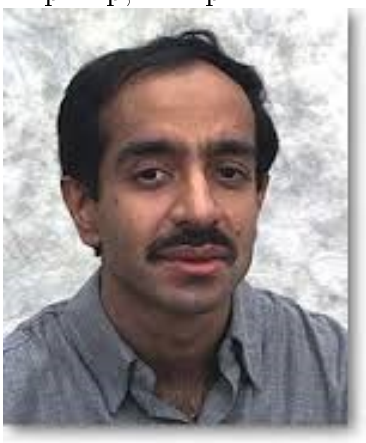
В первых двух лекция дается краткое введение в квантовую механику, необходимое для понимания дальнейшего. По этому предмету есть великолепные физические монографии, начиная с канонической книги Льва Ландау и Евгения Лифшица [3] и многих других столь же превосходных книг. Однако квантовые вычисления диктуют несколько иной, более формальный и краткий стиль изложения, основанный на линейной алгебре. Такой подход позволяет быстро освоить формальный язык, на котором будут описываться квантовые вычислительные процессы. Это позволит сформулировать абстрактную модель квантового компьютера по Фейнману - с пользовательским интерфейсом в виде квантовых гейтов, и перейти к квантовым алгоритмам.

Мы опишем подробно три таких алгоритма, решающие математические задачи: алгоритм Гровера, быстрое квантовое преобразование Фурье и связанный с ним алгоритм факторизации целых чисел Шора, а также алгоритм Залки - Визнера. Первые два иллюстрируют свойство быстрой концентрации амплитуды на целевом состоянии, что позволяет достичь так называемого квантового ускорения классических вычислений. Здесь же мы обсудим вычисления с внешним объектом - оракулом, и его квантовый вид. Будет уделено также внимание нижним оценкам квантовой сложности - предельным возможностям квантовых вычислений. Третий алгоритм предназначен для предсказательного моделирования реальной эволюции сложной системы на квантовом уровне. Выбор именно этих алгоритмов продиктован тем, что именно они полностью раскрывают суть квантовых вычислений и их возможные приложения в области математических задач.

Мы также коснемся квантовых алгоритмов для распределенных вычислений, преимущество которых - в использовании квантовой нелокальности. Будет разобрана схема фермионных квантовых вычислений и управления ими. Будет также разобрана основа квантовой метрологии - особого вида специализированных квантовых вычислений, который предназначен для тестирования прецизионных приборов. Совсем бегло мы коснемся квантовой криптографии - например протокола BB84.

Одна лекция будет посвящена адиабатическим квантовым вычислениям, прояс-

Рис. 3: Лов Гровер, автор квантового перебора



няющим особый статус самого главного уравнения квантовой физики - уравнения Шредингера.

Внимание будет уделено и физической реализации фейнмановской модели квантовых вычислений - квантовых гейтов. Мы разберем конкретную технологию гейтов - на оптических полостях, которая основана на конечномерных моделях КЭД - квантовой электродинамики.

Наконец, мы рассмотрим роль квантовых вычислений в определении пределов применимости самой квантовой теории, а также возможную схему квантовой операционной системы. Квантовые алгоритмы и вычисления используют эту операционную систему как технический базис, но его ограничения непосредстенно влияют на сами алгоритмы. Квантовые вычисления становятся, таким образом, экспериментальной площадкой для определения формы квантовых законов в области сложных процессов.

В заключении мы дадим выводы и возможные пути развития квантовых вычислений и их приложений.

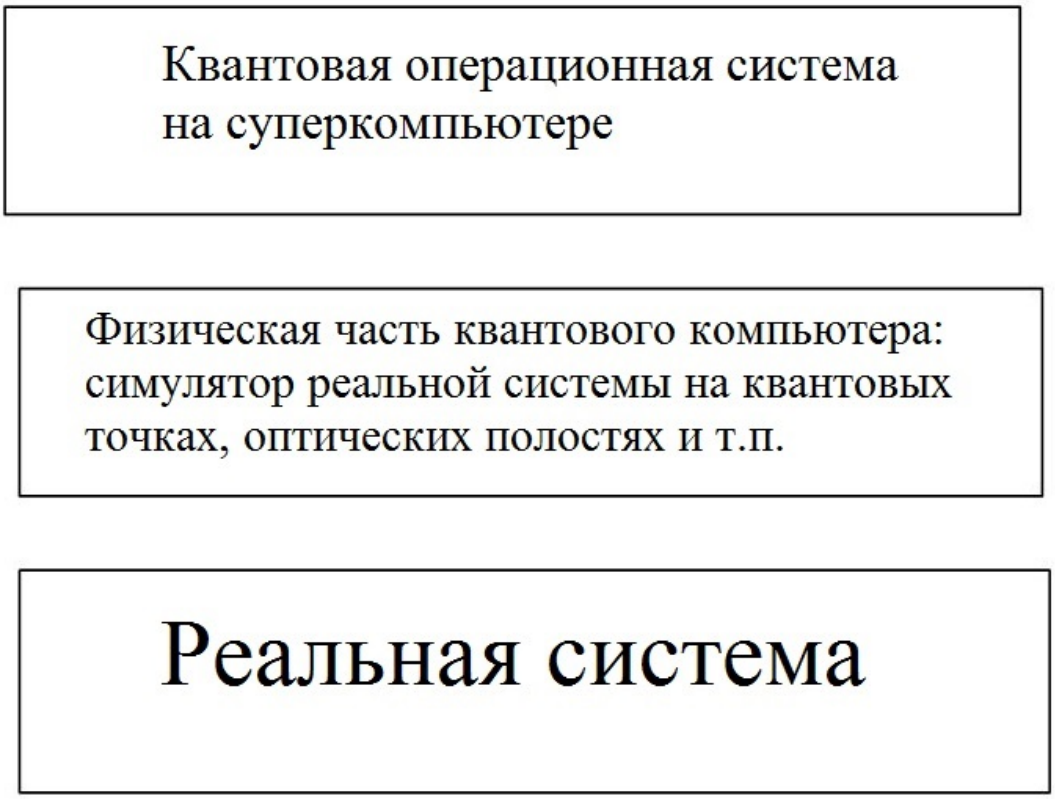
# 1 Лекция 1. Квантовая механика и моделирование Природы

*Все истинное просто и ясно, а там где туман, там всегда какая-то муть*

*Лев Ландау*

Моделирование естественных процессов есть основная задача физики. Если до первой половины 20 века моделирование сводилось, в основном, к алгебраическим вычислениям, которые непосредственно сравнивались с эсперментом, то в конце 20 века выделился компьютер как основной прибор теоретической физики, в который можно загрузить все аналитические выкладки и более того - он может идти гораздо

Рис. 4: Моделирование реального процесса на квантовом компьютере




дальше этих выкладок, представляя нам реальность в виде результата своей работы - как вычисление.

Условимся об основной терминологии. Пусть у нас имеется некое устройство, называемое *компьютером*, которое может находиться в определенном наборе состояний, множество которых мы обозначим через $\mathcal{C}$. *Алгоритмом* мы будем называть отображение $\mathcal{F}$ этого множества в себя:

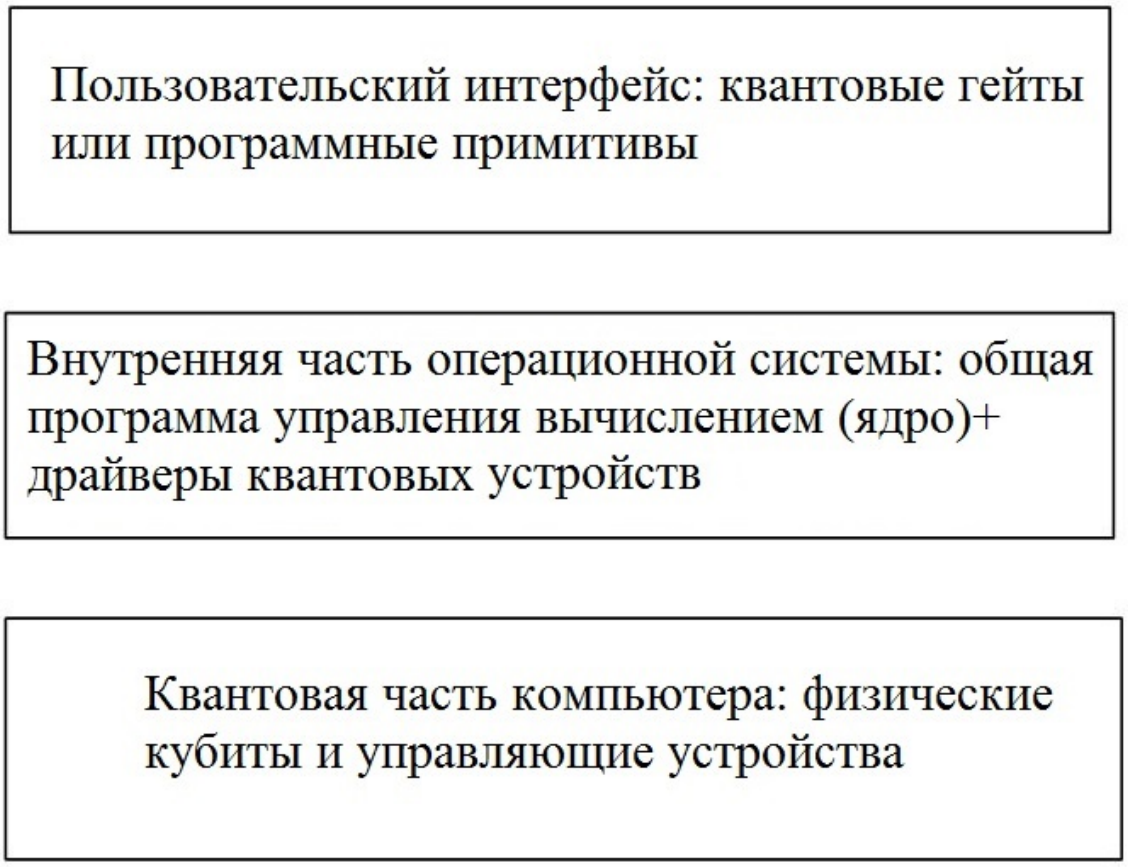
$$\mathcal{F} : \mathcal{C} \to \mathcal{C}.$$

Алгоритм задается в виде некоего правила, которое позволяет по заданному состоянию компьютера получать другое его состояние. Это правило практически чаще всего оформляется в виде компьютерной программы, или в виде рецепта, формулируемого на обычном человеческом языке "надо сделать то-то и то-то".

В классической теории алгоритмов множество состояний компьютера $\mathcal{C}$ является просто набором всевозможных булевских строк вида $a_0, a_1, ..., a_{n-1}$, где $n$ - размер памяти компьютера, $a_j \in \{0, 1\}$.

*Вычислением*, соответствующим данному алгоритму, называется последовательность применения отображения $\mathcal{F}$ к начальному состоянию $\mathcal{C}_0$:

Рис. 5: Схема квантового компьютера



$$\mathcal{C}_0 \longrightarrow \mathcal{F}(\mathcal{C}_0) \longrightarrow \mathcal{F}(\mathcal{F}(\mathcal{C}_0)) \longrightarrow \ldots \longrightarrow \underbrace{\mathcal{F}(\ldots\mathcal{F}}_{T}(\mathcal{C}_0)\ldots) = \mathcal{F}^{\{T\}}(\mathcal{C}_0), \qquad (1)$$

где к конечному состоянию правило $\mathcal{F}$ уже не применимо. Число $T(\mathcal{C}_0)$ называется сложностью работы алгоритма над данным начальным словом $\mathcal{C}_0$; если $T = \infty$, то сложность бесконечна, то есть алгоритм никогда не завершает работу. Так определенная сложность фактически является временем работы, выраженным в абстрактных единицах - числе применений этого оператора.

Отображение $\mathcal{F}$ может зависеть от времени, которое мы определили выше. Для того, чтобы эта ситуация не отличалась от стандартной модели с постоянным оператором $\mathcal{F}$ необходимо включить время в сами состояния $C \in \mathcal{C}$. Такой прием применяется в квантовой электродинамике. Однако с практической точки зрения переменный оператор $\mathcal{F}$ - случай, требующий специальных подходов - это будет обсуждаться в лекции, посвященной адиабатическим вычислениям. В дальнейшем по умолчанию оператор $\mathcal{F}$ не будет зависеть от времени.

Мы понимаем вычисление в широком смысле слова: любой реальный процесс представляется нам в виде некоторого вычисления. Поэтому

**алгоритмом является любой закон природы, который мы можем сформулировать в точных терминах.**

Эта алгоритмическая концепция - конструктивная математика, была создана Андреем Марковым-младшим (см. [4],[5]) и является основой для применения компьютеров к моделированию реальных процессов.

Любой квантовый алгоритм, в конечном счете, является алгоритмом, моделирующим некоторый реальный процесс (см. рисунок 4); и если вычисление по этому алгоритму не дает нужного результата, мы должны сделать вывод, что данный алгоритм неверен. Квантовые алгоритмы есть всего лишь классические *записи* элементарных квантовых операций, которые ведут к нужному результату при условии, что мы правильно понимаем действие законов самой квантовой физики применительно к квантовой части нашего компьютера. Непосредственно проверить факт такого знания невозможно - это можно проверить только на эксперименте.

Отсюда следует неожиданный вывод о том, что построение квантового компьютера есть проверка самой квантовой теории в той области, где она еще никогда не проверялась - в области сложных систем. В задачах физики 20 века мы имели дело с системами простыми, сложность там не играла особой роли, так как эти задачи можно было редуцировать, устранив так называемую запутанность. Дя сложных систем, находящихся в фокусе науки сегодня, этого сделать нельзя.

Наращивание числа кубитов ведет к экспоненциально быстрому росту сложности; с кубитовой памятью мы очень быстро выходим за пределы простых систем, которые легко поддавались анализу физиков прошедшего века. Поэтому квантовые вычисления есть физика нового времени, и наши представления о ней надо еще проверить экспериментально. Мы будем двилаться по стандартному пути копенгагенской квантовой теории, отлично проверенной для простых задач, и посмотрим, куда она нас приведет в области задач сложных.

Пусть мы каким-то образом определили сложность $C(\mathcal{C})$ состояния компьютера $\mathcal{C}$. Возьмем максимальную сложность работы алгорима на начальных состояниях сложности не больше данного натурального $n$ :

$$C(\mathcal{F})(n) = max_{C(\mathcal{C}_0)\leq n} T(\mathcal{C}_0)$$

тогда мы получим функцию натурального аргумента, называемую сложностью алгоритма $\mathcal{F}$.

Для вычислений часто используется внешнее устройство, которое называется *оракулом*. Оракул - объект значительно более сложный, по сравнению с компьютером; его даже вряд ли можно назвать объектом, это, скорее, субъект, который вообще не подлежит алгоритмическому описанию. Например, оракулом может быть пользователь компьютера.

Формально оракул - эта другая функция вида

$$\mathcal{O} : \mathcal{C} \to \mathcal{C}$$

Пусть в множестве состояний компьютера $\mathcal{C}$ выделено некоторое подмножество $\mathcal{Q} \subseteq \mathcal{C}$, состояния которого называются вопросными. Пара $(\mathcal{O}, \mathcal{F})$ называется алгоритмом с оракулом. Вычисление, соответствующее данному алгориму с оракулом, есть последовательность вида

$$\mathcal{C}_0 \longrightarrow \mathcal{L}(\mathcal{C}_0) \longrightarrow \mathcal{L}(\mathcal{L}(\mathcal{C}_0)) \longrightarrow \ldots \longrightarrow \underbrace{\mathcal{L}(\ldots\mathcal{L}}_{T}(\mathcal{C}_0)\ldots) = \mathcal{F}^{\{L\}}(\mathcal{C}_0), \qquad (2)$$

где отображение $\mathcal{L}$ действует как $\mathcal{F}$, если его аргумент не принадлежит $\mathcal{Q}$, и как $\mathcal{O}$, если его аргумент принадлежит $\mathcal{Q}$. Здесь так же, как и выше, отображение $\mathcal{L}$ неприменимо к конечному состоянию комьютера. Такое вычисление работает как $\mathcal{F}$ до тех пор, пока не встретилось вопросное состояние. Если такое состояние встретилось, применяется не обычная функция $\mathcal{F}$, а оракул $\mathcal{O}$.

Немного подумав, мы придем к выводу о том, что взаимодействие пользователя с компьтером в точности укладывается в схему вычисления с оракулом, если последний обозначает пользователя.

## Оракул = пользователь компьютера

Сложностью вычисления с оракулом называется число применений оракула в цепочке (2); сложность алгоритма с оракулом определяется также, как и выше.

Вычисление (1) есть абстрактная модель любого естественного процесса, который описывается законом $\mathcal{F}$, то есть любого реального процесса. Форма вычисления зависит от формы описания состояний рассматриваемой системы. Например, в классической физике состояния из множества $\mathcal{C}$ - это бинарные строки длиины $n$, общее число которых $N = 2^n$. Заметим, что применение математического анализа требует предельного перехода $n \to \infty$. Однако это требование картезианской математики не точно соответствует реальному миру. Например, если речь идет о воздухе в данной комнате, мы не можем, строго говоря, считать его непрерывным: он состоит из

молекул конечного размера. При компьютерном расчете любое представление будет конечным, так как память компьютера всегда ограничена. Именно это обстоятельство означает, что компьютерное моделирование способно более адекватно отражать реальные физические процессы по сравнению с аналитическими формулами.

Можно ли ускорить эволюцию, если расширить память компьютера? Можно ли купить время заплатив за него пространством? Нельзя! Эволюция, в общем случае, не может быть ускорена путем вовлечения новых ресурсов. Распараллеливается только узкий круг задач, называемых переборными. Ускорить выполнение всех задач не сможет и квантовый компьютер.

*Теорема ([6]).*

*Вероятность того, что итерация длины $O(N^{1/7})$ произвольно выбранного из равномерного распределения "черных ящиков" $\mathcal{F}$ может быть ускорена хотя бы на единицу на квантовом компьютере, стремится к нулю при размерности пространства, стремящегося к бесконечности.*

Смысл этой теоремы: доля задач, допускающих квантовое ускорение хотя бы на единицу, исчезающе мала среди всех возможных задач.

Иными словами:

**Квантовое ускорение - редкий феномен, имеющий место лишь для задач типа перебора**

Это объединяет квантовый параллелизм с классическим. Преимущество квантового компьютера состоит в а) потенциальной возможности решения переборных задач быстрее, чем на классическом компьютере, и б) в гораздо более адекватном моделировании реальных процессов.

Преимущество пункта а) не является абсолютным, так как нам неизвестны физические ограничения на использование квантового фрмализма в сложных системах. Преимущество пункта б) имеет огромные перспективы. В частности, мы можем использовать феномен квантовой нелокальности для улучшения качества некоторых вычислений.

## 1.1 Квантовое представление состояний

Описание состояний в виде бинарных строк сооответствует классической физике - это описание через классические алгоритмы.

Для сравнительно простых процессов классическая вычислительная модель (1) вполне адекватна. Однако для процессов сложных это не так. Дело в том, что само бинарное представление состояний в виде бинарных строк неадекватно реальности в случае, когда существенным являются очень малые погрешности в определении состояния. Так бывает в состояниях неустойчивого равновесия, когда для точного моделирования мы должны рассматривать очень малые отрезки времени $dt$ и пространства $dx$, то есть вторгаться в микромир. Здесь важна величина элементарного действия $dS$ (элемент энергии, умноженный на элемент времени), которое используется при моделирования: если $dS \gg \hbar \approx 3 \cdot 10^{-27}$ эрг$\cdot$ сек, классическое описание динамики адекватно, если же $dS$ становится сравнимым с постоянным Планка $\hbar$, описание с точки зрения классической физики становится неадекватным, и оно должно быть заменено квантовым.

Главная особенность квантового описания реальности - множественность. При квантовом описании любой объект может сразу находиться в нескольких классических состояниях. Квантовое состояние есть вектор, который изменяется по матричному правилу: в следующий момент времени он умножается на матрицу эволюции.

Сам же вектор имеет вероятностный смысл. Это означает, что квантовое описание относится не к одному отдельно взятому объекту, а к целой огромной серии одинаково приготовленных объектов; только имея такую серию, мы можем набрать статистику для того, чтобы сравнить теорию и эксперимент.

В квантовом представлении природы любое состояние из множества $\mathcal{C}$ является **линейной комбинацией** (суперпозицией) бинарных строк длины $N$.

Пусть $\mathcal{C}_0, \mathcal{C}_1, ..., \mathcal{C}_{N-1}$ - классические состояния некоторой системы, под которой мы будем всегда понимать оперативную память компьютера. Тогда квантовое состояние этой системы будет иметь вид

$$|\Psi\rangle = \sum_{j=0}^{j=N-1} \lambda_j |\mathcal{C}_j\rangle \tag{3}$$

где комплексные числа $\lambda_j$ называются *амплитудами* состояний $\mathcal{C}_j$. Это означает, что квантовая оперативная память может находиться одновременно во всех возможных классических состояниях, но в каждом таком состоянии $|\mathcal{C}_j\rangle$ - со своей амплитудой $\lambda_j$. В этом - суть квантового параллелизма и возможности квантового ускорения решения переборных задач по сравнению с классическим компьютером.

Например, если классический компьютер имеет оперативную память, состоящую из $n$ битов, то квантовый аналог такого компьютера будет иметь память, состоящую из $n$ квантовых битов (кубитов).

Помимо оперативной памяти, у любого компьютера есть долговременная. Именно в долговременной памяти хранится описание алгоритма $\mathcal{F}$, который не меняется при применении этого отображения, подобно генетическому коду в живой клетке. Таким образом, алгоритм может менять только оперативную память, но не долговременную. В случае классического компьютера эти виды памяти имеют идентичное математическое описание в виде бинарных строк. В квантовом компьютере ситуация иная. Здесь долговременная память также является бинарной строкой, предназначенной для хранения записи алгоритма, но оперативная будет находиться в так называемом квантовом состоянии, который мы называем еще вектор - состоянием. В дальнейшем под памятью мы понимаем, по умолчанию, оперативную память.

Состояние же компьютера есть пара: состояние оперативной и долговременной памяти. Например, состояние, определяющее окончание работы алгоритма, или вопросное преобразование всегда определяется в долговременной памяти компьютера. Здесь мы ограничиваем традиционную теорию алгоритмов, которые допускают "непредсказуемое" поведение времени вычислений. В теории квантовых вычислений момент их конца всегда предсказуем.

Пусть классическое состояние оперативной памяти компьютера имело вид бинарной строки $a_0, a_1, ..., a_{n-1}$. Мы будем представлять такую строку натуральным числом

$$a = a_0 + 2a_1 + ... + 2^{n-1}a_{n-1}$$

лежащим в множестве $\{0, 1, ..., N-1\}$, где $N = 2^n$, и это представление будет взаимно-

однозначным. Тогда квантовое состояние этой памяти будет иметь вид

$$|\Psi\rangle = \sum_{j=0}^{N-1} \lambda_j |j\rangle = \begin{pmatrix} \lambda_0 \\ \lambda_1 \\ \vdots \\ \lambda_{N-1} \end{pmatrix}; \ |0\rangle = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ |1\rangle = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \ ..., |N-1\rangle = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}. \quad (4)$$

Итак, $|\Psi\rangle$ есть вектор - столбец, принадлежащий пространству $C^N$, и все компоненты $|j\rangle$ также есть векторы - столбцы, у каждого из которых все нули, кроме $j$- го элемента, который равен единице. Таким образом, (4) есть разложение произвольного вектора в $N$- мерном комплексном пространстве по базису $|j\rangle$.

Символы | - бра, и $\rangle$ - кет, введены Дираком; они очень удобны и мы всегда будем ими пользоваться.

В этом пространстве определено скалярное произведение, так что векторы $|j\rangle$ образуют ортонормированный базис в нем. Векторы $|\Psi\rangle$ можно складывать и умножать на любое число - при этом будут получаться новые состояния квантовой памяти, которые так же как и $|j\rangle$ являются физически реализуемыми квантовыми состояниями.

Мы введем объект вида $\langle\Psi|$ как результат сопряжения вектора $|\Psi\rangle$, то есть вектор - строка, состоящая из комплексно - сопряженных элементов. Тогда матричное произведение вида $\langle\Psi| \cdot |\Phi\rangle$, которое мы будем кратко записывать как $\langle\Psi|\Phi\rangle$ будет скалярным произведением векторов $|\Psi\rangle$ и $|\Phi\rangle$. Таким образом, мы можем записать условие нормировки на единицу в виде $\langle\Psi|\Psi\rangle = 1$. Для того, чтобы пронормировать любой вектор - состояние $|\Psi\rangle$, нужно разделить его на его собственную норму: $\frac{1}{\sqrt{\langle\Psi|\Psi\rangle}}|\Psi\rangle$. Длина такого пронормированного вектора будет единичной.

В дираковских обозначениях удобно записывать матрицы. Например, матричное произведение столбца на строку вида $|i\rangle\langle j|$ есть матрица, у которой единица стоит на месте $(i, j)$, а в других местах стоят нули. Тогда любую матрицу $A = (a_{i,j})$ можно представить в виде разложения

$$A = \sum_{i,j} a_{i,j} |i\rangle\langle j|$$

а сопряженная матрица - результат транспонирования и комплексного сопряжения элементов, обозначаемая через $A^*$ или $A^+$, будет иметь вид $A^+ = \sum_{i,j} \bar{a}_{i,j} |j\rangle\langle i| = \sum_{i,j} \bar{a}_{j,i} |i\rangle\langle j|$.

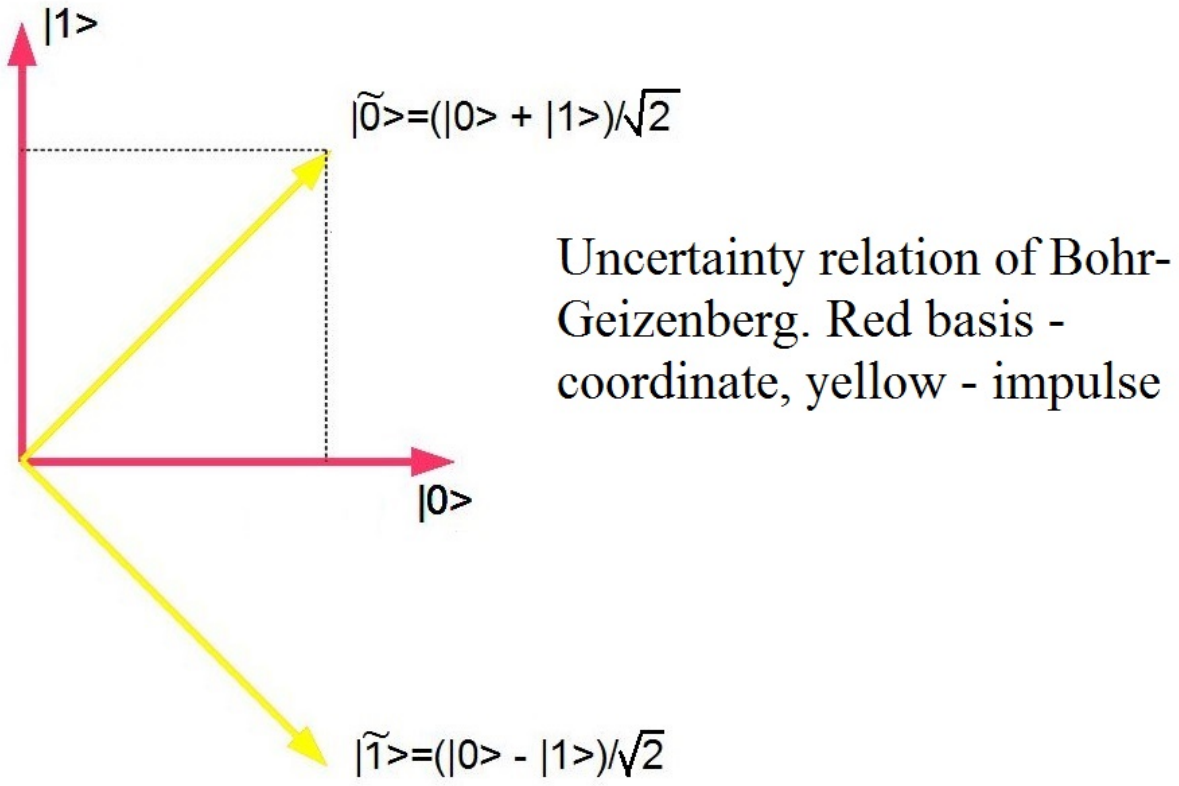
Пусть состояние $|\Psi\rangle$ вида (4) нормировано (на единицу). Тогда его *измерением* называется случайная величина, принимающая значения $|j\rangle$ с вероятностями $p_j = |\lambda_j|^2$. Полная вероятность будет равна единице в силу нормированности этого состояния.

Унитарным оператором $C^N \to C^N$ называется линейный оператор, сохраняющий длину любого вектора. Это эквивалентно тому, что он переводит один ортонормированный базис в другой ортонормированный базис.

В пространстве $C^N$ можно ввести другие базисы, отличные от $|j\rangle$. Это делается применением какого-либо унитарного преобразования $U$ : $|\tilde{j}\rangle = U|j\rangle$. Тогда мы можем обобщить понятие измерения на новый базис $|\tilde{j}\rangle$. А именно, назовем измерением

системы, находящейся в состоянии $|\Psi\rangle$ в базисе $|\tilde{j}\rangle$ случайную величину, принимающую значения $|\tilde{j}\rangle$ с вероятностью $\tilde{p}_j = |\langle\tilde{j}|\Psi\rangle|^2$.

Рис. 6: Соотношение неопределенностей "координата-импульс" для одного кубита. Если точно определена координата, импульс полностью неопределен, и наоборот.



Линейный оператор $H: \ C^N \to C^N$ называется эрмитовым (или самосопряженным), если $H = H^+$. Из линейной алгебры изместно, что для любого унитарного оператора $U$ найдется такой эрмитовый оператор $H$, что $U = exp(iH)$, где матричная экспонента определяется, как и числовая, через ряд $exp(A) = \sum\limits_{n=0}^{\infty} A^n/n!$. Верно и обратное, для любого эрмитова оператора $H$ оператор $e^{iH}$ унитарен.

Известно также, что для любого унитарного или эрмитова оператора имеется его система собственных векторов, которая представляет собой ортонормированный базис всего пространства состояний. Это позволяет ввести понятие *наблюдения*, родственного понятию измерения. Эрмитов оператор $H$ мы будем называть *наблюдаемой*, если выделен базис пространства $C^N$, состоящий из собственных векторов $|\phi_j\rangle$ оператора $H$ с собственными значениями $a_j$: $H|\phi_j\rangle = a_j|\phi_j\rangle$. *Наблюдение* системы, находящейся в состоянии $|\Psi\rangle$, соответствующее *наблюдаемой* $H$ есть случайная величина, принимающая значения $a_j$ с вероятностями $P_j = |\langle\phi_j|\Psi\rangle|^2$.

Итак, измерение и наблюдение - почти одно и тоже, разница лишь в том, что при измерении результатом будут собственные состояния некоторого эрмитова оператора - базис $|\tilde{j}\rangle$ можно рассматривать именно как такие состояния, а при наблюдении - соответствующие этим состояниям собственные значения. Если измерение осуществляет прибор, называемый измерителем, но наблюдение осуществляет наблюдатель.

Измерение есть физический процесс, в ходе которого состояние $|\Psi\rangle$ вида (4) превращается в одно из состояний $|j\rangle, \ j = 0, 1, ..., N-1$. При этом теряется всякая информация о амплитудах $\lambda_j$. Такой процесс происходит при контакте рассматриваемой системы со специальным устройством, которое называется измерителем, или наблюдателем. В квантовой механике нет точного определения какой объект может быть измерителем. Однако термин "наблюдатель" может означать, что таким прибором может быть субъект любой природы, например, человек. Мы пока не будем вдаваться в этот вопрос глубоко, предполагая, что пользователь компьютера всегда может по своей воле инициировать измерение памяти компьютера.

Измерение или наблюдение есть единственный способ хоть что-либо узнать о квантовом состоянии $|\Psi\rangle$, в котором находится данная система. Квантовая механика, таким образом, описывает только вероятности, но не классические состояния. Из этого следует парадоксальный вывод. У одной, отдельно взятой системы, вообще говоря, нет никакого квантового состояния! Квантовое состояние - это характеристика не одного объекта, а огромного числа одинаково приготовленных объектов.

Например, пусть мы рассматриваем электрон в атоме водорода и интересуемся, где он там находится. Измерить его координату можно, облучив атом жестким излучением - фотоном очень высокой частоты. Этот фотон, провзаимодействовав с электроном, вылетит из атома и мы сможем его зафиксировать, после чего можно будет приближенно вычислить, в каком месте находился электрон. Но в результате взаимодействия электрон получит такой импульс, что вылетит из атома совсем! И для следующего эксперимента нам придется взять уже другой атом - предыдущий полностью лишился своего первоначального состояния. Таким образом, для того, чтобы говорить о "квантовом состоянии электрона в атоме водорода", нам нужно иметь огромное количество одинаково приготовленных атомов водорода, чем нас обеспечивает природа. Если бы у нас был всего один, уникальный атом водорода, мы не могли

бы ничего сказать о том, в каком вектор - состоянии находится электрон внутри него.

Квантовая теория не занимается отдельными частицами или отдельными системами частиц. Она занимается только ансамблями независимо и одинаково приготовленных систем или частиц. Вектор - состояние характеризует не отдельную систему атомов, представляющих память квантового компьютера в данном эксперименте, а результат огромного числа одинаковых экспериментов. Квантовые вычисления, таким образом, есть вероятностные вычисления особого рода. Они радикально отличаются от классических вероятностных вычислений, основанных на классической физике. Квантовые вычисления целиком моделируют квантовую динамику реальных сложных систем, в силу чего они претендуют на не только описание, но и управление сложными процессами.

В ходе квантового вычисления мы должны прийти к состоянию вида $|j\rangle$ - к базисному состоянию, измерение которого неизменно дает один и тот же результат. В этом состоит искусство квантовых вычислений.

## 1.2 Унитарная эволюция

Что происходит с памятью квантового компьютера, когда она предоставлена сама себе, и ее никто не измеряет? Тогда ее вектор - состояние удовлетворяет уравнению Шредингера, имеющему вид

$$i\hbar|\dot{\Psi}\rangle = H|\Psi\rangle \tag{5}$$

где $H$ - эрмитов оператор, называемый оператором энергии системы или *Гамильтонианом*, $\hbar \approx 3 \cdot 10^{-27}\ erg \cdot sec$ - постоянная Планка. Если задано начальное вектор - состояние $|\Psi(0)\rangle$, то решение уравнения Шредингера будет иметь вид

$$|\Psi(t)\rangle = exp(-\frac{i}{\hbar}Ht)|\Psi(0)\rangle \tag{6}$$

Формула (6) выражает тот факт, что траектория квантовой системы есть орбита унитарного оператора эволюции $U_t = exp(-\frac{i}{\hbar}Ht)$, действующего на всем пространстве состояний, в отличие от динамики классической системы, которая эволюционирует по своей траектории, заданной начальным значением. Из этого, в частности, следует, что если мы немного ошиблись в исходном векторе состояния $|\Psi(0)\rangle$, то эта ошибка в точности сохранится на любом, сколь угодно длинном промежутке времени, и не будет возрастать, как это возможно в случае классической динамики.

Пусть мы произвели диагонализацию оператора энергии $H$, то есть нашли его собственные функции - вектора $|\phi_0\rangle, |\phi_1\rangle, ..., |\phi_{N-1}\rangle$ и соответствующие собственные значения $E_0 < E_1 \leq E_2 \leq ... \leq E_{N-1}$ (первое неравенство всегда строгое, остальные нестрогие). Тогда мы можем выразить решение уравнение Шредингера с начальным условием $|\Psi(0)\rangle$ в виде такого разложения:

$$|\Psi(t)\rangle = \sum_{j=0}^{N-1} \lambda_j e^{-\frac{i}{\hbar}E_j t}|\phi_j\rangle,\ \lambda_j = \langle\phi_j|\Psi(0)\rangle, \tag{7}$$

что проверяется непосредственно. Таким образом, решение уравнения Шредингера сводится к решению задачи на собственные значения гамильтониана:

$$H|\phi_j\rangle = E_j|\phi_j\rangle. \tag{8}$$

Введем матрицы Паули:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\ \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{9}$$

Матрицы Паули будут и эрмитовыми и унитарными одновременно, и их собственные числа будут равны $\pm 1$ (проверьте это!).

Рассмотрим, в качестве примера, один кубит, состояние которого имеет общий вид $\lambda_0|0\rangle + \lambda_1|1\rangle$. Найдем решение уравнения Шредингера для него с гамильтонианом $H = -\sigma_x$. Собственные векторы состояния имеют вид $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ - для собственного значения $E_0 = -1$, и $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ - для собственного значения $E_1 = 1$, так что общее решение уравнения Шредингера с начальным условием $|\Psi(0)\rangle = |0\rangle$ по формуле (7) после приведения подобных членов примет вид:

$$|\Psi(t)\rangle = cos\left(\frac{t}{\hbar}\right)|0\rangle + i\ sin\left(\frac{t}{\hbar}\right)|1\rangle \tag{10}$$

и мы видим, что со временем будут происходить осцилляции вида: $|0\rangle \to i|1\rangle \to -|0\rangle \to ...$, так что в состояние $|0\rangle$ кубит вернется за время $t = 2\pi\hbar$.

Матрица плотности Ландау состояния $|\Psi\rangle$ определяется равенством $\rho_\Psi = |\Psi\rangle\langle\Psi|$ Предлагается доказать, что уравнение Шредингера для матрицы плотности имеет вид

$$i\hbar\dot{\rho} = [H, \rho] = H\rho - \rho H.$$

## 1.3 Матричная динамика

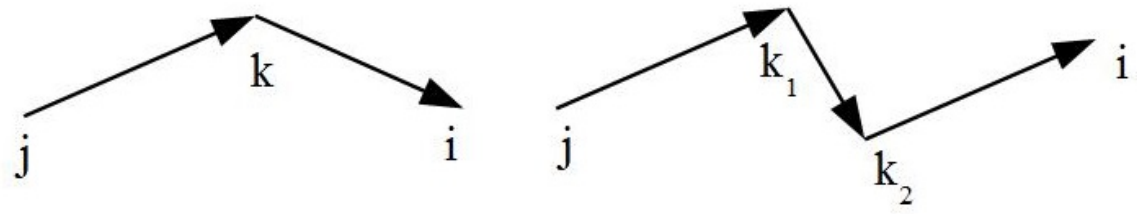
Уравнение (6) означает, что вектор состояния преобразуется во времени путем домножения на некую матрицу эволюции $exp(-\frac{i}{\hbar}Ht)$. Мы предполагаем, что $H$ - постоянная матрица, но она может быть и зависимой от времени - в последнем случае экспоненту надо трактовать как хронологическую экспоненту; мы не будет заниматься этим вопросом, так как такая трактовка ничего не изменит по существу.

Пусть элементы матрицы эволюции обозначаются как $u_{ij}$, а начальное состояние $|\Psi\rangle = |\Psi(0)\rangle$ имеет вид

$$|\Psi(0)\rangle = \sum_i \lambda_i(0)|i\rangle. \tag{11}$$

Тогда правило матричного умножения дает равенство $\lambda_i(t) = \sum_{j=0}^{N-1} \lambda_j(0)u_{ij}$. Рассмотрим его подробнее. Оно означает, что результирующая амплитуда $\lambda_i(t)$ любого состояния $|i\rangle$ получается суммированием разных вкладов: от каждого состояния $|j\rangle$, от его амплитуды $\lambda_j(0)$ этот вклад получается домножением на $u_{ij}$. Таким образом, число $u_{ij}$ является амплитудой перехода $|j\rangle \to |i\rangle$.

Рис. 7: Матричная динамика




А теперь рассмотрим два последовательных интервала времени: $[0,t]$ и $[t,2t]$. Результирующий вектор состояния $|\Psi(2t)\rangle$ будет получаться умножением начального вектора на вторую степень матрицы эволюции $U_t^2$. По правилу матричного умножения мы имеем

$$\lambda_i(2t) = \sum_{j,k=0}^{N-1} \lambda_j u_{kj} u_{ik} \tag{12}$$

то есть переход осуществляется в два этапа: сначала от состояния $|j\rangle$ к состоянию $|k\rangle$, а затем от $|k\rangle$ к $|i\rangle$. Обобщая это на случай конечного времени $T = nt$ мы получим переход от состояния $|j\rangle$ в состояние $|i\rangle$ вдоль пути

$$|j\rangle \to |k_1\rangle \to ... \to |k_{n-1}\rangle \to |i\rangle \tag{13}$$

по $n-1$ звенной ломаной, так что результирующая амплитуды найдется по формуле

$$\lambda_i(nt) = \sum_{j,k_1,r_2,...,k_{n-1}} \lambda_j(0) u_{ik_{n-1}} ... u_{k_2k_1} u_{k_1j} \tag{14}$$

- см. рисунок 7.

Для матрицы эволюции $U_t = exp(-\frac{i}{\hbar}Ht)$ ее элемент $\langle a|U_t|b\rangle$ является амплитудой перехода от состояния $|b\rangle$ к состоянию $|a\rangle$. В первом приближении по $t$ экспоненты мы получаем

$$\langle a|U_t|b\rangle \approx \langle i|1 - \frac{i}{\hbar}Ht|j\rangle = \delta_{ab} - \frac{i}{\hbar}\langle a|H|b\rangle. \tag{15}$$

Из этого мы можем сделать простой вывод. Правило нахождения амплитуды результирующего перехода состоит в том, что а) надо сложить амплитуды перехода вдоль всех путей, ведущих от всех начальных точек в конечную и б) вдоль любого из этих путей амплитуды перехода перемножаются. Это правило лежит в основе "метода циферблата", предложенного Фейнманом в книге [7] для простого объяснения закона квантовой эволюции.

Итак: отдельная квантовая частица ведет себя как рой независимых частиц - ее экземпляров, так что

а) для получения результирующего комплексного числа $\Psi(x,t)$ в данной точке $x$ вдоль каждого пути амплитуда экземпляра умножается , в по всем путям, ведущим в эту точку $x$, амплитуды складываются, и

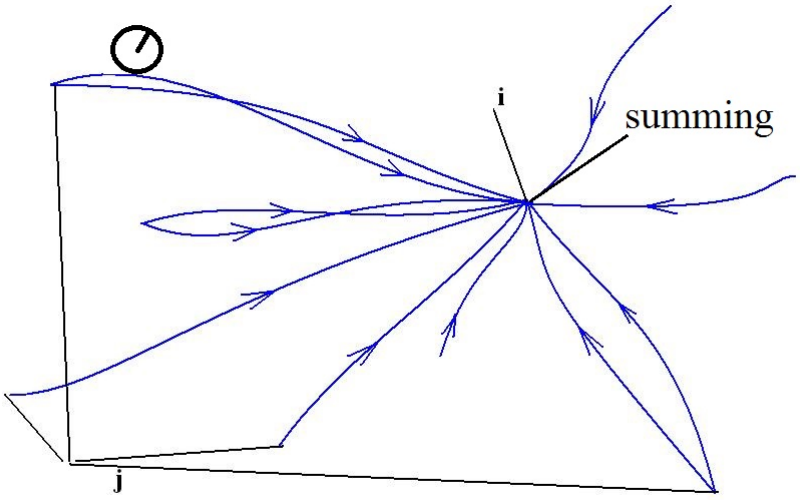



Рис. 8: Матричный закон: стрелки циферблата поворачиваются пропорционально пройденному пути, в конечной точке все стрелки складываются

b) плотность вероятности обнаружения частицы в точке $x$ есть его квадрат модуля: $|\Psi(x,t)|^2$.

Матричная динамика может быть представлена как стрелки циферблата, поворачивающиеся вдоль пройденного пути (см. рисунок 8).

Иллюстрация конструктивной и деструктивной интерференции показана на рисунках 9 и 10

## 1.4 Интегралы по путям

Что получится в пределе, когда мы устремим элементарное время $t$ к нулю, а число звеньев $n$ к бесконечности, так что $T = tn$ будет постоянным? Ломаные траектории (13) заменятся на непрерывные кривые вида $\gamma: \ x = x(t), \ t \in [0,T]$. Для простоты снова рассмотрим случай одномерной частицы. Суммирование в (14) можно разбить на две суммы: одна по $j$, другая - по всем промежуточным точкам $k_1, k_2, ..., k_{n-1}$. Первая сумма даст интеграл

$$\Psi(y,t) = \int\limits_R K(y,x,t)\Psi(x,0)dx, \tag{16}$$

а вторая превратится в правило вычисления матрицы сложного перехода в непрерывном случае:

$$K(y,x,t) = \int\limits_{\gamma:\ x\to y} exp(\frac{i}{\hbar}S[\gamma])\mathcal{D}\gamma, \tag{17}$$

где $S[\gamma]$ - действие вдоль траектории $\gamma$, которое вычисляется по формуле $S[\gamma] = \int\limits_0^t L(\dot{x},x,t)dt$, где $L(\dot{x},x,t) = E_{kin} - V$ - лагранжиан, равный разности кинетической и

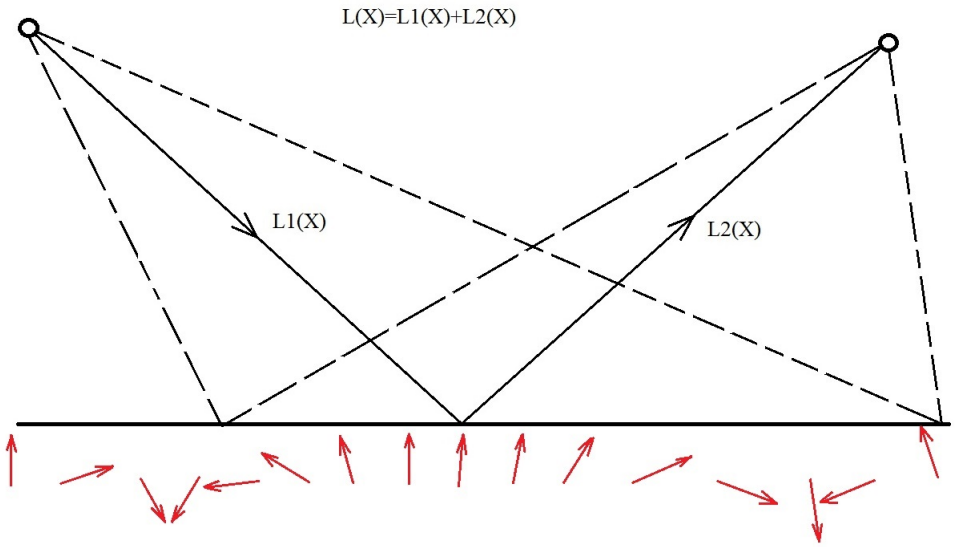



Рис. 9: Отражение света от зеркала

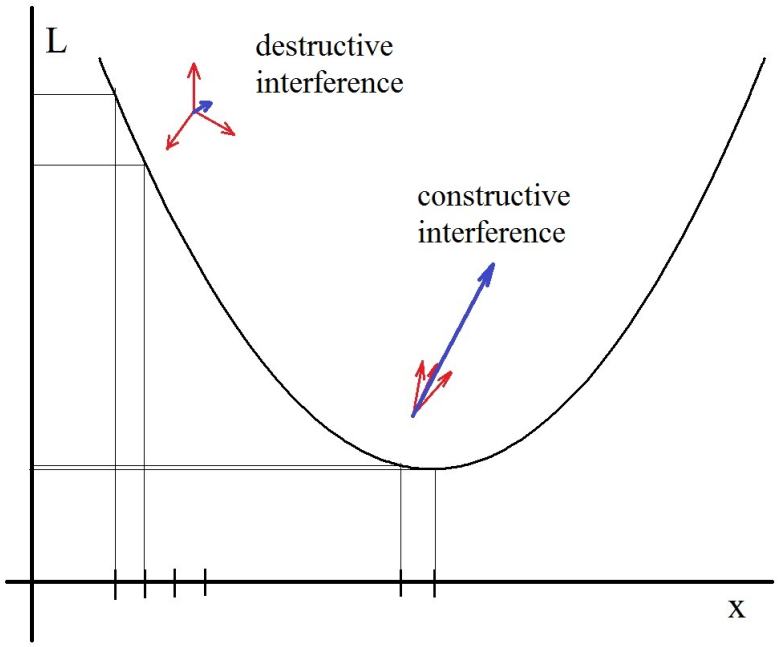



Рис. 10: Конструктивная и деструктивная интерференция

потенциальной энергии частицы, движущейся из точки $x(0) = x$ в точку $x(t) = y$. Эта функция $K(y, x, t)$ называется ядром Фейнмана, а интеграл (17) - фейнмановским интергалом по траекториям.

Аналогия с дискретным случаем проста: $x$ играет роль $j$, $y$ - роль $i$, а $K(y, x, t)$ - роль матрицы эволюции $U_t$. Тогда суммирование превращается в интегрирование по траекториям.

Если начальное состояние частицы $\Psi(x, t)$ - дельта-функция, сосредоточенная в точке $x_0$, то фейнмановское ядро есть волновая функция в момент $t$. (Дельта-функцию мы рассмотрим дальше, пока ее можно неформально представлять себе как состояние, при котором частица находится строго в точке $x_0$, так что вся амплитуды сосредоточена только в этой точке.) Для случая свободной частицы $V = 0$, так что действие будет интегралом от кинетической энергии. Можно показать (см. [8]), что ядро для свободной частицы имеет вид $c \cdot exp(-im(x - x_0)^2/2\hbar t)$ для константы $c$, зависящей лишь от времени $t$. Это определяет расплывание квантового состояния свободной частицы, первоначально сосредоточенной в точке $x_0$: она распространится на всю ось $(-\infty, +\infty)$ за любой, сколь угодно короткий промежуток времени $t > 0$, что иллюстрирует соотношение неопределенности "координата-импульс".

Рассмотрев подынтегральное выражение в (17) мы можем увидеть некоторое несоответствие с формулой (6), а именно: здесь нет знака минус, и при вычислении показателя экспоненты вместо гамильтониана, как в (6) используется лагранжиан, у которого потенциальная энергия стоит со знаком минус. Как это объяснить?

Рассмотрим уравнение Шредингера для частицы в потенциале $V$. Если не обращать внимание на кинетическую энергию, со знаками будет все в порядке: минус впереди показателя экспоненты компенсирует минус в лагранжиане. Займемся кинетической энергией. Ее выражение в $H = \frac{p^2}{2m} + V_{pot}$ как $p^2/2m$ совпадает с выражением через лагранжиан в (17): $m\dot{x}^2/2$, но не сходится знак. Однако, в уравнении Шредингера (5) импульс входит как квантовый импульс $p = \frac{\hbar}{i}\nabla$ а в (17) - как классический импульс $m\dot{x}$. Для того, чтобы перейти от него к квантовому, надо совершить обратное преобразование Фурье, которое изменит знак: $p^2/2m$ превратится в $-p^2/2m$, что в точности нужно для согласования уравнения Шредингера с интегралом по путям. Для малого участка траектории

$$m\dot{x}^2 t/2 = -p^2 t/2m + px.$$

Разумеется, это рассуждение не есть доказательство того, что фейнмановские интегралы по путям эквивалентны уравнению Шредингера, формальное доказательство приведено в книге [8], к которой мы и отсылаем слушателя за деталями.

Фейнмановские интегралы являются, таким образом, непрерывным аналогом матричной динамики, который подчеркивает естественность перехода от непрерывных величин к дискретным. Эти интегралы естественно обобщаются на случай композитных систем многих частиц, или заряженных частиц и электромагнитного поля, что позволяет вычислять, например, амплитуду испускания фотона релаксирующим атомом (см. книгу [8]), а также и обобщать квантовую динамику на релятивистский случай, когда движения зарядов происходят со скоростью, сравнимой со скоростью света.

Важнейшим достоинством интегралов Фейнмана является простое объяснение перехода от квантового описания динамики к классическому.

Сначала рассмотрим отражение света от зеркала, классический закон которого: угол падения равен углу отражения. Рассмотрим фазу $\phi$ воображаемой "волновой функции фотона" $\psi(x,t) = e^{i\phi(x,t)}$, считая его точечной частицей, и ее изменение вдоль различных путей, кажый из которых определяется точкой отражения $x$ от зеркала (см. рисунок 9). (В действительности волновая функция фотона есть отображение вида $|\Psi_{ph}\rangle : \mathcal{K} \to C$, где $\mathcal{K}$ - множество всех классических состояний электромагнитного поля. Под "волновой функцией" мы понимаем здесь то классическое состояние $exp(ip(x-ct))$, на котором $|\Psi_{ph}\rangle$ концентрирует основную часть амплитуды.) Классическая траектория обладает таким свойством. Если ее немного возмутить, то длина пути не слишком изменится, и результирующие фазы вдоль исходного и возбужденного путей (фаза пропорциональна длине пути) будут примерно одинаковы (см. рисунок 10). Это значит, что вклад траекторий, близких к классической, будет преобладать, и можно считать, что свет движется по классической траектории, где угол падения равен углу отражения. Но если длина путей очень мала (источник света очень близок к приемнику), то это рассуждение не пройдет, надо будет учитывать вклад всех траекторий, а не только классической, так как тогда изменение длины пути будет сопоставимо с его длиной.

Это рассуждение переносится на общий случай и показывает границы применения классической физики.

Рассмотрим формулу для ядра (17). Здесь производится интеграция по всем путям, идущим от начальной точки к конечной. Но среди этих путей есть один выделенный путь $\gamma_{class}$ - классическая траектория. Эта траектория выделяется из множества всех других тем, что она удовлетворяет принципу нулевой вариации действия Мопертьюи:

$$\delta S[\gamma_{class}]/\delta\gamma = 0, \tag{18}$$

который ошибочно называют принципом наименьшего действия (действие там отнюдь не наименьшее, его вариация при вариации траектории нулевая). Действительно, рассмотрим Лагранжиан:

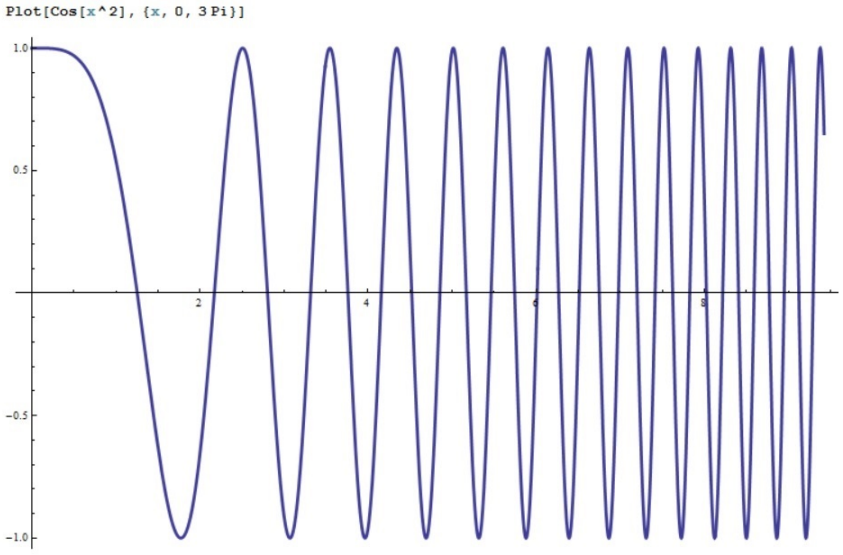
$$L(\dot{x},x,t) = m\dot{x}^2/2 - V,\ S[\gamma] = \int\limits_0^T L(\dot{x},x,t)dt,\ \gamma :\ x = x(t),\ 0 \le t \le T$$

и придадим приращение $\delta x$ координате. Тогда $x \to x + \delta x,\ \dot{x} \to \dot{x} + \delta\dot{x}$, и мы будем иметь

$$\delta S[\gamma]/\delta\gamma = \int\limits_0^T L(\dot{x}+\delta\dot{x}, x+\delta x, t)dt - \int\limits_0^T L(\dot{x},s,t)dt =$$
$$\int\limits_0^T \left(\frac{\partial L}{\partial\dot{x}}\delta\dot{x} + \frac{\partial L}{\partial x}\delta x\right)dt = \int\limits_0^T \frac{\partial L}{\partial\dot{x}}d\delta x + \int\limits_0^T \frac{\partial L}{\partial x}\delta x dt =$$
$$\frac{\partial L}{\partial\dot{x}}\delta x\Big|_0^T - \int\limits_0^T \frac{d}{dt}\frac{\partial L}{\partial\dot{x}}\delta x dt + \int\limits_0^T \frac{\partial L}{\partial x}\delta x dt = 0 \equiv$$
$$\frac{\partial L}{\partial x} = \frac{d}{dt}\frac{\partial L}{\partial\dot{x}} \equiv -\frac{\partial V}{\partial x} = m\ddot{x} \equiv F = ma.$$

Допустим, мы моделируем какой-либо процесс, выбирая шаг по времени $dt$. Если этот процесс можно адекватно представить, выбрав такое $dt$, при котором изменение действия $dS$ будет намного больше постоянной Планка $\hbar \approx 10^{-27}$ ерг сек., то в

Рис. 11: Вещественная часть ядра Фейнмана свободной частицы.



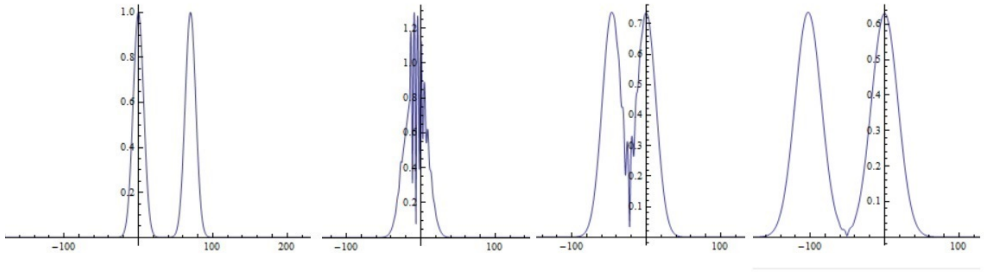

формуле (17) "выживут" только те траектории, которые близки к $\gamma_{class}$, потому что действие по порядку величины сравнимо с его вариацией, так что для окружения (окружение - это семейство траекторий, близких к) неклассической траектории, окажется очень малым из-за быстрой осцилляции экспоненты и вытекающего из этого деструктивного характера интерференции - сумма будет содержать львиную долю сокращений и окажется гораздо меньше вклада окружения классической траектории.

Если же для адекватного описания процесса необходимо взять такой малый шаг по времени $dt$, что изменение действия на нем $dS$ будет сравнимо с $\hbar$, придется учитывать и неклассические траектории. Мы можем описывать полет пули с помощью квантовой механики, и тогда на малом $dt$ пуля будет вести себя как квантовый объект; точность конечного результата будет такой же, как и при классическом подходе, но вычислительные сложности сделают такой путь неразумным. Иное дело - движение электрона в атоме - здесь надо сделать $dt$ очень малым, так что пренебречь неклассическими траекториями уже будет невозможно.

Итак, мы здесь опираемся на возможность простого отбрасывания очень малых амплитуд - мощный эвристический подход, который в дальнейшем снова приведет нас к необходимости некоего детерминизма, но уже не сводимого к ньютоновской механике - пост-квантового детерминизма для сложных систем.

Попробуем с помощью фейнмановских интегралов по траекториям выяснить, как будет выглядеть состояние свободной точечной частицы, движущейся вдоль оси $OX$, в момент $t > 0$, если в нулевой момент она находилась в начале координат. Мы предположим, что траектории экземпляров этой частицы при малом $t$ являются отрезками прямой, причем скорость ее движения вдоль этих отрезков постоянна. Тогда на отрезке длины $x$ скорость будет равна $x/t$, и подставляя в выражение для лагранжиана данное значение скорости, мы получим ядро Фейнмана в виде $a\ exp(\frac{imx^2}{2ht})$, где $a$ константа. График вещественной части данной функции изображен на рисунке 11.

Рис. 12: Столкновение двух гауссианов; хаос при столкновении сменяется восстановлением вида гауссианов в дальнейшем; программный код из Математики



```
NDSolve[{ I D[u[t, x], t] == -D[u[t, x], x, x],
  u[0, x] == Exp[-0.01 x^2] + Exp[-0.01 (x - 70)^2 - I 1.5 x], u[t, -250] == u[t, 250]},
 u, {t, 0, 60}, {x, -250, 250}]
{{u → InterpolatingFunction[{{0., 60.}, {-250., 250.}}, <>]}}

Animate[Plot[Evaluate[Abs[u[t, x]] /. %], {x, -250, 250}, PlotRange → All], {t, 0, 60},
 AnimationRunning → False]
```

*Покажите, что это состояние согласуется с волной де Бройля*

$$exp\left(\frac{ipx}{\hbar} - \frac{iEt}{\hbar}\right)$$

*в следующем смысле: экземпляры частицы, достигшие точки $x$ за время $t$, будут иметь тот же период осцилляций по де-Бройлю, что и по Фейнману в 11.*

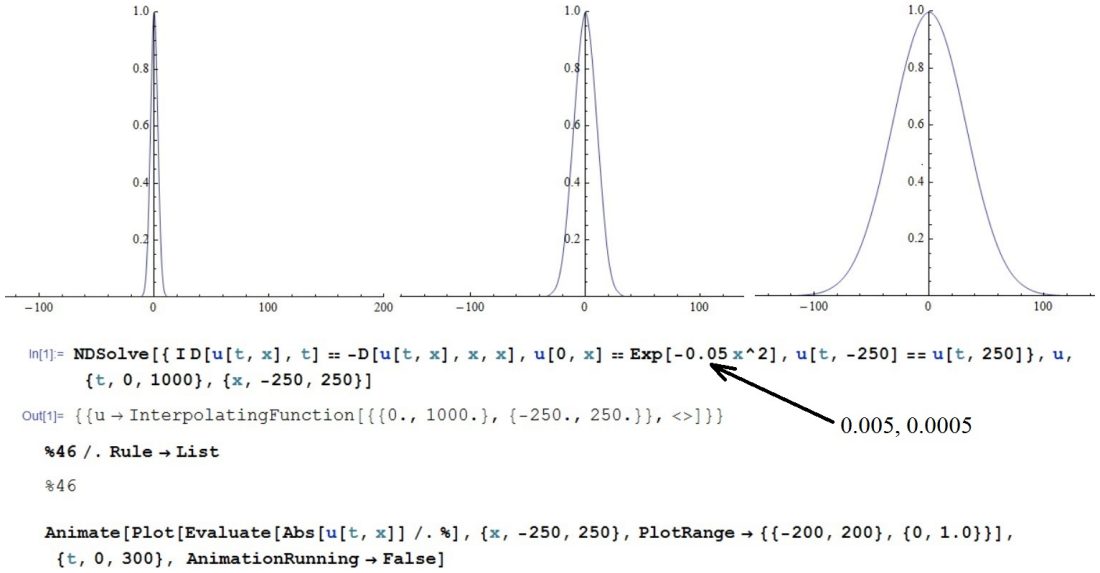
Для свободной частицы очень существенно наличие экземпляров, обладающих разными скоростями, причем распределение по всем скоростям должно быть равномерным, так что любая скорость в виртуальном рое экземпляров должна быть представлена одинаковым числом экземпляров.

Динамику свободной частицы нельзя заменить простыми перемещениями от одной точки к соседней на множестве точек вида $x = \epsilon, 2\epsilon, 3\epsilon, ...$, так как свободная частица обладает способностью "прыгать" сразу через много точек. Эта особенность должна учитываться при моделировании свободного движения в терминах перемещений фотона между оптическими полостями, что разбирается во второй главе.

## 1.5 Упражнения

1. Объяснить эффект восстановления формы частей волновой функции - гауссианов при их "столкновении"(рисунок 12).

Рис. 13: Расплывание гауссианов с первоначальной разной дисперсией; код из Математики

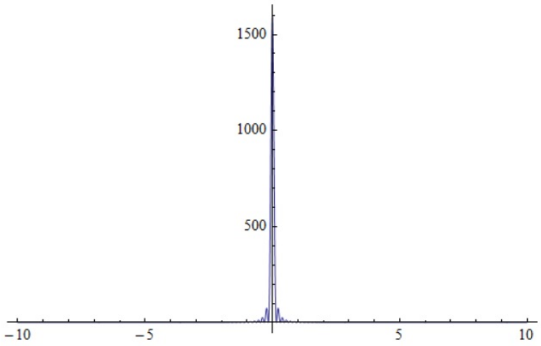



2. Объяснить эффект разной скорости расплывания волнового пакета в виде гамильтониана с разной степенью дисперсии. Нет ли здесь противоречия с теоремой о существовании и единственности решения задачи Коши для уравнения Шредингера? (см. рисунок 13 ). Скорость расплывания сильно уменьшается от левого рисунка к правому.

Рис. 14: Приближение Дельта-функции Дирака, с ограничением пространственного сегмента; аргумент $p$

```
A = 20;
R[x_] := (Exp[I * x * A] - Exp[-I * x * A]) /
   (I * x);

Plot[Abs[R[x]]^2, {x, -10, 10},
 PlotRange → All]
```




3. Вычислить приближение дельта - функции Дирака в виде

$$\phi(p) = \mathcal{F}e^{\frac{i}{\hbar}p_0 x} = \int_{-A}^{A} e^{\frac{i}{\hbar}p_0 x} e^{-\frac{i}{\hbar}px} dx$$

(см. рисунок 14).

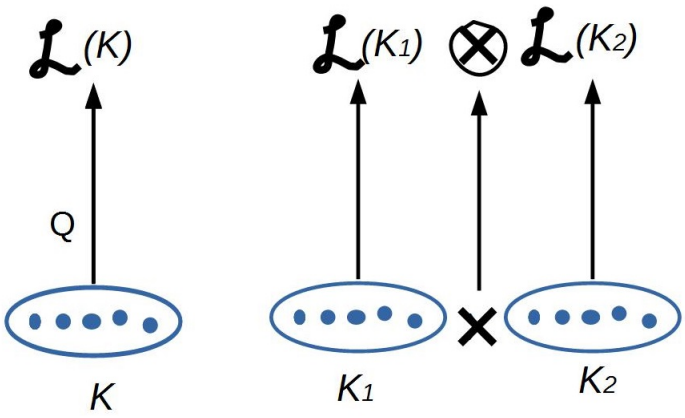



Рис. 15: Тензорное произведение - результат подъема декартова с помощью операции квантовая $Q$ - взятия линейной оболочки

# 2 Лекция 2. Композитные системы

### 2.0.1 Тензорные произведения

Простейший гейт, реализующий унитарную операцию $\sigma_x$, мы уже получили: надо создать квантовую точку, эволюция которой подчиняется гамильтониану $\sigma_x$, и подождать время $t = 2\pi\hbar$. Такая точка - заряд в двухъямном потенциале.

Но для полноценных квантовых вычислений нам нужны более сложные гейты, двух-кубитные. Для этого надо ввести понятие тензорного произведения.

Пусть у нас есть два множества (два регистра) кубитов: $A$ и $B$ по $n_A$ и $n_B$ кубитов в каждом. Множества классических состояний этих регистров: $K_A = \{0, 1, ..., N_A - 1\}$ и $K_B = \{0, 1, ..., N_B - 1\}$ соответственно, где $N_A = 2^{n_A}, N_B = 2^{n_B}$. Пространство квантовых состояний для регистра $A$ - это $L_A = C^{N_A}$, для регистра $B$ - $L_B = C^{N_B}$. Тензорным произведением $L_A \otimes L_B$ пространств $L_A$ и $L_B$ называется пространство состояний композитной системы кубитов $A \cup B$ - $C^N$, где $N = 2^n,\ n = n_A + n_B$. Его ортонормированным базисом будет декартово произведение $K_A \times K_B$ (см. рисунок 15).

Общий вид вектора из тензорного произведения пространств будет таким:

$$|\Psi\rangle = \sum_{j\in\{0,1,...,N_A-1\},k\in\{0,1,...,N_B-1\}} \lambda_{j,k}|jk\rangle \tag{19}$$

Пусть $|\Psi_A\rangle = \sum\limits_{a=0}^{N_A-1} \lambda_a|a\rangle$ и $|\Psi_B\rangle = \sum\limits_{b=0}^{N_B-1} \lambda_b|b\rangle$ - квантовые состояния регистров $A$ и $B$. Определим их тензорное произведение как $|\Psi_A\rangle\otimes|\Psi_B\rangle = |\Psi_A\rangle|\Psi_B\rangle = \sum\limits_{a\in K_A, b\in K_b} \lambda_a\lambda_b|a\rangle|b\rangle$. Будем опускать кет-бра и писать просто $|ab\rangle$. Тензорное произведение подчиняется тем же правилам, что и обычное, можно также выносить за скобки.

Состояние композитной системы, которое нельзя представить как тензорное произведение $|\Psi_A\rangle|\Psi_B\rangle$, называется запутанным. Пример такого состояния - ЭПР пара:

$|00\rangle + |11\rangle$.

*Докажите, что это состояние не представимо в виде тензорного произведения состояний одного и второго кубита.*

*Попробуйте формализовать вопрос и ответить на него: "Каких состояний больше: запутанных или не запутанных?"*

Пусть $U_A : \ L_A \to L_A$, $U_B : \ L_B \to L_B$ - два линейных оператора на пространствах квантовых состояний этих регистров. Тензорное произведение этих операторов $U_A \otimes U_B$ определим для базисных векторов так: $U_A \otimes U_B |ab\rangle = U_A|a\rangle \ \otimes U_B|b\rangle$, а на все пространство распространим по линейности. Правило нахождения матрицы тензорного произведения для однокубитных пространств проиллюстрируем на примере:

$$U_A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, U_B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}, U_A \otimes U_B = \begin{pmatrix} a_{11}U_B & a_{12}U_B \\ a_{21}U_B & a_{22}U_B \end{pmatrix},$$

обобщение этого правила на более высокие размерности очевидно. Матрица тензорного произведения будет иметь размерность, равную произведению размерностей исходных матриц. Докажите это, используя стандартные обозначения базисных векторов в виде столбцов, и переходя к дираковским обозначениям. Используйте естественное упорядочение на базисных вектора из тензорного произведения: для одного кубита $|0\rangle$, $|1\rangle$, для двух кубитов $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$. На пространства большей размерности обобщение очевидно.

Предлагается доказать следующие формулы:

$$e^{A\otimes I} = e^A \otimes I, (A \otimes I) \cdot (I \otimes B) = A \otimes B, e^{A\otimes I} \cdot e^{I\otimes B} = e^{(A\otimes I)+(I\otimes B)}, [(A \otimes I), (I \otimes B)] = 0,$$

где $\cdot$ обозначает обычное матричное произведение, $I$ - идентичную матрицу.

## 2.1 Частичные измерения. Смешанные состояния

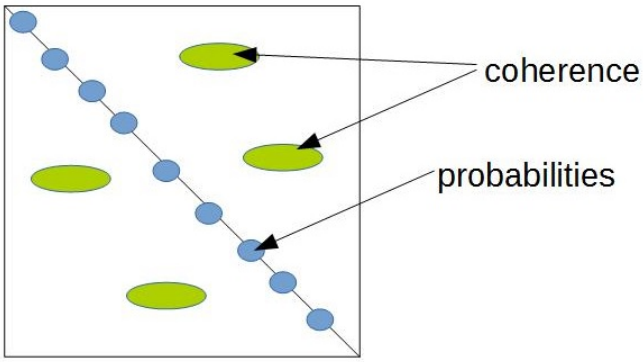



Рис. 16: Матрица плотности.

Для многочастичных систем возникает новый вопрос о частичном измерении. Если у нас имеется две частицы, например, два кубита, мы можем измерить только один

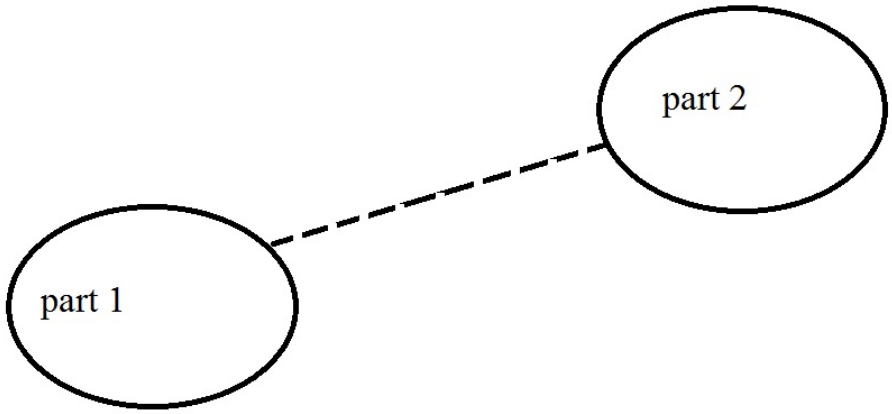



Рис. 17: Двухчастичная запутанность.

из них, оставив второй не затронутым. В каком состоянии тогда окажется незатронутый измерением кубит? Для решения этого вопроса обратимся к алгебраической форме результата измерения.

Сначала рассмотрим случай одного кубита и определенного выше измерения его состояния $|\Psi\rangle$ как случайной величины. Из правила матричного умножения сразу вытекает равенство

$$p_j = \langle j|\rho_\Psi|j\rangle$$

След матрицы плотности будет находиться по формуле $tr(\rho_\Psi) = \sum_j \langle j|\rho_\Psi|j\rangle$ и для одного кубита эта сумма будет равна 1. Мы видим, что конфигурация вида $\langle a|b\rangle$ всегда дает число, причем если $a$ и $b$ - векторы из ортонормированного базиса состояний одного кубита, это число равно $\delta_{ab}$ - символ Кронекера, равный нулю при $a \neq b$ и единице при $a = b$. Это наблюдение позволяет обобщить правило работы с дираковскими символами на тензорные произведения, если мы примем, что в этом случае $a$ и $b$ должны относиться к одной и той же реальной частице.

Рассмотрим матрицу плотности композитной системы вида

$$\rho = \sum_{j',j'',k',k''} \rho_{j',k',j'',k''}|j',j''\rangle\langle k',k''| \tag{20}$$

где один штрих обозначает первую подсистему, а два штриха - вторую.

Допустим, например, что мы измеряем первый кубит и получили значение $|j\rangle$. В каком тогда состоянии будет находиться второй кубит? Нам надо получить матрицу плотности $\rho_2$ второго кубита так же, как мы получали вероятность в случае, когда у нас был только один кубит: обкладывая исходную матрицу плотности слева и справа. Только теперь обкладывать надо только состоянием первого кубита, равным $|j\rangle$. Принимая во внимание ортонормированность всех состояний, относящихся к одной и той же подсистеме, мы имеем:

$$\rho_2^j = \sum_{j',j''k',k''} \rho_{j',k',j'',k''} \langle j|j'\rangle |j''\rangle\langle k'|\langle k''|j\rangle = \rho_{j,j,j'',k''} |j''\rangle\langle k''|$$

Заметим, что след такой матрицы не обязан быть единичным, так как мы априори выделили результат измерения первого кубита $|j\rangle$.

Суммируя по $j$, мы получаем

$$\rho_2 = \sum_{j'',k''} r_{j''k''} |j''\rangle\langle k''|, \quad r_{j''k''} = \sum_j \rho_{jjj''k''} \tag{21}$$

Формула (21) дает простое мнемоническое правило для определения результата частичного измерения: для получения элемента $\rho_2(j'', k'')$ матрицы плотности первого кубита надо просуммировать все элементы матрицы плотности обоих кубитов с номерами, полученными всевозможными одинаковыми дополнениями пары $j'', k''$ до пары индексов двух-кубитной матрицы плотности.

Однако матрица $\rho_2$, полученная по формуле (21), вообще говоря, уже не будет иметь вида $|\psi\rangle\langle\psi|$ ни для какого состояния $|\psi\rangle$ первого кубита. Что убедиться в этом, рассмотрим пример: $|\Psi\rangle = |EPR\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

Матрица плотности состояния $|EPR\rangle$ суть

$$\begin{pmatrix} 1/2 & 0 & 0 & 1/2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1/2 & 0 & 0 & 1/2 \end{pmatrix} \tag{22}$$

Слушателю предлагается убедиться в том, что измерение второго кубита в этом состоянии дает матрицу

$$\begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix} \tag{23}$$

Матрица (23) имеет ранг 2, и потому она не может быть матрицей плотности никакого квантового вектора состояния. Мы, таким образом, приходим к необходимости расширить понятие состояния. Вектора-состояния мы будет называть чистыми, а "состояния", которые описываются матрицами, сходными с (23), мы будем называть смешанными - см. Рисунок 18.

Итак, смешанное состояние есть результат измерения одной части какого-либо вектора- состояния композитной системы. Допустим, вектор-состояние композитной двухкубитной системы имеет вид:

$$|\Psi\rangle = \lambda_{00}|00\rangle + \lambda_{01}|01\rangle + \lambda_{10}|10\rangle + \lambda_{11}|11\rangle.$$

Если мы измеряем только второй кубит, то результат такого измерения должен быть либо $|0\rangle$, либо $|1\rangle$. С какой вероятностью $p_2(0)$ получится $|0\rangle$ для второго кубита? Эта вероятность, по логике измерения, должна быть равна $p_2(0) = \sum\limits_j |\lambda_{j0}|^2$. Аналогично, вероятность получить во втором кубите $|1\rangle$ будет $p_2(1) = \sum\limits_j |\lambda_{j1}|^2$. Суммарная

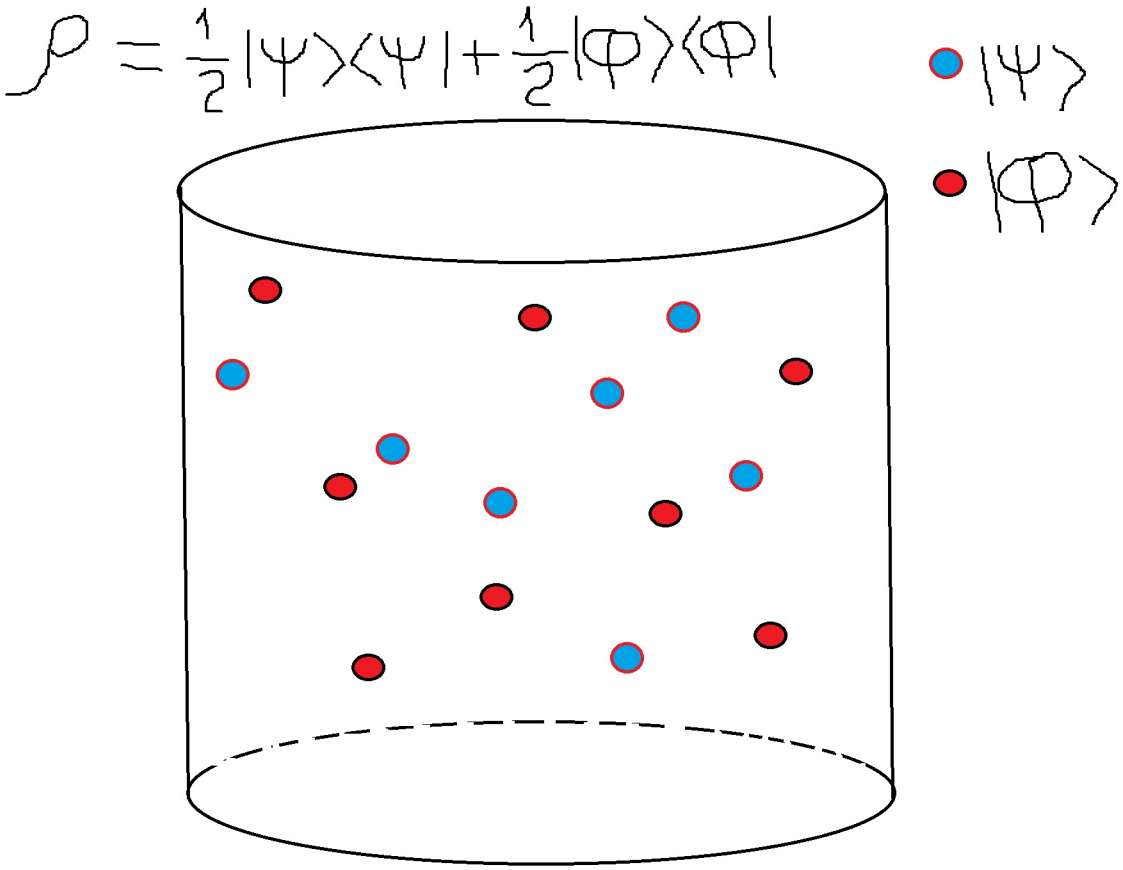



Рис. 18: Смешанное состояние - это резервуар с чистыми состояниями.

вероятность будет, конечно, единичной. Если получится во втором кубите $|0\rangle$, то в первом, незатронутом измерением непосредственно, должно получиться состояние $|\psi_0\rangle = a_0 \sum\limits_j \lambda_{j0}|j\rangle$, где нормировочный коэффициент $a_0 = (\sum\limits_j |\lambda_{j0}|^2)^{-1/2}$. Аналогично, если во втором кубите получилось состояние $|1\rangle$, то первый кубит окажется в состоянии $|\psi_1\rangle = a_1 \sum\limits_j \lambda_{j1}|j\rangle$, где нормировочный коэффициент $a_1 = (\sum\limits_j |\lambda_{j1}|^2)^{-1/2}$.

Поскольку в общем случае $|\psi_1\rangle$ не совпадает с $|\psi_0\rangle$, мы не можем суммировать эти состояния как вектора в гильбертовых пространствах. Но можно суммировать их матрицы плотности, вводя для каждой из них свой весовой коэффициент: $p_2(0)$ или $p_2(1)$. в итоге получим матрицу "плотности" вида

$$\rho_1 = p_2(0)|\psi_0\rangle\langle\psi_0| + p_2(1)|\psi_1\rangle\langle\psi_1|. \tag{24}$$

Слушателю предлагается убедиться, что это в точности совпадает с матрицей (21).

Таким образом, и в общем случае, когда система разделена на две подсистемы, матрица "плотности" результата измерения второй подсистемы, найденная по формуле (21), будет иметь вид

$$\rho_1 = \sum_k p_k|\psi_k\rangle\langle\psi_k|, \tag{25}$$

где $|\psi_k\rangle$ - вектора состояния первой подсистемы, полученные в результате измерения

второй подсистемы при условии, что результат этого измерения для второй подсистемы оказался равным $|k\rangle$.

Формула (25) задает общий вид смешанного состояния, которое мы будем отождествлять с матрицей плотности $\rho_1$. Однако по заданной матрице плотности $\rho_1$ разложение (25) определено не однозначно. Дело в том, что система, находящаяся в чистом состоянии $|\Psi\rangle$ может также с вероятностью $|\langle\Psi|\Phi\rangle|^2$ находиться также и в другом чистом состоянии $|\Phi\rangle$.

Смешанное состояние означает, что система находится в каком-то чистом состоянии, но мы не знаем, в каком именно. Поэтому если все чистые состояния $|\psi_k\rangle$ в (25) взаимно ортогональны, между ними нет когерентности, и в этом случае данное разложение определено однозначно.

Возникает естественный вопрос: как физически отличить ЭПР- пару $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ от смеси вида $\frac{1}{2}|00\rangle\langle 00| + \frac{1}{2}|11\rangle\langle 11|$? Измерения в стандартном базисе, как мы видели, не позволяют этого сделать. Но если изменить базисы измерения, это скажется на диагонали матрицы плотности, и мы сможем различить ЭПР- пару от смеси. Слушателю предлагается рассмотреть все детали самостоятельно.

В каком случае частичное измерение одного кубита в каком-либо чистом состоянии двухкубитной системы дает в результате не смешанное, а чистое состояние? *Докажите, что это происходит в том и только в том случае, когда исходное состояние является незапутанным.*

Пусть $M$ - множество кубитов рассматриваемой системы, состоящее из $n$ кубитов, а $|\Psi\rangle$ - какое-либо квантовое состояние этих кубитов. Оно называется незапутанным, если существует такое разбиение $M = M_1 \cup M_2$ на два непересекающихся непустых множества и состояния $|\Psi_1\rangle$, $|\Psi_2\rangle$ на этих множествах, такие что $|\Psi\rangle = |\Psi_1\rangle \otimes |\Psi_2\rangle$. В противном случае состояние $|\Psi\rangle$ называется запутанным.

*Наивной сложностью* состояния $|\Psi\rangle$ на множестве $M$ называется размер в кубитах носителя его максимального запутанного тензорного делителя. Иначе говоря, наивная сложность состояния есть максимальное из натуральных чисел $s$, таких что существует подмножество $M_1 \subseteq M$ и состояния $|\Psi_1\rangle$, $|\Psi_2\rangle$ на $M_1$ и $M - M_1$ соответственно, такие что $|\Psi\rangle = |\Psi_1\rangle \otimes |\Psi_2\rangle$, $M_1$ содержит $s$ элементов и $|\Psi_1\rangle$ является запутанным. Такое состояние $|\Psi_1\rangle$ называется квантовым ядром состояния $|\Psi\rangle$, а соответствующее ему множество $M_1$ - носителем ядра.

Ядер может быть несколько, так как максимальное число $s$ из определения может соответствовать разным наборам $M_1$ кубитов. Естественно, данное определение может зависеть от очень малых амплитуд, так что сложное состояние может оказаться очень близко к простому. Однако если мы рассматриваем только состояния, амплитуды $\lambda_j$ которых имеют "зернистый" вид

$$\lambda_j = \epsilon n_j + i\epsilon m_j, \quad n_j, m_j \in Z,$$

эта близость будет ограничена величиной зерна $\epsilon$. Из дальнейшего будет ясно, что устремлять $\epsilon$ к нулю для сложных систем нельзя, и потому наивная сложность определена таким образом корректно. Данный вид сложности зависит от базиса, в котором мы рассматриваем состояния.

## 2.2 Теорема Шмидта

Запутанное состояние в композитной системе, состоящей из двух компонент $S_1$ и $S_2$, имеет вид (26) и непредставимо в виде тензорного произведения.

$$|\Psi\rangle = \sum_{j=0,...,N-1,k=0,...,M-1} \lambda_{jk}|j_1 k_2\rangle \tag{26}$$

Его хранение в памяти компьютера весьма затратно: надо хранить матрицу $\lambda_{jk}$ в отличие от состояния (27),

$$|\Psi\rangle \otimes |\Phi\rangle = \sum_{j=0}^{N-1} \lambda_j |j\rangle \otimes \sum_{k=0}^{M-1} \mu_k |k\rangle = \sum_{j=0,...,N-1;k=0,...,M-1} \lambda_j \mu_k |jk\rangle \tag{27}$$

где надо хранить в памяти всего лишь два вектора. Оказывается, есть возможность более экономичного представления запутанности, однако это представление годится лишь для данного фиксированного состояния, так как это требует изменения базиса в обоих пространствах - специально для данного фиксированного $|\Psi\rangle \in C^N \otimes C^M$.

А именно, имеет место следующая

**Теорема (Шмидт).** *Для любого состояния $|\Psi\rangle$ вида (26) композитной системы существуют новые ортонормированные базисы $|J_0\rangle, |J_1\rangle, ..., |J_{N-1}\rangle$; $|K_0\rangle, |K_1\rangle, ..., |K_{M-1}\rangle$ в пространствах - компонентах $C^N$, $C^M$, такие что*

$$|\Psi\rangle = \sum_{q=0}^{S} \alpha_q |J_q\rangle |K_q\rangle \tag{28}$$

*где $S = min(N-1, M-1)$, а $\alpha_q$ - неотрицательные вещественные числа, такие что $\sum\limits_{q=0}^{S} |\alpha_q|^2 = 1$.*

Доказательство этой теоремы проводится индукцией по $max(N, M)$. Пусть $|\Psi\rangle = |\Psi_1\rangle|\Psi_2\rangle$ - незапутанное состояние. Тогда теорема выполнена очевидным образом. Разберем случай, когда $|\Psi\rangle$ - запутанное состояние.

Множество незапутанных состояний $\mathcal{N}$- замкнуто как подмножество евклидова пространства. Действительно, если $|\psi_1^n\rangle|\psi_2^n\rangle \to |\Psi\rangle$, то последовательности $|\psi_1^n\rangle$ и $|\psi_2^n\rangle$ имеют пределы $|\psi_1\rangle$ и $|\psi_2\rangle$ соответственно, и мы будем иметь $|\psi_1^n\rangle|\psi_2^n\rangle \to |\psi_1\rangle|\psi_2\rangle$ при $n \to \infty$.

Значит, существует точка в $\mathcal{N}$, расстояние от которой до конца вектора $|\Psi\rangle$ минимально, пусть это конец ненормированного вектора $|\Phi_0\rangle$: $|\Psi\rangle = |\Phi_0\rangle + |A\rangle$, так что $\|A\|$ есть расстояние от $|\Psi\rangle$ до $\mathcal{N}$. Поскольку $|\Phi_0\rangle \in \mathcal{N}$, мы имеем $|\Phi_0\rangle = |J_0\rangle|K_0\rangle$ для каких-то векторов $|J_0\rangle \in C^N$, $|K_0\rangle \in C^M$; эти векторы мы и возьмем в качестве

начальных векторов в разложении (28). Нам надо доказать, что в разложении $|A\rangle$ не присутствуют ни один из этих векторов, тогда будет сделан шаг индукции, так как с $|A\rangle$ мы потом поступим так же, как и с $|\Psi\rangle$. Если бы в разложени $|A\rangle$ присутствовал один из векторов $|J_0\rangle$, $|K_0\rangle$, мы бы получили противоречие с минимальностью вектора $|A\rangle$, потому что можно было бы "отщепить" от него еще немного, что невозможно в силу выбора $|A\rangle$. Детали предоставляются слушателю.

Теорема Шмидта дает численную характеристику меры запутанности композитного состояния $|\Psi\rangle \in C^N \otimes C^M$ как энтропии вероятностного распределения $|\alpha_q|^2$. Энтропия распределения вероятностей $\bar{p}$ определяется как $E(\bar{p}) = -\sum\limits_i ln(p_i)p_i$.

У этой Теоремы есть и другое полезное следствие - существование так называемого $SVD$- разложения произвольной матрицы $A$ в виде $SAV = D$, где $S$, $V$- унитарные матрицы, а $D$- диагональная. Это разложение обобщает теорему о приведении к диагональному виду эрмитовых и унитарных матриц; только здесь матрица $A$ - произвольная, даже не обязательно квадратная, а $S$ и $V$ никак не связаны, могут даже иметь разные размерности. Это следствие сразу получается, если представить матрицу $A$ как набор коэффициентов $\lambda_{jk}$ из разложения (26) состояния композитной системы; тогда $S$ и $V$ будут матрицами перехода к базисам $|J_i\rangle$ и $|K_j\rangle$ в условии Теоремы.

Что если в нашем распоряжении есть только одна из двух компонент композитной системы, например, $S_1$, а другая $S_2$ находится вне доступа? В этом случае у нас имеется, фактически, только матрица плотности $\rho_1$ первой подсистемы, так что мы даже не знаем о существовании второй компоненты. Можно ли в этом случае "восстановить" чистое состояние $|\Psi\rangle$, такое что $\rho_1 = tr_2(|\Psi\rangle\langle\Psi|)$?

Да, это можно сделать, и очень просто. Пусть $C^N$- пространство квантовых состояний подсистемы $S_1$ Возьмем еще один экземпляр $S_1$, который обозначим через $S_1'$, и соответствующее ему пространство квантовых состояний $C^N$, вектора которого будем обозначать теми же буквами, что и для $S_1$, что не вызовет недоразумений, так как мы в тензорном произведении всегда пишем состояний $S_1$ первым, а $S_1'$ вторым. Взяв собственные числа $A_i$ матрицы $\rho_1$ и соответствующие им собственные вектора $|\phi_i\rangle$, положим $\alpha_i = \sqrt{A}_i$, и определим $|\Psi\rangle \in C^N \otimes C^N$ как $\sum\limits_{i=0}^{N-1} \alpha_i|\phi_i\rangle|\phi_i\rangle$. Тогда из правила нахождения относительной матрицы плотности (21) мы получаем $\rho_1 = tr_2(|\Psi\rangle\langle\Psi|)$.

Из этого наблюдения следует и способ нахождения матриц $S$ и $V$ в $SVD$ - разложении. Надо превратить матрицу $A$ в состояние $|\Psi\rangle$ композитной системы, взяв в разложении (26) ее коэффициенты, затем найти ее матрицу плотности $\rho_\Psi = |\Psi\rangle\langle\Psi|$, относительные матрицы плотности $\rho_2 = tr_1(\rho_\Psi)$ и $\rho_1 = tr_2(\rho_\Psi)$, у которых будут одинаковые наборы собственных значений, совпадающие с числами $|\alpha_i|^2$ в разложении Шмидта для $|\Psi\rangle$, после чего искать разложение Шмидта состояния $|\Psi\rangle$, выбирая в качестве $|J_i\rangle$, $|K_i\rangle$ собственные вектора операторов $\rho_1$ и $\rho_2$.

## 2.3 Парадокс квантовой энтропии

Что такое порядок в сложной системе? Порядок - это альтернатива хаосу. Если система классическая, и $\bar{p} = (p_0, p_1, ..., p_{N-1})$ - список вероятностей нахождения этой системы в классических состояниях $x_0, x_1, ..., x_{N-1}$, то степень хаоса есть энтропия Шеннона

$$Sh(\bar{p}) = -\sum_{i=0}^{N-1} p_i \; ln(p_i),$$

(см. Приложение). При добавлении в систему новых элементов классическая энтропия $Sh(\bar{p})$ может только увеличиться, следовательно, порядок возрасти не может.

Как обобщить энтропию Шеннона на случай квантовой системы? Естественным обобщением является энтропия фон Неймана

$$N(\rho) = -tr(\rho \; ln(\rho)),$$

где $\rho$ - матрица плотности, которая в квантовом случае заменяет распределение вероятностей $\bar{p}$.

Рассмотрим состояние двух кубитов $|\Psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Его энтропия равна нулю. Действительно, энтропия вообще любого чистого состояния равна нулю. *Докажите это, приведя матрицу $\rho$ к диагональному виду и показав, что энтропия состояния вида $|j\rangle\langle j|$, где $|j\rangle$ - один из базисных векторов, равна нулю.*

Предположим, что мы удалили второй кубит на большое расстояние, так что в наших руках остался только первый кубит. Тогда этот кубит будет находиться в смешанном состоянии $\rho_1 = tr_2(|\Psi\rangle\langle\Psi|)$, и $N(\rho_1) = ln(2) > 0$. То есть при добавлении второго кубита энтропия квантового состояния уменьшится.

Эффект возрастания порядка при расширении системы - контринтуитивный, чисто квантовый эффект. Он происходит из-за наличия запутанности, которая связывает различные физические части системы многих тел.

# 3 Лекция 3. Квантовые гейты

Пользовательский интерфейс квантового компьютера по Фейнману основан на квантовых гейтах и массивах из них (quantum gate arrays). Квантовый гейт - это унитарный оператор, действующий в пространстве состояний одного, двух или трех кубитов, который можно реализовать физически. Если взять все однокубитовые гейты и добавить к ним почти любой двух-кубитовый, например, гейт
CNOT: $|x, y\rangle \to |x, y \oplus x\rangle$, можно получить полную систему гейтов: через гейты из этого набора можно выразить любое унитарное преобразование с любой, наперед заданной точностью (см. [9])[1].

[1]На комбинациях гейтов можно построить огромное разнообразие интересных операторов. Слушатель, любящий алгебраические упражнения, может обратиться к книге [10], содержащей много интересных задач на квантовые вычисления.

Рис. 19: R.Feynman

Таким образом, первая задача реализации фейнмановской схемы квантовых вычислений: реализация однокубитных гейтов и CNOT. Рассмотрим гейт CiNOT, близкий к CNOT: $CiNOT|x,y\rangle = e^{i\pi x/2}CNOT|x,y\rangle$. Мы покажем, как реализовать однокубитный гейт $iNOT : |x\rangle \rightarrow i|x \oplus 1\rangle$ и квантовый гейт CiNOT на зарядовых состояниях электронов в квантовых точках. Имея однокубитные гейты и CiNOT, можно реализовать и CNOT, так как он получается из CiNOT применением к первому кубиту однокубитного относительного вращения фазы $e^{-i\pi x/2}$. Данная реализация CNOT - одно из первых предложений реализации запутывающих гейтов на зарядовых состояниях (см. [11]), ее схема наиболее проста, хотя представляет определенные технологические трудности.

Уравнение Шредингера в непрерывной форме для одномерной квантовой частицы имеет вид

$$i\hbar\dot{\Psi} = H\Psi,\ H = \frac{p^2}{2m} + V,\ p = \frac{\hbar}{i}\frac{\partial}{\partial x},$$

где $V = V(x)$ - потенциал, в котором движется частица.

Потенциальная яма бесконечной глубины есть простейшая форма квантовой точки. Задача Коши для такой ямы выглядит так:

$$i\hbar\dot{\Psi} = -\frac{\hbar^2}{2m}\frac{\partial^2\Psi}{\partial^2 x} + V\Psi.\ \Psi(t,0) = \Psi(t,L) = 0, \Psi(0,x) = \Psi_0(x),\ x \in [0,L] \qquad (29)$$

Собственные функции такой системы - решения уравнения $H\phi_n = E_n\phi_n$ с краевыми условиями, взятыми из (29), выглядят так: $\phi_n = c_n\ sin(\pi x n/L)$, где $c_n$ есть нормирующий коэффициент, который можно найти из условия равенства единице полной вероятности: $\int\limits_0^L |\phi_n(x)|^2 dx = 1$.

Введем понятие квантовой точки. Это малая область в твердотельной структуре, в которой создан потенциал в виде двух ям с достаточно высоким потенциальным барьером между ними, причем в этом потенциале может находиться один электрон (см. рисунок 20).

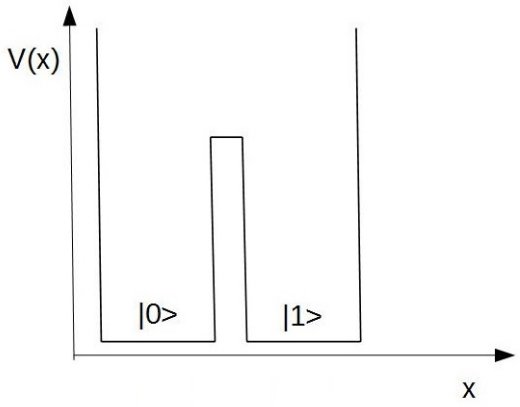



Рис. 20: Квантовая точка в виде двух-ямного потенциала

Нахождение электрона в правой яме означает состояние $|0\rangle$, в левой $|1\rangle$.

Неклассическое поведение частицы в системе ассиметричных потенциальных ям показано на рисунке 21.

Гамильтониан такой системы имеет вид $H = c_1 I - b\sigma_x$, где $\sigma_x$ - определенная в (9) первая матрица Паули, $b > 0$. Слушателю предоставляется показать, что собственными состояниями этого гамильтониана будут

$$|\phi_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |\phi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \tag{30}$$

причем их собственные значения упорядочены так, что $E_0 < E_1$, так что $|\phi_0\rangle$ будет основным, а $|\phi_1\rangle$ - возбужденным состоянием. Мы находим решение задачи Коши для уравнения Шредингера с таким гамильтонианом в виде

$$|\Psi(t)\rangle = A_0 e^{-\frac{iE_0 t}{\hbar}}|\phi_0\rangle + A_1 e^{-\frac{iE_1 t}{\hbar}}|\phi_1\rangle = e^{-\frac{iE_0 t}{\hbar}}(A_0|\phi_0\rangle + e^{-\frac{i(E_1-E_0)t}{\hbar}}A_1|\phi_1\rangle) \tag{31}$$

и теперь, учитывая что состояния $e^{i\theta}|\Psi\rangle$ физически неразличимы для любого вектора $|\Psi\rangle$, мы приходим к выводу, что для реализации гейта NOT: $|0\rangle \to |1\rangle$, $|1\rangle \to |0\rangle$ достаточно просто подождать время $\frac{1}{2}\tau = \pi\hbar/(E_1 - E_0)$.

Из формулы (100) следует, что базисные состояния электрона в квантовой точке осциллируют, то есть переходят одно в другое $|0\rangle \to |1\rangle \to |0\rangle$ и $|1\rangle \to |0\rangle \to |1\rangle$ с периодом $\tau = 2\pi\hbar/(E_1 - E_0)$, который мы назовем периодом осцилляций.

*Здесь мы игнорировали фазовый множитель $e^{-\frac{iE_0 t}{\hbar}}$, который не имеет физического смысла, если оператор NOT совершается для любых состояний. Но предположим, что NOT совершается условно, например, только если какой-либо другой кубит имеет значение 1, а если его значение 0, то NOT над $x$ не совершается. В этом случае надо учитывать общий набег фазы, и учитывать данный множитель. Найдите $E_0$ и $E_1$ и напишите точное выражение для оператора, реализуемого данной подпрограммой при $x = 1$ за время $\tau/2$. Ответ: это оператор $i\sigma_x$. В следующей главе мы покажем, как реализовать оператор, близкий к CNOT на атомных возбуждениях, там гамильтониан будет иметь обратный знак, и аналогичный оператор будет иметь вид $-i\sigma_x$.*

```
eigv[c_, a_] := Eigenvalues[{{0, -c}, {-c, a}}];
eigvec[c_, a_] := Eigenvectors[{{0, -c}, {-c, a}}];

solution[ini_, c_, a_, t_] := Exp[-I eigv[c, a][[1]] t] (Normalize[eigvec[c, a][[1]]].ini) Normalize[eigvec[c, a][[1]]] +
   Exp[-I eigv[c, a][[2]] t] (Normalize[eigvec[c, a][[2]]].ini) Normalize[eigvec[c, a][[2]]];
```

$$\begin{pmatrix} 0 & -c \\ -c & a \end{pmatrix}$$

```
c = 1;
a = 10;
ini = {0, 1};

Plot[{Abs[solution[ini, c, a, t][[1]]]^2, Abs[solution[ini, c, a, t][[2]]]^2}, {t, 0, Pi}, PlotLegends → "Expressions"]
```

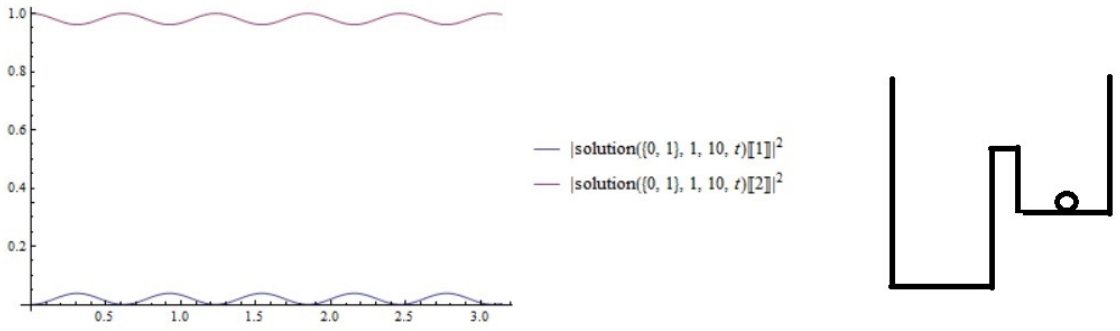



Рис. 21: Две ассиметричные потенциальные ямы. Неклассическое поведение частицы: если начальное состояние - в яме с более высокой энергией, частица остается в ней с высокой вероятностью

Реализация гейта CiNOT требует двух квантовых точек, расположенных перпендикулярно друг к другу, как показано на рисунке 22. Кулоновское взаимодействие двух электронов, каждый из которых находится в одной из этих точек, приводит к эффекту изменения потенциального барьера в точке $y$. Потенциальный барьер между ямами в точке $y$ оказывается выше, если электрон точки $x$ находится в состоянии $|1\rangle$, по сравнению с ситуацией, когда электрон точки $x$ находится в состоянии $|0\rangle$ в силу того, что отталкивание электронов выше на близком расстоянии.

Допустим сначала, что положение электрона $x$ нам удалось каким-то образом зафиксировать, так что он не туннелирует между своими ямами. Тогда можно подыскать такое время $\tau_{CiNOT}$, что через это время произойдет преобразование $CiNOT$. Действительно, пусть разность энергетических уровней $y$- электрона, соответствующая положениям $x$ - электрона $|0\rangle$ и $|1\rangle$, равна $dE^0 = E_1^0 - E_0^0$ и $dE^1 = E_1^1 - E_0^1$ соответственно. Тогда периоды осцилляций для $y$- электрона при нахождении $x$- электрона в положении $|0\rangle$ и $|1\rangle$ будут, соответственно $\tau_0 = 2\pi\hbar/(dE^0)$ и $\tau_1 = 2\pi\hbar/(dE^1)$. Можно, варьируя расстояние между точками, подобрать эти значения таким образом, чтобы для некоторого значения времени $\tau_{CiNOT}$ в него укладывалось бы четное число осцилляций с верхним индексом 0 и нечетное - с верхним индексом 1, что и даст нам требуемый оператор $CNOT$ при фиксации положения $x$- электрона. Детали предоставляются слушателю.

Как предотвратить туннелирование $x$- электрона? Это можно сделать, повысив потенциальный барьер между ямами в $x$- точке так, чтобы за время туннелирования между ними $x$- электрона было существенно меньше $\tau_{CiNOT}$, а затем, после

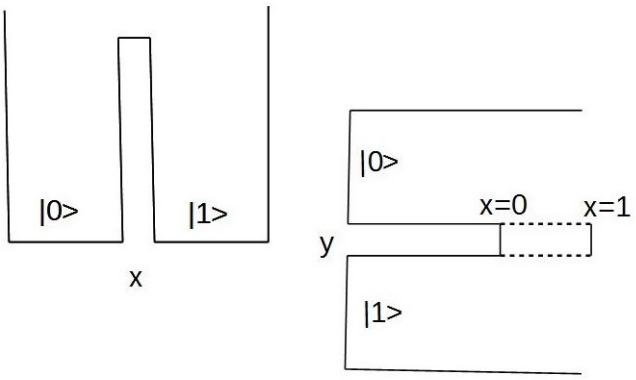



Рис. 22: CiNOT на зарядовых состояниях

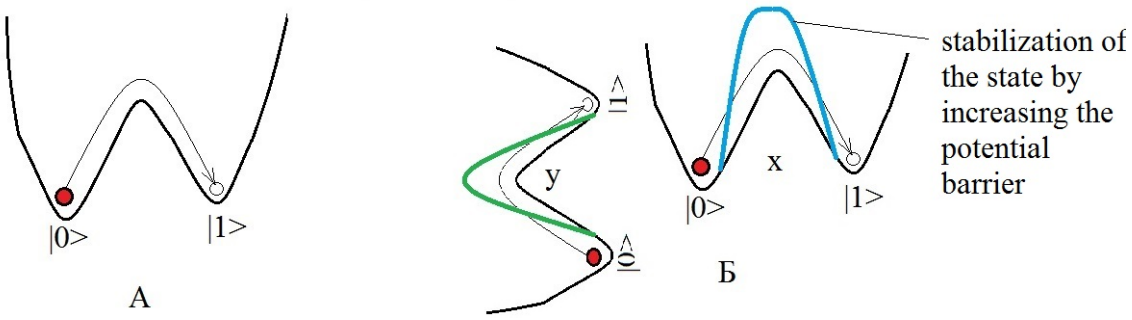



Рис. 23: The work of two dots implementing CNOT gate

совершения $CiNOT$, снова снизить этот барьер до обычного уровня, что делается внешним потенциалом. Так реализуется гейт $CiNOT$. Проблема состоит в том, что электрон, находящийся в возбужденном состоянии $|\phi_1\rangle$ в одной точке, способен испустить фотон, перейдя в состояние $|\phi_0\rangle$, что помешает реализации гейта $CiNOT$ по данной схеме. Подобная проблема возникает всегда при реализации запутывающих гейтов - ошибки. Для коротких вычислений они могут быть пренебрежимыми, однако для практически важных длинных вычислений они представляют проблему. Мы еще вернемся к этой теме позже, при изучении более реалистичных моделей квантовых компьютеров.

Иной путь реализации гейта CNOT показан на рисунках 24, 25

## 3.1 Гейты однокубитные, $CNOT, CSign, \Lambda_\phi$ и $Toffoli$

Докажите, что однокубитные гейты имеют вид

$$e^\alpha \begin{pmatrix} e^{i(\phi+\xi)}cos(\theta) & e^{i(\phi+\xi)}sin(\theta) \\ -e^{i\phi}sin(\theta) & cos(\theta) \end{pmatrix}$$

для некоторых вещественных $\alpha, \xi, \theta, \phi$. *Указание: найти число независимых вещественных параметров, определяющих унитарный оператор.*

Как получить корень из гейта $NOT$ - то есть такой гейт $V$, что $V^2 = NOT$?

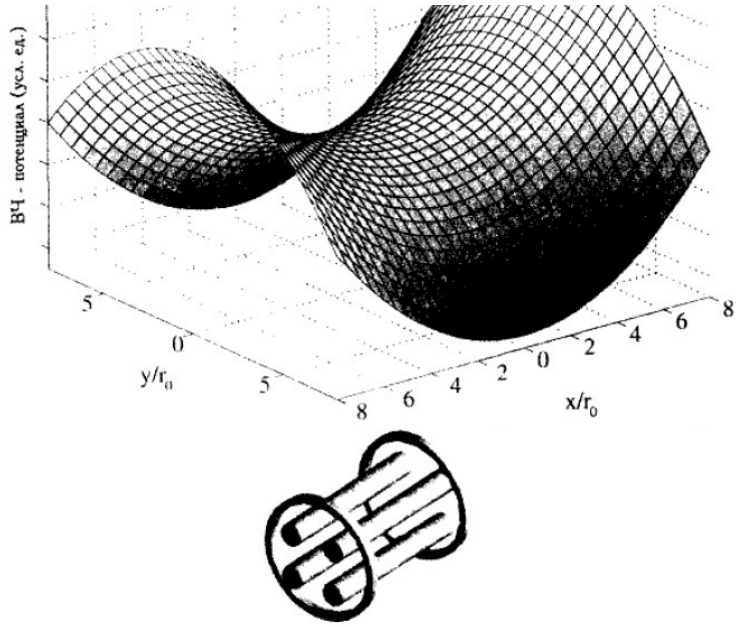



Рис. 24: Псевдо-потенциал ловушки Пауля

Гейт $CNOT$ есть 1-контролируемый NOT, он определяется как $CNOT|x,y\rangle = |x, x \oplus y\rangle$, где $\oplus$ - сложение по модулю 2. Построить матрицу $CNOT$.

2- контролируемый гейт $U$ определяется как

$$\Lambda_2 U : |x,y,z\rangle = \begin{cases} |x,y,z\rangle & if\ xy = 0, \\ |x,y\rangle U|x\rangle, & if\ xy = 1 \end{cases}$$

Покажите, что гейт $\Lambda_2 U$ можно реализовать с помощью системы квантовых гейтов, изображенной на рисунке 26.

*Указания. Рассмотреть только действия гейтов на базисных состояниях.*

## 3.2 Понятие о квантовой криптографии

Практическое применение квантовых однокубитных гейтов дает квантовая криптография. Мы покажем ее преимущество перед классической криптографией на примере квантового криптографического протокола BB84, первого из большой серии подобных протоколов.

Дадим короткое введение в задачу криптографии. Она состоит в обеспечении безопасной связи между передающим субъектом (Алиса) и принимающим (Боб) - см. рисунок 27. Если Алиса шлет Бобу бинарную строку $e_1, e_2, ...$, то Ева (подслушиватель) может перехватить ее на линии связи, скопировать и переслать Бобу без изменений, таким образом узнать информацию, не обнаружив себя. Для предотвращения подобного сценария у Алисы и Боба должен быть общий ключь - бинарная строка $k_1, k_2, ....$ Алиса кодирует свое сообщение, отправляя Бобу не $e_1, e_2, ...$, а $e_1 \oplus k_1, e_2 \oplus k_2, ...$ и Ева, не зная ключа, не сможет ничего расшифровать. Боб же легко это сделает, прибавив $k_i$ к полученному сообщению $e_i \oplus k_i$, и получив исходное $e_i$. Задача криптографии, таким образом, сводится к распределению секретного ключа $\bar{k}$.

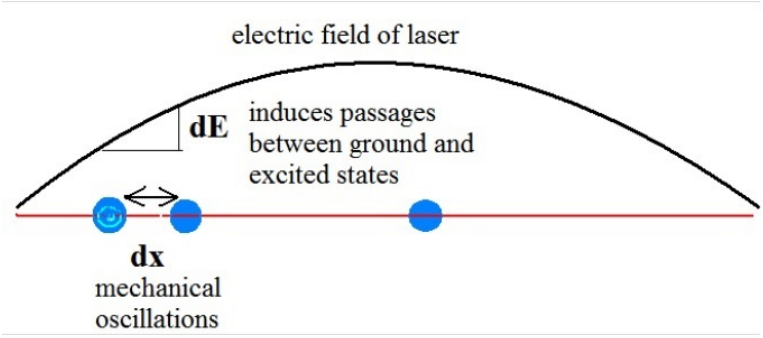



Рис. 25: Схематическое представление реализации гейта CNOT на ловушке Пауля. Логические кубиты - это внутренние состояния атомов; механические осцилляции атомов играют роль анциллы. Металлические положительные ионы в ловушке фактически фиксированы в своих потенциальных ямах вдоль оси ловушки; эти ямы создаются осциллирующим электрическим потенциалом, подаваемым на провода, идущие вдоль ловушки, что и создает, вместе с кулоновским отталкиванием между ионами, псевдо-потенциал.

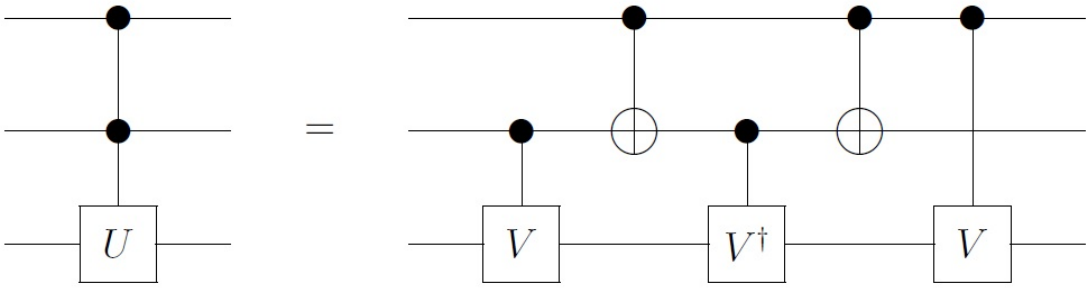



Рис. 26: Реализация 2-контролируемого гейта с помощью CNOT и однокубитного $V$, где $V^2 = U$

Никакой классический метод не может обеспечить безопасное распространение ключа по следующей причине: любое классическое сообщение может быть скопировано. Копирование есть отображение вида

$$U_{clon} : |\Psi\rangle|0\rangle \to |\Psi\rangle|\Psi\rangle \tag{32}$$

и в случае классического - базового - состояния это делается простым применением оператора $CNOT$. Однако если $|\Psi\rangle$ - суперпозиция классических состояний, этот прием не пройдет. Действительно, предположим, что существует такой унитарный оператор $U$, что равенство (32) выполнено для любого квантового состояния $|\Psi\rangle$. Возьмем в качестве $|\Psi\rangle$ состояние $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Тогда мы имеем:

$$\begin{aligned} U|\Psi\rangle|0\rangle &= \tfrac{1}{2}(|00\rangle + 01\rangle + |10\rangle + |11\rangle), \\ U|\Psi\rangle|0\rangle &= \tfrac{1}{2}U||00\rangle + U|10\rangle = \tfrac{1}{2}(|00\rangle + |11\rangle) \end{aligned}$$

то есть противоречие.

Итак, копирование квантовых состояний невозможно, причем именно потому что мы можем использовать супрепозицию базисных состояний. Это можно практически использовать так.

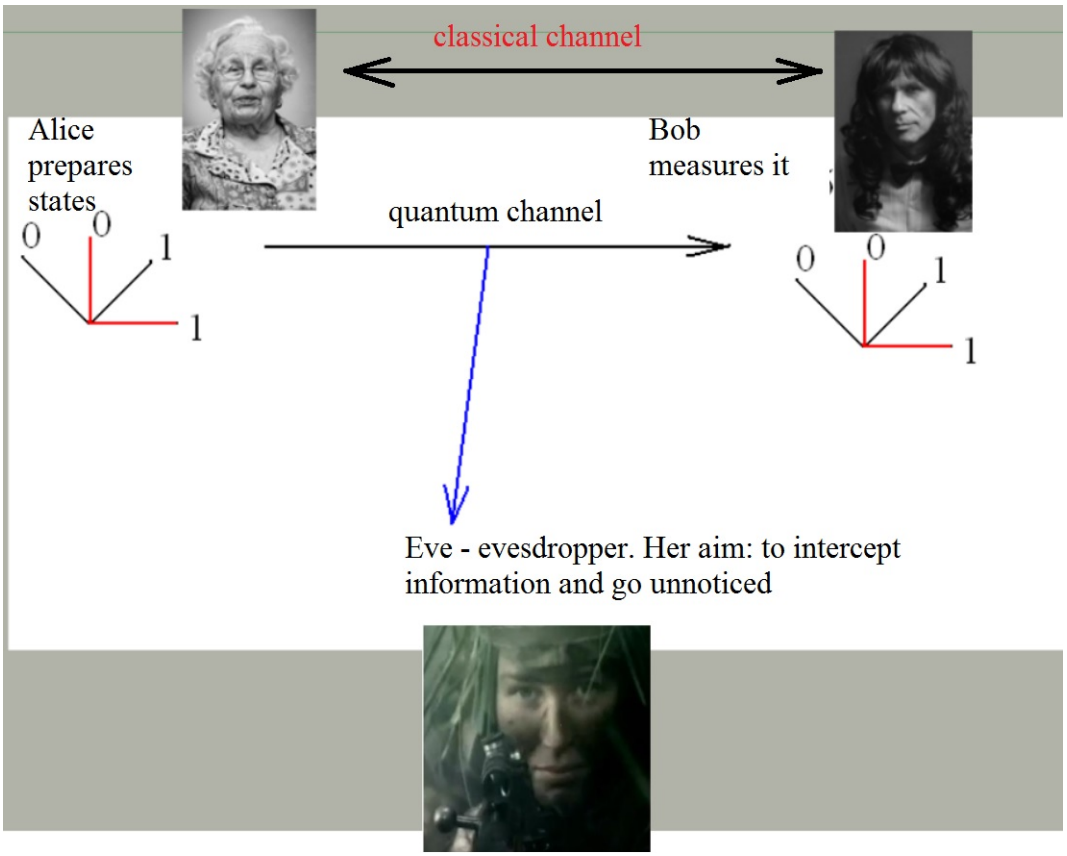



Рис. 27: Cryptography scheme: quantum key distribution between Alice and Bob

Пусть $A = \frac{1}{\sqrt{2}}(\sigma_x + \sigma_z)$ - гейт Адамара. Алиса, помимо основной "заготовки" ключа $k_1, k_2, ...$ создает еще и случайную последовательность бинарных знаков $bas_1, bas_2, ...$, и кодирует любой $k_i$ в виде $k_i$, если $bas_i = 0$ и в виде $A|k_i$, если $bas_i = 1$. Так закодированную строку $bas(k_1), bas(k_2), ...$ она посылает Бобу. Если бы Боб знал последовательность $bas_1, bas_2, ...$, он бы быстро расшифровал послание Алисы, но он этой последовательности не знает. Тогда Алиса поступает неожиданным образом - она посылает Бобу второе послание - эту последовательность $bas_1, bas_2, ...$ - по открытому классическому каналу связи, который Ева слушает, но исказить не может! Боб, естественно, сразу восстанавливает "заготовку" ключа $k_1, k_2, ....$

Если Ева есть в канале, она должна своим вмешательством исказить состояния $bas(k_i))$, иначе она ничего не узнает, то есть фактически, ее в канале нет. Как узнать, если ли Ева в канале? Очень просто. Алиса шлет Бобу значения $k_i$ из наугад выбранной последовательности $i = i_1, i_2, ...$ и Боб, приняв это сообщение, и сравнивая со своей расшифровкой $k_i$, определяет присутствие Евы по несовпадению. Таким образом, присутствие Евы в канале связи может быть надежно детектировано, и если ее нет, можно передавать безопасно. В этом состоит идея протокола BB84. Дальше применяется так называемое усиление секретности, когда данная процедура делается не на всей заготовке $k_i$ а только на ее части, и т.д. Мы не будем здесь вникать в детали.

Квантовая криптография превратилась сейчас в огромную область, известно множество квантовых криптографических протоколов, и все они основаны на запрете квантового клонирования произвольных состояний. Мы видим, что даже без исполь-

зования запутанности, квантовая механика одного кубита дает нам ощутимое преимущество по сравнению с классическими методами в области защиты информации.

Обратим внимание на то, что в этой области существенно используется понятие "кто-то знает". Это - не математическое понятие, а, скорее, гуманитарное и его использование в математике не может считаться корректным. Поэтому для обеспечения секретности квантовых криптографических протоколов необходимо формализовать понятие "кто-то что-то знает".

Квантовая энтропия фон Неймана для смешанного состояния $\rho$ определяется как

$$S(\rho) = -tr(\rho\ log(\rho)).$$

Определим понятие квантовой относительной энтропии для пары матриц плотности $\rho, \sigma$ как

$$S(\rho\|\sigma) = tr(\rho(log(\rho) - log(\sigma))$$

.

Взаимная информация между двумя субъектами $A$ и $B$ теперь может быть определена как

$$I(A:B) = S(\rho_A) + S(\rho_B) - S(\rho_{AB})$$

где $A$ и $B$ - две части одной системы $AB$, и нижний индекс обозначает относительную матрицу плотности.

Можно показать, что

$$I(A:B) = S(\rho_{AB}\|\rho_A \otimes \rho_B).$$

Это стандартное определение понятия степени "знания" субъекта $A$ о субъекте $B$. Оно, тем самым, полностью укладывается в математический формализм квантовой теории. Возможная атака на квантовый криптографический канал может состоять либо в использовании шума как прикрытия, либо использования ограничений на квантовое описание состояний как таковое. Первый метод работает только если уровень шума в канале существенно превышает 12% . Второй путь предполагает существование ограничений на квантовый формализм как таковой, что в простых системых невозможно: эти ограничения наступают только в сложных системах. Таким образом, квантовая криптография обеспечивает надежность распространения ключа принципиально более высокую, чем классическая, и используется для передачи данных особой важности.

## 3.3 Квантовая телепортация

Теорема о запрете клонирования играет важную роль в квантовой криптографии, делая ее абсолютно надежным способом передачи информации. Однако возможно перемещение квантового состояния на расстояние без перемещения его носителя. Для этого нужен своеобразный информационный канал, образованный ЭПР парой $|epr\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Этот протокол называется квантовой телепортацией.

Он состоит в следующем. У Алисы и Боба есть ЭПР пара, кубиты которой мы обозначаем индексами $A$ и $B$ соотвественно. У Алисы есть, к тому же, еще один

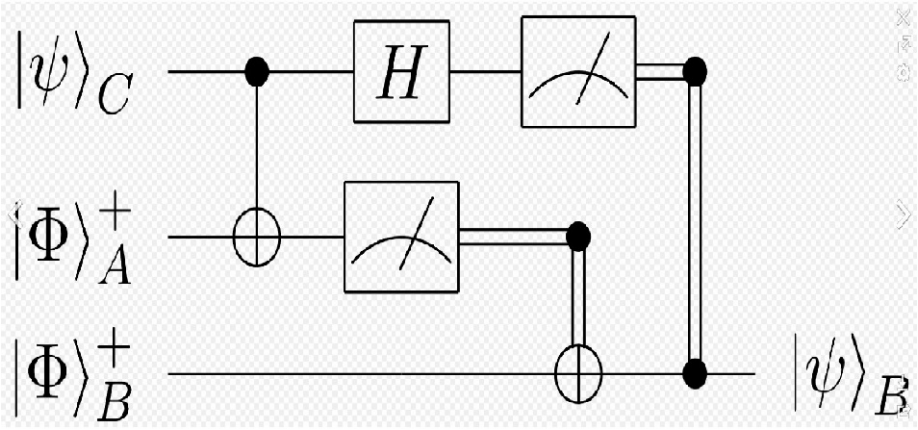



Рис. 28: Схема телепортации

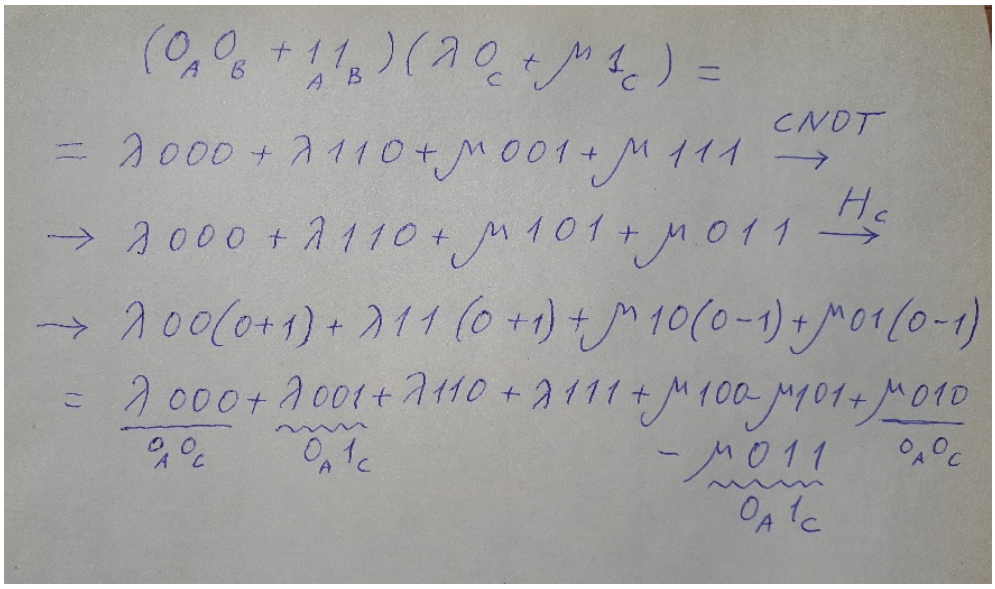



Рис. 29: Вычисление результата телепортации

дополнительный кубит, который мы обозначаем через $C$ в неизвестном состоянии $\lambda|0\rangle + \mu|1\rangle$, состояние которого Алиса хочет передать Бобу. С этой целью Алиса совершает над кубитами $C$ и $A$ оператор $CNOT$, затем над $C$ оан совершает преобразование Адамара:

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

после чего измеряет ба своих кубита и пересылает результат измерения - классическое состояние двух кубитов - Бобу. Боб способен по полученной информации восстановить в своем кубите неизвестное состояние $|\Psi\rangle$. Схема телепортации изображена на рисунке 28.

Корректность работы такой схемы проверяется вычислением, приведенным на рисунке 29. Здесь принят порядок следования кубитов: $A, B, C$, и опущены нормировочные коэффициенты.

$$
\begin{aligned}
&(|0_A 0_B\rangle + |1_A 1_B\rangle)(\lambda|0_C\rangle + \mu|1_C\rangle) = \\
&\lambda|000\rangle + \lambda|110\rangle + \mu|001\rangle + \mu|111\rangle \rightarrow \\
&\lambda|000\rangle + \lambda|001\rangle + \mu|101\rangle + \mu|011\rangle \rightarrow \\
&\lambda|00\rangle(|0\rangle + |1\rangle) + \lambda|11\rangle(|0\rangle + |1\rangle) + \mu|10\rangle(|0\rangle - |1\rangle) + \mu|01\rangle(|0\rangle - |1\rangle) = \\
&\lambda|000\rangle + \lambda|001\rangle + \lambda|110\rangle + \lambda|111\rangle + \mu|100\rangle - \mu|101\rangle + \mu|010\rangle - \mu|011\rangle
\end{aligned}
\tag{33}
$$

Экспериментальная реализация квантовой телепортации на поляризация фотонов была реализована между двумя островами Канарского архипелага(см. рисунок 30).

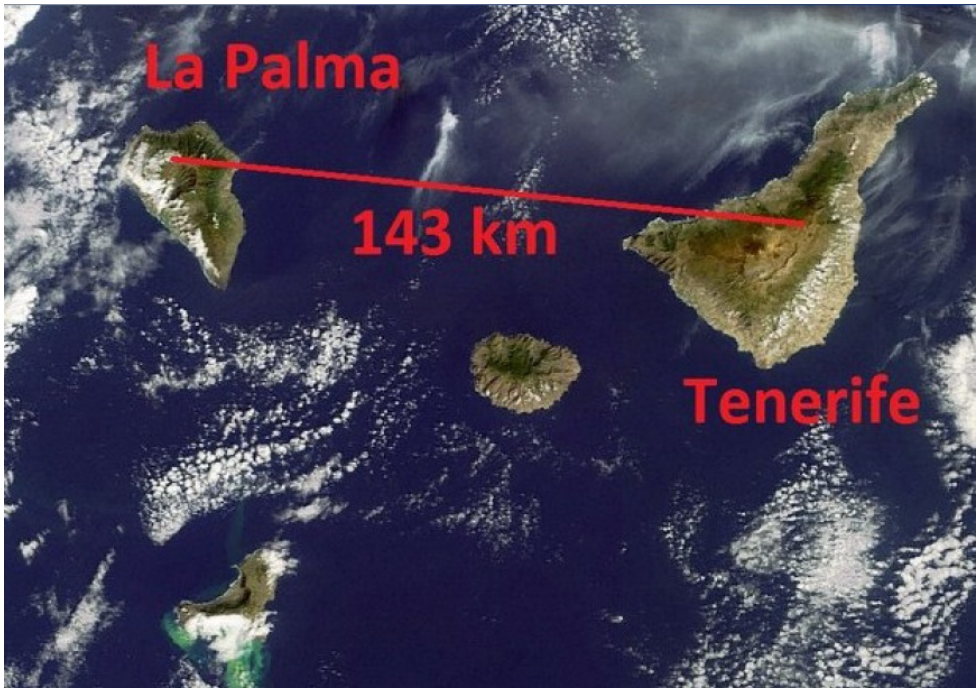



Рис. 30: Квантовая телепортация между двумя Канарскими островами

# 4 Лекция 4. Алгоритм Гровера

Для практического построения квантовых алгоритмов мы должны теперь конкретизировать вид той функции $\mathcal{F}$, которую мы ранее назвали алгоритмом. Квантовый алгоритм - это рисунок, состоящий из $n$ параллельных проводов, расположенных друг над другом, с выделенными началами и концами. Эти провода соединены перпендикулярными перемычками, каждая из которых соответствует определенному квантовому гейту. Пример алгоритма приведен на рисунке 26.

*Квантовое вычисление*, соответствующее заданному алгоритму, есть последовательность вида

$$\mathcal{C}_0 \longrightarrow \mathcal{F}_0(\mathcal{C}_0) \longrightarrow \mathcal{F}_1(\mathcal{F}_0(\mathcal{C}_0)) \longrightarrow \ldots \longrightarrow \mathcal{F}_{T-1}(\ldots \mathcal{F}_0(\mathcal{C}_0)\ldots), \tag{34}$$

состоящая из результатов последовательных применений гейтов алгоритма слева направо, где начальное состояние $|\mathcal{C}_0\rangle$ памяти размещается в началах проводов по кубитам, снизу вверх. Таким образом, провода фактически задают направление времени работы алгоритма. Конечное состояние получается как состояние конечных вершин проводов. После окончания работы оно может быть измерено, тогда результат работы алгоритма будет бинарной строкой, или не измеряться - в этом случае алгоритм можно использовать в качестве подпрограммы, встраивая его в другие алгоритмы. Часто рисунки алгоритмов оказываются похожими, что позволяет параметризовать набор алгоритмов с помощью числа $n$ - числа проводов, совпадающего с объемом оперативной памяти, и называть такой набор единым алгоритмом. В этом случае сложность определяется, как и выше.

Вместо изображения алгоритма рисунком можно задачать его словами: "сначала делаем с первым и вторым кубитами то-то и то-то, потом делаем с третьим то-то и т.д." Заметим, что некоторые из гейтов могут быть оракулом - гейтом с многими переменными, который реализует некоторый фиксированный унитарный оператор, так что мы фактически определили и квантовые вычисления с оракулом. Его сложность определяется дословно аналогично приведенному выше.

Мы разберем лишь один быстрый квантовый алгоритм, найденный Ловом Гровером в 1996 году (см. [12]) - алгоритм GSA (Grover search algorithm). Этот алгоритм содержит минимальное число деталей, и потому на нем можно самым наглядным образом показать важнейшее свойство квантовой динамики - способность концентрировать амплитуду на отдельных состояниях, причем тех, которые заранее не известны. Скорость такой концентрации необычайно велика, так что этот процесс невозможно воспроизвести на классическом компьютере.

GSA - фундаментальный квантовый алгоритм. Он может служить моделью сложных процессов на квантовом уровне, что будет более подробно разобрано в третьей главе. Там же будут рассматриваться превращения амплитуды квантовых состояний при вычислении по этому алгоритму. Здесь же мы опишем GSA с "внешней" стороны, в терминах гильбертова формализма. Это описание коротко и красиво, и потому начнем с него.

Пусть задана булева функция $f$ от $n$ переменных, причем уравнение

$$f(x) = 1 \tag{35}$$

имеет ровно один корень $x_{tar}$, который нам надо найти, обращаясь к функции $f$ наименьшее число раз. Если бы у нас был классический компьютер, число таких обращений было бы по порядку величины не меньше $N = 2^n$, так как это классическая переборная задача, в которой нет лучшего способа нахождения ответа кроме прямого перебора всех возможных вариантов - всех булевых $n$- ок. Это очевидно, если $f$ задана нам в виде "черного ящика"; в случае, если у нас имеется явная схема из функциональных элементов, вычисляющая $f$, необходимость перебора строго не доказана, просто никакого более быстрого метода поиска решения (35) до сих пор не найдено.

На квантовом компьютере можно найти $x_{tar}$ за $[\pi\sqrt{N}/4]$ обращений к функции $f$. Если у нас имеется классическое устройство, вычисляющее $f(x)$ для любого $x \in \{0,1\}^n$, из него можно сделать квантовый алгоритм, вычисляющий функцию вида

$$f_{quant}: \ |x,y\rangle \to |x, f(x) \oplus y\rangle \tag{36}$$

Продемонстрируем идею такого построения на примере простейшей тождественной функции $I: \ |x\rangle \to |x\rangle$. Тогда $I_{quant}$ называется $CNOT$ и действует как $CNOT|x,y\rangle = |x, x \oplus y\rangle$. Можно показать для различных технологий квантовых компьютеров независимо, что такой унитарный оператор, теоретически, можно реализовать в любой из технологий; за деталями слушатель может обратиться к архиву препринтов.

Отражением пространства квантовых состояний вдоль вектора $|a\rangle$ называется зеркальное отражение относительно подпространства, ортогонального $|a\rangle$:

$$I_a|b\rangle = \begin{cases} |b\rangle, & \text{если} \quad \langle a|b\rangle = 0, \\ -\ |a\rangle, & \text{если} \quad |a\rangle = |b\rangle \end{cases} \tag{37}$$

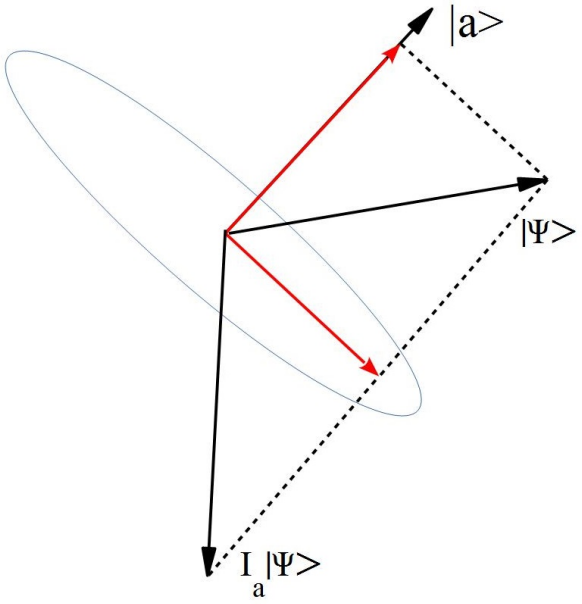
Определенное так отображение линейно продолжается на все пространство; это продолжение мы будем обозначать тем же символом $I_a$.

Отражение графически изображено на рисунке 31.

Имея оператор $f_{quant}$, который действует на все линейные комбинации базисных состояний, а не только на одно базисное, как в классическом случае, мы можем построить оператор отражения $I_{x_{tar}}$ вдоль вектора $|x_{tar}\rangle$, хотя сам этот вектор нам и неизвестен. Для этого введем анциллу (вспомогательный кубит), инициализировав ее состоянием $|anc\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, и применим к состоянию вида $|\Psi\rangle|anc\rangle$ оператор $f_{quant}$. Из определений вытекает, что получится состояние $I_{x_{tar}}|\Psi\rangle|anc\rangle$ и анциллу можно выкинуть, не опасаясь порчи текущего состояния, поскольку анцилла, сыгравшая свою роль во введения минуса при базисном состоянии $|x_{tar}\rangle$ в суперпозиции $|\Psi\rangle$, снова является незапутанной с основным массивом кубитов.

Здесь надо сделать важное замечание. Если бы мы инициализировали анциллу состоянием $|0\rangle$, а затем совершили бы преобразование $f_{quant}$, чтобы затем изменить знак при $x_{tar}$ оператором $\sigma_z$, примененным к анцилле (что было бы естественно в классическом компьютере), то это создало бы, вообще говоря, запутанное состояние между основным массивом кубитов и анциллой, и просто выкинуть анциллу было бы нельзя: ее измерение привело бы к необратимой порче основного состояния, и мы не получили бы $I_{x_{tar}}|\Psi\rangle$ в итоге. Здесь необходимо было бы применить $f_{quant}$ еще раз, чтобы анцилла снова перешла в отдельное состояние $|0\rangle$, то есть на одну инверсию вдоль $|x_{tar}\rangle$ мы потратили бы два вызова функции $f_{quant}$ вместо одного

Рис. 31: Отражение пространства вдоль вектора $|a\rangle$.




при нетривиальной инициализации анциллы; при такой инициализации изменение нужного знака в линейной комбинации на входе происходит с одновременной чисткой анциллы.

Построим состояние вида $|\tilde{0}\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} |j\rangle$ - это можно сделать, совершая преобразование Адамара

$$H = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2}- & 1/\sqrt{2} \end{pmatrix} \tag{38}$$

над каждым кубитом в состоянии основного массива $n$ кубит $|\bar{0}\rangle = |00...0\rangle$, где все кубиты имеют значение $|0\rangle$ (докажите!). Такой оператор иначе можно записать как тензорную $n$ - ную степень оператора $H$; его еще называют оператором Уолша-Адамара: $WH = H^{\otimes n}$.

*Слушатель может попробовать (это необязательно) выяснить общий вид элемента матрицы оператора $WH$: $w_{i,j}$. Указание: надо использовать кубитовое представление натуральных чисел $i$ и $j$.*

Далее, мы уже видели, как реализовать гейт Тоффоли $T: \ |x, y, z\rangle \to |x, y, xy \oplus z\rangle$ на любой технологии квантового компьютера, на которой можно реализовать $CNOT$ (можно показать, что $T$ выражается через $CNOT$ и однокубитные гейты).

Покажем, как совершить преобразование $I_{\bar{0}}$.

Рассмотрим оператор $R$, который реализуется массивом гейтов, показанным на рисунке 33. Заведем дополнительно $n$ анцилл, инициализированных нулями, и занумеруем их натуральными числами $1, 2, ..., n$. и еще один дополнительный кубит,, который назовем результатом $res$. Будем совершать преобразование $R$ последовательно над $x, y, z$, которые представляют собой: $i$-й кубит основного массива,$i$ - й кубит анциллы и $res$ соотвественно. Затем совершим $-\sigma_z(res)$. В кубите $res$ будет 1

Рис. 32: Последовательные применения оператора $R$ - каждое применение после одновременного сдвига управляющих стрелок

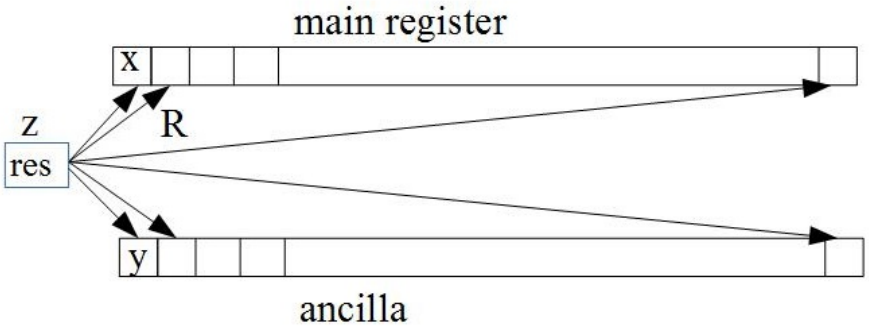
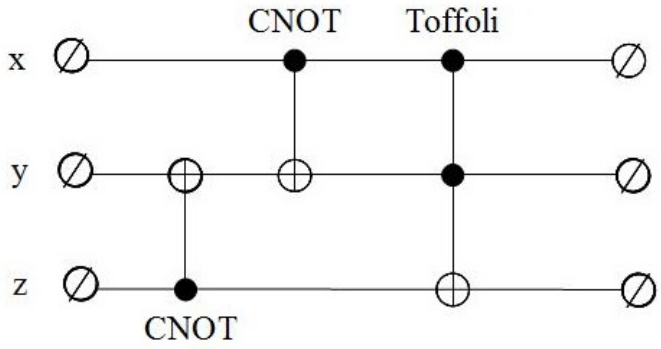



Рис. 33: Схема, реализующая оператор $R$. Его главное свойство: отображения $|000\rangle \to |000\rangle, |100\rangle \to |111\rangle, |101\rangle \to |101\rangle, |001\rangle \to |011\rangle$.




тогда и только тогда, когда $x \neq 0$. Для обязательной очистки анциллы совершим все описанные преобразования в обратном порядке (см. рисунок 32 ).

Теперь мы можем совершить и $I_{\tilde{0}}$, заметив, что $I_{\tilde{0}} = H^{\otimes n}\ I_{\bar{0}}\ H^{\otimes n}$.

После этого будем делать последовательные применения оператора $G = -I_{\tilde{0}} I_{x_{tar}}$, начиная с $|\tilde{0}\rangle$ $[\pi\sqrt{N}/4]$ раз. Покажем, что результат с высокой точностью совпадет с $|x_{tar}\rangle$. Действительно, вся эволюция вектора состояния $n$- кубитной системы будет происходить в вещественной линейной оболочке двух почти ортогональных векторов $|\tilde{0}\rangle$ и $|x_{tar}\rangle$, причем $G$ будет дважды инвертировать ориентацию этой двумерной вещественной плоскости. Значит, $G$ есть ее поворот на некий угол $\beta$, найти который можно, следя за одной единственной точкой, например, за концом вектора $|\tilde{0}\rangle$. Легко показать (сделайте это!), что $\beta = 2\ arcsin(1/\sqrt{N})$. Теперь из высокой точности равенства $\alpha \approx \arcsin(\alpha)$ следует искомое равенство

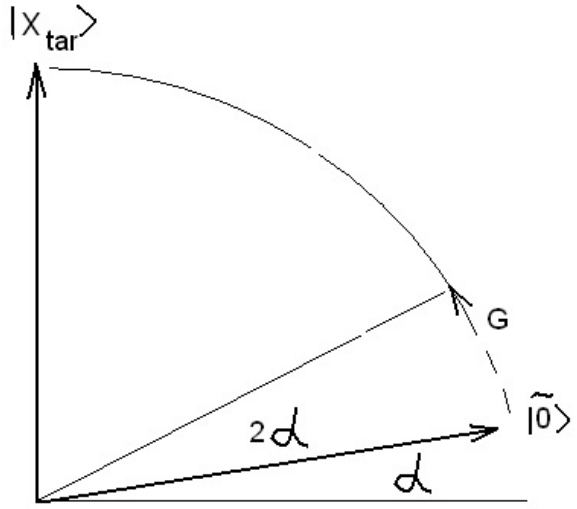
$$|x_{tar}\rangle \approx G^{\tau}|\tilde{0}\rangle,$$

что и требовалось.

Работа GSA изображена на рисунке 34.

Итак, квантовый алгоритм Гровера требует порядка $\sqrt{N}$ обращений к оракулу, то есть ускоряет вычисление неизвестного решения (35) на уровне, недоступном никакому классическому компьютеру. Можно показать (см. [13], что данный алгоритм

Рис. 34: Работа GSA - последовательные повороты на угол, примерно равный $2\ arcsin(\sqrt{l/N}$.




является оптимальным в следующем точном смысле. Любой иной алгоритм, работающий существенно быстрее, будет давать неверный ответ для переборной задачи (35) для подавляющего большинства функций $f$ (См. также [14], [15]).

*Если уравнение* (35) *имеет несколько решений:* $x_1, x_2, ..., x_l$, *то в точности повторив схему GSA, только взяв* $\tau = [4\pi\sqrt{N/l}]$, *мы получим в результате хорошее приближение состояния* $|X_{tar}\rangle = \frac{1}{\sqrt{l}} \sum_{j=1}^{l} |x_j\rangle$, *после чего измерение позволит нам найти одно из* $x_j$. *Проверьте этот факт, убедившись, что все рассуждения сохранятся, только* $x_{tar}$ *надо заменить на* $X_{tar}$ *с соответствующей коррекцией времени* $\tau$.

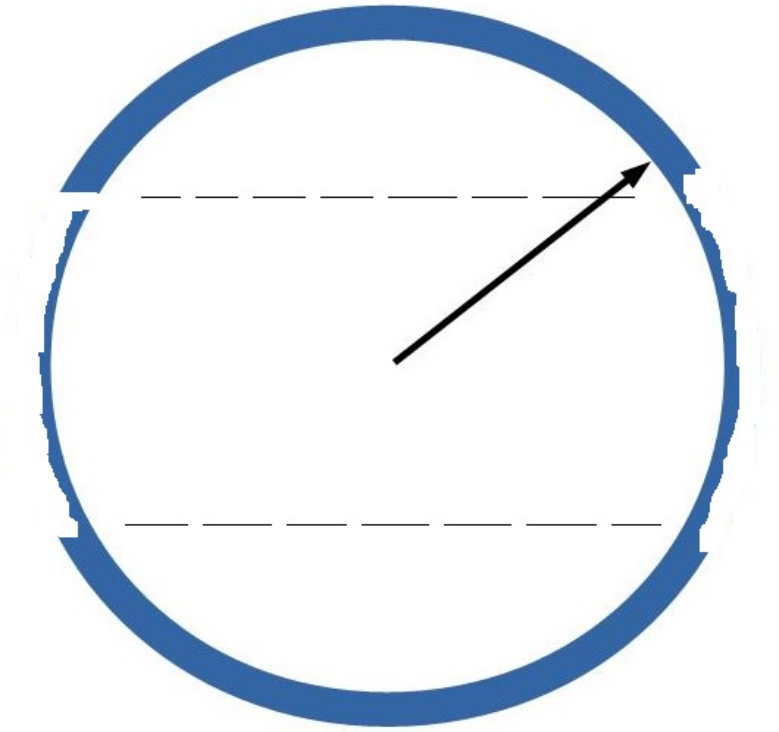
*Если* $l$ *нам неизвестно (практически важный случай), можно итерировать схему GSA, производя* $\tau_s$ *операций GSA для* $\tau_s = 2^s$, *последовательно, для* $s = 1, 2, ...$ *(см. рисунок 35). Покажите, что число шагов такого итерационного применения GSA будет иметь порядок* $O(\sqrt{N/l})$, *то есть корня из классического времени. Это - максимально возможное квантовое ускорение для большинства классических алгоритмов при неограниченной длине вычисления - мы покажем это ниже; если же рассмотреть короткие классические алгоритмы, их в большинстве случаев, нельзя ускорить на квантовом компьютере даже на один шаг (см. [6]).*

## 4.1 Непрерывная версия алгоритма Гровера

Алгоритм Гровера имеет непрерывную версию, когда получение конечного состояния $|x_{tar}\rangle = |w\rangle$ происходит как унитарная эволюция вектора состояния в двумерном подпространстве, порожденном векторами $|w\rangle$ и $|\tilde{0}\rangle$ под действием гамильтониана

$$H + \frac{1}{\sqrt{2}}(|\tilde{0}\rangle\langle\tilde{0}| + |w\rangle\langle w|)$$

Рис. 35: Достаточно достичь "неиспорченной" зоны окружности



где $|\tilde{0}\rangle = \frac{1}{N}\sum_{j=0}^{N-1}|j\rangle$. Мы имеем: $\langle\tilde{0}|w\rangle = sin(\alpha) = \frac{1}{\sqrt{N}}$. Матрица гамильтониана $H$ в стандартном базисе имеет вид

$$|w\rangle\langle w| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, |\tilde{0}\rangle\langle\tilde{0}| = \begin{pmatrix} cos\ \alpha \\ -sin\ \alpha \end{pmatrix}\begin{pmatrix} cos\ \alpha & -sin\ \alpha \end{pmatrix} = \begin{pmatrix} cos^2\ \alpha & -cos\ \alpha\ sin\ \alpha \\ -cos\ \alpha\ sin\ \alpha & sin^2\ \alpha \end{pmatrix}.$$

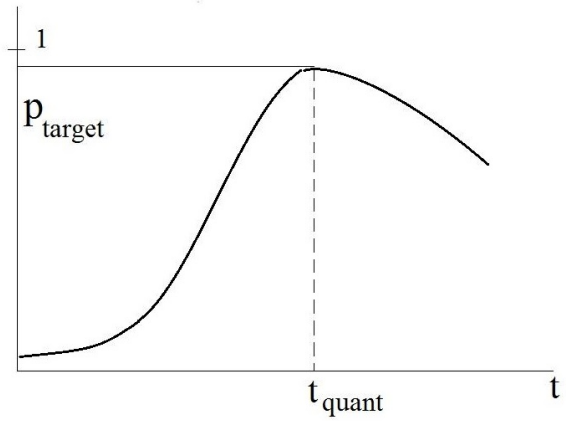
Находя собственные значения энергии $H$, получаем $E_{1,2} = \frac{1}{\sqrt{2}} \pm sin(\alpha/2)$, так что разница между основным и возбужденным уровнями составляет 2 $sin(\alpha/2)$ что с большой точностью равно $\alpha$. Отсюда, решая уравнение Шредингера для $H$, получаем, что за время порядка $\sqrt{N}$ из состояния $|\tilde{0}\rangle$ эволюция приведет нас в состояние $|w\rangle$, то есть непрерывная версия алгоритма Гровера дает то же ускорение классического вычисления, что и стандартная версия.

## 4.2 Квантовое ускорение классических вычислений и его пределы

Квантовое ускорение классических вычислений получается, если время поиска рашения како-либо задачи на квантовом компьютере меньше чем аналогичное время на любом из классических алгоритмов (см. рисунок 36).

Если говорить кратко, квантовое ускорение вычислений состоит вот в чем. Допустим, мы имеем некий абстрактный квантовый компьютер, в котором реализует-

Рис. 36: Квантовое ускорение классического вычисления $x_{tar}$ получается, если квантовое время поиска меньше классического: $t_{quant} < t_{class}$.




ся под нашим контролем над гамильтонианом $H$ эволюция $exp(-\frac{i}{h}Ht)$. Можем ли мы с помощью такого устройства предсказать будущее произвольной классической системы? И если да, то насколько быстро? К этому вопросу, по-существу, сводится важнейшая проблема верификации того факта, что кто-либо построил именно квантовый компьютер, а не подделал его работу с помощью спрятанного в подвале суперкомпьтера.

Именно это называется квантовым ускорением классического вычисления. Мы покажем, что если понимать под классической системой конкретную функцию $f : \mathcal{K} \longrightarrow \mathcal{K}$ из конфигурационного пространство в себя (закон классической эволюции), то ответ на этот вопрос будет зависеть от того, на каком промежутке времени $t$ мы рассматриваем предсказание. Если не накладывать на $t$ никакого ограничения, то квантовое время будет иметь порядок не меньше квадратного корня из классического, то есть квантовое ускорение для большинства классических задач не превзойдет гроверовского - для перебора.

Если же потребовать, чтобы время $t$ было достаточно малым (по сравнению с числом всех возможных конфигураций компьютера), у нас получится совсем удивительный факт: квантовый компьютер потратит на моделирование такое же время, какое занимает сама классическая эволюция (см. [6]).

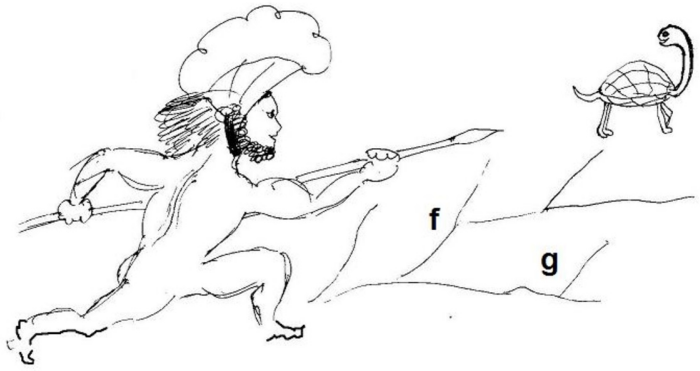
**Квантовый Ахиллес может не догнать классическую черепаху!**

Мы покажем, как устанавливается нижняя граница в квадратный корень из классического времени для квантовой сложности нахождения результата итераций классического оракула. Заметим, что такие результаты показывают фундаментальные пределы скорости "квантового Ахиллеса"; их невозможно преодолеть никаким совершенствованием его структуры.

Итак, классическая эволюция представляется в виде итерации некоторой функции $f$, так что она имеет вид

$$x_0 \longrightarrow f(x_0) \longrightarrow f(f(x_0)) \longrightarrow \ldots \longrightarrow f^k(x_0) \longrightarrow \ldots \longrightarrow f^T(x_0),$$

Рис. 37: Квантовый Ахиллес и классическая черепаха




где через $f^k(x_0)$ обозначена $k$- кратная итерация $f$. Значение $x_0$ не играет в данном случае никакой роли, так что мы пишем просто $f^k$.

Квантовый компьютер, наш Ахиллес - см. рисунок 37, имеет в своем распоряжении функцию $f$, и может ее использовать как квантовый оракул $Qu_f : |x, y\rangle \longrightarrow |x, y \oplus f(x)\rangle$. Все слова $f^k$ принадлежат базисным состояниям квантового гильбертова пространства, так что любое из этих слов можно подставить вместо $x$ или $y$. Итак, мы можем считать, что $f^k$ принадлежат базисным состояниям нашего компьютера. Тогда, после надлежащей группировки нескольких последовательных операций в вычислении, мы можем считать, что каждое такое состояние $e$ вызывает оракул $f$ на некотором слове $q(e)$ из того же набора (группировка необходима, чтобы в каждой группе было ровно одно вопросное состояние).

Мы можем группировать элементарные операции, как угодно; нам нужна только унитарность всех квантовых переходов, использующаяся в дальнейших неравенствах. Тогда вероятность того, что квантовое состояние

$$|\Psi\rangle = \sum_j \lambda_j |j\rangle$$

нашего Ахиллеса вызовет оракул $f$ на слове $a$, будет считаться по формуле

$$\delta_a(\Psi) = \sum_{j:\ q(j)=a} |\lambda_j|^2,$$

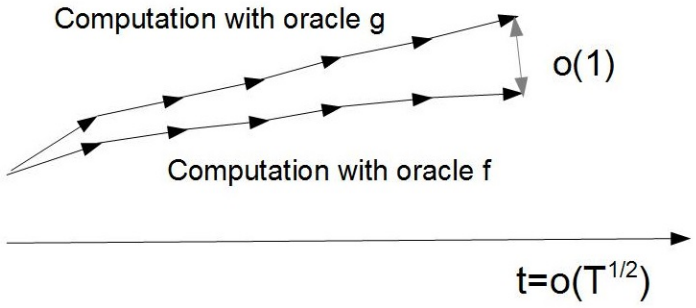
вытекающей из правила Борна. Положим $d_a(\Psi) = \sqrt{\delta_a(\Psi)}$.

Вся скорость Ахиллеса - в этом параллелизме! Он может догнать черепаху - классическое вычисление - лишь за счет того, что спрашивает оракул сразу на всех словах, а не только на одном, как она. Но посмотрим, что ему удастся сделать?

Как определить разницу между двумя стратегиями классической черепахи: функциями $f$ и $g$, которые определяют классическую динамику? Самое естественное - обобщить определение $d_a(\Psi)$, и определить расстояние между стратегиями черепахи как

$$d_\Psi(f, g) = [\sum_{a:\ f(a)\neq g(a)} \delta_a(\Psi)]^{1/2}.$$

Рис. 38: Вычисления с двумя оракулами




Из этого определения сразу вытекает, что

$$\|Qu_f(\Psi) - Qu_g(\Psi)\| \leq 2d_\Psi(f,g). \tag{39}$$

В этой оценке - слабая сторона Ахиллеса. Оператор вопроса к оракулу $Qu_f$ - унитарен, и это связывает квантовую скорость. Поскольку мы анализируем возможности квантового компьютера по отношению ко всем классическим, наша черепаха может применить, так сказать, обманный ход. Что будет, если изменить значение $f$ только на одном слове? Понятно, что это, в большинстве случаев, изменит и значение конечного состояния $f^T$. Но сможет ли наш Ахиллес уловить подмену? Если его квантовые состояния будут мало отличаться при работе с этими двумя оракулами, он не сможет их различить при измерении, и будет обманут! Иллюстрация приведена на рисунке 38.

Рассмотрим два пути Ахиллеса: с оракулом $f$ и с оракулом $g$ соответственно:

$$\begin{array}{rl} & \Psi_0 \longrightarrow \Psi_1 \longrightarrow \ldots \longrightarrow \Psi_t, \\ \Psi'_0 = & \Psi_0 \longrightarrow \Psi'_1 \longrightarrow \ldots \longrightarrow \Psi'_t, \end{array} \tag{40}$$

Пусть $f$ действуют всюду одинаково, кроме одного слова $a$, на котором $f(a) \neq g(a)$. Из неравенства (39) простой индукцией по $t$ непосредственно устанавливается, что

$$\|\Psi_t - \Psi'_t\| \leq 2\sum_{i=0}^{t-1} d_a(\Psi_i). \tag{41}$$

Теперь нам надо выбрать $a$ так, чтобы доставить Ахиллесу максимум неудобств. Определим матрицу

$$a_{ij} = \delta_{f^j}(\Psi_i),\ i = 1,2,\ldots,t;\ j = 1,2,\ldots,T.$$

Здесь $t$ - время Ахиллеса, а $T$- время черепахи; $T/t$ - коэффициент квантового ускорения. Как связаны эти времена? Максимальное неудобство для нашего Ахиллеса будет доставлено вот таким выбором $a = f^\tau$, где $\tau$ выбрано так, что $\sum_{i=1}^{t} a_{i\tau} \leq t/T$. Это возможно потому, что сумма матричных элементов по любой строке равняется

1 - это полная вероятность; значит, сумма всех вообще элементов будет не больше $t$. Теперь мы имеем

$$\|\Psi_t - \Psi'_t\| \leq 2\sum_i \sqrt{a_{i\tau}} \leq 2\sqrt{t\sum_i a_{i\tau}} \leq 2t/\sqrt{T}.$$

Второй переход здесь вытекает из неравенства между нормами в пространствах $l_1$ и $l_2$, доказательство которого мы предоставляем слушателю в качестве упражнения. Мы видим, что если $t = o(\sqrt{T})$, то Ахиллес проиграл, потому что он не сможет отличить положение классической черепахи $f^T$ от иных. То есть невозможно получить более чем квадратичное квантовое ускорение для большинства классических алгоритмов.

Есть и нижние границы квантовой сложности иного типа. Например, устанавливающие, что квантовый компьютер не может решить переборную задачу существенно быстрее, чем по алгоритму Гровера (см. [14], [15]), а также, что любой квантовый алгоритм, более быстрый, чем гроверовский, должен почти для всех переборных задач давать ошибочный ответ (см. [13]).

Более детальное рассмотрение квантового вычисления [6] показывают, что Ахиллес в большинстве случаев, вообще не способен обогнать черепаху классического компьютера.

*Теорема ([6]).*

*Вероятность того, что итерация длины $O(N^{1/7})$ произвольно выбранного из равномерного распределения "черного ящика" $\mathcal{F}$ может быть ускорена хотя бы на единицу на квантовом компьютере, стремится к нулю при размерности пространства, стремящегося к бесконечности.*

Таким образом, квантовое ускорение классических вычислений является редким феноменом. Оно имеет место для алгоритмов типа перебора, тех самых, которые допускают ускорение с помощью распараллеливания (см. [16]). Задача типа итераций, рассмотренная нами, относится к типу GMSP (см. [17]) и в общем случае не допускает такого типа ускорения; для нее квантовый компьютер оказывается, в подавляющем большинстве случаев, не лучше классического.

Это - косвенное свидетельство того, что квантовый и классический параллелизм близки друг другу. Что подкрепляет уверенность в том, что и попытки найти какие-либо формы детерминистического описания квантовых эволюций, предпринимавшиеся нами в третьей главе, не являются только лишь математическими упражнениями.

# 5 Лекция 5. Дискретизация функций и операторов

Для реализации главного назначения квантового компьютера - моделирования реальных микро процессов, нам надо научиться переходить от их стандартного, аналитического описания к дискретному. В копенгагенской квантовой механике состояние описывается волновой функцией $\Psi(x,t)$, для которой справедливо уравнение

Шредингера $i\hbar\dot{\Psi} = H\Psi$, где $H$ - непрерывный оператор энергии, который для единичной частицы в обычном пространстве $(x, y, z)$ имеет вид

$$H = \frac{p^2}{2m} + V(x),\ p = \frac{\hbar}{i}\nabla,\ \nabla = grad = \left(\frac{\partial}{\partial x}, \frac{\partial}{\partial y}, \frac{\partial}{\partial z}\right) \tag{42}$$

где $p$ - оператор импульса частицы, $V$ - потенциал, в котором она движется.

Главный этап - представление так называемой волновой функции к вектору состояния.

Если имеется абстракция - волновая функция $\Psi(x)$ от непрерывной переменной $x$, ее можно сделать реалистичной, если ввести дискретное множество возможных значений переменной $x = x_0, x_1 = x_0 + dx, x_2 = x_0 + 2dx, ..., x_N = x_0 + Ndx$, а затем представить приближенно непрерывную функцию $\Psi(x)$ как

$$\Psi(x) \approx \sum_{j=0}^{N-1} \Psi(x_j) d_j(x), \tag{43}$$

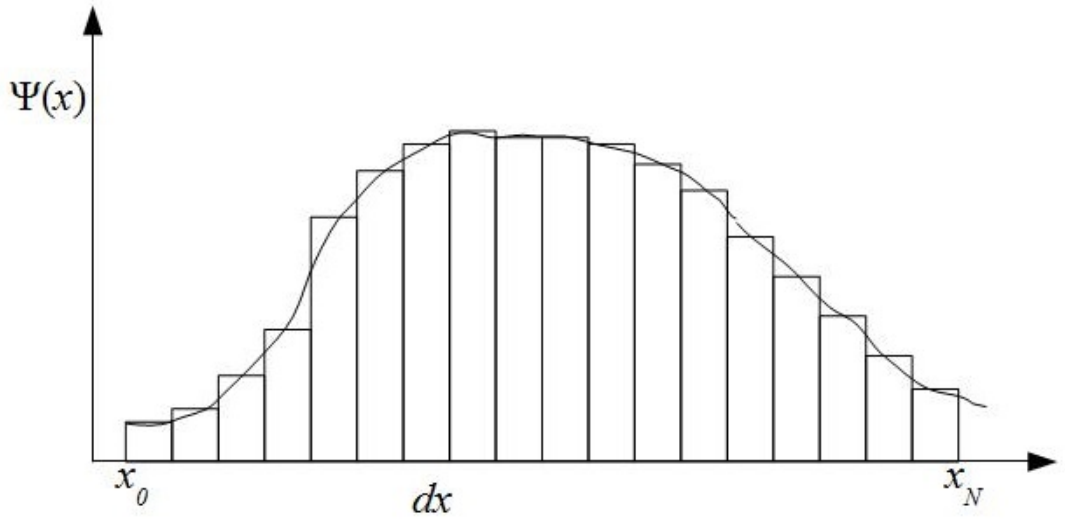
где $d_j(x)$ - характеристическая функция $j$- го отрезка $[x_j, x_{j+1}],\ j = 0, 1, ..., N-1$ (см. рисунок 39). Учитывая скалярное произведение непрерывных функций $\langle f|g\rangle = \int\limits_R \bar{f}g\, dx$, мы можем пронормировать ортогональные векторы $d_j$, получив ортонормированный базис $|j\rangle = d_j/\sqrt{dx}$, и определив $\lambda_j = \Psi(x_j)\sqrt{dx}$, придем к представлению нашей функции в виде вектора состояния $|\Psi\rangle = \sum\limits_{j=0}^{N-1} |j\rangle$. Для волновой функции, определенной на пространстве $R^2$ или $R^3$, вместо $\sqrt{dx}$ будет стоять $\sqrt{dx^2}$ или $\sqrt{dx^3}$ соответственно.

Переход от дискретной записи к непрерывной состоит в том, что все суммы заменяются интегралами, а переменные суммирования - переменными интегрирования. Например, формула (43) превратится в $\Psi(x) = \int\limits_R \Psi(y)\delta_y(x)dy$ где $\delta_y(x)$ есть предел функций $d_j(x)$ при $dx \to 0$, так что $x_j \to y$. Такого предела, конечно, не существует в математическом анализе - среди обычных функций, так как при $dx \to 0$ функция $d_j(x)$ превратится в иглу бесконечно высокую и бесконечно тонкую. Это - так называемая обобщенная функция Дирака (см. параграф 1.5, упражнение 3).

Эта процедура дискретизации всегда будет иметься в виду по умолчанию. Более того, совершая линейное преобразование $\mathcal{D}$ координаты $x$, что эквивалентно выбору новых единиц измерения длины, мы можем считать, что отрезок определения волновой функции $[x_0, x_N]$ совпадает с отрезком $[0, 1]$, а $N = 2^n$, так что $x_j = j/N,\ j = 0, 1, ..., N-1$ и будем записывать приближенное, с точностью $1/N$, значение координаты $x$ в виде последовательности бинарных знаков двоичного разложения $j = \sum\limits_{k=1}^{n} 2^{n-k} e_k$, то есть в виде бинарной строки $|e_1 e_2 ... e_n\rangle,\ e_k \in \{0, 1\}$.

Любая такая строка есть базисное состояние системы $n$ кубитов (квантовых битов), поэтому данное дискретное представление волновых функций будем называть кубитовым. В кубитовом представлении у волновой функции не будет никакой физической размерности. Размерным будет только оператор $\mathcal{D}$ перехода к кубитовому представлению от физической непрерывной функции $\Psi(x)$, и базисные состояния $|j\rangle$.

Рис. 39: Дискретизация непрерывной функции.




*Слушае предлагается потренироваться, оперируя натуральными числами в бинарной записи: перечислять, складывать, умножать и делить. Если верно то, что Природа говорит с нами на языке математики, то основой этого языка являются именно операции с целыми числами в бинарной записи.*

## 5.1 Физические величины как наблюдаемые

Любой физической величине, кроме времени, соответствует в квантовой теории определенная наблюдаемая. При этом собственные значения этой наблюдаемой будут возможными значениями данной величины, а собственное состояние, в котором она имеет данное значение, есть состояние, в котором данная величина определена однозначно - именно данным значением.

Рассмотрим три примера: наблюдение координаты, импульса и энергии.

## 5.2 Наблюдение координаты

Рассмотрим только случай одномерной частицы, обобщение на трехмерный случай не представляет особых затруднений. Наблюдаемая будет оператором умножения волновой функции на ее аргумент- координату, что в непрерывном представлении имеет вид: $x: \ f(x) \to xf(x)$. Вспоминая переход (43) от непрерывного представления вектора состояния к дискретному, можно непосредственно проверить, что в кубитовом представлении матрица оператора координаты - диагональная, и по диагонали стоит арифметическая прогрессия $0, 1/N, ..., (N-1)/N$. Эту матрицу мы обозначим через $x_{discr}$. Таким образом, собственными состояниями данного оператора будут базисные состояния $n$ - кубитной системы, которые мы договорились обо-

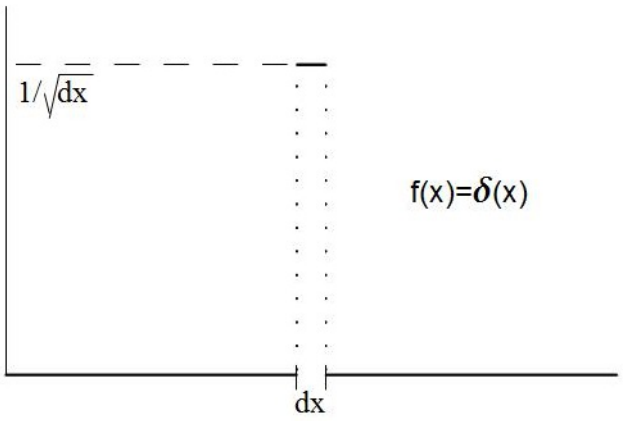



Рис. 40: Собственная функция оператора координаты. Дискретная форма

значать бинарными разложениями натуральныых чисел $|0\rangle, |1\rangle, ..., |N-1\rangle$, и будем при записи отождествлять их с самими этими числами. Собственными значениями их будут сами числа $0, 1/N, ..., (N-1)/N$. Эти базисные состояния по определению составляют ортонормированный базис пространства $C^N$ системы $n$ кубитов.

В непрерывной форме им соответствуют так называемые дельта-функции Дирака $\delta_\lambda$, которые определяются как линейные функционалы вида $\delta_\lambda : \ f \to f(\lambda)$. Эти функционалы не являются обычными функциями, их геометрическое представление - бесконечно высокие иглы, растущие из точек $\lambda$. Они не могут быть нормированы, их нельзя умножать друг на друга. Это еще один пример того, как математический анализ вступает в противоречие с квантовой физикой. Противоречие возникает из-за непрерывного характера переменной $x$; как только мы проведем дискретизацию, это противоречие исчезнет, а "иглы" превратятся в высокие ступеньки $\delta_j(x)$ конечной величины $1/\sqrt{dx}$ где $dx$ - выбранное зерно пространственного разрешения (см. рисунок 40).

Элементом дискретного пространства $C^N$ будут вектора состояния $|\Psi\rangle$ вида $|\Psi\rangle = \sum_{j=0}^{N-1} |j\rangle$, а сопряженное пространство линейных функционалов будет состоять из строк вида $\langle\Psi|$, действующих на состояния естественным образом: $\langle\Psi| : \ |\Phi\rangle \to \langle\Psi|\Phi\rangle$, что делает пространство состояний $C^N$ изоморфным сопряженному (что нарушается в случае непрерывного формализма).

Дискретизация снимает все противоречия физики с математическим аппаратом, и потому мы всегда будет вести речь о конечномерных пространствах, даже используя интегрирование и дифференцирование как приближенные приемы вычисления; такие приемы мы всегда будем контролировать на абсолютно необходимую возможность дискретизации.

## 5.3 Квантовый оператор Фурье и наблюдение импульса

Квантовый оператор импульса в одномерном случае имеет в непрерывном формализме вид

$$p: \ f(x) \to \frac{\hbar}{i}\nabla f \tag{44}$$

Его собственные функции есть комплексные экспоненты $exp(ipx/\hbar)$, с собственными значениями $p$.

*Докажите, что этот оператор эрмитов, используя эквивалентное определение эрмитовости матрицы A:* $\langle i|A|j\rangle = \langle j|\bar{A}|i\rangle$ *(черта обозначает комплексное сопряжение); примените формулу вычисления скалярного произведения через интеграл.*

Для построения корректной дискретной формы оператора импульса следует воспользоваться преобразованием Фурье,

$$f(x) \to \frac{1}{\sqrt{2\pi\hbar}}\int\limits_R exp(-ipx/\hbar)f(x)dx = \phi(p) \tag{45}$$

переводящим функции (44) в дельта-функции Дирака, а также обратным преобразованием Фурье

$$\phi(p) \to \frac{1}{\sqrt{2\pi\hbar}}\int\limits_R exp(ipx/\hbar)\phi(p)dp = f(x) \tag{46}$$

делающим обратный переход.

*Слушателю предлагается убедиться в этом, приняв упрощающее вычисление равенство* $\hbar = 1$*, которое достигается переходом к подходящей системе физических единиц. Подставьте в формулу* (45) *собственную функцию оператора импульса* $f_{p_0}(x) = e^{ip_0x/\hbar}$*, и произведите интегрирование по конечному интервалу вида* $(-A, A)$*. Интеграл берется в конечной форме, и результат при* $A \to +\infty$ *будет все больше и больше напоминать иглу, опирающуюся на точку* $p = p_0$*, и уходящую неограниченно в бесконечность. Таким образом, собственная функция оператора импульса переведется в собственную функцию оператора координаты; название аргументов* $x$ *или* $p$ *не играет никакой роли. Проделайте то же самое с обратным преобразованием. Но при интегрировании по всей прямой получится расходимость; более того, ни дельта-функцию, ни комплексную осцилляцию* $exp(ipx)$ *нельзя пронормировать. Все поправляется только переходом к дискретному представлению.*

Дискретная форма преобразования Фурье и обратного к нему представляет собой операторы, действующие на базисные состояния $n$- кубитной системы так:

$$\begin{aligned} QFT &: |a\rangle \to \tfrac{1}{\sqrt{N}}\sum\limits_{b=0}^{N-1} exp(-2\pi iab/N)|b\rangle \\ QFT^{-1} &: |b\rangle \to \tfrac{1}{\sqrt{N}}\sum\limits_{a=0}^{N-1} exp(2\pi iab/N)|a\rangle \end{aligned} \tag{47}$$

Оба эти взаимно обратные операторы (доказать!) при линейном продолжении на все пространство квантовых состояний $C^N$ дадут унитарные операторы - Фурье и обратного к нему.

Для приложений удобно считать, что для переменной $a$ число $a/\sqrt{N}$ является координатой, принадлежащей отрезку $[0, \sqrt{N}]$ (постоянную Планка в надлежащей

системе единиц можно считать единицей). Тогда $b/\sqrt{N}$ должна быть связана с импульсом. Естественно допустить, что импульс принадлежит отрезку $[-\sqrt{N}/2, \sqrt{N}/2]$, поскольку частица, расположенная на отрезке $[0, \sqrt{N}]$, может двигаться в обе стороны. Поэтому импульс должен быть равен $\sqrt{N}(b/N - 1/2)$.

Соответственно, дискретная форма оператора импульса будет $N$- мерным эрмитовым оператором $p_{discr} = QFT^{-1}\sqrt{N}(x_{discr} - I/2)QFT = A^{-1}QFT^{-1}\sqrt{N}x_{discr}QFT\ A$, где диагональный оператор $A = diag(exp(\pi ia))_{a=0,1,...,N-1}$. Его собственные вектора будут иметь вид $A^{-1}QFT^{-1}|a\rangle$, и их собственными значениями будут числа $\sqrt{N}(a - 1/2);\ a = 0, 1/N, ..., (N-1)/N$.

Итак, в дискретном представлении все собственные состояния основных операторов нормированы на единицу, и нет никаких противоречий с математическим анализом. Мы здесь использовали аналитическую технику непрерывных преобразований Фурье для корректной записи ее дискретного аналога. Нетрудно показать, что все полезные свойства преобразования Фурье: переход от дифференцирования (применения оператора импульса) к умножению на константу а также выявление скрытого периода комплексной экспоненты сохранятся при переходе от непрерывной формы к дискретной, так что мы можем пользоваться именно дискретными операторами в конечномерных пространствах во всех физических задачах, связанных с квантовой теорией.

Операторы (47) называют прямым и обратным квантовым преобразованием Фурье. С их помощью можно построить полиномиальный квантовый алгоритм, находящий разложение числа на нетривиальные множители ([18]).

## 5.4 Реализация квантового преобразования Фурье на квантовом компьютере

Мы будем реализовывать обратное преобразование Фурье в виде

$$QFT^{-1} : |a\rangle \to \frac{1}{\sqrt{N}} \sum_{b=0}^{N-1} exp(2\pi iab/N)|b\rangle.$$

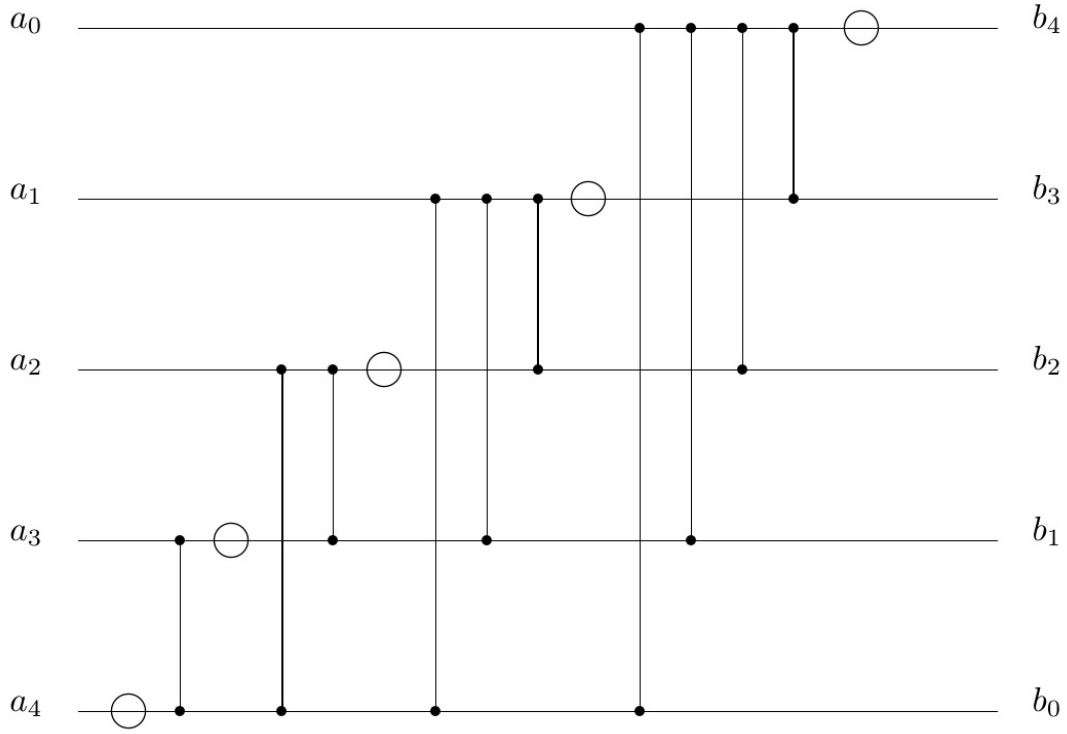
Договоримся представлять целое число вида $a = a_0 + a_1 2 + \ldots + a_{l-1}2^{l-1}$ базисным состоянием $|a_0\ a_1\ \ldots\ a_{l-1}\ \rangle$ и располагать все $a_j$ сверху вниз. Такое же соглашение примем и для выхода, только бинарные знаки $b_j$ числа $b = b_0 + b_1 2 + \ldots + b_{l-1}2^{l-1}$ будем писать в обратном порядке - снизу вверх.

Окружности здесь обозначают преобразование Адамара $(\sigma_x + \sigma_z)\sqrt{2}$, двухкубитовые операции имеют вид:

$$U_{k,j} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\pi/2^{k-j}} \end{pmatrix},\ k > j. \tag{48}$$

Чтобы убедиться в этом, мы рассмотрим амплитуду перехода от базисного состояния $a$ к базисному состоянию $b$. Это понятие законно, так называется соответствующий элемент матрицы рассматриваемого оператора. Здесь нам придется набраться

Рис. 41: Реализация $QFT^{-1}$ в виде массива квантовых гейтов.




терпения - подсчет идейно простой, но требует тщательности. Сначала заметим, что модули всех таких амплитуд одинаковы и, так же как в обратном преобразовании Фурье, равны $1/2^{l/2}$, так что следить надо только за фазовым сдвигом, т.е. за аргументом $\phi$ комплексной амплитуды $e^{i\phi}$. Мы будем учитывать этот набег фазы, суммируя вклады от преобразований Адамара с вкладами от двухкубитных фазовых сдвигов.

Введем для упрощения счета такое сокращенное обозначение: $b'_j = b_{l-1-j}$, $j = 0, 1, \ldots, l-1$ - это понадобится для того, чтобы в нужный момент учесть обратный порядок расположения бинарных разрядов в $a$ и $b$. Представим себе, как меняются состояния при продвижении слева направо по проводам нашей схемы.

Собственно переход от $a$ к $b$ происходит только при совершении операции Адамара, двухкубитные операции диагональны и базисные состояния не меняют, добавляя только слагаемые к фазе. Вклад от операции Адамара будет таким: $\pi a_j b'_j$. Это число не равно нулю только если оба $j$-х разряда наших входных и выходных чисел равны 1, что в точности соответствует определению преобразования Адамара. Вклад от двухкубитовой операции при $j < k$ будет $\pi a_j b'_k / 2^{k-j}$, потому что состояние $a$ меняется на $b$ только при прохождении устройства Адамара, а как видно из рисунка 41, такая двухкубитовая операция совершается в момент, когда $j$-й кубит еще в состоянии $a_j$, а $k$-й - уже в состоянии $b'_k$. Суммируя все эти слагаемые фазового сдвига, и учитывая, что целое кратное $\pi$ можно вообще в расчет не принимать, получаем вот

что:

$$\begin{array}{l}\pi \sum\limits_{l>k>j\geq 0} \frac{a_j b'_k}{2^{k-j}} + \pi \sum\limits_{l>j\geq 0} a_j b'_j = \\ 2\pi \sum\limits_{l>j+k\geq 0} \frac{a_j b_k 2^{j+k}}{2^l} = \\ 2\pi \sum\limits_{l>j,k\geq 0} \frac{a_j b_k 2^{j+k}}{2^l} + 2\pi z = \\ \frac{2\pi}{2^l} \sum\limits_{l>j\geq 0} a_j 2^j \sum\limits_{l>k\geq 0} b_k 2^j + 2\pi z = \frac{2\pi ab}{2^l} + 2\pi z.\end{array} \tag{49}$$

для некоторого натурального $z$. Это как раз то, что требуется в определении обратного преобразования Фурье, так как сдвиг фазы на $+2\pi z$ не меняет комплексного числа. Если нам понадобится совершить прямое преобразование, достаточно обратить порядок функциональных элементов в рассматриваемой схеме и поставить знак минус перед фазовым сдвигом в определении двухкубитных операций.

А теперь посмотрим на то, что мы только что совершили. Построенная нами схема, реализующая преобразование Фурье, содержит порядка $l^2$ функциональных элементов. Заметим, что если мы не будем гнаться за точностью этого преобразования, то можно будет отбросить все двухкубитные операции, в которых участвуют слишком далекие друг от друга кубиты. Действительно, знаменатель в $\pi/2^{k-j}$ для них делает всю дробь пренебрежимо малой, экспонента будет почти единицей, т.е. такие преобразования почти единичны и их можно отбросить. Схема тогда значительно упростится - ее размер вообще будет линейным - порядка $C\ l$, где константа $C$ будет, конечно, зависеть от выбранной нами точности.

## 5.5 Алгоритм Залки-Визнера

Алгоритм GSA, изученный нами, оперирует с кубитами, переводя их классические (базисные) состояния в квантовые с помощью оператора Адамара. Этот прием иллюстрирует важнейшие особенности описания эволюции на квантовом уровне, однако с большой потерей точности. Реальная частица может занимать несколько классических положений, а не только два, как кубит.

Мы рассмотрим алгоритм Z моделирования квантовой унитарной эволюции, предложенный в работе [19] (см. также [20]), который фактически обобщает GSA на случай многих классических состояний каждой частицы. В нем вместо оператора Адамара, "размазывающего" амплитуду по двум возможным состояниями кубита, на каждом шаге вычисляется волновая функция частицы, способной находиться во многих классических пространственных состояниях.

Алгоритм Z отличается от прямого решения уравнения Шредингера на классическом компьютере лишь тем, что амплитуды $\lambda_j$ текущего квантового состояния $|\Psi(t)\rangle$ не вычисляются напрямую, а моделируются квантовой динамикой кубитов в дискретном представлении $|j\rangle = |0\rangle, |1\rangle, ..., |N-1\rangle$ пространства классических состояний в вычислительной памяти $n$ кубит, $N = 2^n$, при котором волновая функция представляется в виде $|\Psi(t)\rangle = \sum\limits_{j=0}^{N-1} \lambda_j |j\rangle$.

Напомним, что реальное одномерное пространство классических состояний сначала переводится линейным преобразованием $\mathcal{D}$ в отрезок $[0, \sqrt{N}]$, который затем

дискретизируется кубитовым представлением чисел с точностью приближения $1/N$: $x_k \approx k/N,\ k = 0, 1, ..., N-1$. Такое представление волнового вектора требует соответствующей дискретизации операторов. Дискретная форма оператора координаты $x_{discr}$ и оператора импульса $p_{discr}$ была рассмотрена в параграфе 5.3.

Оператор потенциальной энергии $V$ при этом становится диагональной матрицей $diag(V(X_0), V(X_1), V(X_2), ..., V(X_{N-1}))$, $X_k = \sqrt{N}x_k$ со значениями потенциальной энергии на главной диагонали, диагональное представление оператора кинетической энергии (в пространстве своих собственных векторов оператора импульса) также диагонально: $K_{diag} = diag(-\hbar^2 p_0^2/2m), -\hbar^2 p_1^2/2m), -\hbar^2 p_2^2/2m), ..., -\hbar^2 (p_{N-1})^2/2m))$, где $p_k = \sqrt{N}(x_k - 1/2)$, так что в координатном базисе кинетическая энергия представится оператором

$$K = A^{-1} QFT^{-1}\ K_{diag}\ QFT\ A, \tag{50}$$

где $A = diag(exp(\pi i a))_{a=0,1,...,N-1}$.

Тогда часть эволюции, соответствующая оператору потенциальной энергии $exp(-iVt/\hbar)$ при простом виде потенциала будет реализуемо как квантовая подпрограмма, квантовое преобразование Фурье может быть также реализовано по изученной нами схеме Шора, и оператор, соответствующий кинетической энергии и времени $t$ также может быть реализован в виде квантовой подпрограммы. Применяя приближение Троттера

$$exp(A + B) \approx [exp(A\ dt)\ exp(B\ dt)]^{t/dt},$$

мы получим алгоритм Z вычисления эволюции в виде:

$$U_t = exp(-\frac{i}{\hbar}Ht) \approx [exp(-\frac{i}{\hbar}K\ dt)\ exp(-\frac{i}{\hbar}V\ dt)]^{t/dt} \tag{51}$$

Мы получаем модель унитарной динамики с квадратичным замедлением по сравнению с реальным процессом. *Докажите это, используя разложение экспоненты до первого порядка по dt. Зафиксируйте порядок ошибки $\epsilon = const$ и, применяя точность приближения Тейлора для экспоненты, установите число операций, нужное для нахождения приближения результирующего состояния. Это число будет равно $t/dt$, откуда и получится квадратичное замедление по времени по сравнению с временем $t$ реального процесса.*

Алгоритм Z может быть обобщен на случай нескольких частиц. При этом преобразование Фурье надо применять по каждой координате каждой частиц по отдельности. Этот алгоритм требует памяти, растущей пропорционально первой степени от числа реальных частиц, но не может использоваться для управления сложной системой, так как он предполагает априорное моделирование процесса с переносом результата на новый аналогичный процесс, тогда как в реальности любой сложный процесс не является в точности воспроизводимым, и потому управление им требует моделирования именно в реальном времени.

Сравнивая это вычисление с вычисление по алгоритму GSA, которое имеет вид $G^\tau = (-I_{\tilde{0}} I_{x_{tar}})^\tau$, мы видим полную аналогию с формулой (51). При этом роль оператора Уолша-Адамара в представлении $I_{\tilde{0}} = WH \cdot I_{\tilde{0}} \cdot WH$ играет квантовый оператор Фуре в (50). Для одного кубита оператор Фурье как раз и совпадает с оператором Адамара, так что алгоритм Z может считаться обобщением GSA на случай многих классических состояний каждой из частиц.

Итак, мы видим, что имеется два приема сверхбыстрой, недоступной классическому компьютеру, концентрации амплитуды на целевом неизвестном состоянии. Первый - алгоритм GSA, второй - квантовое преобразование Фурье. Мы видим, что самым грубым приближением преобразования Фурье является как раз оператор Уолша-Адамара, что сводит эти два приема воедино. Быстрый алгоритм факторизации целых чисел Шора фактически использует те же фундаментальные особенности квантовой динамики, что и GSA. Арсенал квантовых методов ускорения классических вычислений ограничен, таким образом, этим общим приемом концентрации ампитуды для задач переборного типа, в соответствии с общим результатом [6]. В задачах, которые не ускоряются распараллеливанием, квантовый компьютер не проявляет преимуществ по сравнению с классическим, за исключением только лишь удивительного его свойства нелокальности.

## 5.6 Проявление скрытых периодов в помощью QFT

Мы напомним определение QFT:

$$\mathrm{QFT}: \ |a\rangle \longrightarrow \frac{1}{\sqrt{N}} \sum_{b=0}^{N-1} e^{-\frac{2\pi i \ ab}{N}} |b\rangle, \qquad \mathrm{QFT}^{-1}: \ |a\rangle \longrightarrow \frac{1}{\sqrt{N}} \sum_{b=0}^{N-1} e^{\frac{2\pi i \ ab}{N}} |b\rangle. \qquad (52)$$

Мы продемонстрируем возможностси квантового компьютера в проявлении скрытых периодов - собственных частот произвольного унитрного оператора $U$. Идея состоит в том, чтобы применять оператор $U$ столько раз, сколько указано во вспомогательном регистре:

$$U_{cond}|x,\alpha\rangle \longrightarrow |U^{\alpha} \ x,\alpha\rangle.$$

Если у нас есть схема функциональных элементов, реализующих $U$, мы можем построить квантовый алгоритм, реализующий $U_{cond}$.

Пусть собственные значения $U$ имеют вид

$$w_k = e^{2\pi i \omega_k}, \qquad (53)$$

где собственные частоты $\omega_k \in [0,1)$ - это всегда именно так. Мы для простоты предположим, что эти собственные частоты имеют вид $\omega_k = c_k/N$ где $c_k \in \{0,1,...,N-1\}$.

Итак, мы занимаемся поиском собственных частот оператора $U$. Эта частота получится в результате измерения вспомогательного регистра из $n$ кубит, обозначаемого через $\alpha$, предполагая, что выполнено соотношение (53). Интересующиеся общим случаем могут обраатитья к книге [21]. Наш компьютер будет работать с двумя регистрами - основным, где находится аргумент $U$, и вспомогательного, в котором будет содержаться бинарное разложение собственной частоты $U$. В начале мы выберем произвольное состояние $|\xi,\bar{0}\rangle$, где $\xi = \sum\limits_k x_k|\psi_k\rangle$, и $|\psi_k\rangle$ - собственные состояния $U$, соответствующие собственным частотам $\omega_k$.

Описываемый прием был сформулирован Абрамсом и Ллойдом, и он состоит в следующем. Надо инициализировать анциллу начальным состоянием алгоритма Гровера $|\alpha\rangle = |\tilde{0}\rangle = \frac{1}{\sqrt{N}} \sum\limits_{j=0}^{N-1} |j\rangle$ применить оператор

$$\mathrm{QFT}_2 \ U_{cond}. \qquad (54)$$

Начальное состояние будет иметь вид: $\frac{1}{\sqrt{N}}\sum_k\sum_{\alpha=0}^{N-1} x_k|\psi_k,\alpha\rangle$. Затем оператор условного применения $U$, ввиду того что $\psi_k$ являются собственными векторми $U$ даст $U_{cond}|\psi_k,\alpha\rangle = |U^\alpha\psi_k,\alpha\rangle = e^{2i\pi\omega_k\alpha}|\psi_k,\alpha\rangle$, таким образом, все состояние после применения $U_{cond}$ приобретет вид $\frac{1}{\sqrt{N}}\sum_k x_k\sum_\alpha e^{2i\pi\omega_k\alpha}|\psi_k,\alpha\rangle$. Наконец последнее применение QFT приведет к:

$$\frac{1}{N}\sum_k x_k\sum_c\sum_{\alpha=0}^{N-1} e^{2i\pi\alpha(\omega_k-\frac{c}{N})}|\psi_k,c\rangle. \tag{55}$$

Если $c$ является последовательностью бинарных знаков $\omega_k$, то степень экспоненты нулевая и мы после суммировния по $\alpha$ получим сумму единиц в количестве $N$ и коэффициент при этом состоянии $c$ будет $x_k$; сумма квадртов модулей всех $x_k$ равна 1. Тогда для всех прочих $c$ коэффициент будет нулевой. Это можно проверить непосредственно суммируя геометрическую прогрессию: $\sum_{\alpha=0}^{N-1} e^{2i\pi\alpha\beta} = 0$.

Наша процедура даст состояние

$$\sum_k x_k|\psi_k,\omega_k\rangle,$$

где $\omega_k$ есть бинарная запись. Если мы теперь будем измерять результирующее состояние, то в последнем регистре мы получим бинарное разложение собственных частот оператора $U$. В частности, если начальное состояние было собственным для оператора $U$, в последнем регистре будет стоять его собственная частота.

## 5.7 Факторизация

Общий метод нахождения собственных значений, представленный в предыдущем параграфе, был изобретен фактически Шором для частного случая,возникающего при фактризации целых чисел. Проблема факторизации - разложения на нетривиальные сомножиели произвольного целого числа, относитася к важным вычислительным задачам. Сложность решения этой задачи гарантирует секретность так называемой RSA схемы шифрования, применяемого, например, для защиты операционной системы Windows. Наилучший известный алгоритм факторизации целого числа с бинарной записью длины $n$ требует времени порядка $e^{a\ n^{1/3}}$. Эта проблема приналежит к числу предположительно сложный проблем, так как не доказана невозможность ее решения за полиномиальное по $n$ время. Известные классические методы теряют эффективность уже для около 200 разрядов. Квантвоый компьютер с 1000 кубитами и частотой процессора 1 GHz, будь он построен, способен был бы факторизовать числа почти с той же скоростью, что и умножение, что поставило бы под сомнение большую часть современной криптографии.

Алгоритм Шора имеет также большое теоретическое значение. Это первый квантовый алгортм, использующий способность концентрировать амплитуду на целевом состоянии с помощью преобразования Фурье, давая огромный выигрыш во времени по сравнению с классическим компьютером - для задачи факторизации.

Пусть нам дано целое число $q$, которое надо разложить на множители нетривиальным образом, то есть найти $q_1$, $q_2$, такие что $q = q_1q_2$. Это сводится к задаче

поиска минимального мультипликативного периода $r$ произвольного натурального числа $y$ по модулю $q$: $y^r \equiv 1\ (mod\ q)$. Вкратце, эта сводимость выглядит так. Пусть у нас есть метод нахождения $r$. С ненулевой вероятностью это число будет четным. Тогда мы имеем: $y^r - 1 = (y^{r/2} - 1)(y^{r/2} + 1) \equiv 1\ (mod\ q)$, и один из сомножителей будет делителем $q$. Итак, мы должны только быстро найти $r$ по заданным $q$ и $y$. Эта задача сводится к задаче поиска собственной частоты оператора $U$, который является оператором умножения на $y$.

Выберем $n$ так что $2^{n-1} \leq q < 2^n$ и будем работать с квантовой памятью из $n$ кубитов. Рассмотрим оператор $U$: $U|x\rangle \longrightarrow |yx\ (\mathrm{mod}\ q)\rangle$, где $yx$ есть численное умножение. чтобы он действовал на всех базисных векторах, а не только на числах меньших $q$, мы условимся, чтто на числах: $q, q+1, \ldots, 2^n - 1$ он действует как идентичный оператор. десь возникает небольшая трудность: этот оператор может не быть унитарным. Если $y$ и $q$ имеют общий делитель, некоторые элементы могут "склеиться". Дл исключения такой ситуации мы примем, что эти числа взаимно просты: $(y, q) = 1$. Так как мы выбираем $y$ произвольно, это предположение выполнится с некоторой ненулевой вероятностью.

Теперь все готово и мы применим технику квантового вычисления. Собственные векторы $U$ имеют вид либо $|q\rangle, |q+1\rangle, ...$, либо $\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp(-2\pi ikj/r)|y^j\ (\mathrm{mod}\ q)\rangle$ и соответственные собственные значения будут либо 1, либо $\exp(2\pi ij/r)$, что проверяется непосредственно. Если мы применим процедуру проявления собственных частот, описанную в предыдущем параграфе, мы получим значения дробей $j/r$ в бинарной форме, из которой по методу цепных дробей (см. in [22]) мы найдем $r$. Мы будем знать $j/r$ с точностью $1/N$. Эта дробь с неисчезающей вероятностью будет несократимой при случайном выборе $y$ и состояния $\xi$, что позволяет узнать $r$ и точно. Повторяя данную процедуру многократно, мы сможем опредеить $r$ точно с вероятностью, сколь уодно близко к единице. За деталями можно обратиться к оригинальной статье Шора [18], а также к работе [21]. Это и есть схема алгорима Шора.

Теперь оценим грубо сложность данного алгоритма. Квантовое преобразование Фурье требует порядка $n^2$ операций; это число может еще быть доведено до $n$, если мы применим приближенное квантовое преобразование Фурье, отбросив слишком "длинные" двухкубитные гейты, при больших $j - k$. Такае гейты мало отличаются от тождественного оператора, и отбросив их мы получим удовлетворительное приближение. Однако преобразование Фурье не является самой трудоемкой операцией данного алгоритма. Проблема заключается в преобразовании $U_{cond}$. В общем случае она требует порядка $N$ действий, так что мы не получим никакого выигрыша по сравнению с прямым перебором вариантов для факторизации.

Однако в нашем случае можно реализовать $U_{cond}$ гораздо быстрее. А именно, для умножения на $y^\alpha$ можно делать последовательные умножения на: $y, y^2, y^4, \ldots$. Каждая такая серия даст некоторый остаток при делении на $q$. Мы достигнем ближайшей к $q$ степени двойки: $2^{l_1}$. Беря затем остаток $q/2^{l_1}$ и делая с ним то же самое, мы в конце концов реализуем умножение на $y^q$ с числом умножений порядка длины бинарной записи $q$. Каждое умножение требует еще $log^2 q$ элементарных действий, и мы реализуем $U_{cond}$ в нашем случае за время $O(\log^3 q)$.

Это и есть грубая оценка сложности алгоритма Шора, более точная оценка со-

держится в работе [18].

### 5.8 Решение проблемы дискретной оптимизации

Мы продолжим перечень примеров быстрых квантовых алгоритмов, основанных на комбинации приемов GSA и квантового преобразования Фурье. Рассмотрим естественное обобщение проблемы поиска: нахождение экстремума целочисленно функции. Надо нати максимум или минимум целочисленной функции $f : \{0,1\}^n \longrightarrow \{0,1\}^n$. Классическое решение этой задачи требует порядка $N = 2^n$ действий.

Квантовое решение этой задачи основано на схеме Гровера. Мы ищем точку максимума путем последовательных приближений. А именно, мы упорядочиваем все аргументы в порядке возрастания функции $f$ на них: $f(x_0) \leq f(x_1) \leq \ldots \leq f(x_{N-1})$. На каждом шаге $j$ начальным значением будет некоторое $x_{j_k}$. Мы применяем схему GSA для неизвестного числа решений с оракулом, принимающим значение 1 в точности на аргументах $x_j$, для которых $f(x_{j_k}) < f(x_j)$, то есть на $x_{j'}$, $j' > j_k$. После периодических измерений и проверки корректности мы найдем следующее значение $x_{j_{k+1}}$ и т.д., вплоть до момента, когда мы достигнем $x_{N-1}$. Заметим, что эта схема не эквивалентна классическому алгоритму упорядочения, так как здесь используется квантовый поиск аргумента с большим значением функции, чем на предыдущем шаге. Детальный анализ (см. [23]) показывает, что сложность такого алгоритма будет иметь порядок $\sqrt{N}$, то есть даст то же ускорение, что и GSA.

## 6 Лекция 6. Адиабатические квантовые вычисления

До сих пор мы рассматривали вычисления операционного типа, состоящие из последовательных применений квантовых гейтов. Существуют и непрерывные квантовые вычисления, называемые адиабатическими. Они основаны на медленном изменении управляющего гамильтониана системы кубитов. При этом основное состояние исходной системы будет переходить в основное состояние измененной системы - в этом суть адиабатической теоремы.

Рассмотрим уравнение Шредингера с меняющимся гамильтонианом $H(t)$

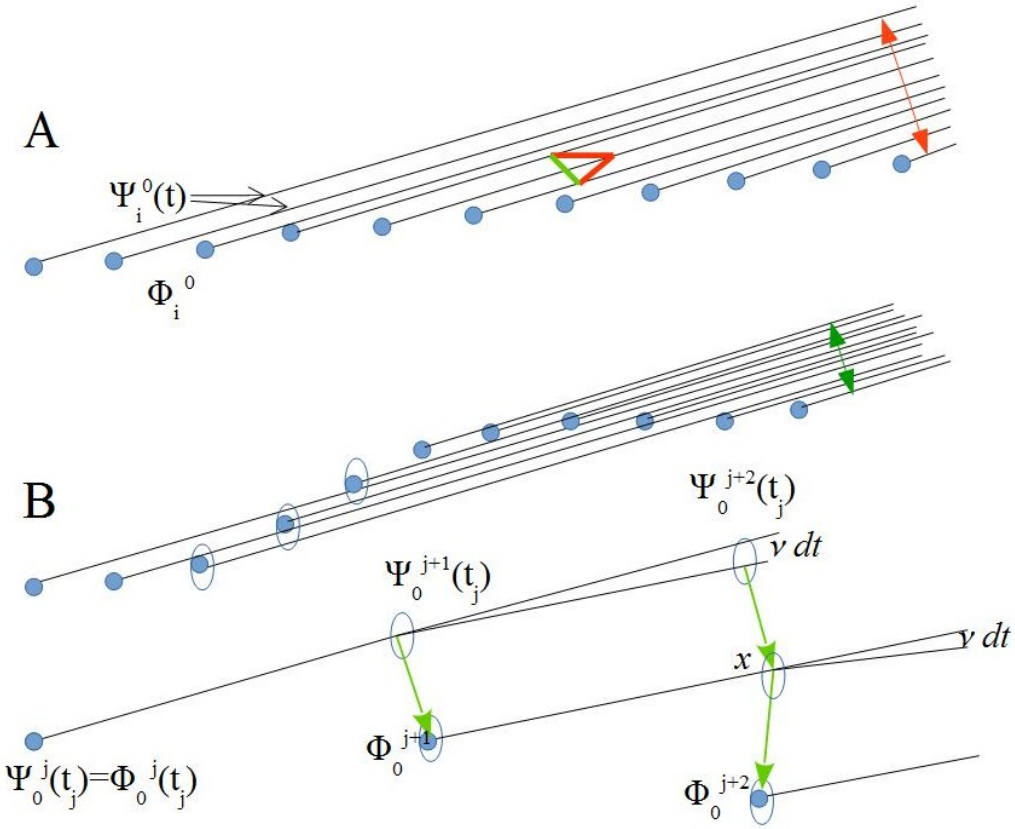
$$i\hbar|\dot{\Psi}\rangle = H(t)|\Psi\rangle. \tag{56}$$

Его решение будет так же, как и в стационарном случае, задаваться формулой

$$|\Psi(t)\rangle = exp(-\frac{i}{\hbar}H(t)t)|\Psi(0)\rangle, \tag{57}$$

но только теперь экспоненту надо понимать как хронологическую экспоненту. Как при плавном изменении гамильтониана $H$ будут меняться его собственные состояния? Если бы $H$ вообще не менялся, они оставались бы неизменными (за исключением фазы, разумеется). Но если $H$ меняется, причем очень медленно, то как будут изменяться собственные состояния этого гамильтониана? Оказывается, они будут эволюционировать как решения задач Коши для уравнения Шредингера с константой $\hbar = 1$. Таким образом, адиабатическая теорема устанавливает особый статус

Рис. 42: Отклонение основного состояния от результата плавно меняющейся унитарной эволюции. Прямое вычисление по данной схеме ведет к очень громоздким выражениям. Для доказательства адиабатической теоремы надо охватить весь процесс сразу на большом интервале времени. Здесь ключевую роль играют интерференционные эффекты - изменение фазы начального состояния с периодом $2\pi/E_0$ и первого возбужденного с периодом $2\pi/E_0$, причем периоды также меняются со временем! Поэтому роль играет разность энергий $E_1 - E_0$.




уравнения Шредингера: этот уравнение является математическим фактом. Физический элемент в нем - только значение постоянной Планка.

## 6.1 Адиабатическая теорема

Сначала мы рассмотрим идею квантовых адиабатичческих процессов, и докажем ослабленный вариант адиабатической теоремы.

Пусть у нас имеется основной гамильтониан $H_0$ и целевой гамильтониан $H_1$. Мы хотим рассмотреть медленное изменение первого гамильтониана, которое приводит в итоге ко второму. Это изменение - гомотопия, задаваемая вещественной функцией $s(t):\ s(0) = 0, s(T) = 1$, где $T$ - большое число, так что $H(t) = (1 - s(t))H_0 + s(t)H_1$ - значение измененного гамильтониана в момент времени $t$.

Адиабатическая теорема состоит в том, что при очень малом значении $\partial H/\partial t$ любое собственное состояние $|\Phi_k^0\rangle$ гамильтониана $H_0$ в результате квантовой эволю-

ции, индуцированной гамильтонианом $H(t)$, перейдет с большой точностью в соответствующее собственное состояние $|\Phi_k^1\rangle$ гамильтониана $H_1$. При этом медленность изменения $H(t)$ означает, что максимальное значение $\partial H/\partial t = \partial s/\partial t$ очень мало по сравнению с минимальной энергетической щелью $g$ - то есть минимальным значением разности собственных энергий $E_k(t) - E_s(t)$ по всем $k > s$ и по всем значениям $t: \ 0 \leq t \leq T$. Мы предполагаем собственные состояния невырожденными, так что равенство $E_k(t) - E_s(t) = 0$ достигается только при $s = k$.

Более детальный анализ показывает, что для точного приближения собственных состояний целевого гамильтониана образами собственных состояний основного гамильтониана необходимо еще усилить требование, а именно, надо потребовать, чтобы $max|\partial s/\partial t|/g^2$ было бы очень малой величиной.

Мы не будем доказывать адиабатическую теорему в этой сильной форме, а только покажем идею адиабатической теоремы, и перейдем к ее использованию в квантовых вычислениях.

Для удобства будем через $|n\rangle = |n(t)\rangle$ обозначать собственное состояние гамильтониана $H(t)$ с номером $n$, а через $E_n$ - соответствующее собственное значение энергии, и опускать явное упоминание о времени.

Пусть зафиксировано некоторое $n_0$, так что $|\Psi(0)\rangle = |n_0(0)\rangle$.

Состояние системы $|\Psi\rangle$ в момент $t$ подчиняется нестационарному уравнению Шредингера

$$i\hbar|\dot{\Psi}\rangle = H(t)|\Psi\rangle \tag{58}$$

и мы можем разложить его по собственным состояниям текущего гамильтониана: $|\Psi\rangle = \sum\limits_n a_n|n\rangle$, где все состояния и коэффициенты будут зависеть от времени $t$.

Мы имеем:

$$a_n(0) = \delta_{n,n_0}. \tag{59}$$

Подставляя это разложение в (58), мы получаем

$$\sum_n (\dot{a}_n|n\rangle + a_n|\dot{n}\rangle) = H\sum_n a_n|n\rangle = \sum_n E_n|n\rangle. \tag{60}$$

Теперь умножим слева это равенство на $\langle m|$ и воспользуемся ортонормированностью базисных векторов $|n\rangle$: $\langle n|m\rangle = \delta_{nm}$. Нам будет важно значение индекса суммирования, и мы разделим сумму на две части так:

$$i\hbar\dot{a}_m + i\hbar\sum_{n\neq m} a_n\langle m|\dot{n}\rangle + i\hbar a_m\langle m|\dot{m}\rangle = a_m E_m. \tag{61}$$

Теперь преобразуем равенство $H|n\rangle = E_n|n\rangle$, продифференцировав его по времени $t$ и умножив полученное равенство на $\langle m|$:

$$\dot{H}|n\rangle + H|\dot{n}\rangle = \dot{E}_n|n\rangle + E_n|\dot{n}\rangle, \langle m|\dot{H}|n\rangle + \langle m|H|\dot{n}\rangle = \dot{E}_n\delta_{nm} + E_n\langle m|\dot{n}\rangle. \tag{62}$$

Далее предполагаем, что $m \neq n$, и, учитывая, что $\langle m|H = E_m\langle m|$ получаем:

$$\langle m|\dot{n}\rangle = \frac{\langle m|\dot{H}|n\rangle}{E_n - E_m}. \tag{63}$$

С учетом (63) равенство (61) приобретает вид

$$i\hbar\dot{a}_m + i\hbar\sum_{n\neq m} a_n\frac{\langle m|\dot{H}|n\rangle}{E_n - E_m} + i\hbar a_m\langle m|\dot{m}\rangle = a_m E_m. \tag{64}$$

Отсюда мы сразу получаем дифференциальное уравнение на $a_m$:

$$\dot{a}_m = -c_m(\frac{i}{\hbar}E_m + \langle m|\dot{m}\rangle) + \sum_{n\neq m} a_n\frac{\langle m|\dot{H}|n\rangle}{E_m - E_n} \tag{65}$$

Мы видим, что если частное $\frac{\langle m|\dot{H}|n\rangle}{E_n - E_m}$ очень мало для любых $m \neq n$ по абсолютной величине, то есть интегралы

$$\Delta_{n,m} = \int_0^T a_n\frac{\langle m|\dot{H}|n\rangle}{E_n - E_m} \tag{66}$$

для $n \neq m$ очень малы, то последнее слагаемое в (65) можно отбросить. и мы получаем для коэффициента $a_m$ задачу Коши:

$$\dot{a}_m = A(t)c_m,\ a_m(0) = 0$$

Учитывая начальное условие (59) и теорему единственности решения задачи Коши, мы получаем $a_m = 0$ для любого $m \neq n_0$.

Итак, если выполнено условие $\Delta_{n,m} = o(1)$, адиабатическое приближение работает хорошо.

Однако, для квантовых адиабатических вычислений нам понадобится более точная формулировка адиабатической теоремы, которую можно найти в книге [24]:

*Адиабатическая теорема (уточненный вариант).*

*Если $|0(t)\rangle$ - основное а $|1(t)\rangle$ - возбужденное состояния гамильтониана $H(t)$, такое что $g = min_{\ 0\leq t\leq T,\ k=1,2,\ldots,N-1}|E_k - E_0|$, где минимум достигается при $k = 1$, то существует константа $C$, такая что для любого $\varepsilon > 0$ если для всех $t:\ 0 \leq t \leq T$ выполнены неравенства:*

$$\left|\frac{\langle 1|\dot{H}|0\rangle}{g}\right| \leq C\varepsilon,\quad \left|\frac{\langle 1|\dot{H}|0\rangle}{g^2}\right| \leq C\varepsilon \tag{67}$$

*и $|\Psi\rangle$ - решение задачи Коши для уравнения Шредингера с гамильтонианом $H$, и начальным условием $|\Psi(0)\rangle = |0(0)\rangle$, то $|\langle 0(T)|\Psi(T)\rangle|^2 \leq 1 - \varepsilon^2$.*

Таким образом, по сравнению с нашим предыдущим рассуждением, надо потребовать, чтобы скорость изменения гамильтониана была бы меньше квадрата минимальной щели между энергиями.

Мы не будем строго доказывать этот вариант адиабатической теоремы, отсылая слушателя к книге [24]; покажем лишь, почему надо требовать малости скорости изменения $H$ большей, чем $g^2$.

Итак, предположим, что выполнено соотношение $\Delta_{n,m} = o(1)$ и условие $\left|\frac{\langle 1|\dot{H}|0\rangle}{g^2}\right| = 0(1)$. Из вида интеграла (66) такого требования прямо не следует. Однако рассмотрим малый промежуток времени $dt$, на котором гамильтониан мало меняется, так что можно считать его константой. Тогда решение уравнения (56) запишется в виде разложения по собственным состояниям текущего гамильтониана $|\phi_i\rangle$:

$$|\psi\rangle = \sum_i e^{\frac{1}{\hbar}E_i dt}\lambda_i|\phi_i\rangle \tag{68}$$

Если взять основное состояние, можно считать, что $E_0 = 0$, сдвинув спектр на величину $E_0$, и тогда мы увидим, что все возбужденные состояния будут иметь коэффициент в виде осциллирующего множителя $exp{-\frac{i}{\hbar}}(E_i - E_0)t$, так что в случае плавного изменения гамильтониана эти осцилляции дадут в итоге знакопеременный ряд Лейбница, в котором члены будут почти полностью сокращать друг друга, так что интеграл (66) сведется к интегралу по одному периоду такой осцилляции, который равен примерно $O(1/g)$, и от него останется величина, по порядку равная $O(\langle 1|\dot{H}|0\rangle/g^2$, то есть пропорциональная скорости изменения самого гамильтониана $H$ (см. рисунок 43).

Рассмотрим основной интеграл (66), и оценим его грубо. Пусть гамильтониан меняется медленно, так что на промежутке $[0, \Delta t]$ он мало меняется, но основные состояния меняют фазу существенно. Считаем, что $\hbar = 1$. Тогда состояния $|0\rangle$ и $|1\rangle$ - основное и возбужденное, на этом промежутке - эволюционируют таким образом:

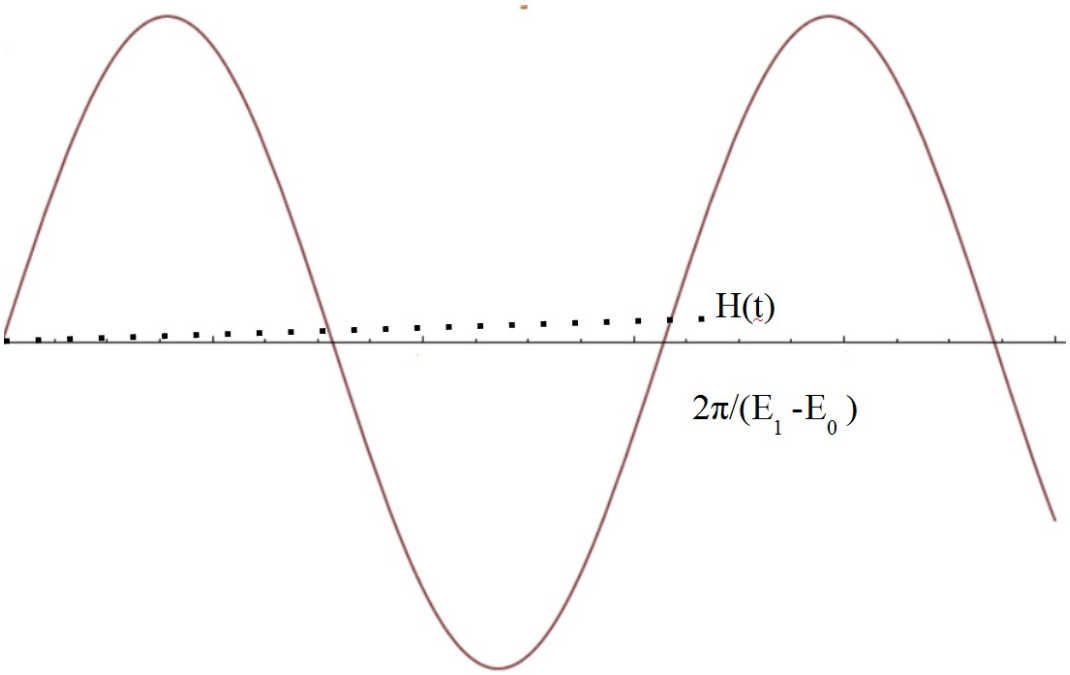
$$|0(dt)\rangle = e^{-iE_0 t}|0(0)\rangle,\ |1(t)\rangle = e^{-iE_1 dt}|1(0)\rangle, \tag{69}$$

Тогда числитель в выражении (66) примет вид

$$e^{i(E_1-E_0)t}\langle 1(0)|\dot{H(t_{average})}|0(0)\rangle \tag{70}$$

и будет осциллировать с периодом порядка $O(1/(E_1 - E_0)$. Предположим, что гамильтониан меняется плавно, так что $\langle 1|\dot{H}|0\rangle$ имеет ограниченно число монотонных участков. Оценим величину (66), учитывая сокращение в интерференции, порожденное осцилляциями комплексной экспоненты в (70) на участке монотонности числителя. Здесь у нас будет ряд Лейбница, сумма которого равна по порядку старшему члену ряда. Так что интеграл сведется к интегралу по участку длины $O(1/E_1 - E_0)$ от выражения $max(\dot{H})$, что и даст в итоге формулу (67). Графическая иллюстрация приведена на рисунке 43.

Рис. 43: Интерференция в отклонении основного состояния от результата плавно меняющейся унитарной эволюции.




## 6.2 Адиабатическая форма алгоритма Гровера

Алгоритм Гровера, первоначально сформулированный в терминах квантовых операций (последовательности гейтов), может иметь и непрерывную форму.

Впервые такую форму предложили Farhi и Gutman. Она состоит в следующем. Пусть нам надо найти неизвестное базисное состояние $|m\rangle$, которое мы назовем целевым. Мы создадим начальное состояние $|s\rangle$ - произвольное начальное состояние, которое нам удобно построить. Возьмем гамильтониан $H = E|m\rangle\langle m| + E|s\rangle\langle s|$.

Тогда, как мы уже видели ранее, шредингеровская эволюция, индуцированная гамильтонианом $H$, приведет нас из начального состояния в целевое за время $\pi/(2E\langle m|s\rangle)$. Это утверждение можно доказать непосредственно, диагонализировав гамильтониан $H$, и найдя решение уравнения Шредингера в явном виде, считая $\hbar = 1$. Однако это утверждение не является тривиальным. Действительно, в канонической версии алгоритма Гровера применется преобразование поворота $U = I_{\tilde{0}} I_m = e^{-i|m\rangle\langle m|} e^{-i|s\rangle\langle s|}$, что не сводится к применению эволюции, индуцированной гамильтонианом $H$, так как гамильтонианы $|m\rangle\langle m|$ и $|s\rangle\langle s|$ не коммутируют.

Как видно, непрерывная версия алгоритма Гровера доставляет то же самое квнатовое ускорение решения переборной задачи, что и GSA.

Однако с адиабатической формой алгоритма Гровера все обстоит не так просто. Мы создадим начальное состояние $|\Psi(0)\rangle = \frac{1}{\sqrt{N}} \sum_{a=0}^{N-1} |a\rangle$, как в операционной форме GSA, и допустим, что мы можем создать эволюцию, индуцированную гамильтониа-

ном $\tilde{H}(s) = (1-s)H_0 + sH_m$, где

$$H_0 = I - |\Psi_0\rangle\langle\Psi_0|,\ H_m = I - |m\rangle\langle m|$$

Адиабатический алгоритм состоит в применении к начальному состоянию $|\Psi_0\rangle$ переменного гамильтониана $H(s)$, где функция $s(t)$ такова, что $s(0) = 0,\ s(T) = 1$ для большого $T$. Искусство адиабатического вычисления состоит в выборе функции замедления $s(t)$.

Заметим, что $|\Psi_0\rangle$ и $|m\rangle$ есть основные состояния гамильтонианов $H_0$ и $H_m$ соответственно, с нулевыми собственными значениями.

Будем через $H(t)$ обозначать зависимость гамильтониана от реального времени $t$, для отличения от $\tilde{H}(s)$ - зависимость от абстрактного параметра $s$. Зависимость $s$ от $t$ означает замедление эволюции.

В условиях адиабатической теоремы для гамильтониана $H(t)$ мы опять будем считать $|0\rangle$ - основным, а $1\rangle$ - возбужденным состоянием, для которого реализуется щель энергии размера $g$. Тогда мы имеем:

$$\langle 1|\dot{H}|0\rangle = \frac{ds}{dt}\langle 1|\frac{d\tilde{H}}{ds}|0\rangle = \frac{1}{T}\langle 1\frac{\tilde{H}}{ds}|0\rangle. \tag{71}$$

Сначала мы попробуем пойти по простому пути, и выберем $s(t)$ - линейной функцией: $s = t/T$ для достаточно большого $T$; тогда гамильтониан будет меняться медленно. Решая задачу на собственные значения для гамильтониана $H$, мы можем найти и энергетическую щель. Результат вычислений таков:

$$g = \sqrt{1 - 4\frac{N-1}{N}s(1-s)}, \tag{72}$$

при этом $|\langle 1|\frac{d\tilde{H}}{ds}|0\rangle| \leq 1$.

Формула (72) графически проиллюстрирована на рисунке 44. Теперь мы найдем минимальную щель, которая равна $g_{min} = 1/\sqrt{N}$ (получается при $s = 1/2$). Тогда условие адиабатической теоремы дает нам неравенство $T \geq N/\varepsilon$. Мы, таким образом, получаем то же время вычисления $|m\rangle$, что и на классическом компьютере, и адиабатический алгоритм не дает квантового ускорения.

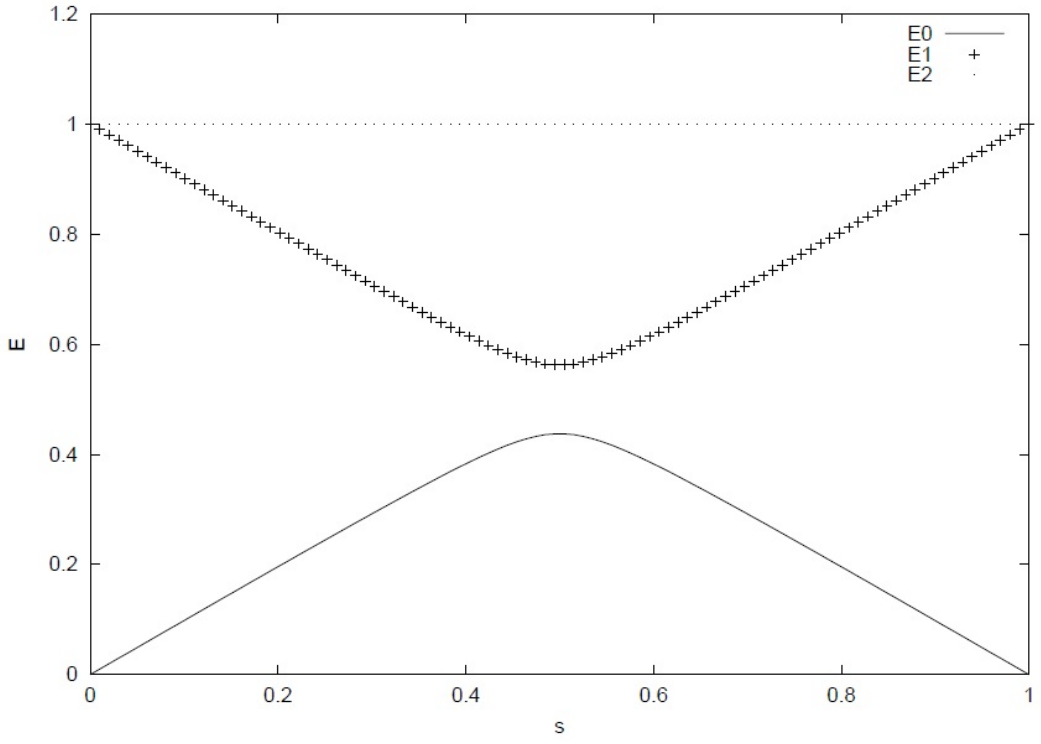
Для получения квантового ускорения мы зададим более сложное, нелинейное замедление времени $s(t)$. Поскольку критическое значение щели $g$ достигается не в любой момент, а только при $s = 1/2$, мы можем улучшить оценку общего времени работы алгоритма, подобрав нелинейное замедление. Для этого мы применим соотношение (67) локально, получив формулу

$$|\dot{s}| \leq g^2(t)/|\langle 1|\frac{d\tilde{H}}{dt}|0\rangle|. \tag{73}$$

Используя соотношение (72) при условии $|\langle 1|\frac{d\tilde{H}}{ds}|0\rangle| \leq 1$, мы получаем уравнение на замедление времени вида:

$$\dot{s} = \varepsilon g^2(t) = \varepsilon(1 - 4(1-1/N)s(1-s)) \tag{74}$$

Рис. 44: Собственные значения гамильтониана $\tilde{H}$ при $N = 64$. Рисунок взят из статьи Roland, Cerf, Quantum Search by Local Adiabatic Evolution (arxive.org, quant-ph/0107015).




для малого $\varepsilon$. Интеграция (74) дает

$$t = \frac{N}{2\varepsilon\sqrt{N-1}}(arctg((2s-1)\sqrt{N-1} + arctg\sqrt{N-1}), \tag{75}$$

инвертируя, мы находим окончательное выражение для замедления времени в виде графика, представленного на рисунке 45. Здесь видно, что наиболее быстро время течет в тех областях, где щель велика, и медленно - где щель мала.

Полное время работы алгоритма найдем, подставляя $s = 1$ в (74): $T = \pi\sqrt{N}/2\varepsilon$ - это именно то ускорение, которое дает стандартный алгоритм Гровера.

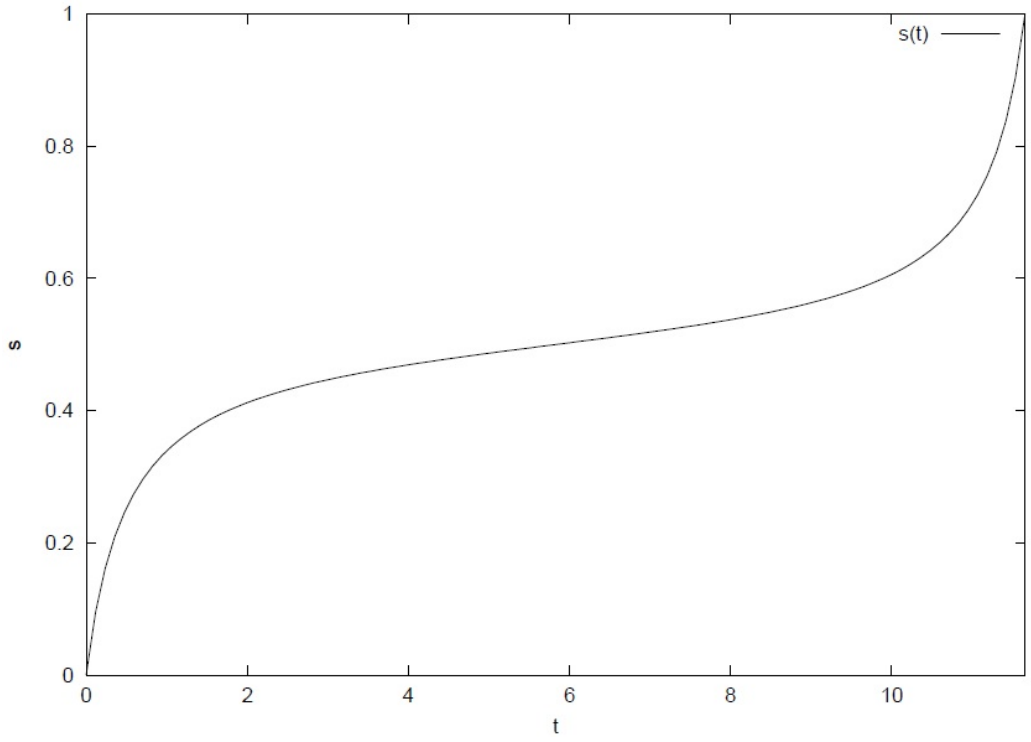
Теперь покажем, что найденное квантовое ускорение адиабатическим методом является оптимальным. Для этого рассмотрим два конкурирующих базисных состояния $|m\rangle$ и $|m'\rangle$, каждое из которых может быть целевым для алгоритма Гровера. Пусть $\psi_m\rangle$ и $|\phi_{m'}\rangle$ - состояния квантового компьютера при адиабатическом вычислении с некоторым замедлением времени $s(t)$. Правильно работающий алгоритм должен их достоверно различать за время $T$, то есть должно выполняться неравенство

$$1 - |\langle\psi_m(T)|\psi_{m'}(T)\rangle|^2 \geq \varepsilon \tag{76}$$

Во введенных нами обозначениях, мы разобъем гамильтониан на два слагаемых: $\tilde{H}(s) = \tilde{H}_1(s) + \tilde{H}_{2m}(s)$, где

$$\tilde{H}_1(s) = I - (1-s)|\psi_0\rangle\langle\psi_0|, \ \tilde{H}_{2m}(s) = -s|m\rangle\langle m|$$

Рис. 45: Оптимальное замедление времени для адиабатической версии GSA. Рисунок взят из статьи Roland, Cerf, Quantum Search by Local Adiabatic Evolution (arxive.org, quant-ph/0107015).




Для зависимости от времени $t$ мы, как и прежде, используем обозначение $H$ без тильд. Тогда $|\psi_m\rangle$ и $|\psi_{m'}\rangle$ будут решениями уравнений

$$i|\dot{\psi}_m\rangle = (H_1 + H_{2m})|\psi\rangle,\ i|\dot{\psi}_{m'}\rangle = (H_1 + H_{2m'})|\psi\rangle$$

с общим начальным условием $|\psi_m(0)\rangle = |\psi_{m'}(0)\rangle = |\psi_0\rangle$.

Мы имеем:

$$\begin{array}{l} \frac{d}{dt}(1 - |\langle\psi_m|\psi_{m'}\rangle|^2) = \\ 2Im(\langle\psi_m|H_{2m} - H_{2m'}|\psi_{m'}\rangle\langle\psi_{m'}|\psi_m\rangle) \\ \leq 2|\langle\psi_m|H_{2m} - H_{2m'}|\psi_{m'}\rangle|\ |\langle\psi_{m'}|\psi_m\rangle| \\ \leq 2(|\langle\psi_m|H_{2m}|\psi_{m'}\rangle| + |\langle\psi_m|H_{2m'}|\psi_{m'}\rangle|). \end{array} \quad (77)$$

Теперь возьмем сумму по $m, m'$ и получим:

$$\begin{array}{l} \frac{d}{dt}\sum\limits_{m,m'}(1 - |\langle\psi_m|\psi_{m'}\rangle|^2) \leq 4\sum\limits_{m,m'}|\langle\psi_m|H_{2m}|\psi_{m'}\rangle| \\ \leq 4\sum\limits_{m,m'}\|H_{2m}|\psi_m\rangle\|\ \||psi_{m'}\rangle\| \leq 4N\sum\limits_{m}\|H_{2m}|\psi_m\rangle\|. \end{array} \quad (78)$$

В последнем переходе использовалось неравенство Коши - Буняковского - Шварца. Заметим также, что для нормированного состояния $|\psi\rangle$ из $\sum\limits_m \|H_{2m}|\psi\rangle\|^2 = s^2$ следует $\sum\limits_m \|H_{2m}|\psi\rangle\| \leq \sqrt{N}s$ (неравенство между нормами в пространствах $l_2$ и $l_1$).

В результате мы имеем:

$$\frac{d}{dt}\sum_{m,m'}(1-|\langle\psi_m|\psi_{m'}\rangle|^2) \leq 4N\sqrt{N}s. \tag{79}$$

Интегрируя это неравенство, мы имеем:

$$\sum_{m,m'}(1-|\langle\psi_m|\psi_{m'}\rangle|^2) \leq 2N\sqrt{N}\int_0^T s(t)dt$$

и, учитывая (76), находим

$$T \geq \varepsilon(N-1)/(4\sqrt{N})$$

что и доказывает, что правильно работающий адиабатический алгоритм для задачи перебора не может работать быстрее корня из классического времени.

У адиабатической теоремы есть множество форм, и оценок погрешностей. Самая простая принадлежит Ландау и Зенеру; она справедлива только для двух-уровневой системы, то есть для одного кубита. Она имеет вид

$$err = O(e^{-C\Delta^2 t_f})$$

где $t_f$ - полное время процесса.

## 6.3 Построение гамильтонианов для адиабатических вычислений

Для реализации адиабатическкого метода необходимо практически построить гамильтонианы с нужным свойством: для начального $H_0$ его основное состояние должно быть достаточно простым, а для целевого $H_1$ основное состояние должно давать решение искомой задачи.

Как правило, основное состояние начального гамильтониана выбирается, как и в операторной версии алгоритма Гровера, в виде $|\tilde{0}\rangle = \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}|j\rangle$. Такой гамильтониан, с таким основным состоянием, имеет вид

$$H_I = \sum_{i-1}^{m}\frac{1-\sigma_i^x}{2}.$$

Действительно, при $m = 1$ это проверяется непосредственно, а для больших $m$ гамильтониан распадается на сумму слагаемых - операторов, для каждого из которых собственными состояниями будут состояния, имеющие в обозначениях из линейной алгебры вида $(...a, a...)^*$, где выделены позиции в векторе - столбце - базисного состояния, соответствущие значениям 0 и 1 фиксированного кубита, а многоточие обозначает произвольные состояния. Но это и означает, что сумма таких операторов имеет собственное состояние $|\tilde{0}\rangle$.

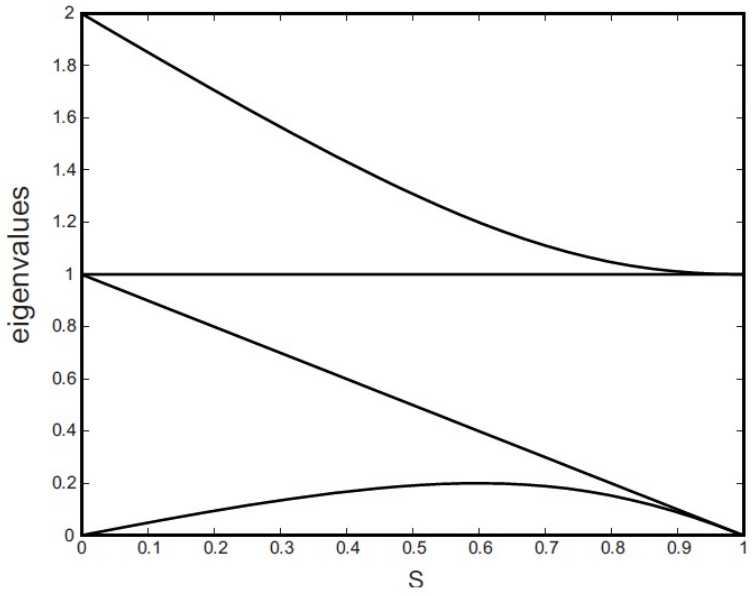



Рис. 46: Поведение 4 собственных значений для алгоритма 2-bit Disagree. Рисунок взят из статьи Adiabatic quanatum computation and quantum annealing (Catherine McGeoch).

Теперь мы займемся целевым гамильтонианом $H_1$. Рассмотрим сначала простой пример. У нас есть два кубита и задача в том, чтобы определить, равны ли их значения. Для такой задачи поиска совпадений основное состояние целевого гамильтониана будет

$$\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle.$$

а целевой гамильтониан будет иметь вид

$$H_1 = \frac{1}{2}(I + \sigma_1^z \sigma_2^z).$$

Это - так называемый 2-bit Disagree алгоритм. На рисунке 46 изображено поведение его спектра в зависимости от режима $s(t)$. Склеивание двух собственных значений в конце процесса не является фатальным, так как нам все равно, какое из основных состояний будет выдано при измерении конечного состояния.

Рассмотрим немного более сложную задачу - точного покрытия. Это задача определения истинности конъюнкции $\&_c C_c$ где каждый сомножитель $C_c$ имеет вид $x_1^c, x_2^c, x_3^c$, $x_j^c = x_i$ или $x_j^c = \not{x}_i$ и $C_c$ истинно тогда и только тогда, когда из $x_1^c, x_2^c, x_3^c$ ровно один член истинен.

Мы для каждого $c$ введем функцию покрытия

$$f_c = (1 - x_1^c - x_2^c - x_3^c)^2$$

и положим $f(\bar{x}) = \sum\limits_c f_c(\bar{x})$. Теперь мы имеем

$$f(\bar{x}) = -2m - \sum_i (B_i x_i + B_i x_i x_i) + \sum_{i<j} C_{ij} x_i x_j = -2m + \sum_{i<j} C_{ij}(1 - s_i)(1 - s_j)$$

где $x_i = (1 - s_i)/2$ - формула для перехода между булевскими переменными $x_i = 0, 1$ и спиновыми переменными $s_i = \pm 1$.

Целевой гамильтониан для этой задачи имеет вид

$$H_1 = \sum_{i<j} C_{ij}(1 - \sigma_i^z)(1 - \sigma_j^z).$$

Теперь рассмотрим общий вид $SAT$ - проблемы - выполнимости формулы логики выказываний. Достаточно считать, что эта формула задана в конъюнктивной нормальной форме, более того, что каждый конъюнктивный член имеет вид $f_c$, только теперь истинность определяется по правилам логики высказываний.

В этом случае определение элементарной функции $f_c$ будет иметь вид

$$f_c(s_1, s_2, s_3) = (5 - s_1 - s_2 - s_3 + s_1 s_2 + s_2 s_3 + s_1 s_3 + 3 s_1 s_2 s_3)/8.$$

Модель Изинга. Функция энергии для базисного состояния $n$ спинов, соединенных попарно, имеет вид

$$H(\bar{s}) = \sum_i h_i s_i + \sum_{i<j} J_{ij} s_i s_j.$$

Проблема нахождения $\bar{s}$, минимизирующей данную функцию NP-полна если спины соединены в виде трехмерной структуры (Истрал). Fu и Anderson показали, что она NP- полна даже для 2D соединений при условии присутствия ненулевых $h_i$. Задача нахождения минимума функции $H(\bar{s})$ эквивалентна нахождению основного состояния гамильтониана

$$H = \sum_i h_i \sigma_i^z + \sum_{i<j} J_{ij} \sigma_i^z \sigma_j^z.$$

Для решения этой задачи можно применить метод квантового отжига.

Он состоит в следующем. У нас есть целевой гамильтониан $H_{tar}$, основное состояние которого нам надо найти. Мы выбираем возмущающий гамильтониан $H_d$ и расписание $G(t)$, выражающее интенсивность возмущения. Это расписание устроено так: $G(0) \gg 1,\ G(t) \to 0\ (t \to \infty)$. Текущий гамильтониан выбирается в виде

$$H(t) = H_{tar} + G(t) H_d.$$

Иллюстрация квантового отжига приведена на рисунке 47

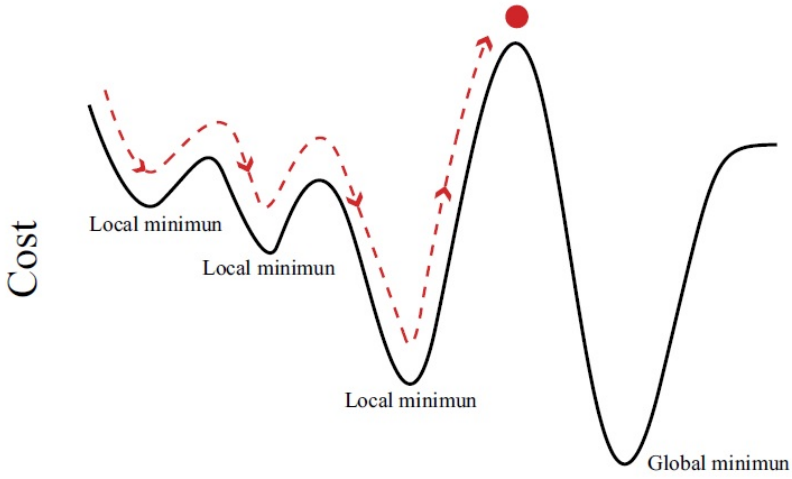



**Figure 3.2:** The objective function and neighborhood rule define a solution landscape. A heuristic search algorithm steps from node to neighbor node looking for an optimal solution while avoiding getting stuck in local minima.

Рис. 47: Схематическое изображение квантового отжига. Рисунок взят из статьи Adiabatic quanatum computation and quantum annealing (Catherine McGeoch).

# 7 Лекция 7. Упрощенное управление и идентичность фермионов в квантовых вычислениях

Квантовый компьютер представляет беспрецедентную проверку квантовой физики и требует такого уровня управления нано-объектами, который никогда раньше не достигался искусственным путем. В то время как математическая теория квантовых вычислений в рамках стандартного копенгагенского формализма хорошо разработана, физическая реализация квантовых вычислений представляет серьезный вызов нашему пониманию Природы. Поэтому важно найти наиболее простую форму реализации таких вычислений, которая бы опиралась на самые основы квантовой теории и представляла бы наименьшие технологические трудности. Два условия для такой схемы должны быть выполнены: адекватное представление квантовых состояний и реалистическое управление вычислением.

Обычно вычислительный элемент - кубит - мы представляем в виде некоторой характеристики элементарной частицы, например, ее спина или пространственного положения. Этот подход хорош для изолированных кубитов. Для системы нескольких кубитов он встречает трудности, происходящие из-за идентичности (неразличимости) элементарных частиц одного типа. В вычислениях мы должны иметь возможность обращения к определенному кубиту, тогда как проблемой является различение этого кубита от близко расположенных других, идентичных кубитов. Конечно, мы могли бы расположить эти кубиты на большом расстоянии друг от друга, но в этом случае нам было бы трудно огранизовать взаимодействие между ними, необходимое для совершения запутывающего гейта, необходимого для квантовых вычислений.

Одно из решениий состоит в том, чтобы использовать пространство Фока чисел заполнения для квантвоых вычислений. Здесь используется идентификация кубитов с уровнями энергии в пространстве Фока, так чтчо нуль трактуется как свободный от частиц уровень, а единица - как уровень, занятый какой-либо частицей. Этот подход дает универсальное квантовое вычисление высокой ценой. Требуется управлять не только внешним полем и туннелированием, но и диагональным взаимодействием между кубитами, а также контактом со сверхпроводником; то есть мы должны уметь управлять динамикой коффициентов $\alpha, \beta, \gamma$ в (87) и дополнительным слагаемым $\delta a_k^+ a_j^+ + \delta^* a_k a_j$.

В этом параграфе мы увидим, как можно уменьшить эту цену, прилекая непрерывные и неконтролируемые взаимодействия. Для этого нужны две вещи: предположение о том, что исходный гамильтониан содержит только внешнее поле, диагональное взаимодействие и туннелирование, и введение нового соответствия между вычислительным базисом квантовых вычислений и пространством чисел заполнения. Тогда для получения универсального квантового вычисдения нам будет нуно только уметь управлять внешним полем и туннелированием, что достижимо с помощью лазеров. Мы дадим общую схему таких вычислений, основываясь на работах [25], [26], и адаптируя изложенные там методы к пространству чисел заполнения.

## 7.1 Однокубитное управление квантовым вычислением

Первая видимая трудность при реализации квантовых вычислений - выполнение двухкубитных запутывающих операций с огромной точностью. Мы должны уметь управлять запутанностью частиц, оперируя с перекрытием носителей их волновых функций в пространственном представлении. При этом мы должны также надежно различать частицы, что возможно только при малом перекрытии их волновых функций; налицо очевидное противоречие в требованиях, чоо делает двухкубитные операции намного более сложными, чем однокубитовые.

Здесь можно поступить так. Мы можем управлять только однокубитовыми операциями, а двухкубитовое естественное взаимодействие оставить без управления, так что оно будет идти в естественном режиме. Такая модель квантового компьютера уже будет более реалистичной, чем абстрактная фейнмановская схема, в которой предусматривается управление также и двухкубитными гейтами. Мы сначала покажем, как эта схема работает для частиц с квадратичным взаимодейтвием. Здесь трудность в том, что такое взаимодейтвие охватывает не только выделенные кубиты, но и соседние с ними, которые не должны принимать участия в работе гейта. Такие "паразитные" взаимодействия мы будем подавлять однокубитными операциями.

Мы покажем, как реализовать квантовое преобразование Фурье в рамках такой модели. Главное наше предположение состоит в том, то двухкубитные взимодействия должны иметь диагональную форму. Для простоты, мы сначала будем предполагать, что потенциал взаимодеййствия между кубитами падает очень быстро с увеличением расстояния между ними, а именно, имеет вид потенциала Юкавы. Этот метод применим к более широкому классу диагональных взаимодействий. Потом мы применим этот подход к многим кубитм с квадратичным взаимодействием.

### 7.1.1 Реализация квантового преобразования Фурье на однокубитном управлении

Квантовое преобразование Фурье - ключевой элемент в квантовых вычислениях, применяемый как подпрограмма в разных алгоритмах, например, для факторизации целых чисел (см. [18]); квантовая схема, реализующая обратное к нему преобразование, показана на рисунке 41. Мы будем, как обычно, представлять целое число в виде $a = a_0 + a_0 2 + \ldots + a_{l-1}2^{l-1}$ и идентифицировать с ним базисное состояние $|a_0\ a_1\ \ldots\ a_{l-1}\ \rangle = |a\rangle$ в $L = 2^l$ мерном гильбертовом пространстве состояний. Эти состояния образуют ортонормированный базис для входных состояний квантовой схемы из гейтов; мы будем располагать кубиты сверху вниз. Аналогично мы будем рассматривать и выходное состояние с бинарными знаками $b_j$ числа $b = b_0 + b_0 2 + \ldots + b_{l-1}2^{l-1}$ которые мы будем располагать в противоположном порядке - снизу вверх, как это делалось ранее.

Наша схема будет выполнять преобразование $QFT^{-1}$ за $O(l^2)$ шагов, тогда как матрица этого преобразования имеет размерность $l^2$. Мы также покажем, как избежать необходимости управлять двухкубитными операциями, чтобы они происходили в фоновом режиме. Итк, мы будем рассматривать взаимодействия между двумя кубитами вида

$$\text{A) } H = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \rho \end{pmatrix}, \quad \rho > 0, \qquad \text{B) } H = \begin{pmatrix} \rho_1 & 0 & 0 & 0 \\ 0 & \rho_2 & 0 & 0 \\ 0 & 0 & \rho_3 & 0 \\ 0 & 0 & 0 & \rho_4 \end{pmatrix}, \qquad (80)$$

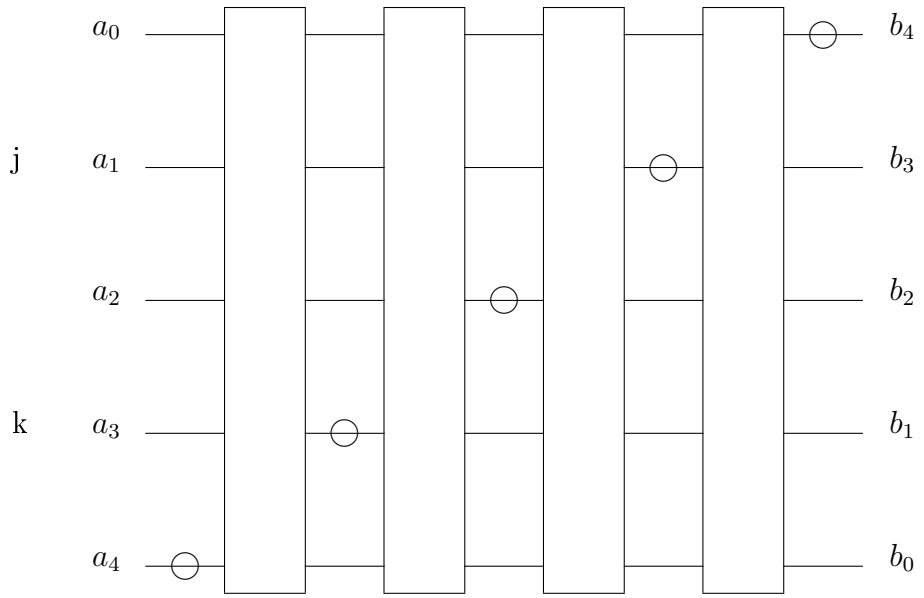
где все $\rho = \rho_0 \frac{e^{-br}}{r}$; $b = const$; $r$ есть расстояние между кубитами и $\rho_1 + \rho_4 \neq \rho_2 + \rho_3$. Мы расположим $l$ кубитов в одну линию с равными интервалами. Пусть взимодейсствие между кубитами $j$ и $k$ имеет гамильтонин $H_{j,k}$вида (80). Такой тип гаимльтониана возникает, нпример, в модели Изинга с частицами спина 1/2. Требуемое расстояние между кубитами мы можем обеспечить, располагая их в отдельных потенциальных ямах. Выбирая подходящую единицу длины, мы можем считать, что $b = 1$. Сначала исследуем взааимодействие вида (80, A) а затем распространим результата на случай (80, B).

#### Реализация QFT с точностью до фазового сдвига

Напомним, что преобразование Фурье QFT и обратное к нему имеет вид:

$$QFT:\ |b\rangle \longrightarrow \frac{1}{\sqrt{L}} \sum_{a=0}^{L-1} e^{-\frac{2\pi i\ ab}{L}} |a\rangle, \qquad QFT^{-1}:\ |a\rangle \longrightarrow \frac{1}{\sqrt{L}} \sum_{b=0}^{L-1} e^{\frac{2\pi i\ ab}{L}} |b\rangle. \qquad (81)$$

Обратное преобразование может быть реализовано следующей схемой гейтов.




.

Рис. 48: Реализация обратного преобразования Фурье с точностью до фазового сдвига. Прямоугольники обозначают непрерывное взаимодействие, круги - оператор Адамара

Здесь прямоугольники обозначают унитарные операторы вида $U = e^{-i\tilde{H}}$, где $\tilde{H} = \sum_{l>j>k\geq 0} \tilde{H}_{j,k}$, и все $\tilde{H}_{j,k}$ имеют вид (80 , A) с $\rho_0 = \pi$, $r = j - k$. Если мы выберем систему единиц, в которой $\hbar\rho_0 = \pi$, причем единица длины такова что $r = j - k$, то $U$ будет в точности оператором, переводящим вектор состояния с данным гамильтонианом в единицу времени. Здесь мы предполагаем, что однокубитные операторы занимают пренебрежимо малое время, так что взаимодеййствие кубитов в течение этого времени не меняет фазу существенно. Для доказательства корректности данной схемы применим метод расчета амплитуды из работы [18].

Пусть дано начальное базисное состояние: $|a\rangle$, и мы рассматриваем какое-либо конечное состояние для данной схемы $|b\rangle$; вычисляем амплитуду перехода $|a\rangle \to |b\rangle$. Ее модуль будет равен всегда $1/\sqrt{L}$, и нам надо только посчитать ее фазу. Введем упрощающее обозначение $a'_j = a_{l-1-j},\ j = 0, 1, \ldots, l-1$. В ходе применения нашей схемы значения кубитов с номерами $j$ и $k \leq j$ проходят через схему слева направо (см. рисунок 48).

Мы выделим 4 типа взаимодействий: $a'_j$ с самим собой и $a'_k$ с самим собой в гейте Адамара, $a'_j$ с $a'_k$ $(j > k)$, $a'_j$ с $b_k$ для $j > k$, и $b_j$ с $b_k$ $(j > k)$. Время этих взаимодействий будет таким: нуль, $k$, $j - k$ и $l - 1 - j$ соответственно. Суммируя вклады от этих взаимодействий в фазу, мы получим результат в виде

$$\pi \sum_{l>j>k\geq 0} \frac{a'_j a_k k}{2^{j-k}(j-k)} + \pi \sum_{l>j>k\geq 0} \frac{a'_j b_k (j-k)}{2^{j-k}(j-k)} + \pi \sum_{l>j\geq 0} a'_j b_j + \pi \sum_{l>j>k\geq 0} \frac{b_j b_k (l-j-1)}{2^{j-k}(j-k)}. \quad (82)$$

Обозначим первое и четвертое слагаемые через $A$ и $B$ соответственно. Их вклад соответствует действию диагональных членов гамильтониана на $|a\rangle$ и $|b\rangle$. Мы временно оставим эти вклады. Займемся вторым и третьим слагаемыми. После замены $j$ на $l-1-j$ их сумма примет вид

$$\pi \sum_{l-1>k+j\geq 0} \frac{a_j b_k 2^{j+k}}{2^{l-1}} + \pi \sum_{l-1\geq j\geq 0} a_{l-1-j} b_k \quad = 2\pi \sum_{l>k+j\geq 0} \frac{a_j b_k 2^{j+k}}{2^l} = 2\pi S + 2\pi \sum_{l>k,j\geq 0} \frac{a_j b_k 2^{j+k}}{2^l} = 2\pi S + 2\pi \frac{ab}{2^l} \tag{83}$$

для некоторого целого $S$. Здесь первое слагаемое не меняет фазы и мы получили желаемое представление обратного Фурье оператора с точностью до вкладов $A$ и $B$.

### Коррекция фазовых сдвигов

Чтобы учесть вклад диагональных членов $A$ и $B$ в фазу мы применим один прием. Рассмотрим сначала слагаемое $A$. Оно состоит из членов вида $A_{j,k} = c_{j,k} a'_j a'_k$, где $c_{j,k}$ зависит только от $j$ и $k$, но не от $a$. Мы назовем $j$-й и $k$-й кубиты выделенными.

Будем примеять однокубитный оператор $NOT$ последовательно ко всем не выделенным кубитам для того, чтобы подавить взаимодействие с ними и оставить лишь взаимодействие между выделенными кубитами. Сначала рассмотрим пару не выделенных кубитов с номерами $p, q,\ q > p$. Их непрерывное взаимодействие в течение времени $\Delta t$ даст слагаемое $d_{p,q}\Delta t\ a'_p a'_q$ в фазе, где вещественное число $d_{p,q}$ зависит только от того, как быстро падает интенсивность взаимодействия с расстоянием, но не от $a'_p, a'_q$. Например, для потенциала Юкавы мы имеем $d_{p,q} = e^{-|q-p|}/|q-p|$. Теперь инвертируем один из этих кубитов, безразлично какой, пусть это будет $q$-й, с помощью гейта $NOT$. Его состояние станет равным $1 - a'_q$. Теперь второй интервал продолжительности $\Delta t$ непрерывного взаимодействия даст слагаемое $d_{p,q}\Delta t\ a'_p(1 - a'_q)$ к фазе. Наконец, мы восстановим значение $q$-го кубита с помощью второго применения $NOT$. Результирующий фазовы сдвиг в этих четырех действиях составит $d_{p,q}\Delta t\ a'_p$ и он зависит только от значения $p$-th кубита.

Теперь мы можем компенсировать этот фазовый сдвиг однокубитным преобразованием. Если рассмотреть пару кубитов с номерами $p, q$, где один, скажем, $p$-й выделен, а другой - не выделен, мы можем компенсировать их взаимодействие с помощью однокубитных операторов: двух NOT для $q$-го и некоторого фозового сдвига для $p$-го. Теперь мы можем модифицировать этот прием, чтобы компенсировать влияние всех не выделенных кубитов одновременно. Для этого будем применять операторы NOT для каждого не выделенного кубита достаточно часто, так что вклады в фазу не выделенных кубитов сократят друг друга. Для этого есть два пути: использовать случайный процесс для генерации моментов совершения операций $NOT$, или делать их периодически с разными периодами для разных кубитов. Сначала рассмотрим первый подход.

### Метод случайных процессов

Для каждого не выделенного кубита с номеромм $p$ м рассмотрим Пуассоновский процесс $\mathcal{A}_p$, генерирующий моменты времени $0 < t_1^p < t_2^p < \ldots < t_{m_p}^p < 1$ с некоторой фиксированной плотностью $\lambda \gg 1$. Пусть все $\mathcal{A}_p$ независимы. Мы выполним операторы NOT на всех невыделенных кубитах с номерами $p$ в моменты времени

$t^p_m$ последовательно. В момент 1 мы выполняем NOT на $p$-м кубите тогда и только тог, когда $m_p$ нечетно, так что после такой процедуры каждый кубит восстанавливает свое первоначальное значение. Посчитаем фазовый сдвиг, генерируемый этой процедурой. Взимодейтвие выделенных кубитов остаетя незатронутым. Зфиксируем какой-то не выделенный кубит и посчитаем его вклад в фазу. Этот вклад отоит из 2 слагаемых: первый есть вклад от взаимодействия его с выделенными, а второй - с не выделенными кубитами. Найдем их последовательно.

Ввиду высокой плотности $\lambda$ Пуассоновкого процесса $\mathcal{A}_p$ около половины всего времени кубит $p$ будет находиться в состоянии $a'_p$, а вторую половину - в состоянии $1-a'_p$. Его взаимодействие с выделенным кубитом, скажем, с $j$-м, даст вклад $\frac{1}{2}d_{p,j}a'_pa'_j + \frac{1}{2}d_{p,j}(1-a'_p)a'_j$ то есть, $\frac{1}{2}d_{p,j}a'_j$. 2. Теперь рассмотрим разные не выделенные кубиты с номерами $q \neq p$. Ввиду независимости моментов времени совершения операторов NOT на $p$-м и $q$-м кубитах и высокой плотности $\lambda$, эти кубиты будут в каждом состоянии $(a'_p,\ a'_q)$, $(a'_p,\ 1-a'_q)$, $(1-a'_p,\ a'_q)$, $(1-a'_p,\ 1-a'_q)$ примерно етверть времени. Результирующий вклд ответ $\frac{1}{4}d_{p,q}[a'_pa'_q + a'_p(1-a'_q) + (1-a'_p)a'_q + (1-a'_p)(1-a'_q)] = \frac{1}{4}d_{p,q}$. Общий фазовый сдвиг, происходящий из за присутствия не выделенных кубитов, находится суммированием значений пунктов 1 и 2 для всех $p \notin \{j,k\}$. Он составит

$$\frac{1}{2}[\sum_{p\notin\{j,k\}} d_{p,j}a'_j + \sum_{p\notin\{j,k\}} d_{p,k}a'_k] + \frac{1}{4}\sum_{p,q\notin\{j,k\}} d_{p,q}.$$

Этот сдвиг можно компенсировать однокубитовым гейтом, так как первые два слагаемых зависят только от значений кубитов, а остальные постоянны. Мы получаем схему с непрерывным взаимодействием, двух кубитов и однокубитовыми операциями, реализующую требуемый фазовый сдвиг $d_{j,k}a'_ja'_k$.

Если взять временной интервал $\Delta t$ вместо единичного в этой процедуре, мы получим фазовый сдвиг на $\Delta t\ d_{j,k}a'_ja'_k$. Для получения сдвига на $-\Delta t\ d_{j,k}a'_ja'_k$, надо сначала применить NOT к $j$-му кубиту, затем предыдущую процедуру, потом опять NOT к $j$-му кубиту, и добавить $-\Delta t\ d_{j,k}a'_k$ через однокубитовую операцию. Так мы сделаем добавку к фазе $c \cdot a'_ja'_k$ для вещественного $c$ независимо от знака. Должная комбинация этих схем даст двиг

$$\sum_{j,k} c_{j,k}a'_ja'_k \tag{84}$$

для любых $c_{j,k}$. Располагая эти операторы перед и после $QFT^{-1}$ в процедуре из предыдущего пункта, мы компенсируем слагаемые $A$ и $B$ в фазе и получим схему, реализующую $QFT^{-1}$. Ошибка, появляющаяся в этой схеме, исходит от неточности пуассоновского распределения моментов времени выполнения операторов NOT и постороннего взаимодействия в ходе этих операций. Ее можно минимизировать, повышая интенсивность пуассоновского процесса и уменьшения времени NOT операций по сравнению с типичным временем двухкубитных операций, определенных $d_{j,k}$.

Оценим замедление, происходящее из-за вставок NOT по сравнению с абстрактной реализацией квантовых вычислений на схеме из квантовых гейтов. Зафиксируем единицу времени так, что один гейт в схеме требует этой единицы времени.

Итак, пусть ось времени разбита на равные интервалы длины $\delta t$ единиц, операции NOT могут выполняться только в моменты вид $k\delta t$ для некоторых целых $k$ с

вероятностью $p = 1/\lambda$, где $\lambda$ - интенсивность процесса. Пусть полное время вычисления составляет $T$, и $M = T/\delta t$ - число NOT операций. Ошибка в фазе, происходящая из низкой интенсивности пуассоновского процесса будет равна среднему квадратичному отклонению суммы независимых величин, принимающих значения $\pm 1$, то есть $\sqrt{M\delta t^2} = \sqrt{T\delta t}$. Она может быть сделана сколь угодно малой при $\delta t \to 0$, однако при $\delta t = const$ ошибка будет нарастать, так что масштабируемого вычисления мы не получим.

Теперь докажем универсальность предложенной модели квантовых вычислений. Мы предполагаем, что взаимодействие между кубитами зависит от их пространственного расположения, которое мы зафиксируем. Единственное условие, которое мы налагаем на взаимодействие - это чтобы оно было диагональным. Так что если $j$ и $k$ обозначают номера двух кубитов, гамильтониан их взаимодействия будет иметь один из видов

$$\text{A) } H_{j,k} = \begin{pmatrix} E_1^{j,k} & 0 & 0 & 0 \\ 0 & E_2^{j,k} & 0 & 0 \\ 0 & 0 & E_3^{j,k} & 0 \\ 0 & 0 & 0 & E_4^{j,k} \end{pmatrix}, \qquad \text{B) } H_{j,k} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & E_{j,k} \end{pmatrix}, \ E_{j,k} > 0. \tag{85}$$

Сначала заметим, что взаимодействие общего вида (80, A) можно свести к виду (80, B) добавкой однокубитных гамильтонианов $H'_{j,k}$, матрицы которых имеют вид

$$\begin{pmatrix} a & 0 & 0 & 0 \\ 0 & a & 0 & 0 \\ 0 & 0 & b & 0 \\ 0 & 0 & 0 & b \end{pmatrix}, \qquad \begin{pmatrix} \alpha & 0 & 0 & 0 \\ 0 & \beta & 0 & 0 \\ 0 & 0 & \alpha & 0 \\ 0 & 0 & 0 & \beta \end{pmatrix}.$$

Эта добавка редуцирует гамильтониан вида (85, A) до формы (85, B) и может быть реализована однокубитными гейтами, так как диагональные матрицы коммутируют. Заметим, что разные пары кубитов могут взаимодействовать по разному, находиться на разных расстояниях, и т.п. Для доказательства универсальности вычислительной модели с непрерывным взаимодействием, нужно показать, как совершать произвольную двухкубитную операцию. Пусть дан унитарный оператор, индуцируемый гамильтонианом (85, B) в единицу времени: $U_{j,k} = \exp(-iH_{j,k})$ (Постоянная Планка единична, как обычно). Мы покажем, как совершить ее на двух кубитах: $j$-м и $k$-м, сохраняя нетронутыми все остальные. Если сделаем это, будет возможным реализовать двухкубитную операцию на любой паре кубитов. Тогда для взаимодействия на большом расстоянии мы получим почти линейное замедление по времени по сравнению с обычной моделью, а для взаимодействия на короткой дистанции надо совершить операции SWAP, чтобы сблизить пару нужных кубитов. Мы, таким образом, получим множитель к времени, пропорциональный размеру памяти.

Чтобы совершить преобразования $U_{j,k}$ надо применять метод NOTов на невыделенных кубитах, как было определено выше, в моменты, определяемые независимыми пуассоновскими процессоми. Однако теперь преимущество нашего метода не столь очевидно, как в случае преобразования Фурье, так как, например, алгоритм Гровера требует более чем логиарифмического времени: оно растет как квадратный корень из классического. Для таких случаев можно применять метод, описанный ниже.

**Метод периодических NOTов**

Будем совершать операции NOT на любом из $j$ кубитах в моменты времени $jk\delta t$ для целых $k$, где $\delta t$ снова есть малый период. Мы можем повторить рассуждения, приведенные выше, избавляясь от нежелательного сдвига по фазе с помощью выбора очень малого $\delta t$.

Этот метод даст по сравнению со стандартной гейтово моделью замедление порядка $n^2$. Достаточно показать, как с помощью операций $U_{j,k}$ мы можем сделать любой двухкубитный гейт. Например, продемонстрируем, как реализовать CNOT на данной паре кубитов.

Пусть $j, k$ фиксировано и мы опускаем индексы. Мы обозначим $\Delta E = E_1 - E_2 - E_3 + E_4$. Если $\frac{\Delta E}{\pi} \notin Q$ ($\frac{\Delta E}{\pi}$ не рационально, то (так как физические параметры, например, периоды циклов, могут быть слегка изменены и сделаны иррациональными, то мы можем считать их иррациональными) мы можем осуществить CNOT операцию в виде

$$\left[ CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \right]$$

на выделенной паре кубитов, испоьзуя для управления лишь один кубит и оставляя фиксированным диагональный оператор $E$ $\left[ E = \begin{pmatrix} \exp(iE_1) & 0 & 0 & 0 \\ 0 & \exp(iE_2) & 0 & 0 \\ 0 & 0 & \exp(iE_3) & 0 \\ 0 & 0 & 0 & \exp(iE_4) \end{pmatrix} \right]$ следующим образом.

I. Обозначим последовательность вращения фазы первого кубита через

$A = \left[ \begin{pmatrix} 1 & 0 \\ 0 & \exp(i(E_1 - E_3)) \end{pmatrix} \right]$, of the second qubit by $B = \left[ \begin{pmatrix} \exp(-iE_1) & 0 \\ 0 & \exp(-iE_2), \end{pmatrix} \right]$

и операцию $E$ как $U\ U = E(A \bigotimes B) = \left[ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \exp(i\Delta E). \end{pmatrix} \right]$

II. Используя иррациональность $\frac{\Delta E}{\pi}$ можно показать, что $\forall \varepsilon > 0 \exists m \in N \exists n \in N$ : $|\Delta E n - \pi(2m+1)| < \varepsilon$, то есть для любой выбранной ошибки $\varepsilon$ существует $n = n(\varepsilon)$ such that $U^n$ приближающий оператор $\Pi\ \Pi = \left[ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \right]$ сне более чем с этой ошибкой.

III. Используя равенство $(I \bigotimes H)\Pi(I \bigotimes H) = CNOT$, where $I$ is the identity matrix and $H$ - is Hadamard operation $H = \frac{1}{\sqrt{2}} \left[ \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \right]$ мы видим, что CNOT находится как $(I \bigotimes H)(E(A \bigotimes B))^n (I \bigotimes H)$ - однокубитное преобразование и оператор E.

## 7.2 Формализм чисел заполнения

Рассмотрим систему, состоящую из $n$ идентичных частиц. Во-первых, мы предположим, что их можно достоверно различить. Тогда состояние этой системы будет вектором пространства с базисом $\psi(r_1, r_2, \ldots, r_n) = \psi_{j_1}(r_1)\psi_{j_2}(r_2)\ldots\psi_{j_n}(r_n)$ где $\{\psi_j\}$некоторый базис одночастичных состояний, $j_s$ принадлежит некоторому фиксированному семейству индексов $1, 2, \ldots, J$, так что $r_j$ содержит как пространственные, так и спиновые координаты частицы $j$. Выбор базиса означает просто, что мы можем найти систему только в одном из базисных состояний после измерения.

Однако в реальной системе идентичных частиц они не могут быть различены надежно. Так что каждое базисное состояние должно содержать все слагаемые вида $\psi_{j_1}(r_1)\psi_{j_2}(r_2))\ldots\psi_{j_n}(r_n)$ с некоторыми коэффициентами. Теперь нам нужно нечто знать о природе рассматриваемых частиц. Они могут быть либо фермионами, как электроны, либо бозонами, как фотоны. Разница между этими классами частиц в том, что спины фермионов получелые (1/2, 3/2, ...) тогда как у бозонов они целые (0,1,2,...). Для нас же существенно, что волновая функция системы фермионов меняет знак при перестановке двух из них, а волновая функция бозонов при такой операции не меняется. Мы установим связь между функциональными обозначениями и кубитовой записью, так что волновая функция системы $n$ фермионов будет иметь вид детерминанта:

$$\Psi = \frac{1}{\sqrt{N!}} \begin{vmatrix} \psi_{j_1}(r_1) & \psi_{j_1}(r_2) & \ldots & \psi_{j_1}(r_n) \\ \vdots & \vdots & \vdots & \vdots \\ \psi_{j_n}(r_1) & \psi_{j_n}(r_2) & \ldots & \psi_{j_n}(r_n) \end{vmatrix}, \tag{86}$$

а для системы идентичных бозонов она имеет фид соответствующего перманента (перманент отличается от детерминанта тем, что в его разложении везде стоят плюсы а не минусы, как у детерминанта, так что перманент не меняется при перестановке его строк или столбцов).

Состояние (86) можно трактовать как ситуацию, когда только состояния $\psi_{j_s}$ для $s = 1, 2, \ldots, n$ заняты частицами, тогда как все остальные состояния $\psi_k$ for $k \in \{1, 2, \ldots, J\}$, не имеющие вида $j_s$ свободны. Если $\psi$ с индексами обозначает собственное состояние одночастичного гамильтониана, мы говорим о занятых или свободных энергетических уровнях, так будет дальше по умолчанию. Но в общем, $\psi_k$ могут образовывать произвольный ортонормированный базис в пространстве состояний одной частицы.

Состояние вида (86) мы будем представлять символом $|\bar{n}_\Psi\rangle = |n_1, n_2, \ldots, n_J\rangle$ где $n_k$ равно единице, если $k$-й энергетический уровень занят, и нулю, если он свободен. Это называется представлением состояний фермионного ансамбля в терминах чисел заполнения. Эти векторы $\bar{n}$ образуют базис в пространстве Фока чисел заполнения, и общий вид состояния рассматриваемой системы в этом базисе будет такой: $\sum_{\bar{n}} \lambda_{\bar{n}} |\bar{n}\rangle$ с амплитудами $\lambda$.

Оператор уничтожения $a_j$ фермиона в состоянии $j$ и сопряженный ему оператор рождения фермиона на данном уровне $a_j^+$ определяется как $a_j|n_1, \ldots, n_J\rangle = \delta_{1,n_j}(-1)^{\sigma_j}|n_1, \ldots, n_{j-1}, n_j - 1, n_{j+1}, \ldots, n_J\rangle$ где $\sigma_j = n_1 + \ldots + n_j$. Эти операторы подчиняются известным коммутационным соотношениям: $a_j^+ a_k + a_k a_j^+ = \delta_{j,k}$, $a_j a_k + a_k a_j =$

$a_j^+ a_k^+ + a_k^+ a_j^+ = 0$.

Предположим, что всякое взаимодействие в Природе затрагивает не более двух частиц. Тогда всякое взаимодейсствие в ансамбле многих тел можно представить в виде суммы одно- или двух- частичных взаимодействий вида $H = H_{one} + H_{two}$ с соответствующими потенциалами $V_1(r)$ и $V_2(r, r')$. Каждое из таких взаимодействий, в свою очередь, можно представить через операторы рождения и уничтожения как $H_{one} = \sum_{k,l} H_{k,l} a_k^+ a_l, \quad H_{two} = \sum_{k,l,m,n} H_{k,l,m,n} a_l^+ a_k^+ a_m a_n$ где

$$H_{k,l} = \langle \psi_k | \; H_{one} \; | \psi_l \rangle = \int \psi_k^*(r) V_1(r) \psi_l(r) dr,$$
$$H_{k,l,m,n} = \langle \psi_l, \psi_k \; | H_{two} \; | \; \psi_m \psi_n \rangle = \int \psi_k^*(r) \psi_l^*(r') V_2(r, r') \psi_m(r) \psi_n(r') dr dr'.$$

Итак, если заданы потенциалы всех взаимодействий, и все базисные состояния $\psi_i$, мы можем, в принципе, найти их представление через операторы рождения и уничтожения, то есть на языке числе заполнения.

Рассмотрим ансамбль с гамильтонианом вид $H = \sum_i H^i_{ext.f.} + \sum_{i,j} (H^{i,j}_{diag.} + H^{i,j}_{tun.})$, где гамильтонианы внешнего поля, диагонального взаимодействия и туннелирования представлены в виде

$$\begin{array}{ll} H^i_{ext.f.} & = \alpha_i a_i^+ a_i, \quad \alpha_i \in \mathrm{R}, \\ H^{i,j}_{diag.} & = \beta_{i,j} a_i^+ a_i a_j^+ a_j, \quad \beta_{i,j} \in \mathrm{R}, \\ H^{i,j}_{tun.} & = \gamma_{i,j} a_i^+ a_j + \gamma^*_{i,j} a_j^+ a_i. \end{array} \tag{87}$$

затрагивает только 2 произвольные частицы в данном ансамбле, которые неразличимы по принципу идентичности. Поэому естественно считать это взаимодействие постоянным и не зависимым от нашего контроля, тогда как мы можем эффективно управлять вычислением с помощью туннельного взаимодействия. Такая форма управления позволяет реализовать любое квантовое вычисление. Она выглядит более реалистичной, чем управление всеми типами взаимодействий; интенсивность туннелирования можно менять с помощью лазерных импульсов.

## 7.3 Вычисления, управляемые туннелированием

Для доказательства универсальности предлагаемой схемы управления вычислением через туннелирование мы должны сделать одно построение: установить нестандартное соответствие между гильбертовым пространством квантовых состояний и фоковским пространством чисел заполнения. Это соответствие не будет очевидным.

Разобъем все энергетические уровни на две равные множества и установим взаимнооднозначное соответствие между этими множествами, которое будем считать отныне фиксированным. Для определенности мы можем взять всякий $k$-й уровень ниже уровня Ферми $\epsilon_F$ условиться, что он соответствует $k$-му уровню выше уровн Ферми $\epsilon_F$. Обозначим $j$-й уровень ниже Ферми обычной буквой, а $j$-й уровень выше Ферми такой же буквой, но со штрихом: $j'$. Назовем первый из них $j$-м нижним уровнем, а второй $j$-м верхним уровнем. Пространство Фока $\mathcal{F}$ можно представить как $\mathcal{F} = \mathcal{F}_1 \bigotimes \mathcal{F}_2 \bigotimes \ldots \bigotimes \mathcal{F}_k$ где каждый $\mathcal{F}_j$ соответствует $j$-й паре соответствующих энергетических уровней.

Рассмотрим подпространство $F_j$ в $\mathcal{F}_j$, порожденное двумя следующими векторами. Первый имеет вид: "$j'$-й уровень занят, $j$-й свободен второй будет: "$j$-й уровень занят, $j'$-й свободен". Обозначим их через $|1\rangle_j$ и $|0\rangle_j$ соответственно. Мы будем работать с подпространством $F = F_1 \bigotimes F_2 \bigotimes \ldots \bigotimes F_k$ в пространстве Фока $\mathcal{F}$.

Определим функцию $\theta$, отображающую наше гильбертово пространство $\mathcal{H}$ в $F$, которое зададим его действием на бизисных векторах:

$$\theta(|\xi_1, \xi_2 \ldots \xi_n\rangle) = |\xi_1\rangle_1 \bigotimes |\xi_2\rangle_2 \bigotimes \ldots \bigotimes |\xi_n\rangle_n,$$

где все $\xi_j$ - нули или единицы. Эта функция $\theta$ устанавливает не стандартное соответствие между гильбертовым и фоковским пространствами (см. рисунок А2).

Однокубитное состояние в гильбертовом пространстве соответствует двухкубитному состоянию в фоковском при естественной идентификации с кубитами (один уровень = один кубит). Мы увидим, что это соответствие лучше подходит для наших целей, чем естественное соответствие между гильбертовым и фоковским пространствами. Теперь можно представить унитарные операторы, действующие в гильбертовом пространстве, через операторы, действующие в числах заполнения. Рассмотрим произвольный эрмитов оператор $H$ в двумерном гильбертовом пространстве состояний одного кубита $\mathcal{H}$. Он имеет вид $H_0 + H_1$, где

$$H_0 = \begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix}, H_1 = \begin{pmatrix} 0 & d \\ \bar{d} & 0 \end{pmatrix}.$$

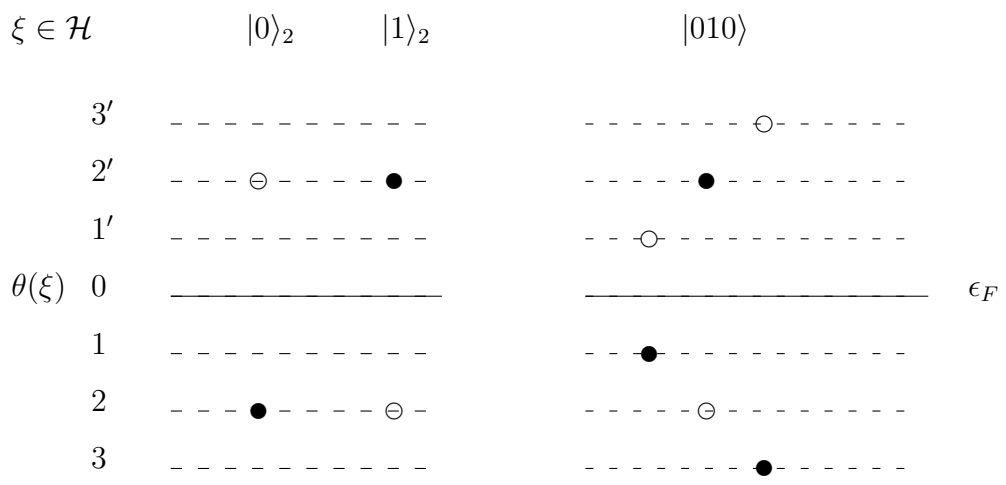


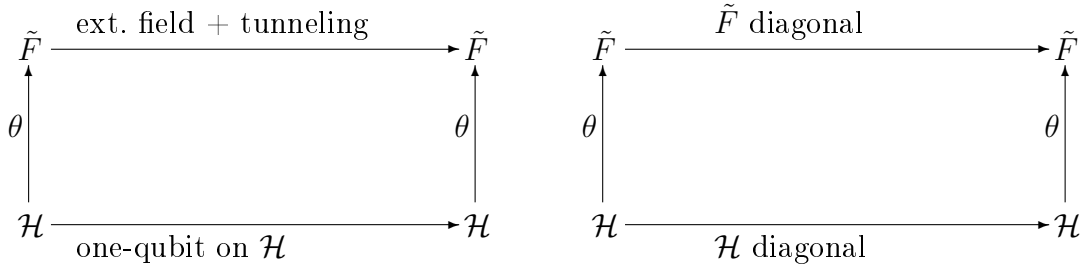

Рисунок А2. Соответствие между пространствами Гильберта и Фока

Неопредственно проверяется, что для операторов $\tilde{H}_0 = d_1 a_k^+ a_k + d_2 a_{k'}^+ a_{k'}$ и $\tilde{H}_1 = d a_k^+ a_{k'} + \bar{d} a_{k'}^+ a_k$ (внешнее поле и туннелирование) имеют место такие равенства: $\tilde{H}_i \theta = \theta H_i$ для $i = 0, 1$. Используя линейность $\theta$, получаем $(\tilde{H}_0 + \tilde{H}_1)\theta = \theta H$. Теперь рассмотрим однокубитный оператор $U$ в гильбертовом пространстве. Он имеет вид $e^{-iH}$ для гамильтониана $H$ мы выбираем единицы измерения так, чтобы избавиться от постоянной Планка и времени). Благодаря линейности $\theta$ и равенству $\theta^{-1} H^s \theta = (\theta^{-1} H \theta)^s$

для целых $s$ мы получим, что для любого однокубитного оператора $U$ можно эффективно найти соответствующий эрмитов оператор в пространстве Фока, содержащий только внешнее поле и туннелирование, так что диаграмма A на рисунке A3 будет замкнутой.

Теперь займемся двухкубитными операторами в гильбертовом пространстве. Так как все диагональные матрицы коммутируют, для всех таких операторов в пространствах $\mathcal{F}_k \bigotimes \mathcal{F}_j$ мы можем эффективно найти соответствующий диагональный оператор в гильбертовом пространстве, который делает замкнутой диаграмму B из рисунка A3.

Теперь все готово к адаптации приема из работы [25] с однокубитным управлением для фоковского пространства. Комбинация диаграмм из рисунка A3 дает диаграмму из рисунка A4.




A B

Рисунок A3. Соответствие операторов в подпространствах Фока и Гольберта. $\tilde{F} = F_j \bigotimes F_k$.

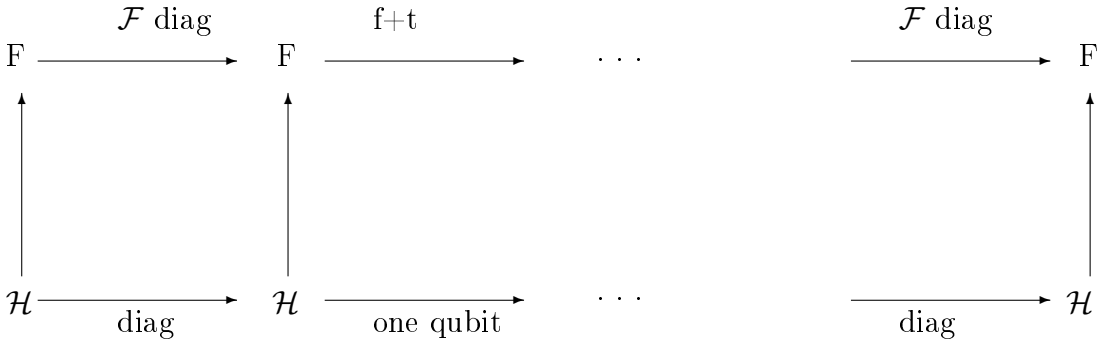



Рисунок А4. Соответствие вычислений в пространствах Фока и Гольберта

Пусть диагональная часть гамильтониана взаимодействия в фоковском пространстве фиксирована и действует непрерывно в неконтролируемом режиме. Мы можем найти соответствующее диагональное взаимодействие в гильбертовом пространстве, замыкая "диагональные" части диаграмм из рисунка А4. В силу результата работы [25] можно найти однокубитные операторы, с помощью которых мы сможем управлять любым квантовым алгоритмом в гильбертовом пространстве в виде нижней последовательности преобразований в этой диаграмме. Фока, которое замыкает всю данную диаграмму. Заметим, что все операторы рождения и уничтожения, рассматриваемые в фоковском пространстве, являются нелокальными ввиду наличия множителя $(-1)^{\sigma_j}$, зависящего от текущего состояния.

Для диагонального оператора $a_j^+ a_j a_k^+ a_k$ и внешнего поля эти сомножители компенсируют друг друга. Оператор туннелирования $a_j^+ a_{j'}$ в пространстве $F$ дает множитель $(-1)^{\sigma'}$ где $\sigma' = \sum_{s+j}^{j'-1} n_s = j' - j$, что не зависит от данного состояния $|\bar{n}\rangle \in F$, так как для такого состояния ровно половина уровней между $j$ и $j'$ занято фермионами. Общий множитель мы можем вынести за скобки из всех состояний, и проигнорировать .

Таким образом, мы построили универсальный квантвоый компьютер в пространстве чисел заполнения, управляемый только внешним полем и туннелированием.

# 8 Лекция 8. Реализация квантовых вычислений на оптических полостях

Физическая реализация квантовых вычислений - отдельная большая тема, требующая физического фундамента для построения гейтов. Здесь мы приведем пример такой реализации на атомных возбуждениях в оптических полостях. Физическая часть описывается в рамках конечномерных моделях квантовой электродинаимик в оптических полостях - модель Джейнса-Каммингса-Хаббарда.

## 8.1 Модель Джейнса-Каммингса

Трудность экспериментального учета электромагнитного поля состоит в том, что его кванты возбуждения путешествуют со скоростью света, так что едва появившись, фотон через секунду уже преодолеет большую часть расстояния от Земли до Луны. Метод удержания фотонов идейно прост: надо расположить друг напротив друга зеркала, отражающие фотон, так, чтобы он бегал между ними и не улетал далеко в течение достаточно большого времени.

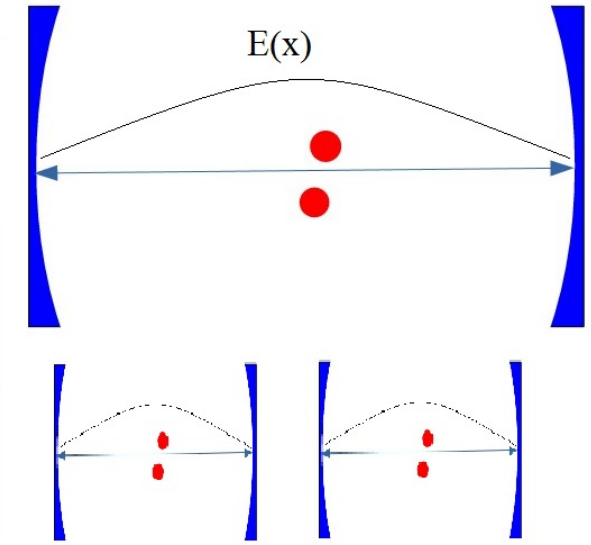



Рис. 49: Оптическая полость с атомами

Это устройство называется интерферометром Фабри-Перо (см. рисунок 49). Два зеркала образуют своеобразную полость, или резонатор, в который фотон можно запустить с помощью лазера, и извлечь с помощью зеркала с переменной отражательной способностью; такое зеркало называется ячейкой Поккельса. На ячейку можно подать напряжение, тогда она начнет отражать упавший на нее фотон; при выключенном же напряжении она становится прозрачной и фотон проходит через нее свободно. Боковые стенки полости также делают из отражающего свет материала.

Возможные манипуляции с атомами в полости показаны на рисунке 50.

Если в такую оптическую полость поместить атом, он сможет взаимодействовать

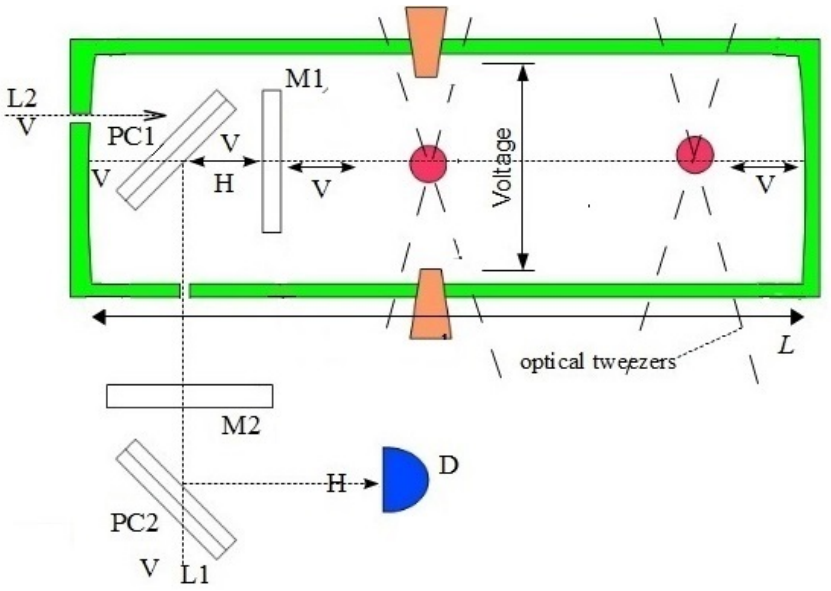



Рис. 50: Манипуляции с атомами в оптической полости

с полем внутри полости, если для каких-то уровней энергии его электронов, которые мы обозначаем через $|0\rangle$ - условно основной, и $|1\rangle$ - условно возбужденный уровни, энергия перехода между этими уровнями $\Delta E = \hbar\omega$ такова, что $\omega$ очень точно приближает частоту фотона в полости. При этом при поглощении фотона атом переходит от основного состояния $|0\rangle$ к возбужденному $|1\rangle$, и наоборот, при обратном переходе атома происходит испускание фотона. Полный цикл взаимодействия атома с полем, включающий поглощение атомом фотона и последующее его испускание, называется осцилляцией Раби. Для того, чтобы произошла одна такая осцилляция, например, в атоме рубидия $Rb^{85}$, где частота перехода между уровнями составляет примерно $\omega_{Rb} \approx 10^{10}\ sek^{-1}$ фотон должен удерживаться в полости достаточно долго, так что за это время он успевает отразиться от зеркал несколько десятков тысяч раз. Поэтому зеркала должны быть очень качественными; их делают из сверхпроводящего материала, например, ниобия, и они функционируют при очень низкой температуре жидкого гелия.

Но качества зеркал недостаточно, так как фотон может просочиться из полости за счет своей интерференционной природы. Эта природа следует из принципа интерференции, который мы кратко описали в первой главе. Я рекомендую слушателю обратиться к детальному разъяснению действия этого принципа по отношению к фотонам, приведенному в книге Р.Фейнмана [7]. Для того, чтобы фотон долго оставался в полости, необходимо, чтобы создаваемое им электрическое поле конструктивно интерферировало само с собой внутри полости, и деструктивно - вне ее. Это обеспечивается длиной полости - расстоянием между зеркалами $L$. Длина должна быть кратной полуволне длины фотона, то есть $L = k\lambda/2$, где $\lambda = 2\pi c/\omega$, $k = 1, 2, ....$

Помещенный в полость атом взаимодействует с полем с энергией взаимодействия $g$, которая вычисляется по формуле

$$g = \sqrt{\frac{\hbar\omega}{V}} dE(x), \tag{88}$$

где $V$- эффективный объем полости (объем, где присутствует фотон), $d$ - абсолютная

величина дипольного перехода $\bar{d}$ между $|0\rangle$ и $|1\rangle$, $E(x)$ - фактор расположения атома внутри полости. Цель состоит в том, чтобы сделать $g$ как можно больше, для возможно быстрейшего проявления свойств взаимодействия света и вещества. Поэтому длина полости должна выбираться так, что $k = 1$, и $L = \lambda/2$. В этом случае конструктивная интерференция электрического поля фотона внутри полости максимальна, и его напряженность распределена по синусоиде, так что $E(x) = sin(\pi x)/L$.

Дипольный переход считается по формуле $\bar{d} = e \int\limits_{R^3} \psi_0^* \bar{r} \psi_1 d\bar{r}$, где $\psi_0,\ \psi_1$ - волновые функции состояний электрона в основном и возбужденном состояниях внутри атома, зависящие от трехмерного вектора $\bar{r}$, $e$ - заряд электрона. Фактический вывод формулы (88) можно найти в книге [8]. Константа $g$, вообще говоря, комплексна, но можно с помощью домножения базисного вектора $|1\rangle$ на подходящее комплексное число $e^{i\phi}$ добиться, чтобы $g$ было вещественным неотрицательным числом, что мы и будем в дальнейшем предполагать.

Таким образом, взаимодействие поля с атомом внутри полости есть взаимодействие атома с квантовым гармоническим осциллятором, описанным в Приложении к [27]. Условная "координата" $x$ поля с точностью до констант выражается через операторы рождения $a^+$ и уничтожения $a$ фотона в поле как $x = a^+ + a$.

Введем, аналогично полевым операторам, операторы $\sigma^+, \sigma$ - атомные операторы возбуждения и релаксации; у нас получится набор операторов поля и атомов вида

$$\begin{array}{lll} a: & |n\rangle_{ph} \to \sqrt{n}|n-1\rangle_{ph}, & a^+ : |n\rangle_{ph} \to \sqrt{n+1}|n+1\rangle_{ph}, \\ \sigma: & |0\rangle_{at} \to 0, & |1\rangle_{at} \to |0\rangle, \\ \sigma^+: & |0\rangle_{at} \to |1\rangle_{at}, & |1\rangle_{at} \to 0, \end{array} \tag{89}$$

так что число фотонов $n = 0, 1, 2, ...$, а число, характеризующее атомное возбуждение, принимает только два значения 0 или 1, причем релаксация $\sigma$ атома, уже находящегося в основном состоянии $|0\rangle_{at}$, приводит к уничтожению состояния как такового (ноль в пространстве состояний), а возбуждение уже возбужденного состояния атома дает тот же результат; в остальных случаях операторы действуют естественным образом.

Введем условную "координату" атомного возбуждения $X$ по аналогии с полевой "координатой": $X = \sigma^+ + \sigma$. Пусть взаимодействие поля с атомом обозначается через $G(x, X)$, где $x,\ X$- условные "координаты" поля и атомного возбуждения соответственно. Раскладывая эту функцию в ряд Тейлора, мы видим, что самый младший член взаимодействия, содержащий обе координаты, имеет вид $gxX = g(a^+ + a)(\sigma^+ + \sigma)$. Это называется дипольным приближением взаимодействия атома и поля. Оно справедливо, если размер атома существенно меньше длины волны фотона; такое предположение выполняется в большинстве практически важных случаев, например, в химии.

Если учесть следующие члены в разложении Тейлора функции
$G(x, X)$, получатся более высокие члены в приближении взаимодействия; ими мы не будем заниматься.

Собственные энергии атома и поля, согласно Приложению, даются формулами $E_{at} = \hbar\omega\sigma^+\sigma$, $E_{ph} = \hbar\omega a^+ a$. Энергию вакуумного состояния $\hbar\omega/2$ мы опускаем, так

как в данном случае она не играет роли.[2] Суммируя их с энергией взаимодействия, мы получаем гамильтониан Джейнса-Каммингса для двух-уровневого атома в оптической полости:

$$H_{JC} = \hbar\omega a^+ a + \hbar\omega\sigma^+\sigma + g(a^+ + a)(\sigma^+ + \sigma). \tag{90}$$

Решать задачу Коши для уравнения Шредингера с таким гамильтонианом довольно сложно. Дело в том, что взаимодействие содержит члены $a\sigma$ и $a^+\sigma^+$. которые по отдельности не сохраняют энергию. Это означает, что для потенциально бесконечной матрицы оператора $H_{JC}$ нет конечномерных инвариантных подпространств, и приходится иметь дело с бесконечностями, что затруднительно и неверно по существу.

К счастью, эта трудность обходится для большей части приложений, где сила взаимодействия $g$ мала по сравнению с энергией возбуждения $\hbar\omega$ атома. Если $g/\hbar\omega \ll 1$, не сохраняющие энергию члены можно отбросить, и гамильтониан примет гораздо более удобный вид

$$H_{JC}^{RWA} = \hbar\omega a^+ a + \hbar\omega\sigma^+\sigma + g(a^+\sigma + a\sigma^+). \tag{91}$$

Это так называемое приближение вращающейся волны RWA, его вывод можно найти в Приложении.

Наша физическая система - композитная. Она состоит из двух частей: поля и атома. Договоримся обозначать базисные состояния, выписывая сначала число фотонов в поле, а затем - атомное возбуждение: $|n, m\rangle$, так что $n = 0, 1, 2, ...$, $m = 0, 1$, и опускать нижние индексы $ph$ и $at$. При записи операторов примем обычно соглашение: если не указан оператор, действующий на другой элемент композитной системы, он предполагается оператором идентичным: $I_{at}$ или $I_{ph}$. Таким образом, например, запись $a^+a$ надо трактовать как $a^+a \otimes I_{at}$, а запись $a\sigma^+$ - либо как $a \otimes \sigma^+$, либо как матричное произведение $a \otimes I_{at} \cdot I_{ph} \otimes \sigma^+$. Проверьте, что оба пути дают один и тот же результат.

Для гамильтониана $H_{JC}^{RWA}$ пространство квантовых состояний распадается в прямую сумму инвариантных двумерных подпространств $\mathcal{H}_n$, каждое соответствует энергии $E_n = \hbar\omega n$, и порождается векторами $|n, 0\rangle,\ |n-1, 1\rangle$. Гамильтониан, ограниченный на $\mathcal{H}_n$, имеет вид

$$H_n = \begin{pmatrix} \hbar\omega n & g\sqrt{n} \\ g\sqrt{n} & \hbar\omega n \end{pmatrix}. \tag{92}$$

Выражение (92) говорит о том, что состояния $|n, 0\rangle$ и $|n-1, 1\rangle$ переходят одно в другое в ходе эволюции, причем их населенность меняется по синусоидальному закону (см. рисунок 51).

Отсюда видно, что населенности состояний $|n, 0\rangle$ и $|n-1, 1\rangle$ чередуются, колеблясь в противофазе. Если на одной из вершин графика населенности состояния $|n, 0\rangle$

[2] Слушателю предоставляется проверить, что добавление константы к гамильтониану, то есть переход от $H$ к $H + cI$, приводит только к появлению дополнительного фазового множителя вида $e^{-ict/\hbar}$ в решении уравнения Шредингера, который не имеет физического смысла и исчезает при переходе к уравнению Шредингера для матрицы плотности.

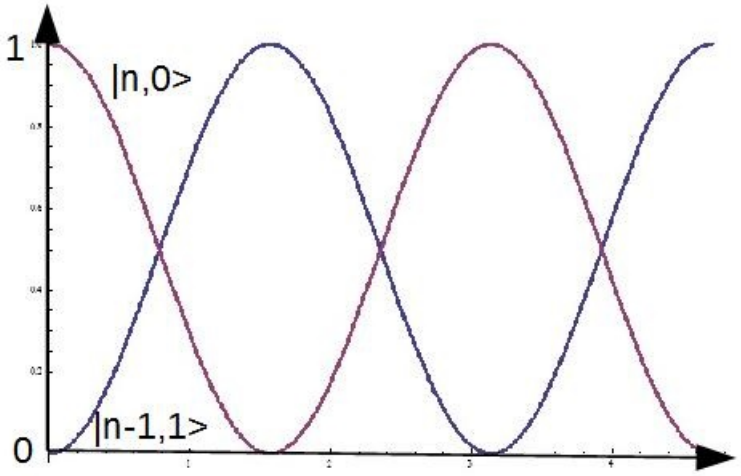



Рис. 51: Осцилляции Раби между населенностями состояний $|n,0\rangle$ и $|n-1,1\rangle$.

каким-то образом извлечь из полости фотоны (это делается с помощью специального оптического зеркала - ячейки Поккельса), то атом останется в полости в основном состоянии. Это важное замечание пригодится нам в дальнейшем, при конструировании квантового гейта coCSign.

## 8.2 Модель Тависа-Каммингса-Хаббарда

Если соединить две полости волноводом, состоящим из оптического волокна, по которому фотоны из одной полости смогут перемещаться в другую полость, мы получим более сложную модель, которая описывается гамильтонианом Тависа-Каммингса-Хаббарда вида

$$H_{TCH} = \sum_{i=1}^{m} H_{TC}^{i} + \sum_{1\leq i<j\leq m} \mu_{ij}(a_i^+ a_j + a_i a_j^+). \tag{93}$$

Эта модель ближе к реальности, чем однополостная, так как здесь уже допускается возможность для фотонов стать различимыми, оказавшись в разных полостях (см. рисунок 52).

## 8.3 Запутывающий гейт в модели JCH

Квантовый компьютинг представляет собой вторжение квантовой теории в область сложных процессов, где действие ее основных законов пока не изучено. Поэтому конструирование наиболее простых схем таких вычислений, в которых квантовые законы проявлялись бы как можно яснее, является актуальной задачей. Темное место здесь - декогерентность, возникающая из-за взаимодействия зарядов и поля, кванты которого тесно связывают квантовый компьютер с окружением. Это делает

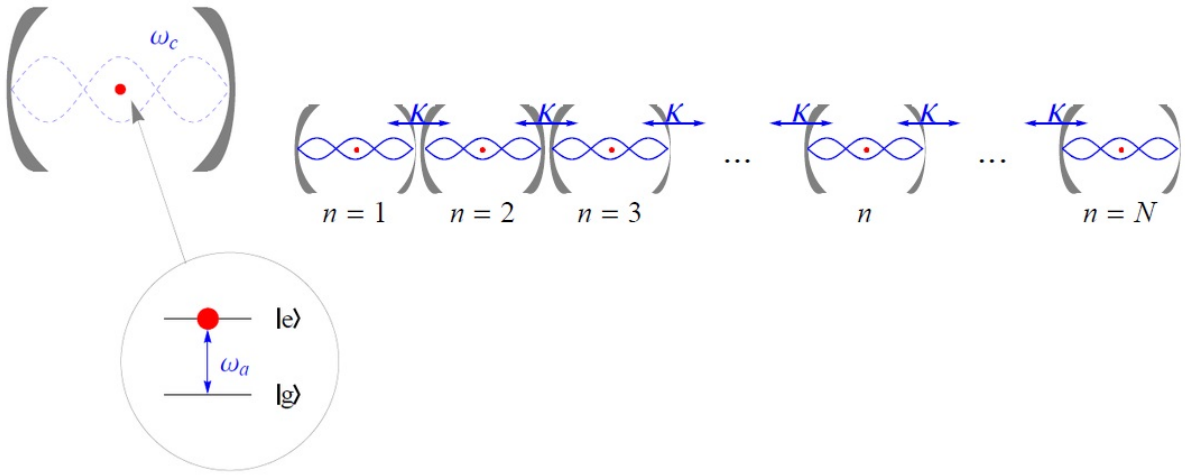



Рис. 52: Модель Джейнса-Каммингса-Хаббарда. Модель ТСН отличается только наличием нескольких атомов в полостях

необходимым учет и контроль, или даже явное использование фотонов в квантовых протоколах.

Фотоны как носители информации дают возможность использовать линейные оптические приборы для реализации однокубитных гейтов, но конструирование запутывающих операций трудно, так как фотоны непосредственно не взаимодействуют друг с другом. Есть популярная KLM- схема (см. [28]), где используются измерения в качестве эрзаца взаимодействия, и ее усовершенствование [29] с телепортацией (см. [30]), значительно повышающее ее эффективность, а также ряд вариантов этой схемы для атомов (см., например, [31]). Однако использование классических вероятностных схем при практической реализации предъявляет повышенные требования к эффективности, по крайней мере, теоретической, квантовых гейтов на единичных частицах. Использование классической вероятности затеняет главный вопрос квантового компьютера: как когерентность работает для сложных систем из разных частиц?

Здесь больше подходят наиболее первопринципные методы, главным из которых являются оптические полости с несколькими атомами, взаимодействие которых с одномодовым полем четко описывается из первых принципов (о возможностях данного типа устройств см., например, [32]). Так, гейт CNOT был реализован с использованием внешних - колебательных - степеней свободы атома (см. [33]). Однако суть квантового компьютинга - в когерентном поведении не отдельного кубита, а в масштабировании фейнмановского квантового процессора, реализующего теоретические возможности унитарной динамики во всем гильбертовом пространстве состояний, дающее, например, алгоритм Гровера [12] на том же оборудовании, что и алгоритм Шора [18]. Использование внешних факторов для демонстрации динамики отдельных атомов и поля полезно именно для отдельных атомов, но вносимые неизбежные помехи наверняка скажутся при масштабировании.

Поэтому ценность представляют схемы реализации гейтов, использующие минимальные средства, которые хорошо описываются из первых принципов. Одна из таких схем предложена в статье Х.Азумы [39], где в качестве кубитов используются двух-рельсовые состояния единичных фотонов. В этой схеме взаимодействие фото-

нов с атомами используется лишь для совершения запутывающего преобразования $CSign$, для которого требуется две оптические полости; необходимы также два светоделителя и фазовращатели.

Мы опишем упрощение схемы Азумы, где используется только одна полость, а светоделители заменены временным сдвигом для фотонов, поступающих в нее. Логическими кубитами у нас будут асинхронные состояния атомов в рабиевских осцилляциях. Эту схему можно переделать для чисто фотонных носителей, со временным сдвигом, определяющим значение кубита. Однако атомы как носители информации обладают тем преимуществом, что их гораздо легче контролировать, как и испускаемые ими фотоны. Достоинство предлагаемой схемы в ее простоте. Недостаток, тот же, что и в схеме [39] - зависимость от временной точности срабатывания ячейки Поккельса или ее аналога, время работы которой надо сделать существенно меньше времени рабиевской осцилляции атома в полости.

По техническим причинам мы будем реализовывать гейт $coCSign : |x,y\rangle \to (-1)^{x(y\oplus 1)}|x,y\rangle$, меняющий знак при единственном состоянии $|10\rangle$, родственный гейту $CSign$, который реализован в [39]; разницы нет никакой, так как $coCSign = CSign\sigma_x(y)$, а однокубитные гейты реализуются линейными оптическими устройствами.

## 8.4 Расчет фазовых сдвигов

Ядро данной схемы - оптическая полость с одним двухуровневым атомом с энергетической щелью $\hbar\omega$ между основным $|0\rangle$ и возбужденным $|1\rangle$ уровнями, где $\omega$ совпадает с частотой фотона определенной моды, удерживаемого в полости. Константа взаимодействия $g$ между атомом и полем предполагается малой: $g/\hbar\omega \ll 1$ (практически, это отношение должно быть не больше $10^{-3}$) для возможности применения RWA приближения, в котором гамильтониан Джейнса-Каммингса системы "атом+поле" ([35]) имеет вид

$$H = H_{JC} = H_0 + H_{int};\ H_0 = \hbar\omega a^+a + \hbar\omega\sigma^+\sigma,\ H_{int} = g(\alpha^+\sigma + a\sigma^+), \qquad (94)$$

где $a, a^+$- операторы уничтожения и рождения фотона, $\sigma, \sigma^+$- релаксации и возбуждения атома. Будем записывать базисные состояния атома и поля в виде $|n\rangle_{ph}|m\rangle_{at}$, где $n = 0, 1, 2, ...$ - число фотонов в полости, $m = 0, 1$ - число атомных возбуждений. У нас будет $n = 0, 1, 2$. Мы будем рассматривать несколько полостей, и снабжать операторы полости $i$ нижним индексом $i$, так что общий гамильтониан будет равен сумме $\sum_i H_i$; взаимодействие атомов с полем $H_{int}$ во всех областях будет тогда равно, соответственно, сумме $\sum_i H_{int\ i}$. Гамильтониан в ходе выполнения гейта $coCSign$ будет меняться: к его слагаемому $H_{int}$ будет добавляться слагаемое вида $H_{jump} = \nu(a_i a_j^+ + a_j a_i^+)$, означающее переход фотона из полости $i$ в полость $j$ и наоборот, но энергия независимых атомов и поля $H_0$ не изменится (модель Джейнса-Каммингса-Хаббарда JCH). Поэтому набег фазы, связанный с $H_0$, будет общим для всех состояний, и его можно игнорировать. Далее мы будем считать набег фазы относительно либо тождественного оператора $I$, либо относительно $\sigma_x$, так как все операции, рассмотренные ниже, сводятся либо к первой, либо ко второй с изменением фазы, так что набег фазы при применении, например, $-i\sigma_x$ составит $-\frac{\pi}{2}$.

Пусть $\tau_1 = \pi\hbar/g,\ \tau_2 = \pi\hbar/g\sqrt{2}$ - периоды рабиевских осцилляций для общей энергии $\hbar\omega$ и $2\hbar\omega$ соответственно. Операторы $U_t = e^{-\frac{i}{\hbar}Ht}$, индуцируемые эволюцией в важные моменты времени, будут зависеть от общей энергии полости. Если она равна $\hbar\omega$, в базисе $|\phi_0\rangle = |1\rangle_{ph}|0\rangle_{at},\ |\phi_1\rangle = |0\rangle_{ph}|1\rangle_{at}$, мы имеем:

$$U_{\tau_1/2} = -i\sigma_x,\ U_{\tau_1} = -I,\ U_{2\tau_1} = I, \tag{95}$$

где $\sigma_x$- матрица Паули, и аналогичные соотношения с заменой $\tau_1$ на $\tau_2$ при общей энергии полости $2\hbar\omega$.

При перемещении фотона из полости $j$ в полость $i$ и наоборот, что реализуется одновременным включением ячеек Поккельса или подобных им устройств в данных полостях, реализуется добавка $H_{jump}$ к взаимодействию $H_{int}$, которая при отсутствии в полостях атомов реализует в точности ту же динамику, что и рабиевские осцилляции, но с периодом $\tau_{jump} = \pi\hbar/\nu_{i,j}$. Мы будем считать, что $\nu \gg g$, так что возможно перемещение фотона из полости в полость так, чтобы атом вообще не влиял на этот процесс, так что набег фаз можно считать по формулам, аналогичным (95). Как отмечено в работе [39] это трудно реализовать в эксперименте, однако есть основания считать это технической трудностью. В случае выполнения этого условия набег фазы при операторе $\sigma_x$, примененной к фотонам двух полостей составит, так же как и для половины рабиевской осцилляции, $-\pi/2$.

В силу несоизмеримости периодов рабиевских осцилляций $\tau_1$ и $\tau_2$ мы можем выбрать такие натуральные числа $n_1$ и $n_2$, что будет выполняться с высокой точностью приближенное равенство

$$2n_2\tau_2 \approx 2n_1\tau_1 + \frac{\tau_1}{2}, \tag{96}$$

которое и будет основой для нелинейного фазового сдвига, необходимого для реализации $coCSing$.

## 8.5 Реализация coCSign

Состояние кубита $|0\rangle$ реализуется в нашей модели как состояние оптической полости вида $|0\rangle_{ph}|1\rangle_{at}$, а состояние кубита $|1\rangle$ - как $|1\rangle_{ph}|0\rangle_{at}$. Таким образом, для состояния $|10\rangle$, которому требуется инвертировать фазу, имеет вид $|10\rangle_{ph}|01\rangle_{at}$, где первый фотонный кубит относится к полости $x$, а второй - к полости $y$. Заметим, что через время $\tau_1/2$ ноль и единица меняются местами с набегом фазы, который входит в $H_0$, и потому игнорируется.

Последовательность операций, реализующих $coCSign$, изображена на рисунке 53, а участвующие полости - на рисунке 54. Сначала мы запускаем во вспомогательную полость с атомом в основном состоянии и вакуумным состоянием поля фотон из полости $x$, затем, с задержкой $\tau_1/2$ - фотон из полости $y$, затем, через время $2n_2\tau_2$, перемещаем фотон из вспомогательной полости в полость $x$, затем, через время $\tau_1/2$ перемещаем фотон из вспомогательной полости в полость $y$. Из нашего выбора времен перемещений фотонов вытекает, что в данные моменты в участвующих полостях будет либо один фотон, либо ни одного, поэтому включение ячеек Поккельса на малом временном отрезке $\delta\tau = \pi\hbar/2\nu \ll \tau_1$ даст именно перемещение фотонов.

Из предыдущих расчетов следует, что при энергии центральной полости $\hbar\omega$ (этот вариант реализуется для начальных состояний $|00\rangle,\ |11\rangle$) набег фазы при переносе

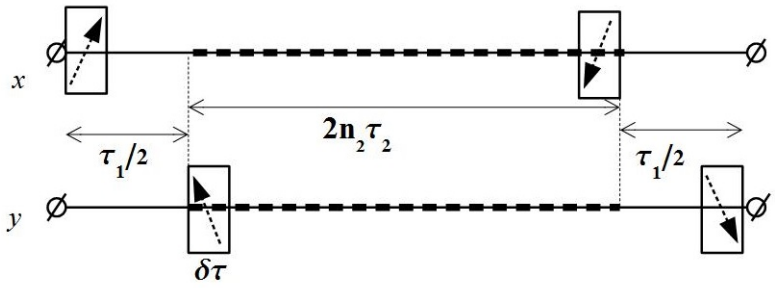



Рис. 53: Последовательность операций при реализация гейта coCSign: $|x, y\rangle \rightarrow (-1)^{x(y\oplus 1)}|x, y\rangle$ на асинхронных атомных возбуждениях в оптических полостях, $\delta\tau = \tau_{jump}/2$

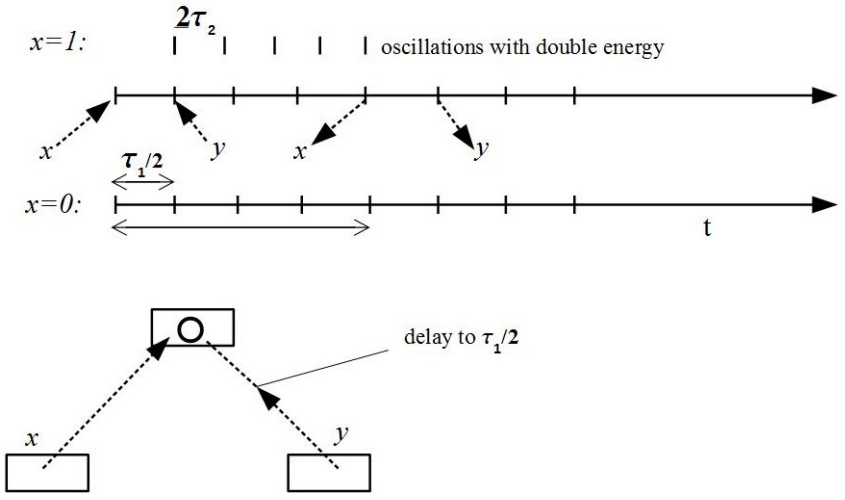



Рис. 54: Реализация гейта coCSign

фотона туда и обратно составит $-\pi$, а во взаимодействии с атомом $-\pi$, так что суммарный набег фазы будет нулевой, как и в случае нулевой энергии центральной полости (начальное состояние $|01\rangle$). Для энергии $2\hbar\omega$ - в случае $x = 1, y = 0$ перенос двух фотонов даст нуль, а взаимодействие даст $-\frac{\pi}{2} - \frac{\pi}{2} = -\pi$, что и требовалось.

Теперь слушатель может сам проверить, что при высокой точности соблюдения равенства (96)данна схема реализует оператор $coCSign$ с высокой точностью.

В статье [36] приведен расчет, из которого следует, что для достижения удовлетворительной точности подобных запутывающих гейтов на нелинейности в полостях достаточно взять числа несоизмеримых периодов $n_1, n_2$, не превосходящие нескольких десятков, что соответствует числу наблюдаемых рабиевских осцилляций в оптических полостях.

## 8.6 Реализация однокубитных гейтов

Для квантового вычисления, кроме запутывающего гейта coCSign, необходимы также однокубитные гейты. Мы покажем, как можно реализовать два гейта: вращатель фазы $|x\rangle \to e^{i\phi x}|x\rangle$ и оператор Адамара $H : |x\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x|1\rangle)$.

Во-первых, заметим, что определенные нами логические кубиты различаются только временем появления явного фотона в полости. Пусть к полости подсоединены два волновода, 1 и 2. Используя быстрое включение и выключение ячейки Поккельса, как и выше, мы можем направить фотон по волноводу 1, в случае, если логический кубит равен нулю, и по волноводу 2, если он равен единице.

Фазовращатель изменяет фазу логического кубита, наращивая ее на угол $\phi$, в том и только в том случае, когда он равен единице. Для такого изменения фазы достаточно удлинить волновод 2, в который попадет фотон, если логический кубит равен единице. Излишек длины наматывается на катушку, так что на выходе у нас снова будут те же фотоны, но сдвиг фазы по волноводу 2 будет равен $\phi$. Так как период рабиевских осцилляций $\tau$ значительно превосходит длину волны фотона, такое удлинение пути фотона во втором волноводе никак не скажется на определении логических кубитов.

Теперь перейдем к гейту Адамара $H$. Для его реализации мы используем линейный светоделитель, изображенный на рисунке 55. Это устройство реализует преобразование фотонов в волноводах 1 и 2 вида:

$$\begin{aligned} |n_1 m_2\rangle = \tfrac{1}{\sqrt{n!m!}}(a_1^+)^n(a_2^+)^m|0_1 0_2\rangle \quad &\to \\ &\tfrac{1}{\sqrt{n!m!}}[\tfrac{1}{\sqrt{2}}(a_1^+ + a_2^+)]^n[\tfrac{1}{\sqrt{2}}(a_1^+ - a_2^+)]^m|0_1 0_2\rangle, \end{aligned} \tag{97}$$

где нижний индекс обозначает номер волновода. При $n = 1, m = 0$ или $n = 0, m = 1$, то есть для одного логического кубита, это преобразование в точности даст оператор Адамара.

Таким образом, однокубитные гейты, необходимые для реализации, например, алгорима Гровера, можно сделать на оптических полостях, в рамках модели Джейнса-Каммингса-Хаббарда. Первая трудность в реализации гейта $coCSign$ - в быстроте срабатывания ячейки Поккельса, что представляется технически преодолимым

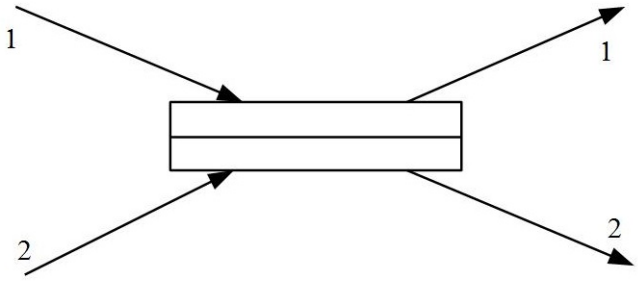



Рис. 55: Светоделитель.

делом. Вторая трудность - уширение спектральных линий полости. Соотношение неопределенностей "энергия - время" означает возникновение неопределенности частоты фотона при его быстром перемещении из полости в полость; это ведет к уменьшению времени жизни фотона в полости. Самый простой выход - в уменьшении силы взаимодействия атомов с полем, что удлинило бы период рабиевских осцилляций, однако это, в свою очередь, привело бы также к уменьшению времени жизни фотона в полости. Обе эти трудности есть и для схемы Азумы; возможности их преодоления они нуждаются в дальнейшем исследовании.

Достоинство предложенной схемы реализации гейтов - в ее простоте и возможности точного следования теоретической модели JCH, что, несмотря на упомянутую техническую трудность внушает оптимизм в плане масштабируемости и сравнения теории квантового компьютера с экспериментами на большом числе кубитов.

## 8.7 Матрица плотности

До сих пор мы рассматривали либо унитарную эволюцию, либо измерение - это идеализированная схема. В реальности квантовая память находится в тесном окружении разичных частиц и электромагнитного поля разных мод. Например, атом в полости взаимодействует с фотоном ограниченное время, так как время жизни фотона в полости ограничено: он вылетаект из нее вовне. При контакте с окружением состояние $|\Psi\rangle$, которое мы в дальнейшем будем называть чистым, портится специфическим образом: оно превращается в смешанное состояние, которое уже нельзя описать в виде вектора состояния $|\Psi\rangle$, а можно лишь в виде матрицы плотности. Ее мы сейчас и изучим.

Рассмотрим матрицу $|\Psi\rangle\langle\Psi| = \rho_\Psi$, ассоциированную с состоянием $|\Psi\rangle$. Это матрица плотности Ландау данного состояния. Она эрмитова и ее ранг и след равны единице. Эти три условия на матрицу, в свою очередь, означают, что она имеет вид $\rho_\Psi$ для некоторого вектора $|\Psi\rangle$. *Слушателю предлагается доказать эти утверждения самостоятельно.* На диагонали матрицы плотности стоят вероятности $p_j$, а внедиагональные члены, называемые когерентностями, символизируют квантовые свойства данного состояния $|\Psi\rangle$: если оно базисное, у него нет квантовых свойств, оно классическое.

При изменении базиса матрица плотности преобразуется по матричному закону: $\rho_\Psi \to T\rho_\Psi T^*$, где $T$ - унитарный оператор перехода к новому базису.

В непрерывном случае матрицы плотности - это функция вида $\bar{\Psi}(r_1,t)\Psi(r_2,t)$, где $r_1, r_2$ - пара возможных положений частицы.

Правило Борна - единственное связующее звено между квантовым формализмом и экспериментами. Мы не можем извлечь никакой информации о состоянии, в котором находится данная частица иначе, чем проведя над ней измерение в каком-либо заранее выбранном базисе. Для определения амплитуд $\lambda_j$ состояния $|\Psi\rangle$ надо произвести много измерений над многими одинаково приготовленными в этом состоянии частицами. Причем после измерения состояние частицы необратимо меняется, так что мы, вообще говоря, не можем использовать одну и ту же частицу.

Может показаться, что если мы измеряем частицу в каком-либо базисе, то после повторного измерения мы получим тот же самый результат, так как результат проекции состояния на выбранный заранее базисный вектор $|j\rangle$ имеет вид $|j\rangle\langle j|$ (докажите!) и его квадрат равен все той же проекции. Но это - грубая ошибка, характерная для копенгагенской физики, в которой формализм существует отдельно от реальности. В действительности измерение не может существовать отдельно от так называемой унитарной динамики, (см. выше, решение уравнение Шредингера) как и унитарная динамика - без измерения. Измеряя, например, координату, мы неизбежно придадим частице такой импульс, что она улетит за пределы нашей лаборатории, так что повторно измерить координату нам придется уже у другой частицы.

Уравнение Шредингера для матрицы плотности имеет вид

$$i\hbar\dot{\rho} = [H,\rho] = H\rho - \rho H; \tag{98}$$

оно эквивалентно обычному уравнению Шредингера и легко выводится из него. Таким образом, решение уравнения (98) представляет собой унитарную динамику в гильбертовом пространстве состояний, то есть динамику в отсутствии декогерентности, когда мы предполагаем отсутствие измеряющего систему влияния окружения.

## 8.8 Открытая квантовая система. Квантовое основное уравнение

Что происходит при контакте рассматриваемой системы со средой, не имеющей долговременной памяти, но способной вызывать измерения какой-то части системы? Этот вопрос имеет большое практическое значение. Например, если атом испускает фотон, и этот фотон улетает прочь, находясь в запутанном состоянии с атомом, измерение этого фотона автоматически приведет к появлению смешанного состояния атома, то есть вызовет декогерентность, при которой атом надо описывать матрицей плотности.

Мы вообще можем не знать, что происходит с вылетевшим фотоном; может быть, его никто и не наблюдает, а он отразится от далекого зеркала и прилетит к нам вновь - все равно если его нет рядом, мы должны рассматривать состояние имеющегося у нас атома как смешанное. Прилетит вновь испущенный когда-то и никем не измеренный фотон - хорошо, система "атом-фотон" опять будет в чистом состоянии, а если прилетит другой фотон вместо нашего, попавшего в чей-то детектор, вот тогда у нас будет матрица плотности смешанного состояния композитной системы. То есть мы

можем определить, подвергался ли фотон измерению только тогда, когда он к нам прилетит вновь. Если мы устроим эксперимент так, что на каждом его повторении к нам будет прилетать фотон, мы можем, изменяя базис, определить методом томографии, было ли измерение, то есть тот ли это фотон, который когда-то вылетел из нашего атома, или другой: при детектировании фотон исчезает.

Однако этот метод - статистический. С его помощью мы можем только проверить, есть ли систематическое измерение вылетающих фотонов в однотипных экспериментах, или измерений нет, и все фотоны отражаются от зеркала, прилетая к нам обратно. Для конкретного случая нельзя сделать такое заключение: выводы квантовой теории всегда только статистические.

Изменение во времени матрицы плотности системы, взаимодействующей со стационарным окружением, не имеющим долговременной памяти, описывается обобщением уравнения Шредингера для матрицы плотности, которое называется квантовым основным уравнением Коссаковского - Линдблада - Глаубера - Сударшана:

$$i\hbar\dot{\rho} = [H,\rho] + i\mathcal{L}(\rho), \quad \mathcal{L}(\rho) = \sum_{j=1}^{N^2-1} \gamma_j (A_j \rho A_j^+ - \frac{1}{2}\{A_j^+ A_j, \rho\}) \tag{99}$$

где операторы $A_j$ называются факторами декогерентности, и должны, вместе с идентичным оператором, образовывать ортонормированный базис в $N^2$- мерном пространстве Лиувилля операторов размера $N \times N$, в котором скалярное произведение определяется по формуле $\langle A|B\rangle = tr(A^+B)$. Здесь через крестик мы, следуя традиции, обозначаем сопряженный оператор, а неотрицательные числа $\gamma_j$ являются интенсивностями действия фактора декогерентности $A_j$.

Это уравнение является обобщением на квантовый случай основного марковского уравнения $\dot{P} = AP$ для распределения вероятностей $P$; если в случайных процессах рассматривается заданная динамика вероятностных распределений, то есть динамика главной диагонали матрицы плотности, то в квантовой физике рассматривается вся матрица плотности, причем исследуются физические причины именно такой динамики.

Численное решение уравнения (99) может быть проведено по методу Эйлера. Дело в том, что основное слагаемое в правой части $[H,\rho]$ соответствует унитарной динамике; эта динамика не увеличивает величину ошибки, поэтому здесь не возникают паталогические случаи ее быстрого роста и, как правило, нет необходимости в применении более точных методов типа Рунге-Кутты. Решение можно представить в виде последовательности шагов, каждый из которых соответствует времени $t_j$, начинается с матрицы плотности $\rho(t_j)$ и состоит из двух действий:

1. Вычисляется унитарная динамика матрицы плотности

$$\tilde{\rho}(t_{j+1}) = \rho(t_j) + \frac{1}{i\hbar}[H,\rho(t_j)]dt.$$

2. Вычисляется действие супероператора Линдблада $\mathcal{L}$ на промежуточную матрицу плотности $\tilde{\rho}(t_{j+1})$:

$$\rho(t_{j+1}) = \tilde{\rho}(t_{j+1}) + \frac{1}{\hbar}\mathcal{L}(\tilde{\rho}(t_{j+1}))dt.$$

Матрица плотности $\rho(t)$ в любой момент времени должна быть положительно определенной, эрмитовой, и иметь единичный след. Последние два условия, при наличии случайных ошибок, можно легко обеспечить переходом от слегка испорченной матрицы $\rho(t)$ к исправленной матрице $(\rho(t) + \rho^{+}(t))/tr(\rho(t))$. Для обеспечения положительной определенности при случайных ошибках можно вычислять один раз, например, за 20 шагов, собственные значения, а затем, при появлении малого отрицательного значения, корректировать эти значения, перераспределяя ошибку на все другие собственные вектора.

# 9 Лекция 9. Сложность квантовой системы и точность ее описания

Сложность квантового состояния системы многих тел имаксимально возможная точность ее описания в терминах векторов состояний связаны таким же соотношением неопределенностей, как координата и импульс. Коэффициент в этом соотношении есть максимальное число кубитов, динамика которых может быть адекватно предсказана квантовой теорией, и этот коэффициент может быть, таким образом, найден экспериментально, в ходе реализации алгоритма GSA. Такое ограничение копенгагенского формализма необходимо именно для сложных систем; оно дает единое описание того, во что в случае сложной системы превращается унитарная динамика, декогерентность и измерения. Это ограничение формализма предполагает наличие минимального ненулевого размера амплитуды квантового состояния, а также отказ от равноправия базисов в гильбертовом пространстве состояний. Квантование амплитуды дает возможность ввести в квантовую динамику некую форму детерминизма, которая может быть важна для сложных систем, для которых невозможен набор статистики и применение стандартных методов квантового предсказания, основанных на расчете вероятностей.

# 10 Вводные замечания

Наше понимание квантовой теории существенно эволюционировало со времени ее возникновения. Если до 80-90 годов 20 века исследовались, как правило, простые, с классической точки зрения, системы: отдельные атомы, молекулы или ансамбли идентичных частиц, которые можно было свести к отдельным независимым объектам, то в последние десятилетия фокус исследований сместился в сторону более сложных систем и процессов. В частности, важность микробиологии и вирусологии стимулировала интерес физиков к изучению объектов, относящихся кк живым организмам, в частности, молекуле ДНК, которая не может быть отнесена к простым системам.

Между тем квантовая теория, лежащая в основе нашего понимания микромира, и, следовательно, в основе понимания сложных процессов, имеет очень жесткий и

точно определенный математический аппарат, основанный на матричной технике. Предсказания квантовой теории всегда совпадали с экспериментом для простых систем, традиционного объекта физики 20 века, но применение ее к сложным системам встречает фундаментальные трудности. В частности, сам процесс нахождения теоретических предсказаний здесь требует невообразимых вычислительных ресурсов, которыми мы никогда не будем обладать.

Если для простых систем процесс вычисления квантового состояния был чисто техническим и не имел отношения к самому процессу, то для сложных систем ситуация иная. Здесь вычисление в широком смысле слова есть важнейший процесс определения самого квантового состояния, и потому должен рассматривать как процесс физический; а устройство, которое выполняет этот процесс есть неотъемлемая часть эксперимента со сложной системой на квантовом уровне.

Это вычисляющее устройство есть абстрактный компьютер, имитирующий эволюцию реальной системы, которую мы изучаем. Все ограничения, имеющиеся для такого компьютера, происходящие из теории алгоритмов, имеют статус физических законов; причем эти законы имеют приоритет перед прочими физическими законами в обычном смысле тогда, когда речь идет о слоных системах.

Эта ситуация не встречалась в классической физике, где процесс получения теоретических предсказаний был не очень сложным. Во всяком случае, сложность этого предсказания всегда находилась в рамках возможностей классических супекомпьютеров, память которых была достаточной для размещения всех элементов реальной системы в удовлетворительном приближении. В квантовой механике сложность растет экспоненциально с ростом частиц в реальной системе, и потому классический путь вычислений становится невозможным, если следовать букве самой квантовой теории. Это было формально доказано с открытием теоретически возможных (с точки зрения копенгагенской теории) процессов, которые невозможно моделировать на классических компьютерах - быстрых квантовых алгоритмов ([18], [12]).

Попытка преодоления барьера сложности с помощью квантоовго компьютера, предложенная Р.Фейнманом в 1982 году ([37]), дала нам более глубокое пониманиие микрокосма и ряд интересных приложений, например, квантовую криптографию и прецизионные приборы. Однако эта попытка не решила главную проблему: масштабирование полнофункционального квантового компьютера до сих пор очень спорно ввиду декогерентности. Декогерентность возникает в результате особого контакта исследуемой системы с ее окружением, что обычно трактуется в рамках концепции открытой квантовой системы, контактирующей с марковским окружением (see [38]), так что влияние среды сводится к неконтролируемым измерениям данной системы со стороны окружения.

Декогерентность является, таким образом, фундаментальным фактором, который енльзя устранить с помощью математических приемов типа коррекции ошибок (коды квантовой коррекции начинают работать только для квантового компьютера с несколькими сотнями кубитов). Для моделирования сложных систем на кванновом уровне декогерентность должна быть включена в сам квантовый формализм, а не привноситься в модель как постороннее влияние. Отклонение эволюции рассматриваемой системы от линейного унитарного закона, вытекающее из декогерентности, должно быть математически выведено из самой эволюции в ее новой форме. Итак,

новый формализм должен налагать ограничение на матричную механику как таковую.

Чем более точно мы хотим знать амплитуды квантового состояния, тем проще это состояние должно быть. Если рассматриваемая система сложна, мы не можем узнать амплитуды ее состояния очень точно; эти аплитуды просто не определены с высокой точностью.

Любое квантовое состояние $|\Psi\rangle$ не является состоянием всего лишь одной системы кубитов. Квантовое состояние есть характеристика огромного числа одинаково приготовленных систем. Состояние $|\Psi\rangle$ фактически является атрибутом некого абстрактного аппарата, который готовит ансамбли именно в этом состоянии. Например, говорить о состоянии $|s\rangle$ электрона в атоме водорода можно только лишь благодаря тому, что у нас в наличии имеется огромное число таких атомов. Если бы атом был единственным, ни о каком квантовом состоянии его не могло бы идти и речи.

Итак, точность кванового состояния есть точность оперделения его амплитуд посредством измерений. Чем больше копий такого состояния мы имеем, тем более точно могут быть определены его амплитуды с помощью последовательного или параллельного измерения этих копий.

Пусть нам дана система $n$ кубитов, относительн которой мы считаем, что она находится в состоянии $|\Psi\rangle$. Мы назовем точностью этого состояния максимально возможное число одинаково приготовленных образцов данной системы. Точность есть, таким образом, максимально возможное число $A$ копий данной системы, которые доступны нам одновременно так, чтобы мы могли их независимо измерять, и, набирая статистику, определить амплитуды этого состояния.

Мы организуем такие образцы $n$ кубитного ансамбля $S_j$, имеющие (предположительно!) одинаковые состояния в виде последовательности $nA$ кубитов вида

$$S_1, S_2, ..., S_A, \quad S_j = (s_1^j, s_2^j, ..., s_n^j),$$

получая, таким образом, память некого абстрактного Главного Компьютера (ГК), посредством которого мы сможем определить, в каком именно состоянии находятся наши образцы. Память ГК не может быть неограниченной, так что существует константа $Q$, такая что

$$An \leq Q. \tag{100}$$

Однако число $n$ кубитов не является точной мерой сложности состояния $|\Psi\rangle$, даже если все эти кубиты в нем запутаны. Для определения настоящей сложности мы должны принять во внимание так называемое каноническое преобразование, которое может радикально снизить число $n$ без изменения состояния $|\Psi\rangle$.

Для верного определения сложности $C$ состояния $|\Psi\rangle$ имеет место следующее соотношение:

$$AC \leq Q. \tag{101}$$

Мы приведем аргументы в пользу такого соотношения точности и сложности в общем случае, а также покажем, что квантование амплитуд позволяет ввести в

квантовую динамику подобие детерминизма, который не сводится к детерминизму классической физики.

# 11 Главный Компьютер

Поведение сложной системы нельзя свести к поведению независимых частиц. Поведение сложных систем можно понять, только опираясь как на квантвоые представления, так и на идеологию вычислений, поскольку здесь традиционная техника математического анализа не работает. Мы должны ввести понятие Главного Компьютера, который адекватно представляет реальный процесс для нас, как абстрактного устройства, законы которого для сложных систем имеют приоритет перед обычными физическими законами; сфера же действия последних ограничена простыми системами и процессами.

Физические прототипы ГК имеют лишь ограниченную мощность, однако они способны адекватно представить процессы, традиционно относимые к химии, так е как и к тем разделам физики, для которых успешно применяются квантвоые методы: прежде всего это электродинамика. Ядерные процессы пока не относятся к этому типу, их сложность радикально превышает сложность электродинамических процессов (см. [40]).

В рамках предложенного ограничения возможностей ГК мы имеем баланс между точностью и сложностью, которые определяются отдельно в каждом конкретном случае.

Для одного кубита мы можем найти амплитуды его состояния с маскимальной точностью. Для простых систем, которые были в фокусе физики 20 века, возможная точность, как правило, совпадала с точностью экспериментов и мы могли определить амплитуды довольно точно. Но для еще более сложных объектов, таких как прототипы квантового компьютера, мы всегда сталкиваемся с барьером, который называют декогерентностью.

Для экстремально сложных систем $A = 1$ и мы имеем единственный экземпляр такой системы, так что мы можем получить только одно базисное состояние. Рисунок 56 представляет все эти случаи.

# 12 Сложность гамильтонианов

Для корректного определения сложности квантового состояния $n$ частиц мы должны рассмотреть каноническое преобразование - главный метод редукции сложности, принятый в физике.

Мы будем представлять классическую координату частицы на единичном отрезке как вещественное число в его бинарной записи $2^{-l}\sum_{j=0}^{l-1} a_j 2^j$ с точностью $2^{-l}$, где $a_j = 0.1$ - значения $l$ кубитов, представляющих эту координату[3] Упорядочивая ку-

[3]Для представления коорддинаты на другом отрезке надо совершить нужное линейное преобра-

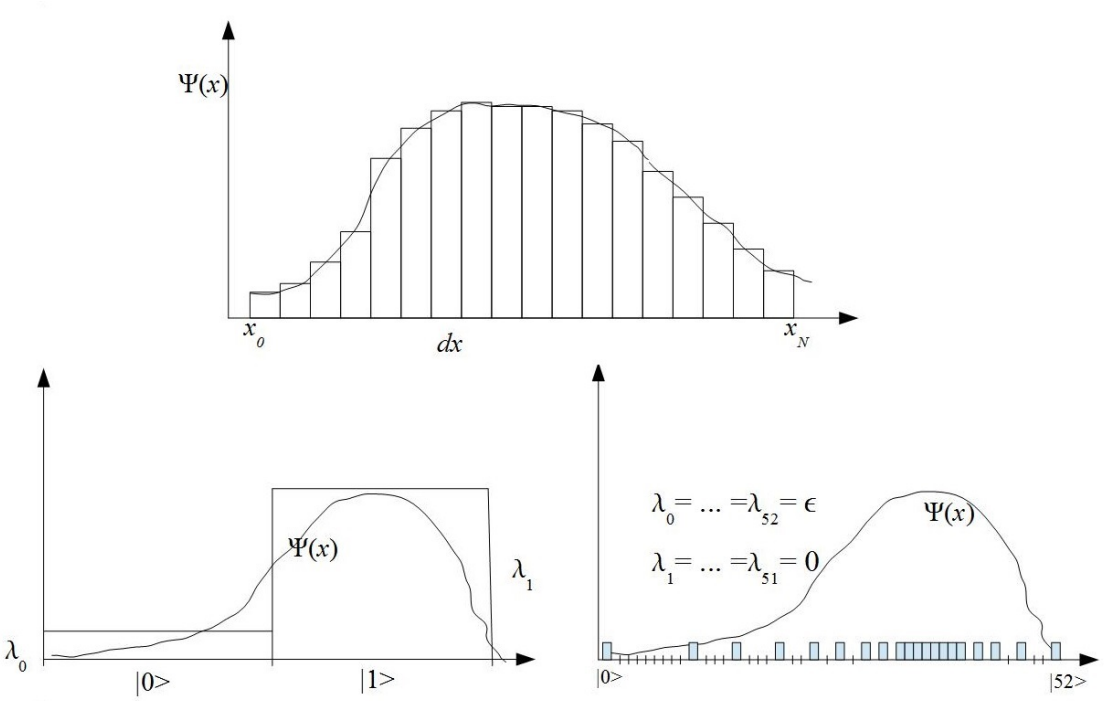



Рис. 56: Представление вектора состояния. Кривые обозначают гипотетическую волновую функцию $|\Psi\rangle$, предсказанную копенгагенской теорией. Прямоугольники обозначают информацию о ней, которую мы можем получить, используя Главный Компьютер. Слева внизу показан случай, когда основная часть вычислительного ресурса занята точностью: $|\Psi\rangle = \lambda_0|0\rangle + \lambda_1\rangle$; если мы ограничим число базисных состояний до 2, как для частицы в двухъямном потенциале, мы получим удовлетворительное сходство с экспериментом. Вверху изображен случай, когда вычислительный ресурс распределен равномерно между точностью и сложностью; это область максимального совпадения с экспериментом - типичная область приложений квантовой механики. Внизу справа основной ресурс занят сложностью: $|\Psi\rangle = \sum_{j=0}^{N-1} \varepsilon|j\rangle$, $\varepsilon \in \{0, \epsilon\}$. Наше знание здесь ограничено только одним базисным состоянием, которое получается в одном единственном измерении. Эта область применения траектории кванта амплитуды (см. ниже).

биты лексикографически, мы получим стандартный порядок базисных векторов, в котором всякий оператор будет иметь определенную матрицу.

Пусть классическое состояние частицы $i$ есть вещественный вектор $x_i$. Тогда классическое состояние системы $n$ частиц будет вектором вида $\bar{x} = (x_1, x_2, ..., x_n)$. Все эти объекты подлежат дискретизации так, как было указано ранее. Пусть $\bar{x}'$ и $\bar{x}$" - два вектора с непустыми множествами координат, такие что их декартово произведение совпадает с $\bar{x}$. Это означает, что мы разбили множество частиц на два непустых подмножества $X'$ и $X$", так что данные векторы являются наборами координат для этих подмножеств. Пусть $H(\bar{x})$ - гамильтониан нашей системы, имеющий вид

$$H(\bar{x}) = H_1(\bar{x}') + H_2(\bar{x}''); \tag{102}$$

где мы, как обычно, принимаем по умолчанию, что $H(\bar{x}')$ есть $H(\bar{x}')\otimes I(\bar{x}")$, то есть на частицах, не включенных в первое подмножество этот член гамильтониана действует как идентичный оператор, и также со вторым членом. В этом случае мы назовем гамильтониан $H$ редуцируемым. Пусть $X'$ -максимальное подмножество компонент вектора $\bar{x}$ (по числу элементов) такое что выполнено равенство (102), и гамильтониан $H_1(\bar{x}')$ не редуцируемый. Тогда $X'$ мы назовем ядром данного гамильтониана.

Примем по умолчанию, что любая эволюция начинается с базисного состояния рассматриваемой системы. Так как (102) влечет равенство $exp(-\frac{i}{\hbar}H) = exp(-\frac{i}{\hbar})H_1 \otimes exp(-\frac{i}{\hbar})H_2$, мы видим, что ядро гамильтониана - это максимальное подмножество частиц, состояние которых в эволюции, индуцируемой данным гамильтонианом $H$ может быть запутанным; мы обозначаем число частиц в нем через $\nu(H)$, и назовем его *наивной* слоностью данного гамильтониана.

Рассмотрим преобразование координат частиц вида

$$q_i = q_i(x_1, x_2, ..., x_n),\ \ i = 1, 2, ..., n; \tag{103}$$

обозначим $\bar{q} = (q_1, q_2, ..., q_n)$ и пусть $H_q = H(x_1(\bar{q}), x_2(\bar{q}), ..., x_n(\bar{q}))$ - первоначальный гамильтониан, но записанный в новых координатах $q_i$, $\bar{x} = \bar{x}(\bar{q})$ которые получаются инвертированием (103). Мы введем новые виртуальные частицы с координатами $q_1, q_2, ..., q_n$,и назовем их квазичастицами.

Классическое состояние системы в первоначальном представлении есть набор определенных значений $x_1, x_2, ..., x_n$. Каждое классическое состояние будет соответствовать другому классическому состоянию той же системы, которое находится с помощью формул (103). Базисный вектор гильбертова пространства переходит, тем самым, в другой базисный вектор того же самого пространства. Стандартное упорядочение базисных векторов, соответствующее кубитовому представлению координат, переходит в другое упорядочение, то есть преобразование классических координат (103) есть перестановка базисных векторов в гильбертовом пространстве квантовых состояний.

При этом преоразовании кубитовое представление значений координат будет иметь

---

зование. Например, если частица находится на отрезке $[-2^{l/2}, 2^{l/2}]$ приближенное кубитовое представление будет иметь вид: $2^{-l/2}\sum\limits_{j=0}^{l-1} a_j 2^j - 2^{l/2-1}$.

уже другой, новый смысл. В новых координатах, координатах квазичастиц, гамильтониан примет новый вид $H_q$. Мы назовем преобразование координат (103) каноническим, если $\nu(H_q)$ минимальное из всех возможных для всех таких перобразований. Тогда переход к квазичастицам будет означать редукцию сложности первоначального гамильтониана. Итак, каноническое преобразование есть перестановка базисных векторов, минимизирующая наивную сложность гамильтониана.

Переход к описанию эволюции в виде квазичастиц имеет вид $H = \tau^{-1} H_q \tau$ где перестановка базисных векторов $e\tau$ есть переход к квазичастицам при каноническом преобразовании. Тогда представление оператора эволюции имеет вид $exp(-\frac{i}{\hbar}Ht) = \tau^{-1} exp(-\frac{i}{\hbar}H_q t)\tau$ и требует меньших вычислительных ресурсов, чем прямое вычисление $exp(-\frac{i}{\hbar}Ht)$, так как главный ресурс тратится на ядро, которое для квазичастичного представления имеет наименьший размер.

## 12.1 Пример: система взаимодействующих гармониических осциллятоов

Мы рассмотрим понятие квазичастицы на модельной задаче о системе взаимодействующих гармонических осцилляторов. Эта задача выбрана ввиду ее особой важности для физических приложений. Для одного осциллятора гамильстониан имеет вид $H = \frac{p^2}{2m} + m\omega^2 q^2/2$; его собственные функции имеют вид

$$\Psi_n(x) = \frac{1}{\sqrt{2^n n!}} \left(\frac{m\omega}{\pi h}\right)^{1/4} exp(-m\omega x^2/2h) H_n(x\sqrt{m\omega/h}) \tag{104}$$

где полиномы Эрмита $H_n = (-1)^n e^{x^2} \frac{d^n}{dx^n} e^{-x^2}$, а соответствующие собственные значения энергии $E_n = h\omega(n + 1/2)$.

Рассмотрим систему $N$ гармонических осцилляторов, взаимодействующих друг с другом по закону Гука. Такой системой может быть, например, цепочка положительных металлических ионов в ловушке Пауля. Кулоновское взаимодействие между ними, если рассматривать малые колебания около положения равновесия, дает квадратичные потенциалы, то есть приближенно можно считать, что сила между ионами подчиняется закону Гука.

Пусть $u_n$ обозначает отклонение осциллятора $n$ от его положения равновесия. Гамильтониан такой системы имеет вид

$$H = \sum_{n=1} N(\frac{p_n^2}{2m} + \kappa u_n^2) - \kappa \sum_{n=1}^{N} u_n u_{n+1}$$

который получен из вычитания сил Гука $-\kappa(u_n - u_{n+1})$ по всем $n$, с приведением подобных членов (так получается $u_n u_{n+1}$) и пренебрежением граничными эффектами.

Борьба с запутанностью есть борьба с взаимодействием. Суть канонического преобразования в том, чтобы избавиться от члена взаимодействия $u_n u_{n+1}$. Этого члена не должно быть для квазичастиц - эти новые "частицы" должны быть не зависимы друг от друга. Оказывается, что для этой цели подходит преобразование Фурье, но не над волновой функцией, как это было при переходе от координатного к импульсному базису в гильбертовом пространстве состояний, а над самими амплитудами $u_n$ колебаний осцилляторов.

Роль координаты $r$ здесь будет играть $n$- номер осциллятора, а роль пси-функции будет играть $u_n$. Значения настоящей пси-функции еще называют амплитудами, поэтому здесь есть полное согласие с лингвистикой. Однако тот факт, что "координата" $n$ и "амплитуда" $u_n$ есть $r$ и $\Psi(r)$ не есть просто забавная аналогия. Он говорит о природе квантовой амплитуды и о ее глубокой связи с роевым представлением реальных частиц. Механические колебательные амплитуды $u_n$ не могут быть комплексными, подобно квантовым амплитудам. И классическое уравнение колебаний, описывающее динамику осцилляторов, также не может быть прообразом уравнения Шредингера, из-за своего детерминизма, что мы уже видели.

Поэтому осцилляторы не годятся как основа для полной модели квантовой динамики в общем случае. Однако, они подходят как модель электромагнитного поля, взаимодействие с которым и дает полную картину динамики частиц, которая оказывается динамикой "частиц + поля". Поле оказывается прибежищем детерминизма. Квантовый же хаос связан именно с тем, что амплитуды там будут комплексными; это связано с хаотической природой самих частиц, и это невозможно преодолеть так же, как в случае детерминистического мира осцилляторов. Это означает, что нам предстоит квантовать поле, то есть систему осцилляторов, что будет, фактически, распространением на поле того внутреннего стохастического поведения, которое первоначально было свойственно частицам материи.

Итак, каноническое преобразование в нашем случае выглядит так:

$$u_n = \frac{1}{\sqrt{N}} \sum_q U_q e^{-iqnd}, \tag{105}$$

а обратное к нему:

$$U_q = \frac{1}{\sqrt{N}} \sum_n u_n e^{iqnd}, \tag{106}$$

где $d = 2\pi/N$. Используя определение импульса $p_n = \frac{h}{i}\frac{\partial}{\partial u_n}$ и правила дифференцирования, можно вывести формулы преобразований импульсов вида

$$p_n = \frac{1}{\sqrt{N}} \sum_q P_q e^{iqnd}, \tag{107}$$

и обратное к нему:

$$P_q = \frac{1}{\sqrt{N}} \sum_n p_n e^{-iqnd}, \tag{108}$$

где $P_n = \frac{h}{i}\frac{\partial}{\partial U_n}$. То что мы допустили здесь комплексные амплитуды, не существенно, потому что мы сейчас вернемся к вещественным числам, чего нельзя было бы сделать, будь у нас пси-функция вместо $u_n$.

Каноническое преобразование - линейно, и переводит любой малый кубик деления конфигурационного пространства в столь же малый параллелепипед, так что вместо одного деления возникнет другое. Более того, наше преобразование вида (105)

будет даже ортогональным, то есть, как мы увидим ниже, кубики перейдут в кубики. Поэтому мы всегда можем представить его как перестановку базисных векторов гильбертова пространства.

Сдвинем также начало координат для $q$ так, чтобы этот параметр, заменяющий $n$, принимал значения из симметричного промежутка. Тогда вместо $q+q'=N$ мы будем писать $q+q'=0$. Отношение неравенства индуцируется из старого набора $1,2,\ldots,N$ так что пар $q>-q$ практически половина (краевым эффектом всюду пренебрегаем)

Переписав гамильтониан в новых координатах, мы имеем:

$$\begin{aligned}
H = & \sum_{n=1}^{N} \frac{1}{2mN}(\sum_{q,q'} P_q P_{q'} e^{1(q+q')nd}) + \frac{K}{N}\sum_q U_q U_{q'} \\
& -\frac{K}{N}\sum_{q,q'}(U_q U_{q'} e^{-iqnd} e^{-iq'(n+1)d}) = \\
& = \frac{1}{2mN}\sum_q P_q P_{-q} - \frac{K}{N}\sum_{q,q'} U_q U_{q'}(\sum_{n=1}^{N} e^{-ind(q+q')}) e^{-iq'd} + \frac{K}{N}\sum_q U_q U_{q'} = \\
& = \frac{1}{2mN}\sum_q P_q P_{-q} - \frac{K}{N}\sum_q U_q U_{-q} e^{+iqd} + \frac{K}{N}\sum_q U_q U_{-q} = \\
& = \frac{1}{2mN}\sum_q P_q P_{-q} + \frac{2K}{N}\sum_{q>-q} U_q U_{-q}(1-cos(qd)).
\end{aligned}$$

Здесь $K=m\omega^2/2$, использовалась стандартная формула для суммирования геометрической прогрессии из экспонент, дающая 0 в случае $q\neq q'$, а также произведено упорядочение пар $q,-q$, так что мы явно выписали только половину, в которых $q>q'$- отсюда коэффициент 2 в последнем слагаемом.

Теперь перейдем еще раз к новым переменным, на этот раз - вещественным:

$$\begin{aligned}
& U_q = X_q + iY_q,\ X_q = \tfrac{U_q+U_{-q}}{2},\ Y_q = \tfrac{U_q-U_{-q}}{2i}; \\
& X_q = \tfrac{1}{\sqrt{N}}\sum_n u_n cos(qnd),\ Y_q = \tfrac{1}{\sqrt{N}}\sum_n u_n sin(qnd), \\
& \tfrac{\partial}{\partial U_q} = \tfrac{\partial}{\partial X_q}\tfrac{1}{2} + \tfrac{\partial}{\partial Y_q}\tfrac{1}{2i}, \\
& \tfrac{\partial}{\partial U_{-q}} = \tfrac{\partial}{\partial X_q}\tfrac{1}{2} - \tfrac{\partial}{\partial Y_q}\tfrac{1}{2i}, \\
& \tfrac{\partial^2}{\partial U_q \partial U_{-q}} = \tfrac{1}{4}\left(\tfrac{\partial^2}{\partial X_q^2} + \tfrac{\partial^2}{\partial Y_q^2}\right).
\end{aligned}$$

Окончательно получаем

$$H = -\frac{1}{4mN}\sum_{q>q'}\left(\frac{\partial^2}{\partial X_q^2} + \frac{\partial^2}{\partial Y_q^2}\right) + \frac{2K}{N}\sum_{q>-q}(X_q^2+Y_q^2)(1-cos(qd)).$$

Мы видим, что в новых координатах наша система представляет собой набор независимых гармонических осцилляторов массы $\tilde{m}=2m$, с новым коэффициентом $\tilde{K}=2K(1-cos(qd))$ и частотами

$$\tilde{\omega}_q = \sqrt{\frac{2K}{m}(1-cos(qd)}} \tag{109}$$

Графическое представление квантового состояния в терминах квазичастиц показано на рисунке 57.

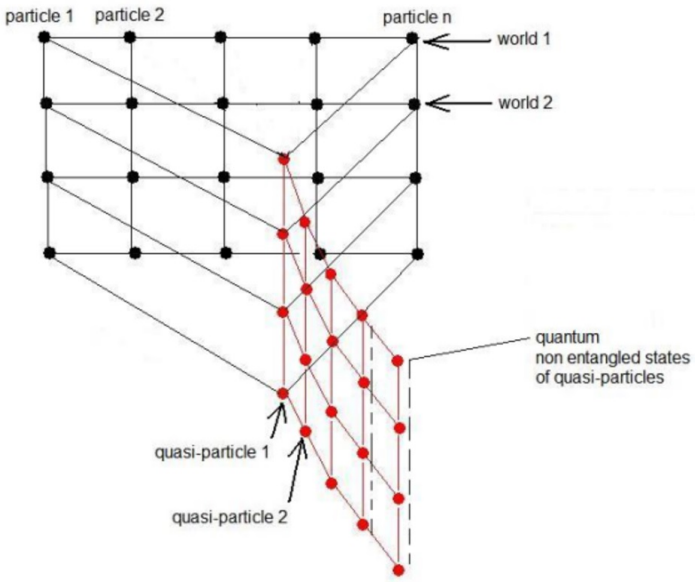



Рис. 57: Квантовое представление квазичастиц

## 12.2 Более простые примеры

Рассмотрим гамильтониан $H$ замкнутой цепочки четырех взаимодействующих кубитов, который редуцируется каноническим преобразованием $CNOT$ до полностью редуцированного гамильтониана $H_q = \sigma_x^{(1)} \otimes I_2 + I_1 \sigma_x^{(2)}$:

$$H = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix} = CNOT \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} CNOT.$$

Заметим, что перестановка базисных векторов, являющаяся каноническим преобразованием, должна быть запутывающим, и, одновременно, распутывающим преобразованием, так как она редуцирует ядро гамильтонииана. Например, оператор $CNOT$, примененный последовательно к состоянию $|00...0\rangle + |11...1\rangle$ полностью его распутывает.

Противоположный пример дает гамильтониан Тависа-Каммингса для $n$ бвухуровневых атомов, взаимодействующих с резонансной модой в оптической полости. Здесь имеется базисное состояние поля и атомов вида $|n\rangle_{ph}|00...0\rangle_{at}$, так что столбец матрицы гамильтониана, соответствующий этому состоянию, состоит из чисел $g\sqrt{n}$ и одного числа $n\hbar\omega$, причем такой столбец единственный. НИкакой гамильтониан вида (102) не можут иметь этого вида даже для $n = 2$, поэтому неидентичного канонического преобразования для гамильтониана Тависа-Каммингса не существует.

**Сложность гамильтониана $H$, обозначаемая через $C(H)$, есть минимальная наивная сложность оператора $\tau^{-1}H\tau$ по всем перестановкам $\tau$ базисных векторов.**

В примерах с системой гармонических осцилляторов и четырехмерным гамильтонианом, приведенных выше, сложность гамильтонианов будет равна 1, то есть они могут быть полностью редуцированы каноническим преобразованием.

## 12.3 Сложность квантового состояния

Сложность квантового состояния $|\Psi\rangle$ определяется аналогичным образом. Его *наивная* сложность, обозначаемая через $\nu(|\Psi\rangle)$, определяется как число частиц в максимальном тензорном делителе $|\Psi_1\rangle$ состояния $|\Psi\rangle = |\Psi_1\rangle \otimes |\Psi_2\rangle$.

Сложность $C(|\Psi\rangle)$ состояния $|\Psi\rangle$ есть минимальная наивная сложность состояний вида $\tau|\Psi\rangle$ по всем перестановкам $\tau$ базисных векторов.

Например, сложность обобщенного GHZ состояния $|GHZ\rangle = \frac{1}{\sqrt{2}}(|00...0\rangle + |11...1\rangle)$ равна единице, так как его можно полностью распутать последовательностью операторов CNOT. Если мы стартуем с базисного состояния $|\Psi(0)\rangle$ в каноническом представлении гамильтониана $H$, то его эволюция, индуцированная этим гамильтонианом, не может содержать состояний сложности, большей чем $C(H)$.

Теперь мы сформулируем гипотезу о соотношении между точностью и слоностью в окончательном виде:

$$C(|\Psi\rangle)A(|\Psi\rangle) \leq Q, \tag{110}$$

где $Q$ есть максимальное число полностью запутанных кубитов, которые нельзя распутать какой-либо перестановкой базисных векторов.

Рассмотрим, для примера, состояние $n$ кубитов вида

$$|\Psi_{GSA}(t)\rangle = \alpha \sum_{j \neq j_0, 0 \leq j < N} |j\rangle + \beta|j\rangle, \tag{111}$$

где $\alpha = cos(t)/\sqrt{N-1}$, $\beta = sin(t)$ для некоторого $t$, и $N = 2^n$. Сложность этого состояния равна $n$, если только $t \neq k\pi/2$ для любого целого $k$. В самом деле, данная суперпозиция имеет то свойство, что все ее базисные компоненты, за исключением ровно одного, имеют одинаковую ненулевую амплитуду, а эта одна компонента имеет другую амплитуду.

Это свойство сохраняется при любой перестановке базисных векторов, то есть при любом квазичастичном представлении. Но если бы это состояние было редуцируемым, оно имело бы вид $\lambda_1|i_1\rangle + \lambda_2|j_2\rangle + ...) \otimes (\lambda_3|j_3\rangle + \lambda_4|j_4\rangle + ...)$ для некоторых базисных $|j_i\rangle$, а такая суперпозиция не может содержать ровно 2 значения амплитуд для всех базисных состояний, потому что здесь должно быть либо как минимум 3 разные ненулевые значения амплитуд, или она должна содержать ровно две разные ненулевые амплитуды, соответствующие двум группам базисных векторов, содержащим равное число элементов. Обе эти возможности исключены для состояний вида (111).

# 13 Зернистость амплитуды

Здесь мы покажем, как можно распространить квантовый формализм за границу $Q$. Это приведет нас к понятию квантового детерминизма, не сводящегося к известным квазиклассическим эффектам.

Кубитовое представление классических координат и импульсов должно быть дополнено зерном разрешения для амплитуды. Для любого разложения квантового

состояния $|\Psi\rangle$ по происзвольному ортонормированному базису $|\psi_j\rangle$ вида

$$|\Psi\rangle = \sum_{j\in J} \lambda_j |\psi_j\rangle,\ \lambda_j \neq 0, \tag{112}$$

модули амплитуд $\lambda_j$ должны быть ограничены снизу некоторой ненулевой константой.

Для сохранения линейности в области, где ненулевой размер амплитуд не играет роли, мы должны принять, что любая амплитуды имеет вид

$$\lambda_j = \epsilon n_j + i\epsilon m_j \tag{113}$$

где $n_j, m_j \in Z$ - целые, $\epsilon > 0$ - константа, называемая квантом амплитуды. Такое ограничение матричного формализма влечет отказ от абсолютной эквивалентности всех базисов в пространстве квантвоых состояний, которое проявляет себя именно в очень малых амплитудых и огромных размерах базисов состояний $J$.

Однако для моделирования на компьютере эквивалентность базисов не всегда важна; эта эквивалентность есть лишь алгебраический факт, который невозможно проверить на сложных системах.

Итак, наименьший размер моуля амплитуды составляет $\epsilon$. Это ограниччение очень хорошо согласуется с вероятностной природой вектора состояния, так как для определения значений $|\lambda_j|^2$ с точностью $\delta$, необходяимо сделать около $1/\delta$ измерений одинаково приготовленный образцов первоначальной системы; для состояний сложных систем с малыми амплитудами $\lambda_j$, это возможно только если минимальная вероятность $\epsilon^2$ отделена от нуля так, что мы сможем найти вероятность даже самого маловероятного события.

Мы можем определить значение $\epsilon$, "размазывая" амплитуду по настолько большому числу базисных состояний, насколоко это возможно, так что присутствие в разложении любой ненулевой амплитуды можно обнаружить в эксперименте. Если все амплитуды равны $\lambda_j = \epsilon$, мы получаем для максимального общего числа базисных компонент в суперпозиции выражение $|J| = 1/\epsilon^2$ - это есть максимальна размерность $2^Q$ гильбертова пространства квантовых состояний, при которой можно применять квантовый формализм. В разложении (112) амлпитуды $\lambda_j$ не имеют физической размерности, размерностью обладают базисные состояния $|\psi_j\rangle$. Максимальное число кубитов, для которых квантвоые состояния реализуемы, равняется $Q$, так что $\epsilon = 2^{-Q/2}$.

Дискретизация амлпитуды в виде (113) позволяет включить измерения в саму унитарную эволюцию. Жесткий контакт системы в состоянии $|\Psi\rangle = \sum\limits_{j\in J} \lambda_j |j\rangle$ с измерителем означает включение состояний измерителя в рассматриваемую систему, то есть происходит переход к состоянию объединенной системы вида $|\Psi_{ex}\rangle = \sum\limits_{j\in J, \nu_j \in \mathcal{N}_j} \mu_{j,\nu_j} |j, \nu_j\rangle$, где в условиях применимости квантовой механики модули всех $\mu_{j,\nu_j}$ должны быть минимальны, что означает что они равны $\epsilon$. Так как контакт с измерителем должен быть унитарной эволюцией, мы имеем $|\lambda_j|^2 = \sum\limits_{\nu_j \in \mathcal{N}_j} |\mu_{j,\nu_j}|^2$ то есть измерение будет случайным выбором одного из состояний $\nu_j$ измерителя, то есть мы получаем стандартную урновую схему теории вероятностей.

## 13.1 Экспериментальное нахожение константы $Q$

Мы можем найти приблизительную оценку константы $Q$, строя состояния вида (111). Это - состояния квантового компьютера, реализующего алгоритм Гровера GSA для единственного целевого состояния $|j_0\rangle$ (see [12]). Пусть $N = 2^n$. Мы положим $t_0 = arcsin(1/\sqrt{N})$. Начнем с состояния

$$|\Psi(0)\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} |j\rangle = (\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)^{\otimes n},$$

сложность которого равна единице. После выполнения первого шага алгоритма $t$ становится равным $t_0$, и мы получаем состояние сложности $n$ вида (111). Уже на первом шаге сложность прыжком от единицы достигает максимального значения. Если $N = 2^Q$, мы выходим за пределы допустимых состояний в амплитудами вида (117), имеющих свойство (110).

Таким образом, мы можем оценить константу $Q$, увеличивая число кубитов $n$, для которого алгортм GSA работает корректно. Здесь под корректной работой подразумевается возможность повышения амплитуды целевого состояния до уровня, скажем, $1/\sqrt{2}$ по сравнению с остальными, которые будут иметь амплитуду порядка $1/\sqrt{N}$. для более грубой оценки мы можем фиксировать подскок амплитуды на $1/\sqrt{N}$ по сравнению с остальными, но это имеет смысл только для малых $n$, не превосходящих 20.

Рисунок 58 Иллюстрирует границу работы алгоритма Гровера в терминах кванта амплитуды.

Вопрос в том, что произойдет с текущим состоянием, если амплитуды, вычисленные по стандартной квантовой теории, становятся по абсолютной величине меньше $\epsilon$, формально открыт. Однако естественно предположить, что малые амплитуды просто исчезают с соответствующим перенормировкой вектора состояния. Это означает, что применение GSA в окрестности $N \approx 2^Q$ we will get the target state very quickly, much faster than when implementing GSA in a normal model. However, this will only happen with an ideal implementation of GSA; in practice, the amplitudes of the main mass of states in $|\Psi_{GSA}(t)\rangle$ in (111) cannot be exactly the same, so that zeroing will not occur simultaneously for all states, which can greatly distort the picture.

Для экспериментального обнаружения такого эффекта надо настолько точно настроить гейты, чтобы достичь максимально возможной размерности ядра квантового $Q$. Ниже мы обсудим оценки на эту константу.

Рассмотрим два процесса: переход состояний электрона в атоме $Rb^{85}$ и распад нестабильного ядра $He^6$. Первый процесс описывается квантовой электродинамикой довольно точно, полное квантовое описание второго пока отсутствует.

Мы будем исходить из критерия точной прорисовки волновой функции, когда каждый шаг его компьютерного описания требует одного нового базисного состояния. Это вытекает из скорости квантового блуждания, при котором фронт волны распространяется с линейной скоростью (в отличие от классического блуждания, при котором скорость пропорциональна квадратному корню из времени). Пусть $t$ - общее время процесса, $dt$ - шаг компьютерного описания этого процесса во времени, тогда

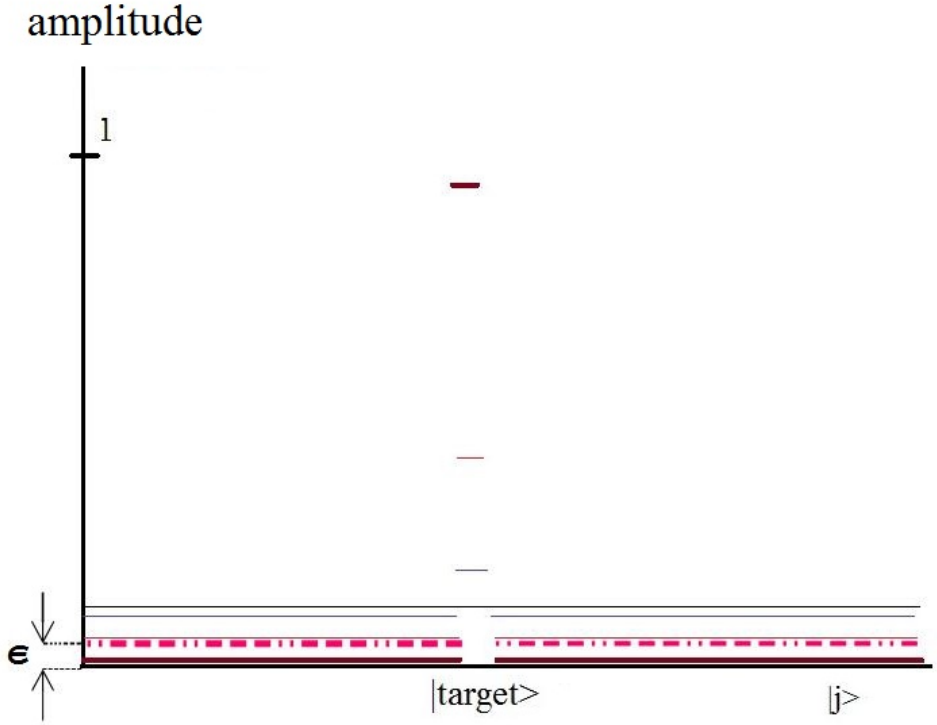



Рис. 58: Граница работы GSA в терминах кванта амплитуды

число базисных состояний, необходимых для "точной прорисовки" процесса составит $N = t/dt$. Значения $t$ определяется экспериментально, а $dt$ находится из соотношения неопределенностей "энергия - время".

Для рабиевской осцилляции атома рубидия, происходящей с испусканием фотона с длиной волны примерно 1.4 $cm$ мы имеем:

$$\omega \approx 10^{10}\ sek^{-1},\ E_{QED} = \hbar\omega \approx 10^{-17},\ dt \approx \hbar/E_{QED} = 10^{-10}.$$

Учитывая время рабиевской осцилляции $t \approx 10^{-6}\ sec$, мы получаем $N = t/dt \approx 10^4$. Тогда $Q \geq 10^4 < 2^{14}$ и для хорошего отображения данного процесса на основании квантовой теории достаточно работы GSA на 14 кубитах, что представляется реальным.

Теперь рассмотрим распад ядра изотопа гелия:

$$He^6 \rightarrow He^5 + n \rightarrow He^4 + 2n$$

(в данном грубом приближении учитываем только нуклоны). Характерное значение энергии будет около 10 $Mev \approx 10^{-5}\ erg$, и соотношение неопределенности "энергия-время" даст $dt \approx 10^{-22}\ sec$. Весь процесс занимает около 1.6 $sec$, откуда $N = t/dt \approx 10^{22} \approx 2^{73}$, и если квантовую механику можно продолжить до ядерных процессов типа распада изотопа гелия - 6 до стабильного изотопа 4, GSA должен хорошо работать уже на 73 кубитах.

Распад изотопа гелия 6 с точки зрения квантовой механики - весьма сложный процесс. Можно рассмотреть только его последнюю стадию, когда от стабильного

ядра гелия 4 отщепляется один нейтрон (см. [41]). Она занимает примерно $10^{-11}$ *sec.* Для нее оценки, аналогичные вышеприведенным, дадут примерно 36 кубитов надежной реализации GSA, что уже менее реалистично, однако соответствующее значение $Q \approx 2^{36}$ можно уже верифицировать на экспериментах по GSA. Таким образом, принятие гипотезы о зерне амплитуды напрямую связывает вопрос о применимости квантовой теории к реальным микропроцессам и реализацию GSA. Реализация GSA становится, таким образом, центральным вопросом квантовой теории и теории сложных систем как таковых.

## 13.2 Зерно амплитуды как причина измерений

Измерение квантового состояния $|\Psi\rangle = \sum\limits_{j\in J} \lambda_j |j\rangle$ есть случайная величина, принимающая знаяения $|j\rangle$, $j \in J$ с вероятностями $|\lambda_j|^2$. Физически оно начинается с контакта исходной системы с измерителем, то есть унитарного преобразования вида

$$|\Psi\rangle|\bar{0}\rangle_{meas} \to \sum_{j\in J} \lambda_j |j\rangle \sum_{i_j \in I_j} \mu_{i_j} |i_j\rangle_{meas}. \tag{114}$$

Если число элементов в каждом множестве состояний измерителя $I_j$ очень велико, так что амплитуды всех конкретных состояний измерителя становятся примерно равными зерну $\epsilon$: $\sum\limits_{i_j \in I_j} \mu_{i_j} \approx \epsilon$, то в силу унитарности перехода (114) числа элементов множеств $I_j$ становятся с большой точностью пропорциональными вероятностям $|\lambda_j|^2$ получения результата $|j\rangle$ в измерении. Поэтому измерение означает выбор наугад из урновой схемы, дающий вероятности исхода в соответствии с правилом Борна.

Итак, наличие зерна устраняет странный барьер между унитарной динамикой и коллапсом волнового вектора, который является помехой для моделирования динамики, так как использование квантового основного уравнения требует квадратичного роста ресурсов памяти при компьютерном моделировании по сравнению с унитарной динамикой, так как приходится хранить в памяти матрицу плотности вместо вектора состояния.

В предельном случае, при полном коллапсе на каждом шаге эволюции, мы получим полностью детерминистическое описание динамики в том случае, если есть некоторое превосходство амплитуды одного единственного состояния $|j_{tar}\rangle$ над всеми другими, как в алгоритме Гровера. Базисные состояния $|j\rangle$, при этом, вообще говоря, должны быть нелокальными в силу фундаментальной квантовой нелокальности; ее мы уже обсуждали выше. Такая форма описания диинамики совершенно необычна, но именно она, вероятнее всего, окажется адекватной реальным сложным системам, которые являются предметом проекта квантового компьютера.

# 14 Равновесные состояния

Теперь мы рассмотрим, как можно было бы работать с системой, имеющей состояния экстремальной сложности $Q$, стартуя с описания состояний в квантовом формализме. Здесь речь пойдет о детерминистическом описании динамики для одной,

отдельно взятой, порции амплитуды. Такая порция остается от всей воображаемой амплитуды, если в нашем распоряжении есть лишь одно измерение системы, приготовленной в данном состоянии.

Мы опишем наиболее широкий класс состояний, для которых можно ввести квантование ампитуды.

Для комплексного числа $z = a+ib,\ a,b \in R$, мы введем обозначение $\{z\} = |a|+|b|$. Для квантового состояния $|\psi\rangle$ мы определим $\{\psi\} = \sum_{i=0}^{N-1} \{\langle i|\psi\rangle\}$.

Пусть $A$ линейный оператор и $|j\rangle$некоторый базисный вектор, $j \in \{0,1,...,N-1\}$. Лпределим $|a_j\rangle = A|j\rangle$. Мы назовем вектор состояния $|\Psi\rangle$ равновесным относительно оператора $A$, если все числа $\{a_j\}$ одинаковы для всех базисных компонент $|j\rangle$ которые в наш вектор входят с ненулевыми амплитудами. Заметим, что определение зависит от выбора базиса в пространстве.

В качестве примера рассмотрим гамильтониан одномерной частицы, движущейся в потенциале $V$ в координатном базисе: $H = \frac{p^2}{2m} + V$. Мы урежем матрицу этого гамильтониана, приняв, что нет слишком длинных переходов в пространстве данной частицы. Тогда равновесные состояния в координатном базиседля данного гамильтониана будут в точности состояния $|\Psi\rangle$, все компоненты которых имеют одинаковый потенциал.

Важным классом многочастичных равновесных состояний являются связные состояния. Вот пример такого состояния. Рассмотрим $k$ двухуровневых атомов в оптической ловушке, удерживающей фотоны моды атомного перехода. Выберем базис из состоний вида $|n\rangle_{ph}|m_1,m_2,...,m_k\rangle_{at}$, где $n$ - число фотонов в полости, $m_j \in \{0,1\rangle$ состояние атома $j$, основное и возбужденное. Пусть $g_j,\ j = 1,2,...,k$ - силы взаимодействия атомов с полем. Тогда динамика системы атомов и поля при условии $g_j/\hbar\omega \ll 1$, где $\omega$ - частота моды полости, будет подчиняться уравнению Шредингера с гамильтонианом Тависа-Каммингса в RWA приближении:

$$H_{TC}^{RWA} = \hbar\omega(a^+a + \sum_{j=1}^{k} \sigma_j^+\sigma_j) + a^+\bar{\sigma} + a\bar{\sigma}^+,\quad \bar{\sigma} = \sum_{j=1}^{k} g_j\sigma_j, \tag{115}$$

где $a, a^+$ - стандартные полевые операторы и $\sigma_j, \sigma_j^+$ - атомные операторы атома $j$. Связанное состояние такой системы будет существовать только при $k = 2$ и $g_1 = g_2$, и это будет либо одно из базисных состояний, либо состояния $|n\rangle_{ph}(\alpha|10\rangle_{at}+\beta|01\rangle_{at})$, из которых во всех за исключением единственного, синглетного состояния при $\beta = -\alpha$ атомы будут взаимодейтвовать с полем. Все такие состояния равновесные.

Заметим, что если мы сделаем полость достаточно длинной, так что зеркала будут расположены далеко от атомов, мы получим примерное равенство $g_1 \approx g_2$, так что любое состояние станет равновесным. Удаление зеркал означает приближение нашей системы к естественному состоянию атомов в вакууме; фотоны, испущенные ими, будут улетать из системы, но темные состояния сохранятся: они вообще не нуждаются в зеркалах.

Общее определение связности выглядит так.

Пусть $H$ гамильтониан в пространстве состояний $n$ кубитов. Если кубит ассоци-

ирован с реальной или виртуальной двухуровневой частицей, $H$ может быть, например, гамильтонианом Тависа-Каммингса или некоторой его модификацией. Пусть $S_n$ - группа перестановок кубитов, которые естественно продолжены до операторов во всем пространстве состояний $\mathcal{H}$, а именно, на всех базисных состояниях $\eta \in S_n$ действует непосредственно, и $\eta \sum\limits_j |j\rangle = \sum\limits_j \eta|j\rangle$.

Обозначим через $G_H$ подгруппу группы перестановок $S_n$, состоящую из всех перестановок кубитов $\tau$ таких что $[H, \tau] = 0$. Пусть $A \subseteq \{0, 1, ..., 2^n - 1\}$ есть подмножество базисных состояний системы $n$кубит. Его линейная оболочка $L(A)$ называется связным подпространство относительно $H$ если для любых двух состояний $|i\rangle,\ |j\rangle \in A$ существует перестановка кубитов $\tau \in G_H$ такая что $\tau(i) = j$. Состояние $|\Psi\rangle$ системы $n$ кубитов называется связным относительно $H$ если оно принадлежит связному относительно $H$ подпространству, и $H|\Psi\rangle \neq 0$.

Связность состояния означает, что все его ненулевые компоненты получаются одна из другой перестановкой таких частиц, поведение которых относительно данного гамильтониана одинаково.

Приведенное выше состояние $|n\rangle_{ph}(\alpha|10\rangle_{at} + \beta|01\rangle_{at})$ будет связным, так как перестановка атомов, одинаково взаимодейтвующих с полем, не меняет гамильтониан. Состояния вида $|n\rangle_{ph}(\alpha|10\rangle_{at} + \beta|01\rangle_{at} + c|00\rangle_{at} + d|11\rangle_{at})$, с ненулевыми амплитудами $a, b, c, d$ не будет связным.

*Лемма*

*Если состояние* $|\Psi\rangle = \sum\limits_j \lambda_j|j\rangle$ *связно относительно* $H$, *то любые два столбца матрицы* $H$ *с номерами* $j_1,\ j_2$, *такие что* $\lambda_{j_1}$ *и* $\lambda_{j_2}$ *ненулевые, отличаются друг от друга только перестановкой элементов. Это же верно и для матрицы унитарной эволюции* $U_t = exp(-\frac{i}{\hbar}Ht)$.

Действительно, для таких базисных состояний $j_1$ и $j_2$, в соответствии с определением связности, существует перестановка $\tau \in G_H$ такая что $j_2 = \tau(j_1)$. Столбцы с номерами $j_1,\ j_2$ состоят из амплитуды состояний $H|j_1\rangle$ и $H|j_2\rangle$, соответственно. Из коммутационного условия мы имеем $\tau H|j_1\rangle = H\tau|j_1\rangle = H|j_2\rangle$, и это означает, что столбец $j_2$ получается из столбца $j_1$ перестановкой элементов, индицированной $\tau$. Переходя к матрице эволюции $U_t$, мы видим, что условие $\tau U_t|j_1\rangle = U_t\tau|j_1\rangle = U_t|j_2\rangle$ будет выполнено и для нее, что и требовалось. Лемма доказана.

Из Леммы следует, что связные относительно $H$ состояния являются равновесными относительно $H$ и относительно оператора эволюции $U_t = e^{-\frac{i}{\hbar}Ht}$, соответствующей этому гамильтониану.

# 15 Кванты амплитуды и детерминизм

Точное описание динамики как в квантовом, так и в классическом случае, имеет некоторую степень недетерминизма или стохастичности (см. [42],[43]). Преимущество квантового языка - в точном ограничении этой стохастичности вектором состояния,

который, согласно главному тезису копенгагенской механики, дает исчерпывающее описание динамики микрочастиц.

Возможность введения детерминизма в квантовую теорию, интересовавшая исследователей с самого ее появления, не потеряла актуальности (см. [44]) и снова находится в фокусе интереса для сложных систем. Например, для систем экстремальной сложности, молекула ДНК определяет будущее ее обладателя с точностью, недостижимой для физических экспериментов. Этот высший тип детерминизма должен иметь некоторый аналог и для простых систем, хорошо описываемых стандартной квантовой теорией.

Мы опишем специфическую форму детерминизма на уровне квантов амплитуды.

Наша цель - показать, что если состояние $|\Psi\rangle$равновесное относительно оператора эколюции $U_t$, то амплитуды всех базисных состояний в нем можно разбить на малые порции - кванты амплитуды, так что траектория каждого кванта при эволюции будет точно определена, если оператор $U_t$ действует в течение фиксированного интервала времени $t$, в частности, будет точно определено, с какими квантами амплитуд он будет контактивать (сокращаться) при суммировании амплитуд при определении результирующего состояния.

Фактически, это будет иметь место для произвольного линейного оператора $A$, для которого мы определим квантование амплитуд.

Пусть $|\Psi\rangle$ произвольное равновесное состояние относительно $A$, разложение которого по базисным имеет вид

$$|\Psi\rangle = \sum_j \lambda_j |j\rangle. \tag{116}$$

Мы введем важное понятие кванта ампитуды как формализацию перехода малой порции амплитуды между двумя различными базисными состояниями при умножении вектора состояния на матрицу $A$. Пусть $T = \{+1, -1, +i, -i\}$ - множество из 4 элементов, которые мы назовем типами амплитуды: вещественный положительной, вещественный отрицательный, и так же мнимые. Умножение типов оперделяется естественно, как произведение чисел.

Квантом амплитуды размера $\varepsilon > 0$ называется список вида

$$\kappa = (\varepsilon, id, |b_{in}\rangle, |b_{fin}\rangle, t_{in}, t_{fin}), \tag{117}$$

где $|b_{in}\rangle$, $|b_{fin}\rangle$ - два разных базисных состояния, $id$ - уникальный идентификационный номер, отличающий данный квант от всех других, $t_{in}, t_{fin} \in T$. Переход вида $|b_{in}\rangle \to |b_{fin}\rangle$называется переходом состояний, $t_{in} \to t_{fin}$называется переходом типов. Мы выберем идентификаторы так, чтобы если они совпадут, все другие атрибуты квантов тоже совпали, так что идентификатор однозначноо опрееляет квант амплитуды. В этом случае должно быть неограниченное число квантов с любом набором атрибутов, за исключением идентификатора. Мы будем отождествлять квант с его идентиикатором без специальных оговорок. Введем обозначения:

$$t_{in}(\kappa) = t_{in},\ t_{fin}(\kappa) = t_{fin},\ s_{in}(\kappa) = b_{in},\ s_{fin}(\kappa) = b_{fin}.$$

Переходы состояний и типов квантово амплитуды указыват, как данный квант будет меняться со временем, и их выбор зависит от $A$; размер кванта амплитуды определяет точность дискретного приближения действия данного оператора $A$ с помощью квантов амплитуды.

Множество $\theta$ квантов амплитуды размера $\varepsilon$ называется квантованием амплитуды, если выполнено следующиее условие:

**Q**. В множестве $\theta$, нет таких квантов $\kappa_1$ и $\kappa_2$ что их переходы состояний одинаковы, $t_{in}(\kappa_1) = t_{in}(\kappa_2)$ и $t_{fin}(\kappa_1) = -t_{fin}(\kappa_2)$, и нет таких квантов $\kappa_1$ и $\kappa_2$ что $s_{in}(\kappa_1) = s_{in}(\kappa_2)$ и $t_{in}(\kappa_1) = -t_{in}(\kappa_2)$.

Условие **Q** означает, что при переходе, обозначаемом символом "$\to$", результат преобразования одного кванта амплитуды не может сократиться с результатом преобразования никакого подобного ему кванта, а также то, что квант амплитуды не может сократиться с дургим непосредственно в начальном состоянии.

Квантование $\theta$ амплитуды задает пару квантовых состояний

$$|\theta_{in}\rangle = \sum_j \lambda_j |j\rangle, \ |\theta_{fin}\rangle = \sum_i \mu_i |i\rangle, \tag{118}$$

по естественному правилу: для любых базисных состояний $|j\rangle$, $|i\rangle$, должны быть выполнены условия

$$\lambda_j = \langle j|\theta_{in}\rangle = \varepsilon \sum_{\kappa\in\theta:\ s_{in}(\kappa)=j} t_{in}(\kappa), \quad \mu_i = \langle i|\theta_{fin}\rangle = \tilde{\varepsilon} \sum_{\kappa\in\theta:\ s_{fin}(\kappa)=i} t_{fin}(\kappa), \tag{119}$$

где $\tilde{\varepsilon}$ - нормализующий коэффициент, так что состояние $|\theta_{fin}\rangle$ имеет единичную норму и $|\theta_{in}\rangle$ имеет произсольную ненулевую норму. Коэффициент $\tilde{\varepsilon}$ не обязан совпадать с $\varepsilon$, так как при квантовании амплитуды обычная форма вектора состояния не сохраняется; если бы мы взяли $\tilde{\varepsilon} = \varepsilon$, то значение $\{|\Psi\rangle\}$ могло бы только уменьшиться в переходе $|\theta_{in}\rangle \to |\theta_{fin}\rangle$; это происходит благодаря тому, что какой-то квант сокращается с другим во второй сумме из (119).

Мы фиксируем размерность $dim(\mathcal{H})$ пространства состояний и будем делать оценки (сверху) рассматриваемых положительных величин: времени и размера кванта амплитуды с точностью до порядка величины, считая все константы зависящими только от независимых констант: $dim(\mathcal{H})$ и от минимальной и максимальной абсолютных величин элементов матрицы $A$. При этом термин "строгий порядок" будет означать оценку как сверху, так и снизу положительными числами, зависящими только от независимых констант. При этом термин "строгий порядок" будет означать оценку как сверху, так и снизу положительными числами, зависящими только от независимых констант.

Для квантования амплитуды $\theta$ и номеров $i, j$ базисных состояний через $n_{i,j}(\theta)$ обозначим число элементов множества $\mathcal{N}_{i,j}(\theta) = \{\kappa \in \theta :\ s_{in}(\kappa) = j,\ s_{fin}(\kappa) = i\}$.

Пусть $\theta(\varepsilon)$ - некоторая функция, отображающая некоторую последовательность положительных чисел $\varepsilon$, сходящуюся к нулю, в квантования амплитуды размера $\varepsilon$. Такую функцию будем называть параметрическим квантованием амплитуды.

Параметрическое квантование амплитуд $\theta(\varepsilon)$ называется согласованным с оператором $A$ и состоянием $|\Psi\rangle$ если для некоторых скалярных функций $c(\varepsilon)$

$$\theta_{in}(\varepsilon) \to |\Psi\rangle,\ c(\varepsilon)\theta_{fin}(\varepsilon) \to A|\Psi\rangle\ (\varepsilon \to 0). \tag{120}$$

Если $A$ - оператор эволюции $U_t$, то наличие параметрического квантования амплитуд $\theta(\varepsilon)$, согласованного с $A$, является совершенно не тривиальным свойством квантовых состояний $|\theta_{in}(\varepsilon)\rangle$, говорящим о том, что для состояний возможно введение скрытого параметра, соответствующего динамике, задаваемой матрицей эволюции $U_t$, и делающего квантовую эволюцию $U_t$ детерминистической. Таким параметром будет квант амплитуды $\kappa \in \theta(\varepsilon)$, где точность детерминистического описания определяется величиной $\varepsilon$.

*Теорема о квантовании амплитуды.*

*Пусть A- произвольная матрица. Для всякого равновесного относительно A состояния $|\Psi\rangle$ существует параметрическое квантование амплитуд $\theta(\varepsilon)$, согласованное с оператором A.*

*Доказательство.*

Пусть задано равновесное относительно $A$ состояние $|\Psi\rangle = \sum\limits_j \lambda_j |j\rangle$ и число $\varepsilon > 0$. Для $|j\rangle$ с ненулевыми $\lambda_j \neq 0$ пусть

$$\lambda_j = \langle j|\Psi\rangle \approx sign_{re}(\underbrace{\varepsilon + \varepsilon + \ldots + \varepsilon}_{M_j}) + sign_{im} i(\underbrace{\varepsilon + \varepsilon + \ldots + \varepsilon}_{N_j}), \tag{121}$$

где $sign_{re}\varepsilon M_j + sign_{im} i\varepsilon N_j \approx \lambda_j$ есть наилучшее приближение амплитуды $\lambda_j$ с точностью $\varepsilon$; $M_j,\ N_j$- натуральные числа, $sign_{re\ (im)} = \pm 1$. Таким образом, первое соотношение стремления из (120) будет выполнено, и надо обеспечить выполнение второго соотношения при согласованности параметрического квантования с гамильтонианом.

Приблизим каждый элемент матрицы эволюции так же, как мы приблизили амплитуды исходного состояния:

$$\langle i|A|j\rangle \approx \pm(\underbrace{\varepsilon + \varepsilon + ... + \varepsilon}_{R_{i,j}}) \pm i(\underbrace{\varepsilon + \varepsilon + ... + \varepsilon}_{I_{i,j}}), \tag{122}$$

где $R_{i,j},\ I_{i,j}$- натуральные числа; действительную и мнимую части - с точностью $\varepsilon$ каждую, а знаки перед действительной и мнимой частями выбираются исходя из того, что данное приближение должно быть максимально точным для выбранного $\varepsilon$.

Амплитуды результирующего состояния $A|\Psi\rangle$ получаются умножением всевозможных выражений (121) на всевозможные выражения (122):

$$\lambda_j\langle i|A|j\rangle \approx (sign_{re}M_j\varepsilon + i\ sign_{im}N_j\varepsilon)(\pm R_{i,j}\varepsilon \pm i\ I_{i,j}\varepsilon). \tag{123}$$

Раскроем в правой части выражения (123) скобки, но не будем производить сокращений. Каждое вхождение выражения $\varepsilon^2$ в амплитуды результирующего состояния после раскрытия скобок в правой части (123) будет получаться умножением определенного вхождения $\varepsilon$ в правую часть (121) на определенное вхождение $\varepsilon$ в правую

часть (122). Проблема заключается в том, что одно и то же вхождение $\varepsilon$ в (121) соответствует не одному, а нескольким вхождениям $\varepsilon^2$ в результат, и потому мы не можем сопоставить кванты амплитуды непосредственно вхождениям $\varepsilon$ в (121).

Скольким вхождениям $\varepsilon^2$ в амплитуды состояния $A|\Psi\rangle$ из результата раскрытия скобок в (123) соответствует одно вхождение $\varepsilon$ в приближение амплитуды $\lambda_j = \langle j|\Psi\rangle$ состояния $|\Psi\rangle$? Это число - кратность данного вхождения $\varepsilon$ - равна $\sum\limits_i (R_{i,j} + I_{i,j})$. Эти числа могут быть различными для произвольного оператора $A$ и состояния $|\Psi\rangle$. Однако поскольку $|\Psi\rangle$ - равновесное относительно $A$, то $\sum\limits_i (R_{i,j} + I_{i,j})$ для разных $j$ будут одинаковыми.

Введем обозначение $\nu = \sum\limits_i (R_{i,j} + I_{i,j})$ - это число вхождений $\varepsilon$ в любой столбец из разложения матрицы (122); это число $\nu$ имеет порядок $1/\varepsilon$ при $\varepsilon \to 0$.

Обозначим через $Z_{i,j}$ множество вхождений буквы $\varepsilon$ в правую часть выражения (122), и пусть $Z_j = \bigcup_i Z_{i,j}$. Тогда число элементов в множестве $Z_j$ будет равно $\nu$.

Рассмотрим меньшее значение кванта амплитуды: $\epsilon = \varepsilon/\nu$. Подставим в выражение (121) вместо каждого вхождения $\varepsilon$ его формальное разложение вида $\varepsilon = \overbrace{\epsilon + \epsilon + \ldots + \epsilon}^{\nu}$, получив разложение амплитуд исходного состояния на числа меньшего размера:

$$\begin{aligned} \lambda_j = \quad & \langle j|\Psi\rangle \approx sign_{re}(\underbrace{\overbrace{\epsilon + \epsilon + \ldots + \epsilon}^{\nu} + \overbrace{\epsilon + \epsilon + \ldots + \epsilon}^{\nu} + \ldots + \overbrace{\epsilon + \epsilon + \ldots + \epsilon}^{\nu}}_{M_j}) + \\ & sign_{im} i(\underbrace{\overbrace{\epsilon + \epsilon + \ldots + \epsilon}^{\nu} + \overbrace{\epsilon + \epsilon + \ldots + \epsilon}^{\nu} + \ldots + \overbrace{\epsilon + \epsilon + \ldots + \epsilon}^{\nu}}_{N_j}). \end{aligned} \tag{124}$$

Пусть $W_1^j, W_2^j, ..., W_{M_j+N_j}^j$ - множества вхождений буквы $\epsilon$ в правую часть выражения (124), отмеченные верхними фигурными скобками. В каждом из этих множеств $\nu$ элементов, как и в определенных ранее множествах $Z_j$. Поэтому мы можем построить для каждого такого множества $W_s^j$ взаимно-однозначное отображение вида $\xi : \ W_s^j \to Z_j$. Для каждого вхождения $\varepsilon$ в (121) естественно определяются его потомки - вхождения $\epsilon$ в (124); потомков для каждого вхождения будет $\nu$.

Мы определим квантование амплитуд $\theta = \theta(\epsilon)$ так, что идентификаторы $id$ квантов амплитуд $\kappa \in \theta$ будут просто вхождениями $\epsilon$ в разложения (124) для всех $j$. Определим, как требуется в (117), начальное состояние и начальный тип этого кванта как состояние и тип данного вхождения. Осталось определить переходы состояний и типов. Это определение дается следующим естественным образом.

Каждой паре вида $(w_s^j, \xi(w_s^j))$, где $w_s^j \in W_s^j$, поставим в соответствие переход состояний и переход типов естественным образом. А именно, переход состояний будет иметь вид $j \to i$ для такого $i$, что $\xi(w_s^j) \in Z_{i,j}$; переход же типов $t_{in} \to t_{fin}$ определяется так, что $t_{in}$ есть тип вхождения[4] $w_s^j$, а тип $t_{fin}$ есть произведение типа вхождения

[4]Тип вхождения определяется естественным путем после раскрытия скобок, например, для вхож-

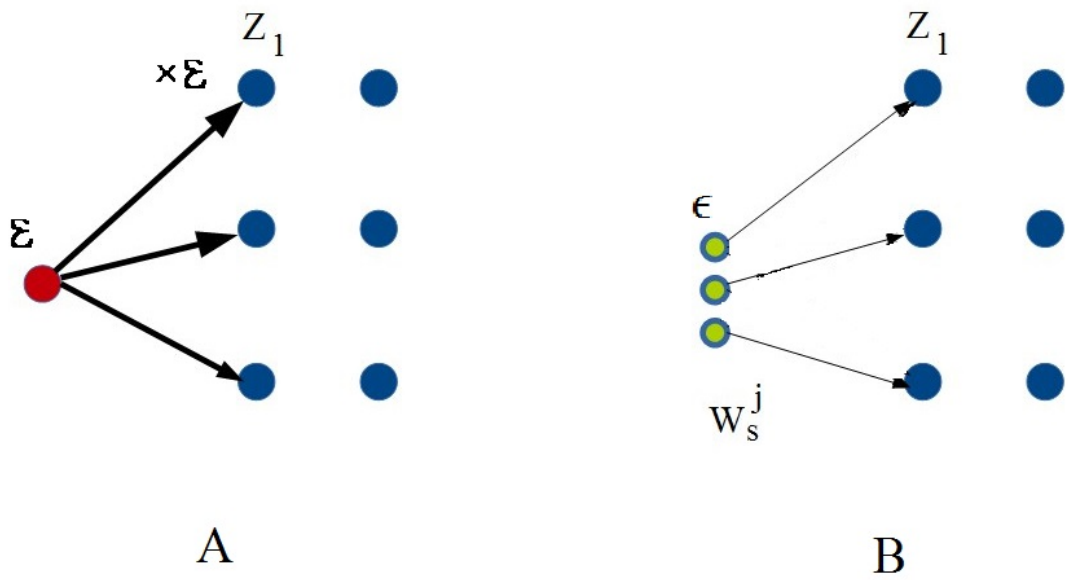



Рис. 59: A. Умножение вектора состояния на матрицу. Вклад каждого вхождения $\varepsilon$ умножается на $\varepsilon$. B. $\theta$- сдвиг исходного состояния. Размер кванта амплитуды $\epsilon$ имеет порядок $\varepsilon^2$.

$t_{in}$ на тип вхождения $\xi(w_s^j)$. Множества $W_s^j$ не пересекаются при разных парах $j, s$, поэтому мы считаем областью определения функции $\xi$ все вхождения буквы $\epsilon$ в правую часть (124) (см. Рис. 59).

Пусть теперь переход состояний и типов для данного кванта $\kappa \in \theta$ соответствует отображению $\xi$ в определенном выше смысле. Условие **Q** при этом будет выполнено, так как в выражении для матричного элемента (122) нет сокращающихся членов. Поэтому мы определили квантование амплитуды.

В силу нашего определения функции $\xi$, распределение амплитуд в состоянии $|\theta\Psi\rangle$ будет примерно пропорциональным распределению амплитуд в состоянии $A|\Psi\rangle$, причем точность будет неограниченно расти с уменьшением $\varepsilon$ до нуля. Для того, чтобы определить нужное для согласованности $\theta$ с оператором $A$ значение функции $c(\epsilon)$, подсчитаем вклад каждого вхождения $\varepsilon^2$ в правую часть равенства (123) и сравним его с вкладом соответствующей ему буквы $\epsilon$ в $|\theta\Psi\rangle$.

Зафиксируем какой-либо переход типов $t_{in} \to t_{fin}$ и переход состояний $s_{in} \to s_{fin}$. Будем называть вхождение $\varepsilon^2$ в результат раскрытия скобок в (123) соответствующим этим переходам, если $j = s_{in}$, $i = s_{fin}$, и это вхождение получается умножением вхождения $\varepsilon$ типа $t_{in}$ в первый сомножитель правой части (123) на вхождение $\varepsilon$ во второй сомножитель типа $t'$, так что $t_{in}t' = t_{fin}$. Каждому такому вхождению $\varepsilon^2$ соответствует ровно один квант амплитуды размера $\epsilon$ из квантования амплитуды, определенного выше через функцию $\xi$, у которого те же самые переходы состояний и типов: этот квант соответствует тому вхождению $\epsilon$, которое взаимно-однозначным отображением $\xi$ переводится в данное вхождение $\varepsilon^2$ (см. Рис. 60).

Итак, вхождения $\varepsilon^2$ в (123) находятся во взаимно-однозначном соответствии с вхождениями $\epsilon$ в (124) и мы получаем $c(\varepsilon) = \varepsilon\nu$.

дения $\ldots - i\epsilon\ldots$ типом будет $-i$.

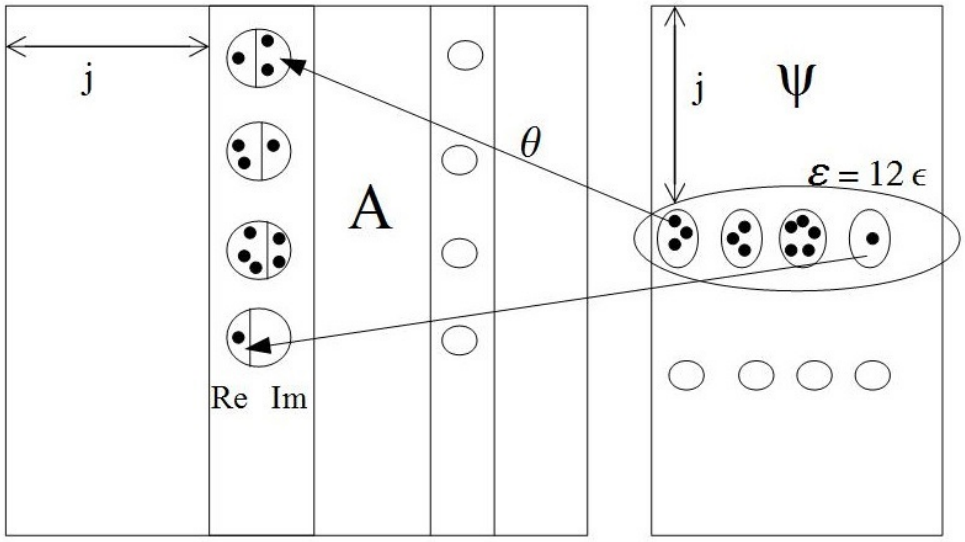



Рис. 60: Дереминизм траекторий при умножении вектора состояния $|\Psi\rangle$ на матрицу $A$. Каждый квант амплитуды переходит в определенный квант амплитуды результирующего состояния, и нет ветвлений.

Заметим, что если $A = 0$, мы можем взять $c(\varepsilon) = 0$ и любое квантование амплитуды будет подходить.

Теорема доказана.

Заметим что если мы откажемся от условия **Q** и условия равновесности состояния $|\Psi\rangle$ относительно $A$, мы тоже сможем определить матричный детерминизм, только мы должны тогда ввести рудицируемые члены вида $\varepsilon - \varepsilon$ в элементы матрицы; тогда формальные вхождения амплитуд во все столбцы $A$ будут содержать одинаковое число членов, и рассуждения останутся справедливыми, но интерференция теперь будет иметь место не только между наследниками разных базисных состояний, как для равновесных состояний $|\Psi\rangle$, то также и между наследниками одного и того же состояния.

Отметим также, квантовые вычисления, для которых используются только гейты $CNOT$ и Адамара имеют то свойство, что для любого гейта число элементов во всех $Z_j$ одинаково, так что для таких вычислений детерминизм обеспечен с интерференцией только между образами разных базисных состояний. В частности, таков алгоритм Гровера.

Более того, для реализации квантовых вычислений через гейты на оптических полостях (см., например, [39]), состояния, полученные после их применения, будут связанными, так что интерференция в ходе таких вычислений будет обладать тем же свойством.

# 16 Заключение

Мы представили аргументы в пользу того, что стандартный матричный вормализм квантовой механики в области слоных систем должен быть ограничен соотношением неопределенностей "точность - сложность" вектора состояния, где коэффициент равен верхней границе числа кубитов, которые могут иметь нередуцированное запутанное состояние. Это не противоречит никаким экспериментам над многокубитными системами, но позволяет строить модели таких систем на существующих суперкомпьютерах. Данное ограничение также касается эквивалентности базисов в пространстве состояний и влечет минимальную ненулевую амплитуду для суперпозиций. Размер кванта амплитуды можно приблизительно найти в экспериментах по реализации алгоритма Гровера. Квантование аплитуд дает возможность введения в квантвоую теорию некоторого типа детерминизма, который не сводится к квазиклассическому приближению.

# 17 Лекция 10. Квантовая нелокальность, неравенство Белла и распределенные квантовые вычисления

Схема эксперимента, доказывающего наличие квантового мгновенного действия на расстоянии, была предложена Дж.Беллом в начале 60-х годов ([45],[46]); сами же эксперименты были проведены впервые в 1980-х годах А.Аспеком и А.Цайлингером ([47], [48], а также ссылки в работах [49] и [50]). В этих экспериментах запутанность проявляется не на ангстремных расстояниях, как в молекуле водорода, а на расстояниях в несколько сотен километров.

В эксперименте получаются состояния вида $|\Psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ для фотонов, которые детектируются на расстояниях с несколько сотен километров между ними. Представим себе, что первый фотон детектируется наблюдателем Алисой, а второй - Бобом. Условия эксперимента таковы, что у Алисы есть две возможности выбрать детектор, то есть измерительный базис в пространстве состояний ее кубита, и у Боба - тоже две возможности. А именно, Алиса может выбрать собственные вектора эрмитова оператора $\sigma_x$ или $\sigma_z$, а Боб: $(\sigma_x + \sigma_z)/\sqrt{2}$ или $(\sigma_x - \sigma_z)/\sqrt{2}$ соответственно. Поскольку у всех перечисленных операторов собственные значения только 1 или $-1$, мы будем считать, что Алиса получила значение $X$ или $Y$, а Боб - $a$ или $b$ соответственно, в вышеприведенном порядке. Например, можем условиться, что 1 означает, что детектируется фотон с горизонтальной поляризацией, а $-1$ - с вертикальной (относительно соответствующего положения детектора). Это эквивалентно выбору каждым участником эксперимента *наблюдаемой* (см. Главу 1) из двух возможностей, для каждой - с вероятностью $1/2$.

Определим случайную величину $\xi$ как произведение результатов измерений Алисы и Боба, взятое со знаком минус, в том случае, когда выборы детекторов были $Y$ и $b$ соответственно, и произведение результатов со знаком плюс во всех других случаях. Значение такой величины получается простым умножением и надлежащим изменением знака, после того, как Алиса и Боб выяснили, какую ориентацию детек-

торов избрал каждый из них; в ходе самого измерения они не согласовывают своего выбора.

Алиса и Боб получают одну за одной пары бифотонов в состоянии $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ и производят свои испытания со случайно выбранными наблюдаемыми, составляя протокол экспериментов. Затем сходятся вместе и вычисляют значение случайной величины $\xi$, которая равна произведению значений наблюдаемых Алисы и Боба, если их выбор детекторов был: $Y, a$ или $X, b$ или $Y, a$, и произведению этих значений с обратным знаком, если выбор был $Y, b$.

При поверхностном взгляде может показаться, что $X, Y, a, b$ есть случайные величины, с которыми можно оперировать, как с обычными числами. Временно примем такую точку зрения, и проведем некоторый несложный подсчет математического ожидания $E$ величины $\xi$. Мы вынесем $X$ и $Y$ за скобки в выражении

$$E = Xa + Xb + Ya - Yb, \tag{125}$$

которое получится, если сложить все возможные результаты вычислений $\xi$. Тогда получится, что в одной скобке стоит 0, а в другой - число, по модулю равное 2. Тогда можно оценить $E$ как $|E| = 2/4 = 1/2$, поскольку все четыре выбора ориентаций детектора равновероятны. Естественно, для случайных величин $X, Y, a, b$ мы будем иметь точно такое же неравенство, причем безразлично, являются ли они зависимыми, или нет. Значит, и для математического ожидания $M(\xi)$ величины $\xi$ мы получим неравенство

$$M(\xi) \leq 1/2, \tag{126}$$

которое называется неравенством Белла.

А теперь подсчитаем $M(\xi)$ для выписанных нами наблюдаемых с помощью квантово - механического правила $\langle A\rangle_\Psi = tr(\rho_\Psi A)$ определения среднего значения (собственных чисел) эрмитова оператора $A$ в состоянии $\Psi$[5]. Несложный расчет[6] покажет, что $M(\xi) = \frac{1}{4}2\sqrt{2}$ (множитель $1/4$ везде возникает из-за равновероятности выбора всех 4 комбинаций детекторов). Именно это и детектируется в эксперименте, к которому мы еще вернемся. В чем же дело? Где мы допустили ошибку в рассуждении? Очевидно, возможность ее совершить только одна: предположение о том, что результаты измерений Алисы и Боба выражаются как случайные величины $X, Y, a, b$ использовалось нами нестрого, в силу того, что мы не применяли определения случайной величины. Сейчас мы восполним этот пробел, и увидим, как это приведет нас к новому пониманию смысла эксперимента с двумя запутанными фотонами.

Рассмотрим эксперимент более строго. Для этого напомним основные понятия колмогоровской теории вероятности. Она включает 3 объекта: вероятностное пространство, случайные величины, и их численные характеристики. Сначала определим центральное понятие: множество элементарных исходов. Это (у нас всегда конечное) множество

$$\Omega = \{\omega_1, \omega_2, \ldots, \omega_k\},$$

[5]Оно вытекает из определенния математического ожидания для собственных значений эрмитова оператора $A$: $\langle A\rangle = \langle\Psi|A|\Psi\rangle$. Слушателю предлагается а) доказать, что математическое ожидание наблюдаемой $A$ в состоянии $|\Psi\rangle$ вычисляется по данной формуле, и б) приведенную в тексте формулу, исходя из данной.

[6]Надо рассмотреть все случаи ориентации детекторов, и для каждого составить редуцированную матрицу плотности нашего состояния, а затем применить правило полной вероятности.

каждый элемент которого отражает всю сущность мира, играющую роль для рассматриваемого эксперимента. Это означает, что выбрав какой либо элемент $\omega_j \in \Omega$, мы автоматически выбираем исход любого эксперимента из рассматриваемого набора, включая положение детектора, состояние всех элементарных частиц в нем, а также всех параметров, которые мы даже не знаем, но которые определяют, каков будет исход эксперимента[7].

В силу негибкой формы "запрета на скрытые параметры" в копенгагенской квантовой механике, мы в ее рамках не имеем возможности рассмотреть даже приближение множества $\Omega$. Таким образом, точное рассмотрение квантово-механических задач для многих частиц обязано выходить за пределы копенгагенской квантовой теории. Выход за пределы подразумевает не нарушение законов, а рассмотрение сущностей, недоступных в копенгагенской теории. Можно выразиться иначе. Стандартные задачи квантовой теории, подразумевающие использование аппарата волновых функций и проекций, не должны использовать скрытых параметров, то есть не должны касаться вероятностной структуры волновой функции. К стандартным относятся задачи о поведении одной квантовой частицы или сводящиеся к ним. Однако наша задача о запутанных фотонах не является стандартной, поскольку она касается уже двух частиц. Хотя запутанное состояние двух частиц в некотором смысле можно свести к одночастичному, но операторы наблюдения, используемые Алисой и Бобом существенно различные, и потому мы имеем дело с существенно не одночастичным квантовым состоянием. Иногда для решения таких задач хватает арсенала копенгагенской теории, но наш случай явно не относится к этой категории, и потому мы должны для нахождения решения использовать теорию вероятностей, рассмотрев множество элементарных исходов $\Omega$. Ограничение стандартного формализма здесь в том, что мы должны считать это множество конечным; хотя в данном случае это никак не скажется на выводах.

На множестве $S$ всех подмножеств $\Omega$ надо определить так называемую вероятность - функцию вида $P: \ S \longrightarrow [0,1]$, удовлетворяющую аксиомам вероятности: $P(A \cup B) = P(A) + P(B)$ для непересекающихся $A, B \in S$, $P(\emptyset) = 0$, $P(\Omega) = 1$. Определить $P$ очень просто: $P(A)$ есть частное от деления числа всех элементов $A$ на $k$. Это иногда называют частотным определением вероятности.

Случайной величиной называется любая функция вида

$$\xi: \ \Omega \longrightarrow R.$$

Мы можем вычислять математическое ожидание случайной величины $\xi$ по стандартной формуле $M(\xi) = \sum\limits_{x \in R} xP(\{\omega \in \Omega \mid \xi(\omega) = x\})$.

Надо сразу сказать, что бессмысленно искать "объяснения" эксперимента с бифотонами, не прибегая к приведенному выше строгому определению вероятности. Единственная математически точная формулировка понятия "вероятность" вытекает из приведенного определения. Теперь рассмотрим, как этот арсенал применяется к рассматриваемой ситуации.

С точки зрения квантовой механики, состояние $|\Psi\rangle$ двух рассматриваемых фото-

[7] То обстоятельство, что мы не знаем структуры $\Omega$, не играет никакой роли. Мы все равно должны рассматривать этот объект явно, если говорим о вероятностях.

нов представляет единый вектор в гильбертовом пространстве состояний. Это означает, что существует такое пространство элементарных исходов $\Omega$, что все величины $X, Y, a, b$ являются случайными величинами над этим пространством, то есть функциями от элементарных исходов: $X(\omega), Y(\omega), a(\omega), b(\omega)$.

Теперь мы должны переформулировать условия эксперимента на языке теории вероятностей. У нас есть следующая ситуация. Алиса и Боб, независимо друг от друга и совершенно случайным образом выбирают каждый какое-либо одно состояние детектора из имеющихся у него двух возможностей, сразу же после чего каждый фотодетектор детектирует попавший в него фотон (конкретный результат измерения есть 1, если получено состояние $|\epsilon_1\rangle$ из базиса собственных векторов оператора наблюдаемой, и $-1$ - если $|\epsilon_2\rangle$, - выбор из этих альтернатив осуществляется исходя из особенностей детектора). Это означает, что выбор ориентации детектора Алисой входит в некоторый объект $\omega_1$, а выбор ориентации детектора Боба входит в объект $\omega_2$, так что элементарный случайный исход одного эксперимента $\omega \in \Omega$ имеет вид $(\omega_1, \omega_2)$. Если у фотонов есть какие-либо скрытые параметры, то параметры фотона, прилетевшего к Алисе, мы считаем входящими в $\omega_1$, а для фотона, прилетевшего к Бобу - в $\omega_2$. Таким образом, мы должны предположить, что $\Omega = \Omega_1 \times \Omega_2$, где множества $\Omega_1$ и $\Omega_2$ соответствуют выборам Алисы и Боба соответственно. Такое предположение выражает так называемую свободу воли у обоих участников эксперимента. Отсутствие свободы воли означало бы попросту то, что выбор, скажем, Алисы, автоматически определял бы и выбор Боба. В реальных экспериментах вопрос с ориентацией решается не людьми, а электроникой, исходя из таких событий, которые с точки зрения здравого смысла, обязаны быть независимыми (например, потоки посторонних фотонов из разных областей космического пространства). Свобода воли участников эксперимента является необходимым предположением, если мы занимаемся наукой.

Теперь рассмотрим, что есть случайные величины $X, Y, a, b$. Поскольку $\omega_1$ автоматически определяет ориентацию детектора Алисы, обозначим через $\Omega_1^X$ такое подмножество $\Omega_1$, которое соответствует ориентации детектора $X$, и аналогично обозначим подмножества, соответствующие $Y, a, b$. При этом $\Omega_1$ будет суммой непересекающихся подмножеств $\Omega_1^X$ и $\Omega_1^Y$, а $\Omega_2$ - суммой также не пересекающихся $\Omega_2^a$ и $\Omega_2^b$. Мы должны принять, что результат детектирования Алисы есть случайная величина $\xi_1(\omega_1, \omega_2)$, а результат детектирования Боба есть случайная величина $\xi_2(\omega_1, \omega_2)$, так что общий результат есть декартово произведение $\xi = (\xi_1, \xi_2)$, причем $X$ есть ограничение функции $\xi(\omega_1, \omega_2)$ на область $\omega_1 \in \Omega_1^X$, $Y$ есть ограничение функции $\xi(\omega_1, \omega_2)$ на область $\omega_1 \in \Omega_1^Y$, $a$ есть ограничение функции $\xi$ на область $\omega_2 \in \Omega_2^a$, и $b$ - на область $\omega_2 \in \Omega_2^b$. Для того, чтобы сделать величины $X, Y, a, b$ определеными на всем множестве элементарных исходов $\Omega$, мы дополним их нулем в тех областях, где они не определены нами явно.

Определим случайную величину $\xi$ так:

$$\xi(\omega_1, \omega_2) = \begin{cases} \xi_1(\omega_1, \omega_2)\xi_2(\omega_1, \omega_2), & \text{если } \omega_1 \notin \Omega_1^Y \text{ или } \omega_2 \notin \Omega_2^b, \\ -\xi_1(\omega_1, \omega_2)\xi_2(\omega_1, \omega_2), & \text{если } \omega_1 \in \Omega_1^Y \text{ и } \omega_2 \in \Omega_2^b. \end{cases}$$

Тогда мы имеем: $\xi = Xa + Xb + Ya - Yb$.

Посчитаем ее матожидание по приведенному определению, выбрав частотное определение вероятности. У нас получится

$$M(\xi) = \frac{1}{k}\sum_{\omega_1,\omega_2} X(\omega_1,\omega_2)a(\omega_1,\omega_2) + X(\omega_1,\omega_2)b(\omega_1,\omega_2) \\ +Y(\omega_1,\omega_2)a(\omega_1,\omega_2) - Y(\omega_1,\omega_2)b(\omega_1,\omega_2).$$

Отметим, что мы при этом пользуемся тем, что многие называют реализмом. Это означает, что мы имеем право неоднократно пользоваться ограниченным количеством букв $\omega_j$ так, что любые их комбинации будут соответствовать реальным экспериментам по детектированию фотонов. По иному это можно сформулировать как свободу воли при выборе из конечного набора вариантов реальности. Нетрудно убедиться, что с данным выражением для матожидания невозможно поступить так, как это было выше проделано с числами при доказательстве неравенства Белла (126), в силу наличия аргументов у случайных величин. Действительно, поскольку результат измерения одного из участников зависит от элементарных исходов для них обоих, мы должны были бы вместо выражения (125) написать другое выражение: $E = Xa + X'b + Ya' - Y'b'$, и у нас не получилось бы вынесения за скобки общих множителей, то есть наше наивное рассуждение было бы неверным.

Однако предположим, что, помимо очевидного для нас реализма, у нас имеется еще и так называемая локальность. Кратко говоря, локальность означает, что результат измерения Алисы никак не зависит от ориентации детектора Боба и наоборот. Мы обсудим физический смысл локальности ниже. Формально локальность означает, что $X$ и $Y$ зависят только от $\omega_1$, а $a$ и $b$ - только от $\omega_2$. Тогда мы сможем проделать с выражением для математического ожидания тот же самый трюк, что и при доказательстве неравенства Белла. А именно, мы сгруппируем все слагаемые большой суммы в группы по 4 вида

$$X(\omega_1)a(\omega_2') + X(\omega_1)b(\omega_2) + Y(\omega_1')a(\omega_2') - Y(\omega_1')b(\omega_2),$$

состоящие из ненулевых членов, так что внутри каждой группы можно будет вынести $X$ и $Y$ за скобки, и так же как и выше доказать, что эта группа не превышает 2. Поскольку в группе задействуется 4 различных $\omega$, мы получаем, что математическое ожидание $\xi$ не превосходит $1/2$. То есть локальность ведет к выполнению неравенства Белла. Таким образом, мы пришли к выводу, что из эксперимента по детектированию бифотонов вытекает нелокальность квантовой механики.

Теперь рассмотрим нелокальность подробнее. Она означает, что случайные величины, относящиеся к Бобу, зависят не только от его компоненты элементарного исхода, но и от компоненты, принадлежащей Алисе, и наоборот, то есть все исходы $X, Y, a, b$ зависят как от $\omega_1$, так и от $\omega_2$.

Как это может быть реализовано? Только так: есть некоторый объект $\tilde{\omega}$, который путешествует от Алисы к Бобу и обратно, перенося информацию о другой половинке элементарного исхода соответствующего эксперимента. Если этот объект $\tilde{\omega}$ подчиняется ограничению релятивизма, и не может передвигаться быстрее света, то мы можем вывести ограничения на времена испускания бифотона источником и времен детектирования прибытия каждого из фотонов Алисой и Бобом. Пусть $\Delta t$ - естественная неопределенность момента испускания бифотона источником, о которой мы предполагаем, что все бифотоны, время испускания которых лежит вне этого диапазона, не играют никакой роли для получения статистики в данном эксперименте. Наличие такого интервала есть непосредственное следствие соотношения

неопределенности "энергия-время". Теперь мы предположим, что часы Алисы, Боба, и источника бифотона точно синхронизированы, и введем величину $\delta t$, равную разности момента срабатывания детектора и момента выбора его положения (то есть выбора между $X$ и $Y$ и между $a$ и $b$). Тогда, если материальный объект $\tilde{\omega}$, переносящий информацию о другой половинке элементарного исхода, подчиняется релятивизму, то должно выполняться неравенство

$$\Delta t + \delta t \geq d/c, \tag{127}$$

где $d$ есть расстояние между Алисой или Бобом, и источником бифотонов, $c$ скорость света.

Эксперименты свидетельствуют, что это неравенство нарушается для бифотонов, детектируемых на расстояниях в несколько сот километров, что имеет совершенно фундаментальные следствия для квантовой теории. Действительно, нарушение (127) говорит о том, что $\tilde{\omega}$ не может быть скрытым параметром ни одного из фотонов.[8] То есть $\tilde{\omega}$ непосредственно переносит информацию об ориентации детекторов от Алисы в Бобу или наоборот. Этот эффект принято называть "квантовой нелокальностью"; он непосредственно вытекает из стандартного квантового формализма, но в действительности, делает необходимым как раз переход от узких копенгагенских рамок к пост-квантовой теории, в которой случайные исходы $\omega$ должны обрести реальный смысл, а не служить лишь формальной цели - математической согласованности.[9]

Квантовая теория полностью согласуется с принципом релятивизма, согласно которому никакая информация не может перемещаться со скоростью, превосходящей скорость света. Формально это выражается в том, что статистика измерений Алисы никак не зависит от того, измеряет ли Боб свой кубит или нет. То есть с помощью запутанного квантового состояния невозможно передавать информацию, генерированную участниками эксперимента друг другу. Но мы только что выяснили, что это ограничение не распространяется на информацию об элементарных исходах в конкретных экспериментах о измерении квантовых состояний, когда они собраны воедино!

Из этого можно сделать только один вывод. Имеется своего рода административная система, взаимодействие с которой и определяет реальность. Это взаимодействие в точности соответствует взаимодействию пользователя с компьютером. Пользователь, то есть экспериментатор, определяет условия (положение детекторов), после чего административная система, работающая с элементарными исходами, выдает результат эксперимента. При этом время, потраченное административной системой на согласование заданных различными пользователями условий, не является реальным физическим временем.

Мы используем здесь программистскую терминологию, в которой административная система означает вполне определенную вещь, которая должна входить в постквантовый формализм, и потому не должна вызывать никаких иных ассоциаций. Нелокальность элементарных исходов $\omega$ говорит в пользу того, что эти исходы могут

[8] В реальных экспериментах, как правило, проверяют не нарушение (127), а непосредственно предотвращают обратное перенесение информации самими фотонами, выставляя заглушки после их прохождения.

[9] Познакомиться с различными точками зрения на квантовую нелокальность можно, например, по статьям из [51].

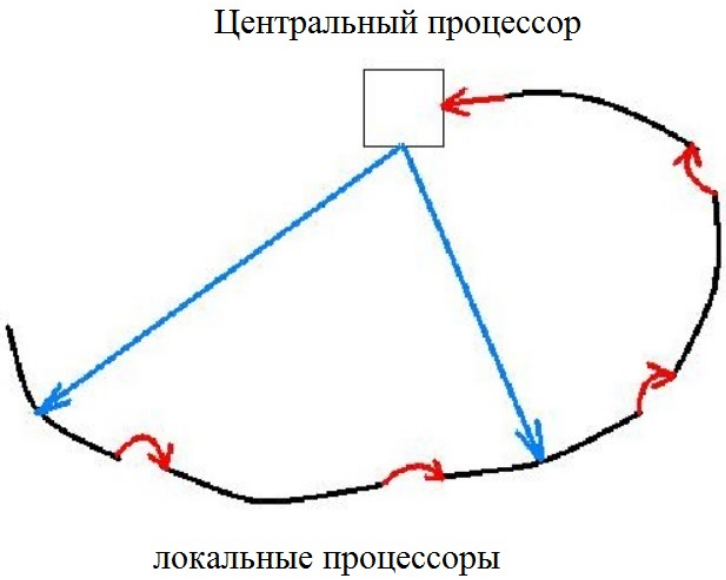



Рис. 61: Схема одностороннего управления

обрести реальный смысл именно для сложных систем и процессов, затрагивающих большие пространственные области. Для простых же систем, например, для одного единственного атома или даже молекулы нелокальность сама по себе не играет большой роли: она проявляется в достаточно тонком эксперименте, описанном нами, и эффект от нее для простых систем даже меньше релятивистских поправок.

Однако квантовое дальнодействие позволяет создавать удивительные протоколы информационного обмена, один из которых мы рассмотрим ниже.

## 17.1 Пример квантового превосходства в распределенных вычислениях с односторонним управлением

Построение квантового компьютера - сложный и многосторонний процесс, и важную роль в нем играют ограниченные модели квантовых вычислений, например, квантовые ветвящиеся программы ([52]) или программы моделирования биохимии ([53].) Преимущество квантовых методов может заключаться не в ускорении вычислений в обычном смысле, а в использовании отдельных элементов квантовой природы для получения финального выигрыша в качестве полученного результата.

Здесь мы продемонстрируем, как нарушение неравенства Белла может помочь повысить эффективность некоторых распределенных вычислений. Пример, который мы приведем (см. [54]), искусственно построен и призван лишь иллюстрировать возможность практического использования удивительного свойства квантовой нелокальности; к тому же эффект от этого использования не слишком велик. Однако данный пример обладает схожестью с биологическим процессом роста сложных молекул с линейной организацией первичной структуры, и потому он говорит о том, что поиск дальнейших приложений квантовой нелокальности может быть плодотворным.

## 17.2 Одностороннее управление

Мы покажем, как эта цель может быть достигнута с использованием нарушения неравенства Белла. Рассмотрим модель распределенных вычислений с односторонним управлением, где все вычислительные устройства подразделяются на центральный процессор (CPU) и удаленные периферийные устройства, способные непосредственно получать команды от CPU. Обратная передача информации от периферийных устройств к центральному процессору не происходит непосредственно, но только в виде последовательного трансфера через цепочку периферийных устройств, которые локально взаимодействуют друг с другом, как показано на рисунке 61. В примере, который мы разберем, использование запутанных состояний фотонов в управлении дает увеличение качества результата вычисления, превосходящее результат классического управления примерно в 1.138 раз. Это - задача синтеза двух удаленных цепочек, состоящих из отдельных звеньев, осуществляемого на двух периферийных устройствах.

Центральный процессор посылает сигнал к двум периферийным процессорам, каждый из которых отвечает за соответствующую подсистему всей системы. Например, CPU решает задачу синтеза на одной подсистеме некоторого полимера $A$, имеющего особую активность, и, одновременно - задачу синтеза другого полимера $B$, который подавляет (или, наоборот, интенсифицирует) данную активность, уже на другой подсистеме. CPU посылает соответствующий сигнал на обе подсистемы, и переключается на другие задания, скажем, на синтез другой пары полимеров $A'$ и $B'$.

Что случилось бы, если периферийные процессоры стали бы посылать сингалы друг другу непосредственно? Пусть у нас есть $m$ подсистем, каждая из которых управляется своим собственным процессором. Для корректной адресации сигналов между всеми возможными парами (их порядка $m^2$) мы должны были бы загрузить CPU этой работой. Центральный процессор вынужден был бы ждать время $cD$ для каждой пары, где $D$ - расстояние между переферийными процессорами, $c$ - скорость света, прежде чем переключиться на следующее задание. Если $m$ достаточно велико (в реальных био-системах это число очень велико), такая схема вычислений, основанная на адресации сигналов через CPU привела бы к фатальной задержке управления, что сделало бы всю схему непригодной.

Мы, таким образом, приходим к необходимости одностороннего управления, когда CPU посылает сигналы периферийным процессорам немедленно, не ожидая отклика от них. Обратная информация же поступает на CPU не непосредственно, а через цепочку посредников, как в клеточном автомате. Эта форма огранизации обработки информации может быть эффективна в живых организмах, так как в них центральная нервная система, играющая роль CPU, должна быть свободна от рутинной работы по управлению метаболизмом.

## 17.3 Квантовые бифотонные сигналы

В рассматриваемой ситуации использование CPU бифотонов (запутанных состояний фотонов) дает преимущество по сравнению с чисто классическим CPU. Для то-

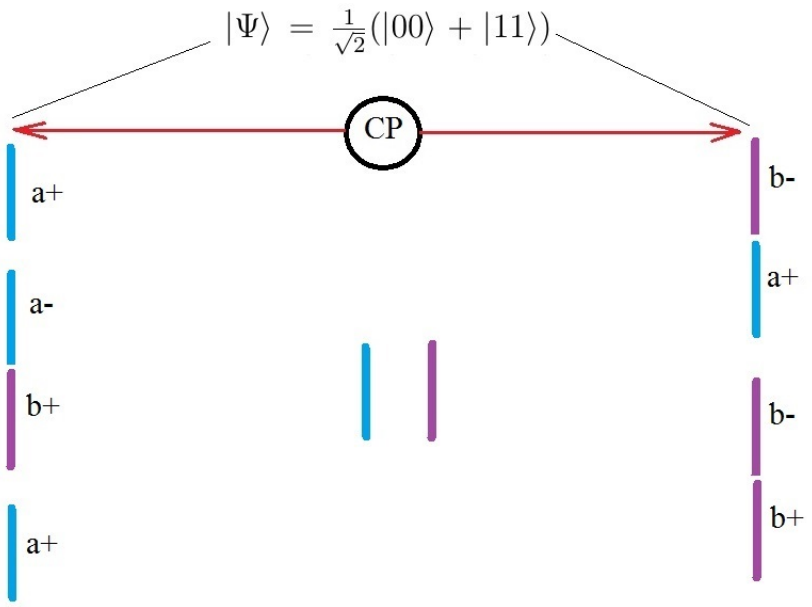



Рис. 62: Распределенный синтез цепочек

го, чтобы продемонстрировать это, мы рассмотрим следующую абстрактную задачу. Предположим, что требуется синтезировать две полимерные молекулы, химическая структура которых имеет вид $C_1 = (c_1^1, c_2^1, ..., c_M^1)$, $C_2 = (c_1^2, c_2^2, ..., c_M^2)$, так что они состоят из моноблоков двух типов: $a$ и $b$: $c_i^j \in \{a, b\}$ (см. рисунок 62

).

Качество такой взаимной сборки двух полимеров проверяется наложением готовых цепочек друг на друга: первая $C_1$ на вторую $C_2$, и критерий качества есть степень склейки этих цепочек. Каждый моноблок имеет внешнюю (выпуклую) и внутреннюю (вогнутую) поверхности, где последняя снабжена специальным шариком, расположенным в ее центре. В фиксированной позиции два моноблока могут склеиться в одном из следующих случаев: 1) их поверхности или половины поверхностей полностью совмещаются вертикальным смещением, или 2) их центральные шарики при таком сдвиге оказываются в одной точке, как показано на рисунке 63.

Физическая структура полимера, от которой зависит склейка, определяется не только последовательностью моноблоков в цепочке; склейка зависит также от дополнительной опции: их точного расположения относительно друг друга в цепочке. Соседние моноблоки в полимере соединены гибкой связью, которая может либо сжаться на $dx$, что составляет четверть длины моноблока, либо растянуться на такую же длину. Мы в этих случаях скажем, что моноблок сдвинут назад или вперед соответственно относительно положения равновесия связи. В ходе синтеза моноблоки устанавливаются с этими ограничениями и их позиции фиксируются. Затем две цепочки накладываются друг на друга и для каждой пары налегающих моноблоков устанавливается наличие склейки. Из принятого ограничения вытекает, что если в такой паре налегающих моноблоков они были сдвинуты в одну сторону, они склеиваются так же, как если бы сдвигов не было; а если в разные - результирующий сдвиг составляет половину длины моноблока.

После этого вычисляется число склеенных пар наложенных друг на друга мо-

ноблоков и это число считается численной характеристикой качества сборки пары цепочек.

Синтез цепочек происходит как последовательное присоединение к каждой из существующих цепочек нового моноблока - того, который первым появился в точке сборки одной и другой цепочки. Моноблоки берутся из среды, окружающей точки роста, где они находятся в хаотическом движении и оба типа распределены поровну. При этом можно сдвинуть вновь присоединенный моноблок либо назад, либо вперед на расстояние $dx$. Мы обозначим сдвиг вперед через $+$, сдвиг назад - через $-$. Каждая $j$-я пара моноблоков в обеих цепочках, наложенных друг на друга после синтеза, соответствуют, таким образом, четверке $c_j^1 c_j^2 s_j^1 s_j^2$, где последние два члена являются сдвигами $s_j^{1,2} \in \{+, -\}$.

Из наших правил (см. рисунок 63) следует, что склейка соответствует парам наложенных моноблоков вида: $aa++(--)$, $ab++(--), bb++(--), ba+-(-+)$, тогда как пары иного вида: $aa+-(-+), ab+-(-+), bb+-(-+), ab++(--)$ склейки не дают. Отметим несимметричное поведение моноблоков типа $a$ и $b$: пары $ab$ и $ba$ склеиваются по разному при одинаковых сдвигах. Эта асимметрия выглядит как асимметрия в неравенстве Белла, что и даст нам повышение качества результирующей склейки при бифотонном управлении по сравнению с классическим управлением.

Мы предполагаем, что рост полимера $C_1$ идет в одной точке, а рост $C_2$ - в другой, причем эти точки разделены большим расстоянием (например, происходят в разных странах). Задача в том, чтобы организовать этот синтез так, чтобы число несклееных пар наложенных моноблоков была бы минимальной, или, иначе говоря, чтобы число склеек было максимальным.

Подобная задача может возникнуть при моделировании синтеза гена и антигена в разных живых клетках. Мы можем создать информационный канал управления ими из одного центра; правда, при большой дистанции между точками сборки такое управление способно замедлить сам процесс сборки, что для реальных полимеров представляет отдельную проблему, выходящую за рамки нашей модели.

Покажем, как использовать бифотонное управление процессом одновременного синтеза для получения квантового превосходства.

Итак, для минимизации критических (несклеенных) пар моноблоков мы используем сигналы CPU в виде EPR состояний $|\Psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, и подсчитаем число критических пар, возникающих при таком управлении. Если бы управление было классическим, в обозначениях из предыдущего параграфа мы имели бы неравенство Белла

$$E(a_1 b_2 + b_1 b_2 + a_1 a_2 - b_1 a_2) \leq 2. \tag{128}$$

Примем следующее соглашение. Нижний индекс обозначает точку сборки (номер полимера) 1 или 2. Буква $a$ или $b$ обозначает тип моноблока, присоединяемого к цепочке, знак соответствует направлению сдвига этого моноблока, как мы условились. Результат присоединения моноблоков в обеих точках сборки определен, если для 1 и 2 нижнего индекса мы имеем во-первых, букву $a$ или $b$, и во-вторых, знак сдвига $+$ или $-$. Буква $a$ или $b$ всегда определяет тип моноблока, ближайшего к точке сборки

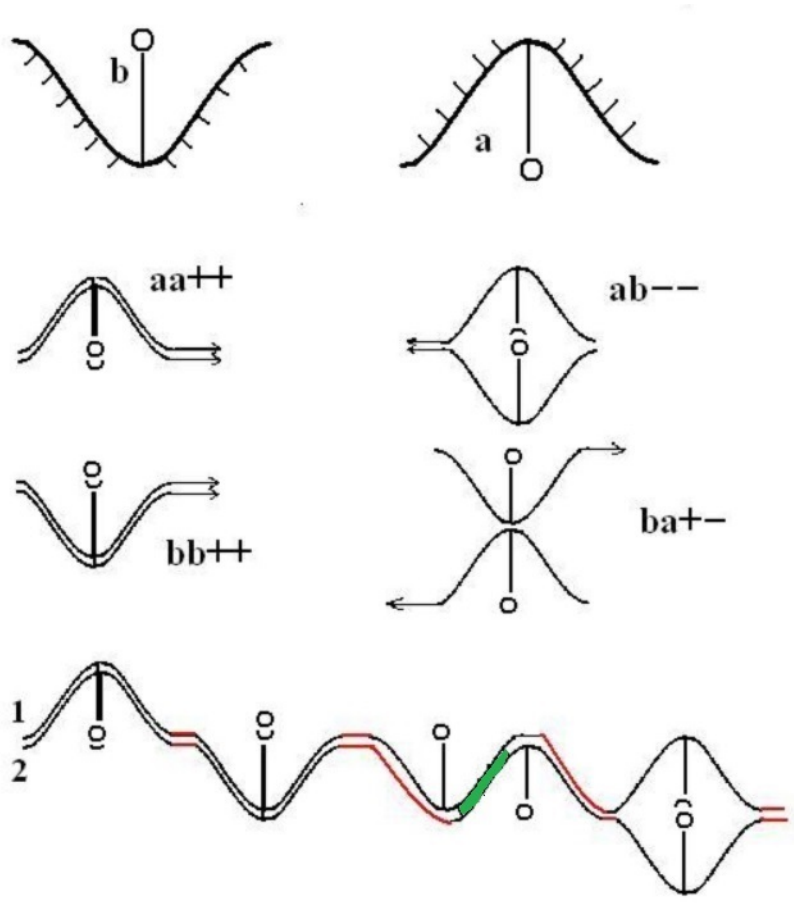



Рис. 63: Наложение двух полимеров. Стрелки обозначают направление растяжения связей (красный цвет) между соседними моноблоками при синтезе полимера. Наложения вида $aa{+}{+}(-{-}), ab{+}{+}(-{-}), bb{+}{+}(-{-}), ba{+}{-}(-{+})$ дают склейку, остальные склейки не дают. Внизу все пары дают склейки.

в данный момент.

Работающий на принципах классической физики центральный процессор может, таким образом, управлять сборкой только выбирая знак сдвига + или − в обеих точках сборки. CPU выбирает эти знаки одновременно, так что никакое ожидание прохождения сигнала между точками сборки не может замедлить процесс: информация о знаке появляется в обеих точках одновременно, и как раз в момент, когда она нужна. Если бы мы допустили задержку по времени, можно было бы сделать сборку вообще идеальной, избежав критических пар совсем.

Для классического типа корреляции между выбором знаков мы имеем неравенство Белла. Для каждого шага процесса мы введем индекс критичности $Cr = +1$, если наложение соответствующих моноблоков некритично (есть склейка), и $Cr = -1$ в противном случае. Нас интересует результирующее число некритических наложений по всей длине цепочек синтезированных полимеров: $NonCr$; наша цель - сделать это число максимальным.

Для одной пары моноблоков мы имеем $NonCr = \frac{1}{2}(1 + Cr)$. Так как все комбинации $aa, ab, ba, bb$ для обеих точек синтеза имеют одинаковые вероятности $1/4$, для среднего значения $E(Cr)$ индекса критичности мы имеем

$$E(Cr) = \frac{1}{4}(a_1b_2 + b_1b_2 + a_1a_2 - b_1a_2), \tag{129}$$

где буква $a$ или $b$ с индексом обозначает случайную величину, соответствующую выбору типа моноблока со знаком $\pm 1$, зависящим от знака сдвига, выбранного для нее.

Для классического управления ввиду неравенства Белла для $E(Cr)$ вида (129) среднее число критических наложений удовлетворяет неравенству

$$E(NonCr) \leq \frac{1}{2}(1 + \frac{2}{4}) = \frac{3}{4} = 0.75.$$

В случае квантового бифотонного управления ситуация будет иной. Здесь мы не можем рассматривать $a_1$ и $b_1$ как случайные величины, определенные на отдельных множествах элементарных исходов для $a_2,\ b_2$, то есть оценка (128) не будет следовать из очевидного выражения $a(X + Y) + b(X - Y) \leq 2$ для чисел $a, b, X, Y = \pm 1$; мы здесь должны писать $a_1b_2 + b_1b_2' + a_1'a_2 - b_1'a_2'$ вместо левой части неравенства (128), что сделает данное неравенство неверным.

Для бифотонного управления наши случайные величины определены на одном и том же множестве элементарных исходов, мы не имеем неравенства Белла и должны считать вероятности напрямую, используя правило Борна.

Пусть для каждой из точек сборки у нас имеется фотодетектор, который может быть мгновенно ориентирован в соответствии с наблюдаемыми, которые мы ассоциируем с $a$ и $b$. Для первой и второй точек сборки эти наблюдаемые пусть имеют вид:

$$\begin{array}{ll} a_1 = \sigma_x, & b_1 = \sigma_z, \\ a_2 = \frac{1}{\sqrt{2}}(\sigma_x - \sigma_z), & b_2 = \frac{1}{\sqrt{2}}(\sigma_x + \sigma_z) \end{array} \tag{130}$$

соответственно. Здесь мы не рассматриваем интересный вопрос о практической реализации таких наблюдаемых.

Условимся, что тип текущего моноблока определяет положение детектора для обеих точек и знак сдвига моноблока есть значение соответствующей наблюдаемой. Так как все комбинации типов моноблоков $aa, ab, ba, bb$ равновероятны, мы можем использовать формулу (129) для среднего значения индекса критичности.

Теперь имеем: $E = E(a_1b_2+b_1b_2+a_1a_2-b_1a_2) = E(a_1b_2)+E(b_1b_2)+E(a_1a_2)-E(b_1a_2)$. Используя определение наблюдаемых (130) и применяя правило вычисления средних $\langle A\rangle_\psi = tr(A\rho_\psi)$ для всех наблюдаемых $A$, взятых из (130), мы найдем $E = 2\sqrt{2}$ и для среднего значения числа некритических наложений (склеек) мы получим значение $E(NonCr) = \frac{1}{2}(1+\frac{2\sqrt{2}}{4}) \approx 0.85$. Итак, использование EPR пар фотонов в управлении сборкой дает существенный выигрыш в качестве - немного более 1.138 для такой формулировки задачи.

# 18 Благодарности

Работа над курсом выполнена в Московском центре фундаментальной и прикладной математики.

Автор признателен проф. Надежде Викторовой и проф. Хай Вонгу за ценные замечания.

# Список литературы


[1] Richard P. Feynman, Simulating Physics with Computers, International Journal of Theoretical Physics, VoL 21, Nos. 6/7, 1982, pp. 467-488.

[2] D.Deutsch, (1985), "Quantum theory, the Church-Turing principle and the universal quantum computer"(PDF). Proceedings of the Royal Society A. 400 (1818): 97–117.

[3] Ландау Л.Д., Лифшиц Е.М., Квантовая механика, Москва, Физ-мат. литература, 2012 — 224 pp. — ISBN 978-5-9221-0819-5.

[4] A.A.Markov - Jn, About the continuiosly of constructive functions, Uspehi mat. nauk, 1954, 9, N 3 (61), pp. 226-229.

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

[6] Ozhigov Y.I. Quantum computers speed up classical with probability zero, Chaos, Solitons and Fractals, 1999, 10, 1147-1163.

[7] R.Feynman, QED: The strange theory of linght and matter, Princeton University Press, 1985.

[8] R.Feynman, D.Hibbs, Quantum mechanics and path integrals, 1984,

[9] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, H. Weinfurte r, Elementary gates for quantum computation Phys.Rev. A52 (1995) 3457.

[10] A. Kitaev, A. Shen, M.Vialyi, Classical and quantum computations, 1999. 192 pp. ISBN 5-900916-35-9.

[11] L. Fedichkin, M. Yanchenko, K. A. Valiev, Novel coherent quantum bit using spatial quantization levels in semiconductor quantum dot, Quantum Computers and Computing 1, 58 (2000).

[12] 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.

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

[14] 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.

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

[16] V.V.Voevodin, Vl.V.Voevodin, Parallel computations, BXV-Peterburg, 2002, — 608 pp. ISBN 5-94157-160-7.

[17] Limits to Parallel Computation: P-Completeness Theory, R. Greenlaw, H. J. Hoover, W. L. Ruzzo, Oxford University Press, 1995, pp. 336.

[18] Shor P. Algorithms for Quantum Computation: Discrete Logarithms and Factoring // Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on — IEEE, 1994. — P. 124–134. — ISBN 0-8186-6580-7 — doi:10.1109/SFCS.1994.365700

[19] C.Zalka, Simulating quantum systems on a quantum computer, Proceedings of The Royal Society A 454(1969):313-322, January 1998.

[20] S.Wiesner, Simulations of Many-Body Quantum Systems by a Quantum Computer, arXiv:quant-ph/9603028.

[21] Ozhigov Y.I., Quantum computations, $http://sqi.cs.msu.ru/store/storage/g1xr51z_ozhigov.pdf$

[22] Donald E. Knuth, The Art of Computer Programming (TAOCP), ISBN 0-201-89683-4

[23] A.S.Holevo, Some estimats of quantity of information transmitted by quanatum channels, Problemi peredachi informatsii, 1973, vol. 9, N3, pp. 3–11.

[24] A.Messiah, Quantum mechanics, Dover publication, 2017, ISSN 0486409244.

[25] Y.Ozhigov, L.Fedichkin, Quantum computer with fixed interaction is universal, Pis'ma v ZhETF, vol. 11, pp. 328-330.

[26] Ожигов Ю.И., Квантовые вычисления с ансамблями идентичных фермионов и стационарным взаимодействием, в журнале Письма в "Журнал экспериментальной и теоретической физики том 93, № 5, с. 321-322.

[27] Y.I.Ozhigov, Quantum computer, Max Press (Rus), 2020, ISBN 978-5-317-06403-7, 174 pp.

[28] Knill, E., Laflamme, R., Milburn, G. J. (2001). "A scheme for efficient quantum computation with linear optics". Nature. Nature Publishing Group. 409 (6816): 46–52

[29] Gottesman, D., Chuang, I. L. (1999-11-25). "Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations". Nature. 402 (6760): 390–393

[30] Bennett, Charles H.; Brassard, Gilles; Crépeau, Claude; Jozsa, Richard; Peres, Asher; Wootters, William K. (1993-03-29). "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels". Physical Review Letters. 70 (13): 1895–1899.

[31] Popescu, S., Knill-Laflamme-Milburn Quantum Computation with Bosonic Atoms, PRL 99, 130503 (2007).

[32] G. Rempe, H. Walther, and N. Klein. Observation of quantum collapse and revival in a one-atom maser, Phys. Rev. Lett., 1987, Vol. 58, no. 4, p. 353.

[33] C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano, and D. J. Wineland, Demonstration of a Fundamental Quantum Logic Gate, Phys. Rev. Lett. 75, 4714 (1995).

[34] Azuma H., Quantum computation with the Jaynes-Cummings model, Prog. Theor. Phys. 126, 369-385 (2011).

[35] E.T. Jaynes, F.W. Cummings, Comparison of quantum and semiclassical radiation theories with application to the beam maser, Proc. IEEE 51 (1): 89–109, (1963). doi:10.1109/PROC.1963.1664

[36] V. Ladunov, Y. Ozhigov, N. Skovoroda , Computer simulation of quantum effects in Tavis-Cummings model and its applications, SPIE Proceedings, vol. 10224, International Conference on Micro- and Nano-Electronics 2016; 102242X (2017) https://doi.org/10.1117/12.2267190

[37] Richard P. Feynman, Simulating Physics with Computers, International Journal of Theoretical Physics, VoL 21, Nos. 6/7, 1982, pp. 467-488.

[38] H. Breuer and F. Petruccione, The Theory of Open Quantum Systems, Oxford (2002).

[39] Azuma H., Quantum computation with the Jaynes-Cummings model, Prog. Theor. Phys. 126, 369-385 (2011).

[40] Y.Ozhigov, About quantum computer software, Quantum Information and Computation, Vol. 20, No. 7&8 (2020) 570-580.

[41] V. P. Maslov, “Rotation of a Neutron in the Coat of Helium-5 as a Classical Particle for a Relatively Large Value of the Hidden Parameter t meas ”, Math. Notes, 103:1 (2018), 67–74.

[42] Flavio Del Santo, Nicolas Gisin , Reply to a "Comment on ’Physics without determinism: Alternative interpretations of classical physics’ Phys. Rev. A 102, 036202 (2020)

[43] Flavio Del Santo and Nicolas Gisin, Physics without determinism: Alternative interpretations of classical physics, Phys. Rev. A 100, 062107, 2019, DOI:https://doi.org/10.1103/PhysRevA.100.062107

[44] Arthur Jabs, A conjecture concerning determinism, reduction, and measurement in quantum mechanics, Quantum Studies: Mathematics and Foundtions, Vol.3 (4) 279-292, 2016.

[45] J. Bell, "On the Einstein Podolsky Rosen Paradox"; Physics, (1964), 1 (3): 195–200.

[46] J. Bell, "On the problem of hidden variables in quantum mechanics"; Reeview of Modern Physics, (1966), 38, N3, стр. 447-452.

[47] Aspect, Alain; Dalibard, Jean; Roger, Gérard (December 1982). "Experimental Test of Bell’s Inequalities Using Time- Varying Analyzers". Physical Review Letters. 49 (25): 1804–1807.

[48] Jian-Wei Pan; D. Bouwmeester; M. Daniell; H. Weinfurter; A. Zeilinger (2000). "Experimental test of quantum nonlocality in three-photon GHZ entanglement". Nature. 403 (6769): 515–519.

[49] Aspect, Alain; Dalibard, Jean; Roger, Gérard, (1982), Experimental Test of Bell's Inequalities Using Time- Varying Analyzers. Physical Review Letters. 49 (25): 1804–1807. Bibcode:1982PhRvL..49.1804A. doi:10.1103/PhysRevLett.49.1804.

[50] Daniel M. Greenberger, Michael A. Horne, Anton Zeilinger, Going Beyond Bell's Theorem, in: 'Bell's Theorem, Quantum Theory, and Conceptions of the Universe', M. Kafatos (Ed.), Kluwer, Dordrecht, 69-72 (1989).

[51] AIP Conference Proceedings, vol. 962, Quantum Theory: Reconsideration of foundations -4, ed. Guillaume Adenier, Andrei Yu. Khrennikov, Pekka Lahti, Vladimir I. Man'ko and Theo M. Nieuwenhuizen, (2007), ISBN: 978-0-7354-0479-3.

[52] F.Ablayev, C.Moore, C.Pollett, Quantum and Stochastic Branching Programs of Bounded Width, International Colloquium on Automata, Languages, and Programming , ICALP 2002: Automata, Languages and Programming pp 343-354.

[53] Dovesi, R., Civalleri, B., Roetti, C., Saunders, V. R. and Orlando, R. (2005) Ab Initio Quantum Simulation in Solid State Chemistry, in Reviews in Computational Chemistry, Volume 21 (eds K. B. Lipkowitz, R. Larter and T. R. Cundari), John Wiley & Sons, Inc., Hoboken, NJ, USA. doi: 10.1002/0471720895.ch1

[54] Y.I.Ozhigov, Distributed synthesis of chains with one-way biphotonic control, Quantum Information and Computation, vol. 18, 7-8, pp. 0592-0598.