Квантовая информация

О.Г. Смолянов, С.А. Шкарин

Механико-математический факультет

Московского государственного университета им. М.В. Ломоносова

В статье, носящей в основном обзорный характер, рассматриваются различные способы описания состояний открытых квантовых систем и их эволюции, а также связанных с ними процессов измерения. Специальное внимание уделяется квантовым системам, пространства состояний которых конечномерны; в частности, рассматривается алгоритм Шора факторизации больших натуральных чисел, описываемый с помощью унитарных операторов в конечномерных гильбертовых пространствах и некоторых операторов проектирования (соответствующих процессам измерения).

Квантовый компьютер можно идентифицировать с парой, первый элемент которой — это унитарный оператор в конечномерном комплексном гильбертовом пространстве, а второй элемент — это оператор проектирования, описывающий процесс измерения, причем благодаря неустранимому взаимодействию с окружением, квантовый компьютер является открытой квантовой системой. Таким образом, задачи, которым посвящена статья, тесно связаны с квантовыми компьютерами. Отсутствие в заглавии последнего термина объясняется тем, что квантовые компьютеры все еще являются математическими объектами, а не реально действующими устройствами; таким образом, в настоящее время правильнее говорить о квантовой информации и ее преобразованиях, а не о квантовых компьютерах (напрашивающийся термин "квантовая кибернетика" должен иметь — при его естественном понимании — более широкое значение).

Как известно, на протяжении последних 40 лет быстродействие компьютеров удваивается, а минимальные размеры деталей процессора уменьшаются вдвое каждые два–три года (соответствующие графики приведены в книге [1]).

Если бы этот закон действовал еще 15–20 лет, то минимальные размеры деталей процессора достигли бы атомных, а быстродействие соответствовало бы длине волны того же порядка.

Конечно, сказанное означает, что экспоненциальное улучшение параметров компьютера в близком будущем прекратится (как прекратились недавно некоторые экспоненциальные процессы, связанные с развитием общества, например, экспоненциальный рост ежегодного числа публикаций в научных журналах (а также и числа самих журналов), экспоненциальный рост числа научных работников, экспоненциальный рост числа профессиональных водителей и т.д.).

В то же время сказанное показывает, что очень скоро при разработке компьютеров окажется необходимым учитывать квантовые эффекты.

Это касается не только самих компьютеров, т.е. устройств, перерабатывающих информацию, но и устройств, ее передающих. При этом вполне естественно предположение, что квантовые эффекты могут не только создавать помехи и определять ограничения для существующих типов компьютеров (которые сейчас принято называть классическими), но и играть конструктивную роль. Именно такова роль этих эффектов в квантовых компьютерах.

В самых общих чертах идея квантового компьютера — восходящая к Фейнману — состоит в замене вероятностей, описывающих работу вероятностного классического компьютера, квантовыми амплитудами вероятностей.

Принципиальным обстоятельством, коренным образом отличающим работу квантового компьютера от вероятностного классического (аналогом которого служит квантовый компьютер), является то, что преобразования, соответствующие различным амплитудам, осуществляются не последовательно во времени, как в классическом вероятностном компьютере, а параллельно (одновременно); именно в этом и состоит то, что сейчас обычно называется квантовым параллелизмом.

То же различие можно описать еще и так. Информация в квантовом компьютере представляется векторами некоторого конечномерного гильбертова пространства E , а вычисления осуществляются с помощью унитарных преобразований этого пространства. Разумеется, эти унитарные преобразования могут быть выполнены и на классических компьютерах; однако в квантовом компьютере унитарное преобразование может рассматриваться как один такт (элементарная операция), тогда как классический компьютер для вычисления образа вектора относительно унитарного линейного оператора, задаваемого как (мнимая) экспонента от (самомопряженного) оператора — гамильтониана $\hat{\mathcal{H}}$ — потребует (даже если заданным считается унитарный оператор) более n^2 ($n = \dim E$) шагов. Именно в этом и состоит объяснение возможного увеличения быстродействия квантового компьютера по сравнению с классическим.

Отметим попутно, что из сказанного вытекает также, что программирование квантового компьютера может рассматриваться или как представление произвольного унитарного оператора в конечномерном комплексном пространстве в виде произведения (унитарных) операторов, принадлежащих к некоторому ограниченному списку таких операторов, или как аналогичное представление самосопряженного оператора в виде суммы самосопряженных операторов специального вида.

В работе четыре раздела. В первом мы напоминаем стандартную аксиоматику квантовой механики (восходящую к фон Нейману) и делаем несколько замечаний о проблеме скрытых параметров. Кроме того, этот раздел содержит краткое описание двух известных квантовых эффектов, связанных с передачей информации. Во втором разделе рассматриваются различные способы описания смешанных состояний квантовых систем; некоторым новшеством здесь является описание смешанных состояний с помощью гауссовских мер на гильбертовом пространстве чистых состояний. В следующем, третьем разделе дается обзор различных способов описания марковской аппроксимации эволюции открытых квантовых систем. В четвертом разделе рассматривается алгоритм Шора.

1. Постулаты квантовой механики. Они делятся на две группы — постулаты, описывающие квантовомеханическую эволюцию, и постулат, описывающий процесс измерения. Существуют различные способы сведения последнего к первым, но ни один из них не является пока общепринятым, и мы не будем их обсуждать.

Известно много эквивалентных наборов постулатов квантовой механики. Мы сформулируем их следующим образом.

Постулат 1. Пространство (чистых) состояний квантовой системы — это сепарабельное гильбертово пространство E (конечномерное или бесконечномерное). Ненулевые векторы этого пространства мы будем называть (чистыми) состояниями; два чистых состояния h_1 , h_2 считаются физически неразличимыми (т.е. представляют одно и то же физическое состояние), если они пропорциональны. Т.о., мы различаем (чистые) состояния как элементы E и соответствующие им физические состояния; фактически множество физических состояний совпадает с комплексным проективным пространст-

вом, размерность которого на единицу меньше размерности E .

Во многих случаях (чистые) состояния отождествляются с нормированными векторами пространства E . Однако в этом случае их оказывается все равно больше, чем физических состояний; кроме того, именно структура векторного пространства E существенно используется в уравнениях квантовой механики; она же выражает принцип суперпозиции, а также используется при конструировании новых пространств исходя из заданных (см. ниже постулат 3). Наконец, целесообразный выбор нормировки вектора иногда позволяет получить более простое уравнение для эволюции. Рандомизированное чистое состояние называется смешанным состоянием; т.о., смешанное состояние отождествляется с вероятностной мерой на E (определяемой неоднозначно — см. ниже).

Постулат 2. Эволюция чистого состояния описывается уравнением Шредингера

$$i\frac{\partial\psi}{\partial t} = \hat{\mathcal{H}}\psi(t)\,,$$

где $\hat{\mathcal{H}}$ — самосопряженный оператор в E, называемый гамильтонианом.

Постулат 3. Если E_1 и E_2 — гильбертовы пространства состояний двух квантовых систем, то предполагается, что пространством состояний составленной из них системы является их гильбертово тензорное произведение $E_1 \otimes E_2$.

Постулат 4. Каждой принимающей числовые значения физической величине, относящейся к квантовой системе с гильбертовым пространством состояний E, соответствует самосопряженный оператор A в E , называемый наблюдаемой; при этом связь с экспериментальным измерением этой физической величины состоит в следующем: если система находится в (чистом) состоянии $\varphi \in E$, причем E реализовано как пространство $\mathcal{L}_2 = \mathcal{L}_2(\mathbb{R}^1, \nu, E_0)$ функций на $\mathbb{R}^1$, принимающих значения в некотором гильбертовом пространстве E_0 , квадратично суммируемых относительно ν , а оператор A реализован как оператор умножения на аргумент, то функция $\frac{1}{\|\varphi\|_{\mathcal{L}_2}}\|\varphi\|^2_{E_0}$ представляет собой плотность вероятностной меры $P_{\varphi,A}$ (на $\mathbb{R}^1$) относительно ν , описывающей результаты измерений рассматриваемой физической величины. При этом предполагается, что, если $\nu(\{x\}) > 0$ для некоторого $x \in \mathbb{R}^1$, то измерение можно выполнить так, что сразу после измерения состояние системы — в той же реализации — будет описываться функцией $\psi \in \mathcal{L}_2(R^1, \nu, E_0)$ $(= E)$, определяемой так: $\psi(z) = 0$, если $z \neq x$ и $\psi(x) = \varphi(x)$ (авторы книги [3] не согласны с тем, что такое измерение — хотя бы в принципе — всегда существует, см. обсуждение в конце параграфа 7 этой книги).

Отсюда следует, в частности, что математическое ожидание эначения этой физической величины равно числу $(A\varphi, \varphi)$ (соответствующие равенства для смешанных состояний приводятся в п. **2**).

Покажем теперь, что всякое состояние заданной квантовой системы можно описать с помощью подходящей вероятностной меры (определяемой отнюдь не однозначно) на некотором измеримом пространстве, элементы которого можно называть скрытыми параметрами. Это описание представляет, по-видимому, лишь чисто математический интерес и далее не используется.

Подчеркнем, что как измеримое пространство, так и мера на нем определяются в высшей степени неоднозначно. Мы опишем сейчас одну из возможных конструкций.

Пусть S — множество всех наблюдаемых (= самосопряженных операторов в E), пусть $\Omega = \Omega(E)$ — множество всех вещественных функций на S и $\mathfrak{A}$ — σ-алгебра подмножеств Ω, порожденная функционалами вычисления. Если $\varphi \in E$, $\|\varphi\|_E = 1$, то каждому конечному набору попарно коммутирующих наблюдаемых $A_1, \ldots, A_n$ соответствует (вероятностная) мера $\eta(\varphi, A_1, \ldots, A_n)$ на $\mathbb{R}^n$, определяемая совместным распределением их значений. Пусть теперь P_φ — какая-либо вероятностная мера на

Ω, такая, что для всякого набора $A_1, \ldots, A_n$ попарно коммутирующих наблюдаемых $P_\varphi\{\omega \in \Omega : \omega(A_j) \in (\alpha_j, \beta_j)\} = \eta(\varphi, A_1, \ldots, A_n)(\prod_{j=1}^{n}(\alpha_j, \beta_j))$.

Ясно, что такая мера существует; при этом, поскольку последнее равенство означает, что совместное вероятностное распределение случайных величин $\omega(A_1), \ldots \omega(A_n)$ совпадает с совместным вероятностным распределением измеряемых значений (попарно коммутирующих) наблюдаемых $A_1, \ldots, A_n$ (в состоянии φ), элементы ω пространства Ω можно считать скрытыми параметрами. Смешанные состояния описываются аналогично. Модель, описывающая ситуацию, когда допускаются измерения лишь части наблюдаемых, строится аналогичным образом; фактически она получается из только что описанной модели с помощью операции естественного проектирования.

Конечно, после каждого измерения значения скрытых параметров могут измениться, что соответствует невозможности одновременного измерения некоммутирующих наблюдаемых.

Приведем теперь пример (принадлежащий Дж.Беллу) ситуации когда значения скрытых параметров действительно должны изменяться.

Пусть $E = \mathbb{C}^2$ и пусть P — мера на $\Omega(E)$, соответствующая некоторому (вообще говоря, смешанному) состоянию. Пусть еще, для каждого $\varphi \in E$, π_φ — оператор проектирования на φ, $\Pi = \{\pi_\varphi : \varphi \in E\}$, Ω_Π — множество всех вещественных функций на Π, $\Omega \to \Omega_\Pi$ — естественная проекция и P_Π — образ P относительно этой проекции. Тогда мера P_Π сосредоточена на множестве всех функций на Π, принимающих значения 0 и 1.

При этом, если $\varphi_1, \varphi_2, \varphi_3 \in E$, то

$$P_\Pi\{\omega \in \Omega_\Pi : \omega(\pi_{\varphi_2}) = 1, \omega(\pi_{\varphi_3}) = 0\} \leqslant P_\Pi\{\omega \in \Omega : \omega(\pi_{\varphi_1}) = 1, \omega(\pi_{\varphi_2}) = 1\} + \\ + P_\Pi\{\omega(\pi_{\varphi_1}) = 0, \omega(\pi_{\varphi_3}) = 0\}. \quad (1)$$

Это следует из равенства

$$P_\Pi\{\omega \in \Omega_\Pi : \omega(\pi_{\varphi_2}) = 1, \omega(\pi_{\varphi_3}) = 0\} = \\ = P_\Pi\{\omega \in \Omega_\Pi : \omega(\pi_{\varphi_1}) = 1, \omega(\pi_{\varphi_2}) = 1, \omega(\pi_{\varphi_3}) = 0\} + \\ + P_\Pi\{\omega \in \Omega_\Pi : \omega(\pi_{\varphi_1}) = 0, \omega(\pi_{\varphi_2}) = 1, \omega(\pi_{\varphi_3}) = 0\};$$

так как его правая часть мажорируется правой частью предыдущего равенства.

Пусть φ_1, φ_2, φ_3 — векторы в двумерном вещественном подпространстве пространства E, причем угол между векторами φ_3 и φ_2 , отсчитываемый в направлении против часовой стрелки, равен α, а угол между φ_1 и φ_2 (в том же направлении) равен β .

Тогда, согласно стандартной формуле для условных вероятностей и правилам квантовой механики,

$$P_\Pi\{\omega(\pi_{\varphi_2}) = 1, \omega(\pi_{\varphi_3}) = 0\} = P_\Pi\{\omega(\pi_{\varphi_2}) = 1\} \cdot \sin^2\alpha, \quad (2)$$

$$P_\Pi\{\omega(\pi_{\varphi_1}) = 1, \omega(\pi_{\varphi_2}) = 1\} = P_\Pi\{\omega(\pi_{\varphi_1}) = 1\} \cdot \cos^2\beta, \quad (3)$$

$$P_\Pi\{\omega(\pi_{\varphi_1}) = 0, \omega(\pi_{\varphi_3}) = 0\} = P_\Pi\{\omega(\pi_{\varphi_1}) = 0\} \cdot \cos^2(\alpha + \beta). \quad (4)$$

Пусть смешанное состояние системы (до всех наблюдений) таково, что

$$P_\Pi\{\omega(\pi_{\varphi_1}) = 0\} = P_\Pi\{\omega(\pi_{\varphi_2}) = 1\} \quad (= \frac{1}{2}).$$

Тогда из (1) следует неравенство Белла $\sin^2\alpha \leqslant \cos^2\beta + \cos^2(\alpha+\beta)$, которое не выполняется для $\alpha = \beta = \frac{3}{8}\pi$.

Это означает, что формула для условной вероятности здесь неприменима, что, в свою очередь, означает, что после измерения состояние системы должно измениться. Т.о., после измерения наблюдаемой π_{φ_2} "скрытый параметр" — т.е. элемент ω — должен измениться.

Заметим теперь, что, используя две связанные копии исследуемой квантовой системы, можно реализовать рассматриваемое смешанное состояние как некоторое чистое состояние сложной системы, состоящей из этих двух копий. Действительно, гильбертово пространство состояний этой сложной системы — это $E_1 \otimes E_2$; если (e_1^1, e_2^1) и (e_1^2, e_2^2) — это ортонормированный базис, соответственно, в E_1 и E_2 , то вектор $e_1^1 \otimes e_2^1 + e_1^2 \otimes e_2^2 \in E_1 \otimes E_2$ и описывает рассматриваемое выше смешанное состояние (аналогичное утверждение справедливо и для произвольных смешанных состояний произвольных квантовых систем — см. ниже).

Это означает, что наблюдаемые π_φ , относящиеся к одной копии, могут быть измерены с помощью экспериментов над второй копией независимо от расстояния в (физическом) пространстве между ними.

В свою очередь, это значит, что возмущения "скрытых параметров" должны передаваться с бесконечной скоростью. Конечно, это может означать, что скрытые параметры — это чисто математические объекты, которым не соответствует физическая реальность (именно в этом и состоит точка зрения, считающаяся стандартной).

Изменение состояния одной из двух связанных квантовых систем при воздействии на другую позволяет осуществить (называемую телепортацией) передачу на расстояние вектора (чистого) состояния третьей квантовой системы; при этом предполагается, что в точке приема уже имеется точная копия той системы, состояние которой передается, так что передается только элемент комплексного проективного гильбертова пространства; кроме того, после передачи состояние той системы, которое до передачи описывалось этим элементом, меняется (непредсказуемым образом); наконец, как в точке передачи, так и в точке приема передаваемое состояние остается неизвестным, так как всякое получение информации о квантовом состоянии его разрушает (кстати, именно поэтому долгое время считалось, что передача квантового состояния невозможна). Описание процесса телепортации состояния двумерной квантовой системы (это состояние называется кубитом) заключается в следующем. Пусть E_j $(j = 1, 2, 3)$ — три двумерных комплексных гильбертовых пространства. Считается, что E_1 и E_2 — пространства состояний удаленных друг от друга квантовых систем и E_3 — пространство состояний третьей квантовой системы, находящейся там же, где первая. Мы не будем для краткости различать чистые состояния и описывающие их векторы, а также квантовые системы и их пространства состояний. Задача состоит в передаче $a \in E_3$. Пусть $E = E_1 \otimes E_2 \otimes E_3$, $g \in E_1 \otimes E_2$, $g = h_1 \otimes k_1 + h_2 \otimes k_1$, $((h_j), (k_j)$ — ортонормированные базисы, соответственно, в E_1 и в E_2). Совокупность системы E_1 и E_2 вместе с вектором g может рассматриваться как передающее устройство. Мы считаем, что до передачи системы $E_1 \otimes E_2$ не взаимодействовали, так что начальный вектор их общего состояния — это $g \otimes a$. Пусть $a = \alpha e_1 + \beta e_2$ $(e_1,\ e_2$ — ортонормированный базис в $E_3)$. Непосредственно проверяется (с помощью элементарных алгебраических преобразований), что $a = B_1(\alpha k_1 + \beta k_2) + B_2(-\alpha k_1 + \beta k_2) + B_3(\alpha k_2 - \beta k_1) + B_1(-\alpha k_2 - \beta k_1) = \sum\limits_{j=1}^{4} B_j a_j$, причем B_j — векторы некоторого ортонормированного базиса в $E_3 \otimes E_1$. После измерения в точке передачи наблюдаемой $\sum\limits_{j=1}^{4} j \cdot B_j \otimes B_j$ (смешанное) состояние системы $E_3 \otimes E_1$

перейдет в чистое, описываемое одним из векторов B_j ; после передачи (по обычному "классическому" каналу связи) информации о величине измеренного j в точке приема станет известно, что состояние системы E_2 описывается вектором a_j . Чтобы восстановить вектор a_1 (совпадающий с передаваемым), достаточно применить подходящее унитарное преобразование (в пространстве E_2), т.е. — физически — надлежащим образом повернуть приборы, окружающие систему E_2 . Опишем еще процесс, называемый квантовым сжатием информации. Можно показать, что, в силу свойств квантовых систем, максимальное количество информации, которое можно получить при измерении, проводимом над системой с двумерным пространством состояний, равно $\ln 2$ (некоторые результаты в этом направлении, восходящие к А.С.Холево, можно найти в [2]). Тем не менее, оказывается, что с помощью перемещения в пространстве физического экземпляра такой системы можно передать вдвое больше информации. В качестве "передатчика" здесь используется та же самая система, что и раньше. Т.о., ее пространство состояний — $E_1 \otimes E_2$. Пусть теперь $a_{11} = h_1 \otimes k_1 + h_2 \otimes k_2$, $a_{12} = h_1 \otimes k_1 - h_2 \otimes k_2$, $a_{21} = h_1 \otimes k_2 + h_2 \otimes k_1$, $a_{22} = h_1 \otimes k_2 - h_2 \otimes k_1$, (векторы a_{ij} называются иногда векторами Белла; они образуют ортонормированный базис в $E_1 \otimes E_2$). Для определенности примем, что начальное состояние снова описывается вектором $a_{11}(= g)$. Процесс передачи сообщения использует наблюдение, состоящее в том, что с помощью унитарных преобразований в E_2 можно перевести вектор a_{11} в любой из остальных векторов. Т.о., для передачи сообщения, состоящего в выборе одной из четырех возможностей — т.е. одного из четырех векторов a_{ij} — достаточно провести подходящее унитарное преобразование в E_2 , затем переместить саму систему E_2 (т.е. электрон или фотон) в то место, где находится система E_1 — и затем провести измерение наблюдаемой $a_{11} \otimes a_{11} + 2a_{12} \otimes a_{12} + 3a_{21} \otimes a_{21} + 4a_{22} \otimes a_{22}$. Тем самым будет передана информация, количество которой равно $\ln 4$. Отметим, что только что описанный процесс может рассматриваться как отчасти двойственный телепортации: в последнем случае передается информация об измерении в одном месте и восстанавливается квантовое состояние в другом; в первом случае перемещается сам объект в нужном квантовом состоянии и затем производится измерение. Общая теорема о сжатии квантовой информации принадлежит Б. Шумахеру; ее можно найти в [2].

2. Смешанные состояния. Согласно приведенному в п. 1 определению, смешанное состояние — это рандомизированное чистое состояние. Т.о., мы будем сопоставлять смешанным состояниям (борелевские) вероятностные меры на гильбертовом пространстве E чистых состояний. Подчеркнем, что эти меры не имеют ничего общего с мерами на пространстве "скрытых параметров", о которых говорилось в предыдущем пункте.

При этом, если ν — вероятностная мера на E, то среднее значение A_ν наблюдаемой A в задаваемом мерой ν состоянии определяется равенством

$$\bar{A}_\nu = \int \frac{(Ax, x)}{(x, x)} \nu(dx). \tag{5}$$

Если ν — центрированная гауссовская мера, то $\bar{A}_\nu = \frac{1}{\mathrm{tr}\, T_\nu} \mathrm{tr}\, T_\nu A$, где T_ν — корреляционный оператор меры ν , определяемый равенством $T_\nu = \int x \otimes x \nu(dx)$, а интеграл справа — это интеграл Бохнера. В частности, если ν — гауссовская мера и $\mathrm{tr}\, T_\nu = 1$, то $\bar{A}_\nu = \int (Ax, x)\nu(dx) = \mathrm{tr}\,(T_\nu A)$. Таким образом, корреляционный оператор T_ν можно отождествить с оператором плотности фон Неймана. Но, согласно принципам квантовой механики, два смешанных состояния, которым соответствуют одинаковые операторы плотности, физически неразличимы. Таким образом, среди мер ν на E, описывающих одно и то же (физическое) состояние квантовой системы, существует ровно одна гауссовская мера ν, корреляционный оператор T_ν которой обладает единичным следом; этот оператор является оператором плотности, описывающим то же самое физическое

состояние.

То же самое (смешанное) состояние может быть описано с помощью подходящего *чистого* состояния некоторой расширенной квантовой системы. Именно, пусть E_1 — (комплексное сепарабельное) гильбертово пространство и $K = E \otimes E_1$ (гильбертово тензорное произведение), причем $\dim E_1 = \dim E$. Пусть (h_j) — ортонормированный базис в E и (k_j) — ортонормированный базис в E_1 . Пусть, наконец, $T = \sum t_j k_j \otimes k_j$; это означает, что, для каждого $x \in E$, $Tx = \sum t_j (k_j, x) k_j$; мы предполагаем, что $\mathrm{tr}\, T = 1$.

Определим вектор $z \in E \otimes E_1$ равенством $z = \sum \sqrt{t_j} h_j \otimes k_j$. Тогда оператор плотности смешанного состояния исходной квантовой системы (с гильбертовым пространством состояний E) — это $\mathrm{tr}_{E_1}(z \otimes z)$, где, для каждого оператора B в $E \otimes E_1$ оператор $\mathrm{tr}_{E_1} B$ (частичный след B) определяется равенством $((\mathrm{tr}_{E_1} B)x, v)_E = \sum\limits_j (Bx \otimes h_j, v \otimes k_j)_K$. Непосредственно проверяется, что $\mathrm{tr}_{E_1} z \otimes z = T$. Это означает, что если A — наблюдаемая в E, то значение всякой наблюдаемой $A \otimes \mathrm{Id}$ в K (Id — единичный оператор в E_1) в чистом состоянии z совпадает со средним значением наблюдаемой A в смешанном состоянии T. Действительно, $((A \otimes \mathrm{Id})z, z)_K = \mathrm{tr}(AT)$. Таким образом, никакие измерения, производимые только над системой с гильбертовым пространством состояний E, не могут различить смешанное состояние этой системы, определяемое центрированной гауссовской мерой ν_T с корреляционным оператором T, и чистое состояние z расширенной системы с пространством состояний $K = E \otimes E_1$. Иначе говоря, вектор $z \in K$ и гауссова мера ν_T определяют одно и то же смешанное состояние квантовой системы с гильбертовым пространством E (чистых) состояний.

3. Стохастическое уравнение Шредингера. В этом разделе кратко рассмотрен один из возможных подходов к описанию эволюции состояний открытых квантовых систем, т.е., иначе говоря, частей некоторых "больших" систем. Конечно, точное описание такой эволюции может быть получено путем решения уравнения Шредингера для "большой" квантовой системы и последующего применения операции взятия частичного следа. Однако в силу сложности этой задачи полезной оказывается так называемая "марковская аппроксимация". В настоящее время известно два способа получения такой аппроксимации. Один из них может быть определен в рамках квантовой теории случайных процессов; в рамках этой теории, исходя из уравнений Гейзенберга для "большой" квантовой системы и используя принадлежащий Ван Хову метод перехода к "пределу слабого взаимодействия" [9] между квантовой (под)системой и ее окружением, можно получить так называемые квантовые стохастические дифференциальные уравнения, описывающие поведение этой подсистемы. Применение к решению этого последнего уравнения некоторого процесса усреднения позволяет, в свою очередь, получить уравнение Линдблада, описывающее "квантовую динамическую полугруппу" (стоит впрочем отметить, что впервые это уравнение было получено совершенно иным путем, исходя из аксиоматического описания этой полугруппы). Второй способ состоит в использовании стохастических уравнений Шредингера (-Белавкина). Они описывают предельное поведение системы, подвергаемой в дискретные равноотстоящие моменты времени "неточным наблюдениям", при условии, что точность наблюдений и интервалы времени между ними стремятся к нулю [4,5,6,8]; т.о., это уравнение можно интерпретировать как описывающее эволюцию системы, находящейся под непрерывным наблюдением. В частности, уравнение такого типа, описывающее движение одномерной частицы в процессе непрерывного измерения ее координаты, имеет вид

$$d\varphi = (-i\hat{\mathcal{H}} - \frac{\lambda}{4} q^2 + \lambda q \bar{q})\varphi dt + \sqrt{\lambda/2} q \varphi dw; \qquad (6)$$

здесь φ — случайная функция вещественного аргумента, принимающая значения в

гильбертовом пространстве $E = \mathcal{L}_2(\mathbb{R}^1)$, $\hat{\mathcal{H}}$ — квантово-механический гамильтониан системы, находящейся под наблюденим, $\lambda > 0$ — параметр, характеризующий точность измерения, $\bar{q}$ — квантово-механическое среднее координаты q и w — стандартный винеровский процесс. Отметим, что при выводе этого уравнения существенно используется возможность целесообразной нормировки элемента гильбертова пространства. Отметим также, что вывод уравнения (6) основывается на описанном в предыдущем пункте представлении смешанного состояния мерой на гильбертовом пространстве. Решением задачи Коши для этого уравнения является негауссовская случайная функция со значениями в E; тем не менее для каждого $t \in [0, \infty)$ существует гауссовская мера $\nu_G(t)$ с нулевым средним на E, обладающая тем же корреляционным функционалом, что и негауссовская мера $\nu(t)$, порожденная случайным элементом $\varphi(t)$ пространства E. Обе эти меры описывают одно и то же смешанное состояние. Следует еще отметить, что из вывода уравнения (6) следует, что сумму $B(t) = \int\limits_0^t \sqrt{2\lambda}\bar{q}(\tau)\,d\tau + w(t)$ можно интерпретировать как результат измерения [4]. Само же уравнение (6) можно переписать в следующем виде:

$$d\varphi = (-i\hat{\mathcal{H}} - \frac{\lambda}{4}q^2)\varphi dt + \sqrt{\lambda/2}q\varphi dB\,,$$

что позволяет, в частности, представить его решение с помощью (рандомизированных) функциональных интегралов.

Подчеркнем еще раз, что эволюция, описываемая уравнениями (6) и последним, не является унитарной (норма гильбертовозначной случайной функции $\varphi(\cdot)$ не сохраняется); конечно, можно написать и уравнение для функции $t \mapsto \|\varphi(t)\|^{-1}\varphi(t)$; это (нелинейное) уравнение описывает унитарную эволюцию. Последнее уравнение порождает обычным образом обратное уравнение Колмогорова, сопряженным к которому является уравение Фоккера–Планка (называемое также прямым уравнением Колмогорова); последнее является уравнением относительно функций вещественного аргумента, принимающих значения в пространстве мер на E.

Если $t \mapsto \nu(t)$ — это решение уравнения Фоккера–Планка и если, для каждого t из его области определения,

$$T_1(t) = \int_E x \otimes x\nu(t)(dx) \qquad \left(\equiv \int (x \otimes x)\nu_G(t)(dx)\right)\,,$$

то функция $T(t) = (\operatorname{tr} T_1(t))^{-1}T_1(t)$ (принимающая значения в пространстве ядерных положительно определенных операторов в E) удовлетворяет следующему уравнению Линдблада:

$$T'(t) = -i[\hat{\mathcal{H}}, T(t)] - \frac{\lambda}{4}[R[R, T(t)]]\,,$$

где R — это оператор координаты в E.

Стохастические уравнения Шредингера и порождаемые ими уравнения Колмогорова (а также и уравнения Линдблада) можно использовать для феноменологического описания процесса редукции вектора состояния при его измерении, а также для описания возникновения декогерентности в квантовых компьютерах. При этом решения уравнений Колмогорова и Линдблада содержат одинаковую информацию; решение стохастического уравнения Шредингера содержит больше информации, так как оно явно зависит от "выходного процесса" $B(\cdot)$.

В заключение отметим, что прямое уравнение Колмогорова (= уравнение Фоккера-Планка) для эволюции меры на E, описывающей состояние системы, можно получить и совершенно иначе. Именно, исследуемую квантовую систему и ее окружение следует рассмотреть как единую "большую" квантовую систему; далее, следует интерпретировать уравнение Шредингера для нее как уравнение Гамильтона для некоторой (бесконечномерной) гамильтоновой системы и в соответствующем ему уравнении Лиувилля (оно является уравнением относительно функций вещественного аргумента, принимающих значения в пространстве мер на гильбертовом пространстве состояний "большой" системы) перейти к пределу "слабой связи".

4. Квантовые вычисления. Полиномиальный алгоритм факторизации чисел. В этом разделе мы коротко излагаем идею квантовых вычислений и понятия сложности решения задачи квантовым алгоритмом. Мы также приводим центральные идеи, лежащие в основе построения квантового полиномиального алгоритма П. Шора [13] факторизации целых чисел.

Состоянием классического компьютера является двоичный вектор x длины n, то есть $x \in \{0,1\}^n = B_n$. Состоянием же квантового компьютера является единичный вектор конечномерного комплексного гильбертова пространства $\mathcal{H}_n = \mathbb{C}^{B_n}$. Если $\{e_x : x \in B_n\}$ — стандартный ортонормированный базис пространства $\mathcal{H}_n$ и $\alpha = \sum_{x \in B_n} \alpha_x e_x \in \mathcal{H}_n$, $|\alpha| = 1$ — состояние квантового компьютера, то число $|\alpha_x|^2$ — это вероятность получить двоичный вектор x при измерении состояния квантового компьютера.

Эволюция состояния квантового компьютера осуществляется унитарным преобразованием пространства $\mathcal{H}_n$. Если $1 \leq i_1 < \cdots < i_k \leq n$ и V — унитарный оператор на $\mathcal{H}_k$, то символом $V_{i_1,\ldots,i_k}$ обозначим унитарный оператор на H_n такой, что

$$(V_{i_1,\ldots,i_k} e_x, e_y) = \begin{cases} (V e_{x_{i_1},\ldots,x_{i_k}}, e_{y_{i_1},\ldots,y_{i_k}}), & \text{если } x_i = y_i \text{ при } i \notin \{i_1,\ldots,i_k\}, \\ 0 & \text{в противном случае.} \end{cases} \qquad (A)$$

Об унитарных операторах на H_n, имеющих вид $V_{i_1,\ldots,i_k}$ для некоторого унитарного оператора V на $\mathcal{H}_k$ говорят, что они зависят только от (квантовых) битов с номерами $i_1,\ldots,i_k$ и преобразуют только эти биты.

Обратимое преобразование $S : B_n \to B_n$ задает унитарное преобразование V^S пространства $\mathcal{H}_n$, действующее по формуле

$$V^S e_x = e_{S(x)}. \qquad (B)$$

Это обстоятельство является отражением того факта, что вычисления на гипотетическом квантовом компьютере включают в себя обратимые классические вычисления. Фиксируем некоторый набор унитарных преобразований, которые будем называть элементарными.

Пусть $S : B_3 \to B_3$ — отображение Тоффоли:

$$(x_1, x_2, x_3) \mapsto S(x_1, x_2, x_3) = (x_1, x_2, x_1 \cdot x_2 + x_3),$$

и V^S унитарное преобразование 8-мерного гильбертова пространства $\mathcal{H}_3$, определяемое по S по формуле (B). Пусть унитарное преобразование R на $\mathcal{H}_1$ задается в стандартном базисе $\{e_0, e_1\}$ матрицей

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

и унитарное преобразование S^k на $\mathcal{H}_2$ $(0 \leq k \leq n)$ задается в стандартном базисе $\{e_{00}, e_{01}, e_{10}, e_{11}\}$ матрицей

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\pi/2^k} \end{pmatrix}.$$

Элементарными преобразованиями мы будем называть преобразования вида R_i $(1 \leq i \leq n)$, S_{ij}^k $(1 \leq i, j \leq n,\ i \neq j)$ и V_{ijk}^S $(1 \leq i, j, k \leq n,\ i \neq j,\ k \neq j,\ k \neq i)$, где операция $V \mapsto V_{i_1,\ldots,i_k}$ определяется формулой (A).

Подобно тому как при классических вычислениях сложность алгоритма определяется количеством элементарных операций, необходимых для его реализации, так и сложность квантового вычисления (=унитарного преобразования V на $\mathcal{H}_n$) — это минимальное m, при котором существуют элементарные преобразования $V_1, \ldots, V_m$ такие, что

$$V = V_1 \cdot \cdots \cdot V_n. \qquad (C)$$

Разумеется приведенный выбор элементарных преобразований не является единственным.

Квантовое вычисление состоит из трех этапов:

1. Подготовка начального сотояния, то есть приведение квантового компьютера в состояние, являющееся данным вектором из $a_0 \in \mathcal{H}_n$.

2. Эволюция квантового компьютера, то есть последовательное применение к начальному состоянию цепочки элементарных преобразований (C).

3. Измерение результата. Этот этап дает нам $x \in B_n$ с вероятностью $|(Va_0, e_x)|^2$.

Класс задач, которые могут быть решены за полиномиальное (от длины входа, то есть от n) число шагов (=время) с помощью классической машины Тьюринга, обычно обозначается символом P, класс задач, которые могут быть решены за полиномиальное время на недетерминированной машине Тьюринга (то есть при фактически неограниченном распараллеливании вычислений) обозначается NP. Класс задач QP, которые могут быть за полиномиальное время решены с помощью квантового компьютера, является промежуточным между двумя первыми классами: $P \subseteq QP \subseteq NP$. Совпадают ли классы P и NP — это знаменитая нерешенная проблема, хотя общественное мнение (среди математиков) склоняется к тому, что эти классы не совпадают. Существуют так называемые NP-полные задачи, то есть задачи, к которым полиномиальным (классическим) алгоритмом может быть сведена любая задача из NP. Найти полиномиальный алгоритм решения NP-полной задачи значит доказать, что $P = QP = NP$.

Что касается задачи факторизации (= разложения на простые множители) целых чисел, то известно, что она принадлежит NP и не является NP-полной. Так что если вдруг появится классический полиномиальный от длины l входного числа m в двоичной записи алгоритм разложения m на простые множители, то это не повлечет катастрофических для теории сложности последствий типа совпадения P и NP. Тем не менее в настоящее время не известно полиномиального классического алгоритма факторизации. Наилучший из известных классических алгоритмов имеет сложность $e^{O((\log l)^{1/3}(\log\log l)^{2/3})}$.

Теперь мы перейдем к описанию идеи полиномиального квантового алгоритма П. Шора факторизации больших целых чисел. В основе этого алгоритма лежит квантовое дискретное преобразование Фурье, то есть унитарное преобразование A_q пространства $\mathcal{H}_n$, задаваемое формулой

$$A_q e_x = \frac{1}{2^{n/2}} \sum_{y \in B_n} e^{2^{1-n}\pi i \tilde{x}\tilde{y}} e_y,$$

где

$$\widetilde{x} = \sum_j x_j 2^{j-1}, \quad \widetilde{y} = \sum_j y_j 2^{j-1}. \tag{D}$$

Возможность вычисления квантового дискретного преобразования Фурье за полиномиальное время вытекает из следующего равенства

$$A_q = R_{l-1} S^1_{l-2,l-1} R_{l-2} S^2_{l-3,l-1} S^1_{l-3,l-2} R_{l-3} \cdot \cdots \cdot R_1 S^{l-1}_{0,l-1} S^{l-2}_{0,l-2} \cdots S^2_{0,2} S^1_{0,1} R_0.$$

Пусть m — составное натуральное число. Как показано в работе [14], задача факторизации m вероятностным полиномиальным алгоритмом сводится задаче нахождения порядка элемента мультипликативной группы кольца $\mathbf{Z}/m\mathbf{Z}$. Пусть $n \in \mathbb{N}$ таково, что

$$m^2 \leq 2^n = q \leq 2m^2.$$

Пусть также $x \in B_n$ и тем самым $0 \leq \widetilde{x} \leq q-1$, где число $\widetilde{x}$ определяется по x согласно формуле (D). Мы ищем порядок r числа $\widetilde{x}$ в мультипликативной группе кольца $\mathbf{Z}/m\mathbf{Z}$, считая, что числа $\widetilde{x}$ и m взаимно просты.

Начальным сотоянием алгоритма Шора служит вектор

$$\frac{1}{2^{n/2}} \sum_{y \in B_n} e_y \otimes e_0 \in \mathcal{H}_n \otimes \mathcal{H}_n = \mathcal{H}_{2n}. \tag{E}$$

Следующий шаг состоит в переводе вектора (E) в вектор

$$\frac{1}{2^{n/2}} \sum_{y \in B_n} e_y \otimes e_{\psi(x,y)}, \text{ где } \widetilde{\psi(x,y)} = \widetilde{x}^{\widetilde{y}} (\mathrm{mod}\ m). \tag{F}$$

Эта операция может быть осуществлена посредством применения полиномиального (от $\log m$) числа матриц вида V^S_{ijk}. Далее мы применяем квантовое дискретное преобразование Фурье к первому регистру (то есть по первой половине переменных), что приводит нас к вектору

$$\frac{1}{q} \sum_{y \in B_n} \sum_{z \in B_n} e^{\frac{2\pi i \widetilde{z}\widetilde{y}}{q}} e_z \otimes e_{\psi(x,y)}.$$

Далее мы производим измерение состояния нашего квантового компьютера и получаем пару (z, y). Рассматриваем дробь $\frac{\widetilde{z}}{q}$ и находим (с помощью непрерывных дробей) ближайшее к ней рациональное число $\frac{d}{t}$ со знаменателем t меньшим m. Можно показать, что t совпадает с искомым периодом r с вероятностью не меньшей чем $\frac{\phi(r)}{r} = O\left(\frac{1}{\log\log r}\right)$ (здесь ϕ — функция Эйлера). То есть для нахождения r с большой вероятностью достаточно повторить описанную процедуру $O(\log\log m)$ раз. Сложность описанного алгоритма является полиномиальной от $\log m$, и он использует квантовые вычисления с $4\log m + O(1)$ квантовыми битами.

ЛИТЕРАТУРА.

1. Williams Colin P., Cleurwater Scott H., Explotions in Quantum Computing, Springer, 1997.

2. Preskill John, Quantum Information and Computation, Lecture Notes for Physics, California Institute of Technology, 1998.

3. Ландау Л. Д., Лифшиц Е. М. Теоретическая физика. Т. III Квантовая механика. Нерелятивистская теория — М.: Наука, 1989.

4. Albeverio S., Kolokol'tsov V.N., Smolyanov O.G. Continuous quantum measurements: local and global approaches.// — Reviews in Mathematical Physics, Vol. 9, № 8 (1997), 907-920.

5. Albeverio S., Kolokol'tsov V.N., Smolyanov O.G.: Representations of the Belavkin quantum measurement equation by the Menski functional formula.// — Comptes Rendus Acad Sci. Paris t.323, ser. 1, 1996, 661–664.

6. Белавкин В.П., Смолянов О.Г. Интеграл Фейнмана по траекториям, соответствующий стохастическому уравнению Шредингера.// ДАН, 1998, Т.360. No.5. С.589–593.

7. Смолянов О. Г., Шавгулидзе Е. Т. Континуальные интегралы. — Москва, Издательство МГУ, 1990.

8. Альбеверио С., Смолянов О.Г. Бесконечномерные стохастические уравнения Шредингера–Белавкина.// Успехи матем. наук, т. 52, вып. 4., 1997.

9. Accardi L., Gough J., Lu Y.G. On the Stochastic Limit of Quantum Field Theory.// Rep. Math. Phys., 36, № 2/3, (1995), 155–187.

10. Lindblad G. On the generators of quantum dynamical semigroups.// Commun. Math. Phys., 1976, V. 48, N 2, 119–130.

11. Холево А.С. Квантовое стохастическое исчисление.// Итоги науки и техники. Современные проблемы математики. т. 36, М., ВИНИТИ, 1990, 1–28.

12. Смолянов О. Г. Бесконечномерные псевдодифференциальные операторы и квантование по Шредингеру.// — Доклады АН СССР, 1982, т.263, N 3, 558–561.

13. Shor P. Factoring with Quantum Computer.// Proc. of the 35th Annual Symp. on Found. of Comp. Science, Santa Fe, Nov. 20–22, 1994, pp. 124–134)

14. G. L. Miller, Riemann's Hypothesis and Tests of Primarity.// J. Comput. System Sci., vol. 13, pp. 300–317, 1994.