Становление базовых представлений квантовой информатики

Д.И. Сергеев

Аннотация. В статье рассмотрены некоторые базовые понятия и представления квантовой информатики. Большое внимание уделено ключевым свойствам квантовых систем – квантовой суперпозиции и квантовой запутанности, позволяющим реализовать преимущество квантовых параллельных вычислений и квантовых сетей. Излагается коммуникационный протокол квантовой телепортации. Обсуждаются некоторые результаты создания квантовых сетей и квантовых компьютеров.

Ключевые слова: квантовые вычисления, кубит, квантовая суперпозиция, квантовая запутанность.

К истории вопроса

Квантовые идеи в той или иной форме известны уже тысячелетия [1], долгую историю имеют и работы по защите сообщений, которые предпринимались ещё в древнейших цивилизациях, пройдя путь от прообразов «Скитала»[1] до «Энигмы»[2] [2], сформировав современную криптологию. Криптоанализ, как знание о дешифровании информации, уже с середины прошлого века не только тесно связан с вычислительными средствами, но является одним из основных стимулов для их создания. Рассмотрим кратко некоторые события позднейшей истории информатики в её квантовом варианте.

В конце 60-х гг. Стивеном Виснером проведены исследования по квантовой криптографии, но работа длительное время не принималась в печать [3, 4].

В 1973 г. Александр Холево сформулировал и доказал теорему о квантовой границе классической информации, показывающую верхнюю границу количества классической информации, которая может быть получена о квантовом состоянии [5].

Одной из первых работ, в которых рассматривались преимущества создания вычислительных устройств на основе квантовых свойств микросистем, была монография Юрия Манина «Вычислимое и невычислимое» (1980 г.) [6].

В исследованиях Пола Бенёва в 1980–1982 гг. [7-9] была предложена теоретическая схема работы квантового компьютера, также показано, что единичная или унитарная квантовая эволюция обладает не меньшей вычислительной мощностью, чем классический компьютер.

В 1981 г. Ричард Фейнман сделал доклад на Первой Конференции по физике вычислений в Массачусетском технологическом институте «Моделирование физики на компьютерах», опубликованный в 1982 г. [10], в котором предложил возможность имитации физических процессов на фундаментальном уровне, используя вычисления присущие квантовой природе материи.

В 1982 г. Вильямом Вуттерсом, Воджичем Зуреком и независимо – Дэннисом Диэксом была доказана теорема о невозможности

[1] «Скитал» – древнейшее криптографическое устройство ленточного типа (около 400 г. до н.э.).

[2] «Энигма» – криптографический прибор, применявшийся с 20-х годов XX века. Использовался Германией во время Второй мировой войны.

клонирования, утверждающая невозможность создания идеальной копии произвольного неизвестного квантового состояния [11, 12].

В 1985 г. выходит статья Ричарда Фейнмана «Квантово-механические компьютеры» [13], в которой исследуются ограничения, накладываемые на компьютеры квантовой механикой.

В важнейшей работе – статье Дэвида Дойча «Квантовая теория, принцип Чёрча – Тьюринга и универсальный квантовый компьютер» (1985 г.) [14] впервые была предложена гибкая схема работы универсального квантового компьютера и доказана его возможность более эффективного решения вычислительных задач в сравнении с классическим компьютером, построенным на архитектуре Алана Тьюринга, а также возможность получения и реализации любой единичной эволюции, имитирующей развитие любой физической системы. Этой работой были заложены основы квантовой теории вычислений.

В статье 1989 г., «Quantum computational networks» [15] Дэвид Дойч дал определение квантовых сетей и квантовых логических элементов – гейтов, позволяющих описывать единичные изменения состояния квантовых систем.

Эти работы совместно раскрыли преимущества возможных вычислений на основе квантовых закономерностей, экспоненциально превышающих эффективность классических вычислений. Такая эффективность оказывается возможной из-за наличия таких квантовых свойств как квантовая суперпозиция состояний и квантовая запутанность.

Но интерес к теме квантовых вычислений значительно усилился лишь в 1994 г., когда Питер Шор создал квантовый алгоритм решения задачи факторизации – алгоритм разложения натурального числа n на простые множители за время, полиномиально зависящее от n [16]. Причина этому – возможность расшифровки распространенных криптографических систем с открытым ключом типа RSA[3]. Понятно, что причина возросшего внимания к теме была не только научной.

Задача факторизации – разложение на простые множители больших натуральных чисел является одной из фундаментальных проблем математики. Лучший алгоритм классической факторизации – алгоритм А. Ленстры и Х. Ленстры с сотрудниками (1993 г.) – общий метод решета числового поля (GNFS[4]) имеет экспоненциальную сложность (число шагов или тактов) ~ $O(\exp(cn^{1/3}(\log n)^{2/3}))$, где c – некоторая постоянная. Квантовый алгоритм Шора имеет полиномиальную сложность ~ $O(n^2 \log n \log\log n)$ [16, 17]. Например, факторизация числа порядка $n \sim 2^{800}$ не решаема на классическом компьютере за разумное время. Использование же квантового алгоритма при тактовой частоте в 1Мгц потребовало бы дня два [18]. Получаемый результат в квантовых алгоритмах вероятностный, но возможность быстрой проверки приближает его к достоверному.

Успех Питера Шора в создании квантового алгоритма поиска простых сомножителей целых чисел и вычисления дискретного алгоритма был дополнен в 1995 г. созданием Ловом Гровером квантового алгоритма «нахождения иголки в стоге сена» – поиска в неупорядоченной базе данных [19]. Если классический способ поиска имеет сложность ~ $O(n)$, то в случае алгоритма Гровера ~ $O(\sqrt{n})$. Преимущество очевидно.

О битах и кубитах

Классической мерой количества информации в двоичной системе счисления принят *бит* (сокр. от *binary digit* – двоичное число) – система, принимающая два альтернативных значения (состояния) – обычно это «0» или «1». Дискретность же может достигаться искусственным разделением аналоговых величин[5].

Подобием классического бита в квантовой информатике является квантовый бит – *кубит* (*q-bit*, *quantum bit*), имеющий также два базисных состояния, в которых он может находится уже одновременно, и кроме этого, имеющий квантовую суперпозицию или интерференцию

[3] RSA – асимметричная криптосистема (с открытым ключом), разработанная Рональдом Ривестом, Ади Шамиром и Леонардом Адлеманом из Массачусетского технологического Института (1977 г.).

[4] GNFS – General Number Field Sieve – общий метод решета числового поля.

[5] Например, в TTL-микросхемах логическому «0» может соответствует напряжение от 0 до 0,8 В, а «1» – от 2,4 до 5,0 В, соответственно.

этих базисных состояний. Возможность использования информации, содержащейся в квантовой системе с двумя состояниями как единицу измерения впервые предложили Ричард Джозса и Бен Шумахер в 1994 г. [20, 21], показавшие, что системы с двумя базисными состояниями в квантовой теории информации подобны биту в классической теории. При этом «объем квантовой информации, содержащийся в любой квантовой системе может быть выражен минимальным числом систем с двумя состояниями – называемыми теперь квантовыми битами или кубитами и которые необходимы для хранения или передачи с высокой точностью состояния системы» [3, с.19–20]. Важно, что число состояний квантовой системы в состоянии суперпозиции не ограничено. Примеры реализации такой системы могут быть различны: фотон с противоположной поляризацией, атом с двумя различными энергетическими состояниями и др. Причем в случае кубита мы имеем естественно-квантованные состояния. И благодаря квантовой суперпозиции состояний можно надеяться на экспоненциальный рост эффективности квантовых вычислений.

О квантовой суперпозиции и квантовом параллелизме

Используя обозначения П. Дирака, изолированные когерентные состояния квантовой системы могут быть описаны волновой функцией или вектором состояния $|\Psi>$ в некотором гильбертовом пространстве, например, в конечномерном векторном пространстве над полем комплексных чисел. Сопряженный вектор для состояния $|\Psi>$ обозначается как $<\Psi|$. Для квантовых физических состояний выполняется условие нормировки для скалярного произведения: $<\Psi|\Psi>=1$. В случае кубита мы имеем двухбазисное или двухуровневое квантовое состояние в двумерном комплекснозначном гильбертовом пространстве. В силу линейности квантовой механики возможность находиться системе в двух базисных состояниях $|0>$ и $|1>$ позволяет ей находиться и в неограниченной линейной комбинации (суперпозиции) этих состояний: $c_1|0>+c_2|1>$, с комплексными амплитудами c_1 и c_2, при условии нормировки: $|c_1|^2+|c_2|^2=1$.

Иногда удобно представить суперпозицию двухбазисного состояния кубита как неограниченное количество точек на поверхности единичной сферы – сферы Блоха. При измерении бесконечное число состояний стягиваются к одному из полюсов. Вычислительные операции могут быть заданы как унитарные вращения сферы, а параметры вращения соответствуют параметрам воздействия на квантовый объект.

В случае системы из двух кубитов мы имеем четыре двухбазисных квантовых состояния: $|00>$, $|01>$, $|10>$ и $|11>$. Вектор состояния имеет вид:

$|\Psi>=c_1|00>+c_2|01>+c_3|10>+c_4|11>$, где $c_1, \ldots, c_4$ – амплитуды вероятности, причем вероятность при измерении $|\Psi>$ получить значение «00» равно $|c_1|^2$ и т.д.

При наличии в квантовой системе некоторого числа L упорядоченных кубитов можно говорить о квантовом регистре, имеющем 2^L базисных состояний одновременно. Вектор состояния для L кубитов или когерентная суперпозиция базисных состояний имеет вид:

$$|\Psi> = \sum_{n=0}^{2^L-1} c_n |n>, \qquad (1)$$

где $|n>$ – базисные квантовые состояния в двоичной записи;

$|n>=|n_{L-1}, n_{L-2}, \ldots, n_0>$; n_j=0,1. (в двоичной записи); c_n – амплитуды или комплексные числа такие, для которых $|c_n|^2$ – есть вероятность определения системы в базисном состоянии $|n>$ [17, 22].

Таким образом, если классический регистр в некоторое время находится только в одном из базисных состояний $|n>$, то квантовый регистр, состоящий из L кубитов, находится во всех 2^L базисных состояниях одновременно. В этом проявляется *когерентная суперпозиция* базисных состояний (1) и тем самым реализуется возможность одновременных параллельных изменений каждого из 2^L состояний. Т.е. квантовым системам внутренне присущ *квантовый параллелизм*, позволяющий за один такт изменений базисных состояний выполнять одновременно 2^L вычислений, что экспоненциально превышает возможности классических аналогов.

При всех отмеченных преимуществах считывание результата, полученного при параллельных изменениях (вычислениях) квантового регистра, сопряжено с фундаментальными

ограничениями на измерение квантовых систем. Но сначала рассмотрим, в чём состоит изменение или эволюция квантовой системы.

Эволюция состояния кубита

Для изменения состояния квантовой системы в целях квантовых вычислений необходимо обеспечить избирательное воздействие на каждый кубит регистра. Алгоритм последовательности селективных воздействий на систему кубитов составляет аналог программы для квантовых вычислений. Формально, изменение состояния кубита эквивалентно действию оператора эволюции $\hat{U}$. Для его нахождения вспомним, что вектор состояния квантовой системы или её волновая функция $|\Psi(t)>$ описывается уравнением Шрёдингера:

$$i\hbar\frac{d}{dt}|\Psi(t)> = \hat{H}|\Psi(t)>, \qquad (2)$$

где $\hat{H}$ – оператор Гамильтона – эрмитов оператор данной квантовой системы; $\hbar = h/2\pi$, где h– постоянная Планка.

Перепишем уравнение (2) в виде:

$\frac{d|\Psi(t)>}{|\Psi(t)>} = -\frac{i}{\hbar}\hat{H}dt$. Принимая, что $\hat{H}$ не зависит от t, интегрируя, получаем:

$$\ln|\Psi(t)>|_0^t = -\frac{i}{\hbar}\int_0^t \hat{H}dt = -\frac{i}{\hbar}\hat{H}t,$$

$$|\Psi(t)> = \exp(-\frac{i}{\hbar}\hat{H}t)|\Psi(0)> = \hat{U}|\Psi(0)>,$$

где $\hat{U} = \exp(-\frac{i}{\hbar}\hat{H}t)$ – унитарный оператор эволюции, определяемый оператором Гамильтона системы кубитов и реализующий унитарное преобразование данной квантовой системы.

В силу эрмитовости оператора Гамильтона, оператор эволюции является унитарным: $\hat{U}^+\hat{U}=\hat{U}\hat{U}^+=1$; где $\hat{U}^+$– сопряжённый оператор. Это обеспечивает сохранение нормы волновой функции и существование обратного оператора $\hat{U}^{-1}=\hat{U}^+$. Поэтому по конечному состоянию системы возможно восстановить начальное: $|\Psi(0)>=\hat{U}^+|\Psi(t)>$. Т.е. эволюция или изменение изолированной квантовой системы является как унитарной, так и обратимой [22].

Теперь вернёмся к системе кубитов, приведенных к начальному состоянию суперпозиции в начальный момент времени и описываемых разложением (1). Введенные данные в систему кубитов подвергаются избирательному воздействию последовательности квантовых логических элементов (гейтов), формирующих квантовый алгоритм. Действие логических элементов формально эквивалентно действию оператора эволюции, изменяющего состояние системы кубитов. При этом начальное состояние суперпозиции системы (1) преобразуется в новое состояние:

$$|\Psi(t)> = \sum_{n=0}^{2^L-1} c_n\,\hat{U}|n>.$$

Чтобы результаты вычислений стали доступны, необходимо их считывание или измерение. А здесь нас ждут весьма серьёзные ограничения.

Измерение состояния кубита

Измерение или наблюдение в квантовой системе представляет действие, при котором квантовая система взаимодействует с классической системой или внешней средой, теряя изолированность и внутреннюю целостность. Такой классической системой может быть как измерительный прибор, так и просто условия наблюдения.

Вспомним опыт с интерференцией фотонов на двух щелях, при котором одиночные фотоны, проходя через диафрагму с двумя щелями, формируют интерференционную картину на экране-детекторе. То же оказывается верно и для частиц с ненулевой массой покоя (например, [23, 24]). В данном случае, интерференция – это проявление квантовой суперпозиции состояния частиц. Частица, проявляя волновые свойства, оказывается в этом смысле *нелокализованной* и «проходит» одновременно через обе щели.

Измерение или наблюдение факта прохождения частицы около какой-либо из щелей требует взаимодействия частицы с классическим измерительным прибором или средой наблюдения, тем самым приводя к декогерентности и разрушая интерференцию. Суперпозиция свёртывается, частица проявляет локальность, оставляя только классическое распределение интенсивностей.

Поставим в соответствие наблюдаемой физической величине A эрмитов оператор $\hat{A}$; и пусть $|\Psi_1>$, $|\Psi_2>$ …, $|\Psi_n>$ – собственные векторы оператора $\hat{A}$, составляющие базис в некотором гильбертовом (линейном) пространстве состояний H, тогда для вектора состояния кубита имеем:

$$|\Psi> = \sum_{i=1}^{\infty} c_i\,|\Psi_i>, \qquad (3)$$

где c_i – комплексные числа (амплитуды вероятности), причем $|c_i|^2$ – вероятность того, что кубит при измерении величины А окажется в базисном состоянии $|\Psi_i>$, при этом наблюдаемая величина А принимает значения a_i, – собственные значения оператора $\hat{A}$: $\hat{A}|\Psi_i> = a_i|\Psi_i>$.

Таким образом состояние, описываемое соотношением (3), показывает, что кубит в данное время может находится во всём неограниченном множестве своих состояний, реализуя когерентную суперпозицию. Измерение или наблюдение создаёт коллапс волновой функции кубита, редуцируя её к одному из своих базисных состояний $|\Psi_i>$ с вероятностью $|c_i|^2$ [24, 17].

Поскольку результаты, получаемые в квантовой механике, носят вероятностный, статистический характер, ограничения при измерении состояния квантового регистра часто требуют многократных измерений для получения распределения вероятностей конечного результата [22].

Теперь рассмотрим ограничения, накладываемые на измеряемые, наблюдаемые величины. Ограничивающий принцип – принцип неопределённости может быть выражен следующим образом: невозможно посредством измерения состояния квантовой системы определить осуществление двух взаимоисключающих событий без одновременного разрушения интерференционной картины [23]. В другом виде такое ограничение известно, как соотношение неопределенностей Гейзенберга: $\Delta p \Delta q \geq \frac{\hbar}{2\pi}$, где Δp и Δq – вероятная погрешность измерения канонически сопряженных переменных, например, координаты и импульса; энергии и времени. Т.е. чем меньше вероятная погрешность измерения одной величины, тем больше погрешность измерения другой. По этой причине понятие траектории отсутствует в квантовой механике.

Более полное описание квантовых систем возможно лишь с помощью двух взаимоисключающих классических понятий, входящих в соотношение неопределенностей. Такой принцип описания посредством взаимоисключающих понятий и в тоже время взаимодополняющих друг друга, составляет *принцип дополнительности Бора*. В 1933 г. Вернер Гейзенберг в своём нобелевском докладе отмечал: «Это соотношение дополнительности между различными аспектами одного и того же физического процесса действительно является характерным для всего типа закономерностей квантовой механики … описание энергетических закономерностей находится в исключающем соотношении к исследованию пространственно-временно*г*о течения событий. Подобным же образом рассмотрение химических свойств молекулы является дополнительным к исследованию движений отдельных электронов в молекуле; наблюдение явлений интерференции стоит в дополнительном соотношении к наблюдению отдельного светового кванта… Классическая физика представляет тот вид стремления к познанию природы, при котором мы стараемся заключить об объективных процессах, по существу исходя из наших ощущений; поэтому мы отказываемся здесь от учета влияний, которые оказывают все наблюдения на наблюдаемый объект. Классическая физика как раз и кончается в том месте, где нельзя уже отказаться от учета влияния наблюдения на исследуемые процессы. Квантовая механика, наоборот покупает возможность рассмотрения атомных процессов путём частичного отказа от их описания в пространстве и времени и их объективирования.» [25, с.32] Важно отметить, что как методологический принцип описания некоторого целостного состояния, принцип дополнительности сохраняет свою значимость и за пределами естественно-научного знания.

* * *

Одночастичные состояния, описываемые соотношением (3), т.е. отвечающие требованиям состояния кубита, называют *чистыми состояниями*. Чистые состояния являются безэнтропийными. Некогерентные смеси чистых состояний могут формировать многочастичное *смешанное состояние*, которое не может быть описано набором векторов их квантовых состояний. Такое описание возможно с помощью тензорного произведения пространств векторов состояний этих частиц. Но не всякий вектор состояния может быть представлен в виде тензорного произведения векторов соответствующих пространств состояний. Такие состояния

называют *запутанными* [26]. Эти состояния нельзя свести к комбинации отдельных состояний. Их формализованное описание, как и других многочастичных смешанных состояний, может быть осуществлено с помощью матриц плотности.

Запутанные состояния (entangled states)

Совместно с состоянием квантовой суперпозиции (интерференции) *запутанное состояние* (*entangled state*)[6] является важнейшим состоянием многочастичной квантовой системы и проявляет себя как фундаментальный ресурс Природы [27]. Такие состояния могут появляться, например, когда частицы некоторое время взаимодействуют, а потом разлетаются.

Рассмотрим систему, образованную двумя однофотонными пучками с различными квантовыми состояниями [29]. Для суперпозиции четырёх возможных поляризационных состояний фотонной пары имеем:
$|\Psi_{12}\rangle=c_1|0\rangle_1|0\rangle_2+c_2|1\rangle_1|1\rangle_2+c_3|0\rangle_1|1\rangle_1+c_4|1\rangle_2|0\rangle_2$, где $|0\rangle$ и $|1\rangle$ – векторы состояния фотонов с разной поляризацией. Каждый фотон одного пучка связан с фотонами другого пучка и эта связь не равна произведению волновых функций фотонов. Т.е. вектор запутанного состояния не может быть представлен в виде тензорного произведения векторов состояний отдельных частиц.

В 1964 г. Джон Белл, рассматривая ЭПР-парадокс[7], ввёл удобные базисные состояния для двух частиц, соответствующие их максимальной запутанности – состояния Белла:

$$|\Psi^-\rangle_{12}=(|0\rangle_1|1\rangle_2-|1\rangle_1|0\rangle_2)/\sqrt{2};$$
$$|\Psi^+\rangle_{12}=(|0\rangle_1|1\rangle_2+|1\rangle_1|0\rangle_2)/\sqrt{2};$$
$$|\Phi^-\rangle_{12}=(|0\rangle_1|0\rangle_2-|1\rangle_1|1\rangle_2)/\sqrt{2};$$
$$|\Phi^+\rangle_{12}=(|0\rangle_1|0\rangle_2+|1\rangle_1|1\rangle_2)/\sqrt{2}.$$

Эти состояния обладают интересными свойствами: если посредством какого-либо измерения один из фотонов редуцируется (проецируется) к состоянию с определенной поляризацией, то поляризация фотона из другого пучка становится противоположной, т.е. также определенной. Таким образом, измерение (наблюдение) проводимое над одной частицей, мгновенно изменяет состояние другой, независимо от удалённости обеих. Такие свойства запутанных состояний нашли экспериментальное подтверждение [32]. С другой стороны, если измерение одной частицы не влияет на состояние другой, то частицы не являются запутанными. Важно также отметить, что определение состояния всей системы запутанных частиц не означает такой же определенности в состоянии её частей. Отдельные частицы в запутанном состоянии теряют свои индивидуальные свойства.

* * *

Реальная опасность взлома асимметричных криптосистем типа RSA, а также возможная опасность дешифровки симметричных систем таких как AES-256[8], заставляет исследователей задуматься над созданием криптосистемы, построенной на других информационных принципах. Теорема о невозможности копирования квантового состояния, как и коллапс состояния квантовой системы при её измерении позволяют реализовать квантовый криптографический протокол передачи информации, имеющий несколько модификаций. Попытка перехвата передаваемого кода сводится к той или иной форме измерения состояния передаваемых квантовых систем и тем самым к редукции передаваемого квантового состояния, что не может остаться незамеченным.

[6] От англ. *Entanglement* – перевод немецкого термина *Verschrankung*, который использовал Эрвин Шрёдингер в 1935 г. [28]. В русскоязычной литературе кроме слова «запутанные» используются также синонимы: «перепутанные», «сцепленные» и «связанные».

[7] ЭПР-парадокс – мысленный эксперимент, рассмотренный в статье А. Эйнштейна, Б. Подольского и Н. Розена [30], когда две частицы после взаимодействия разлетаются на большое расстояние. Частицы находятся в запутанном состоянии, поэтому измерения состояния одной из частиц изменяет состояние другой, создавая видимость дальнодействия и возможности сверхсветовой передачи сигнала. В статье [30] авторы пытались показать неполноту квантовой механики в вероятностной (копенгагенской) интерпретации. Отметим, что некоторые исследователи квантовых явлений придерживаются многомировой интерпретации, предложенной Хью Эвереттом в 1957 г. [31].

[8] AES-256 – Advanced Encryption Standard – один из наиболее используемых и безопасных алгоритмов шифрования с ключом в 256 бит.

О коммуникационном протоколе квантовой телепортации

Теоретическая возможность переноса квантового состояния одного объекта на другой была предложена Чарльзом Бенетом с сотрудниками в 1993 г. [33]. Но экспериментальная проверка была выполнена в конце 1997 г. группой Антона Цайлингера [34].

Предположим, что Алиса[9] хочет передать состояние своей частицы 1 (фотона) Бобу, но непосредственно передать эту частицу не может. Вектор состояния этого фотона имеет вид: $|\Psi_1\rangle=c_1|1\rangle_1+c_2|0\rangle_1$.

Далее полагаем, что имеется вспомогательный источник двух частиц (фотонов) в перепутанном состоянии – источник ЭПР-пары[10], состояние которой для частиц 2 и 3 описывается вектором состояния: $|\Psi^-\rangle_{23}=(|0\rangle_2|1\rangle_3-|1\rangle_2|0\rangle_3)/\sqrt{2}$.

Частица 2 передаётся Алисе, а частица 3 – Бобу. Состояние трёх частиц может быть представлено в виде суперпозиции четырёх состояний Белла, т.е. разложено по базисным состояниям Белла, при этом частицы 1 и 2 изначально не являются запутанными. Таким образом, имеем:

$$|\Psi\rangle_{123}=|\Psi\rangle_1\otimes|\Psi\rangle_{23}=$$
$$=[|\Psi^-\rangle_{12}\,(c_1|1\rangle_3+c_2|0\rangle_3)+|\Psi^+\rangle_{12}\,(-c_1|1\rangle_3+c_2|0\rangle_3)+$$
$$+|\Phi^-\rangle_{12}\,(c_1|0\rangle_3+c_2|1\rangle_3+)+|\Phi^+\rangle_{12}\,(c_1|0\rangle_3-c_2|1\rangle_3)]/2.$$

Алиса выполняет измерения состояния Белла над частицами 1 и 2, т.е. редуцирует состояния частиц 1 и 2 в одно из состояний Белла, например, в $|\Psi^-\rangle_{12}$, тем самым создавая запутанную пару, при этом состояние частицы 3, находящейся у Боба, мгновенно[11] оказывается в состоянии, соответствующем изначальному состоянию частицы 1, т.е. $|\Psi_3\rangle=c_1|1\rangle_3+c_2|0\rangle_3$ и не зависит от расстояния между Алисой и Бобом. Далее Алиса оповещает Боба о результатах своих измерений с помощью классического канала связи. В случае, если Алиса редуцирует свои две частицы в другое состояние Белла, то Бобу для получения начального состояния частицы 1 после оповещения от Алисы следует выполнить соответствующее унитарное преобразование над своей частицей [29, 35]. На этом протокол квантовой телепортации завершается.

Заметим, что при измерении или редукции начальное состояние первой частицы необратимо разрушается, а сама частица становится частью запутанной пары частиц 1 и 2. Поэтому при квантовой телепортации не нарушается теорема о невозможности копирования квантового состояния. Факт телепортации может быть не известен Бобу, а Алиса может не знать состояние телепортируемой частицы.

Наряду с протоколом квантовой телепортации существует протокол квантового плотного кодирования, позволяющий удвоить плотность коммуникационного канала по сравнению с классическим. Он был предложен Чарльзом Беннетом и Стивеном Виснером [35].

О практической реализации

Учитывая достижения в создании однофотонных источников, современный технологический уровень позволяет реализовать некоторые квантовые криптографические системы. Так, с конца 90-х начали работать коммерческие сети, использующие квантовые коммуникационные протоколы, на расстояние до 50 км. В 2007 г. на выборах в Швейцарии повсеместно использовались квантовые сети [36]. Недавно была показана возможность реализации протокола квантовой телепортации через стандартные городские оптоволоконные кабели. Исследования проводились независимо в Университете Калгари (Канада) и в Китайском Университете науки и технологий [37, 38].

Основной проблемой при создании как квантовых сетей, так и квантовых вычислений

[9] Алиса, Боб и пытающаяся подслушать их Ева – имена, используемые в криптографии и в компьютерной безопасности, символизирующие агентов коммуникационных протоколов и не всегда связанные с людьми.

[10] Источник ЭПР-пары – источник двух запутанных частиц, рассмотренный в мысленном эксперименте А. Эйнштейна, Б. Подольского и Н. Розена [30]. Например, две частицы, удалившиеся друг от друга после взаимодействия. Такую пару частиц с общим вектором состояния и не представимой в виде произведения векторов состояний каждой из частиц, называют ЭПР-парой.

[11] При этом, по-видимому, нет превышения скорости света при передаче состояния системы и противоречия с теорией относительности, поскольку изменения, вносимые в квантовую систему, носят случайный характер, а мгновенная передача изменений, проявляющая запутанность двух частиц, не несёт информации (сигнала) [17]. Необходимость использования классического канала связи, заведомо ограниченного скоростью света, снимает эти опасения.

является потеря квантовой системой состояния суперпозиции – *проблема декогерентности*. Возможные решения направлены на создание максимально изолированных квантовых систем – с одной стороны, и увеличение времени когерентности – с другой. Если в создании квантовых сетей прогресс уже заметен, то в отношении квантовых вычислительных средств дела обстоят сложнее, но и здесь есть успехи. Отметим некоторые из них.

В 2001 г. IBM сообщила об успешном испытании 7-кубитного компьютера, созданного на основе ЯМР[12]. На нём был реализован алгоритм факторизации Питера Шора в отношении числа 15 [39].

Начиная с 2007 г. канадская компания D-Wave Systems начала заявлять о создании квантовых компьютеров адиабатического типа: 2007 г. – 16 кубитов («Orion»); ноябрь 2007 г. – 28 кубитов; май 2011 г. – 128 кубитов («D-Wave One»); май 2013 г. – 512 кубитов («D-Wave Two»); август 2015 г. – 1152 кубита («D-Wave 2X») [40]. В конце сентября 2016 г. на конференции в Санта-Фе (Нью-Мексико) представлен компьютер на 2000 кубитах [41]. Компьютеры D-Wave основаны на естественной физической эволюции системы, постепенно достигающей состояния энергетического минимума и способны решать ограниченные задачи на оптимизацию – квантовую нормализацию (квантовый отжиг). С мая 2011 г. D-Wave вышла на рынок с «D-Wave One» (128 кубитов) – среди покупателей Lockheed Martin Corporation. Заказчиками «D-Wave Two» становятся, кроме Lockheed Martin, также Google, NASA и URSA[13]. А к заказчикам версии «D-Wave 2X» добавляется уже и Los Alamos National Laboratory [40].

В конце 2015 г. эксперты из Google подтвердили наличие в 1152 кубитовом «D-Wave 2X» квантовых эффектов. Они сравнили квантовую нормализацию, которая физически происходит внутри «D-Wave 2X», с его алгоритмической имитацией. В результате «D-Wave 2X» работает в 100 млн раз быстрее, но эта скорость может достигаться за счет квантового туннельного эффекта, а не квантовой суперпозиции, обеспечивающей квантовое (экспоненциальное) ускорение. При решении оптимизационной задачи – поиске минимума функции среди наборов других решений – «D-Wave 2X» обгоняет неоптимизированный алгоритм для классического компьютера, а более эффективному алгоритму Селби уже уступает [42, 43]. Анонсированная 2000 кубитная версия, по мнению разработчиков, позволит использовать стандартные алгоритмы квантовых вычислений, а также сочетать квантовые и классические алгоритмы для повышения производительности и оптимизации выборки результатов [41].

Заключение

Квантовая информатика, впитавшая в себя идеи многих областей научного знания, испытывает существенный подъём в своём развитии, что в свою очередь положительно влияет на развитие таких дисциплин, как квантовая механика, квантовая оптика, криптография, программирование, и др. Однако опережающее развитие теории несколько диссонирует с уровнем практической реализации. Вместе с тем квантовые линии связи постепенно выходят за пределы исследовательских лабораторий, осваивая коммерческий и государственный сегмент. Квантовые компьютеры, представленные на рынке, ориентированы на узкий класс задач и даже в них трудно обнаружить квантовое ускорение. Несмотря на возможность приведения множества задач к уже реализованному виду, об универсальности вычислений говорить пока рано.

Но с другой стороны, отсутствие технологического прорыва в создании квантового «железа» – не самая плохая новость для законопослушного пользователя. Предположим, что в сети присутствует полноценный квантовый компьютер, способный успешно выполнять факторизацию тысячезначных чисел за приемлемое (полиномиальное) время. Наличие при этом недоброй воли позволит взламывать криптосистемы с ассиметричным кодом (RSA), а при создании соответствующих алгоритмов – и с симметричным кодом (AES-256, TDEA

[12] ЯМР – ядерно-магнитный резонанс.
[13] URSA – Universities Space Research Association.

(3DES)[14], «Serpent», «ГОСТ 28147-89 (Магма)»[15] и др.), что сделает прозрачными далеко не только аккаунты социальных сетей и электронной почты.

Теоретические работы по квантовой информатике имеют, кроме прикладного, большое самостоятельное значение, поскольку позволяют осознать неполноту традиционного, классического мировосприятия, ограниченного «локальным реализмом».

Литература

1. Шрёдингер Э. 2400 лет квантовой теории // Шрёдингер Э. Избранные труды по квантовой механике. М.: Наука, 1976. С.254–260.
2. Экерт А., Жизан Н., Хаттнер Б., Инамори Х., Вайнфуртер Х. Квантовая криптография // Физика квантовой информации. Под ред. Боумейстера Д., Экерта А., Цайлингера А. М.: Постмаркет, 2002.
3. Стин Э. Квантовые вычисления. Ижевск: «Регулярная и хаотическая динамика», 2000.
4. Wiesner S. Conjugate coding. SIGART News. 1983. 15. 78–88.
5. Холево А.С. Некоторые оценки для количества информации, передаваемого квантовым каналом связи // Проблемы передачи информации. 1973. Т.9. №3. С.3–11.
6. Манин Ю.И. Вычислимое и невычислимое. М.: Сов. радио, 1980. С. 15.
7. Benioff P. The computer as a physical system: a microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines // J. Stat. Phys. 1980. 22. 563.
8. Бенёв П. Квантовомеханические гамильтоновы модели машин Тьюринга // Квантовый компьютер и квантовые вычисления. Т.2. / Пер. с англ. – Ижевск: «Регулярная и хаотическая динамика», 1999. С.53–95. (Benioff P. Quantum mechanical Hamiltonian models of Turing machines // J. Stat. Phys. 1982. 29. 515–546.)
9. Benioff P. Quantum mechanical model of Turing machines that dissipate no energy // Phys. Rev. 1982. Lett. 48. 1581–1585.
10. Фейнман Р. Моделирование физики на компьютерах // Квантовый компьютер и квантовые вычисления. Т.2. / Пер. с англ. – Ижевск: «Регулярная и хаотическая динамика», 1999. С.96–124. (Feynman R. Simulating physics with computers // International Journal of Theoretical Physics. 1982. V.21. No 6/7, P.467–488.)
11. Wootters W.K., Zurek W.H. A single quantum cannot be cloned // Nature. 299. 802–803 (1982).
12. Dieks D. Communication by EPR devices // Physics Letters. A 92 (6). 271–272.
13. Feynman R. Quantum mechanical computers // Optics News. February. 1985.
14. Дойч Д. Квантовая теория, принцип Чёрча – Тьюринга и универсальный квантовый компьютер // Квантовый компьютер и квантовые вычисления. Т.2. / Пер. с англ. – Ижевск: «Регулярная и хаотическая динамика», 1999. С.157–189. (Deutsch D. Quantum theory, the Church – Turing principle and the universal quantum computer // Proc. Roy. Soc. Lond. 1985. A400, P. 97–117.)
15. Deutsch D. Quantum computational networks // Proc. Roy. Soc. London. 1989. A 425. 73–90.
16. Шор П. Полиномиальные по времени алгоритмы разложения числа на простые множители и нахождения дискретного алгоритма для квантового компьютера // Квантовый компьютер и квантовые вычисления. Т.II. / Пер. с англ. – Ижевск: «Регулярная и хаотическая динамика», 1999. С.200–247. (Shor P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer // SIAM Journal on Computing. 26. 5. 1484–1509.)
17. Гуц А.К. Основы квантовой кибернетики. Омск: КАН, 2008.
18. Холево А.С. Введение в квантовую теорию информации. М.: МЦНМО, 2013.
19. Гровер Л.К. Квантовая механика помогает найти иголку в стоге сена // Квантовый компьютер и квантовые вычисления. Т.I. / Пер. с англ. – Ижевск: «Регулярная и хаотическая динамика», 1999. С.101–109. (Grover L.K. Quantum mechanics helps in searching for a needle in a haystack // Phys. Rev. Lett. 79. 325–328.)
20. Jozsa R., Schumacher B. A new proof of the quantum noiseless coding theorem // J. Mod. Optics. 41. 2343–2349. 1994.
21. Schumacher B. Quantum coding // Phys. Rev. A. 51. 2738–2747. 1995.
22. Качаев И.А. Квантовые вычисления. Протвино: Препринт ИФВЭ, 2001.
23. Фейнман Р., Лейтон Р., Сэндс М. Фейнмановские лекции по физике. Вып.3, 8. М.: Мир, 1966.
24. Боумейстер Д., Цайлингер А. Физика квантовой информации: основные понятия // Физика квантовой информации. Под ред. Боумейстера Д., Экерта А., Цайлингера А. М.: Постмаркет, 2002.
25. Гейзенберг В. Развитие квантовой механики // Современная квантовая механика. Три нобелевских доклада. М.-Л.: Гостехиздат, 1934.
26. Кронберг Д.А., Ожигов Ю.И., Чернявский А.Ю. Квантовая информатика и квантовый компьютер. М.: Макс Пресс, 2011.
27. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация. М.: Мир, 2006.
28. Шрёдингер Э. Современное состояние квантовой механики / Пер. с нем. // Успехи химии. 1936. Т.5. С.390 (395–442). (Schrödinger E. Die gegenwärtige Situation in der Quantenmechanik // Naturwissenschaften. 1935. 23. P. 807–812. 823–828. 844–849. Engl. transl.: John D. Trimmer. Proceedings of the American Philosophical Society. 124. 323–338. 1980. Reprinted in: Quantum Theory and Measurement. P.152. 1983.)
29. Килин С.Я. Квантовая информация // Успехи физических наук. 1999. Т.169. №5. С.507–527.

[14] TDEA (3DES) – Triple Data Encryption Algorithm – симметричный блочный алгоритм шифрования данных.

[15] «ГОСТ 28147-89 (Магма)» – российский стандарт шифрования.

30. Эйнштейн А., Подольский Б., Розен Н. Можно ли считать квантово-механическое описание физической реальности полным? / Пер. с англ. // Успехи физических наук. 1936. Т.16. Вып.4. (Einstein A., Podolsky B., Rosen N. Can Quantum-Mechanical Description of Physical Reality be Considered Complete? // Phys. Rev. American Physical Society. 1935. Vol. 47. Iss. 10. P. 777–780.) URL: http://ufn.ru/ufn36/ufn36_4/Russian/r364_b.pdf
31. Дойч Д. Структура реальности. Ижевск: «Регулярная и хаотическая динамика», 2001.
32. Greenberger D.M., Horne M.A., Zeilinger A. Multiparticle Interferometry and the Superposition Principle. Phys. Today. 46 (8). 22. 1993.
33. Bennett Ch., Brassard G. et al. Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels // Physical Review Letters. 70. 1895. (1993).
34. Боувмеестер Д., Ян-Вэй Пан, Маттл К., Эйбл М., Вайнфуртер Г., Цайлингер А. Экспериментальная квантовая телепортация / Пер. с англ. // Квантовый компьютер и квантовые вычисления. Т.I. Ижевск: «Регулярная и хаотическая динамика», 1999. С.114–129. (Bouwmeester D., Pan J.-W., Mattle K., Eibl M., Weinfurtner H., Zeilinger A. Experimental Quantum Teleportation. Nature. London. 390. 575. 1997.)
35. Боумейстер Д., Вайнфуртер Х., Цайлингер А. Квантовая плотная кодировка и квантовая телепортация // Физика квантовой информации. Под ред. Боумейстера Д., Экерта А., Цайлингера А. М.: Постмаркет, 2002.
36. Квантовая криптография // URL: https://ru.wikipedia.org/wiki/Квантовая_криптография
37. Grosshans F. Quantum communications: Teleportation becomes streetwise // Nature Photonics. 10. 623–625. (2016). URL: http://www.nature.com/nphoton/journal/v10/n10/pdf/nphoton.2016.190.pdf
38. Qi-Chao Sun, Ya-Li Mao, Si-Jing Chen et al. Quantum teleportation with independent sources and prior entanglement distribution over a network // Nature Photonics. 10. 671–675. (2016). URL: http://www.nature.com/nphoton/journal/v10/n10/pdf/nphoton.2016.179.pdf
39. Квантовый компьютер // URL: https://ru.wikipedia.org/wiki/Квантовый_компьютер
40. D-Wave Systems // URL: https://en.wikipedia.org/wiki/D-Wave_Systems
41. D-Wave Systems Previews 2000-Qubit Quantum System // URL: http://www.dwavesys.com/press-releases/d-wave-systems-previews-2000-qubit-quantum-system
42. Добрынин С. Квантовое ускорение // URL: http://www.svoboda.org/a/27423981.html
43. Google experiments suggest that the D-Wave computer exploits quantum phenomena // URL: http://news.mit.edu/2015/3q-scott-aaronson-google-quantum-computing-paper-1211

Сергеев Дмитрий Ильич. Инженер-исследователь ИСА ФИЦ ИУ РАН. Окончил МИФИ в 1987 году. Количество печатных работ: 4. Область научных интересов: квантовая информатика, безэнтропийные состояния. E-mail: dms135@yandex.ru

Formation of basic ideas in quantum computer science

D.I. Sergeev

Abstract. In article some basic concepts and ideas of quantum computer science are considered. Much attention is paid to key properties of quantum systems – the quantum superposition and a quantum entanglement, which allows to realize the advantage of quantum parallel computing and quantum networks. The communications protocol of quantum teleportation is explained. Some results of creation of quantum networks and quantum computers are discussed.
Keywords: quantum computing, qubit, quantum superposition, quantum entanglement.

References

1. Schrödinger E. 2400 of the quantum theory // Schrödinger E. The selected works on a quantum mechanics. M.: Nauka, 1976. P. 254-260.
2. Ekert A., Zhizan N., Hattner B., Inamori X., Vaynfurter X. Quantum cryptography // D. Bouwmeester, A. Ekert, A. Zeilinger (Eds.) The Physics of Quantum Information. M.: Postmarket, 2002.
3. Steen E. Quantum computings. Izhevsk: "Regular and chaotic dynamics", 2000.
4. Wiesner S. Conjugate coding. SIGART News. 1983. 15. 78–88.
5. Holevo A.S. Some estimates of the amount of information transmitted by a quantum communication channel // Problems of information transmission. 1973. T. 9. No. 3. Pp. 3–11.
6. Manin Yu.I. Computable and not computable. M.: Sov. radio, 1980. P.15.
7. Benioff P. The computer as a physical system: a microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines // J. Stat. Phys. 1980. 22. 563.
8. Benioff P. Quantum mechanical Hamiltonian models of Turing machines // J. Stat. Phys. 1982. 29. 515–546.
9. Benioff P. Quantum mechanical model of Turing machines that dissipate no energy // Phys. Rev. 1982. Lett. 48. 1581–1585.

10. Feynman R. Simulating physics with computers // International Journal of Theoretical Physics. 1982. V.21. No 6/7, P.467–488.
11. Wootters W.K., Zurek W.H. A single quantum cannot be cloned // Nature. 299. 802–803 (1982).
12. Dieks D. Communication by EPR devices // Physics Letters. A 92 (6). 271–272.
13. Feynman R. Quantum mechanical computers // Optics News. February. 1985.
14. Deutsch D. Quantum theory, the Church – Turing principle and the universal quantum computer // Proc. Roy. Soc. Lond. 1985. A400, P. 97–117.
15. Deutsch D. Quantum computational networks // Proc. Roy. Soc. London. 1989. A 425. 73–90.
16. Shor P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer // SIAM Journal on Computing. 26. 5. 1484–1509.
17. Guts A. K. Foundations of quantum Cybernetics. Omsk: CAN, 2008.
18. Holevo A. S. Introduction to the quantum theory of information. M.: MTsNMO, 2013.
19. Grover L.K. Quantum mechanics helps in searching for a needle in a haystack // Phys. Rev. Lett. 79. 325–328.
20. Jozsa R., Schumacher B. A new proof of the quantum noiseless coding theorem // J. Mod. Optics. 41. 2343–2349. 1994.
21. Schumacher B. Quantum coding // Phys. Rev. A. 51. 2738–2747. 1995.
22. Kachaev I. A. Quantum computings. Protvino: IFVE preprint. 2001.
23. Feynman R., Leighton R., Sands M. The Feynman lectures on physics. Issue 8. M.: Mir, 1966.
24. Boumeyster D., Tsaylinger A. Physics of quantum information: basic concepts // Boumeyster D., Ekert And., Tsaylinger A. (Ads.) Physics of quantum information. M.: Postmarket, 2002.
25. Heisenberg Development of quantum mechanics / Modern quantum mechanics. Three Nobel report. M.-L.: Gostekhizdat, 1934.
26. Kronberg D. A., Ozhigov Yu. I., Chernyavsky A. Yu. Quantum informatics and quantum computer. M.: Max Press, 2011.
27. Nielsen M., Chuang I. Quantum computings and quantum information. M.: Mir, 2006.
28. Schrödinger E. The current state of a quantum mechanics // Achievements of chemistry. 1936. T.5. P. 390 (395–442).
29. Kilin S.Ya. Quantum information//Achievements of physical sciences. 1999. T.169. No. 5. P. 507-527.
30. Einstein A., Podolsky B., Rosen N. Can Quantum-Mechanical Description of Physical Reality be Considered Complete? // Phys. Rev. American Physical Society. 1935. Vol. 47. Iss. 10. P. 777–780. Available at: http://ufn.ru/ufn36/ufn36_4/Russian/r364_b.pdf (accessed November 16, 2016).
31. Deutsch D. The fabric of reality. Izhevsk: "Regular and chaotic dynamics", 2001.
32. Greenberger D.M., Horne M.A., Zeilinger A. Multiparticle Interferometry and the Superposition Principle. Phys. Today. 46 (8). 22. 1993.
33. Bennett Ch., Brassard G., et al. Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels // Physical Review Letters. 70. 1895. (1993).
34. Bouwmeester D., Pan J.-W., Mattle K., Eibl M., Weinfurtner H., Zeilinger A. Experimental Quantum Teleportation. Nature. London. 390. 575. (1997).
35. Baumeister, D., Weinfurter H., Zeilinger A. Quantum dense coding and quantum teleportation // Baumeister D., Ekert A., Zeilinger A. (Ads.) The Physics of quantum information. M.: Postmarket, 2002.
36. Quantum cryptography. Available at: https://ru.wikipedia.org/wiki/Квантовая_криптография (accessed November 16, 2016).
37. Grosshans F. Quantum communications: Teleportation becomes streetwise // Nature Photonics. 10. 623–625. (2016). Available at: http://www.nature.com/nphoton/journal/v10/n10/pdf/nphoton.2016.190.pdf (accessed November 16, 2016).
38. Qi-Chao Sun, Ya-Li Mao, Si-Jing Chen et al. Quantum teleportation with independent sources and prior entanglement distribution over a network // Nature Photonics. 10. 671–675. (2016). Available at: http://www.nature.com/nphoton/journal/v10/n10/pdf/nphoton.2016.179.pdf (accessed November 16, 2016).
39. A quantum computer. Available at: https://ru.wikipedia.org/wiki/Квантовый_компьютер (accessed November 16, 2016).
40. D-Wave Systems. Available at: https://en.wikipedia.org/wiki/D-Wave_Systems (accessed November 16, 2016).
41. D-Wave Systems Previews 2000-Qubit Quantum System. Available at: http://www.dwavesys.com/press-releases/d-wave-systems-previews-2000-qubit-quantum-system (accessed November 16, 2016).
42. Dobrynin S. Quantum acceleration. Available at: http://www.svoboda.org/a/27423981.html (accessed November 16, 2016).
43. Google experiments suggest that the D-Wave computer exploits quantum phenomena. Available at: http://news.mit.edu/2015/3q-scott-aaronson-google-quantum-computing-paper-1211 (accessed November 16, 2016).

D.I. Sergeev. Research engineer ISA FRC CSC RAS. Graduated in 1987 MEPhI. Number of publications: 4. Research interests: quantum computing science, non-entropic state. E-mail: dms135@yandex.ru