

КВАНТОВАЯ ИНФОРМАТИКА

Парфенов Константин Владимирович, физический факультет МГУ

Вероятностные законы квантовой физики приводят к существованию нового типа данных — информации о состоянии квантового объекта. Кроме того, как мы видели из некоторых примеров, возникают и принципиально новые алгоритмы работы с ее носителями. Специалисты по теории информации говорят о возникновении ее нового раздела — *квантовой информатики*.

Для начала вспомним о типичном физическом устройстве, которое используется для хранения информации. В классическом мире его называют так же, как и классическую единицу информации — *бит*. Это любой физический объект, который может находиться в двух различных состояниях, с помощью которых мы кодируем числа «0» и «1» (например: лампочка не светит $\equiv 0$, лампочка светит $\equiv 1$). В квантовом мире это объект, который при измерении какой-либо его характеристики (принимавшей значения 0 или 1) измерительный прибор переведет в одно из двух базисных состояний $|0\rangle$ или $|1\rangle$. Такой объект называют *кубитом* («квантовым битом»).

Подобных систем можно создать много. Например, если мы работаем с фотонами, у которых измеряем только линейную поляризацию в некотором базисе: фотоны движутся вдоль оси z , а базисные состояния отвечают поляризациям по осям x и y . Тогда эти поляризационные состояния можно считать состояниями кубита: $(|x\rangle \equiv |0\rangle \text{ и } |y\rangle \equiv |1\rangle)$.

Другой пример — «ловушки» для заряженных частиц (электронов, атомов или ионов) в некоторых кристаллических решетках. В такой «ловушке» движение заряженной частицы ограничено кристаллическим полем по всем трем направлениям, и у частицы есть «связанное» состояние. Это состояние может быть свободно (что отвечает состоянию кубита $|0\rangle$) или занято ($|1\rangle$). Довольно популярная в реальных устройствах реализация кубита — сверхпроводящий контур с непроводящей вставкой. Носители заряда могут туннелировать через вставку, благодаря чему ток в таком контуре либо есть, либо нет с некоторыми вероятностями — снова возникает система с двумя состояниями. Вспомним про спин (собственный момент количества движения квантовых частиц) и про магнитный момент, который есть у многих частиц со спином. Тогда мы поймем, что у частицы спина $\frac{1}{2}$ возможны два состояния с разными энергиями во внешнем магнитном поле: магнитный момент направлен по полю или против него. Значит, эти два состояния можно различить измерением энергии, и это тоже кубит.

Есть и другие примеры, но отметим, что все перечисленные уже реализуются на практике и используются в реальных устройствах квантовой информатики.

Как мы теперь знаем, произвольное состояние кубита — это *квантовая суперпозиция* двух базисных состояний $|0\rangle$ и $|1\rangle$, и поэтому запишем его так:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle.$$

Здесь коэффициенты разложения определяют вероятности, что при *измерении* кубит окажется в каждом из базисных состояний: $w_0 = |\alpha|^2$ и, соответственно, $w_1 = 1 - w_0 = |\beta|^2$.

Кубит, как и все квантовые объекты, обладает волновыми свойствами. Отвечающая ему волна — это волна вероятности. Как это учесть в записи формулы для квантовой

суперпозиции? В очередной раз воспользуюсь аналогией с описанием поведения света в классической теории. По образному выражению Франсуа Араго: «Самое удивительное в волновой теории света — что свет, слагаясь со светом, может дать тьму».

Если мы описываем свет как электромагнитную волну, в которой происходят колебания напряженности электрического поля и индукции магнитного поля, а интенсивность пропорциональна квадрату амплитуды колебаний электрического поля. Тогда, если две складываемые волны не *когерентны* — у них разные частоты или разность фаз колебаний изменяется случайно, то общая интенсивность равна сумме интенсивностей. В этом случае сложение «света со светом» не даст «тьму». А у *когерентных* электромагнитных волн складываются векторные величины — напряженности электрического поля, которые при сложении в *противофазе* дают ноль!

Аналогично квантовая суперпозиция состояний — это наложение когерентных волн вероятности. Результат их *интерференции* зависит не только от амплитуд складываемых волн, но и от сдвига их по фазе относительно друг друга.

Вероятность — неотрицательная величина, и суммирование ненулевых вероятностей не может дать ноль, в то время как в состоянии квантовой суперпозиции вероятность некоторых событий может оказаться нулем. Значит, она выражается через модуль амплитуды, а сами колебания волны происходят с величиной, значения которой — не просто неотрицательные числа. Нужно использовать более сложные величины.

начнем с некоторой информации из математики. Она выходит за рамки школьной программы, но, надеюсь, многих заинтересует как сама по себе, так и по ее применениям для описания квантового мира.

В классической теории колебаний разработан удобный математический метод, который позволяет анализировать сложение когерентных колебаний с учетом разности фаз — *метод комплексных амплитуд*. И в формуле для записи квантовой суперпозиции нам на самом деле тоже нужно учесть, что коэффициенты α и β содержат информацию не только об амплитудах волн вероятности, но и о фазах. Для этого удобно считать их *комплексными числами*.

Математическое дополнение 1: Что такое комплексные числа?

Если задаться целью научиться извлекать квадратные корни из отрицательных чисел, можно определить мнимую единицу $i \equiv \sqrt{-1}$, а вслед за ней — множество комплексных чисел

$$z = x + iy.$$

В этой записи x и y — два вещественных числа, называемых вещественной и мнимой частью комплексного числа z :

$$x = \text{Re}(z), y = \text{Im}(z).$$

Комплексные числа перемножают и делят друг на друга, получая снова комплексные числа. Эти операции определяются следующими формулами:

$$\begin{aligned} z_1 \cdot z_2 &= (x_1 + iy_1)(x_2 + iy_2) = (x_1x_2 - y_1y_2) + i(x_1y_2 + x_2y_1), \\ \frac{z_1}{z_2} &= \frac{x_1 + iy_1}{x_2 + iy_2} = \frac{(x_1 + iy_1)(x_2 - iy_2)}{(x_2 + iy_2)(x_2 - iy_2)} = \frac{x_1x_2 + y_1y_2}{x_2^2 + y_2^2} + i \frac{x_2y_1 - x_1y_2}{x_2^2 + y_2^2} \end{aligned}$$

Вообще, с комплексными числами можно проводить любые алгебраические операции. На множестве комплексных чисел определяются многие известные функции. Например, для экспоненты справедлива *формула Эйлера*:

$$e^z = e^x \cdot e^{iy} = e^x \cdot [\cos(y) + i \cdot \sin(y)].$$

Комплексное число $z^* \equiv x - iy$ называют сопряженным к числу z . Вещественная неотрицательная величина $|z| \equiv \sqrt{z \cdot z^*} = \sqrt{x^2 + y^2}$ называется *модулем* комплексного числа. С помощью определения его *фазы* φ

$$\begin{cases} \cos(\varphi) \equiv \frac{x}{\sqrt{x^2 + y^2}} \\ \sin(\varphi) \equiv \frac{y}{\sqrt{x^2 + y^2}} \end{cases}$$

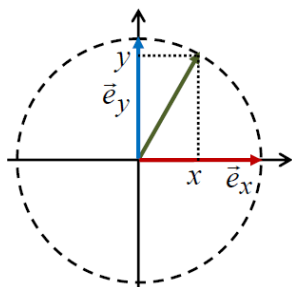
можно ввести запись комплексного числа, представленного в экспоненциальной форме

$$z = |z| \cdot e^{i\varphi}.$$

Именно эта запись указывает нам на возможность объединить в одном комплексном числе и коэффициент $|z|$, умножение на который описывает изменение амплитуды, и множитель $e^{i\varphi}$, умножение на который описывает фазовый сдвиг.

Возвращаясь к описанию состояний кубита, заметим: описание произвольного состояния как квантовой суперпозиции демонстрирует нам, что набор этих состояний «значительно больше» набора состояний бита — их бесконечно много! С точки зрения математика суперпозиция означает, что состояния кубита образуют *векторное пространство*. Поясним это с помощью геометрической аналогии. В обычном двумерном евклидовом пространстве (в плоскости) используют базисные вектора $\vec{e}_x$ и $\vec{e}_y$, по которым раскладывается любой вектор, лежащий в этой плоскости: $\vec{r} = x \cdot \vec{e}_x + y \cdot \vec{e}_y$.

Отметим, что в качестве базиса удобно использовать пару перпендикулярных векторов единичной длины:



$$|\vec{e}_x| = |\vec{e}_y| = 1 \text{ и } \vec{e}_x \perp \vec{e}_y.$$

Наглядно реализация этой идеи показана на рисунке.

Если дополнительно потребовать, чтобы

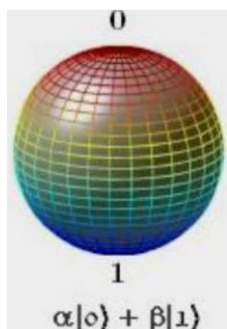
$$|\vec{r}| = \sqrt{x^2 + y^2} = 1,$$

то мы получим набор векторов единичной длины в плоскости x y .

Любой такой вектор можно «закодировать» величиной угла γ между

осью x и нашим вектором — ведь для единичного вектора ясно, что $x = \cos(\gamma)$ и $y = \sin(\gamma)$.

Однако для состояний кубита одного угла явно недостаточно. В этом случае «координаты» — это комплексные числа α и β . Полная вероятность перехода в одно из двух возможных базисных состояний равна 1. Это требование приводит к уравнению $w_0 + w_1 = |\alpha|^2 + |\beta|^2 = 1$, которое позволяет записать все «подходящие» комплексные числа через два вещественных параметра — углы ϑ и φ : $\alpha = \cos(\vartheta/2)$, $\beta = \sin(\vartheta/2) \cdot e^{i\varphi}$.



Договоримся эти углы воспринимать как сферические углы: ϑ — угол между заданным направлением и осью z системы координат, а φ — угол между осью x и проекцией этого направления на плоскость x y . Тогда можно изображать состояния кубита точками на сфере единичного радиуса (ее называют *сферой Блоха*), или векторами, проведенными из центра сферы в соответствующие точки. Например, сами базисные состояния $|0\rangle$ и $|1\rangle$ изображаются единичными векторами, идущими по оси z и против нее. В качестве примера на рисунке также показано состояние

$$|A\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle.$$

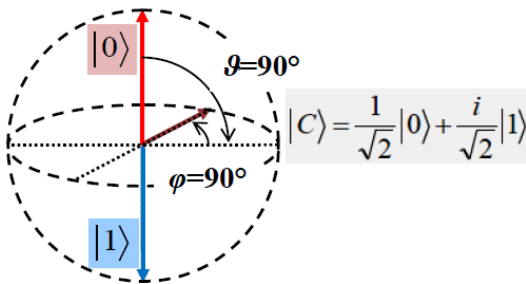
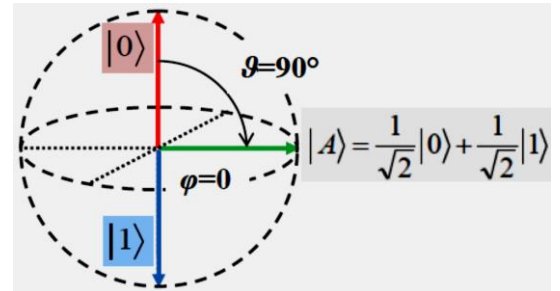
В состоянии при измерении кубита в базисе ($|0\rangle, |1\rangle$), т.е. при взаимодействии кубита с прибором, отправляющим его в одно из этих состояний, вероятности получить 0 или 1 равны по $\frac{1}{2}$ (по 50 %).

Как видно, на сфере Блоха такому состоянию отвечает точка, сферические углы которой равны $\vartheta=90^\circ$ и $\varphi=0^\circ$. Действительно, в этом случае

$$\alpha = \cos(45^\circ) = \frac{1}{\sqrt{2}} \text{ и } \beta = \sin(45^\circ) \cdot e^0 = \frac{1}{\sqrt{2}}.$$

Отметим, что (в соответствии с формулой Эйлера, из которой следует $e^{i\varphi} = \cos(\varphi) + i \cdot \sin(\varphi)$) углы $\varphi \neq 0, 180^\circ$ отвечают комплексным значениям β . Например, углы $\vartheta=90^\circ$ и $\varphi=90^\circ$ отвечают значениям коэффициентов

$$\alpha = \cos(45^\circ) = \frac{1}{\sqrt{2}} \text{ и } \beta = \sin(45^\circ) \cdot e^{i\pi/2} = \frac{1}{\sqrt{2}} \cdot (\cos(90^\circ) + i \cdot \sin(90^\circ)) = \frac{i}{\sqrt{2}}.$$



Поэтому они «кодируют» состояние

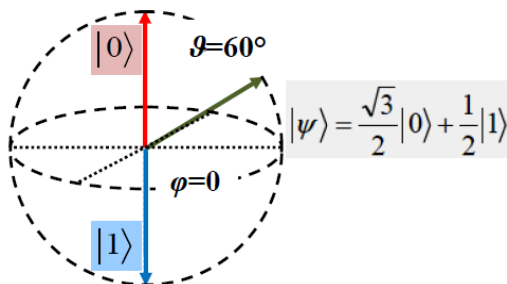
$$|C\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle.$$

В качестве еще одного примера приведем случай $\vartheta=60^\circ$ и $\varphi=0^\circ$, для которого

$$\alpha = \cos(30^\circ) = \frac{\sqrt{3}}{2}, \quad \beta = \sin(30^\circ) \cdot e^0 = \frac{1}{2}$$

Соответствующий вектор состояния, который показан на рисунке, записывается в виде

$$|\psi\rangle = \frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle.$$



Вспомним, что у квантовой системы существует множество величин, доступных измерению. Мы можем сконструировать разные приборы, которые при взаимодействии с кубитом будут отправлять его в одно из пары базисных состояний. Это значит, что таких пар неограниченное количество. На диаграмме Блоха они всегда изображаются парой единичных векторов, направленных в разные стороны (подобно $|0\rangle$ и $|1\rangle$).

В частности, такой базис образуют вектора

$$|A\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \text{ и } |B\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle.$$

Следует обратить внимание, что измерение в базисе ($|A\rangle, |B\rangle$) — взаимодействие кубита с «новым» прибором — можно выполнить в любом состоянии этого кубита. А разобранный нами математический аппарат позволяет предсказывать вероятности разных исходов измерений. В качестве примера покажем, как предсказать статистику измерений в базисе ($|A\rangle, |B\rangle$) для состояния

$$|\psi\rangle = \frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle?$$

Приведем здесь необходимую выкладку. Сначала, почленно складывая и вычитая выражения

$$|A\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \text{ и } |B\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle,$$

выражаем вектора базиса ($|0\rangle, |1\rangle$):

$$\begin{cases} |A\rangle + |B\rangle = \sqrt{2}|0\rangle \\ |A\rangle - |B\rangle = \sqrt{2}|1\rangle \end{cases} \Rightarrow \begin{cases} |0\rangle = \frac{1}{\sqrt{2}}|A\rangle + \frac{1}{\sqrt{2}}|B\rangle \\ |1\rangle = \frac{1}{\sqrt{2}}|A\rangle - \frac{1}{\sqrt{2}}|B\rangle \end{cases}.$$

Затем подставляем эти выражения в формулу разложения для нужного вектора:

$$|\psi\rangle = \frac{\sqrt{3}}{2\sqrt{2}}(|A\rangle + |B\rangle) + \frac{1}{2\sqrt{2}}(|A\rangle - |B\rangle) = \frac{\sqrt{3}+1}{2\sqrt{2}}|A\rangle + \frac{\sqrt{3}-1}{2\sqrt{2}}|B\rangle.$$

Это позволит для кубита в состоянии $|\psi\rangle$ определить вероятности получения результатов A или B :

$$w_A = \left| \frac{\sqrt{3}+1}{2\sqrt{2}} \right|^2 = \frac{1}{2} + \frac{\sqrt{3}}{4} \approx 0,933, \quad w_B = \left| \frac{\sqrt{3}-1}{2\sqrt{2}} \right|^2 = \frac{1}{2} - \frac{\sqrt{3}}{4} \approx 0,067.$$

Конечно, $w_A + w_B = 1$.

Нам пришлось поработать с формулами, но иначе мы никак не смогли бы выдать *количественные предсказания*. А сейчас мы это сделали, причем использовали для этого хоть и необычные, но достаточно простые по сути математические действия.

Математическое дополнение 2: Возможные базисы и скалярное произведение

Еще немного поговорим о математике. Учащимся школ известно про *скалярное произведение векторов* в «обычном» евклидовом двумерном пространстве. На языке геометрии:

$$(\vec{r}_1 \cdot \vec{r}_2) \equiv |\vec{r}_1| \cdot |\vec{r}_2| \cdot \cos(\gamma), \text{ где } \gamma \text{ — угол между векторами.}$$

Видно, что перпендикулярность векторов означает равенство нулю их скалярного произведения. Эта величина выражается через координаты векторов

$$(\vec{r}_1 \cdot \vec{r}_2) = x_1 x_2 + y_1 y_2.$$

Пара базисных векторов $\vec{e}_x$ и $\vec{e}_y$, ортогональны друг другу, и у них единичная длина. Все эти требования можно записать через скалярное произведение:

$$(\vec{e}_x \cdot \vec{e}_x) = (\vec{e}_y \cdot \vec{e}_y) = 1 \text{ и } (\vec{e}_x \cdot \vec{e}_y) = 0.$$

Ясно, что, кроме $\vec{e}_x$ и $\vec{e}_y$, можно выбрать и другие пары базисных векторов, но важно, чтобы они удовлетворяли этим соотношениям. Тогда они все будут состоять из единичных перпендикулярных векторов.

В пространстве состояний кубита, где координаты — комплексные числа, *скалярное произведение* обычно вводят похожим образом:

$$\langle \psi_1 | \psi_2 \rangle \equiv (\alpha_1)^* \alpha_2 + (\beta_1)^* \beta_2.$$

В этом случае единичность длины вектора тоже запишем через скалярные произведения: $\langle 0|0\rangle = \langle 1|1\rangle = 1$, а базисные вектора будем считать «перпендикулярными» (не по геометрическому образу в диаграмме Блоха, а по скалярному произведению!): $\langle 0|1\rangle = 0$. Нетрудно проверить, что это выполняется для любого базиса. Например,

$$\begin{aligned}\langle A|A\rangle &= \frac{1}{\sqrt{2}} \cdot \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} \cdot \frac{1}{\sqrt{2}} = 1, \\ \langle B|B\rangle &= \frac{1}{\sqrt{2}} \cdot \frac{1}{\sqrt{2}} + \left(-\frac{1}{\sqrt{2}}\right) \cdot \left(-\frac{1}{\sqrt{2}}\right) = 1 \\ \text{и } \langle A|B\rangle &= \frac{1}{\sqrt{2}} \cdot \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} \cdot \left(-\frac{1}{\sqrt{2}}\right) = 0.\end{aligned}$$

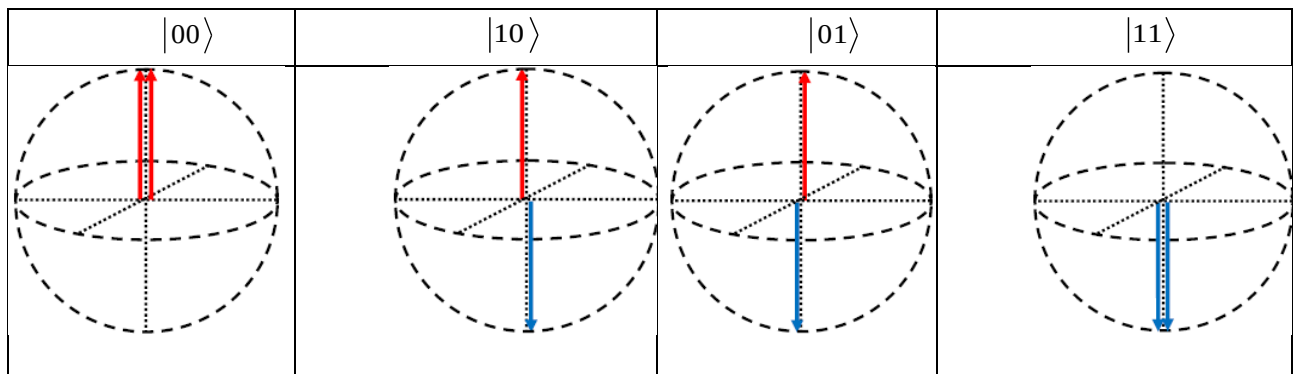
Получается, в двумерном гильбертовом пространстве базис — это тоже пара ортогональных единичных векторов, но только нужно использовать правильное определение ортогональности.

Воспользуемся новыми знаниями, чтобы описать систему из **двух кубитов**. Легко догадаться, что тогда измерения каждого из кубитов в базисе $(|0\rangle, |1\rangle)$ будут отправлять двухкубитовую систему в одно из четырех двухкубитовых состояний: $|00\rangle$, $|01\rangle$, $|10\rangle$ или $|11\rangle$. Так что эти четыре состояния образуют базис для двухкубитовой системы, а произвольное состояние такой системы

$$|\Psi\rangle = \alpha|00\rangle + \beta|10\rangle + \gamma|01\rangle + \delta|11\rangle,$$

где $w_{00} + w_{10} + w_{01} + w_{11} = |\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$.

Теперь снова построим множество двухкубитовых базисов и свяжем с каждым из них процедуру измерения. Только теперь результат измерения — пара символов. Впрочем, при желании мы можем снова использовать один символ, но «пробегающий» четыре значения. Изобразим двухкубитовый базис на диаграмме Блоха:



Рассуждая аналогично, поймем, что базис в пространстве состояний системы из N кубитов должен состоять из 2^N состояний.

Но среди допустимых состояний системы из нескольких кубитов есть такие, в которых состояние одного из кубитов может быть связанным с состоянием других. Такие состояния называют **запутанными**. Рассмотрим конкретный пример для двухкубитовой системы.

Самое естественное выделенное направление для фотона — это направление его движения. У фотонов есть спин (собственный момент количества движения). В стандартных единицах $\hbar \equiv h/2\pi$ проекция спина фотона на направление движения может принимать значения ± 1 . Среди частиц микромира существуют π^0 — *мезоны*, спин которых равен нулю.

Эти частицы нестабильны, и основной канал их распада — это распад на два фотона. Если наблюдать такой распад из системы отсчета, в которой до распада π^0 покоился, то суммарный импульс пары фотонов равен нулю:

$$\vec{P}_1 + \vec{P}_2 = 0.$$

Момент импульса системы фотонов — сумма их спинов и орбитального момента, связанного с их движением относительно выбранной СО. Но эти фотоны почти всегда разлетаются вдоль одной прямой (естественно, в разные стороны), так что орбитальный момент равен нулю. В результате, в соответствии с законом сохранения момента импульса в распаде $\pi^0 \rightarrow \gamma\gamma$, сумма спиновых моментов фотонов равна нулю:

$$\vec{S}_1 + \vec{S}_2 = 0!$$

Совместное использование законов сохранения приводит к четкому предсказанию. Если у одного фотона проекция спина на направление движения равна +1, то у другого тоже должна быть +1; если у одного она равна -1, то и у другого -1. Законы сохранения требуют, чтобы оба рожденных в таком распаде фотона имели одинаковые проекции спина на направление движения. Но в реальности до распада выделенных направлений нет, направления полета фотона после распада неизвестно, поэтому для каждого фотона из симметрии понятно, что его состояние — квантовая суперпозиция состояний с проекциями ± 1 с равными вероятностями.

Если считать спиновые состояния фотона состояниями кубита (например: $|0\rangle$ отвечает проекции +1, а $|1\rangle$ отвечает проекции -1), то видно, что законы сохранения создали связь между состояниями этих кубитов. При этом состояние пары фотонов, рожденных в распаде π^0 , описывается выражением

$$|\Psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle.$$

Это и есть запутанное состояние.

Отметим, что квантовая запутанность состояния влияет на статистику измерений, несмотря на невозможность «информационного общения» фотонов — ведь они летят со скоростью света в вакууме в разные стороны. Пусть, например, на пути одного из них наблюдатель Алиса (А) установила прибор, измеряющий проекцию спина фотона, а наблюдатель Василий (В) установил такой же прибор на пути второго. При этом В проводил измерение позже А, и в промежутке времени между распадом π^0 и вторым измерением система не взаимодействовала ни с чем, кроме измерительных приборов А и В.

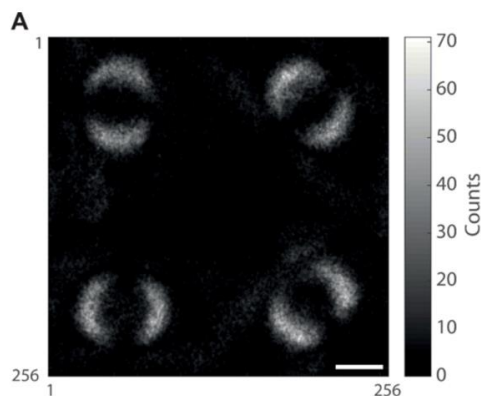
В статистике, собранной по многим парам, А и В должны обнаружить, что каждый из них получает +1 или -1 с равными вероятностями. И в отношении конкретного фотона А не может предсказать результат своего измерения. Но из-за запутанности она всегда знает результат, который получит В для фотона, «парного» к только что измеренному ей. Результат В всегда должен совпадать с результатом А, полученным чуть ранее. Но как фотон, который измерялся В, «узнал», каким должно быть его состояние? Ведь фотон, измеряемый А, перешел в свое состояние только в момент измерения А, а сигнал от А не успел бы дойти до фотона В раньше измерения!

Альберт Эйнштейн считал это «провалом» теории. С его точки зрения совпадение результата В со случайным результатом А означает, что квантовая информация может распространяться быстрее света в вакууме. Ни для какого материального сигнала это невозможно, и Эйнштейн называл это *призрачным дальнодействием*. Квантовая теория утверждает, что сигнал не нужен. Волны вероятности запутанных фотонов не были локализованы — каждый из них мог оказаться и около А, и около В. Только в момент

измерения А произошел коллапс волн вероятности и определилось, к какому наблюдателю попадет каждый фотон. Так что быстрее света движутся границы областей локализации фотонов. Реальные измерения по этой схеме подтвердили правильность предсказаний квантовой теории.

Более того — измерения с реальными запутанными кубитами указывают: квантовая информация иногда передается практически мгновенно! Как видно, введение в квантовую теорию вероятностных законов нарушает классический принцип причинности, в том числе и в этом отношении.

Известный пример проявления квантовой запутанности состояний фотонов представлен на фотографии (рис.), взятой из открытых источников. Ее часто называют «первым фото квантовой запутанности».



Мы видим «пятнышки» на фотопластинке, которые получились при попадании на нее пучков фотонов, запутанных по состоянию поляризации. В этом случае

$$|\Psi\rangle = \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle,$$

причем $|0\rangle$ отвечает поляризации по оси x , а $|1\rangle$ — по оси y .

Установка сделана так, что положение темной полосы на «пятнышке» указывает на положение плоскости поляризации. В левой части фотографии мы видим отметки пучков, на которые в пути от места рождения до фотопластинки не производили никаких воздействий. Заметим, что поляризации фотонов пучков взаимно-перпендикулярны. В правой части фотографии картина изменилась, потому что фотоны одного пучка подверглись воздействию, которое повернуло плоскость их поляризации на некий угол. Обратите внимание: плоскости поляризации двух пучков остались перпендикулярны, но у второго пучка плоскость повернулась на такой же угол, хотя никакого воздействия на него не было!

Можно ли использовать квантовую запутанность для совершенствования технологий работы с информацией? Да. Причем в учебниках по квантовой информатике есть множество примеров такого «усовершенствования». Я ограничусь лишь двумя, наиболее известными.

Пример 1: *Плотное кодирование* информации с помощью запутанных кубитов.

Пусть А должна передать В два бита классической информации по «почте», которая позволяет пересылать носители информации. Если в распоряжении А и В есть «классическая почта», позволяющая пересылать классические биты, то А, естественно, придется отправить две «посылки». Можно ли обойтись одной «посылкой», если в их распоряжении оказалась «квантовая почта», по которой можно пересылать кубиты? Для этого наши герои могут воспользоваться следующим алгоритмом действий.

- А и В заранее приготовили пару запутанных кубитов в состоянии

$$|I\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \text{ и «поделили» ее (т.е. при удалении друг от друга у каждого}$$

остался один кубит, но им удалось сохранить двухкубитную систему от внешних воздействий, меняющих состояние).

- А воздействует на свой кубит, изменяя его состояние одним из четырех способов:

$$\text{I. Ничего не делает, и пара кубитов остается в состоянии } |I\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle.$$

II. Воздействует так, чтобы $|0\rangle \rightarrow |1\rangle$, а $|1\rangle \rightarrow |0\rangle$,

и тогда конечное состояние пары $|II\rangle = \frac{1}{\sqrt{2}}|10\rangle + \frac{1}{\sqrt{2}}|01\rangle$.

III. Воздействует так, чтобы $|0\rangle \rightarrow -|1\rangle$, а $|1\rangle \rightarrow |0\rangle$,

и тогда конечное состояние пары $|III\rangle = -\frac{1}{\sqrt{2}}|10\rangle + \frac{1}{\sqrt{2}}|01\rangle$.

IV. Воздействует так, чтобы $|0\rangle \rightarrow |0\rangle$, а $|1\rangle \rightarrow -|1\rangle$,

и тогда конечное состояние пары $|IV\rangle = \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle$.

Отметим, что $|I - IV\rangle$ образуют базис в пространстве состояний двухкубитовой системы — у всех этих четырех векторов единичная длина и они «перпендикулярны» (их скалярные произведения равны нулю).

- А пересылает свой кубит В одной посылкой по квантовой почте, и у В есть двухкубитовая система.
- В измеряет двухкубитовую систему в базисе $|I - IV\rangle$, и узнает, какое из четырех чисел I-IV сообщила ему А. Два бита классической информации переданы.

Отметим важное обстоятельство, связанное с этим алгоритмом: мы считаем, что входящие в него воздействия, которые производит А, осуществимы. Более того, считаем, что в процессе изменений состояния при таких воздействиях квантовая информация «не теряется». Хотя базисные состояния меняются, коэффициенты разложения вектора по ним остаются прежними!

В квантовой информатике считается, что осуществление подобных операций — «дело физиков», и на практике они действительно производятся над реальными квантовыми системами. Мы вернемся к этому вопросу в следующем разделе.

Пример 2: *Квантовая телепортация* информации о состоянии кубита.

Если мы слышим слова «квантовая телепортация», то иногда вспоминаем



фантастические фильмы, в которых герои прыгают в некий «портал», и оказываются в другом времени, в другой галактике, другой Вселенной. Есть нечто подобное в реальном мире? Удивительно, но сегодня мы уже умеем телепортировать квантовую информацию.

Рассмотрим следующую ситуацию.

Пусть, как и в предыдущем примере, А и В заранее приготовили пару запутанных кубитов в

состоянии $|I\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ и «поделили» ее.

Но теперь некто приготовил свой кубит (далее мы будем называть его «телепортируемым кубитом») в произвольном состоянии $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, причем А и В не знают, какое конкретно это состояние. Этот кубит прислан А по квантовой почте, и она должна отправить его В, но тот находится «слишком далеко», и квантовая почта не может доставить кубит от А к В. Тем не менее существуют алгоритмы, позволяющие выполнить задачу.

Рассмотрим один из них.

- А «присоединяет» телепортируемый кубит к имеющейся системе запутанных кубитов и получает трехкубитовую систему в состоянии

$$|\psi_I\rangle = \frac{\alpha}{\sqrt{2}}|000\rangle + \frac{\alpha}{\sqrt{2}}|011\rangle + \frac{\beta}{\sqrt{2}}|100\rangle + \frac{\beta}{\sqrt{2}}|111\rangle.$$

- А измеряет доступную ей пару кубитов (телепортируемый + ее половинка запутанной пары) в базисе $|I - IV\rangle$.

Чтобы понять, какой получится результат, необходимо переписать формулу для трехкубитового состояния так, чтобы на первых двух позициях находились двухкубитовые базисные состояния, соответствующие измерению. Посмотрев на выражения состояний базиса $|I - IV\rangle$ в примере 1, мы увидим, как из них комбинируются имеющиеся. В самом деле:

$$\begin{cases} |00\rangle = \frac{1}{\sqrt{2}}|I\rangle + \frac{1}{\sqrt{2}}|IV\rangle \\ |01\rangle = \frac{1}{\sqrt{2}}|II\rangle + \frac{1}{\sqrt{2}}|III\rangle \\ |10\rangle = -\frac{1}{\sqrt{2}}|II\rangle + \frac{1}{\sqrt{2}}|III\rangle \\ |11\rangle = \frac{1}{\sqrt{2}}|I\rangle - \frac{1}{\sqrt{2}}|IV\rangle \end{cases}.$$

Подставляя это в нашу формулу, находим, что

$$|\psi_I\rangle = \frac{\alpha}{2}|I\rangle|0\rangle + \frac{\alpha}{2}|IV\rangle|0\rangle + \frac{\alpha}{2}|II\rangle|1\rangle + \frac{\alpha}{2}|III\rangle|1\rangle - \frac{\beta}{2}|II\rangle|0\rangle + \frac{\beta}{2}|III\rangle|0\rangle + \frac{\beta}{2}|I\rangle|1\rangle - \frac{\beta}{2}|IV\rangle|1\rangle.$$

Остается привести подобные, т.е. собрать слагаемые с одинаковыми базисными векторами для кубитов, доступных А:

$$|\psi_I\rangle = \frac{1}{2}|I\rangle(\alpha|0\rangle + \beta|1\rangle) + \frac{1}{2}|II\rangle(-\beta|0\rangle + \alpha|1\rangle) + \frac{1}{2}|III\rangle(\beta|0\rangle + \alpha|1\rangle) + \frac{1}{2}|IV\rangle(\alpha|0\rangle - \beta|1\rangle).$$

Измерение «загоняет» пару кубитов, доступную А, в одно из четырех базисных состояний с вероятностью $\frac{1}{4}$. Состояние кубита В однозначно определяется по результату измерения. Эта связь для удобства восприятия представлена в таблице.

результат А	состояние кубита В
I	$\alpha 0\rangle + \beta 1\rangle$
II	$-\beta 0\rangle + \alpha 1\rangle$
III	$\beta 0\rangle + \alpha 1\rangle$
IV	$\alpha 0\rangle - \beta 1\rangle$

А высылает В по «обычной» линии связи результат своего измерения, и В узнает, каким стало состояние его кубита.

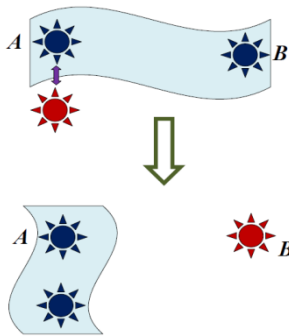
В точно знает, что ему нужно сделать со своим кубитом, чтобы он стал «точной копией» телепортируемого до начала процедуры. И он это делает:

результат А	действия В
I	ничего
II	воздействует так, чтобы $ 0\rangle \rightarrow - 1\rangle$, а $ 1\rangle \rightarrow 0\rangle$
III	воздействует так, чтобы $ 0\rangle \rightarrow 1\rangle$, а $ 1\rangle \rightarrow 0\rangle$

И в итоге свершается небольшое чудо: кубит В оказывается в состоянии телепортируемого кубита

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle.$$

Отметим: А, которая выполнила почти всю работу, даже не знает, что это было за состояние — у нее эта информация уничтожилась измерением. Если некий «злоумышленник» подключится к линии связи А и В и получит сообщение А, он тоже ничего не узнает о состоянии телепортируемого кубита. Потому что без «второй половины» начальной запутанной пары, которая есть у В, это невозможно.



Эта процедура в квантовой информатике и называется **квантовой телепортацией информации о состоянии кубита**.

Отметим два важных обстоятельства.

Во-первых, эффект ярче, чем кажется на первый взгляд: в квантовой теории два фотона в одинаковом состоянии нельзя отличить друг от друга с помощью измерений. Поэтому, хотя на самом деле мы телепортировали не реальную частицу, а только квантовую информацию, все последующие действия В с полученным фотоном по результату совершенно не отличаются от «реальной телепортации».

Во-вторых, все не так просто: хотя «управляемый со стороны А» переход кубита В в «почти правильное» состояние произошел мгновенно (в тот же момент, когда А выполняла измерение), полная длительность процедуры не ноль. Она включает доставку от А к В обычного сигнала с результатом измерения А, которая не может происходить со скоростью, превышающей скорость света в вакууме.

Особо отметим, что описанная процедура уже многократно проводилась на практике в реальных установках. По сообщениям различных лабораторий, удавалось «перебросить» информацию о состоянии фотона на вполне макроскопические расстояния — до 10 метров.

Однако до телепортации реальных предметов еще очень и очень далеко. Ведь для этого нужно «разобрать» предмет на элементарные квантовые частицы, телепортировать каждую из них, а затем (самое сложное!) «собрать» предмет обратно.

Перечислим основные **выводы** этого раздела.

Квантовая ячейка для записи информации — кубит — намного более «емкая», чем классический бит. Квантовая информация не локализована в месте, где мы обнаруживаем ее носителей, и мы можем создавать «запутанные ячейки», у которых состояние каждой может измениться мгновенно при воздействии на одну из них, независимо от расстояний между «ячейками». Есть методы воздействия, позволяющие изменять состояния «ячеек» нужным нам образом, не влияя на содержащуюся в них информацию. Мы можем извлекать нужную нам информацию, производя измерение, что неминуемо меняет состояние системы кубитов. Впрочем, такое изменение иногда происходит и независимо от нас из-за неконтролируемого взаимодействия системы с внешним миром. Одна из самых сложных технологических задач — «уберечь» наши носители информации от такого взаимодействия. Поведение систем кубитов просчитывается на базе квантовых законов, но нужно учитывать, что все наши выводы относительно событий будут выводами о вероятностях их наступления.

Квантовые компьютеры и квантовая криптография

Одно из самых интересных приложений теории информации — возможность автоматического проведения *вычислений*. Соответствующие устройства — «*вычислители*» — мы называем компьютерами. Какими они станут, если их процессоры будут функционировать по законам квантовой физики? На самом деле, конечно, привычные нам электронные устройства уже активно используют квантовые свойства частиц. Например, мы часто управляем туннельными переходами электронов. Но все же в этом случае мы работаем с «большим количеством» квантовых частиц, так что вероятностный характер квантовых законов проявляется только статистически.

Настоящий *квантовый компьютер* должен использовать вероятностные законы непосредственно в алгоритмах действий. Например, его процессор может стать системой *запутанных кубитов*. Конечно, кубит — простейшая квантовая система, существуют и более сложные устройства. Однако с точки зрения математика, многие сложные квантовые системы допустимо описывать с помощью тех же *формул*, что и систему большого числа кубитов. Так что мы можем считать, что работа любого квантового компьютера может быть описана как процесс, происходящий с системой кубитов.

Одним из первых идею использования квантовых систем для вычисления высказал Ричард Фейнман. Рассказывают, что она возникла при решении обратной задачи — задачи моделирования поведения квантовых систем на классическом компьютере. Оказалось, что даже для простых систем (N кубитов при «не очень большом» N) модели получались сложными для анализа. Фейнман указал: это означает, что решение сложных моделей возможно получить на основе наблюдения за простой системой запутанных кубитов. Это и есть базовая идея *квантового компьютеринга*: результат вычисления нужной величины должен получаться *измерением* над такой системой.

Чтобы понять, как будет реализовываться процесс квантовых вычислений, обсудим, какие действия можно производить над системой кубитов. Начнем с одного квантового бита. Его состояние описывается как квантовая суперпозиция базисных состояний

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

в которой коэффициенты — комплексные числа. Это позволяет описывать в общем виде интерференцию соответствующих волн вероятности. Напомним, что для каждого кубита можно выбрать бесконечное количество базисов, и каждый из них отвечает одной из возможных измерительных процедур, которые различают эти состояния. Поэтому выбор базиса — это выбор прибора для измерения кубита. С течением времени состояние кубита может меняться, причем изменение зависит от воздействий на него. Казалось бы, трансформации состояния могут быть какими угодно, но на самом деле важно различать два их вида.

1) Изменения, в которых *сохраняется квантовая когерентность состояния*. Это выражение означает, что потери информации о предыдущем состоянии не происходит. В этом случае

$$|\psi(t)\rangle = \alpha(t)|0\rangle + \beta(t)|1\rangle,$$

где функции $\alpha(t)$ и $\beta(t)$ достаточно регулярны и в любой момент времени удовлетворяют условию нормировки вероятности

$$|\alpha(t)|^2 + |\beta(t)|^2 \equiv 1.$$

Напомним смысл этого условия: вероятность обнаружить кубит в «каком-нибудь» из двух базисных состояний равна 100% в любой момент времени.

Такое изменение состояния в информатике называют *унитарной операцией*. Разберемся, как это выглядит с точки зрения физика-теоретика, стараясь обходиться без формул везде, где это возможно.

На самом деле теоретик описывает изменение состояния кубита, решая дифференциальные уравнения квантовой теории на коэффициенты $\alpha(t)$ и $\beta(t)$. Если он знает, как описать зависимость энергии взаимодействия кубита с внешними телами от времени, он может по «начальным» значениям коэффициентов $\alpha(t_0)$ и $\beta(t_0)$ (заданным в любой момент времени t_0) определить их значения в любой момент времени. Тогда смена состояния кубита в известных внешних условиях, которые изменяются без «скачков» и «сингулярностей» (обращений энергии взаимодействия в бесконечность), — это *унитарная операция*. При этом наш теоретик всегда может подобрать некий «новый базис» ($|\tilde{0}(t)\rangle, |\tilde{1}(t)\rangle$), в котором состояние в момент времени t будет записывать как квантовую суперпозицию новых базисных векторов с прежними коэффициентами:

$$|\psi(t)\rangle = \alpha(t_0)|\tilde{0}(t)\rangle + \beta(t_0)|\tilde{1}(t)\rangle.$$

Таким образом, любую унитарную операцию допустимо математически описать как изменение базиса

$$\begin{cases} |0\rangle \rightarrow |\tilde{0}(t)\rangle \\ |1\rangle \rightarrow |\tilde{1}(t)\rangle \end{cases}.$$

И наоборот — любое изменение базиса может быть реализовано как унитарная операция на промежутке времени от t_0 до t .

Для физика это означает, что для любого реального устройства под любое изменение его состояния, описанное как смена базиса, он может подобрать необходимые внешние условия, в которых с кубитом произойдет именно такая трансформация. Именно поэтому в примерах из раздела о квантовой информатике мы описывали результаты воздействий персонажей на кубиты как изменения базиса.

Для многокубитовых систем все происходит так же, только базисы становятся больше (для системы из N кубитов базис содержит 2^N состояний), а вычисления — более громоздкими.

2) Изменения, в которых происходит *потеря квантовой когерентности*, т.е. «коллапс» состояния с утерей информации. Это не что иное как *измерения*. В физике это взаимодействие кубита с макроскопическим *измерительным прибором*, в результате которого кубит отправлен в одно из состояний, принадлежащих базису этого прибора.

Вспомним: состояние кубита перед измерением влияет на вероятности его попадания в одно из базисных состояний. Для определения всех этих вероятностей необходимы результаты многократных однотипных измерений. При одиночном измерении над одним кубитом мы узнаем только результат измерения — состояние, в которое он попал, и почти ничего не узнаем, что с ним происходило до измерения. Поэтому мы и говорим о «коллапсе» состояния.

Теперь мы можем четко указать, как реализуется *квантовое вычисление*. Необходимо:

- создать систему N кубитов и обеспечить на некоторое время отсутствие «неконтролируемых» внешних воздействий на эту систему;
- поместить систему в условия, в которых контролируемые нами воздействия произведут некоторую унитарную операцию;
- произвести финальное измерение, которое выдаст результат вычисления.

Конечно, вычисления бывают и более сложными. Например, когда результат складывается из последовательности шагов, в которых результат предыдущего шага определяет действия на последующих. Но все равно такая задача сводится к осуществлению каждого отдельного шага.

Для физика в первую очередь важны:

- необходимое число N ;
- *время декогеренции* системы τ — это время, на котором «проявится» наличие неконтролируемых внешних воздействий, хотя на самом деле, конечно же, они всегда присущи реальным системам;
- унитарная операция, которую необходимо осуществить;
- величина, которую необходимо измерить.

Он создает конкретные устройства — кубиты — и систему управления ими с помощью контролируемых воздействий за время, не превышающее τ .

Для математика важно придумать «алгоритм» — последовательность вычислений, приводящих к нужному результату. Отметим, что большинство алгоритмов для классических компьютеров не эффективны для квантовых вычислителей. Поэтому математики сейчас интенсивно разрабатывают наборы новых алгоритмов специально для квантовых компьютеров. Так, один из самых известных — *алгоритм Шора* — схема квантового вычисления, которая позволяет разложить число из N знаков в произведение простых множителей. Он может быть реализован в системе из N запутанных кубитов с достаточным временем декогеренции.

Для программиста важно уметь превращать каждый алгоритм в «программу» — последовательность относительно простых («типичных») унитарных операций и измерений.

Наконец, реализация конкретного процесса вычисления — снова задача для физика, который подберет необходимые воздействия на систему для реализации каждой унитарной операции и технологию финального измерения.

Конечно, это только «базовая» задача. Как помним, все уравнения квантовой теории описывают изменения вероятностей исходов всех наших действий. В частности, вероятность получения правильного результата обычно не равна 100%, ведь есть ошибки вычислений из-за квантовых флуктуаций. Кроме того, возникают и «обычные ошибки», когда мы не полностью «заблокировали» неконтролируемые внешние воздействия. Поэтому нам также необходимы процедуры выявления и устранения ошибок. На уровне математики и информатики обычно говорят о разработке *протокола* действий, а на уровне физики — поиск способов «корректировки» ошибок дополнительными воздействиями. Создание таких процедур — важная часть квантовых вычислений.

Многие протоколы выявления и устранения ошибок выполняются с помощью многократного повторения вычисления. Например, если вероятность получения правильного ответа в финальном измерении равна 99%, и вероятность ошибки в 1% для нас «слишком велика», то допустимо просто произвести это вычисление, например пять раз. Тогда, если все попытки выдали один и тот же результат, вероятность случайного совпадения и ошибочности результата равна $(0,01)^5 = 10^{-10}$. Как видим, увеличивая число повторений, можно практически неограниченно уменьшать вероятность ошибки.

Еще одно важное направление квантовых информационных технологий — *квантовая криптография*. В целом криптография — наука о методах шифрования данных, чтобы обеспечить их целостность и конфиденциальность, а также о способах аутентификации легитимных пользователей и защите от вмешательства «злоумышленников». Обычно

криптографические системы занимаются выработкой «ключей» (паролей) и их распределением между легитимными пользователями.

Я не планирую описывать криптографию детально — для этого существуют соответствующая литература и отдельные курсы. Нам интересно обсудить, какие новые возможности создают для криптографии квантовые системы.

Мы уже видели в примерах из рассказа об информатике, что квантовую информацию о состоянии кубита можно передавать на большое расстояние за малое время при использовании квантовой запутанности (особенно показателен пример с квантовой телепортацией). При этом если «злоумышленник» перехватит всю классическую информацию, он все равно не получит передаваемое сообщение ни вместе с легитимным пользователем, ни вместо него. Для этого нужен физический доступ к части запутанной системы кубитов, которая остается в распоряжении легитимного пользователя. Допустим, злоумышленник найдет способ воздействовать на квантовое устройство, которое сохраняет когерентность состояний системы запутанных кубитов. Но максимум, что у него получится в результате — вызвать коллапс ее состояния и тем самым помешать передаче сообщения. Кроме того, разработаны квантовые алгоритмы, позволяющие отправителю и легитимному пользователю обнаружить стороннее вмешательство и скорректировать передачу данных, чтобы его исключить.

Конечно, это чрезвычайно привлекательно для практических приложений — ведь в этом случае секретность передачи данных обеспечивается не сложностью используемых устройств, а законами природы. В некотором смысле квантовая криптография обеспечивает «абсолютное» решение задачи шифрования данных. При этом квантовые компьютеры способны «взломать» практически любой классический шифр, а не только простейший «шифр замены». Так что в перспективе без квантовой криптографии, как единственного надежного способа защиты от «квантового взлома», обеспечить секретность передачи данных станет невозможно.

Например, в современных криптографических системах в качестве «ключа» часто используется разложение длинного числа (из нескольких тысяч знаков) в простые сомножители. Проверка такого пароля — перемножение введенных простых чисел с получением заданного произведения — производится быстро. А его «взлом», т.е. поиск простых сомножителей по известному значению произведения, требует огромного объема вычислений. Для числа знаков $N > 4000$ время решения такой задачи самым совершенным классическим компьютером середины 2020-х годов превышает 10 млрд. лет. Поэтому такой ключ считается надежным. Но для квантового компьютера разработан алгоритм Шора (см. выше), позволяющий эффективно решить эту задачу, используя систему N спутанных кубитов.

Снова наступило время сказать про самое удивительное в этой истории. Квантовая криптография уже давно превратилась из математической теории в науку о реально используемых устройствах. «Квантовые телефоны» и прочие устройства передачи данных с «абсолютной» защитой от неконтролируемого вмешательства злоумышленника уже работают.

Центральный элемент квантовых криптографических систем — устройство, обеспечивающее создание и поддержание когерентности системы запутанных кубитов — *квантовый ретранслятор*. Именно оно ответственно за «телепортацию» квантовой информации.

Как мы помним из разобранных примеров, для реальной передачи информации необходимы также устройства передачи классической информации — протоколов действий

отправителя и результатов его измерений. В этом случае секретность не обязательна, и соответствующая часть системы может остаться «незащищенной территорией». Впрочем, и здесь иногда используются квантовые устройства, например, квантовый генератор случайных чисел для создания открытых ключей или лазер для оптоволоконной системы связи. Но это вспомогательные части системы, а не те, что обеспечивают ее уникальные криптографические свойства.

