Классические и квантовые вычисления

А. Китаев; написал М. Вялый

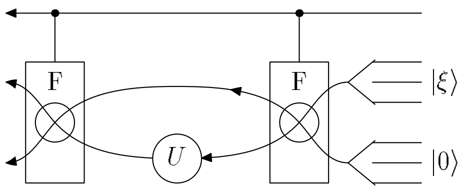
10 лекция (16/04/98)

Квантовые алгоритмы (продолжение)

По поводу рассказанного в прошлый раз алгоритма возникает ряд естественных вопросов. Начнем с ответов на них.

— *Можно ли находить собственные числа других операторов так же, как в алгоритме вычисления периода?*

Можно находить собственные числа таких операторов U, для которых $U|0\rangle = |0\rangle$ и есть полиномиальная схема реализации оператора $\Lambda(U)$. Если для самого оператора U есть полиномиальная схема, то для оператора $\Lambda(U)$ ее также можно построить, используя *элемент Фредкина* — управляемый обмен битами. Элемент Фредкина задается соотношениями



$$|a, b, c\rangle \mapsto \begin{cases} |0, b, c\rangle & \text{если } a = 0 \\ |1, c, b\rangle & \text{если } a = 1 \end{cases}$$

На врезке показано, как из схемы для U, сохраняющего $|0\rangle$, построить схему для $\Lambda(U)$. В прямоугольниках происходит управляемый обмен q-битами (параллельно действует нужное количество элементов Фредкина). Если управляющий q-бит равен $|1\rangle$, то на вход схемы, вычисляющей U будет подан $|\xi\rangle$, в противном случае — $|0\rangle$.

Точность определения собственных чисел произвольного оператора невелика, полиномиально зависит от размера схемы. Если можно эффективно вычислять степени оператора (как и было в рассмотренном в прошлый раз алгоритме), то точность можно сделать экспоненциальной.

— *Какие собственные числа мы находим?*

Мы находим значение случайно выбранного собственного числа. Распределением по множеству всех собственных чисел можно управлять, выбирая начальное состояние (в алгоритме вычисления периода — $|1\rangle$). Взяв начальным состояние, задаваемое диагональной матрицей плотности $\rho = \frac{1}{t}\sum\limits_a |a\rangle\langle a| = \frac{1}{t}\sum\limits_k |\xi_k\rangle\langle\xi_k|$ (где $|\xi_k\rangle$ пробегает множество собственных векторов U), получим равномерное распределение на множестве всех собственных чисел. В алгоритме нахождения периода начальное состояние выбиралось *иначе*: мы выбирали такой вектор, чтобы получить равномерное распределение на собственных числах, соответствующих определенной орбите, остальные собственные значения не порождались.

— *Какие еще примеры квантовых алгоритмов известны?*

Это хороший вопрос. На самом деле, таких алгоритмов известно довольно мало. Фактически, есть три существенно различных случая:

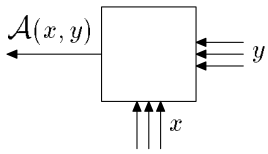
1) задача о построении стабилизатора действия абелевой группы (она включает в себя и задачу о вычислении периода, и задачу нахождения дискретного логарифма);

2) моделирование квантово-механических систем;

3) общая переборная задача (в оракульной постановке).

Рассмотрим все эти три случая.

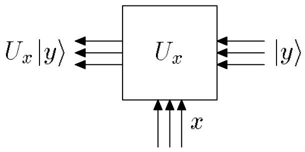
Общая переборная задача (квантовый поиск)



Пусть имеется устройство, которое по входам x и y определяет значение некоторого предиката $\mathcal{A}(x,y)$ (оно изображено на врезке). Нас интересует предикат $F(x) = \exists\, y \mathcal{A}(x,y)$. Это похоже на определение класса $\mathcal{NP}$, но сейчас нам недоступна внутренняя структура устройства, вычисляющего предикат $\mathcal{A}$. Вычислить в таких условиях значение предиката $F(x)$ на классическом компьютере нельзя быстрее чем за $K = 2^n$ шагов (n — количество бит в записи y).

Оказывается, что на квантовом компьютере можно вычислить значение предиката $F(x)$ и даже найти y, на котором выполнено $\mathcal{A}(x,y)$, за время $O(\sqrt{K})$. Получены также и нижние оценки (по порядку такие же), показывающие, что в этой постановке квантовые устройства дают лишь полиномиальное ускорение по сравнению с классическими.

В квантовой постановке задача выглядит так. Вход x по-прежнему классический, но сам "черный ящик" — квантовое устройство, и вход y (варианты ответа) мы будем считать квантовым. Поэтому наш оракул (или "черный ящик") задает оператор U_x, действующий по правилу



$$U_x|y\rangle \;=\; \begin{cases} \;\;|y\rangle & \text{если } \mathcal{A}(x,y)=0 \\ -|y\rangle & \text{если } \mathcal{A}(x,y)=1 \end{cases} .$$

Нужно вычислить значение $F(x)$ и найти "ответ" y (при котором выполнен $\mathcal{A}(x,y)$).

Результаты, о которых уже упоминалось, формулируются так: *Существуют две константы C_1 и C_2 такие, что есть схема размера $\le C_1\sqrt{K}$, решающая любую задачу указанного вида; а для любой схемы размера $\le C_2\sqrt{K}$ существует задача, которая не решается не этой схеме (то есть схема дает неправильный ответ с вероятностью $> 2/3$.*

Мы разберем упрощенную постановку: считаем, что "ответ" существует и единствен, обозначим его через y_0; нужно найти y_0. Схема, которую мы для этого построим, будет примером "прямого" квантового вычисления; она будет описана в терминах преобразований базисных векторов.

Рассмотрим два оператора:

$$U = I - 2|y_0\rangle\langle y_0| \quad \text{и еще один}$$

$$V = I - 2|\xi\rangle\langle\xi| \quad \text{где } |\xi\rangle = \frac{1}{\sqrt{K}}\sum_y |y\rangle, \quad \text{так что } V = \begin{pmatrix} 1-\frac{2}{K} & \dots & -\frac{2}{K} \\ \vdots & \ddots & \vdots \\ -\frac{2}{K} & \dots & 1-\frac{2}{K} \end{pmatrix}.$$

Оператор U нам задан (это оракул), построим квантовую схему, вычисляющую V. Действовать будем так: переведем $|\xi\rangle$ в $|0\rangle$, а затем реализуем аналогично U, но с известным $y_0 = 0$.

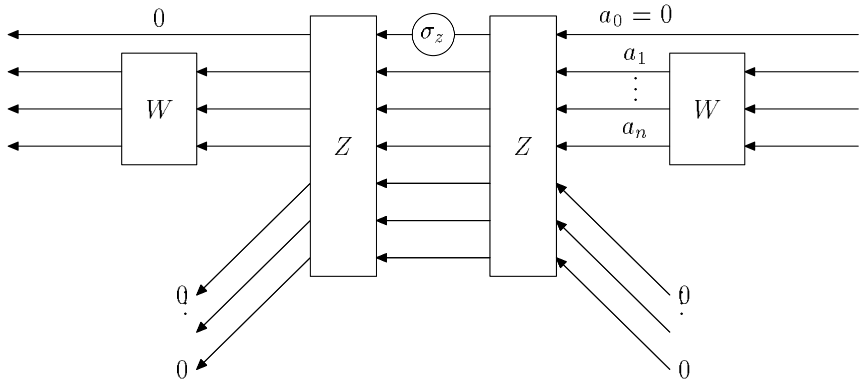
Сначала построим оператор W, который переводит $|\xi\rangle$ в $|0^n\rangle$ (напомним, что $K = 2^n$). Это просто, $W = \underbrace{S\otimes S\otimes\dots\otimes S}_{n\,\text{раз}}$, где $S = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. Действительно, $|\xi\rangle = \frac{1}{\sqrt{2^n}}\left(|0\rangle + |1\rangle\right)^{\otimes n}$, а $S : \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \mapsto |0\rangle$.

Нам потребуется реализация оператора $Y = I - 2|0^n\rangle\langle 0^n|$. Чтобы ее построить, используем обратимую (классическую) схему, реализующую оператор $Z : \{0,1\}^{n+1} \to \{0,1\}^{n+1}$,

$$\begin{aligned} Z|a_0,\ldots,a_n\rangle &= |a_0 \oplus f(a_1,a_2,\ldots,a_n), a_1,\ldots,a_n\rangle; \\ f(a_1,\ldots,a_n) &= \begin{cases} 1, & \text{если } a_1 = \cdots = a_n = 0, \\ 0, & \text{если } \exists\, i : a_i \neq 0 \end{cases} . \end{aligned}$$

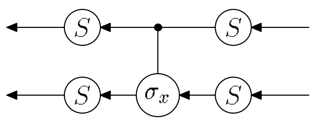
(В обозначениях, введенных на первой лекции, $Z = \hat{f}_\oplus$). Поскольку f имеет малую схемную сложность (в обычном смысле), по общей теореме, доказанной ранее, для существует небольшая схема, вычисляющая Z, в которой “берутся напрокат” дополнительные регистры с 0.

Теперь можно изобразить схему, реализующую оператор V. Центральная часть, включающая в себя Z, σ^z и Z, реализует оператор Y. В схеме используется оператор $\sigma^z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Физически σ^z соответствует действию магнитного поля, направленного вдоль оси z.



Заметим, что $W^2 = \mathrm{id}$, $Z^2 = \mathrm{id}$ по крайней мере на векторах с нулевыми значениями битов, взятых напрокат. Поэтому решающее действие оказывает оператор σ^z, действующий на q-бит, который также не меняется после всего вычисления.

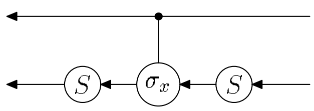
Не нужно смущаться тем, что σ^z действует только на “управляемый” q-бит, а меняется в результате весь вектор. Вообще, различие между “чтением” и “записью” в квантовом случае неабсолютно и зависит от выбора базиса. Приведем соответствующий пример.



Напишем матрицу $\Lambda(\sigma^x) : |a,b\rangle \mapsto |a, a\oplus b\rangle$ в базисе $\frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ для каждого из бит. Другими словами, запишем матрицу для оператора $X = (S\otimes S)\ \Lambda(\sigma^x)\ (S\otimes S)$. Схема для этого оператора изображена на врезке. Вычисление будем производит последовательно $X|a,b\rangle = \frac{1}{2}(S\otimes S)\,\Lambda(\sigma^x)\sum\limits_{c,d}(-1)^{ac+bd}|c,d\rangle$. Поскольку $\Lambda(\sigma^x)|c,d\rangle = |c, c\oplus d\rangle$, можно записать

$$X|a,b\rangle = \frac{1}{2}(S\otimes S)\sum_{c,d}(-1)^{ac+bd}|c, c\oplus d\rangle = \frac{1}{4}\sum_{\alpha,\beta,c,d}(-1)^{\alpha c+\beta(c+d)}(-1)^{ac+bd}|\alpha,\beta\rangle =$$
$$\frac{1}{4}\cdot 2\delta_{b,\beta}\cdot 2\delta_{a,(\alpha+\beta)}\sum_{\alpha,\beta}|\alpha,\beta\rangle = |a\oplus b, b\rangle.$$

Итак, в этом базисе управляющий и управляемый биты поменялись местами. Какой бит “управляющий”, или какой “читается”, зависит от выбора базиса. Разумеется, такое положение дел противоречит нашей классической интуиции. Трудно представить, как при переходе к другому базису квантовый принтер вдруг становится квантовым сканнером.

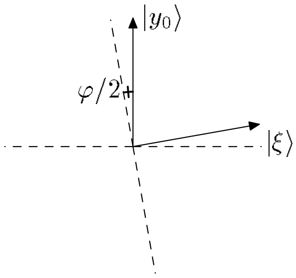


Задача. Что будет, если изменить базис только в одном бите? Например, как будет выглядеть матрица оператора, схема которого изображена на врезке? Можно также поменять базис в другом бите.

Вернемся к построению схемы для универсальной переборной задачи. Оракул $U = I - 2|y_0\rangle\langle y_0|$ нам задан, и мы реализовали оператор $V = I - 2|\xi\rangle\langle\xi|$. Теперь с помощью этих двух операторов построим из вектора $|\xi\rangle = W|0^n\rangle$ искомый вектор $|y_0\rangle$. Для этого будем поочередно действовать операторами V, U:

$$\ldots V\,U\,V\,U\,|\xi\rangle = (VU)^s|\xi\rangle.$$

Что при этом получается? Геометрически оба оператора есть отражения относительно гиперплоскости. Подпространство $\mathcal{L} = (|\xi\rangle, |y_0\rangle)$ инвариантно относительно обоих операторов, а, значит, и относительно VU. Поскольку мы стартуем из вектора, принадлежащего этому подпространству, ограничимся действием VU на нем.



Композиция двух отражений относительно двух прямых есть поворот на удвоенный угол между этими прямыми. Угол легко вычислить, $\langle\xi|y_0\rangle = \dfrac{1}{\sqrt{K}} = \sin\dfrac{\varphi}{2}$. Т. е. эти прямые почти перпендикулярны, поэтому можно написать $VU = -R$, где R — поворот на малый угол φ. Но тогда $(VU)^s = (-1)^s R^s$, где R^s – поворот на угол $s\varphi$. Знак нас не интересует (фазовый множитель не изменит вероятностей, поскольку он по модулю равен 1). При больших K $\varphi \sim \dfrac{2}{\sqrt{K}}$. Тогда после $s \approx \dfrac{\pi}{4}\sqrt{K}$ итераций исходный вектор повернется на угол $s\varphi \approx \dfrac{\pi}{2}$ и станет близок к искомому вектору.

Если решается общая переборная задача (т. е. ответов может быть несколько, а может не быть вообще), требуются дополнительные технические ухищрения. Число шагов для поворота от исходного вектора к какому-нибудь вектору из подпространства, порожденного векторами ответов, обратно пропорционально корню из числа решений. Заметим, что точность (величина угла φ) при увеличении числа решений падает.

Универсальная квантовая схема и квантовые алгоритмы

“Моделирование квантовомеханических систем” — нечетко поставленная задача, так как большую роль в ней играет выбор конкретной системы и выделение “существенных” степеней свободы. С математической точки зрения, можно говорить о моделировании квантовых схем.

Квантовые схемы имеют конструктивное описание, если указать точность, с которой известны матричные элементы операторов, входящих в схему. Пусть есть описание квантовой схемы Z, размера $\le L$ и точности δ. Обозначим оператор, реализуемый этой схемой, через $Op(Z)$.

Можно построить *универсальную квантовую схему* размера $poly(L, \log\frac{1}{\delta})$, реализующую оператор U со следующим свойством:

$$\Big|U(|Z\rangle \otimes |\xi\rangle) - |Z\rangle \otimes Op(Z)|\xi\rangle\Big| \le cL\delta.$$

До сих пор у нас были неоднородные вычисления (вычислялись булевы функции), нужно также иметь возможность вычислять функции на словах произвольной длины (алгоритмы). Определение квантового алгоритма можно дать, используя уже введенные квантовые схемы. Пусть есть функция $P : \{0,1\}^* \to \{0,1\}^*$, длина результата — полином от длины входа. Ей сопоставляется последовательность булевых функций (ограничения на входы длины n) $F_n : \{0,1\}^n \to \{0,1\}^{m(n)}$. *Квантовый алгоритм* для вычисления P — это однородная последовательность схем, вычисляющих F_n. “Однородная” означает, что по n можно построить описание соответствующей схемы на обычной полиномиально ограниченной машине Тьюринга.

Можно определить квантовую машину Тьюринга и непосредственно (первоначальное определение Deutsch'а было именно таким), через суперпозиции различных состояний ленты МТ. Наше определение оказывается эквивалентным.

Задача об абелевом стабилизаторе

Пусть на конечном множестве M действует группа $\mathbb{Z}^k$. Будем предполагать, что по $g = (m_1, \dots, m_k) \in \mathbb{Z}^k$ и $x \in M$ результат действия $F(g,x) \in M$ вычислим за время $poly(\log|M| + \sum_j \log(|m_j|+1))$. Для определенности можно считать, что $M = \{0,1\}^n$. Естественно, функция F удовлетворяет условию $F(g_1, F(g_2, x)) = F(g_1 + g_2, x)$.

Стабилизатором элемента $a \in M$ называется множество $E = St_F(a) = \{g \in \mathbb{Z}^k : F(g,a) = a\}$. Это подгруппа конечного индекса $\leq |M| \leq 2^n$ в $\mathbb{Z}^k$. Следовательно, стабилизатор $\mathrm{St}_F(a)$ изоморфен $\mathbb{Z}^k$ и имеет базис $\{g_1, \dots, g_k\}$ полиномиального размера.

Задача об абелевом стабилизаторе состоит в нахождении какого-нибудь из базисов стабилизатора заданного элемента a.

Задача о вычислении периода является частным случаем задачи о стабилизаторе. Напомним, что $\mathrm{per}_q(a) = \min\{t \geq 1 : a^t \equiv 1 \pmod q\}$. Пусть $M = \{0, \dots, q-1\}$, $F(a,x) = a^m x \pmod q$. Тогда период — это образующая $\mathrm{St}_F(1)$.

Задача о вычислении дискретного логарифма также может быть сведена к задаче о вычислении стабилизатора, там нужно уже рассматривать действие $\mathbb{Z}^2$.

Опишем коротко квантовый алгоритм решения задачи о стабилизаторе. Он аналогичен алгоритму для вычисления периода. Рассматриваются операторы $U_1, \dots, U_k$, соответствующие действию образующих $\mathbb{Z}^k$: $g_1 = (1,0,\dots,0), \dots, g_k = (0,\dots,0,1)$. Эти операторы коммутируют, поэтому у них есть общий базис из собственных векторов, и, значит, можно определять их собственные значения одновременно. Набор собственных чисел $\lambda_1, \dots, \lambda_k$ для этих операторов задает характер группы $\mathbb{Z}^k$, т. е. отображение $\lambda : \mathbb{Z}^k \to U(1)$ такое, что $g = (m_1, \dots, m_k) \mapsto \lambda_1^{m_1} \cdot \ldots \cdot \lambda_k^{m_k} \in U(1)$ (все собственные числа по модулю равны 1).

Если $g \in \mathrm{St}_F(a)$, то $\lambda(g) = 1$. Поэтому процедура измерения собственных чисел порождает случайный характер для группы $E = \mathbb{Z}^k / \mathrm{St}_F(a)$, имеющий вид $(e^{2\pi i \varphi_1}, \dots, e^{2\pi i \varphi_k})$. Вычисление φ_j производится так же, как и в алгоритме вычисления периода. Набрав достаточно много точек, мы с большой вероятностью породим всю группу характеров $H = E^*$. Найти после этого $\mathrm{St}_F(a)$ можно стандартным полиномиальным алгоритмом.