Квантовые компьютеры
часть 1

И.И. Клебанов

доцент, старший научный сотрудник кафедры СП, канд. физ.-мат.наук, доцент

Квантовый компьютер —

вычислительное устройство, которое использует явления квантовой механики (квантовая суперпозиция, квантовая запутанность) для передачи и обработки данных. Квантовый компьютер (в отличие от обычного) оперирует не битами (способными принимать значение либо 0, либо 1), а кубитами, имеющими значения одновременно и 0, и 1.

$$|\psi> = \alpha\ |0> + \beta\ |1>$$

Математический аппарат квантовой механики

Линейное (векторное) пространство – множество элементов X с введёнными на нём операциями сложения элементов $x+y$ и умножения $x\cdot\lambda$ на элемент поля K (в нашем случае поля комплексных чисел). Операции эти должны быть замкнуты (результат должен принадлежать множеству X) и должны выполняться 8 аксиом.

Математический аппарат квантовой механики

В **метрическом пространстве** X для любых элементов $x,y \in X$ определено расстояние $p(x,y)$, которое удовлетворяет требованиям (аксиомам метрического пространства):

- $p(x,y) \geq 0$, при этом $p(x,y) = 0$ тогда и только тогда, когда x и y совпадают;
- $p(x,y) = p(y,x)$
- $p(x,y) \leq p(x,z) + p(z,y)$ – неравенство треугольника

Математический аппарат квантовой механики

В **нормированном пространстве** X для любого элемента $x \in X$ существует вещественное число $||x|| \in R$, называемое его нормой и удовлетворяющее, опять же, трём аксиомам:

- $||x|| \geq 0$, если же $||x||=0$, то $x = 0$ – нулевой элемент;
- $||\lambda \cdot x|| = |\lambda| \cdot ||x||$;
- $||x+y|| \leq ||x|| + ||y||$.

Математический аппарат квантовой механики

Скалярное произведение является функцией, отображающей множество пар

векторов во множество комплексных чисел.

$|\psi> = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$ – кет- вектор

$<\varphi| = (b_1^* \dots b_n^*)$ – бра- вектор

Скалярное произведение $<\varphi|\,\psi> = \sum_{i=1}^{n} b_i^* a_i$

Ортогональные векторы $<\varphi|\,\psi> = 0$

Математический аппарат квантовой механики

Гильбертово пространство является полным нормированным метрическим линейным пространством с нормой

$$\|x\| = \sqrt{< x|x >}$$

Нормированный вектор $\|x\| = 1$

Математический аппарат квантовой механики

Операторы.

$$\hat{A}=\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}$$

$\hat{A}\sum_{i=1}^{n}\lambda_i\cdot|\psi_i>=\sum_{i=1}^{n}\lambda_i\cdot\hat{A}|\psi_i>$ – линейность

$\hat{A}^{+}=\begin{pmatrix} a_{11}^{*} & \cdots & a_{n1}^{*} \\ \vdots & & \vdots \\ a_{1n}^{*} & \cdots & a_{nn}^{*} \end{pmatrix}$ – эрмитово сопряжение

Математический аппарат квантовой механики

Операторы.

$\hat{A} = \hat{A}^{+}$– эрмитов оператор

$\hat{A} \cdot \hat{A}^{+} = \hat{I}$ – унитарный оператор

$\hat{I}$ – единичный оператор

Гейты

Единичный

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Гейт Адамара

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Гейты Паули

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Тензорное произведение

Тензорным произведением двух гильбертовых пространств H_1 и H_2 называется гильбертово пространство, обозначаемое $H_1 \otimes H_2$.

Важные нам свойства:

1. Размерность получившегося пространства равна произведению размерностей исходных пространств: $\dim H_1 \otimes H_2 = \dim H_1 \cdot \dim H_2$;
2. Если $\{|e_i>\}_{i=1}^{m}$ – базис H_1, а $\{|f_i>\}_{j=1}^{n}$ – базис H_2, то $\{|e_i \otimes f_i>\}_{i=1,j=1}^{m,n}$ – порождающий базис $H_1 \otimes H_2$.

Тензорным же произведенем операторов A из H_1^* и B из H_2^*(оператор A представлен матрицей, показанной выше) называется оператор $A \otimes B$ из $[H_1 \otimes H_2]^*$ с матрицей

$$A \otimes B = \begin{pmatrix} a_{11} \cdot B & a_{12} \cdot B & a_{13} \cdot B & \cdots & a_{1m} \cdot B \\ a_{21} \cdot B & a_{22} \cdot B & a_{23} \cdot B & \cdots & a_{2m} \cdot B \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{m1} \cdot B & a_{m2} \cdot B & a_{m3} \cdot B & \cdots & a_{mm} \cdot B \end{pmatrix}$$

Кубит

Кубит

$$|0> = \begin{bmatrix}1\\0\end{bmatrix}, |1> = \begin{bmatrix}0\\1\end{bmatrix},$$

произвольный вектор $|\psi> \epsilon H^2$ можно выразить следующим образом:

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

$$|\alpha|^2 + |\beta|^2 = 1$$

Квантовый регистр из двух кубитов

$$|00> = |0> \otimes |0> = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}. \quad |01> = |0> \otimes |1> = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}.$$

$$|10> = |1> \otimes |0> = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}. \quad |11> = |1> \otimes |1> = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}.$$

Квантовый регистр из двух кубитов

$$|\phi> \alpha_1|00> + \alpha_2|01> + \alpha_3|10> + \alpha_4|11>.$$

$$|\alpha_1|^2 + |\alpha_2|^2 + |\alpha_3|^2 + |\alpha_4|^2 = 1$$

Основы квантовой механики

Постулат 2. Эволюция *замкнутой* квантовой системы описывается *унитарным преобразованием*. Другими словами, состояние $|\psi>$ системы в момент времени t_1 связано с ее состоянием $|\psi'>$ в момент t_2 посредством унитарного оператора U, зависящего только от моментов времени t_1 и t_2:

$$|\boldsymbol{\psi}'> = \mathbf{U}|\,\boldsymbol{\psi}>$$

Основы квантовой механики

Постулат 2'. Эволюция состояния замкнутой квантовой системы во времени описывается уравнением Шрёдингера

$$i\hbar \cdot \frac{d|\psi>}{dt} = H\,|\,\psi >$$

H – гамильтониан, $\hbar$ – постоянная Планка

Основы квантовой механики

Постулат 3. Квантовые измерения описываются набором {Mm} операторов измерения. Это операторы, действующие в пространстве состояний системы, подлежащей измерению.

Постулат 4. Пространство состояний составной системы представляет собой тензорное произведение пространств состояний входящих в нее систем.

Квантовые алгоритмы

Квантовый алгоритм включает в себя:

- Инициализацию квантового регистра;
- Набор унитарных преобразований над ним;
- Измерение результата.

Орёл или решка

Давайте для примера рассмотрим простейший квантовый алгоритм: он будет генерировать случайный бит — ноль или один, орла или решку.

Для алгоритма нам понадобится всего один кубит. Пусть в начальный момент времени он находится в состоянии |0>. Теперь применим к нему гейт Адамара H чтобы получить состояние $H|0> = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}$.

Орёл или решка

Если мы сейчас измерим полученную систему, с вероятностью $\left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}$ она окажется в состоянии |0> и с точно такой же вероятностью в состоянии|1>.

Нетривиальный пример

Алгоритм Дойча-Йожи, позволяющий за один вызов функции определить, константна функция или сбалансирована

0) Постановка задачи

a) классическое детерминированное решение

b) классическое вероятностное решение

c) квантовое решение

Алгоритм Дойча-Йожи

0) *Постановка задачи*

Пусть дана булева функция f: $\{0, 1\}^n \to \{0, 1\}$ и о ней априорно известно, что она или константна, то есть для любого из своих аргументов всегда возвращает либо 0, либо 1, или сбалансирована, то есть ровно на половине своих аргументов возвращает 0, а ровно на половине 1. Требуется определить, константна функция или сбалансирована. При этом считается, что время вызова функции несоизмеримо больше любых других операций, поэтому сложность алгоритма определяется количеством вызовов функции.

Алгоритм Дойча-Йожи

а) *Классическое детерминированное решение*
Давайте, для начала, решим задачу в классической модели вычислений. Для этого в худшем случае понадобится вызвать функцию на $2^{n-1} + 1$ аргументах: ровно на половине и ещё одном. Если все вычисленные значения одинаковы, то функция, очевидно, константна. Если же существуют хотя-бы два различных результата, функция сбалансирована. Сложность детерминированного алгоритма экспоненциальна и составляет $O(2^{n-1} +1)$.

Алгоритм Дойча-Йожи

b) *Классическое вероятностное решение*
А что, если вместо половины аргументов мы проверим меньшее их число и вынесем вердикт? Точным ответ уже не будет, но с какой вероятностью мы ошибёмся? Допустим, мы вычислили функцию на
$k < 2^{n-1} + 1$ аргументах. Если среди значений функции есть два различных, то всё просто – функция сбалансирована. Иначе, мы объявляем её константной с вероятностью $p(k) < 1$.

Алгоритм Дойча-Йожи

b) *Классическое вероятностное решение*

Предположим, что мы ошиблись и функция на самом деле сбалансирована. Посчитаем вероятность ошибки 1 - $p(k)$. Если мы выбирали аргументы равномерно, то вероятность того, что два подряд идущих значения функции одинаковы, равна 1/2, а вероятность же встретить k одинаковых подряд идущих значений равна $1/2^{k-1}$.

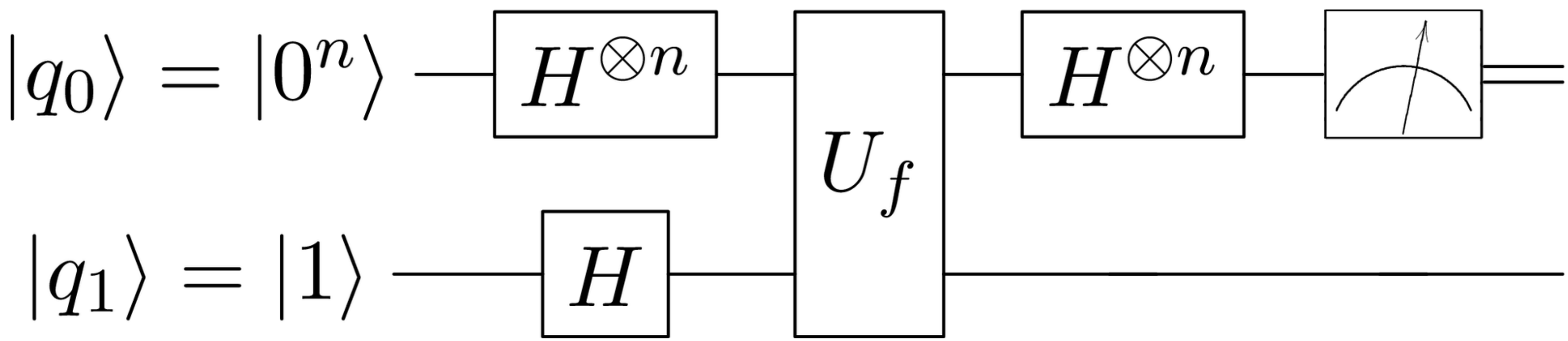
$$1 - p(k) = \frac{1}{2^{k-1}},$$

$$k(p) = 1 + \log_2 \frac{1}{1-p}.$$

Чтобы быть уверенным в ответе на 99.99%, необходимо вызвать функцию всего 15 раз.

Алгоритм Дойча-Йожи

с) *Квантовое решение*



Если результатом измерения станет 0, то функция константна, иначе – сбалансирована.

Алгоритм Дойча-Йожи

На входе алгоритма есть булева функция $f(x_1, x_2, \ldots, x_n)$ от n булевых переменных. Алгоритм представляет собой применение к нулевому вектору |0> оператора $H^{\otimes n}\ U_f\ H^{\otimes n}$ и измерение состояния регистра. Если все биты регистра равны 0, значит значение функции $f(x)$ не зависит от x в противном случае функция является сбалансированной.

Алгоритм Дойча-Йожи

$$\lambda_0 \cdot |0> + \lambda_1 \cdot |1> \xrightarrow{U_f} (-1)^{f(0)} \cdot \lambda_0 \cdot |0> + (-1)^{f(1)} \cdot \lambda_1 \cdot |1>$$

Пусть $x \epsilon [0,1]$

1. Константы (0,0) и (1,1)
2. Сбалансированные(1,0) и (0,1)

$|\varphi> = 1 \cdot |0> + 0|1>$

$|\varphi_1> = \mathrm{H}|\ \varphi >$

$|\varphi_2> = \mathrm{U}_f\ |\ \varphi_1 >$

$\mathrm{H}|\ \varphi_2 > = (-1)^{f(0)} + (-1)^{f(1)}) \cdot \frac{1}{2}\ |0> + (-1)^{f(0)} - (-1)^{f(1)}) \cdot \frac{1}{2}\ |1>$

БЛАГОДАРЮ

ЗА ВНИМАНИЕ