(1)

Квантовые вычисления

Лекция 22

Идея квантовых компьютеров возникла ~ 1980 г.

Манин Ю.И.

~ 1981 г.

Фейнман 1981

Вся окружающая нас природа "управляется" квантовой механикой, в том числе и техника, используемая для вычислений

Память компьютера — магнетизм / спонтанная намагниченность } не возм. понять без законов КМ.

Работа элементов схем — диоды, транзисторы

Однако основной элемент классич. компьютера

$\longrightarrow$ классический бит: да (1) или нет (0)

Например элемент памяти ~~основан~~.

— намагн. макроскоп. части вещества — включает большое / макроскопическое число частиц, и поэтому фактически является классическим.

В основе идеи квантовых вычислений —

1) — научиться манипулировать / "производить вычисления" над достаточно большими системами на квантовом уровне, используя квантовомех. явления — интерференцию, запутанность.

2) Число атомов во Вселенной $N \sim 10^{75}$ (считая 1 протон на 1 см^3)

Размерность пространства состояний N квантовых спинов $\sim 2^N$

Если приравнять эти два числа

$$10^{75} = 2^N \Rightarrow N \sim 250 \,!$$

Кубиты и основные квантовые вентили

Квантовый бит $\equiv$ кубит — элемент 2-мерного КМ
qubit — гильбертового пространства

$$|\psi\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix} \qquad |\alpha|^2+|\beta|^2 = 1 \Leftarrow \langle\psi|\psi\rangle = 1$$

$$(\mathrm{Re}\,\alpha)^2+(\mathrm{Im}\,\alpha)^2+(\mathrm{Re}\,\beta)^2+(\mathrm{Im}\,\beta)^2 = 1$$

Состояние кубита — можно задать точкой на единичной 3-сфере в 4-мерном пространстве

Сравним это с классическим битом, где сост. $\to$ 1 или 0.

$$|\psi\rangle = \alpha\begin{pmatrix}1\\0\end{pmatrix}+\beta\begin{pmatrix}0\\1\end{pmatrix} \equiv \alpha|0\rangle+\beta|1\rangle$$

Операции над кубитом — даются унитарными операторами — унитарными матрицами 2×2, $\hat U\cdot\hat U^{+} = 1$

$|\psi'\rangle = U|\psi\rangle$

Сохранение нормы $\langle\psi|\psi\rangle \Rightarrow \langle\psi'|\psi'\rangle$ требует.

Произвольный унитарный оператор, выражается через $\vec\sigma$-матрицы $\sigma_x = \begin{pmatrix}0&1\\1&0\end{pmatrix}$ $\sigma_y = \begin{pmatrix}0&-i\\i&0\end{pmatrix}$ $\sigma_z = \begin{pmatrix}1&0\\0&-1\end{pmatrix}$

$$\hat U = e^{i\frac{\vec\sigma}{2}\vec n\cdot\varphi}$$

где $\vec n$ — единичный вектор.
φ — веществ. число.

③

Основные однокубитные вентили

1) NOT — квантовый "НЕТ"

$U_{NOT}|0\rangle = |1\rangle$ — действие U_{NOT} на базис.

$U_{NOT}|1\rangle = |0\rangle$

$$U_{NOT} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \sigma_x$$

2) Вентиль Адамара — U_H

$$U_H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \qquad U_H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{\sigma_x + \sigma_z}{\sqrt{2}}$$

$$U_H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Многокубитные состояния — регистр кубитов

$$|\psi_1, \psi_2, \psi_3, \ldots, \psi_n\rangle = \prod_{i=1}^{n} |\psi_i\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \ldots \otimes |\psi_n\rangle$$

Для 2^x кубитного случая

$$\begin{pmatrix} \alpha_1 \\ \beta_1 \end{pmatrix} \otimes \begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix} = \left[\alpha_1|0\rangle + \beta_1|1\rangle\right] \otimes \left[\alpha_2|0\rangle + \beta_2|1\rangle\right] =$$

$$= \alpha_1\alpha_2|0,0\rangle + \alpha_1\beta_2|0,1\rangle + \beta_1\alpha_2|1,0\rangle + \beta_1\beta_2|1,1\rangle$$

Итак $|2\text{-qubit}\rangle = a|0,0\rangle + b|0,1\rangle + c|1,0\rangle + d|1,1\rangle$

самое общее 2-qubit состояние / нормировка $|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$

Состояние имеет $a = \alpha_1\alpha_2$ $b = \alpha_1\beta_2$ $c = \beta_1\alpha_2$ $d = \beta_1\beta_2$

Для него $a \cdot d = b \cdot c$ ← что не является требованием для 2-qubit в общем случае

Понятие запутанности

Если $|2\text{-qubit}\rangle \neq |\alpha\rangle \otimes |\beta\rangle$ — такое состояние называют запутанным (entangled – in english)

Запутанные состояния играют определяющую роль в теории квантовых вычислений.

Действие произведения вентилей Адамара на 2-qubit состояние $|0,0\rangle$

$$\hat{U}_H \otimes U_H |0,0\rangle = \frac{1}{2}[|0\rangle + |1\rangle] \otimes [|0\rangle + |1\rangle] = \frac{1}{2}(|0,0\rangle + |0,1\rangle + |1,0\rangle + |1,1\rangle)$$

В двоичной системе исчисления. Поэтому правую часть можно представить коротко как: $\frac{1}{2}(|0\rangle + |1\rangle + |2\rangle + |3\rangle)$

$0 = 00$
$1 = 01$
$2 = 10$
$3 = 11$

Для квантовых вычислений недостаточны лишь однокубитные вентили. Поэтому

2-qubit вентиль CNOT = "Controlled NOT" контролируемое нет.

$$\hat{U}_{CNOT}|a,b\rangle = |a, a+b\rangle$$

сложение по модулю 2

$\hat{U}_{CNOT}|0,0\rangle = |0,0\rangle$ $\quad$ $\hat{U}_{CNOT}|1,0\rangle = |1,1\rangle$

$\hat{U}_{CNOT}|0,1\rangle = |0,1\rangle$ $\quad$ $U_{CNOT}|1,1\rangle = |1,0\rangle$

Подействуем $\hat{U}_{CNOT}$ на 2-qubit состояние, являющимся

произведением 1-qubit состояний

$$\hat{U}_{CNOT}\left[\alpha_1|0\rangle+\beta_1|1\rangle\right]\otimes\left[\alpha_2|0\rangle+\beta_2|1\rangle\right]=\alpha_1\alpha_2|0,0\rangle+\alpha_1\beta_2|0,1\rangle+$$
$$+\beta_1\alpha_2|1,1\rangle+\beta_1\beta_2|1,0\rangle=$$

$$=a|0,0\rangle+b|0,1\rangle+c|1,0\rangle+d|1,1\rangle$$

Тогда $a=\alpha_1\alpha_2$ $\quad b=\alpha_1\beta_2$ $\quad c=\beta_1\beta_2$ $\quad d=\beta_1\alpha_2$

$$a\cdot d=\alpha_1\alpha_2^2\beta_1\neq b\cdot c=\alpha_1\beta_2^2\beta_1$$

То есть, после действия $\hat{U}_{CNOT}$, изначально не запутанное состояние стало — запутанным!

Схема квантового вычисления

$|input\rangle \longrightarrow \hat{U} \longrightarrow |output\rangle \longrightarrow$ измерение

$|input\rangle$ — исходное квантовое сост. регистра данных

$\hat{U}$ — операция над данными

$|output\rangle$ — полученное квантовое состояние регистра данных

$\longrightarrow$ $\hat{U}$ — унитарный оператор с точки зрения КМ

$\longrightarrow$ процесс измерения в КМ носит вероятности. характер, происходит редукция волн. функции.

$$\begin{pmatrix}\alpha\\ \beta\end{pmatrix} \xrightarrow{\text{измерение}} \begin{pmatrix}1\\0\end{pmatrix} \text{ вероятн. } |\alpha|^2$$

$$\begin{pmatrix}\alpha\\ \beta\end{pmatrix} \xrightarrow{\text{измерение}} \begin{pmatrix}0\\1\end{pmatrix} \text{ вероятн. } |\beta|^2$$

Произвольное унитарное преобразование представимо в виде действия однокубитных преобразований произвольного вида и 2-кубит вентелей $\hat{U}_{CNOT}$

Пример: преобразование 3-кубит вектора $|\psi_i\rangle = (\alpha|0\rangle + \beta|1\rangle)|00\rangle$

в $|\psi_f\rangle = \alpha|000\rangle + \beta|111\rangle$

Рассмотрим действие на $|\psi_i\rangle$

$$U^{(12)}_{CNOT} \otimes I_3 \Big(\alpha|000\rangle + \beta|100\rangle\Big) = \alpha|000\rangle + \beta|110\rangle$$

теперь, на подействуем оператором $I_1 \otimes U^{(23)}_{CNOT}$

$$I_1 \otimes U^{(23)}_{CNOT}\Big(\alpha|000\rangle + \beta|110\rangle\Big) = \alpha|000\rangle + \beta|111\rangle$$

Пример квантового вычисления.
Задача Дойча

Пусть задана бинарная функция $f(x)$, где $x \in (0,1)$ и $f(x) \in (0,1)$

Итого имеем 4 возможности

$$\underbrace{\begin{matrix} f(0)=0 & f(0)=1 \\ f(1)=0 & f(1)=1 \end{matrix}}_{\text{функция } f(x) = const} \qquad \underbrace{\begin{matrix} f(0)=0 & f(0)=1 \\ f(1)=1 & f(1)=0 \end{matrix}}_{\text{функция } f(x) \text{ – "сбалансированная"}}$$

$f(0) = f(1)$

$f(1) = 1 + f(0)$

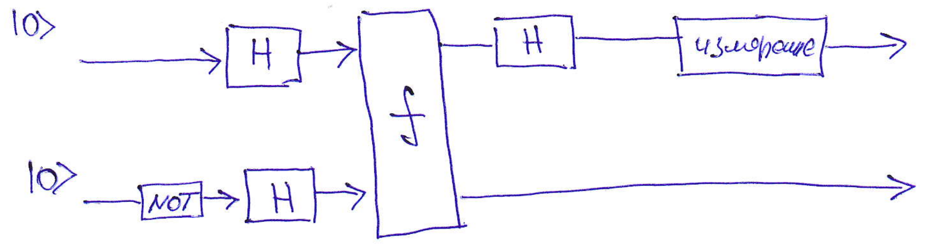
сложение по модулю 2

Вопрос задачи Дойча — является $f(x)$ — константой или $f(x)$ — сбалансированная функция?

Для решения задачи на классическом компьютере нужно вычислить $f(0)$ и $f(1)$ — 2 цикла работы класс. компьютера

Дойч предложил алгоритм квантового компьютера, для которого нужен один цикл работы.

Блок схема!



$\boxed{f}$ — 2-qubit операция $\hat{U}_f\,|x, y\rangle = |x, y + f(x)\rangle$

↑ сложение по модулю 2.

$\boxed{H}$ — 1-qubit вентиль Адамара

$\boxed{NOT}$ — 1-qubit вентиль NOT

Итак оператор U — в алгоритме Дойча

$$\hat{U} = (\hat{U}_H \otimes I)\,\hat{U}_f\,(\hat{U}_H \otimes \hat{U}_H)(I \otimes \hat{U}_{NOT})$$

$|\psi_f\rangle = \hat{U}\,|\psi_i\rangle$ где $|\psi_i\rangle = |0, 0\rangle = |0\rangle \otimes |0\rangle$

Опускаю вычисление — часть задачи из вашего задания

$$|\psi_f\rangle = \frac{1}{2^{3/2}}\Big\{ |0\rangle \otimes \big(|f(0)\rangle - |1+f(0)\rangle + |f(1)\rangle - |1+f(1)\rangle\big) + |1\rangle \otimes \big(|f(0)\rangle - |1+f(0)\rangle - |f(1)\rangle + |1+f(1)\rangle\big) \Big\}$$

если $\boxed{f(x) = const}$ $f(0)=f(1)$

$$|\psi_f\rangle = (-1)^{f(0)} |0\rangle \otimes (|0\rangle - |1\rangle)\frac{1}{\sqrt{2}}$$

если $f(1) = 1 + f(0)$ – функция сбалансированная

$$|\psi_f\rangle = (-1)^{f(0)} |1\rangle \otimes (|0\rangle - |1\rangle)\frac{1}{\sqrt{2}}$$

Квантовое измерение первого qubit – конечная фаза алгоритма Дойча, с вероятностью 100% даст $|0\rangle$ или $|1\rangle$ – в зависимости от того, является ли $f(x) = const$, или $f(x)$ – сбалансированная функция.

если $f(x) = const$ $\quad f(0) = f(1)$

$$|\psi_f\rangle = (-1)^{f(0)} |0\rangle \otimes (|0\rangle - |1\rangle)\frac{1}{\sqrt{2}}$$

если $f(1) = 1 + f(0)$ — функция сбалансированная

$$|\psi_f\rangle = (-1)^{f(0)} |1\rangle \otimes (|0\rangle - |1\rangle)\frac{1}{\sqrt{2}}$$

Квантовое измерение первого qubit — конечная фаза алгоритма Дойча, с вероятностью 100% даст $|0\rangle$ или $|1\rangle$ — в зависимости от того, является ли $f(x) = const$, или $f(x)$ — сбалансированная функция.