Універсальний набір гейтів. Елементарні квантові алгоритми.

Лекція 5

07 березня 2023

Універсальний набір гейтів

Теорема

Будь-яку унітарну операцію U на n кубітах можна реалізувати як послідовність $\mathrm{CNOT}_{k,l}$ та одно-кубітнитних гейтів.

Дворівневі унітарні операції

Унітарна U є дворівневою, якщо вона має вигляд

$$\begin{pmatrix} I & \vdots & \ddots & \vdots & \ddots \\ \dots & a & \dots & c & \dots \\ \ddots & \vdots & I & \vdots & \ddots \\ \dots & b & \dots & d & \dots \\ \ddots & \vdots & \ddots & \vdots & I \end{pmatrix}$$

При цьому

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix}$$

буде унітарною.

Теорема про універсальний набір

Шлях доведення:

1. Розкладаємо U у добуток дворівневих
2. Розкладаємо дворівневі у добуток мультиконтрольованих однокубітних
3. Розкладаємо мультиконтрольовані однокубітні (див. попередню лекцію). Тобто зводимо до двоконтрольованих, а потім їх вже до добутку $\mathrm{CNOT}_{k,l}$ та однокубітних

Розклад у добуток дворівневих

Нехай унітарна U дорівнює

$$U = \begin{pmatrix} a & d & g \\ b & e & h \\ c & f & j \end{pmatrix}$$

Якщо помножити її справа на матрицю

$$U_1 = \begin{pmatrix} \bar{a}/\sqrt{|a|^2+|b|^2} & \bar{b}/\sqrt{|a|^2+|b|^2} & 0 \\ b/\sqrt{|a|^2+|b|^2} & -a/\sqrt{|a|^2+|b|^2} & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

то вийде

$$U_1 U = \begin{pmatrix} a' & d' & g' \\ 0 & e' & h' \\ c' & f' & j' \end{pmatrix}.$$

Перестановочні матриці

Якщо було би $|a|^2 + |b|^2 = 0$, то значить $c \neq 0$.
Значить, перестановочною матрицею можна звести до випадку $|a|^2 + |b|^2 \neq 0$.

Будь-яка перестановка є добутком транспозицій (де тільки два елементи переставляються).

Відповідна перестановочна матриця для транспозиції є дворівневою, а саме

$$\begin{pmatrix} I & \vdots & \ddots & \vdots & \ddots \\ \dots & 0 & \dots & 1 & \dots \\ \ddots & \vdots & I & \vdots & \ddots \\ \dots & 1 & \dots & 0 & \dots \\ \ddots & \vdots & \ddots & \vdots & I \end{pmatrix}$$

Розклад у добуток дворівневих

Множимо далі $U_1 U$ на

$$U_2 = \begin{pmatrix} \bar{a}'/\sqrt{|a'|^2+|c'|^2} & 0 & \bar{c}'/\sqrt{|a'|^2+|c'|^2} \\ 0 & 1 & 0 \\ c'/\sqrt{|a'|^2+|c'|^2} & 0 & -a'/\sqrt{|a'|^2+|c'|^2} \end{pmatrix}$$

і отримуємо

$$U_2 U_1 U = \begin{pmatrix} 1 & d' & g' \\ 0 & e' & h' \\ 0 & f' & j' \end{pmatrix}$$

Але оскільки результат є унітарна матриця, то $d' = g' = 0$.
Тож $U_2 U_1 U$ вже буде дворівнева.
Загалом виходить

$$U = U_1^\dagger \cdot U_2^\dagger \cdot (U_2 U_1 U).$$

Розклад у добуток дворівневих

Загалом, для U розміру $m \times m$ знадобиться не більше за $m(m-1)/2$ дворівневих матриць у розкладі.

Тобто, у випадку n кубітів вийде не більше за $2^n(2^n-1)/2$ множників.

Розклад дворівневих до мультиконтрольованих

Нехай U це мультиконтрольована однокубітна операція, де контроль йде по всім кубітам, окрім цільового кубіту. Тобто,

$$U = C_{[0,\ldots,k-1,k+1,\ldots,n-1],k}(V)[a_0 \ldots a_{k-1} a_{k+1} \ldots a_{n-1}],$$

що діє за правилом

$$|b_0 b_1 \ldots b_{k-1} b_k b_{k+1} \ldots b_{n-1}\rangle \longrightarrow |b_0 b_1 \ldots b_{k-1}\rangle |b'_k\rangle |b_{k+1} \ldots b_{n-1}\rangle,$$

де майже завжди $|b'_k\rangle = |b_k\rangle$, а $|b'_k\rangle = V|b_k\rangle$ тільки якщо

$$b_0 \ldots b_{k-1} b_{k+1} \ldots b_{n-1} = a_0 \ldots a_{k-1} a_{k+1} \ldots a_{n-1}.$$

Така операція є дворівневою, де індекси рівнів це $s = a_0 \ldots a_{k-1} 0 a_{k+1} \ldots a_{n-1}$ та $t = a_0 \ldots a_{k-1} 1 a_{k+1} \ldots a_{n-1}$. Як видно, індекси рівнів відрізняються лише в одному біті. А значить, не будь-яка дво-рівнева матриця має такий тип. Але є процедура зведення, яка полягає в застосуванні кодів Грея.

Коди Грея

Код Грея це послідовність бітових строк, де сусідні строки відрізняються лише одним бітом.

Наприклад, код

$$
\begin{array}{c}
101001 \\
101011 \\
100011 \\
110011
\end{array}
$$

з'єднує строку $s = 101001$ та $t = 110011$.

Розклад дворівневих до мультиконтрольованих

Нехай тепер у нас є будь-яка дво-рівнева матриця U, індекси рівнів якої це s та t. Беремо код Грея, що їх з'єднує, тобто $g_1 = s, g_2, \ldots, g_{m-1}, g_m = t$, де індекси g_i, g_{i+1} відрізняються лише в одному біті.
Через $T_{g_i,g_{i+1}}$ позначимо дворівневу унітарну операцію, що переставляє рівні g_i, g_{i+1}, (тобто для неї $a = d = 0, b = c = 1$).
Така операція є мультиконтрольованим X, де індекс кубіту цілі – це там де g_i, g_{i+1} відрізняються в одному біті, всі інші кубіти є кубітами контролю, а контроль іде по значенням g_i, що співпадають з g_{i+1}.
Тоді $U^{(1)} = T_{g_1,g_2} U T_{g_1,g_2}$ це вийде дво-рівнева матриця, індекси рівнів якої вже будуть g_2, t. Загалом,

$$U^{(m-2)} = T_{g_{m-2},g_{m-1}} \ldots T_{g_1,g_2} U T_{g_1,g_2} \ldots T_{g_{m-2},g_{m-1}}$$

буде дво-рівнева матриця, в якої рівні це g_{m-1} та $g_m = t$, яка є мультиконтрольованою однокубітною.

Елементарні квантові алгоритми. Функції оракули.

Нехай є функція $f : \mathbf{B^n} \to \mathbf{B^m}$, про яку ми нічого не знаємо (чорний ящик), але ми може робити *запити* до неї, тобто підставляти значення x та отримувати результат $f(x)$.

Загальна задача полягає в знаходженні властивостей f за мінімальну кількість запитів, якщо на f накладені деякі умови.

Наприклад, в класичному випадку, якщо про f нічого не відомо, то потрібно зробити 2^n запитів для її відтворення. А якщо відомо, що f це константа, то достатньо лише одного.

Квантові оракули

Нагадаємо, що f відповідає квантова унітарна операція U_f на $n+m$ кубітах:

$$U_f \left|x\right\rangle \left|y\right\rangle = \left|x\right\rangle \left|y \oplus f(x)\right\rangle .$$

В квантовому випадку один *запит* – це отримання стану $U_f \left|\phi\right\rangle$ (який потім можна вимірювати чи проводити інші операції), де $\left|\phi\right\rangle$ це стан, що ми подали на вхід.

Виявляється, що в деяких випадках, квантових запитів потрібно зробити набагато менше для знаходження властивостей f, ніж класичних.

Задача Дойча

Припустимо, що $f : \mathbf{B} \to \mathbf{B}$ будь-яка. Питається, чи є f константою, тобто чи $f(0) = f(1)$? Очевидно, що в класичному випадку потрібно зробити 2 запити.

Але в квантовому випадку достатньо лише одного запиту до U_f!

Відкат фази (phase kickback)

Поглянемо, як діє U_f на стан $|x\rangle|-\rangle$. Маємо

$$U_f|x\rangle|-\rangle = \frac{1}{\sqrt{2}}(U_f|x\rangle|0\rangle - U_f|x\rangle|1\rangle) = \frac{1}{\sqrt{2}}(|x\rangle|f(x)\rangle - |x\rangle|1\oplus f(x)\rangle)$$

$$= \begin{cases} \frac{1}{\sqrt{2}}(|x\rangle|0\rangle - |x\rangle|1\rangle), & f(x)=0, \\ \frac{1}{\sqrt{2}}(|x\rangle|1\rangle - |x\rangle|0\rangle), & f(x)=1 \end{cases} = (-1)^{f(x)}|x\rangle|-\rangle,$$

тобто

$$U_f|x\rangle|-\rangle = (-1)^{f(x)}|x\rangle|-\rangle.$$

Такий самий трюк діє і для $n>1, m=1$.

Розв'язання задачі Дойча

Для відповіді на питання підставимо $|\phi\rangle = |+\rangle|-\rangle$. Маємо

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

$$= \begin{cases} \pm|+\rangle|-\rangle, & f(0) = f(1), \\ \pm|-\rangle|-\rangle, & f(0) \neq f(1). \end{cases}$$

Щоб розрізнити ці два випадки достатньо провести вимірювання першого кубіту результату у базисі $|+\rangle, |-\rangle$.

Задача Дойча-Йожи

Ця задача є узагальненням попередньої. Нехай $f : \mathbf{B^n} \to \mathbf{B}$ і додатково відомо, що f або константна, або сбалансована, тобто $f(x) = 1$ рівно для половини всіх можливих x (для 2^{n-1} значень).

Як розрізнити ці два випадки за найменшу кількість запитів? Не важко бачити, що в найгіршому випадку доведеться зробити $2^{n-1} + 1$ класичних запитів.

Але квантового запиту до U_f достатньо лише одного!

У якості $|\phi\rangle$ беремо $|u\rangle|-\rangle$, де

$$|u\rangle = H^{\otimes n}|00\ldots0\rangle = |+ + \cdots +\rangle =$$

$$= \frac{1}{(\sqrt{2})^n}(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes \cdots \otimes (|0\rangle + |1\rangle) =$$

$$= \frac{1}{2^{n/2}}\Big(\sum_{\mathbf{s}=s_0 s_1 \ldots s_{n-1},\ s_i \in \mathbf{B}}^{2^n} |\mathbf{s}\rangle \Big) = \frac{1}{2^{n/2}}\Big(\sum_{\mathbf{s}\in \mathbf{B^n}} |\mathbf{s}\rangle \Big),$$

що є рівномірною суперпозицією усіх базисних станів. Такий стан часто застосовується в квантових алгоритмах, і в деякому сенсі є реалізацією *квантового паралелізму*.

Задача Дойча-Йожи

Маємо, що

$$U_f \left|u\right\rangle \left|-\right\rangle = \frac{1}{2^{n/2}} \Big(\sum_{\mathbf{s}\in\mathbf{B^n}} U_f \left|\mathbf{s}\right\rangle \left|-\right\rangle \Big) = \frac{1}{2^{n/2}} \Big(\sum_{\mathbf{s}\in\mathbf{B^n}} (-1)^{f(\mathbf{s})} \left|\mathbf{s}\right\rangle \Big) \left|-\right\rangle .$$

Якщо f константа, то $U_f \left|u\right\rangle \left|-\right\rangle = \pm \left|u\right\rangle \left|-\right\rangle$. Якщо сбалансована, то $U_f \left|u\right\rangle \left|-\right\rangle = \left|u'\right\rangle \left|-\right\rangle$, де $\left|u'\right\rangle$ це (нормалізована) суперпозиція усіх базисних станів, в якій рівно половина коефіцієнтів дорівнює $+1$, а половина -1.

Не важко бачити, що $\left\langle u|u'\right\rangle = 0$ для будь-якого такого u'. Звідси $\left\langle u\right| H^{\otimes n} \cdot H^{\otimes n} \left|u'\right\rangle = 0$. Але ж $H^{\otimes n} \left|u\right\rangle = \left|00\ldots0\right\rangle$. Це означає, що у $H^{\otimes n} \left|u'\right\rangle$ в розкладі по стандартному базису буде відсутній елемент $\left|00\ldots0\right\rangle$ (тобто коефіцієнт при ньому буде 0).

Задача Дойча-Йожи

А значить, стандартне вимірювання $H^{\otimes n} |u\rangle$ завжди видасть результат $00\ldots0$, натомість при вимірюванні $H^{\otimes n} |u'\rangle$ результату $00\ldots0$ ніколи не буде. Тобто ми однозначно можемо відрізнити ці два випадки.

Задача Бернштейна-Вазірані

Нехай $f : \mathbf{B^n} \to \mathbf{B}$ така, що

$$f(\mathbf{x}) = (\mathbf{a} \cdot \mathbf{x}) \oplus b,$$

де $\mathbf{a} \cdot \mathbf{x} = \sum_i a_i x_i \mod 2$. Задача полягає у знаходженні $\mathbf{a}$ та b. В класичному випадку знадобиться $n + 1$ запит. Функцію f можна розуміти як лінійне відображення з векторного простору F_2^n до F_2, де F_2 це поле з двох елементів $\{0, 1\}$. Тож в якості запитів можна взяти 0^n та будь-який базис F_2^n.

В квантовій версії достастньо лише двох запитів до U_f.

За перший запит з $|\phi\rangle = |0^n\rangle |0\rangle$ визначаємо біт b, оскільки $U_f |\phi\rangle = |0^n\rangle |0 \oplus f(0^n)\rangle = |0^n\rangle |b\rangle$.

Задача Бернштейна-Вазірані

Для визначення **a** достатньо запиту $|\phi\rangle = |u\rangle|-\rangle = |+\rangle^{\otimes n}|-\rangle$ (так як і в попередній задачі). Дійсно, маємо що

$$U_f|\phi\rangle = \frac{1}{2^{n/2}}\Big(\sum_{\mathbf{s}\in\mathbf{B^n}}(-1)^{f(\mathbf{s})}|\mathbf{s}\rangle\Big)|-\rangle = \frac{1}{2^{n/2}}\Big(\sum_{\mathbf{s}\in\mathbf{B^n}}(-1)^{\mathbf{a}\cdot\mathbf{s}\oplus b}|\mathbf{s}\rangle\Big)|-\rangle =$$

$$= (-1)^b\frac{1}{2^{n/2}}\Big(\sum_{\mathbf{s}\in\mathbf{B^n}}(-1)^{\mathbf{a}\cdot\mathbf{s}}|\mathbf{s}\rangle\Big)|-\rangle.$$

З іншого боку,

$$H^{\otimes n}|\mathbf{a}\rangle = \frac{1}{2^{n/2}}(|0\rangle+(-1)^{a_0}|1\rangle)\otimes(|0\rangle+(-1)^{a_1}|1\rangle)\otimes\ldots(|0\rangle+(-1)^{a_{n-1}}|1\rangle$$

$$= \frac{1}{2^{n/2}}\Big(\sum_{\mathbf{s}\in\mathbf{B^n}}(-1)^{\sum_i a_i s_i}|\mathbf{s}\rangle\Big).$$

Задача Бернштейна-Вазірані

Звідси

$$U_f \left|\phi\right\rangle = (-1)^b \left(H^{\otimes n} \left|\mathbf{a}\right\rangle \right) \left|-\right\rangle,$$

а отже

$$\left|\mathbf{a}\right\rangle \left|-\right\rangle = (-1)^b (H^{\otimes n} \otimes I) U_f \left|\phi\right\rangle \left|-\right\rangle,$$

і значить стандартне вимірювання дасть нам $\mathbf{a}$.

Завдання

3.1. $U = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -i & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & i & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$

$n = 3$

Записати як добуток мультиконтрол.

(код Грея $110 \to 111 \to 101$)

3.2. $f(a_1, a_2) = a_1 \oplus a_2$

$|\psi\rangle = U_f |+\rangle|+\rangle|-\rangle$

$H \otimes H \otimes I \cdot |\psi\rangle = ?$