Задача Сімонса. Алгоритм Гровера.

Лекція 6

14 березня 2023

Задача Сімонса

Нехай $f : \mathbf{B^n} \to \mathbf{B^n}$ така, що або
1) f обертовна (тобто перестановка множини $\mathbf{B^n}$)
2) f періодична з періодом 2 та є відображенням 2-до-1 (тобто кожний елемент образу має рівно 2 прообрази):
$\exists \mathbf{s} \neq \mathbf{0}\ \forall \mathbf{x}\ f(\mathbf{x} \oplus \mathbf{s}) = f(\mathbf{x})$ та
$\forall \mathbf{x}, \mathbf{y}\ f(\mathbf{y}) = f(\mathbf{x}) \implies \mathbf{y} = \mathbf{x}\ \mathrm{OR}\ \mathbf{y} = \mathbf{x} \oplus \mathbf{s}$
Іншими словами
$\exists \mathbf{s} \neq \mathbf{0}\ \forall \mathbf{x} \neq \mathbf{y}\ f(\mathbf{x}) = f(\mathbf{y}) \iff \mathbf{x} \oplus \mathbf{y} = \mathbf{s}$

Потрібно визначити випадок та $\mathbf{s}$ (в деякому сенсі, першому випадку відповідає $\mathbf{s} = \mathbf{0}$).

Задача Сімонса

Наприклад, $f : \mathbf{B^3} \to \mathbf{B^3}$, $s = 110$,

$$000, 110 \xrightarrow{f} 101,$$

$$001, 111 \xrightarrow{f} 010,$$

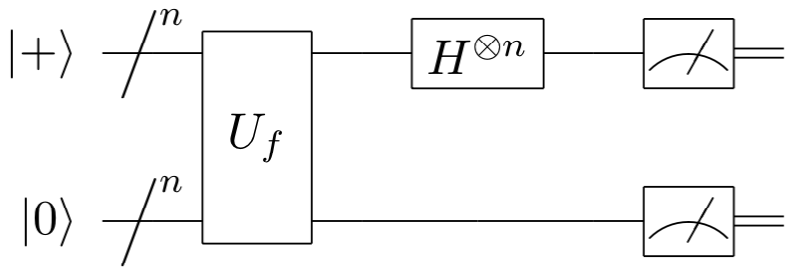
$$010, 100 \xrightarrow{f} 000,$$

$$011, 101 \xrightarrow{f} 110.$$

Для визначення **s** шукаємо різні x, y, що $f(x) = f(y)$. Тоді $s = x \oplus y$. В найгіршому випадку доведеться зробити не менше за $2^{n/2}$ класичних запитів. Адже q запитів дозволять перевірити не більше за $q(q-1)/2$ можливих значень **s**. Тож має бути $q(q-1)/2 \geqslant 2^n$. В середньому також знадобиться приблизно $O(\sqrt{2^n})$ запитів.
Натомість, існує алгоритм який в середньому визначає **s** за $O(n)$ квантових запитів до U_f.

Задача Сімонса, розв'язок

Для розв'язку застосовуємо наступну схему:



Тобто, на вход подаємо

$$|\phi\rangle = |u\rangle\,|0^n\rangle = |+\rangle^n\,|0^n\rangle = \frac{1}{2^{n/2}} \sum_{\mathbf{x}\in\mathbf{B^n}} |\mathbf{x}\rangle\,|0^n\rangle\,.$$

Маємо, що

$$U_f\,|\phi\rangle = \frac{1}{2^{n/2}} \sum_{\mathbf{x}\in\mathbf{B^n}} |\mathbf{x}\rangle\,|f(\mathbf{x})\rangle\,.$$

Використовуємо формулу з попередньої лекції

$$H^{\otimes n}\,|\mathbf{x}\rangle = \frac{1}{2^{n/2}} \sum_{\mathbf{y}\in\mathbf{B^n}} (-1)^{\mathbf{x}\cdot\mathbf{y}}\,|\mathbf{y}\rangle\,.$$

Задача Сімонса, розв'язок

Отримуємо

$$(H^{\otimes n} \otimes I)\, U_f \,|\phi\rangle = \frac{1}{2^{n/2}} \sum_{\mathbf{x}\in\mathbf{B^n}} H^{\otimes n} \,|\mathbf{x}\rangle\,|f(\mathbf{x})\rangle$$

$$= \frac{1}{2^n} \sum_{\mathbf{x}\in\mathbf{B^n}} \sum_{\mathbf{y}\in\mathbf{B^n}} (-1)^{\mathbf{x}\cdot\mathbf{y}} \,|\mathbf{y}\rangle\,|f(\mathbf{x})\rangle =$$

$$= \frac{1}{2^n} \sum_{\mathbf{y}\in\mathbf{B^n}} \sum_{\mathbf{z}\in\mathbf{B^n}} \alpha_{\mathbf{y},\mathbf{z}} \,|\mathbf{y}\rangle\,|\mathbf{z}\rangle\,, \qquad \alpha_{\mathbf{y},\mathbf{z}} = \sum_{\mathbf{x}:f(\mathbf{x})=\mathbf{z}} (-1)^{\mathbf{x}\cdot\mathbf{y}}.$$

При стандартному вимірюванні ми отримаємо $\mathbf{y}, \mathbf{z}$ з ймовірністю $\frac{1}{2^{2n}}|\alpha_{\mathbf{y},\mathbf{z}}|^2$.

Задача Сімонса, розв'язок

Подивимось чому дорівнює

$$\alpha_{\mathbf{y},\mathbf{z}} = \sum_{\mathbf{x}:f(\mathbf{x})=\mathbf{z}} (-1)^{\mathbf{x}\cdot\mathbf{y}}$$

при різних випадках.
Якщо f обертовна, то для кожного $\mathbf{z}$ існує єдиний відповідний $\mathbf{x}$. Тобто $|\alpha_{\mathbf{y},\mathbf{z}}| = 1$.
Якщо f необертовна, тобто вона є другого типу, то це розбивається на два випадки. Якщо $\mathbf{z}$ не належить образу f, то $\alpha_{\mathbf{y},\mathbf{z}} = 0$. Інакше, для $\mathbf{z}$ існують два прообрази, а значить

$$\alpha_{\mathbf{y},\mathbf{z}} = (-1)^{\mathbf{x}\cdot\mathbf{y}} + (-1)^{(\mathbf{x}\oplus\mathbf{s})\cdot\mathbf{y}},$$

де $f(\mathbf{x}) = f(\mathbf{x}\oplus\mathbf{s}) = \mathbf{z}$. Звідси $|\alpha_{\mathbf{y},\mathbf{z}}| = |1 + (-1)^{\mathbf{s}\cdot\mathbf{y}}|$.

Задача Сімонса, розв'язок

Проаналізуємо ймовірності результатів для верхнього регістру, тобто

$$\Pr(\mathbf{y}) = \frac{1}{2^{2n}} \sum_{\mathbf{z}} |\alpha_{\mathbf{y},\mathbf{z}}|^2.$$

Якщо f обертовна, то $\Pr(\mathbf{y}) = \frac{1}{2^n}$.
Якщо f другого типу, то

$$\Pr(\mathbf{y}) = \frac{2^n}{2} \frac{1}{2^{2n}} |1 + (-1)^{\mathbf{s}\cdot\mathbf{y}}|^2 = \begin{cases} 0, & \mathbf{s}\cdot\mathbf{y} \neq 0 \\ \frac{2}{2^n}, & \mathbf{s}\cdot\mathbf{y} = 0 \end{cases}$$

У будь-якому випадку бачимо, що якщо $\Pr(\mathbf{y}) \neq 0$, то $\mathbf{s}\cdot\mathbf{y} = 0$. Тобто значення $\mathbf{y}$, яке ми будемо отримувати при вимірюваннях, завжди буде ортогонально до $\mathbf{s}$ (у просторі F_2^n).

Задача Сімонса, розв'язок

Припустимо, що за деяку кількість вимірювань ми знайшли $n-1$ таких $\mathbf{y_i}$, які є лінійно незалежні. Це дає систему лінійних рівнянь

$$\begin{cases} \mathbf{s} \cdot \mathbf{y_1} = 0, \\ \mathbf{s} \cdot \mathbf{y_2} = 0, \\ \vdots \\ \mathbf{s} \cdot \mathbf{y_{n-1}} = 0, \end{cases}$$

яка розв'язується класичним чином. Розв'язками будуть $\mathbf{0}$ та якийсь $\mathbf{s}' \neq \mathbf{0}$.

Перевіряємо умову $f(\mathbf{0}) = f(\mathbf{s}')$. Якщо вона виконується, то значить f другого типу та $\mathbf{s} = \mathbf{s}'$. Якщо ні, то значить f першого типу (обертовна, $\mathbf{s} = 0$).

Задача Сімонса, розв'язок

Це працює лише якщо ми отримали $n-1$ лінійно незалежних $\mathbf{y_i}$. Але ймовірність цього досить висока. Загалом, ймовірність того, що випадкові n елементів в F_2^n є лінійно незалежними дорівнює

$$\prod_{k=1}^{n}(1-\frac{1}{2^k}) > \prod_{k=1}^{\infty}(1-\frac{1}{2^k}) > 0.288788 > 1/4.$$

Алгоритм пошуку Гровера

Нехай для функції $f : \mathbf{B^n} \to \mathbf{B}$ відома кількість $t \ll 2^n$ прообразів 1. Потрібно знайти хоча б один з цих прообразів, тобто такий $\mathbf{x} \in \mathbf{B^n}$, що $f(\mathbf{x}) = 1$.

Очевидно, що в найгіршому випадку доведеться зробити $2^n - t$ класичних запитів, щоб знайти $\mathbf{x}$. В середньому таких запитів потрібно приблизно $2^n/t$.

Алгоритм Гровера, натомість, дозволяє розв'язати цю задачу за $O(\sqrt{2^n/t})$ квантових запитів до U_f.

Оператор дифузії Гровера

Нехай $|u\rangle = |+\rangle^{\otimes n} = \frac{1}{2^{n/2}} \sum_{\mathbf{x}\in\mathbf{B^n}} |\mathbf{x}\rangle$.

Визначимо унітарний *оператор дифузії Гровера*:

$$U_G = 2|u\rangle\langle u| - I.$$

Не важко бачити, що $U_G U_G^\dagger = I$. До того ж, $U_G^2 = I$. Оператори такого типу також називають рефлексіями (відбиттями).

Геометрично оператор U_G можна уявляти як рефлексію навколо вектору $|u\rangle$. Дійсно, для будь-якого $|\psi\rangle$ результат дії

$$|\psi'\rangle = U_G|\psi\rangle = (2\langle u|\psi\rangle)|u\rangle - |\psi\rangle$$

лежить в площині векторів $|u\rangle, |\psi\rangle$, при цьому відповідні кути співпадають, тобто $\langle u|\psi'\rangle = 2\langle u|\psi\rangle - \langle u|\psi\rangle = \langle u|\psi\rangle$.

Оператор дифузії Гровера

Найцікавіше для нас те, як U_G діє на коефіцієнти $\alpha_{\mathbf{x}}$ вектору $|\psi\rangle = \sum_{\mathbf{x}\in\mathbf{B^n}} \alpha_{\mathbf{x}} |\mathbf{x}\rangle$ в розкладі по стандартному базису.
Маємо, що

$$|\psi'\rangle = U_G |\psi\rangle = (2|u\rangle\langle u| - I) \sum_{\mathbf{x}\in\mathbf{B^n}} \alpha_{\mathbf{x}} |\mathbf{x}\rangle =$$

$$= 2|u\rangle \sum_{\mathbf{x}\in\mathbf{B^n}} \alpha_{\mathbf{x}} \langle u|\mathbf{x}\rangle - \sum_{\mathbf{x}\in\mathbf{B^n}} \alpha_{\mathbf{x}} |\mathbf{x}\rangle = \frac{2}{2^n}\Big(\sum_{\mathbf{x}\in\mathbf{B^n}} |\mathbf{x}\rangle\Big)\Big(\sum_{\mathbf{x}\in\mathbf{B^n}} \alpha_{\mathbf{x}}\Big) - \sum_{\mathbf{x}\in\mathbf{B^n}} \alpha_{\mathbf{x}} |\mathbf{x}\rangle$$

$$= \sum_{\mathbf{x}\in\mathbf{B^n}} (2\mathrm{avg}(\alpha) - \alpha_{\mathbf{x}}) |\mathbf{x}\rangle, \qquad \mathrm{avg}(\alpha_{\mathbf{x}}) = \frac{1}{2^n} \sum_{\mathbf{x}\in\mathbf{B^n}} \alpha_{\mathbf{x}}.$$

Таким чином

$$\alpha'_{\mathbf{x}} = 2\mathrm{avg}(\alpha_{\mathbf{x}}) - \alpha_{\mathbf{x}}, \qquad \mathrm{avg}(\alpha'_{\mathbf{x}}) = \mathrm{avg}(\alpha_{\mathbf{x}}).$$

Алгоритм пошуку Гровера, дія $U_f U_G$

Згадаємо тепер про метод відкату фази. Маємо, що

$$U_f |\psi\rangle |-\rangle = \sum_{\mathbf{x}\in\mathbf{B^n}} U_f \alpha_{\mathbf{x}} |\mathbf{x}\rangle |-\rangle = \sum_{\mathbf{x}\in\mathbf{B^n}} (-1)^{f(\mathbf{x})} \alpha_{\mathbf{x}} |\mathbf{x}\rangle |-\rangle .$$

Тобто дія U_f множить коефіцієнт $\alpha_{\mathbf{x}}$ на -1 якщо $f(\mathbf{x}) = 1$.

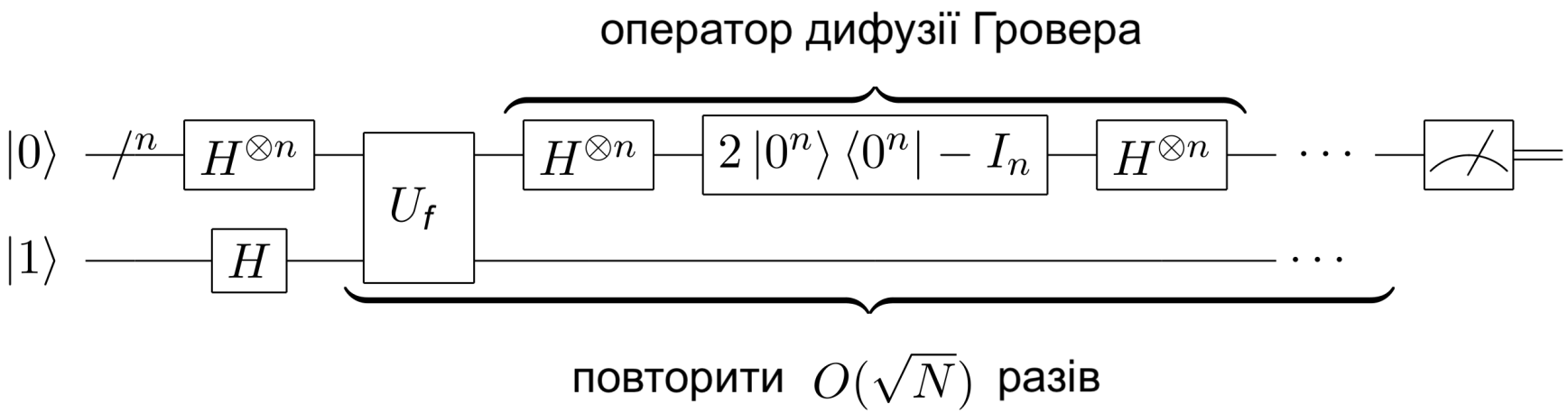
Припустимо, що усі $\alpha_{\mathbf{x}} = \frac{1}{2^{n/2}}$. Тоді $\mathrm{avg}((-1)^{f(\mathbf{x})}\alpha_{\mathbf{x}}) <\approx \mathrm{avg}(\alpha_{\mathbf{x}}) = \frac{1}{2^{n/2}}$ оскільки $t \ll 2^n$. Після застосування оператору Гровера до верхнього регістру отримаємо нові значення коефіцієнтів

$$\alpha'_{\mathbf{x}} = 2\mathrm{avg}((-1)^{f(\mathbf{x})}\alpha_{\mathbf{x}}) - (-1)^{f(\mathbf{x})}\alpha_{\mathbf{x}}.$$

Не важко бачити, що $\alpha'_{\mathbf{x}} >\approx \alpha_{\mathbf{x}}$ там де $f(\mathbf{x}) = 1$, та $\alpha'_{\mathbf{x}} <\approx \alpha_{\mathbf{x}}$ там де $f(\mathbf{x}) = 0$.

Алгоритм пошуку Гровера

Ідея алгоритму Гровера полягає у рекурсивному застосуванні пари операторів U_f та U_G, щоб в результаті збільшити модулі коефіцієнтів $\alpha_{\mathbf{x}}$ там де $f(\mathbf{x}) = 1$, та зменшити там де $f(\mathbf{x}) = 0$.



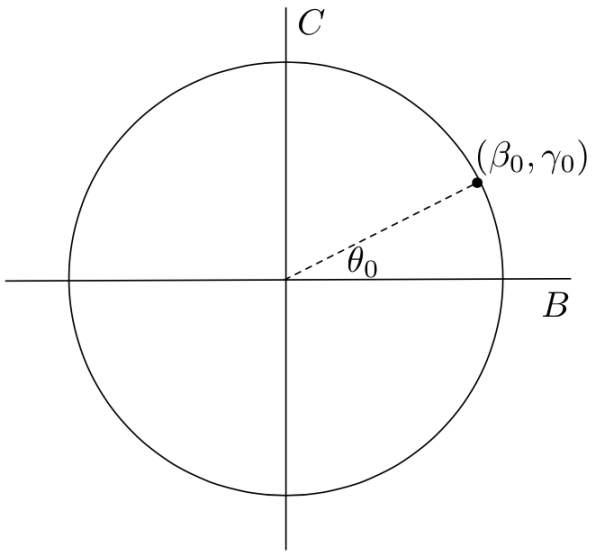
Оптимальним значенням ітерацій буде $\approx \frac{\pi}{4}\sqrt{2^n/t}$ з ймовірністю $> 1/2$ отримати шукане значення $\mathbf{x}$ при вимірюванні. Покажемо це.

Алгоритм пошуку Гровера, доведення

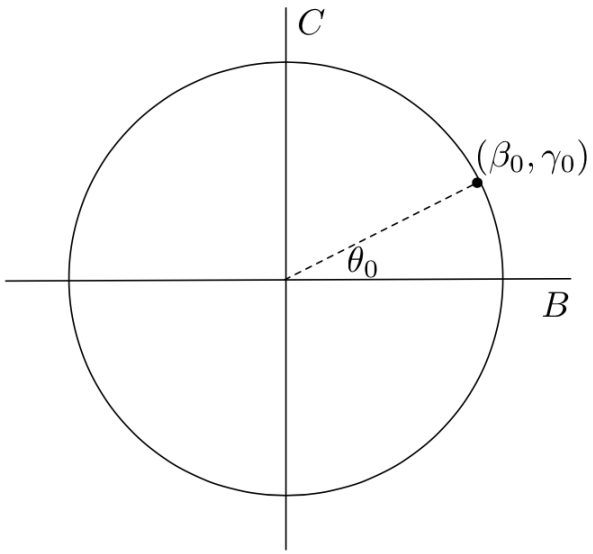
Стан верхнього регістру після i ітерацій буде мати вигляд

$$|\psi_i\rangle = \beta_i \frac{1}{\sqrt{2^n - t}} \sum_{\mathbf{x}: f(\mathbf{x})=0} |\mathbf{x}\rangle + \gamma_i \frac{1}{\sqrt{t}} \sum_{\mathbf{x}: f(\mathbf{x})=1} |\mathbf{x}\rangle,$$

де $\beta_i^2 + \gamma_i^2 = 1$. Причому $\beta_0 = \sqrt{\frac{2^n - t}{2^n}}$, $\gamma_0 = \sqrt{\frac{t}{2^n}}$.
Таку пару чисел β_i, γ_i зручно параметризувати кутом θ_i, таким що $\sin(\theta_i) = \gamma_i$, $\cos(\theta_i) = \beta_i$.



Алгоритм пошуку Гровера, доведення



Операція U_f буде діяти як $(\beta, \gamma) \to (\beta, -\gamma)$, тобто як рефлексія відносно вісі B. В свою чергу, операція U_G буде діяти як рефлексія відносно вектору (β_0, γ_0). Разом ці дві рефлексії діють як поворот на кут $2\theta_0$ проти годинникової стрілки. Звідси

$$\theta_i = (2i + 1)\theta_0.$$

Найкращий час для вимірювання це коли $\beta_i \approx 0$, тобто $\theta_i \approx \pi/2$.

Алгоритм пошуку Гровера, доведення

Тож ідеальна кількість кроків k задовольняє рівнянню

$$(2k+1)\theta_0 \approx \pi/2,$$

звідси k потрібно взяти найближчим цілим числом до

$$\frac{1}{2}\left(\frac{\pi}{2\theta_0} - 1\right) = \frac{\pi}{4\arcsin\left(\sqrt{t/2^n}\right)} - \frac{1}{2} \approx \frac{\pi}{4}\sqrt{2^n/t}.$$

При цьому ймовірність отримати шуканий $\mathbf{x}$ при вимірюванні буде

$$\gamma_k^2 \gg \frac{1}{2}.$$

Алгоритм пошуку Гровера

Якщо t наперед не відомо, то можна пробувати перебирати $k = 1, 2, 4, 8, \ldots, \frac{\pi}{4}\sqrt{2^n}$ послідовно. Оскільки це геометрична прогресія, то загальна кількість кроків буде мати порядок $O(\sqrt{2^n})$.

Відомо, що алгоритм Гровера є асимптотично оптимальним, тобто для розв'язання задачі пошуку кількість запитів до оракулу має бути порядку $\Omega(\sqrt{2^n})$.

Завдання

1. Яка ймовірність отримати $y = 0^n$ при вимірюванні верхнього регістру в агоритмі Сімонса, якщо
а) f обертовна (першого типу)
б) f другого типу

2. Нехай в задачі Сімонса f другого типу. Чи можна в якихось випадках знайти s, якщо провести менше ніж $n-1$ вимірювань в алгоритмі Сімонса? (тобто знаючи лише $y_1, \ldots, y_k$, $k < n-1$)

3. Зобразити оператор $I - 2\left|0^n\right\rangle\left\langle 0^n\right|$, що діє на n кубітах, як мультиконтрольовану однокубітну операцію.