Алгоритми Шора розкладу числа на множники та дискретного логарифмування

Лекція 8

28 березня 2023

Знаходження порядку числа

Нехай x та N це взаємно прості числа. Порядком числа x по модулю N називають найменше число $r > 0$, таке що

$$x^r = 1 \mod N.$$

Задача знаходження порядку є важкою в класичному випадку. Покажемо, як квантова оцінка фази дозволяє її розв'язати.

Знаходження порядку числа

Візьмемо L кубітів, щоб $N < 2^L$. Розглянемо унітарну операцію U, що діє наступним чином $(0 \leqslant y < 2^L)$:

$$U|y\rangle = \begin{cases} |yx \mod N\rangle, & y < N, \\ |y\rangle, & N \leqslant y < 2^L. \end{cases}$$

Оскільки $x^r = 1 \mod N$, то $U^r = I$, причому $U^s \neq I$ для $0 < s < r$.
Рівність $U^r = I$ означає, що серед власних значень U є примітивні корені степеня r з одиниці, тобто $e^{2\pi is/r}$.

Тож ми можемо використати QPE, щоб отримати оцінки дробів s/r і використитати цю інформацію для відтворення r.

Знаходження порядку числа

Розглянемо r власних векторів $|u_s\rangle$, $s = 0, \ldots, r-1$:

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi i s k/r} \left| x^k \mod N \right\rangle,$$

$$U |u_s\rangle = e^{2\pi i s/r} |u_s\rangle.$$

Оскільки

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = |\mathbf{1}\rangle,$$

то

$$QPE \left|0^t\right\rangle |\mathbf{1}\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \left| \widetilde{s/r} \right\rangle |u_s\rangle,$$

тож одне вимірювання дасть нам оцінку $\widetilde{s/r}$ (тобто t бітів) дробу s/r для випадкового $0 \leqslant s \leqslant r-1$.

Знаходження порядку числа

Для застосування *QPE* потрібно зрозуміти як реалізувати послідовність дій $C_k = C(U^{2^k})$. Нехай $z = z_1 z_2 \dots z_t$ складається з t бітів $z_i \in \mathbf{B}$. Застосування $\prod_{k=1}^{t} C_k$ до $|z\rangle |y\rangle$ буде мати результат

$$\prod_{k=1}^{t} C_k |z\rangle |y\rangle = |z\rangle (U^{2^{t-1}})^{z_t} \dots (U^2)^{z_2} U^{z_1} |y\rangle =$$

$$= |z\rangle \left| y x^{2^{t-1} z_t + \dots + 2 z_2 + z_1} \mod N \right\rangle = |z\rangle |y x^z \mod N\rangle .$$

Це можна реалізувати як композицію

$$\begin{aligned} |z\rangle |y\rangle \left|0^L\right\rangle &\longrightarrow \\ |z\rangle |y\rangle |x^z \mod N\rangle &\longrightarrow \\ |z\rangle |y x^z \mod N\rangle |x^z \mod N\rangle &\longrightarrow \\ |z\rangle |y x^z \mod N\rangle \left|0^L\right\rangle . & \end{aligned}$$

Знаходження порядку числа

Оскільки функції $f_a(b) = a^b \mod N$ та $f(a,b) = ab \mod N$ є швидкі класично, то для них існують ефективні класичні логічні схеми, а значить існують і ефективні квантові.

Загалом, для реалізації $\prod_{k=1}^{t} C_k$ достатньо $O(tL^2)$ примітивних гейтів.

Знаходження порядку числа, оцінка точності

Твердження Якщо в алгоритмі *QPE* взяти $t = 2L + 1 + \lceil \log_2(2 + 1/2\varepsilon) \rceil$, то ймовірність отримати оцінку $\phi \approx s/r$, що має точність в $2L + 1$ бітів (тобто перші $2L + 1$ бітів ϕ та s/r співпадають, $|\phi - s/r| \leqslant 1/2^{2L+1}$), буде не менша за $(1 - \varepsilon)$.

Доведення Нехай $\Phi = 0.\Phi_1\Phi_2 \dots \Phi_t$ це перші t бітів s/r, а значить

$$|(s/r - \Phi)2^t| \leqslant 1.$$

Якщо ϕ не достатньо точне, тобто $|\phi - s/r| > 1/2^{2L+1}$, то

$$|(\phi - \Phi)2^t| = |(\phi - s/r)2^t + (s/r - \Phi)2^t| > 2^t/2^{2L+1} - 1 > 1 + 1/2\varepsilon.$$

За твердженням з попередньої лекції ймовірність цього $\leqslant 1/2(1 + 1/2\varepsilon - 1) = \varepsilon$. □

Зауважимо, що якщо $|\phi - s/r| \leqslant 1/2^{2L+1}$, то $|\phi - s/r| \leqslant 1/2r^2$, оскільки $2^{2L+1} = 2 \cdot 2^{2L} \geqslant 2N^2 \geqslant 2r^2$.

Алгоритм відтворення ланцюгового дробу

Ланцюговий дріб – це запис дробового числа у вигляді

$$\frac{p}{q} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}}$$

Його позначають $[a_0, a_1, \ldots, a_n]$. Алгоритм *CFE* (continued fraction expansion) – це алгоритм знаходження ланцюгового запису для числа. Наприклад,

$$\frac{31}{13} = 2 + \frac{5}{13} = 2 + \frac{1}{\frac{13}{5}} = 2 + \frac{1}{2 + \frac{3}{5}} = 2 + \frac{1}{2 + \frac{1}{\frac{5}{3}}} = 2 + \frac{1}{2 + \frac{1}{1 + \frac{2}{3}}}$$

$$= 2 + \frac{1}{2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2}}}}$$

Алгоритм відтворення ланцюгового дробу

Дріб $\frac{p_k}{q_k} = [a_0, a_1, \ldots, a_k]$ називають k-им наближенням p/q. Основна властивість ланцюгового запису – якщо два числа близькі, то їх наближення співпадають. Має місце наступна теорема:

Теорема Якщо для додатніх чисел a, b виконується

$$\left|\frac{p}{q} - \frac{a}{b}\right| \leqslant \frac{1}{2b^2},$$

то $\frac{a}{b} = \frac{p_k}{q_k}$ для деякого k.

Оскільки $|\phi - s/r| \leqslant 1/2r^2$, то застосувавши *CFE* до $\frac{p}{q} = \phi$ ми будемо мати $\frac{p_k}{q_k} = s/r$ для якогось k.

Ймовірність того, що s/r це нескоротний дріб дорівнює $\varphi(r)/r$, що є достатньо високою. З такою ймовірністю $q_k = r$ для якогось k. Потрібно лише перевірити умову $x^{q_k} = 1 \mod N$, щоб пересвідчитись у цьому.

Алгоритм Шора факторизації числа

Насправді, основною частиною алгоритму Шора, де використовуються квантові комп'ютери, є знаходження порядку числа, яку ми вже розібрали. Подивимось, як він виглядає в цілому.

Нехай N це деяке число, яке ми хочемо розкласти на множники. Для цього нам достатньо знайти хоча б один дільник N, далі можна розкладати по рекурсії.

Ідея полягає в тому, щоб знайти таке $0 < x < N$, що $x^2 = 1 \mod N$, але $x \neq \pm 1 \mod N$. Тоді $(x-1)(x+1)$ ділиться на N, причому $(x-1)$ та $(x+1)$ окремо не діляться. Звідси $\gcd(x-1, N)$ та $\gcd(x+1, N)$ є нетривіальними дільниками N.

Алгоритм Шора факторизації числа

Для того щоб знайти таке x ми беремо випадкове $0 < y < N$ і шукаємо його порядок r, тобто $y^r = 1 \mod N$. Якщо r виявиться парним, то для $x = y^{r/2}$ ми будемо мати $x^2 = 1 \mod N$. І якщо нам повезе, то $y^{r/2} \neq \pm 1 \mod N$, тобто x підходяще.

Ймовірність такого результату для випадкового y досить висока – вона не менша за $1 - 1/2^{k-1}$, де k це кількість різних непарних простих дільників числа N.

Знаходження періодів функцій

Нехай фунція $f : \mathbb{Z} \longrightarrow \mathbf{B}^m$ є періодичною, тобто існує найменше $r > 0$ таке, що $\forall x : f(x + r) = f(x)$. Більше того, вважатимемо, що $f(x + s) \neq f(x)$ для будь-яких x та $0 < s < r$ (звідси $r < 2^m$).

Задача полягає в знаходженні періоду r за мінімальну кількість запитів до f. Нагадаємо, що квантова версія U_f діє як $U_f |x\rangle |0^m\rangle = |x\rangle |f(x)\rangle$, для $0 \leqslant x \leqslant 2^t - 1$.

Для стану $|0^t\rangle |0^m\rangle$ застосуємо операцію $H^{\otimes t}$ до першого регістру та U_f до всього стану. Будемо мати

$$U_f (H^{\otimes t} \otimes I) |0^t\rangle |0^m\rangle = U_f \frac{1}{2^{t/2}} \sum_{x=0}^{2^t-1} |x\rangle |0^m\rangle = \frac{1}{2^{t/2}} \sum_{x=0}^{2^t-1} |x\rangle |f(x)\rangle .$$

Знаходження періодів функцій

Позначимо для $y = 0, 1, \ldots, r-1$

$$\left|\hat{f}(y)\right\rangle = \frac{1}{\sqrt{r}} \sum_{x=0}^{r-1} e^{-2\pi i x y / r} \left|f(x)\right\rangle.$$

Тоді

$$\left|f(x)\right\rangle = \frac{1}{\sqrt{r}} \sum_{y=0}^{r-1} e^{2\pi i x y / r} \left|\hat{f}(y)\right\rangle.$$

Іншими словами, це перетворення Фур'є порядку r (але тут ми це використовуємо лише як математичний запис, а не квантову операцію).

Зауважимо, що оскільки всі $f(0), f(1), \ldots, f(r-1)$ різні, то всі $\left|\hat{f}(0)\right\rangle, \left|\hat{f}(1)\right\rangle, \ldots, \left|\hat{f}(r-1)\right\rangle$ є ортогональні.

Знаходження періодів функцій

Маємо, що

$$\frac{1}{2^{t/2}}\sum_{x=0}^{2^t-1}|x\rangle|f(x)\rangle = \frac{1}{2^{t/2}}\sum_{x=0}^{2^t-1}|x\rangle\frac{1}{\sqrt{r}}\sum_{y=0}^{r-1}e^{2\pi ixy/r}\left|\hat{f}(y)\right\rangle =$$

$$= \frac{1}{\sqrt{r}}\sum_{y=0}^{r-1}\left(\frac{1}{2^{t/2}}\sum_{x=0}^{2^t-1}e^{2\pi ix(y/r)}|x\rangle\right)\left|\hat{f}(y)\right\rangle = \frac{1}{\sqrt{r}}\sum_{y=0}^{r-1}|X_y\rangle\left|\hat{f}(y)\right\rangle.$$

Оскільки усі $\left|\hat{f}(y)\right\rangle$ ортогональні, то перший регістр окремо є рівномірною сумішу станів $|X_y\rangle$.

Знаходження періодів функцій

Так як і в алгоритмі оцінки фази застосування $QFT_{2^t}^{-1}$ до $|X_y\rangle$ дасть стан

$$QFT_{2^t}^{-1} \frac{1}{2^{t/2}} \sum_{x=0}^{2^t-1} e^{2\pi i x(y/r)} |x\rangle = \left|\widetilde{y/r}\right\rangle,$$

вимірювання якого дасть оцінку фази y/r.

Оскільки перший регістр це рівномірна суміш $|X_y\rangle$, то ми будемо отримувати оцінку y/r для випадкового y. Як і раніше, r можна знайти алгоритмом CFE відтворення ланцюгового дробу.

Застосування цього алгоритму до функції $f(x) = a^x \mod N$ по суті еквівалентно знаходженню порядку числа a.

Дискретне логарифмування

Нехай $N > 0$ і нам дані числа a, b такі, що $b = a^s \mod N$ для деякого s. Задача дискретного логарифмування полягає у знаходженні числа s. Класично ця задача вважається складною і ця складність використовується в криптографічних алгоритмах (зокрема, в алгоритмах на еліптичних кривих). Поглянемо, як ця задача розв'язується на квантовому комп'ютері.

Нехай r це порядок числа a, тобто $a^r = 1 \mod N$. Розглянемо функцію $f(x_1, x_2) = b^{x_1} a^{x_2} \mod N = a^{sx_1 + x_2} \mod N$. Вона є періодичною з періодом $(1, -s)$, оскільки $f(x_1 + 1, x_2 - s) = f(x_1, x_2)$. До того ж вона є періодичною по кожному аргументу: $f(x_1 + r, x_2) = f(x_1, x_2 + r) = f(x_1, x_2)$.

Відповідною квантовою операцією буде $U_f |x_1\rangle |x_2\rangle |y\rangle = |x_1\rangle |x_2\rangle |y \oplus f(x)\rangle$, де перші два регістри складаються з t кубітів, а третій з m кубітів, $2^m > N$.

Дискретне логарифмування

Використовуємо стандартний прийом – до стану $|0^t\rangle|0^t\rangle|0^m\rangle$ застосовуємо операцію Уолша-Адамара до перших регістрів та U_f до результату:

$$U_f(H^{\otimes t}\otimes H^{\otimes t}\otimes I)\left|0^t\right\rangle\left|0^t\right\rangle|0^m\rangle = \frac{1}{2^t}\sum_{x_1=0}^{2^t-1}\sum_{x_2=0}^{2^t-1}|x_1\rangle|x_2\rangle|f(x_1,x_2)\rangle.$$

По аналогії до попереднього позначимо для $l_1, l_2 = 0, 1, \ldots, r-1$

$$\left|\hat{f}(l_1,l_2)\right\rangle = \frac{1}{r\sqrt{r}}\sum_{x_1=0}^{r-1}\sum_{x_2=0}^{r-1} e^{-2\pi i(l_1x_1+l_2x_2)/r}\,|f(x_1,x_2)\rangle.$$

Тоді

$$|f(x_1,x_2)\rangle = \frac{1}{\sqrt{r}}\sum_{l_1=0}^{r-1}\sum_{l_2=0}^{r-1} e^{2\pi i(l_1x_1+l_2x_2)/r}\left|\hat{f}(l_1,l_2)\right\rangle.$$

Дискретне логарифмування

Оскільки $f(x_1, x_2) = f(0, x_2 + sx_1)$, то зробивши заміну змінних $j = x_2 + sx_1 \mod r$ матимемо

$$\left|\hat{f}(l_1, l_2)\right\rangle = \frac{1}{r\sqrt{r}} \sum_{x_1=0}^{r-1} \sum_{j=0}^{r-1} e^{-2\pi i(l_1 x_1 + l_2(j - sx_1))/r} \left|f(0, j)\right\rangle =$$

$$= \frac{1}{r\sqrt{r}} \sum_{j=0}^{r-1} e^{-2\pi i l_2 j/r} \sum_{x_1=0}^{r-1} e^{-2\pi i x_1(l_1 - sl_2)/r} \left|f(0, j)\right\rangle =$$

$$= \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} e^{-2\pi i l_2 j/r} \left|f(0, j)\right\rangle,$$

якщо $l_1 - sl_2 = 0 \mod r$, та дорівнює 0 інакше. Звідси

$$\left|f(x_1, x_2)\right\rangle = \frac{1}{\sqrt{r}} \sum_{l_2=0}^{r-1} e^{2\pi i(sl_2 x_1 + l_2 x_2)/r} \left|\hat{f}(sl_2, l_2)\right\rangle.$$

Дискретне логарифмування

Загалом, можемо написати, що

$$\frac{1}{2^t}\sum_{x_1=0}^{2^t-1}\sum_{x_2=0}^{2^t-1}|x_1\rangle|x_2\rangle|f(x_1,x_2)\rangle =$$

$$= \frac{1}{2^t\sqrt{r}}\sum_{l_2=0}^{r-1}\sum_{x_1=0}^{2^t-1}\sum_{x_2=0}^{2^t-1} e^{2\pi i(sl_2x_1+l_2x_2)/r}\,|x_1\rangle|x_2\rangle\left|\hat{f}(sl_2,l_2)\right\rangle =$$

$$= \frac{1}{2^t\sqrt{r}}\sum_{l_2=0}^{r-1}\left(\sum_{x_1=0}^{2^t-1} e^{2\pi isl_2x_1/r}\,|x_1\rangle\right)\left(\sum_{x_2=0}^{2^t-1} e^{2\pi il_2x_2/r}\,|x_2\rangle\right)\left|\hat{f}(sl_2,l_2)\right\rangle.$$

Застосування $QFT_{2^t}^{-1}$ до кожного з перших двох регістрів дасть нам стан

$$\frac{1}{\sqrt{r}}\sum_{l_2=0}^{r-1}\left|\widetilde{sl_2/r}\right\rangle\left|\widetilde{l_2/r}\right\rangle\left|\hat{f}(sl_2,l_2)\right\rangle.$$

Вимірювання перших двох регістрів дасть нам оцінку дробів sl_2/r та l_2/r для випадкового значення l_2 (з однаковою ймовірністю). Звідси s знаходиться застосуванням CFE.

Завдання

Нехай є якийсь стан $|v\rangle = \sum_{i=1}^{r} \alpha_i |x_i\rangle |y_i\rangle$ на просторі з $t + m$ кубітів, де $\{|y_i\rangle\}$ ортонормовані (тобто частина якогось повного базису, не обов'язково стандартного), а $\{|x_i\rangle\}$ просто будь-які стани з нормою 1.

Відомо, що для базисного стану $|b\rangle = |b_1 b_2 .. b_t\rangle$ виконується нерівність $|\langle b|x_i\rangle|^2 < \varepsilon$ для кожного i.

Показати, що ймовірність отримати b при вимірюванні першого регістру $|v\rangle$ в стандартному базисі не перевищує ε.
(використати матрицю густини)