Квантове перетворення Фур'є. Алгоритм оцінки фази.

Лекція 7

21 березня 2023

Матриця перетворення Фур'є

Нехай $N > 0$, через $\omega = e^{2\pi i/N}$ позначимо примітивний корінь степеня N з одиниці. Матрицею Фур'є називають матрицю розміру $N \times N$, що складається з коефіцієнтів $\{\omega^{ij}/\sqrt{N}\}_{i,j=0}^{N-1}$:

$$F_N = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{N-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \dots & \omega^{(N-1)(N-1)} \end{pmatrix}$$

Ця матриця є унітарною, а обернена до неї матриця $F_N^{-1} = F_N^\dagger$ має коефіцієнти $\{\omega^{-ij}/\sqrt{N}\}_{i,j=0}^{N-1}$. Тобто $F_N^\dagger = \overline{F_N}$.

Матриця F_N^{-1} відповідає перетворенню N чисел $\{x_k\}_{k=0}^{N-1} \in \mathbb{C}$ при дискретному перетворенні Фур'є:

$$\widetilde{x_k} = \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} \omega^{-kl} x_l$$

Квантове перетворення Фур'є

У випадку $N = 2^n$ ця матриця визначає *квантове перетворення Фур'є*:

$$F_{2^n} = \frac{1}{\sqrt{2^n}} \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{2^n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{2^n-1} & \omega^{2(2^n-1)} & \dots & \omega^{(2^n-1)(2^n-1)} \end{pmatrix}$$

що діє на просторі станів системи з n кубітів.

Квантове перетворення Фур'є має численні застосування в конструюванні квантових алгоритмів. Хоча F_{2^n} і має розмір $2^n \times 2^n$, її можна реалізувати за допомогою порядку $O(n^2)$ примітивних гейтів (CNOT та однокубітних).

Дія перетворення Фур'є F_{2^n} на стандартний базис

Для $b_i \in \mathbf{B}$ позначимо

$$0.b_1 b_2 \ldots b_n = (b_1 b_2 \ldots b_n)_2 / 2^n = b_1/2 + b_2/4 + \cdots + b_n/2^n,$$

тобто це двійковий дробовий запис.

Має місце наступна лема

Лема

$$F_{2^n} |b_1 b_2 \ldots b_n\rangle =$$

$$= \frac{1}{2^{n/2}} (|0\rangle + e^{2\pi i 0.b_n} |1\rangle) \otimes (|0\rangle + e^{2\pi i 0.b_{n-1} b_n} |1\rangle) \otimes$$

$$\cdots \otimes (|0\rangle + e^{2\pi i 0.b_1 b_2 \ldots b_n} |1\rangle).$$

Дія перетворення Фур'є F_{2^n} на стандартний базис

Доведення.
Позначимо $\mathbf{b} = (b_1 b_2 \dots b_n)_2$. Для $k = 0, \dots, n-1$ маємо:

$$0.b_{k+1} \dots b_n = b_1 \dots b_k . b_{k+1} \dots b_n \bmod 1 =$$

$$= (b_1 b_2 \dots b_n)_2 \cdot 2^k / 2^n - (b_1 b_2 \dots b_k)_2 \bmod 1 = \mathbf{b} \cdot 2^k / 2^n \bmod 1,$$

Звідси

$$e^{2\pi i 0.b_k b_{k+1} \dots b_n} = e^{2\pi i \cdot \mathbf{b} \cdot 2^k / 2^n}.$$

Дія перетворення Фур'є F_{2^n} на стандартний базис

Маємо, що

$$\frac{1}{2^{n/2}}(|0\rangle+e^{2\pi i 0.b_n}|1\rangle)\otimes(|0\rangle+e^{2\pi i 0.b_{n-1}b_n}|1\rangle)\otimes\cdots\otimes(|0\rangle+e^{2\pi i 0.b_1 b_2 \ldots b_n}|1\rangle)$$

$$= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \sum_{m_l=0}^{1} e^{2\pi i \cdot m_l \cdot \mathbf{b} \cdot 2^{n-l}/2^n} |m_l\rangle =$$

$$= \frac{1}{2^{n/2}} \sum_{m_1=0}^{1} \sum_{m_2=0}^{1} \cdots \sum_{m_n=0}^{1} \bigotimes_{l=1}^{n} e^{2\pi i \cdot m_l \cdot \mathbf{b} \cdot 2^{n-l}/2^n} |m_l\rangle =$$

$$= \frac{1}{2^{n/2}} \sum_{m_1=0}^{1} \sum_{m_2=0}^{1} \cdots \sum_{m_n=0}^{1} e^{2\pi i \cdot \mathbf{b} \cdot \sum_l m_l \cdot 2^{n-l}/2^n} |m_1 m_2 \ldots m_n\rangle =$$

$$= \frac{1}{2^{n/2}} \sum_{\mathbf{m}} e^{2\pi i \cdot \mathbf{b} \cdot \mathbf{m}/2^n} |\mathbf{m}\rangle = F_{2^n} |\mathbf{b}\rangle .$$

Розклад перетворення Фур'є F_{2^n}

Нехай $|\mathbf{x}\rangle = |x_1 x_2 \dots x_n\rangle$, $x_i \in \mathbf{B}$. Позначимо

$$|y_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i 0.x_n} |1\rangle),$$

$$|y_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i 0.x_{n-1}x_n} |1\rangle),$$

$$\vdots$$

$$|y_n\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i 0.x_1 \dots x_n} |1\rangle).$$

Тобто за лемою маємо, що

$$F_{2^n} |x_1 \dots x_n\rangle = |y_1\rangle |y_2\rangle \dots |y_n\rangle .$$

Розклад перетворення Фур'є F_{2^n}

Позначимо

$$R_m = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^m} \end{pmatrix}, \qquad R_1 = Z, R_2 = S, R_3 = T.$$

Не важко бачити, що для будь-якого $k = 0, \ldots, n-1$:

$$\begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i 0.x_{k+1}x_{k+2}\ldots x_n} \end{pmatrix} = R_1^{x_{k+1}} R_2^{x_{k+2}} \ldots R_{n-k}^{x_n}.$$

Тож можна записати, що

$$|y_{n-k}\rangle = R_{n-k}^{x_n} \ldots R_2^{x_{k+2}} R_1^{x_{k+1}} |+\rangle.$$

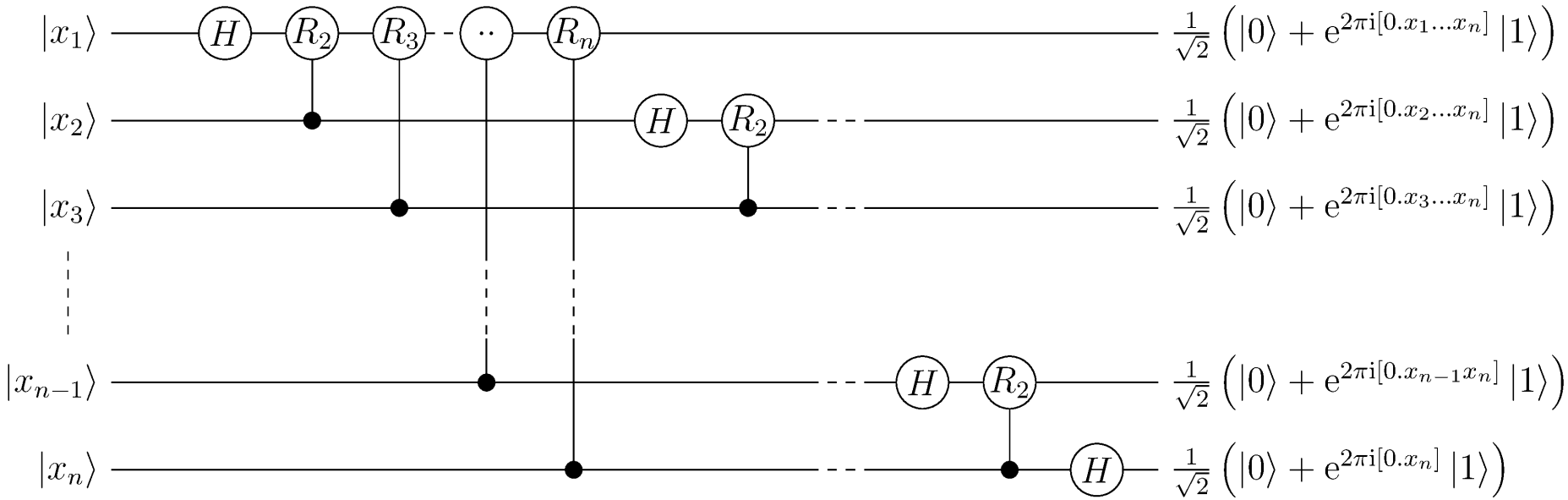
Оскільки $Z^b |+\rangle = H |b\rangle$ для $b \in \mathbf{B}$, то це можна спростити до

$$|y_{n-k}\rangle = R_{n-k}^{x_n} \ldots R_2^{x_{k+2}} H |x_{k+1}\rangle.$$

Зокрема,
$|y_1\rangle = H |x_n\rangle, \quad |y_2\rangle = R_2^{x_n} H |x_{n-1}\rangle, \quad |y_3\rangle = R_3^{x_n} R_2^{x_{n-1}} H |x_{n-2}\rangle.$

Розклад перетворення Фур'є F_{2^n}

Але ж дія $R_m^{x_k}$ відповідає контрольованій дії $C(R_m)$ на цільовий кубіт, де контроль іде по кубіту, який має значення $|x_k\rangle$. Це можна зобразити наступною схемою



Ця схема задає перетворення $|x_1 \ldots x_n\rangle \longrightarrow |y_n\rangle \ldots |y_1\rangle$. Залишається зробити перетворення $|y_n\rangle \ldots |y_2\rangle |y_1\rangle \longrightarrow |y_1\rangle |y_2\rangle \ldots |y_n\rangle$, що можна зробити за допомогою $n/2$ SWAP гейтів.

Алгоритм оцінки фази

Будемо вважати, що невідома нам унітарна операція U діє на n кубітах, і ми маємо доступ до її застосування. Більше того, ми маємо можливість застосовувати контрольовані версії $C(U^{2^k})$.

Нехай $|u\rangle$ це її власний вектор, тобто $U|u\rangle = e^{2\pi i\theta}|u\rangle$.
Припустимо, для початку, що $|u\rangle$ нам відомий.

Задача полягає у наближеному знаходженні відповідного власного значення (фази) $e^{2\pi i\theta}$, тобто параметру $\theta \in [0, 1)$.

Алгоритм оцінки фази

Спершу, поглянемо як діє $C(U^{2^k})$ на $|\psi\rangle|u\rangle$.
Маємо, що

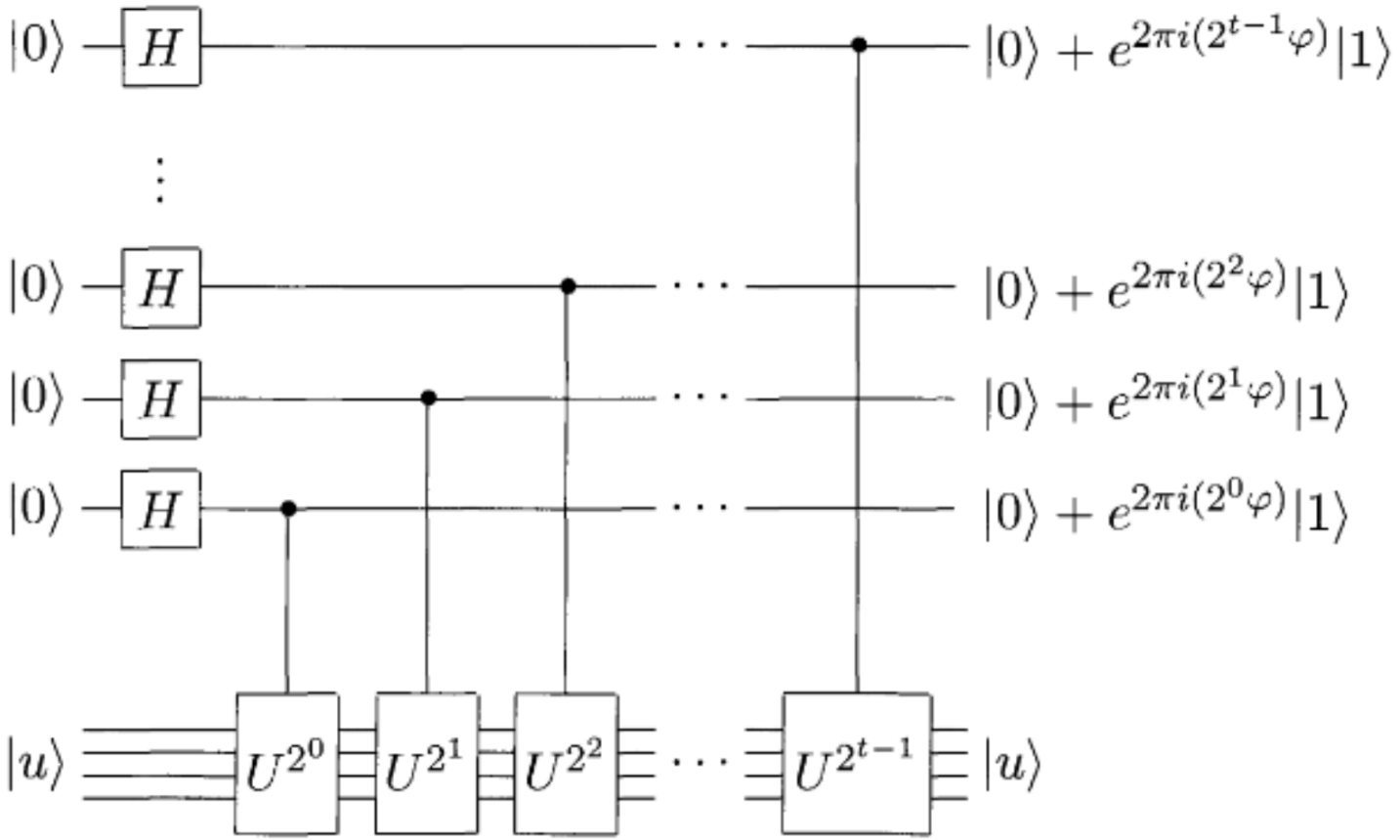
$$C(U^{2^k})|0\rangle|u\rangle = |0\rangle|u\rangle,$$
$$C(U^{2^k})|1\rangle|u\rangle = e^{2\pi i\theta 2^k}|1\rangle|u\rangle,$$

звідси

$$C(U^{2^k})|+\rangle|u\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i\theta 2^k}|1\rangle)|u\rangle.$$

Розглянемо тепер схему з двох регістрів, де перший регістр складається з t кубітів в початковому стані $|+\rangle$, а другий регістр з n кубітів у стані $|u\rangle$:

Алгоритм оцінки фази



Застосуємо t операцій $C_k = C_{[t-k],(t+1\ldots t+n)}(U^{2^k})$, $k = 0, \ldots, t-1$, тобто в операції C_k контроль іде по кубіту з індексом $t-k$.

Алгоритм оцінки фази

Маємо, що

$$\left(\prod_{k=0}^{t-1} C_k\right) |+\rangle^{\otimes t} |u\rangle =$$

$$= \frac{1}{2^{t/2}}(|0\rangle + e^{2\pi i\theta 2^{t-1}} |1\rangle) \otimes (|0\rangle + e^{2\pi i\theta 2^{t-2}} |1\rangle) \dots (|0\rangle + e^{2\pi i\theta 2^{0}} |1\rangle) |u\rangle =$$

$$= \frac{1}{2^{t/2}} \sum_{\mathbf{b}=0}^{2^t-1} e^{2\pi i\theta \mathbf{b}} |\mathbf{b}\rangle |u\rangle,$$

де $\mathbf{b} = (b_1 b_2 \dots b_t)_2 = b_1 2^{t-1} + b_2 2^{t-2} + \dots + b_t$.

Алгоритм оцінки фази

Якщо θ у двійковому розкладі має рівно t бітів, тобто $\theta = 0.\theta_1\theta_2\ldots\theta_t$, то стан першого регістру результату дорівнював би в точності

$$\frac{1}{2^{t/2}} \sum_{\mathbf{b}=0}^{2^t-1} e^{2\pi i\theta\mathbf{b}} \left|\mathbf{b}\right\rangle = F_{2^t} \left|\theta_1\theta_2\ldots\theta_t\right\rangle,$$

оскільки $\theta = (\theta_1\theta_2\ldots\theta_t)_2/2^t$. І тому застосування оберненого перетворення Фур'є до першого регістру дало би стан $\left|\theta_1\theta_2\ldots\theta_t\right\rangle$, вимірювання якого дає нам значення θ_i з ймовірністю одиниця.

Подивимось, що буде в загальній ситуації, коли $\theta = 0.\theta_1\theta_2\ldots\theta_t\theta_{t+1}\ldots$.

Алгоритм оцінки фази

Результатом оберненого перетворення Фур'є буде

$$F_{2^t}^{-1} \frac{1}{2^{t/2}} \sum_{\mathbf{b}=0}^{2^t-1} e^{2\pi i \theta \mathbf{b}} |\mathbf{b}\rangle = \left|\widetilde{\theta}\right\rangle,$$

де $\left|\widetilde{\theta}\right\rangle$ це деякий стан, який взагалі кажучі, не буде базисним.

Нехай $\Theta = (\Theta_1 \Theta_2 \dots \Theta_t)_2$ це ціле число, що найкраще наближає $\theta 2^t = (\theta_1 \theta_2 \dots \theta_t . \theta_{t+1} \theta_{t+2} \dots)_2$.

Тобто, $\Theta = (\theta_1 \theta_2 \dots \theta_t)_2$ якщо $\theta_{t+1} = 0$, інакше $\Theta = (\theta_1 \theta_2 \dots \theta_t)_2 + 1$ (або ж 0, якщо вийшло 2^t).

Для похибки $\Delta = \theta 2^t - \Theta$ маємо оцінку

$$|\Delta| \leqslant 1/2.$$

Алгоритм оцінки фази

Оцінимо похибку $p_\Theta = |\left\langle \Theta \middle| \widetilde{\theta} \right\rangle|^2$.

$$|\Theta\rangle = F_{2^t}^{-1} \frac{1}{2^{t/2}} \sum_{\mathbf{s}=0}^{2^t-1} e^{2\pi i \Theta \mathbf{s}/2^t} |\mathbf{s}\rangle,$$

$$\left\langle \Theta \middle| \widetilde{\theta} \right\rangle = \frac{1}{2^t} \Big(\sum_{\mathbf{s}=0}^{2^t-1} e^{-2\pi i \Theta \mathbf{s}/2^t} \langle \mathbf{s}| \Big) \Big(\sum_{\mathbf{b}=0}^{2^t-1} e^{2\pi i \theta \mathbf{b}} |\mathbf{b}\rangle \Big) =$$

$$= \frac{1}{2^t} \sum_{\mathbf{b}=0}^{2^t-1} e^{2\pi i \mathbf{b}(\theta - \Theta/2^t)} = \frac{1}{2^t} (1 - e^{2\pi i 2^t (\theta - \Theta/2^t)}) / (1 - e^{2\pi i (\theta - \Theta/2^t)}).$$

Алгоритм оцінки фази

Маємо, що

$$|\left\langle \Theta \middle| \widetilde{\theta} \right\rangle| = \frac{1}{2^t}|1 - e^{2\pi i \Delta}|/|1 - e^{2\pi i \Delta / 2^t}|.$$

Використовуючи рівність $|1 - e^{2ix}| = 2|\sin(x)|$ отримуємо

$$|\left\langle \Theta \middle| \widetilde{\theta} \right\rangle| = \frac{1}{2^t}|\sin(\pi\Delta)|/|\sin(\pi\Delta/2^t)|.$$

Оскільки $|\sin(x)| \leqslant |x|$ та $|\sin(x)| \geqslant |x|/(\pi/2)$ для $|x| \leqslant \pi/2$, виходить, що

$$|\left\langle \Theta \middle| \widetilde{\theta} \right\rangle| \geqslant \frac{1}{2^t}|\pi\Delta|/(\pi/2)/|\pi\Delta/2^t| = 2/\pi.$$

Звідси $p_\Theta \geqslant 4/\pi^2$, а значить ймовірність отримати Θ при вимірюванні $\left|\widetilde{\theta}\right\rangle$ у стандартному базисі більше 40%.

Твердження. Ймовірність p_δ при вимірюванні отримати Θ' таке, що $|\Theta' - \Theta| > \delta$, не перевищує $1/2(\delta - 1)$.

Алгоритм оцінки фази

Нехай тепер власний вектор $|u\rangle$ операції U нам невідомий. В такій ситуації ми можемо оцінити фазу випадкого власного вектору.

По спектральній теоремі U має 2^n власних векторів, що утворюють базис усього простору H. Тобто, $\forall k = 1, \ldots, 2^n$ $\exists\, |u_k\rangle$:

$$U\,|u_k\rangle = e^{2\pi i \phi_k}\,|u_k\rangle\,.$$

Алгоритм оцінки фази

Будь-який вектор можна розкласти у базисі $\{|u_k\rangle\}$:

$$|u\rangle = \sum_{k=1}^{2^n} \alpha_k |u_k\rangle .$$

По лінійності, результатом алгоритму квантової оцінки фази (QPE), застосованої до випадкового стану $|u\rangle$ (замість власного) буде стан

$$QPE \left|0^t\right\rangle |u\rangle = \sum_{k=1}^{2^n} \alpha_k \left|\widetilde{\phi_k}\right\rangle |u_k\rangle .$$

Тож вимірювання першого регістру дасть нам значення Φ_k з ймовірністю $|\alpha_k|^2$, де Φ_k це гарна апроксимація параметру ϕ_k (з великою ймовірністю).

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

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

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

Оскільки

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

то одне застосування QPE до $|0^t\rangle|\mathbf{1}\rangle$ дасть нам оцінку якогось s/r для $0 \leqslant s \leqslant r-1$.

Завдання

1. Довести, що матриця Фур'є F_N є унітарною

2. Чому в схемі для перетворення Фур'є не можна змінити порядок груп операцій? (одна група - це послідовність контрольованих операцій $H, R_2, R_3, \ldots, R_k$)

3. Перевірити, що в алгоритмі оцінки фази, застосування контрольованих операцій $C_k = C_{[t-k],(t+1\ldots t+n)}(U^{2^k})$, $k = 0, \ldots, t-1$, до стану $|+\rangle^{\otimes t} |u\rangle$, не залежить від їх порядку.