PC 5228 10.31.2023

Outline

- Quantum Fourier tranform
- Quantum phase estimation
- Order finding, Shor's algorithm

Quantum Fourier Transform.

(I) Discrete Fourier Transform

- Def: $y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \, e^{2\pi i \frac{jk}{N}}$ $\qquad \omega_N = e^{2\pi i/N}$

$$y_0 = \frac{1}{\sqrt{N}} (x_0 + x_1 + \cdots + x_{N-1})$$
$$y_1 = \frac{1}{\sqrt{N}} (x_0 + \omega_N x_1 + \cdots + \omega^{N-1} x_{N-1})$$
$$\vdots$$
$$y_{N-1} = \frac{1}{\sqrt{N}} (x_0 + \omega_N^{N-1} x_1 + \cdots + \omega^{(N-1)^2} x_{N-1})$$

$$\begin{pmatrix} \phi_0 \\ \phi_1 \\ \phi_2 \\ \vdots \\ \phi_{N-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \dots & \omega^{2(N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \dots & \omega^{(N-1)^2} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{N-1} \end{pmatrix}.$$

- Classical algorithm (Fast Fourier transform)

  complexity $O(N \log N)$

(II) Quantum Fourier Transform (QFT)

- Unitary operation U_F $\quad j = 0, 1, \cdots, N-1$

  $k = 0, 1, \cdots, N-1$

  ▷ $U_F|j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i \frac{jk}{N}} |k\rangle$

  ▷ $\sum_{j=0}^{N-1} x_j |j\rangle \xrightarrow{U_F} \sum_{k=0}^{N-1} y_k |k\rangle$

- Binary numbers

  ▷ Decimal number $10.13 = \cdots$

  ▷ Binary number $101.01 = \cdots$

  ▷ Operations of binary number

  addition

  multiplication

$$
\begin{array}{r}
111 \\
110 \\
\hline
000 \\
111 \\
111 \\
\hline
101010
\end{array}
$$

- $e^{2\pi i x}$ $\quad x = p_1 \cdots p_n . q_1 \cdots q_m$

  $\exp(2\pi i x) = \exp(2\pi i \cdot 0.q_1 \cdots q_m)$

- Encoding binary number as a quantum state

  $N = 2^n$

  $j = j_1 \cdots j_n \mapsto |j_1\rangle \otimes \cdots \otimes |j_n\rangle = |j_1 \cdots j_n\rangle$

  $j = j_1 2^{n-1} + \cdots + j_n 2^0$

$$\frac{j\cdot k}{N} = \frac{j\cdot k}{N} = j\cdot\frac{k_1 2^n + \cdots + k_n 2^0}{2^n}$$

$$\begin{aligned}
|j\rangle \to & \frac{1}{2^{n/2}}\sum_{k=0}^{2^n-1} e^{2\pi i jk/2^n}|k\rangle \\
= & \frac{1}{2^{n/2}}\sum_{k_1=0}^{1}\cdots\sum_{k_n=0}^{1} e^{2\pi i j\left(\sum_{l=1}^{n} k_l 2^{-l}\right)}|k_1\ldots k_n\rangle \\
= & \frac{1}{2^{n/2}}\sum_{k_1=0}^{1}\cdots\sum_{k_n=0}^{1}\bigotimes_{l=1}^{n} e^{2\pi i j k_l 2^{-l}}|k_l\rangle \\
= & \frac{1}{2^{n/2}}\bigotimes_{l=1}^{n}\left[\sum_{k_l=0}^{1} e^{2\pi i j k_l 2^{-l}}|k_l\rangle\right] \\
= & \frac{1}{2^{n/2}}\bigotimes_{l=1}^{n}\left[|0\rangle + e^{2\pi i j 2^{-l}}|1\rangle\right] \\
= & \frac{\left(|0\rangle + e^{2\pi i 0.j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle\right)\cdots\left(|0\rangle + e^{2\pi i 0.j_1 j_2\cdots j_n}|1\rangle\right)}{2^{n/2}}.
\end{aligned}$$

(III) QFT algorithm.

- A phase gate $R_l = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^l}\end{pmatrix}$
- Hadamard gate trick

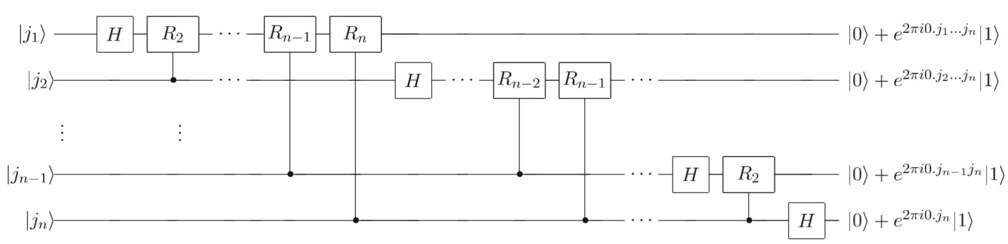
$$H|x\rangle = \frac{1}{\sqrt{2}}\sum(-1)^x|x\rangle$$

$$H|x\rangle = \frac{1}{\sqrt{2}}\sum_z(-1)^{xz}|z\rangle$$

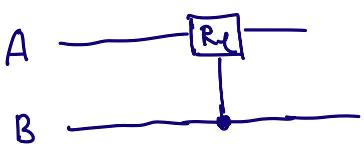
last time (Simon)

$$H|x\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\, 0.x}|1\rangle\right)$$

- Circuit



$C(R_l)$:



$$|\psi\rangle_A = \alpha|0\rangle + \beta|1\rangle$$

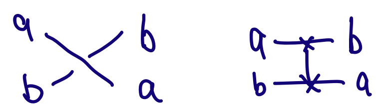
$$\psi_A \otimes b \xrightarrow{C(R_\ell)} \begin{cases} \psi_A & b=0 \\ R_\ell\, \psi_A & b=1 \end{cases} = \begin{cases} \alpha|0\rangle + \beta|1\rangle \\ \alpha|0\rangle + \beta e^{2\pi i/2^\ell}|1\rangle \end{cases}$$

$$= \begin{cases} \alpha|0\rangle + \beta\, e^{2\pi i \cdot \frac{0}{2^\ell}}\, |1\rangle \\ \alpha|0\rangle + \beta\, e^{2\pi i \cdot \frac{1}{2^\ell}}\, |1\rangle \end{cases}$$

$$= \left(\alpha|0\rangle + \beta\, e^{2\pi i \frac{b}{2^\ell}} |1\rangle\right) \otimes |b\rangle$$

- Gate complexity: $\Theta(n^2) = \Theta((\log N)^2)$

- Swap gates. $U_{swap} = \sum_{a,b} E_{a,b} \otimes E_{b,a}$
$$= \frac{1}{2} \sum_{\alpha=0}^{3} \sigma_\alpha \otimes \sigma_\alpha$$



(IV) Inverse QFT.

readout

$$\frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i \frac{kj}{N}} |k\rangle \xrightarrow{U_F^\dagger} |j\rangle$$

▷ $H^\dagger = H$

▷ $C(R_\ell)^\dagger = C(R_\ell^\dagger)$

$$C(R_\ell) = \Pi_0 \otimes I + \Pi_1 \otimes R_\ell = \mathrm{diag}(1, 1, 1, e^{2\pi i/2^\ell})$$

Quantum phase estimation

(I) phase estimation

- The problem: Given a unitary matrix U and an eigenvector

$|u\rangle$, find or estimate its eigenvalue.

remark: Unitary matrix must have eigenvalues of the form $e^{i\theta}$, thus we need to find φ, the is the name "phase estimation"

- Classical solution
  - ▷ $U|u\rangle = e^{i\theta}|u\rangle = e^{2\pi i\varphi}|u\rangle$
  - ▷ U $\quad N\times N$ matrix
  - ▷ complexity $O(N)$ elementary arithmetic operations.

(II) Quantum phase estimation

- Two black boxes
  1. prepare state $|u\rangle$
  2. Controlled $-U^{2^{\ell}}$ gate.

- $U|u\rangle = e^{2\pi i\varphi}|u\rangle \qquad 0\leqslant\varphi<1$

  suppose $\varphi = 0.j_1\cdots j_m \rightsquigarrow j = j_1\cdots j_m$

  $$\frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} e^{2\pi i\frac{k\cdot j}{N}}|k\rangle \mapsto j$$

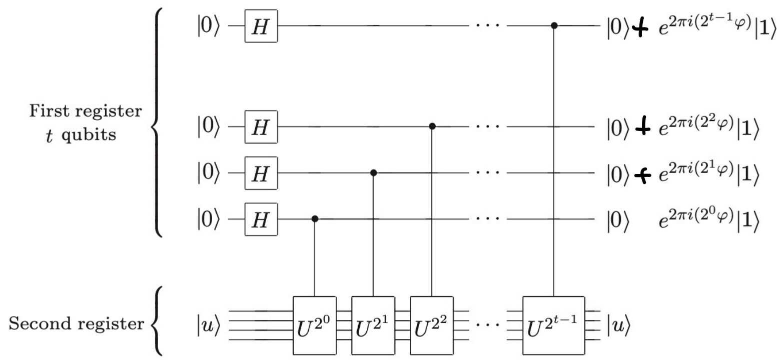
- $U|u\rangle = e^{2\pi i\varphi}$

  $$U^{\alpha}|u\rangle = (e^{2\pi i\varphi})^{\alpha}|u\rangle$$

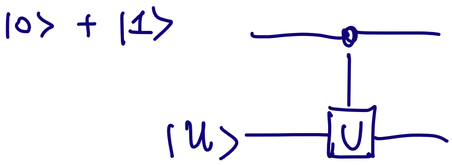
  $$= e^{2\pi i\,\alpha\cdot\varphi}$$

$$U^{2^\ell}|u\rangle = e^{2\pi i\, 2^\ell \cdot \varphi}|u\rangle$$

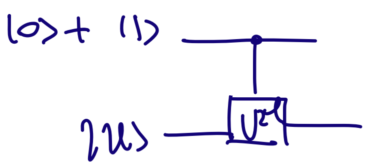
- Circuit



▷ controlled – U

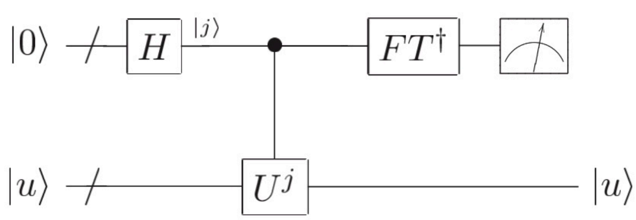


$$|0\rangle|u\rangle + |1\rangle\, U|u\rangle$$
$$\|$$
$$|0\rangle|u\rangle + e^{2\pi i\varphi}|1\rangle|u\rangle$$
$$= (|0\rangle + e^{2\pi i\varphi}|1\rangle)\,|u\rangle$$



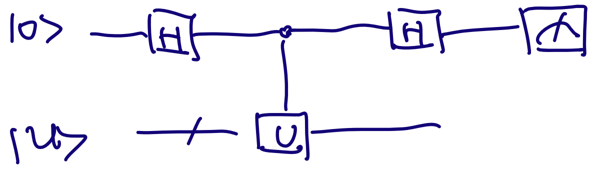
$$(|0\rangle + e^{2\pi i\, \varphi \cdot 2^\ell}|1\rangle) \otimes |u\rangle$$

- $\left(\frac{1}{\sqrt{2^m}} \sum_{k=0}^{2^m-1} e^{2\pi i \frac{j}{2^m}\cdot k}|k\rangle\right) \otimes |u\rangle$



- Complexity $\quad \mathcal{O}(2m + m^2) = \mathcal{O}(m^2)$

(III) Kitaev's phase estimation



final state is $\frac{1+e^{2\pi i \varphi}}{2} |0\rangle + \frac{1-e^{2\pi i \varphi}}{2} |1\rangle$

$\text{Prob}(0) = \cos^2(\pi \varphi)$