科学计算中的量子算法：量子傅立叶变换与量子相位估计

安冬

北京大学北京国际数学研究中心（BICMR）

andong@bicmr.pku.edu.cn

24-25 学年第 2 学期

大纲

- 量子傅立叶变换（Quantum Fourier Transform）
- 量子相位估计（Quantum Phase Estimation）

量子傅立叶变换

定义：

$$U_{\text{QFT}}|j\rangle = \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} e^{i2\pi jk/N}|k\rangle, \quad U_{\text{QFT}} = \frac{1}{\sqrt{N}}(e^{i2\pi jk/N})_{j\in[N],k\in[N]}$$

$$U_{\text{QFT}}^{\dagger}|j\rangle = \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} e^{-i2\pi jk/N}|k\rangle$$

$$U_{\text{QFT}}|0\rangle = \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}|k\rangle = H^{\otimes n}|0\rangle$$

- 传统意义上的逆傅立叶变换
- 传统快速傅立叶变换（FFT）：$\mathcal{O}(N\log(N))$

量子傅立叶变换（QFT）

$$U_{\mathrm{QFT}}\left|j\right\rangle = \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} e^{i2\pi jk/N}\left|k\right\rangle$$

核心思想： U_{QFT} 具有 "类似于张量积" 的形式

QFT：记号

$$N = 2^n$$

$$k = (k_{n-1} \cdots k_1 k_0)_2 = \sum_{l=0}^{n-1} k_l 2^l$$

$$j = (j_{n-1} \cdots j_1 j_0)_2 = \sum_{l=0}^{n-1} j_l 2^l$$

QFT：分解

$$\frac{jk}{N} = \frac{j}{2^n}\sum_{l=0}^{n-1} k_l 2^l = \sum_{l=0}^{n-1} k_l \frac{j}{2^{n-l}}$$
$$= k_0(.j_{n-1}j_{n-2}\cdots j_1 j_0)_2 + k_1(j_{n-1}.j_{n-2}\cdots j_1 j_0)_2 + \cdots + k_{n-1}(j_{n-1}j_{n-2}\cdots j_1.j_0)_2$$

$$e^{i2\pi jk/N} = e^{i2\pi k_0(.j_{n-1}\cdots j_0)_2} e^{i2\pi k_1(j_{n-1}.j_{n-2}\cdots j_0)_2} \dots e^{i2\pi k_{n-2}(j_{n-1}\cdots j_2.j_1 j_0)_2} e^{i2\pi k_{n-1}(j_{n-1}\cdots j_1.j_0)_2}$$
$$= e^{i2\pi k_0(.j_{n-1}\cdots j_0)_2} e^{i2\pi k_1(.j_{n-2}\cdots j_0)_2} \dots e^{i2\pi k_{n-2}(.j_1 j_0)_2} e^{i2\pi k_{n-1}(.j_0)_2}$$

QFT：分解

$$U_{\text{QFT}}\left|j\right\rangle = \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} e^{i2\pi jk/N}\left|k\right\rangle$$

$$= \frac{1}{\sqrt{2^n}}\sum_{k_{n-1},\cdots,k_0} e^{i2\pi k_0(.j_{n-1}\cdots j_0)_2} e^{i2\pi k_1(.j_{n-2}\cdots j_0)_2}\cdots e^{i2\pi k_{n-2}(.j_1 j_0)_2} e^{i2\pi k_{n-1}(.j_0)_2}\left|k_{n-1}\cdots k_1 k_0\right\rangle$$

$$= \frac{1}{\sqrt{2^n}}\left(\sum_{k_{n-1}} e^{i2\pi k_{n-1}(.j_0)_2}\left|k_{n-1}\right\rangle\right)\otimes\left(\sum_{k_{n-2}} e^{i2\pi k_{n-2}(.j_1 j_0)_2}\left|k_{n-2}\right\rangle\right)$$

$$\otimes\cdots\otimes\left(\sum_{k_0} e^{i2\pi k_0(.j_{n-1}\cdots j_1 j_0)_2}\left|k_0\right\rangle\right)$$

$$= \frac{1}{\sqrt{2^n}}\left(\left|0\right\rangle + e^{i2\pi(.j_0)_2}\left|1\right\rangle\right)\otimes\left(\left|0\right\rangle + e^{i2\pi(.j_1 j_0)_2}\left|1\right\rangle\right)\otimes\cdots\otimes\left(\left|0\right\rangle + e^{i2\pi(.j_{n-1}\cdots j_0)_2}\left|1\right\rangle\right)$$

QFT：分解

$$
\begin{aligned}
&|j_{n-1}\rangle \otimes |j_{n-2}\rangle \otimes \cdots \otimes |j_1\rangle \otimes |j_0\rangle \\
\mapsto\ & \frac{1}{\sqrt{2^n}} \left(|0\rangle + e^{i2\pi(.j_0)_2}|1\rangle\right) \otimes \left(|0\rangle + e^{i2\pi(.j_1 j_0)_2}|1\rangle\right) \otimes \cdots \otimes \left(|0\rangle + e^{i2\pi(.j_{n-1}\cdots j_0)_2}|1\rangle\right)
\end{aligned}
$$

我们先暂时交换输出量子比特的顺序，并考虑：

$$
\begin{aligned}
&|j_{n-1}\rangle \otimes \cdots \otimes |j_1\rangle \otimes |j_0\rangle \\
\mapsto\ & \frac{1}{\sqrt{2^n}} \left(|0\rangle + e^{i2\pi(.j_{n-1}\cdots j_0)_2}|1\rangle\right) \otimes \cdots \otimes \left(|0\rangle + e^{i2\pi(.j_1 j_0)_2}|1\rangle\right) \otimes \left(|0\rangle + e^{i2\pi(.j_0)_2}|1\rangle\right)
\end{aligned}
$$

QFT：算法

0: Hadamard

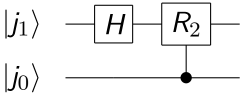
$$|j_0\rangle \mapsto \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i2\pi(.j_0)_2}|1\rangle\right)$$

1:

$$|j_1\rangle \mapsto \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i2\pi(.j_1j_0)_2}|1\rangle\right) = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i2\pi(.0j_0)_2}e^{i2\pi(.j_1)_2}|1\rangle\right)$$

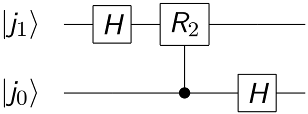
$$|j_1\rangle \mapsto \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i2\pi(.j_1)_2}|1\rangle\right) \mapsto \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i2\pi(.0j_0)_2}e^{i2\pi(.j_1)_2}|1\rangle\right)$$

QFT：算法



$$R_2 = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/2} \end{pmatrix}$$

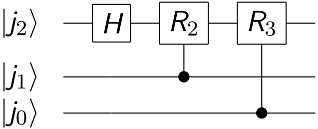
总的运算： $|j_1\rangle\,|j_0\rangle \mapsto \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i2\pi(.j_1j_0)_2}\,|1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i2\pi(.j_0)_2}\,|1\rangle\right)$



QFT：算法

2:

$$|j_2\rangle \mapsto \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i2\pi(.j_2j_1j_0)_2}\,|1\rangle\right) = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i2\pi(.00j_0)_2}\,e^{i2\pi(.0j_1)_2}\,e^{i2\pi(.j_2)_2}\,|1\rangle\right)$$

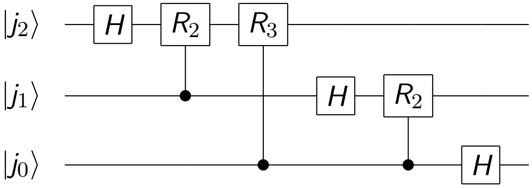


$$R_2 = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/2} \end{pmatrix}, \quad R_3 = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/2^2} \end{pmatrix}$$

QFT：算法

总的运算：

$$
\begin{aligned}
&|j_2\rangle\,|j_1\rangle\,|j_0\rangle \\
\mapsto\ & \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i2\pi(.j_2 j_1 j_0)_2}\,|1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i2\pi(.j_1 j_0)_2}\,|1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i2\pi(.j_0)_2}\,|1\rangle\right)
\end{aligned}
$$

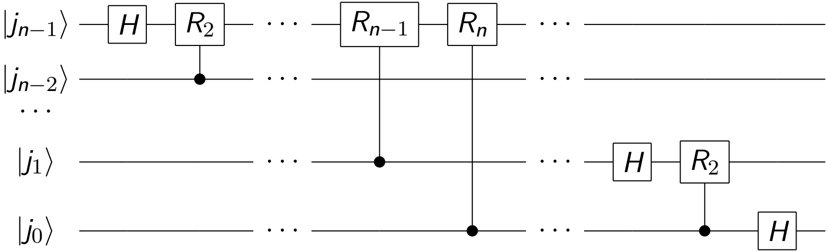


$$
R_l = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/2^{l-1}} \end{pmatrix}
$$

QFT：算法

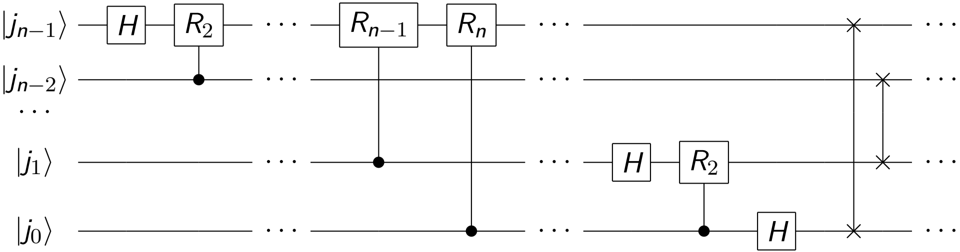
一般情况（注意此时输出比特的顺序是反的）:

$$
\begin{aligned}
&|j_{n-1}\rangle \otimes \cdots \otimes |j_1\rangle \otimes |j_0\rangle \\
\mapsto &\frac{1}{\sqrt{2^n}} \left(|0\rangle + e^{i2\pi(.j_{n-1}\cdots j_0)_2}|1\rangle\right) \otimes \cdots \otimes \left(|0\rangle + e^{i2\pi(.j_1 j_0)_2}|1\rangle\right) \otimes \left(|0\rangle + e^{i2\pi(.j_0)_2}|1\rangle\right)
\end{aligned}
$$



QFT：算法

QFT 最终算法：



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

量子门复杂度： $\mathcal{O}((\log(N))^2)$ （对比经典 FFT： $\mathcal{O}(N\log(N))$）

QFT：小结

$$U_{\mathrm{QFT}}|j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{i2\pi jk/N} |k\rangle$$

量子门复杂度：$\mathcal{O}(n^2) = \mathcal{O}((\log(N))^2)$

拓展：

- 近似量子傅立叶变换（Approximate Quantum Fourier Transform）
- 量子余弦/正弦变换（Quantum Cosine/Sine Transform）
- 量子拉普拉斯变换（Quantum Laplace Transform）

量子相位估计（QPE）

U 是一个酉矩阵，$|\psi\rangle$ 是它的一个特征向量，满足：

$$U\,|\psi\rangle = e^{i2\pi\phi}\,|\psi\rangle\,, \quad \phi \in [0,1)$$

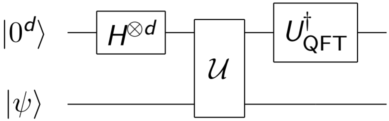
目标：求 ϕ

QPE：精确情况

假设 ϕ 可以被 d 位二进制精确表示：

$$\phi = (0.\phi_{d-1}\cdots\phi_1\phi_0)_2$$
$$\Longleftrightarrow \quad \exists k \in [2^d] \quad s.t. \quad \phi = \frac{k}{2^d}$$

QPE：精确情况



$$\mathcal{U} = \sum_{j\in[2^d]} |j\rangle\langle j| \otimes U^j$$

$$|0^d\rangle|\psi\rangle \to \frac{1}{\sqrt{2^d}}\sum_{j\in[2^d]}|j\rangle|\psi\rangle \to \frac{1}{\sqrt{2^d}}\sum_{j\in[2^d]}|j\rangle U^j|\psi\rangle = \frac{1}{\sqrt{2^d}}\sum_{j\in[2^d]}|j\rangle e^{i2\pi\phi j}|\psi\rangle$$

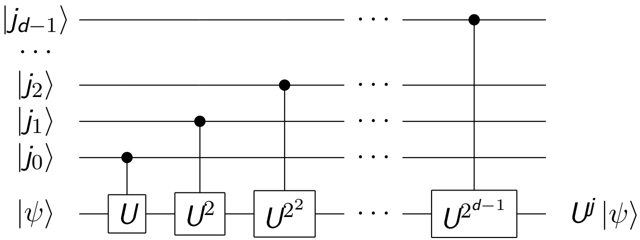
$$\to \frac{1}{2^d}\sum_{j\in[2^d]}\left(\sum_{k'\in[2^d]} e^{-i2\pi jk'/2^d}|k'\rangle\right)e^{i2\pi\phi j}|\psi\rangle$$

$$= \sum_{k'\in[2^d]}\left(\frac{1}{2^d}\sum_{j\in[2^d]} e^{i2\pi j(\phi-k'/2^d)}\right)|k'\rangle|\psi\rangle = |k\rangle|\psi\rangle$$

QPE：精确情况

$$j = (j_{d-1} \cdots j_1 j_0)_2 = \sum_{l=0}^{d-1} j_l 2^l$$

$$\mathcal{U} = \sum_{j \in [2^d]} |j\rangle \langle j| \otimes U^j = \sum_{j_{d-1}, \cdots, j_0} (|j_{d-1}\rangle \langle j_{d-1}| \otimes \cdots \otimes |j_0\rangle \langle j_0|) \otimes \prod_{l=0}^{d-1} \left(U^{2^l}\right)^{j_l}$$



访问复杂度： $1 + 2 + 2^2 + \cdots + 2^{d-1} = \mathcal{O}(2^d)$

QPE：近似情况

$$U|\psi\rangle = e^{i2\pi\phi}|\psi\rangle, \quad \phi \in [0,1)$$

1. ϕ 不一定有精确 d 位二进制表示
2. $|\psi\rangle$ 不一定是精确的特征向量
3. U 的实现可能有误差

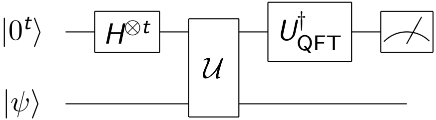
我们接下来分别分析 1 和 3 的情况

QPE：近似情况

对于一般的 $\phi \in [0, 1)$，希望找到一个误差不超过 $\epsilon = 2^{-d}$ 的近似

$$|\theta|_1 = \min\{(\theta \bmod 1), 1 - (\theta \bmod 1)\}$$

思路： 取足够多 $(t > d)$ 的辅助量子比特，使得需要的部分振幅足够大



$$|0^t\rangle|\psi\rangle \to \sum_{k' \in [T]} \left(\frac{1}{T} \sum_{j \in [T]} e^{i 2\pi j(\phi - k'/T)} \right) |k'\rangle |\psi\rangle$$

QPE：近似情况

$$|0^t\rangle |\psi\rangle \to \sum_{k' \in [T]} \left(\frac{1}{T} \sum_{j \in [T]} e^{i2\pi j(\phi - k'/T)} \right) |k'\rangle |\psi\rangle = \sum_{k' \in [T]} \gamma_{k'} |k'\rangle |\psi\rangle$$

$$\gamma_{k'} = \frac{1}{T} \sum_{j \in [T]} e^{i2\pi j(\phi - k'/T)} = \frac{1}{T} \frac{1 - e^{i2\pi T(\phi - k'/T)}}{1 - e^{i2\pi(\phi - k'/T)}}$$

$$\mathbb{P}(k') = |\gamma_{k'}|^2 = \frac{1}{T^2} \frac{\sin^2(\pi T(\phi - k'/T))}{\sin^2(\pi(\phi - k'/T))} \leq \frac{1}{4T^2 |\phi - k'/T|_1^2}$$

QPE：近似情况

记测量之后的第一个寄存器变为 $|\tilde{k}\rangle$，对应的特征值估计为 $\tilde{k}/T$

$$\begin{aligned}\mathbb{P}(|\phi - \tilde{k}/T|_1 \geq \epsilon) &= \sum_{k':|\phi - k'/T|_1 \geq \epsilon} \mathbb{P}(k') \leq \sum_{k':|\phi - k'/T|_1 \geq \epsilon} \frac{1}{4T^2|\phi - k'/T|_1^2} \\ &\leq \frac{1}{2T}\int_x^\infty \frac{1}{x^2} + \frac{1}{2T^2\epsilon^2} = \frac{1}{2T\epsilon} + \frac{1}{2(T\epsilon)^2} \leq \frac{1}{T\epsilon}\end{aligned}$$

为了保证算法至少以 $1-\delta$ 的概率成功，我们可以取 $T = 1/(\epsilon\delta)$

- 访问复杂度：$\mathcal{O}(T) = \mathcal{O}(1/(\epsilon\delta))$
- 额外的量子比特数量：$t = d + \log_2(1/\delta)$

QPE：酉矩阵的误差

考虑 U 的实际量子线路实现 $\widetilde{U}$，满足

$$\|\widetilde{U} - U\| \leq \epsilon$$

Theorem (Theorem VI.3.11[1])

设 U 和 $\widetilde{U}$ 是两个酉矩阵，λ_j 和 $\widetilde{\lambda}_j$ 是它们的特征值（经过适当的重排），那么

$$|\widetilde{\lambda}_j - \lambda_j| \leq \|\widetilde{U} - U\|$$

[1] Rajendra Bhatia. Matrix Analysis, volume 169 of Graduate Texts in Mathematics. Springer, 1997.

QPE：酉矩阵的误差

记 $\widetilde{\phi}$ 是对 $\widetilde{U}$ 做 QPE 得到的精确结果，那么

$$\left|e^{i2\pi\widetilde{\phi}} - e^{i2\pi\phi}\right| \leq \|\widetilde{U} - U\| \leq \epsilon.$$

又

$$\left|e^{i2\pi\widetilde{\phi}} - e^{i2\pi\phi}\right| = 2\sin(\pi(\widetilde{\phi} - \phi)) \geq 4|\widetilde{\phi} - \phi|_1,$$

我们有

$$|\widetilde{\phi} - \phi|_1 \leq \frac{\epsilon}{4}.$$

QPE：小结

$$U|\psi\rangle = e^{i2\pi\phi}|\psi\rangle, \quad \phi \in [0,1)$$

访问复杂度：$\mathcal{O}(1/(\epsilon\delta))$

额外的量子比特数量：$\log_2(1/\epsilon) + \log_2(1/\delta)$

拓展：

- QPE 的初始化
- 其他版本的 QPE

阅读

阅读：

- LL: Chapter 3.3, 3.4, 3.5, 3.2*