量子信息与量子密码

Quantum Information & Quantum Cryptology

[第7次课] 量子算法

授课教师：杨理

授课时间：2022年4月18日

内容概要

第一部分：Shor因子分解量子算法

一、 量子Fourier变换

二、 相位估计

三、 离散对数量子算法举例

四、 求阶

五、因子分解

一、 量子Fourier变换

1. 量子Fourier变换

经典离散 Fourier 变换（DFT）

$$y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi ijk/N} .$$

量子情形，定义

$$|j\rangle \xrightarrow{\mathrm{QFT}(N)} \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi ijk/N} |k\rangle,$$

量子Fourier变换

易知，对任意态 $\sum_{j=0}^{N-1} x_j |j\rangle$ 有：

$$\sum_{j=0}^{N-1} x_j |j\rangle \xrightarrow{\mathrm{QFT}(N)} \sum_{j=0}^{N-1} x_j \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi ijk/N} |k\rangle$$

$$= \sum_{k=0}^{N-1} \left(\frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi ijk/N} \right) |k\rangle$$

$$= \sum_{k=0}^{N-1} y_k |k\rangle .$$

量子Fourier变换

QFT的酉性：只需证明 $\left|j_1'\right\rangle = \mathrm{QFT}(N)\left|j_1\right\rangle$ 与 $\left|j_2'\right\rangle = \mathrm{QFT}(N)\left|j_2\right\rangle$

满足 $\left\langle j_1'\middle|j_2'\right\rangle = \delta_{j_1' j_2'}$ 即可.

QFT的积形式：$\begin{cases} j \text{ 可表示为 } j_1 j_2 \cdots j_n \text{ 形式（二进制），} \\ j = j_1 2^{n-1} + j_2 2^{n-2} + \cdots + j_n . \end{cases}$

$$\left|j_1, \cdots, j_n\right\rangle \xrightarrow{\mathrm{QFT}} \frac{1}{\sqrt{2^n}}\left(\left|0\right\rangle + e^{2\pi i 0.j_n}\left|1\right\rangle\right)\left(\left|0\right\rangle + e^{2\pi i 0.j_{n-1}j_n}\left|1\right\rangle\right)\cdots$$

$$\cdots\left(\left|0\right\rangle + e^{2\pi i 0.j_1 j_2 \cdots j_n}\left|1\right\rangle\right).$$

量子Fourier变换

其中 $0.j_l j_{l+1}\cdots j_m \equiv \frac{j_l}{2}+\frac{j_{l+1}}{4}+\cdots+\frac{j_m}{2^{m-l+1}}$ 称为二进制小数。

证明：

$$\mathrm{QFT}\left|j\right\rangle = \frac{1}{2^{n/2}}\sum_{k=0}^{2^n-1} e^{2\pi ijk/2^n}\left|k\right\rangle = \frac{1}{2^{n/2}}\sum_{k_1=0}^{1}\cdots\sum_{k_n=0}^{1} e^{2\pi ij\sum_{l=1}^{n}k_l 2^{-l}}\left|k_1\cdots k_n\right\rangle$$

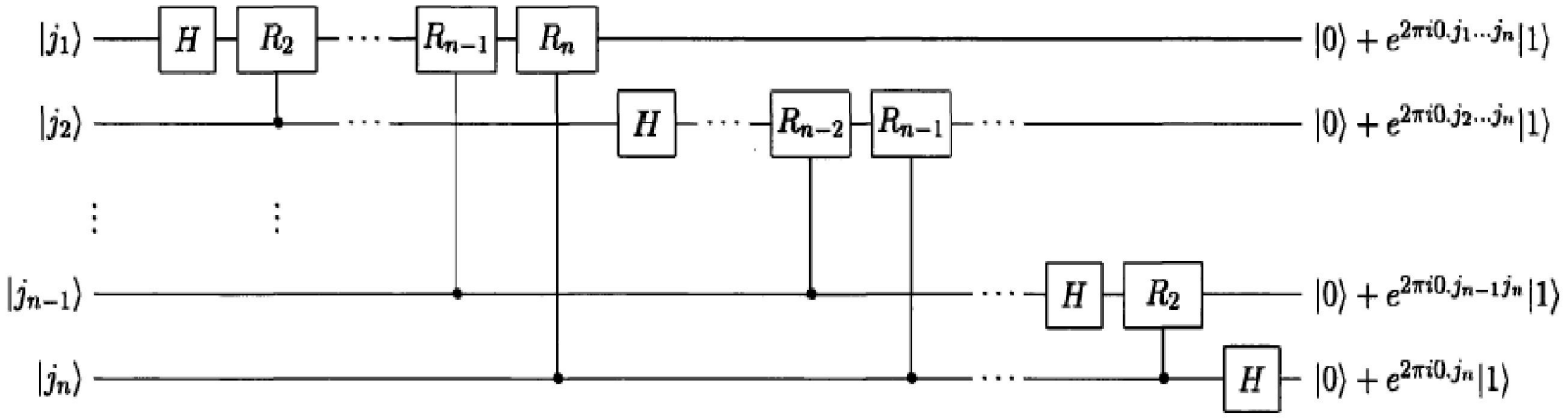
$$= \frac{1}{2^{n/2}}\sum_{k_1=0}^{1}\cdots\sum_{k_n=0}^{1} e^{2\pi ijk_1 2^{-1}}\left|k_1\right\rangle\cdots e^{2\pi ijk_n 2^{-n}}\left|k_n\right\rangle$$

$$= \frac{1}{2^{n/2}}\left(\left|0\right\rangle + e^{2\pi ij2^{-1}}\left|1\right\rangle\right)\cdots\left(\left|0\right\rangle + e^{2\pi ij2^{-n}}\left|1\right\rangle\right)$$

$$= \frac{1}{2^{n/2}}\left(\left|0\right\rangle + e^{2\pi i0.j_n}\left|1\right\rangle\right)\left(\left|0\right\rangle + e^{2\pi i0.j_{n-1}j_n}\left|1\right\rangle\right)\cdots\left(\left|0\right\rangle + e^{2\pi i0.j_1 j_2\cdots j_n}\left|1\right\rangle\right)$$

量子Fourier变换

QFT的有效线路：



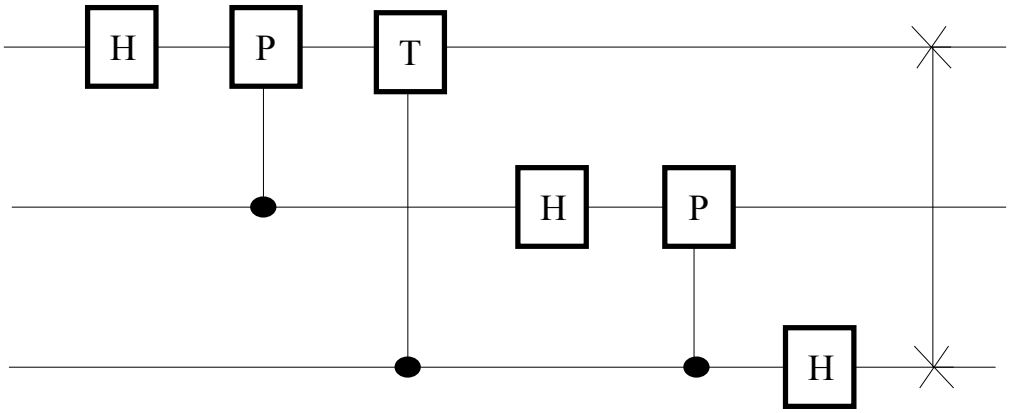
其中 $R_k \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix}$.

注意：受控酉运算在控制位上会产生一个相位差$e^{i\alpha}$ 。

量子Fourier变换

这是一个 $\Theta\left(n^2\right)$ 算法，远较经典算法 $\left(\Theta\left(n2^n\right)\right)$ 为好。

3qubit QFT，即 QFT(8)：$P=\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}$ $T=\begin{bmatrix}1 & 0\\ 0 & e^{i\frac{\pi}{4}}\end{bmatrix}$



二、 相位估计

调用量子黑盒的算法。

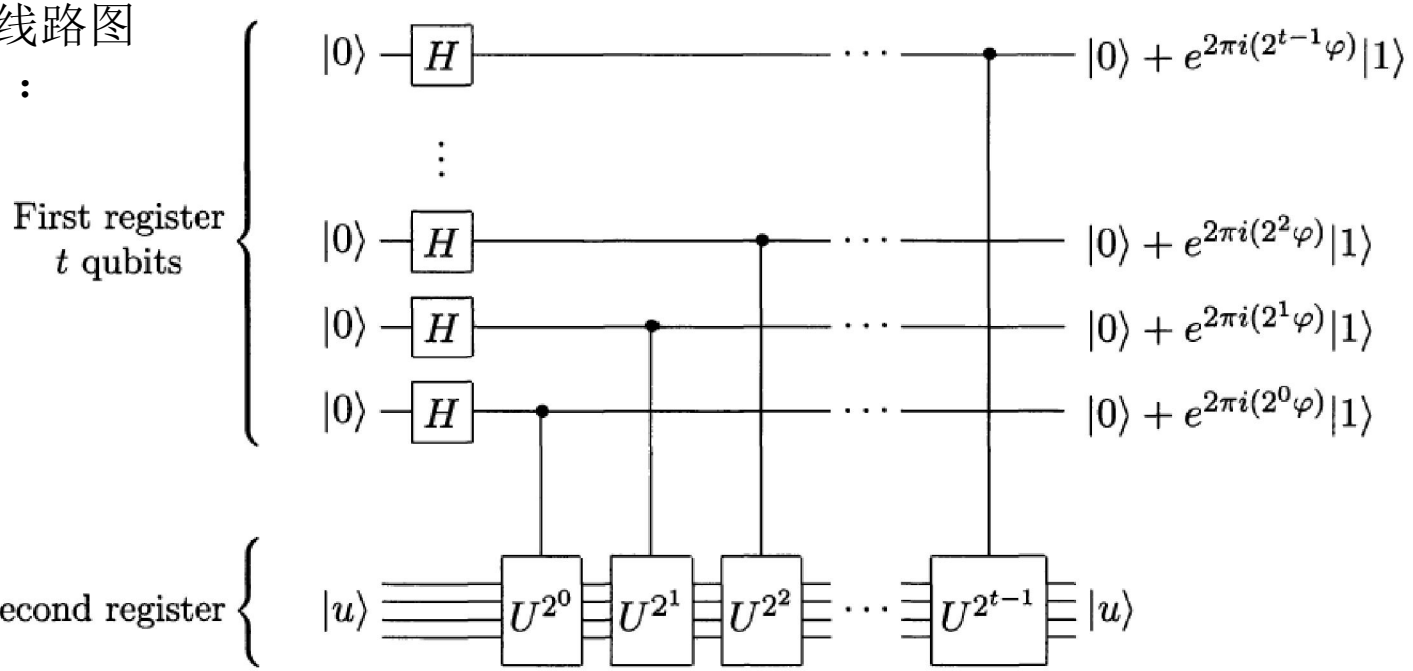
利用 $U|u\rangle = e^{2\pi i\varphi}|u\rangle$,

即：构造 U 算子及其本征态 $|u\rangle$，使得其本征值为 $e^{2\pi i\varphi}$.

受控 U 运算：把 $|j\rangle|u\rangle$ 变为 $|j\rangle U^j|u\rangle$.

相位估计

①线路图


First register
t qubits
Second register
$|0\rangle$
$|u\rangle$
H
U^{2^0}
U^{2^1}
U^{2^2}
$U^{2^{t-1}}$
$|0\rangle + e^{2\pi i(2^{t-1}\varphi)}|1\rangle$
$|0\rangle + e^{2\pi i(2^2\varphi)}|1\rangle$
$|0\rangle + e^{2\pi i(2^1\varphi)}|1\rangle$
$|0\rangle + e^{2\pi i(2^0\varphi)}|1\rangle$
$|u\rangle$

相位估计

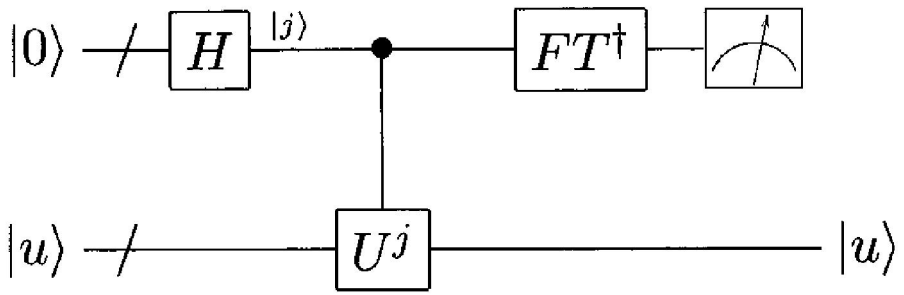
$$\frac{1}{2^{t/2}}\left(|0\rangle+e^{2\pi i 2^{t-1}\varphi}|1\rangle\right)\cdots\left(|0\rangle+e^{2\pi i 2^{0}\varphi}|1\rangle\right)=\frac{1}{2^{t/2}}\sum_{k=0}^{2^t-1}e^{2\pi i\varphi k}|k\rangle$$

当 $\varphi=\frac{j}{N}$，$N=2^t$ 时，易见：

$$(\mathrm{QFT})^{-1}\left[\frac{1}{2^{t/2}}\sum_{k=0}^{2^t-1}e^{2\pi ijk/N}|k\rangle\right]=|j\rangle \overset{\text{测量}}{\Rightarrow} \varphi=\frac{j}{N}$$

相位估计

相位估计的总线路图：



上面的t 个量子位（ ‘/’表示一束线）是第一个寄存器；

下面的一些量子位是第二个寄存器, 其量子位数目须保证可以执行U.

相位估计

② 逆QFT：

$$\frac{1}{2^{t/2}}\sum_{k=0}^{2^t-1} e^{2\pi i\varphi k}\left|k\right\rangle \xrightarrow{QFT^{-1}} \frac{1}{2^t}\sum_{k.l=0}^{2^t-1} e^{-2\pi ikl/2^t} e^{2\pi i\varphi k}\left|l\right\rangle$$

当 $\varphi = t$ 比特整数$/2^t$ ，即$\varphi = 0.\varphi_1\cdots\varphi_t$，则

①中线路给出结果正是QFT的积形式 $\overset{\text{QFT}^{-1}}{\Rightarrow}\left|\varphi_1\cdots\varphi_t\right\rangle.$

否则 QFT $^{-1}$ 后给出的是计算基态的叠加。

可以证明能够实现以给定的概率得到φ 的一个给定精度内的近似值。

相位估计

教材上（5.22）式写得不明确：

如果 $|\tilde{\varphi}\rangle$ 表示计算基的叠加态，就不能写成 $\tilde{\varphi}$，因为 $\tilde{\varphi}$ 又被认为是 φ 的近似值。

③ 参数估计：

取 $0<b<2^t-1$，$b/2^t=0.b_1\cdots b_t$，满足 $0\le\delta\equiv\varphi_u-b/2^t\le 2^{-t}$，

即：在小于 φ 的数中 b 是 φ 的 t 比特最佳近似。

相位估计

$$\frac{1}{2^t}\sum_{k.l=0}^{2^t-1} e^{-2\pi ikl/2^t} e^{2\pi i\varphi k}\left|l\right\rangle \equiv \sum a_l \left|(b+l)\left(\mathrm{mod}\,2^t\right)\right\rangle$$

则可得：

$$a_l = \frac{1}{2^t}\sum_{k=0}^{2^t-1}\left(e^{2\pi i\left(\varphi-(b+l)/2^t\right)}\right)^k$$

$$= \frac{1}{2^t}\frac{1-e^{2\pi i\left(2^t\varphi-(b+l)\right)}}{1-e^{2\pi i\left(\varphi-(b+l)/2^t\right)}} \qquad (1)$$

相位估计

$$p\left(\left|m-b\right|>e\right)\equiv\sum_{\left|l-b\right|>e}\left|a_l\right|^2$$

$$=\sum_{-2^{t-1}<l<-(e+1)}\left|a_l\right|^2+\sum_{e+1<l<2^{t-1}}\left|a_l\right|^2 \qquad (2)$$

由（1），当 $-2^{t-1}<l<2^{t-1}$ 时，

$$\left|a_l\right|\le\left|\frac{1}{2^{t+1}\left(\delta-l/2^t\right)}\right| \qquad (3)$$

又 $0\le 2^t\delta\le 1$，所以有

$$p\left(\left|m-b\right|>e\right)\le\frac{1}{2(e-1)}.$$

相位估计

选择相位φ估计的精确度：

精确到 $2^{-n} \to e = 2^{t-n} - 1$,

如果算法中用 $t = n + p$ 量子比特，可知获得此精度的概率为

$$1 - p\left(\left|m - b\right| > e\right)\Big|_{e=2^{t-n}-1}$$

$$\geq 1 - \frac{1}{2(e-1)} = 1 - \frac{1}{2\left(2^{t-n}-2\right)} \equiv 1 - \varepsilon ,$$

则有： $2\varepsilon = \dfrac{1}{2^{t-n}-2}$, $\dfrac{1}{2\varepsilon} + 2 = 2^{t-n}$,

$$\boxed{t = n + \left\lceil \log\left(2 + \frac{1}{2\varepsilon}\right) \right\rceil}$$

相位估计

④ 量子相位估计算法

输入：　(1) 对整数 j 进行受控 U^j 运算的黑箱；

(2) 制备出 U 的本征值为 $e^{2\pi i\varphi_u}$ 的本征态 $|u\rangle$，

(3) 初始化 $t = n + \left\lceil \log\left(2 + \frac{1}{2\varepsilon}\right)\right\rceil$ 个量子比特处于 $|0\rangle$.

输出：φ_u 的 n 比特近似值 $\tilde{\varphi}_u$.

运行时间：$O(t^2)$ 个操作和一个受控 U^j 运算

成功率 $\geq 1-\varepsilon$.

相位估计

Procedure:

1.	$\|0\rangle\|u\rangle$	initial state
2.	$\rightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} \|j\rangle\|u\rangle$	create superposition
3.	$\rightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} \|j\rangle U^j\|u\rangle$	apply black box
	$= \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} e^{2\pi i j \varphi_u} \|j\rangle\|u\rangle$	result of black box
4.	$\rightarrow \|\widetilde{\varphi_u}\rangle\|u\rangle$	apply inverse Fourier transform
5.	$\rightarrow \widetilde{\varphi_u}$	measure first register

测量后系统进入的是计算基底态$|m\rangle$。中译本改得不对。

相位估计

即：

当 φ_u 不能精确地表为 t 比特时，$\left|\tilde{\varphi}_u\right\rangle$ 应是一个计算基底态的叠加。

测量后才随机地进入一个计算基底态 $\left|m\right\rangle$，而且 $\left|m/2^t-\varphi\right|<2^{-n}$

的概率为 $1-\varepsilon$.

三、 离散对数量子算法举例

Diffie-Hellman 体制：经典的密钥交换，最初的密钥交换协议。

①基于计算假设。

②可被量子计算机攻破，不得不发展量子密钥分配（QKD）协议。

p 为大素数，g 为模 p 的原根，

p, g：公开参数。

离散对数量子算法举例

1. A：选 $0<a<p$ 发送 $g^a \pmod p$
2. B：选 $0<b<p$ 发送 $g^b \pmod p$
3. A 计算 $\left(g^b\right)^a \equiv g^{ab} \pmod p$,

   B 计算 $\left(g^a\right)^b \equiv g^{ab} \pmod p$.

$g^{ab} \pmod p$ 即为 A、B 约定的密钥。

易见，如果能解 $n \equiv g^x \pmod p$ 问题（即：Z_p 上的离散对数问题），上述协议无安全性可言，而量子算法即能有效完成此任务。。

离散对数量子算法举例

阶、原根与指数：

① h 与 p 互素，满足 $h^r \equiv 1 \pmod{p}$ 的最小整数 r 称为 h 模 p 的阶；

② 阶为 $p-1$ 的数 g 称为模 p 的一个原根；

③ $\forall n, p$不能整除$n, \exists a$ 满足 $n \equiv g^a \pmod{p}, 0 \le a < p-1$ 则称 a 为 n 模 p 的指数：$a = \mathrm{ind}_g n$ 。（用原根来表达的幂次，即离散对数）

离散对数量子算法举例

离散对数问题 $\log_P Q \equiv ?\left(\mathrm{mod}\, N\right)$ 的简单量子算法（van Dam）：

设 $P^k \equiv Q\left(\mathrm{mod}\, N\right)$,

$$\frac{1}{N}\sum_{x,y=0}^{N-1}|x\rangle_{\mathrm{I}}|y\rangle_{\mathrm{II}}|0\rangle_{\mathrm{III}} \to \frac{1}{N}\sum_{x,y=0}^{N-1}|x\rangle_{\mathrm{I}}|y\rangle_{\mathrm{II}}\left|Q^x\cdot P^y\right\rangle_{\mathrm{III}}$$

$$=\frac{1}{N}\sum_{x,y=0}^{N-1}|x\rangle_{\mathrm{I}}|y\rangle_{\mathrm{II}}\left|P^{kx+y}\right\rangle_{\mathrm{III}}$$

测量量子寄存器III，得

$$\frac{1}{N}\sum_{x=0}^{N-1}|x\rangle_{\mathrm{I}}|c-kx\rangle_{\mathrm{II}}\left|P^c\right\rangle_{\mathrm{III}}$$

离散对数量子算法举例

应用 $\mathrm{QFT}_N \otimes \mathrm{QFT}_N$ 到量子寄存器I和II：

$$
\begin{aligned}
&\rightarrow \frac{1}{N}\sum_{x=0}^{N-1}\left(\sum_{i=o}^{N-1}\zeta_N^{ix}\left|i\right\rangle_{\mathbf{I}} \otimes \sum_{j=0}^{N-1}\zeta_N^{j(c-xk)}\left|j\right\rangle_{\mathbf{II}}\right) \\
&= \sum_{i,j=0}^{N-1}\zeta_N^{jc}\left(\frac{1}{N}\sum_{x=0}^{N-1}\zeta_N^{x(i-jk)}\right)\left|i\right\rangle_{\mathbf{I}}\left|j\right\rangle_{\mathbf{II}} \\
&= \sum_{j=0}^{N-1}\zeta_N^{jc}\left|jk\right\rangle_{\mathbf{I}}\left|j\right\rangle_{\mathbf{II}}
\end{aligned}
$$

离散对数量子算法举例

这里用到

$$\left(\frac{1}{N} \sum_{x=0}^{N-1} \zeta_N^{x(i-jk)} \right) = \delta_{0,i-jk},$$

上式可从 $i - jk \neq 0$ 时

$$\sum_{j=0}^{N-1} \zeta^{jk} = \frac{1-\zeta^{kN}}{1-\zeta^{k}} = \frac{1-\left(e^{2\pi i}\right)^{k}}{1-e^{2\pi i \cdot \frac{k}{N}}} = 0.$$

看出。

测量量子寄存器 I，II，比较即得 k.

因为寄存器有限位，所以都是在 $\bmod N$ 意义上讨论的。

四、 求阶

由 $$\left|u_s\right\rangle \equiv \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}\exp\left[\frac{-2\pi isk}{r}\right]\left|x^k \bmod N\right\rangle,$$

有 $$\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}\left|u_s\right\rangle = \frac{1}{r}\sum_{s,k=0}^{r-1}\exp\left[\frac{-2\pi isk}{r}\right]\left|x^k \bmod N\right\rangle$$

$$= \sum_{k=0}^{r-1}\left[\frac{1}{r}\sum_{s=0}^{r-1}\exp\left[\frac{-2\pi iks}{r}\right]\right]\left|x^k \bmod N\right\rangle$$

$$= \sum_{k=0}^{r-1}\delta_{0,k}\left|x^k \bmod N\right\rangle$$

$$= \left|1\right\rangle$$

求阶

一、任给正整数 k 有：

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

证明：记 $k_0=k\left(\bmod r\right)$,

$$\begin{aligned}
\text{左}&=\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}e^{2\pi isk/r}\frac{1}{\sqrt{r}}\sum_{k'=0}^{r-1}\exp\left[\frac{-2\pi isk'}{r}\right]\left|x^{k'} \bmod N\right\rangle\\
&=\frac{1}{r}\sum_{s=0}^{r-1}\sum_{k'=0}^{r-1}e^{2\pi i\frac{s}{r}(k_0-k')}\left|x^{k'} \bmod N\right\rangle=\frac{1}{r}\sum_{k'=0}^{r-1}\left(\sum_{s=0}^{r-1}e^{-2\pi i\frac{k'-k_0}{r}s}\right)\left|x^{k'} \bmod N\right\rangle\\
&=\frac{1}{r}\sum_{k'=0}^{r-1}r\cdot\delta_{k'k_0}\left|x^{k'} \bmod N\right\rangle=\left|x^{k_0} \bmod N\right\rangle\\
&=\left|x^k \bmod N\right\rangle
\end{aligned}$$

求阶

二、证明：$U\left|u_s\right\rangle=\exp\left[\frac{2\pi is}{r}\right]\left|u_s\right\rangle$.

(1) $\left|u_s\right\rangle$的定义： $\left|u_s\right\rangle\equiv\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}\exp\left[\frac{-2\pi isk}{r}\right]\left|x^k \bmod N\right\rangle$

(2) U算子的定义： $U\left|y\right\rangle\equiv\left|xy\left(\bmod N\right)\right\rangle$

(3) 阶的定义： $x^r\equiv1\left(\bmod N\right)$

$$\overset{(1,2,3)}{\Longrightarrow}U\left|u_s\right\rangle=\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}\exp\left[\frac{-2\pi isk}{r}\right]\left|x^{k+1} \bmod N\right\rangle$$

$$=\exp\left[\frac{2\pi is}{r}\right]\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}\exp\left[\frac{-2\pi is\left(k+1\right)}{r}\right]\left|x^{k+1} \bmod N\right\rangle$$

求阶

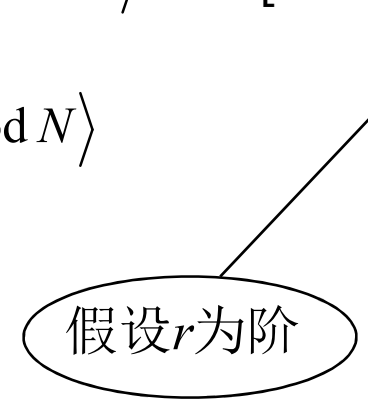
$$= \exp\left[\frac{2\pi is}{r}\right]\frac{1}{\sqrt{r}}\sum_{k=1}^{r}\exp\left[\frac{-2\pi isk}{r}\right]\left|x^k \bmod N\right\rangle$$

$$= \exp\left[\frac{2\pi is}{r}\right]\frac{1}{\sqrt{r}}\left[\sum_{k=1}^{r-1}\exp\left[\frac{-2\pi isk}{r}\right]\left|x^k \bmod N\right\rangle + \exp\left[-2\pi is\right]\left|x^r \bmod N\right\rangle\right]$$

$$= \exp\left[\frac{2\pi is}{r}\right]\frac{1}{\sqrt{r}}\left[\sum_{k=1}^{r-1}\exp\left[\frac{-2\pi isk}{r}\right]\left|x^k \bmod N\right\rangle + \exp\left[-2\pi i\cdot 0\right]\left|x^0 \bmod N\right\rangle\right]$$

$$= \exp\left[\frac{2\pi is}{r}\right]\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}\exp\left[\frac{-2\pi ik}{r}\right]\left|x^k \bmod N\right\rangle$$

$$= \exp\left[\frac{2\pi is}{r}\right]\left|u_s\right\rangle.$$

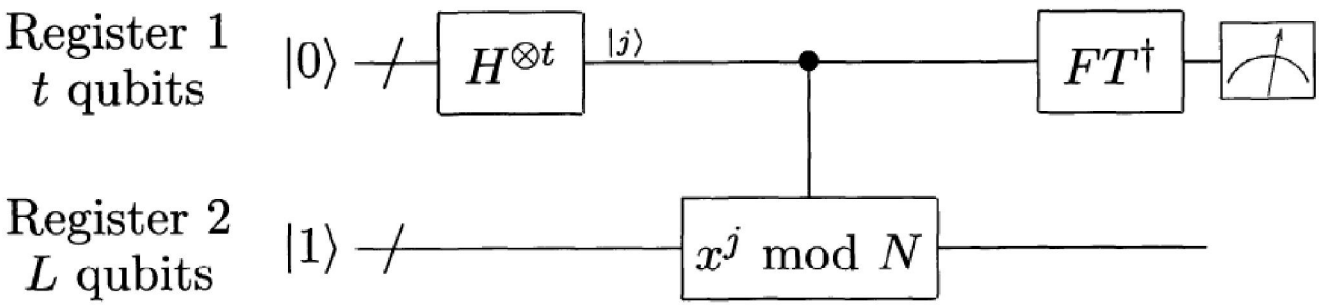


求阶

Procedure:

1.	$\|0\rangle\|1\rangle$	initial state
2.	$\rightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} \|j\rangle\|1\rangle$	create superposition
3.	$\rightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} \|j\rangle\|x^j \bmod N\rangle$	apply $U_{x,N}$
	$\approx \frac{1}{\sqrt{r2^t}} \sum_{s=0}^{r-1} \sum_{j=0}^{2^t-1} e^{2\pi i s j/r} \|j\rangle\|u_s\rangle$	
4.	$\rightarrow \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \|\widetilde{s/r}\rangle\|u_s\rangle$	apply inverse Fourier transform to first register
5.	$\rightarrow \widetilde{s/r}$	measure first register
6.	$\rightarrow r$	apply continued fractions algorithm

求阶


Register 1
t qubits
$|0\rangle$
$H^{\otimes t}$
$|j\rangle$
$FT^{\dagger}$
Register 2
L qubits
$|1\rangle$
$x^j \bmod N$

求阶

问题：1. 第三步中的约等号可以是等号吗?

2. 第四步中的 $\left|(s/r)'\right\rangle$ 应代表由逆Fourier变换生成的叠加态，不是单一的计算基态，只是相对s/r 近似较好的分量几率幅较大，到第五步时才由于测量而坍缩到一个确定的态。

3. 测量值$(s/r)'$是s/r的2L+1比特近似，即2L+1有效位二进制小数。

由 $r \le N \le 2^L$, 知 $\left|s/r-(s/r)'\right| \le 2^{-2L-1} \le \frac{1}{2N^2} \le \frac{1}{2r^2}$

求阶

记 $\varphi \equiv \left(s/r\right)'$，有 $\left|s/r - \varphi\right| \le \frac{1}{2r^2}$，则由定理5.1可知 s/r 是 φ 的一个渐近值，且可用连分式算法在 $\mathrm{O}\left(L^3\right)$ 个运算之内计算出所有的渐近值，即得到 $\left\{\frac{s_i'}{r_i'}, i = 1, \cdots, n\right\}$，$n = \mathrm{O}\left(L\right)$.

由于 φ 的任意两个相邻的渐近分数中至少有一个满足 $\left|s/r - \varphi\right| \le \frac{1}{2r^2}$，似乎无法确定 $\left\{\frac{s_i'}{r_i'}, i = 1, \cdots, n\right\}$ 中哪一个是 s/r，一种办法是逐个验算：$x^{r_i'} \bmod N \stackrel{?}{=} 1$，一种办法是证明事实上只有一个值满足不等式。

五、因子分解

设$N = p \cdot q$，分解 N等价于求 解$F_N(a) \equiv y^a \bmod N$ 的周期：

若 $F_N(a) = F_N(a + kr)$，即 r 是 F_N 的周期，则有 $y^r \equiv 1 \bmod N$。

从欧拉定理知$r < N$。 设r已求出。

当 r 为偶数时，令 $x = y^{r/2}$，则有 $x^2 \equiv 1 \bmod N$，

$(x-1)(x+1) \equiv 0 \bmod N,$

故知 p，q 必包含在 $x-1$ 和 $x+1$的因子之中，

即计算 $\begin{cases} \gcd(x-1, N) \\ \gcd(x+1, N) \end{cases}$ 可得 $\begin{cases} p \\ q \end{cases}$

因子分解

例：$N=15,$ 取 $y=7,\ 7^2\equiv 4\bmod 15,\ 7^4\equiv 1\bmod 15\Rightarrow r=4.$

$$x=y^{r/2}=49,$$

$$(x+1)(x-1)=50\times 48=10\times 16\times 15\equiv 0\bmod 15,$$

$$\gcd(50,15)=5,\ \gcd(48,15)=3,$$

从而得到：$N=3\times 5$

连分式展开：

$$[a_0,a_1,\ldots,a_M]\equiv a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{\ldots+\cfrac{1}{a_M}}}}$$

内容概要

第二部分： Grover量子搜索算法

一、U_a 变换

二、U_s 变换

三、 Grover 迭代

四、从 N 中求 1 问题

五、多搜索目标问题

六、关于“量子摇晃”

Grover算法 —— “从干草堆中找出一根针”

一、 U_a 变换

设有量子黑盒，可计算函数 $f_a(x)$，

$$\begin{cases} f_a(x=a)=1, \\ f_a(x\neq a)=0. \end{cases}$$

$a=(a_1,\cdots,a_n)\in\{0,1\}^n$， $|a\rangle$ 是计算基态之一。

基于调用黑盒，定义酉算子 U_a：

$$U_a|x\rangle|y\rangle\equiv|x\rangle|y\oplus f_a(x)\rangle,$$

U_a 变换

可知 $U_a\left[|x\rangle\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\right]$

$$=|x\rangle\frac{1}{\sqrt{2}}\left(|0\oplus f_a(x)\rangle-|1\oplus f_a(x)\rangle\right)$$

$$=(-1)^{f_a(x)}|x\rangle\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle).$$

略去辅助量子比特，可将酉算子记为

$$U_a|x\rangle=(-1)^{f_a(x)}|x\rangle.$$

U_a 变换

设在上述情形中 $\{|x\rangle \mid x\}$ 为一组正交态，可将 U_a 表达为：

$$U_a = I - 2|a\rangle\langle a|.$$

不知道 a 的情况下，可通过辅助比特和量子黑盒实现 U_a.

U_a 对态空间一般矢量的作用的几何图像：只将 $|a\rangle$ 方向分量的符号改变，相当于对任意态作关于垂直于 $|a\rangle$ 的超平面的反射。

二、U_s 变换

设 $|a\rangle$ 是计算基态之一，$|s\rangle=\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle$，$N=2^n$ $(H^{(n)}|0\rangle=|s\rangle)$，

则 $\langle a|s\rangle=\frac{1}{\sqrt{N}}$，构造 $U_s=2|s\rangle\langle s|-I$，可见 U_s 保持 $|s\rangle$ 态不变，

即 $U_s|s\rangle=2|s\rangle-\langle s|=|s\rangle$，但对于任意与 $|s\rangle$ 正交的态 $|s'\rangle$ 有

$$U_s|s'\rangle=2|s\rangle\langle s|s'\rangle-|s'\rangle=-|s'\rangle,$$

$|s'\rangle$ 易于构造：任意两计算基态相减即可。

U_s 变换

U_s 对态空间一般矢量的作用的几何图像：

在与 $|s\rangle$ 正交的 2^n-1 维子空间中做中心反射变换。即：改变所有与 $|s\rangle$ 垂直的分量的符号。

三、 Grover 迭代

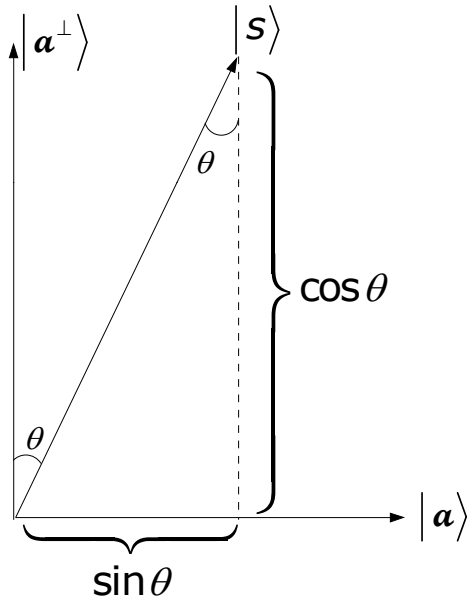
构造酉算子： $U = U_s U_a$,

由于

$$\left|\langle a|s\rangle\right| = \frac{1}{\sqrt{N}} \overset{记}{=} \sin\theta ,$$

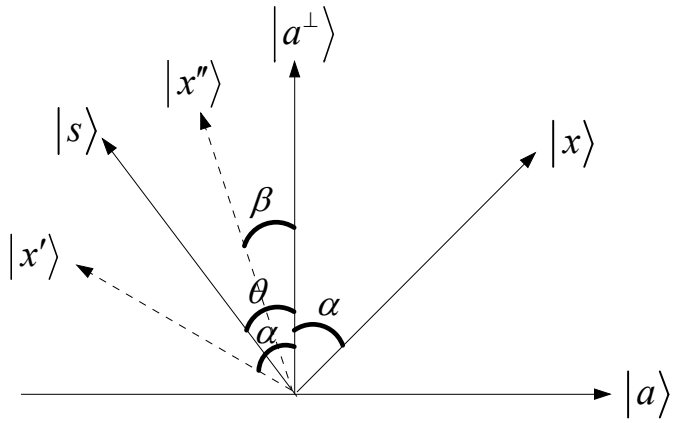
可知 $|s\rangle = \pm\sin\theta|a\rangle \pm \cos\theta|a^{\perp}\rangle$

即：$|s\rangle$ 是一个与 $|a^{\perp}\rangle$ 相差 θ 角的态矢量。



Grover 迭代

$U = U_s\, U_a$ 的作用： $U|x\rangle = U_s\,|x'\rangle = |x''\rangle$.



即： $|x\rangle \xrightarrow[\text{反射}]{\text{相对}|a^{\perp}\rangle\text{轴}} |x'\rangle \xrightarrow[\text{反射}]{\text{相对}|s\rangle\text{轴}} |x''\rangle$.

$$\Rightarrow \frac{\alpha-\beta}{2}+\beta=\theta\,.$$

$$\Rightarrow \alpha+\beta=2\theta\,.$$

故知： U 的作用是将任意态矢量在 由$|a\rangle$和$|s\rangle$ 确定的平面中转过 2θ 角，其中 θ 满足 $\sin\theta=\dfrac{1}{\sqrt{N}}$. （ $|x\rangle$与$|x''\rangle$ 的夹角是 $\alpha+\beta$. ）

四、从 N 中求 1 问题

黑盒中的参数 a 是未知的，计算者制备初态 $|s\rangle$ 后，进行 $U|s\rangle$ 运算一次，调用黑盒一次。

问：调用黑盒多少次，可以在测量态矢量时以接近 1 的概率得到 a ？

从 N 中求 1 问题

用类似经典的方法，随机选取一个 x，计算 $f_a(x)$，遇到 $f_a(x)=1$

（即$x=a$）的概率是 $\frac{1}{N}$. 因此平均需要 $\frac{1}{2}N$ 次调用黑盒才能知道 a.

现用 Grover 迭代 T 次后，$|s\rangle$ 与 $|a^{\perp}\rangle$ 的角度为 $\theta+2T\theta$.

如果 T 满足 $(2T+1)\theta\approx\frac{\pi}{2}$，即 $T\overset{T\text{很大}}{\approx}\frac{\pi}{4}\cdot\frac{1}{\theta}\overset{N\text{很大}}{\approx}\frac{\pi}{4}\sqrt{N}$，$|s\rangle\xrightarrow{U^{(T)}}|a\rangle$，

测量系统末态即可以接近 1 的概率得到黑盒的 a.

五、 多搜索目标问题

即：

$$f_a(x)=\begin{cases}1,\text{当 } x\in\{a_1,\cdots,a_r\},\\ 0,\text{当 } x\notin\{a_1,\cdots,a_r\}.\end{cases}$$

设 $|a\rangle=\frac{1}{\sqrt{r}}\sum_{i=1}^{r}|a_i\rangle$，则 $\langle s|a\rangle=\sqrt{\frac{r}{N}}\overset{记}{=}\sin\theta\approx\theta\ (N\gg r)$.

从 $|s\rangle$ 出发进行 $T\approx\frac{\pi}{2}\Big/2\theta\approx\frac{\pi}{4}\sqrt{\frac{N}{r}}$ 次 Grover 迭代，可将 $|s\rangle$ 变换为近于 $|a\rangle$.

多搜索目标问题

测量系统末态，则以接近 $\frac{1}{r}$ 概率坍缩到某一个 $|a_i\rangle (i=1,\cdots,r)$ 寻找 r 个目标问题化为一个概率问题，平均需要 $r\cdot\sum_{k=1}^{r}\frac{1}{k}\approx r\ln r$ 次测量。（每一次测量之前需进行约 $\frac{\pi}{4}\sqrt{\frac{N}{r}}$ 次 Grover 迭代）。共需调用黑盒 $\approx\frac{\pi}{4}\sqrt{rN}\ln r$ 次。

六、关于“量子摇晃”

直接看 Grover 迭代是怎样放大 $|a\rangle$ 的几率幅的。仍取 $|s\rangle=\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle$，

设系统状态为任意态 $|\varphi\rangle=\sum_{x=0}^{N-1}C_x|x\rangle$，　记 $\langle C_x\rangle\equiv\frac{1}{N}\sum C_x$，则

$$\langle s|\varphi\rangle=\frac{1}{\sqrt{N}}\sum_x C_x=\sqrt{N}\cdot\frac{1}{N}\sum C_x=\sqrt{N}\langle C_x\rangle,$$

而

$$\begin{aligned}U_s|\varphi\rangle&=\left(2|s\rangle\langle s|-1\right)|\varphi\rangle=2|s\rangle\langle s|\varphi\rangle-|\varphi\rangle\\&=2|s\rangle\sqrt{N}\langle C_x\rangle-\sum_{x=0}^{N-1}C_x|x\rangle\\&=\sum_{x=0}^{N-1}\left(2\langle C_x\rangle-C_x\right)|x\rangle\overset{\text{记}}{=}\sum_{x=0}^{N-1}C'_x|x\rangle.\end{aligned}$$

关于“量子摇晃”

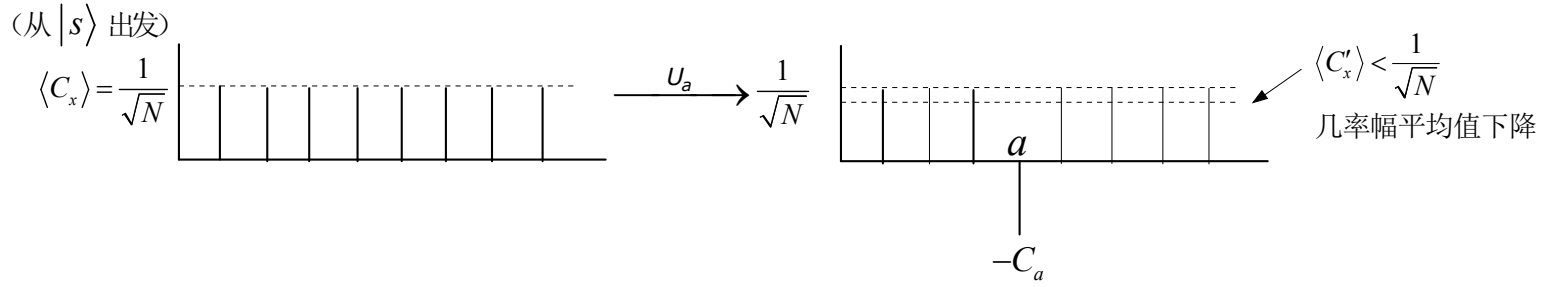
考虑 $|x\rangle$ 的几率幅与平均几率幅之差：$\left(U_s\text{作用后不改变}\langle C_x\rangle\right)$

$$C_x-\langle C_x\rangle \xrightarrow{U_s} \underbrace{2\langle C_x\rangle-C_x}_{C'_x}-\langle C_x\rangle=\langle C_x\rangle-C_x=-\left(C_x-\langle C_x\rangle\right),$$

未作U_s之前的值

即：U_s 使此量反号。由此可推知 U 的作用如下：

① U_a 使 $|a\rangle$ 的几率幅反号：



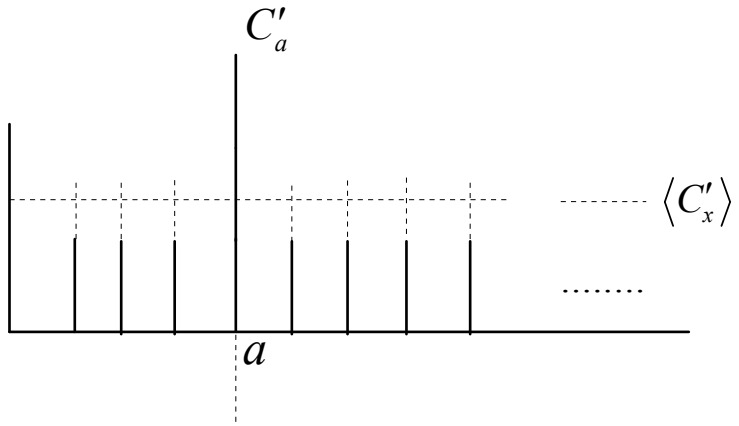
关于“量子摇晃”

② U_s 使系统在 $|x\rangle$ 上的几率幅与平均几率幅之差 $C_x-\langle C_x\rangle$

反号：1） $C_a-\langle C_x\rangle<0\xrightarrow{U_s}C'_a-\langle C'_x\rangle=-\left(C_a-\langle C_x\rangle\right)>0$

2） $x\neq a$ 时，$C_x-\langle C_x\rangle>0\xrightarrow{U_s}-\left(C_x-\langle C_x\rangle\right)<0$

即：



关于“量子摇晃”

U_s 使各几率幅相对于 $\langle C'_x \rangle$ 线反转。 每次反转后 C_a 的增量与 $\langle C'_x \rangle$ 有关，故作用逐次递减。易知

$$C'_a = 2\langle C_x \rangle + C_a \approx 3C_a$$

$$C''_a = 2\langle C'_x \rangle + C'_a \approx 5C_a$$

$$\vdots$$

$$C_a^{(l)} = 2\left\langle C_x^{(l-1)} \right\rangle + C_a^{(l-1)}$$

$$\Rightarrow C_a^{(l)} \square\, lC_a = \frac{l}{\sqrt{N}},$$

故需进行 $l \square \sqrt{N}$ 次迭代。

第六章 量子算法