HUAZHONG UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF PHYSICS

Quantum Computing

Author:
Du Xixiang

Last revised in:
——

Jan 7 , 2023

目录

1 Framework of Quantum Mechanics

需要补充的量子力学知识有: 张量积、纠缠态、密度算符

1.1 Multipartite System, Tensor Product and Entangled State

假设一个系统有两个部分组成: 一个位于 Hilbert 空间 $\mathcal{H}_2$, 一个位于 Hilbert 空间 $\mathcal{H}_2$. 这样的系统叫做 **bipartite**, 位于 Hilbert 空间 $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$. 其中的一个态矢量可以写成

$$|\psi\rangle = \sum_{i,j} c_{ij} |e_{1,i}\rangle \otimes |e_{2,j}\rangle, \quad \sum_{i,j} |c_{i,j}|^2 = 1 \tag{1.1}$$

$\{|e_{a,i}\rangle\}(a = 1, 2)$ 是一组正交基矢量.

若一个右矢 $|\psi\rangle \in \mathcal{H}$ 可以写成 $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$ $(|\psi_a\rangle \in \mathcal{H}_a)$, 这样的态叫做**可分离态 (separable state)** 或**张量积态 (product state)**, 否则称为**纠缠态 (entangled state)**, 例如

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle \otimes |\uparrow\rangle + |\downarrow\rangle \otimes |\downarrow\rangle) \tag{1.2}$$

判断一个态是分离态还是纠缠态可以用矩阵的**奇异值分解 (SVD)** 方法.

1.2 Mixed States and Density Matrices

混合态 (mixed state) 需要用密度矩阵来描述

$$\rho = \sum_{i=1}^{N} p_i |\psi_i\rangle\langle\psi_i| \tag{1.3}$$

一个算符的期望值

$$\langle A\rangle = \sum_{i=1}^{N} p_i \langle\psi_i| A |\psi_i\rangle = \mathrm{Tr}(\rho A) \tag{1.4}$$

以及演化规律

$$\mathrm{i}\hbar \frac{\mathrm{d}}{\mathrm{d}t}\rho = [H, \rho] \tag{1.5}$$

$$\text{mixed state} \begin{cases} \text{uncorrelated} & \rho = \rho_1 \otimes \rho_2, \\ \text{separable} & \rho = \sum_i p_i \rho_{1,i} \otimes \rho_{2,i}, \\ \text{inseparable} & \text{else.} \end{cases}$$

2 Qubits and Quantum Key Distribution

2.1 Qubits

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{2.1}$$

2.2 Quantum Key Distribution (BB84 Protocol)

Alice 向 Bob 传输 $4N$ 个光子, 并随机采用两种编码系统, 将所采用的编码系统序列用经典信道传输给对方, 于是只有 $2N$ 个光子是有效的, 交换其中的 N 个光子来判断是否被窃听, 剩下的 N 个光子用于传递信息.

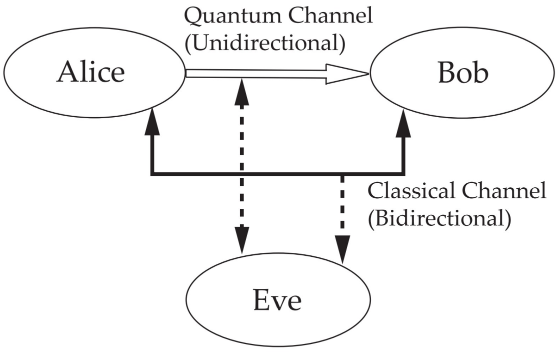

图 1: BB84 协议

3 Quantum Gates, Quantum Circuit and Quantum Computation

3.1 Quantum Gates

3.1.1 简单量子门

$$I = |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{3.1}$$

$$X = |1\rangle\langle 0| + |0\rangle\langle 1| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \sigma_x \tag{3.2}$$

$$Y = |0\rangle\langle 1| - |1\rangle\langle 0| = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = -\mathrm{i}\sigma_y \tag{3.3}$$

$$Z = |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \sigma_z \tag{3.4}$$

CNOT (controlled-NOT) 门 U_{CNOT}, 当第一量子位是 $|1\rangle$ 时, 翻转第二量子位, 反之不变

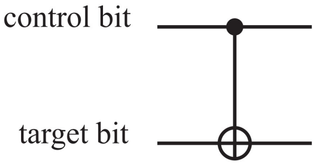

图 2: CNOT 门

$$U_{\mathrm{CNOT}} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X \tag{3.5}$$

以及 controlled-U 门

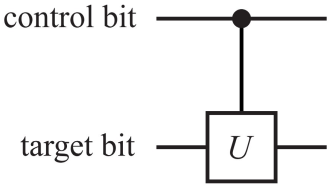

图 3: controlled-U 门

$$V = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U \tag{3.6}$$

CCNOT (Controlled-Controlled-NOT) 门有三个输入位, 当前两个量子位是 $|1\rangle$ 时, 翻转第三个量子位, 其他情况不作操作

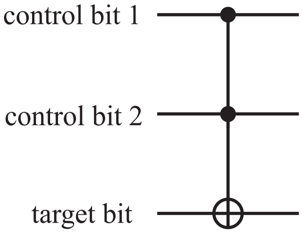

图 4: CCNOT 门

$$U_{CCNOT} = (|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10|) \otimes I + |11\rangle\langle 11| \otimes X \tag{3.7}$$

3.1.2 Walsh-Hadamard Transformation

Hadamard 门定义如下

$$U_{\mathrm{H}} : |0\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |1\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{3.8}$$

矩阵表示为

$$U_{\mathrm{H}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{3.9}$$

当 Hadamard 门作用于态 $|00\cdots 0\rangle$ 的每个量子位, 能够产生所有的 2^n 个态

$$\begin{aligned}
&(H \otimes H \otimes \cdots \otimes H)\,|00\cdots 0\rangle && (3.10)\\
&= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \cdots \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) && (3.11)\\
&= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle && (3.12)
\end{aligned}$$

这是 **Walsh transformation**.

3.1.3 SWAP Gate and Fredkin Gate

交换门定义如下

$$U_{\mathrm{SWAP}} |\psi_1, \psi_2\rangle = |\psi_2, \psi_1\rangle \tag{3.13}$$

矩阵形式

$$\begin{aligned} U_{\mathrm{SWAP}} &= |00\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01| + |11\rangle\langle 11| \qquad (3.14) \\ &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad (3.15) \end{aligned}$$

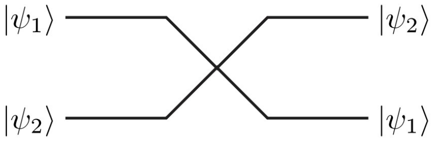

图 5: swap gate

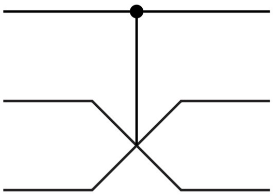

图 6: fredkin gate

3.2 Correspondence with Classical Logic Gates

所有的经典逻辑门都可以用 CCNOT 实现

1. **NOT Gate(非门)**

$$\mathrm{NOT}(x) = \neg x, \quad U_{\mathrm{CCNOT}} |1, 1, x\rangle = |1, 1, \neg x\rangle \tag{3.16}$$

2. **XOR Gate(异或门)**

$$\mathrm{XOR}(x, y) = (x, x \oplus y), \quad U_{\mathrm{CCNOT}} |1, x, y\rangle = |1, x, x \oplus y\rangle \tag{3.17}$$

3. **AND Gate(与门)**

$$\mathrm{AND}(x, y) = x \wedge y, \quad U_{\mathrm{CCNOT}} |x, y, 0\rangle = |x, y, x \wedge y\rangle \tag{3.18}$$

4. **OR Gate(或门)**

$$\mathrm{OR}(x, y) = x \vee y \tag{3.19}$$

3.3 Dense Coding and Quantum Teleportation

密集编码 (dense coding) 和**量子隐形传态 (quantum teleportation)** 是量子门的两个简单应用, 他们都用到了贝尔纠缠态

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{3.20}$$

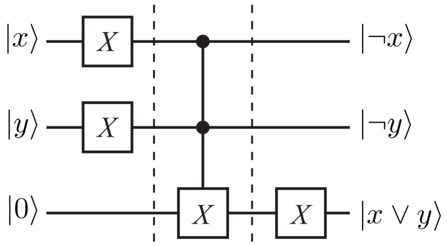

图 7: 或门的 CCNOT 实现

3.3.1 Dense Coding

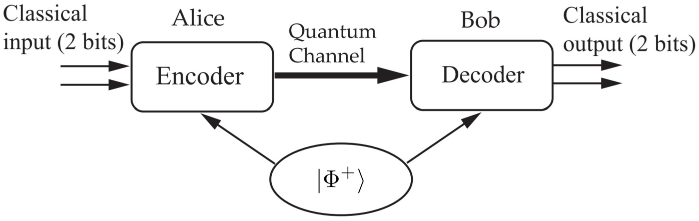

图 8: Communication from Alice to Bob using dense coding. Each qubit of the Bell state $|\Phi^+\rangle$ has been distributed to each of them beforehand. Then two bits of classical information can be transmitted by sending a single qubit through the quantum channel.

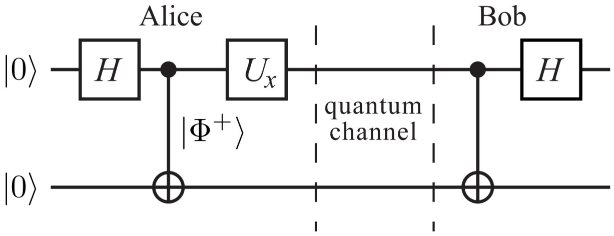

图 9: Quantum circuit implementation of the dense coding system. The leftmost Hadamard gate and the next CNOT gate generate the Bell state. Then a unitary gate U, depending on the bits Alice wants to send, is applied to the first qubit. Bob applies the rightmost CNOT gate and the Hadamard gate to decode Alice’s message.

3.3.2 Quantum Teleportation

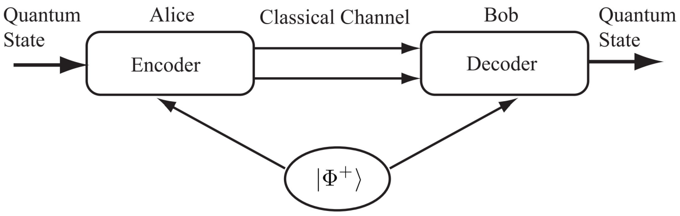

图 10: In quantum teleportation, Alice sends Bob two classical bits so that Bob reproduces a qubit state Alice used to have.

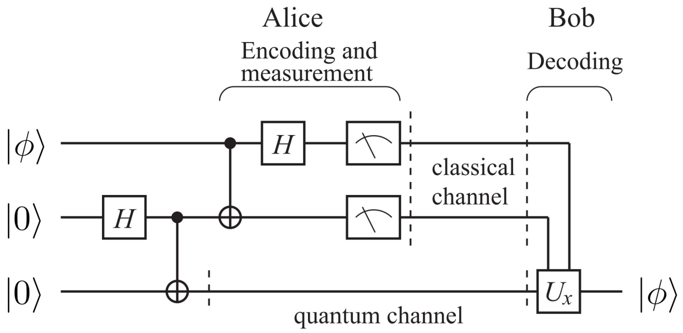

图 11: Quantum circuit implementation of quantum teleportation. Alice operates gates in the left side. The first Hadamard gate and the next CNOT gates generate the Bell state $|\Phi^+\rangle$ from $|00\rangle$. The bottom qubit is sent to Bob through a quantum channel while the first and the second qubits are measured after applying the second set of the CNOT gate and the Hadamard gate on them. The measurement outcome x is sent to Bob through a classical channel.Bob operates a unitary operation U_x, which depends on the received message x, on his qubit.

3.4 Universal Quantum Gates

universality theorem: the set of single qubit gates and CNOT gate form a universal set of quantum circuits.

4 Simple Quantum Algorithms

4.1 Quantum Integral Transforms

定义 4.1 (离散积分变换)**.** $n \in \mathbb{N}, S_n = \{0, 1, \cdots, 2^n - 1\}$ 是全是整数的集合, 考虑一个映射

$$K : S_n \times S_n \mapsto \mathbb{C} \tag{4.1}$$

对于任意函数 $f : S_n \mapsto \mathbb{C}$, 它在核 K 下的离散积分变换 *(DIT)*$\tilde{f} : S_n \mapsto \mathbb{C}$ 定义为:

$$\tilde{f}(y) = \sum_{x=0}^{2^n-1} K(y,x) f(x) \tag{4.2}$$

$f \to \tilde{f}$ 亦称为离散积分变换.

亦可用矩阵来表示

$$\begin{gathered} K = (K(i,j)) \\ f = (f(0), f(1), \cdots, f(N-1))^t \\ \tilde{f} = Kf \end{gathered} \tag{4.3}$$

命题 4.1. 假设核 K 是幺正的,*DIT* 的逆变换 $\tilde{f} \to f$ 存在并由下式给出

$$f(x) = \sum_{y=0}^{N-1} K^\dagger(x,y) \tilde{f}(y) \tag{4.4}$$

命题 4.2. U 是一个 $\mathcal{H} = (\mathbb{C}^2)^{\otimes n}$ 上的幺正变换, 按照如下方式作用于基矢量 $|x\rangle$

$$U|x\rangle = \sum_{y=0}^{N-1} K(y,x)|y\rangle \tag{4.5}$$

则按如下意义计算 $f(x)$ 的 *DIT*

$$U\left[\sum_{x=0}^{N-1} f(x)|x\rangle\right] = \sum_{y=0}^{N-1} \tilde{f}(y)|y\rangle \tag{4.6}$$

这里 $|x\rangle, |y\rangle$ 都是 $\mathcal{H}$ 的基矢量. 这个实现 *DIT* 的幺正矩阵 U 被称作量子积分变换 *(QIT)*.

4.2 Quantum Fourier Transform(QFT)

定义一个离散傅里叶变换的核

$$K(x,y) = \frac{1}{\sqrt{N}} \omega_n^{-xy}, \quad \omega_n = \mathrm{e}^{2\pi \mathrm{i}/N} \tag{4.7}$$

离散傅里叶变换 (DFT) 为

$$\tilde{f}(y) = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \omega_n^{-xy} f(x) \tag{4.8}$$

并且可以证明

$$K^\dagger K(x,y) = \delta_{xy}$$

以 K 为核的量子积分变换被称为量子傅里叶变换 (QFT).

4.3 Implementation of QFT

$n=1$ 情况

实现 $n=1$ 的 QFT 核正是 Hadamard 门

$$U_{\mathrm{H}}\left|x\right\rangle=\frac{1}{\sqrt{2}}(\left|0\right\rangle+(-1)^{x}\left|1\right\rangle)=\frac{1}{\sqrt{2}}\sum_{y=0}^{1}(-1)^{xy}\left|y\right\rangle=U_{\mathrm{QFT1}}\left|y\right\rangle \tag{4.9}$$

$n=2$ 情况

引入 controlled-B_{ij} 门

$$B_{ij}=\begin{pmatrix}1 & 0\\ 0 & \mathrm{e}^{-\mathrm{i}\theta_{jk}}\end{pmatrix},\quad \theta_{jk}=\frac{2\pi}{2^{k-j+1}},\quad k\geq j \tag{4.10}$$

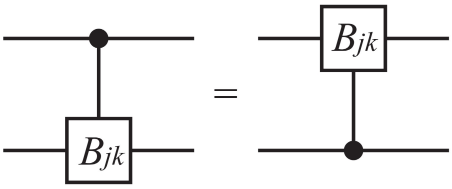

图 12: 容易证明, 这两个控制量子门是等价的

引理 4.1. *controlled-B_{jk} 门作用于基 $\left|x,y\right\rangle$ 上的矩阵 U_{jk}*

$$U_{jk}\left|x,y\right\rangle=\mathrm{e}^{-\mathrm{i}\theta_{jk}xy}\left|x,y\right\rangle=\exp\left(-\frac{2\pi\mathrm{i}}{2^{k-j+1}}xy\right)\left|x,y\right\rangle \tag{4.11}$$

寻找一个幺正矩阵使得

$$U_{\mathrm{QFT2}}=\frac{1}{2}\sum_{y=0}^{3}\omega_2^{-xy}\left|y\right\rangle \tag{4.12}$$

用二进制的形式写出 $x=2x_1+x_0, y=2y_1+y_0$, 可以写出

$$\begin{aligned}U_{\mathrm{QFT2}}\left|x_1x_0\right\rangle&=\frac{1}{2}\sum_{y=0}^{3}\mathrm{e}^{-2\pi\mathrm{i}xy/2^2}\left|y\right\rangle\\&=\frac{1}{2}(\left|0\right\rangle+(-1)^{x_0}\left|1\right\rangle)\otimes B_{12}^{x_0}(\left|0\right\rangle+(-1)^{x_1}\left|1\right\rangle)\\&=(U_{\mathrm{H}}\otimes I)U_{12}(I\otimes U_{\mathrm{H}})U_{\mathrm{SWAP}}\left|x_1x_0\right\rangle\end{aligned} \tag{4.13}$$

命题 4.3. *$n=2$ 的 QFT 门实现如下*

$$U_{QFT2}=(U_{\mathrm{H}}\otimes I)U_{12}(I\otimes U_{\mathrm{H}})U_{SWAP} \tag{4.14}$$

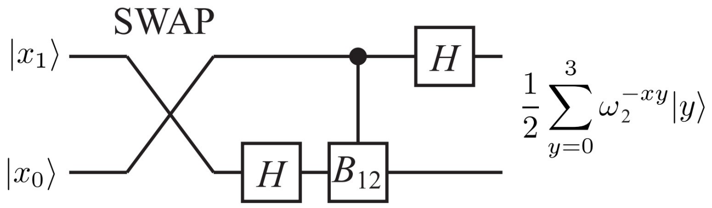

图 13: Implementation of the $n = 2$ QFT,U_{QFT2}

$n = 3$ **情况**

$$\begin{aligned} &U_{\mathrm{QFT3}}\,|x_2x_1x_0\rangle \\ &= \frac{1}{\sqrt{2^3}}(|0\rangle + (-1)^{x_0}\,|1\rangle) \otimes B_{01}^{x_0}(|0\rangle + (-1)^{x_1}\,|1\rangle) \otimes B_{02}^{x_0}B_{12}^{x_1}(|0\rangle + (-1)^{x_2}\,|1\rangle) \\ &= (U_{\mathrm{H}} \otimes I \otimes I)U_{01}(I \otimes U_{\mathrm{H}} \otimes I)U_{02}U_{12}(I \otimes I \otimes U_{\mathrm{H}})P\,|x_2x_1x_0\rangle \end{aligned} \tag{4.15}$$

其中置换算符

$$P\,|x_2x_1x_0\rangle = |x_0x_1x_2\rangle \tag{4.16}$$

$n = 3$ 的 QFT 门实现如下

$$U_{\mathrm{QFT3}} = (U_{\mathrm{H}} \otimes I \otimes I)U_{01}(I \otimes U_{\mathrm{H}} \otimes I)U_{02}U_{12}(I \otimes I \otimes U_{\mathrm{H}})P \tag{4.17}$$

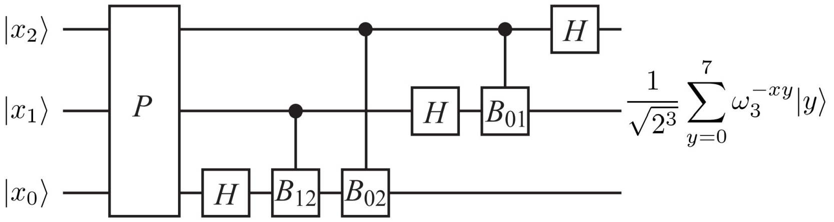

图 14: Implementation of the $n = 3$ QFT,U_{QFT3}

$n = all$ **情况**

$$\begin{aligned} U_{QFTn} &= (U_{\mathrm{H}} \otimes I \otimes \cdots \otimes I)U_{01}(I \otimes U_{\mathrm{H}} \otimes I \otimes \cdots \otimes I)U_{02}U_{12} \\ &\times (I \otimes I \otimes U_{\mathrm{H}} \otimes \cdots \otimes I)\cdots \\ &= U_{0,n-1}U_{1,n-1}\cdots U_{n-2,n-1}(I \otimes \cdots \otimes I \otimes U_{\mathrm{H}})P \end{aligned} \tag{4.18}$$

P 是完全反对称算符

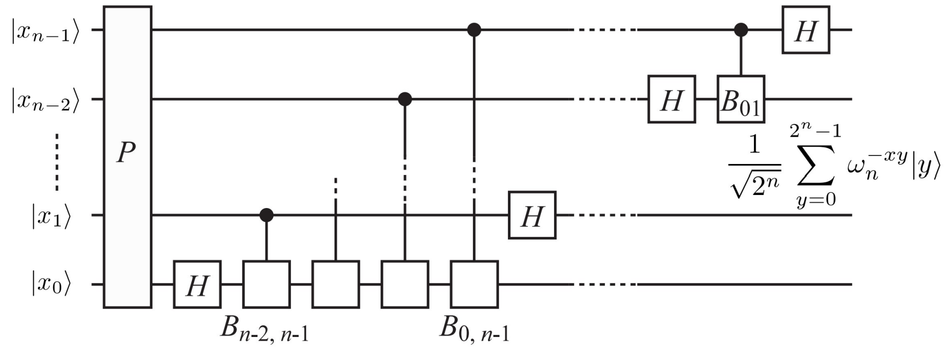

图 15: Implementation of the n-qubit QFT

命题 4.4. *n-qubit 的 QFT 电路需要 $\Theta(n^2)$ 个基本量子门.*

4.4 Walsh-Hadamard Transform

$$W_n(x,y) = U_{\mathrm{H}} \otimes U_{\mathrm{H}} \otimes \cdots \otimes U_{\mathrm{H}} = \frac{1}{\sqrt{N}}(-1)^{x\cdot y} \quad (x, y \in S_n) \tag{4.19}$$

其中

$$x \cdot y = x_{n-1}y_{n-1} \oplus x_{n-2}y_{n-2} \oplus \cdots \oplus x_0 y_0$$

4.5 Selective Phase Rotation Transform

定义 4.2 (Selective Phase Rotation Transform)**.** 定义一个核

$$K_n(x,y) = \mathrm{e}^{\mathrm{i}\theta_x}\delta_{xy}, \quad \forall x, y \in S_n \tag{4.20}$$

其定义的离散积分变换

$$\tilde{f}(y) = \sum_{x=0}^{N-1} K(x,y)f(x) = \sum_{x=0}^{N-1} \mathrm{e}^{\mathrm{i}\theta_x}\delta_{xy}f(x) = \mathrm{e}^{\mathrm{i}\theta_y}f(y) \tag{4.21}$$

即为每个分量作用了相移,K_n 称为 ***selective phase rotation transform***.

5 Grover's Search Algorithm

5.1 Searching for a Single File

$|z\rangle$ 是目标态, 定义函数 $f : S_n \mapsto \{0, 1\}$

$$f(x) = \begin{cases} 1 & (x = z) \\ 0 & (x \neq z) \end{cases} \tag{5.1}$$

STEP 1 定义选择性相移变换 R_f

$$R_f = I - 2\left|z\right\rangle\!\left\langle z\right| \tag{5.2}$$

考虑一个态

$$\left|\phi\right\rangle = \sum_{x=0}^{N-1} w_x \left|x\right\rangle, \quad \sum_x |w_x|^2 = 1 \tag{5.3}$$

R_f 作用于其上

$$R_f \left|\phi\right\rangle = w_0 \left|0\right\rangle + \cdots + (-1) w_z \left|z\right\rangle + \cdots + w_{N-1} \left|N-1\right\rangle \tag{5.4}$$

R_f 改变了 w_z 的符号.

STEP 2 定义一个幺正矩阵

$$D = W_n R_0 W_n \tag{5.5}$$

其中 W_n 是 Walsh-Hadamard 变换

$$W_n(x,y) = \frac{1}{\sqrt{N}}(-1)^{x\cdot y}, \quad (x, y \in S_n) \tag{5.6}$$

R_0 是如下定义的相移变换

$$R_0(x,y) = \mathrm{e}^{\mathrm{i}\pi(1-\delta_{x0})}\delta_{xy} = (-1)^{1-\delta_{x0}}\delta_{xy} \tag{5.7}$$

命题 5.1. 令

$$\left|\phi_0\right\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \left|x\right\rangle \tag{5.8}$$

那么

$$D = -I + 2\left|\phi_0\right\rangle\!\left\langle\phi_0\right| \tag{5.9}$$

更进一步

$$D\left|\phi\right\rangle = \sum_{x=0}^{N-1} (\bar{w} - (w_x - \bar{w}))\left|x\right\rangle \tag{5.10}$$

其中

$$\bar{w} = \frac{1}{N}\sum_{x=0}^{N-1} w_x \tag{5.11}$$

略去证明, 直接计算易得.

STEP 3 下面考虑一个幺正变换 U_f

$$U_f = DR_f = (-I + 2\left|\phi_0\right\rangle\!\left\langle\phi_0\right|)(I - 2\left|z\right\rangle\!\left\langle z\right|) \tag{5.12}$$

作用于 $\left|phi\right\rangle = \sum_x w_x \left|x\right\rangle$

$$\begin{aligned} U_f\left|\phi\right\rangle &= D\left(\sum_{x\neq z} w_x\left|x\right\rangle - w_z\left|z\right\rangle\right) \\ &= \sum_{x\neq z}(2\bar{w} - w_x)\left|x\right\rangle + (2\bar{w} + w_z)\left|z\right\rangle \end{aligned} \tag{5.13}$$

这里

$$\bar{w} = \frac{1}{N}\left(\sum_{x\neq z} w_x - w_z\right) \tag{5.14}$$

命题 5.2. 考虑 U_f 作用在 $|\phi_0\rangle$ 上 k 次

$$U_f^k |\phi_0\rangle = a_k |z\rangle + b_k \sum_{x\neq z} |x\rangle \tag{5.15}$$

初始条件

$$a_0 = b_0 = \frac{1}{\sqrt{N}} \tag{5.16}$$

系数 $\{a_k, b_k\}$ 满足如下递推关系

$$a_k = \frac{N-2}{N}a_{k-1} + \frac{2(N-1)}{N}b_{k-1} \tag{5.17}$$

$$b_k = -\frac{2}{N}a_{k-1} + \frac{N-2}{N}b_{k-1} \tag{5.18}$$

命题 5.3. $\{a_k, b_k\}$ 的解可以显式给出

$$a_k = \sin[(2k+1)\theta], \quad b_k = \frac{1}{\sqrt{N-1}}\cos[(2k+1)\theta] \tag{5.19}$$

以及

$$\sin\theta = \sqrt{\frac{1}{N}}, \quad \cos\theta = \sqrt{1-\frac{1}{N}} \tag{5.20}$$

于是有

$$U_f^k |\phi_0\rangle = \sin[(2k+1)\theta]\,|z\rangle + \frac{1}{\sqrt{N-1}}\cos[(2k-1)\theta]\sum_{x\neq z}|x\rangle \tag{5.21}$$

测量得到 $|z\rangle$ 的概率为

$$P_{z,k} = \sin^2[(2k+1)\theta] \tag{5.22}$$

STEP 4

命题 5.4. 若 $N \gg 1$, 令

$$m = \left\lfloor \frac{\pi}{4\theta} \right\rfloor \tag{5.23}$$

此时 $P_{z,m}$ 具有最大值

$$P_{z,m} \geqslant 1 - \frac{1}{N} \tag{5.24}$$

且

$$m = O(\sqrt{N}) \tag{5.25}$$

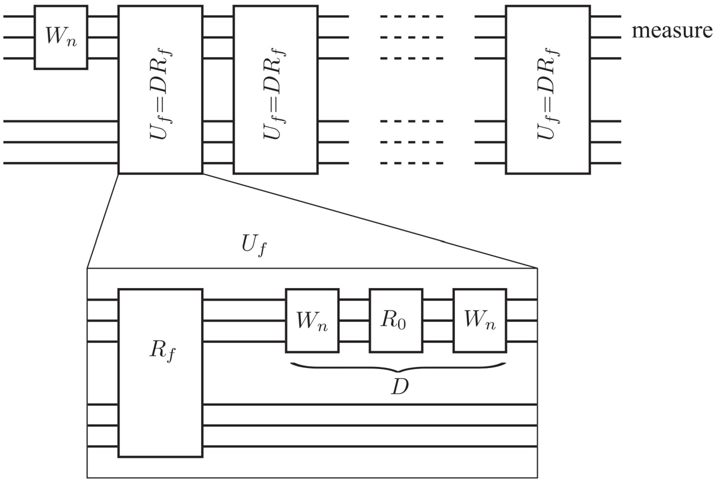

图 16: Implementation of Grover's search algorithm. Details of the box denoted by $U_f = DR_f$ are given in the lower diagram. The box U_f is repeated m times to maximize $P_{z,k}$. The gate R_f is the oracle, and working qubits to implement the oracle are given explicitly.

5.2 Searching for d Files

假设有 d 个我们需要寻找的状态满足条件, 定义函数

$$f(x) = \begin{cases} 1 & (x \in A) \\ 0 & (x \notin A) \end{cases} \tag{5.26}$$

其中 A 是 S_n 的子集, 其中的元素满足所给条件.

定义幺正变换 R_f

$$R_f = I - 2\sum_{z\in A} |z\rangle\langle z| \tag{5.27}$$

作用于 $|\phi\rangle = \sum_{x=0}^{N-1} w_x |x\rangle$

$$R_f |\phi\rangle = \sum_{x\notin A} w_x |x\rangle - \sum_{z\in A} w_z |z\rangle \tag{5.28}$$

以及考虑

$$U_f = DR_f = (-I + 2|\phi_0\rangle\langle\phi_0|)(I - 2\sum_{z\in A}|z\rangle\langle z|) \tag{5.29}$$

U_f 作用于 $|\phi\rangle$ 上产生

$$U_f |\phi\rangle = \sum_{x\notin A}(2\bar{w} - w_x)|x\rangle + \sum_{x\in A}(2\bar{w} + w_z)|z\rangle \tag{5.30}$$

其中

$$\bar{w} = \frac{1}{N}\left(\sum_{x\notin A} w_x - \sum_{x\in A} w_z\right) \tag{5.31}$$

命题 5.5. 考虑 U_f 作用在 $|\phi_0\rangle$ 上 k 次

$$U_f^k |\phi_0\rangle = a_k \sum_{z\in A} |z\rangle + b_k \sum_{x\notin A} |x\rangle \tag{5.32}$$

初始条件

$$a_0 = b_0 = \frac{1}{\sqrt{N}} \tag{5.33}$$

系数 $\{a_k, b_k\}$ 满足如下递推关系

$$a_k = \frac{N-2d}{N} a_{k-1} + \frac{2(N-d)}{N} b_{k-1} \tag{5.34}$$

$$b_k = -\frac{2d}{N} a_{k-1} + \frac{N-2d}{N} b_{k-1} \tag{5.35}$$

可以解出

$$a_k = \frac{1}{\sqrt{d}} \sin[(2k+1)\theta], \quad b_k = \frac{1}{\sqrt{N-d}} \cos[(2k+1)\theta] \tag{5.36}$$

其中

$$\sin\theta = \sqrt{\frac{d}{N}}, \quad \cos\theta = \sqrt{1 - \frac{d}{N}} \tag{5.37}$$

命题 5.6. 若 $N \gg d$, 令

$$m = \left\lfloor \frac{\pi}{4\theta} \right\rfloor \tag{5.38}$$

此时 $P_{z,m}$ 具有最大值

$$P_{z,m} \geqslant 1 - \frac{d}{N} \tag{5.39}$$

且

$$m = O(\sqrt{N/d}) \tag{5.40}$$

6 Shor’s Factorization Algorithm

6.1 Factorization Algorithm

p 和 q 是质数并且 $N = pq$. 我们要将 N 分解成 p 和 q 的乘积. 我们按照如下步骤进行.

STEP 1 随机取一个小于 N 的整数 m. 用欧几里得算法计算 $\gcd(m, N)$. 如果 $\gcd(m, N) \neq 1$, 我们的任务已经完成. 假设 $(gcd) = 1$.

STEP 2 定义 $f_N : a \mapsto m^a \mod N$. 找到最小的 $P \in N$ 使得 $m^P \equiv 1 \mod N$, 这一步实际是在寻找 f_N 的**周期**或者说是**阶**. 我们将用量子计算的 Shor’s algorithm 实现这一步, 其余步骤用经典算法.

STEP 3 如果 P 是偶数, 继续下一步, 否则回到第一步重新选取 m.

STEP 4 因为 P 是偶数

$$(m^{P/2}-1)(m^{P/2}+1)=m^P-1=\equiv 0 \mod N \tag{6.1}$$

如果 $m^{P/2}+1\equiv 0 \mod N$, 有 $\gcd(m^{P/2}-1,N)=1$, 回到第一步重新选取 m. 如果 $m^{P/2}+1\ \ !\equiv 0$ mod N, 那么 $m^{P/2}-1$ 含有 p 或 q.

STEP 5 数

$$d=\gcd(m^{P/2}-1,N) \tag{6.2}$$

就是 p 或 q, 分解完成.

6.2 Quantum Part of Shor's Algorithm

$N=pq\in\mathbb{N}$ 是待分解的数,p,q 都是质数. 找一个 $n\in\mathbb{N}$, 使得

$$N^2\le 2^n<2N^2 \tag{6.3}$$

在这之后, 令 $Q=2^n.f:a\mapsto m^a \mod N$ 限制在集合

$$S_n=\{0,1,\cdots,Q-1\} \tag{6.4}$$

现在让我们细致考虑 STEP 2.

STEP 2.0 我们需要两个 n 位寄存器完成操作, 设置初始状态

$$|\psi_0\rangle=|\text{REG1}\rangle\,|\text{REG2}\rangle=|00\cdots0\rangle\,|00\cdots0\rangle\,. \tag{6.5}$$

STEP 2.0 QFT$\mathcal{F}$ 作用于 REG1 寄存器

$$|\psi_0\rangle=|0\rangle\,|0\rangle \overset{\mathcal{F}\otimes I}{\mapsto} |\psi_1\rangle=\frac{1}{\sqrt{Q}}\sum_{x_0}^{Q-1}|x\rangle\,|0\rangle \tag{6.6}$$

STEP 2.2 实现 f 的幺正矩阵 U_f 以如下方式作用 $U_f\,|x\rangle\,|0\rangle=|x\rangle\,|f(x)\rangle$, 则

$$U_f\,|\psi_1\rangle=|\psi_2\rangle\equiv\frac{1}{\sqrt{Q}}\sum_{x=0}^{Q-1}|x\rangle\,|f(x)\rangle \tag{6.7}$$

STEP 2.3 QFT 作用于 REG1

$$|\psi_3\rangle=(\mathcal{F}\otimes I)\,|\psi_2\rangle=\frac{1}{Q}\sum_{x=0}^{Q-1}\sum_{y=0}^{Q-1}\omega_n{-}xy\,|y\rangle\,|f(x)\rangle \tag{6.8}$$

$$=\frac{1}{Q}\sum_{y=0}^{Q-1}\|\,|\Upsilon(y)\rangle\,\|\,|y\rangle\,\frac{|\Upsilon(y)\rangle}{\|\,|\Upsilon(y)\rangle\,\|} \tag{6.9}$$

其中

$$|\Upsilon(y)\rangle=\sum_{x=0}^{Q-1}\omega_n^{-xy}\,|f(x)\rangle \tag{6.10}$$

STEP 2.4 测量 REG1, 得到结果 $y \in S_n$ 的概率为

$$\mathrm{Prob}(y) = \frac{\| \, |\Upsilon(y)\rangle \, \|^2}{Q^2} \tag{6.11}$$

与此同时, 态矢量将会坍缩到

$$|y\rangle \, \frac{|\Upsilon(y)\rangle}{\| \, |\Upsilon(y)\rangle \, \|}$$

STEP 2.5 从测量结果中提取 P.

6.3 Probability Distribution

细致考虑测量结果的概率分布

命题 6.1. *令 $Q = 2^n = Pq + r, (r \leq r < P), Q_0 = Pq$, 于是*

$$Prob(y) = \begin{cases} \dfrac{r \sin^2\left(\frac{\pi P y}{Q}\left(\frac{Q_0}{P}+1\right)\right) + (P-r)\sin^2\left(\frac{\pi P y}{Q}\cdot\frac{Q_0}{P}\right)}{Q^2 \sin^2\left(\frac{\pi P y}{Q}\right)} & (Py \neq 0 \mod Q) \\ \dfrac{r(Q_0+P)^2 + (P-r)Q_0^2}{Q^2 P^2} & (Py \equiv 0 \mod Q) \end{cases} \tag{6.12}$$

直接计算可得. *若 $Q/P \in \mathbb{Z}$*

$$Prob(y) = \begin{cases} 0 & (Py \neq 0 \mod Q) \\ \dfrac{1}{P} & (Py \equiv 0 \mod Q) \end{cases} \tag{6.13}$$

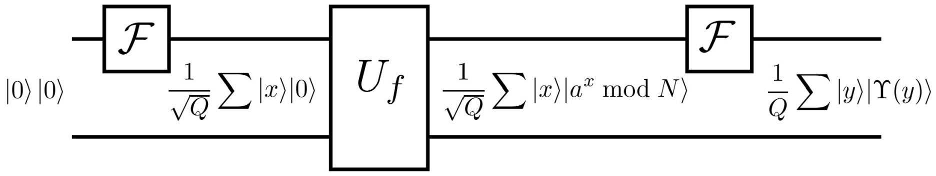
$\mathcal{F}$
$\mathcal{F}$
U_f
$|0\rangle\,|0\rangle$
$\frac{1}{\sqrt{Q}}\sum|x\rangle|0\rangle$
$\frac{1}{\sqrt{Q}}\sum|x\rangle|a^x \bmod N\rangle$
$\frac{1}{Q}\sum|y\rangle|\Upsilon(y)\rangle$

图 17: Quantum circuit to find the order of $f(x) = m^x \mod N$.

6.4 Continued Fractions and Order Finding

我们遵循以下步骤得到 $m^x \mod N$ 的阶 P.

1. 计算 y/Q 的连分数展开 $[a_0, a_1, \cdot, a_M]$, 由于 $y/Q < 1$, 有 $a_0 = 0$.

2. 令 $p_0 = a_0, q_0 = 1, p_1 = a_1 p_0 + 1, q_1 = a_1 q_0$, 并有递推关系 $p_i = a_i p_{i-1} + p_{i-2}$ 和 $q_i = a_i q_{i-1} + q_{i-2}$, 我们得到序列 $(p_0, q_0), (p_1, q_1), \cdots, (p_M, q_M)$

3. 找到最小的 $k(0 \leq k \leq M)$ 使得 $|p_k/q_k - y/Q| \leq 1/(2Q)$, 这样的 k 是唯一的.

4. 得到阶 $P = q_k$.

需要说明的是, 用这种方法得到正确的 P 的充分条件是

$$y \in \mathcal{C} = \left\{ y \middle| \exists d \in \{1, 2, \cdot, P-1\}, \left| \frac{d}{P} - \frac{y}{Q} \right| \le \frac{1}{2Q}, \gcd(P, d) = 1 \right\} \tag{6.14}$$

命题 6.2. *假设 $y \in \mathcal{C}$, 由以上算法得到的 P 是模指数函数 $m^x \mod N$ 的正确阶数.*

6.5 Modular Exponential Function

下面我们要考虑如何用量子电路实现模指数函数

$$U_f |x\rangle |0\rangle = |x\rangle |m^x \mod N\rangle$$

我们需要依次实现

1. 加法运算器, 输出 $a + b$.

2. 模运算器, 输出 $a + b \mod N$.

3. 模乘法运算器, 输出 $ab \mod N$.

4. 模指数函数, 输出 $m^x \mod N$.

6.5.1 Adder

令

$$a = a_{n-1}2^{n-1} + a_{n-2}2^{n-2} + \cdots + a_1 2 + a_0 \tag{6.15}$$

$$b = b_{n-1}2^{n-1} + b_{n-2}2^{n-2} + \cdots + b_1 2 + b_0 \tag{6.16}$$

$$s = s_n 2^n + s_{n-1}2^{n-1} + \cdots + s_1 2 + s_0 \tag{6.17}$$

可以证明, 若引入承载位 c, 有以下递推关系

$$\begin{gathered} s_0 = a_0 \oplus b_0, \quad c_0 = a_0 b_0, \\ s_k = a_k \oplus b_k \oplus c_{k-1}, \quad c_k = a_k b_k \oplus a_k c_{k-1} \oplus b_k c_{k-1} \end{gathered} \tag{6.18}$$

定义两个电路

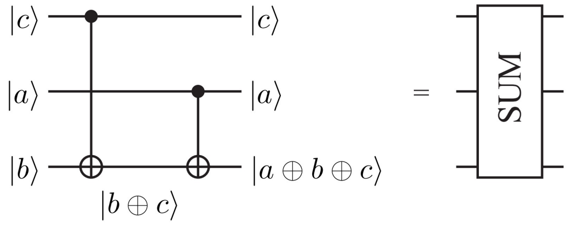

图 18: Quantum circuit to sum two binary bits and a carry bit. It will be also denoted as a black box called SUM.

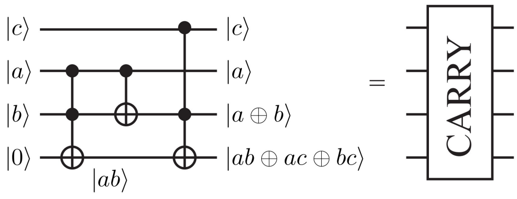

图 19: CARRY gate.

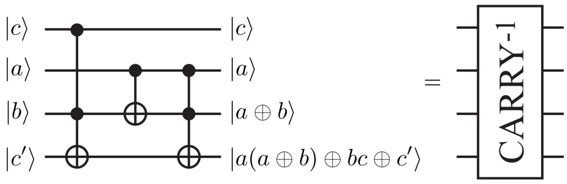

图 20: Inverse of the CARRY gate.

首先实现 ADD(2) 的量子电路

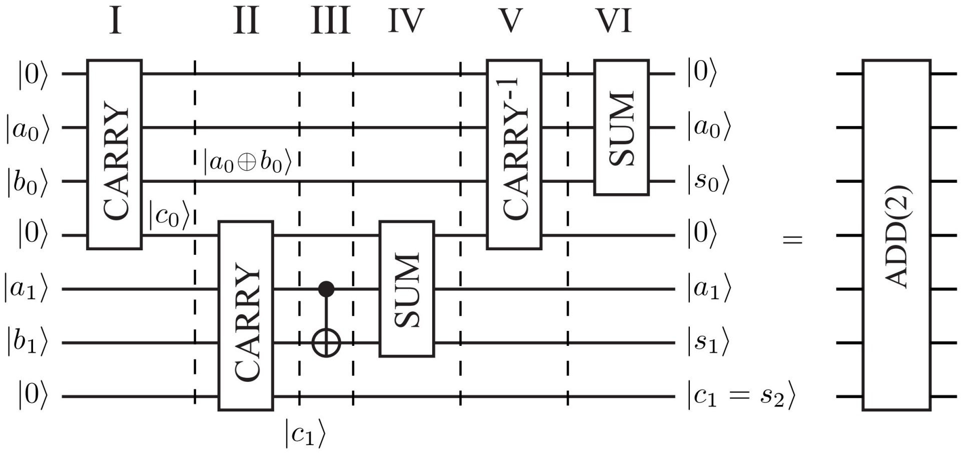

图 21: Quantum circuit to implement the ADD(2) gate, which adds two 2-bit numbers.

- Layer 1: 第一个 CARRY 门计算 $c_0 = a_0b_0$.
- Layer 2: 第二个 CARRY 门从 a_1, b_1, c_0 计算 $c_1 = s_2$.
- Layer 3:CNOT 门还原 $a_1 \oplus b_1$ 为 b_1.
- Layer 4:SUM 门计算 $s_1 = a_1 \oplus b_1 \oplus c_0$.
- Layer 5:CARRY^{-1} 门还原.
- Layer 6:SUM 门从 $|0, a_0, b_0\rangle$ 产生 $|0, a_0, s_0\rangle$.

同样,ADD(n) 可以由如下电路实现

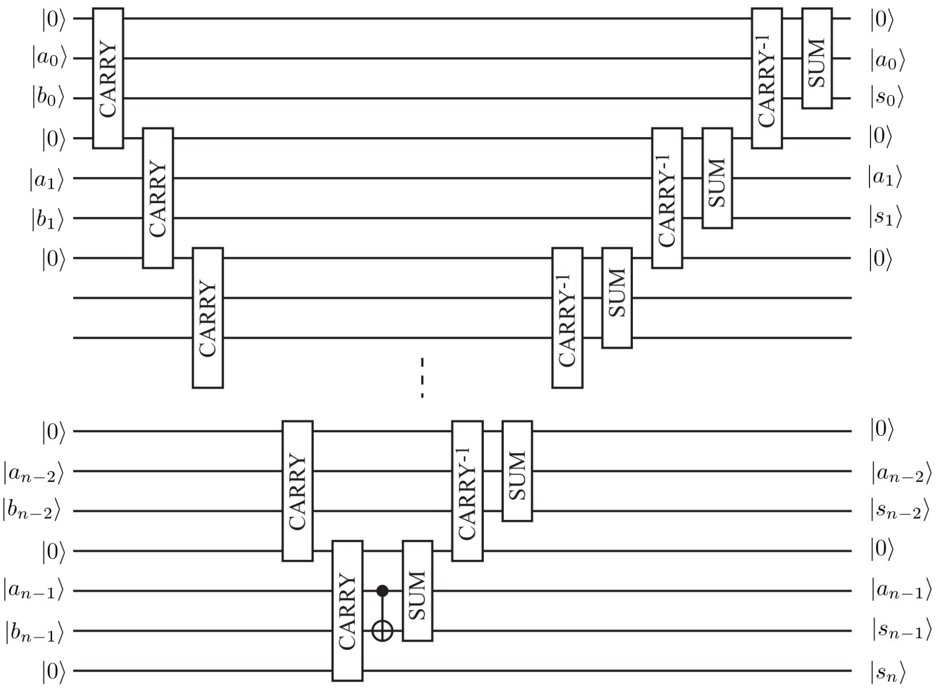

图 22: Quantum circuit to implement the ADD(n) gate,which adds two n-bit numbers a and b. The result is encoded in the qubits$\{|s_k\rangle\}$.

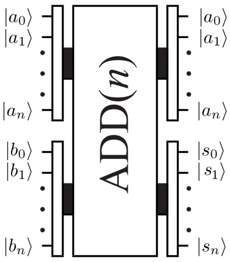

图 23: The black box representation of ADD(n).Note the order of the input bits and the output bits. We have explicitly added$|a_n\rangle = |b_n\rangle = |0\rangle$.

6.5.2 Modular Adder

命题 6.3. *n 位减法由 ADD(n) 实现*

$$ADD(n)^{-1}\,|0,a_0,b_0,0,a_1,b_1,0,\cdots,a_{n-1},b_{n-1},0\rangle = |0,a_0,s_0,0,a_1,s_1,0,\cdots,a_{n-1},s_{n-1},s_n\rangle \quad (6.19)$$

输出位 $s_0 \sim s_{n-1}$ 代表 $b-a$, 当 $s_n = 1$ 时 $b < a$ 反之 $b > a$.

量子电路实现如下, 中间有一步没看懂, 以后再补充.

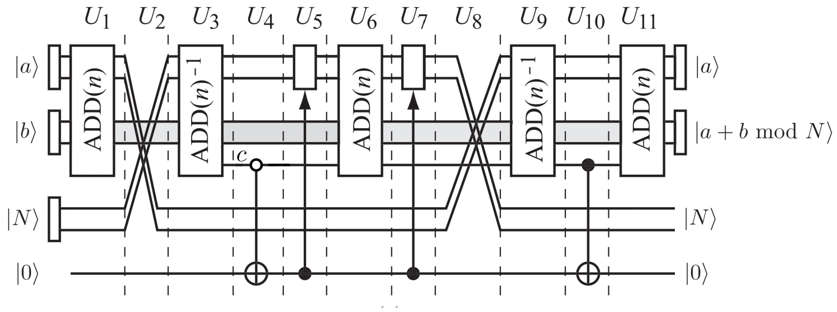

图 24: Modular adder which computes$a + b \mod N$. The gray line shows the information flow of the second register, corresponding to the input b and the output $a + b \mod N$.

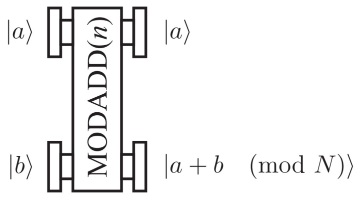

图 25: Modular adder is symbolically denoted as MODADD(n). The third register$|N\rangle$and the carry qubit$|0\rangle$are omitted.

6.5.3 Modular Multiplexer

controlled-modular multiplexer

$$\text{CMODMULTI(n)}\,|c, x, 0, 0\rangle = \begin{cases} |c, x, 0, ax \mod N\rangle & (c = 1) \\ |c, x, 0, x\rangle & (c = 0) \end{cases} \tag{6.20}$$

根据下式, 算法过程很明显

$$ax = ax_{n-1}2^{n-1} + \cdots ax_1 2 + ax_0 = \sum_{x_k=1} a2^k$$

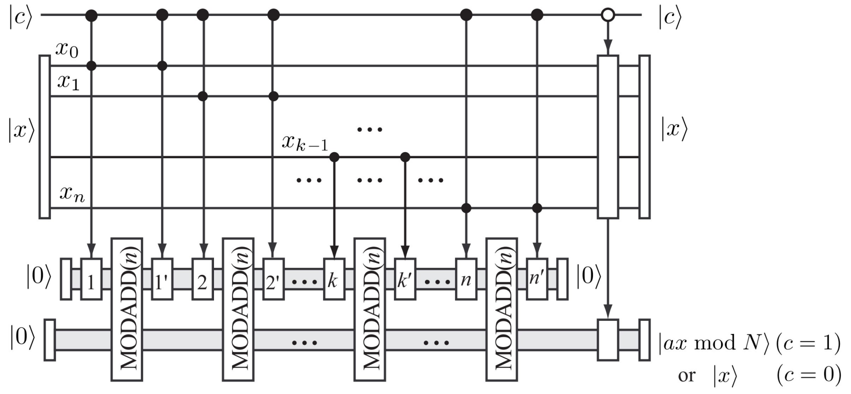

图 26: controlled-modular multiplexer circuit

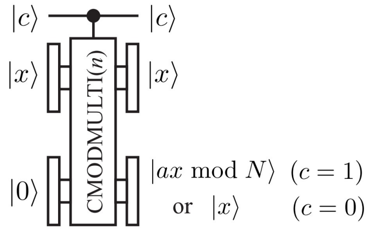

图 27: circuit is denoted as this figure

6.5.4 Modular Exponential Function

令

$$a = a_{n-1}2^{n-1} + \cdots a_1 2 + a_0$$
$$x = x_{n-1}2^{n-1} + \cdots x_1 2 + x_0$$

有

$$a^x = a^{x_{n-1}2^{n-1}} \times a^{x_{n-2}2^{n-2}} \times \cdots \times a^{x_1 2^1} \times a^{x_0} = \prod_{x_k=1} a^{2^k} \tag{6.21}$$

算法可以实现如下

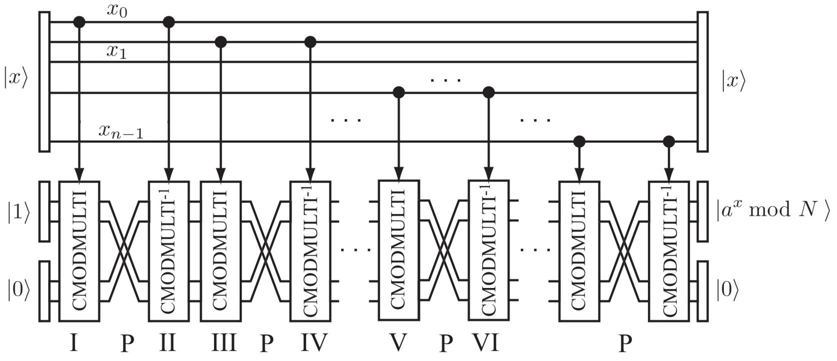

图 28: Quantum cirucuit which implements the modular exponential function$a^x \mod N$

最终我们得到了

$$\text{MODEXP}\,|x,1,0\rangle = |x, a^x \mod N, 0\rangle \tag{6.22}$$