

量子信息与量子密码

Quantum Information & Quantum Cryptology

[第4次课] 量子信息论与早期量子算法

授课教师：杨理

授课时间：2022年3月28日

内容概要

§ 3.1 量子信息论简介

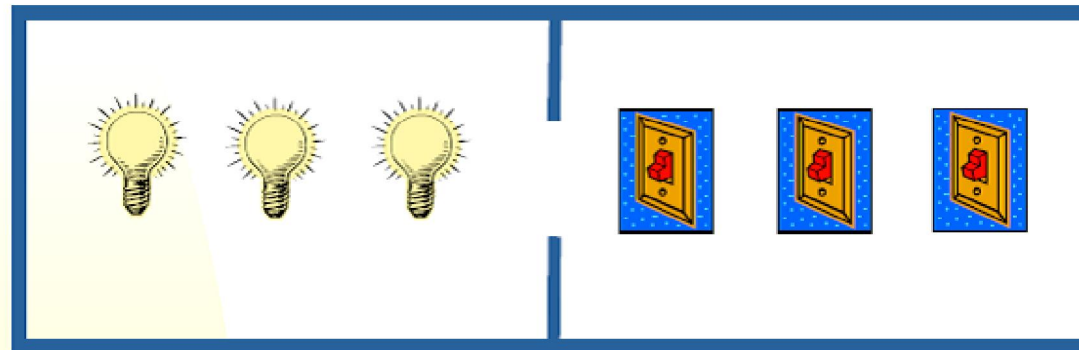
§ 3.2 量子通信

§ 3.3 量子逻辑门

§ 3.4 早期量子算法

A Puzzle

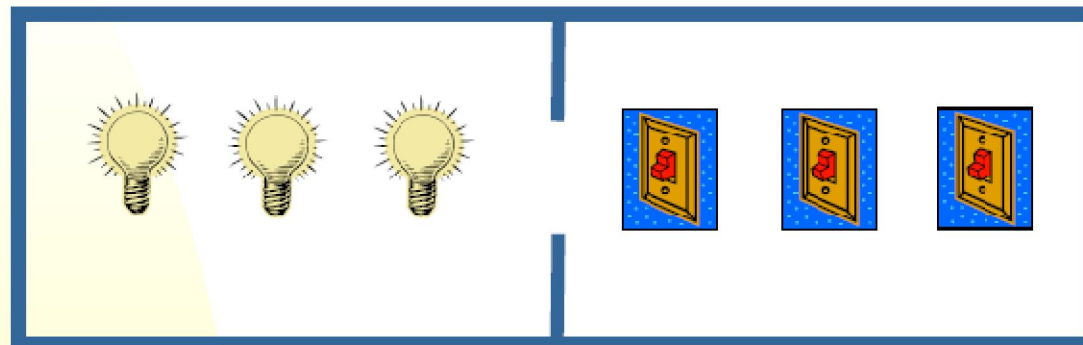
- Two rooms:
 - ◆ One room has three light switches
 - ◆ These are connected to three bulbs in the other room



- You don't know which bulbs are connected to which switches

A Puzzle

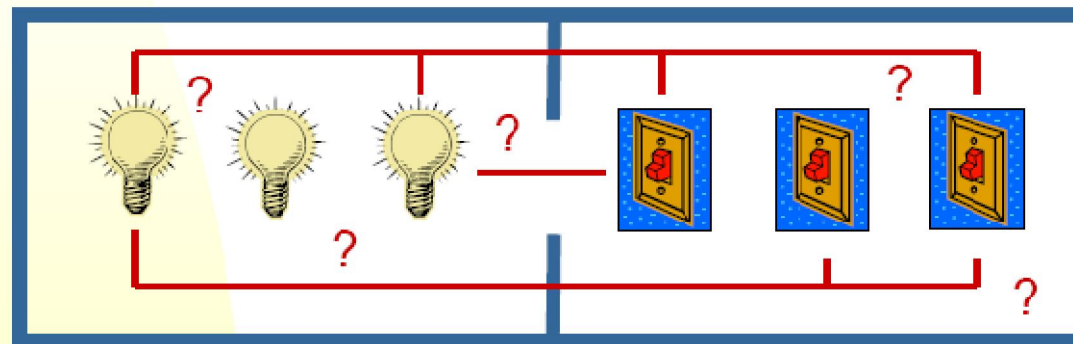
- Condition: you're only allowed to go into each room once



- PROBLEM: how do we figure out which bulb is connected to which switch?

The mathematician's problem

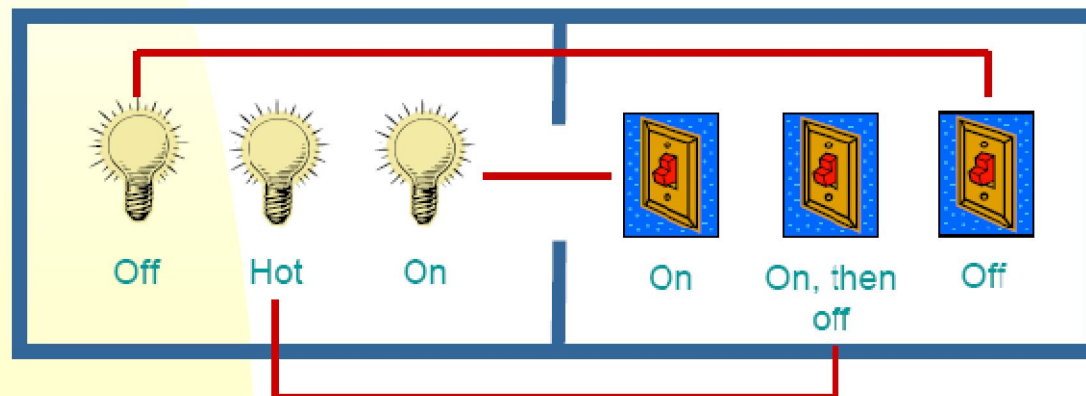
- As a mathematical problem, there is no solution
- I.e., there is no configuration for the switches (which you can only set once) that will give a unique matching of bulbs to switches when you observe the lights



NO SOLUTION?

The physicist's solution

- As a *physics* problem, there *is* a solution
- In the switch room:
 - ◆ Turn on two switches for a few minutes, then turn one off
- In the bulb room:
 - ◆ See which bulb is on, *feel* which other bulb is hot



Information is Physical

- Rolf Landauer

IBM Research

Quantum Computing - ISIT2005 Tutorial

7



Landauer 原理

- ◆ 每擦除一比特，或执行计算机中物理比特的一个扇入运算，至少增加环境的热量 $k_B T \ln 2$ 焦耳，其中

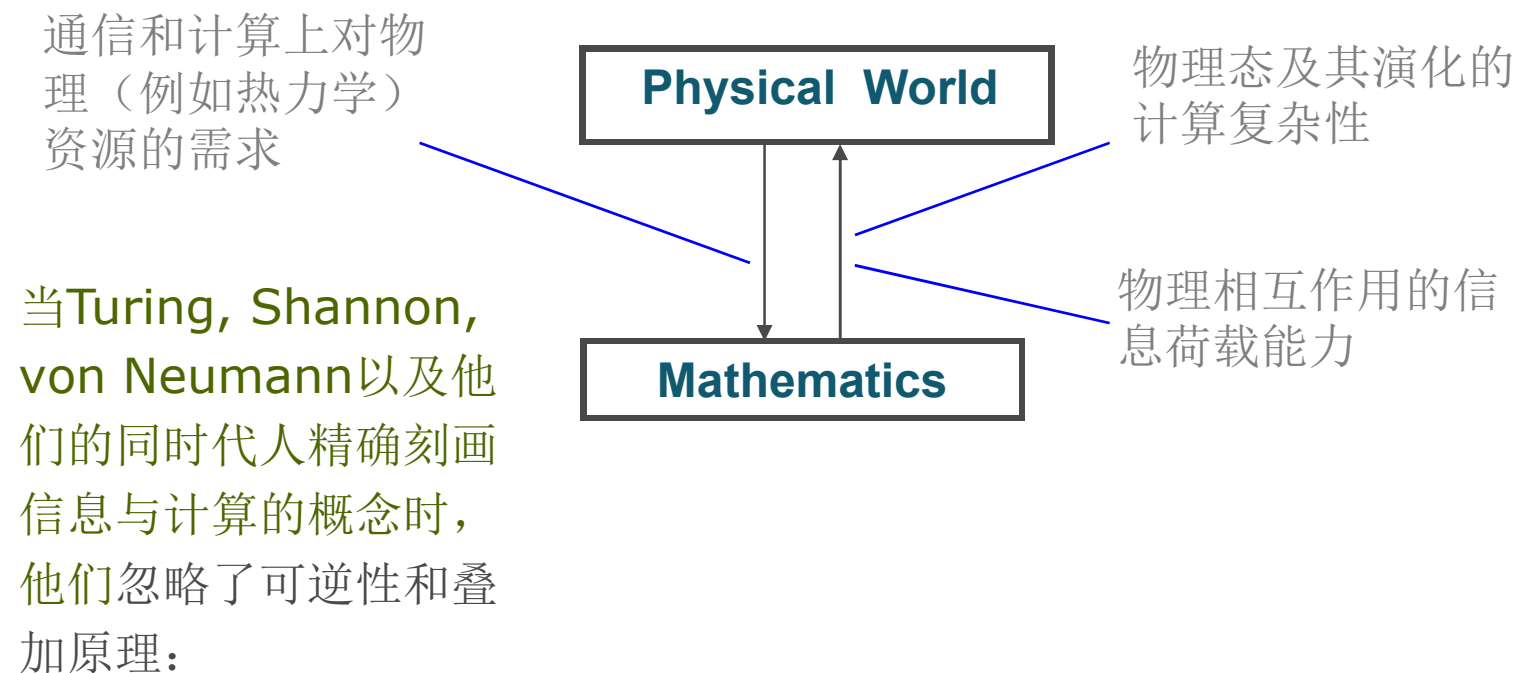
$$k_B = 1.38062 \times 10^{-23} \text{ J/K}$$

为波尔兹曼常数， T 为环境的绝对温度[1]。

[1]R. Landauer, Information is Physical, *Physics Today*, May 1991.

- ◆ 从Landauer原理到Maxwell佯谬的解决（C. Bennett）。

信息是物理的：进一步讨论



可逆性 \Rightarrow 计算热力学 （C. Bennett）

态叠加 \Rightarrow 量子信息的计算理论

电子自旋

- ◆ 1925年G.E.乌伦贝克和S.A.古兹密特受到泡利不相容原理的启发，基于Stern-Gerlach实验和原子光谱的一些实验结果，提出电子具有内禀运动--自旋，并且有与电子自旋相联系的自旋磁矩。
- ◆ 可以解释原子光谱的精细结构及反常塞曼效应。
- ◆ 1928年P.A.M.狄拉克提出电子的相对论波动方程，方程中自然地包括了电子自旋。
- ◆ 电子自旋是量子效应，不能作经典的理解，如果把电子自旋看成绕轴的旋转，则得出与相对论矛盾的结果。

§ 3.1 量子信息论简介

- ◆ 经典信息论主要关心通过经典信道传送经典信息。如果考虑经典信息或量子信息在量子信道中传送，会遇到新的问题。
- ◆ 虽然量子信息论产生于对量子信道的研究，但应用领域众多。
- ◆ 量子信息论在本质上比经典信息论更普适、更丰富、更深刻。
- ◆ 把接收者的accessible information定义为取遍所有测量方案时互信息 $H(X:Y)$ 的最大值，accessible information就是接收者能够在多大程度上推断出发送者制备状态的一种度量。
- ◆ Holevo界是accessible information的上界。

von Neumann Entropy

◆量子统计物理学中的熵算符：

$$\hat{S} \equiv -k_B \ln \hat{\rho}$$

◆量子统计物理学中的von Neumann熵：

$$S \equiv \langle \hat{S} \rangle = \text{Tr}(\hat{\rho} \hat{S}) = -k_B \text{Tr}(\hat{\rho} \ln \hat{\rho}).$$

◆在微正则系综中，上式正是Boltzmann公式

$$S = k_B \ln \Omega(E).$$

◆量子信息科学中的von Neumann 熵：

$$S(\rho) \equiv -\text{Tr}(\rho \log \rho) = -\sum_x \lambda_x \log \lambda_x.$$



Lvdwig Boltzmann

◆定理12.1 (Holevo界)

设Alice以概率 $\{p_0, \dots, p_n\}$ 制备状态 $\{\rho_x | x=1, \dots, n\}$, Bob进行由 POVM元 $\{E_y\} = \{E_0, \dots, E_m\}$ 描述的测量, 测量结果是 Y 。

Holevo证明, Bob的任何测量都满足:

$$H(X:Y) \leq S(\rho) - \sum_x p_x S(\rho_x) \equiv \chi,$$

其中 $\rho = \sum_x p_x \rho_x$ 。

◆Holevo界是 J. P. Gordon 1964年猜想的, Holevo 1973年给出证明。Holevo定理是量子信息论的基石。

◆Holevo界也叫做Holevo χ 量。

Schumacher 定理

◆定理 12.6 (Schumacher 无噪声信道的编码定理)

令 $\{H, \rho\}$ 是独立同分布的量子信源。若 $R > S(\rho)$, 则对该源存在比率为 R 的可靠压缩方案。若 $R < S(\rho)$, 则比率为 R 的任何压缩方案都不可靠。

◆是Shannon第一定理的量子推广，本课程后面将给出严格的证明。

◆ ε -典型序列发展为 ε -典型状态；典型序列定理发展为典型子空间定理。

量子信道上的经典通信- HSW 定理

信道 \mathcal{E} 传递直积态 $\rho_1 \otimes \rho_2 \otimes \cdots \otimes \rho_n$ 编码经典消息，则信道容量

$C^{(1)}(\mathcal{E})$ 由下述定理给出：

HSW 定理 设 \mathcal{E} 是一个保迹量子操作，定义：

$$\chi(\mathcal{E}) \equiv \max_{\{p_i, \rho_i\}} \left[S \left(\mathcal{E} \left(\sum_j p_j \rho_j \right) \right) - \sum_j p_j S \left(\mathcal{E}(\rho_j) \right) \right],$$

其中最大值是在信道的所有可能状态 ρ_j 的系综 $\{p_j, \rho_j\}$ 上取的，则有 $C^{(1)}(\mathcal{E}) = \chi(\mathcal{E})$.

§ 3.2 量子通信

1. Super-dense Coding

Alice和Bob共享一个处于Bell态 $|\Phi^+\rangle$ 的EPR对，Alice 对手中的粒子做下述四个操作之一：

$$\begin{aligned} X_1|\Phi^+\rangle &= |\Psi^+\rangle, Z_1|\Phi^+\rangle = |\Phi^-\rangle, \\ Y_1|\Phi^+\rangle &= |\Psi^-\rangle, I_1|\Phi^+\rangle = |\Phi^+\rangle, \end{aligned}$$

然后将粒子发给Bob，如果Bob可以进行Bell基测量，则可以确知Alice所做的操作，于是实现了一个粒子传递 2 比特经典信息的任务。

2. 量子Teleportation

- ◆如果只通过定域量子操作和经典信号传递 (LOCC) 即可将 $|\Psi\rangle$ 变为 $|\Phi\rangle$, 则称 $|\Psi\rangle$ LOCC可归约为 $|\Phi\rangle$, 记为

$$|\Psi\rangle \xrightarrow{LOCC} |\Phi\rangle$$

- ◆如果 $|\Psi\rangle \xrightarrow{LOCC} |\Phi\rangle$ 且 $|\Phi\rangle \xrightarrow{LOCC} |\Psi\rangle$, 则称 $|\Psi\rangle$ 和 $|\Phi\rangle$ 是LOCC等价的, 记为

$$|\Psi\rangle \xleftrightarrow{LOCC} |\Phi\rangle$$

- ◆如果 $|\Psi\rangle$ 与 $|\Phi\rangle$ 只相差一个定域酉变换, 则称 $|\Psi\rangle$ 与 $|\Phi\rangle$ 是LU等价的。Bennett et al. 证明, 对于纯态, LU等价与LOCC等价是相同的(e-print arXive: quant-ph/9912039)。

量子Teleportation

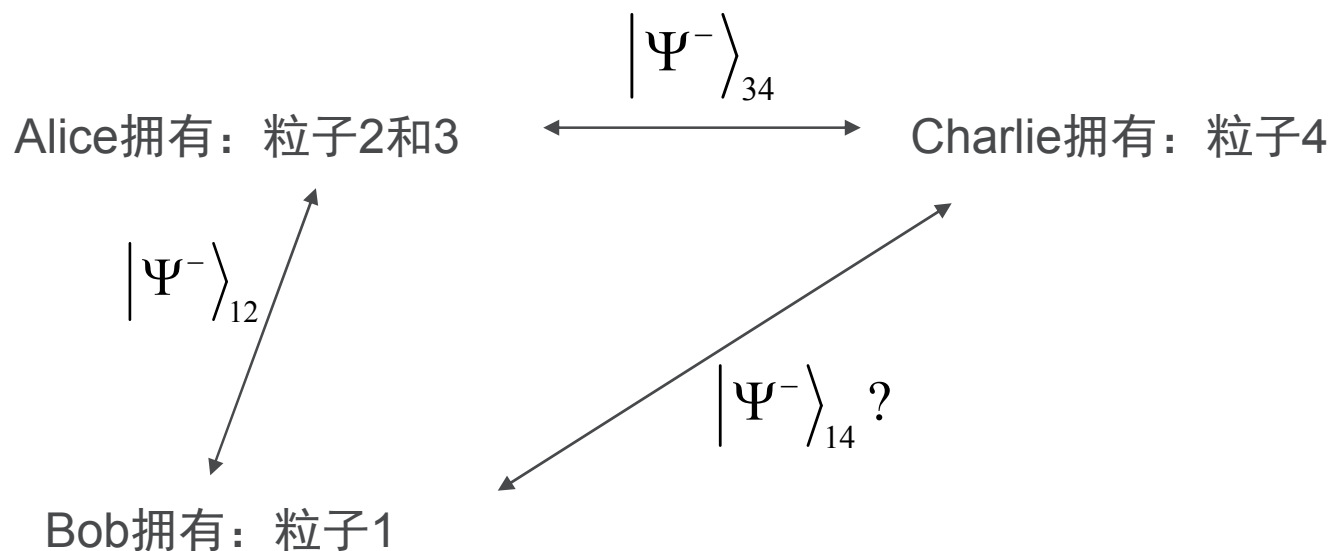
◆从LOCC的观点来看量子 Teleportation:

$$\begin{aligned} |\Psi^-\rangle_{12} |\phi\rangle_3 &= \frac{1}{\sqrt{2}} (|0\rangle_1 |1\rangle_2 - |1\rangle_1 |0\rangle_2) (\alpha |0\rangle_3 + \beta |1\rangle_3) \\ &= \frac{1}{2} \left[(\alpha |1\rangle_1 + \beta |0\rangle_1) |\Phi^+\rangle_{23} + (\alpha |1\rangle_1 - \beta |0\rangle_1) |\Phi^-\rangle_{23} \right. \\ &\quad \left. + (-\alpha |0\rangle_1 - \beta |1\rangle_1) |\Psi^+\rangle_{23} + (\alpha |0\rangle_1 - \beta |1\rangle_1) |\Psi^-\rangle_{23} \right] \end{aligned}$$

Alice 测量手中的2、3粒子处于哪一Bell态，告诉Bob，Bob对粒子1进行操作(X,Y,Z, I)以使粒子1处于 。

3. 量子纠缠交换

◆ 纠缠交换（ Entanglement Swapping ）方案：如何通过LOCC使从未谋面、也未进行直接量子通信的Bob和Charlie共享纠缠态？



量子纠缠交换

◆初态为：

$$|\Psi\rangle_{1234} = \frac{1}{2}(|0\rangle_1|1\rangle_2 - |1\rangle_1|0\rangle_2)(|0\rangle_3|1\rangle_4 - |1\rangle_3|0\rangle_4)$$

◆将其表示为按 $|\Phi^\pm\rangle_{23}$ 和 $|\Psi^\pm\rangle_{23}$ 展开的形式：

$$\begin{aligned} |\Phi\rangle_{1234} = & \frac{1}{2} \left[|0\rangle_1 \frac{1}{\sqrt{2}} (|\Psi^+\rangle_{23} - |\Psi^-\rangle_{23}) |1\rangle_4 \right. \\ & - |0\rangle_1 \frac{1}{\sqrt{2}} (|\Phi^+\rangle_{23} - |\Phi^-\rangle_{23}) |0\rangle_4 \\ & - |1\rangle_1 \frac{1}{\sqrt{2}} (|\Phi^+\rangle_{23} + |\Phi^-\rangle_{23}) |1\rangle_4 \\ & \left. + |1\rangle_1 \frac{1}{\sqrt{2}} (|\Psi^+\rangle_{23} + |\Psi^-\rangle_{23}) |0\rangle_4 \right] \end{aligned}$$

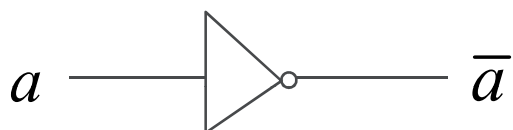
量子纠缠交换

$$= \frac{1}{2} \left(-|\Phi^+\rangle_{23} |\Phi^+\rangle_{14} + |\Phi^-\rangle_{23} |\Phi^-\rangle_{14} \right. \\ \left. + |\Psi^+\rangle_{23} |\Psi^+\rangle_{14} - |\Psi^-\rangle_{23} |\Psi^-\rangle_{14} \right)$$

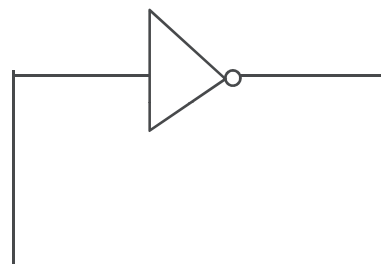
- ① Alice通过定域操作测量粒子2、3；
- ② Alice用经典信道通知Bob和Charlie测量结果；
- ③ Bob和Charlie通过定域操作 (I, X, Y, Z) 共享 $|\Psi^-\rangle_{14}$ 。

1. 基本的经典逻辑门与计算逻辑线路

逻辑线路模型所计算的函数为逻辑函数 $f: \{0,1\}^k \rightarrow \{0,1\}$.
计算的线路模型中所用线路都是无环的。

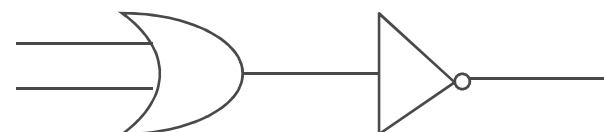
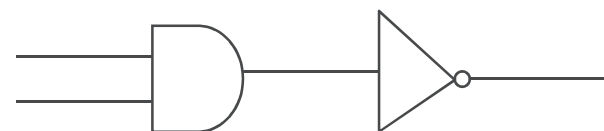
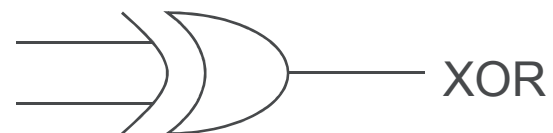
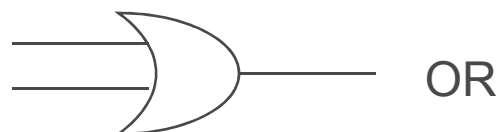
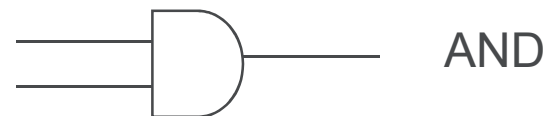
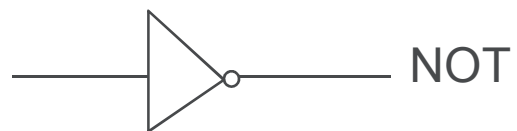


单输入比特上的非门运算路线。

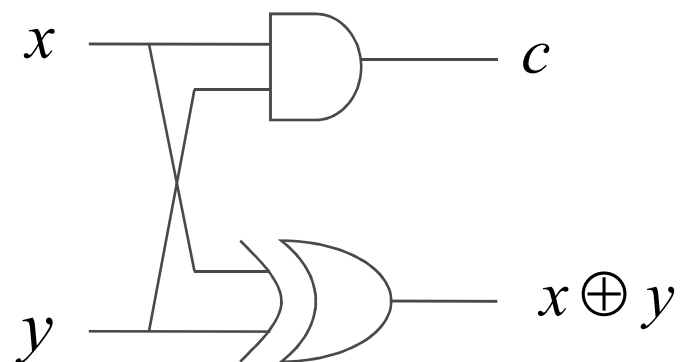


回路可能会不稳定，计算模型中一般不采用回路结构。

1. 基本的经典逻辑门与计算逻辑线路 (2)



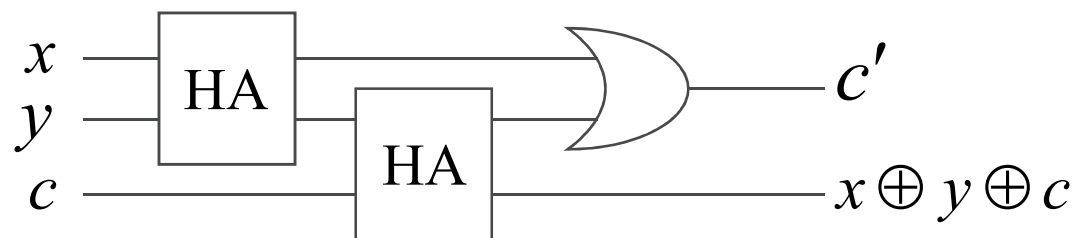
1. 基本的经典逻辑门与计算线路 (3)



半加器 (HA) 线路

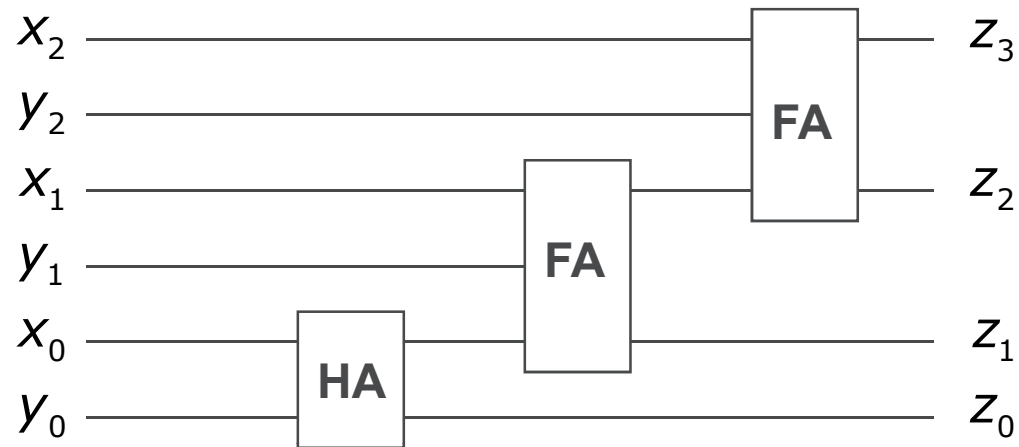
进位比特 c 当 x 和 y 都是1时置1，否则置0。

1. 基本的经典逻辑门与计算逻辑线路 (3)



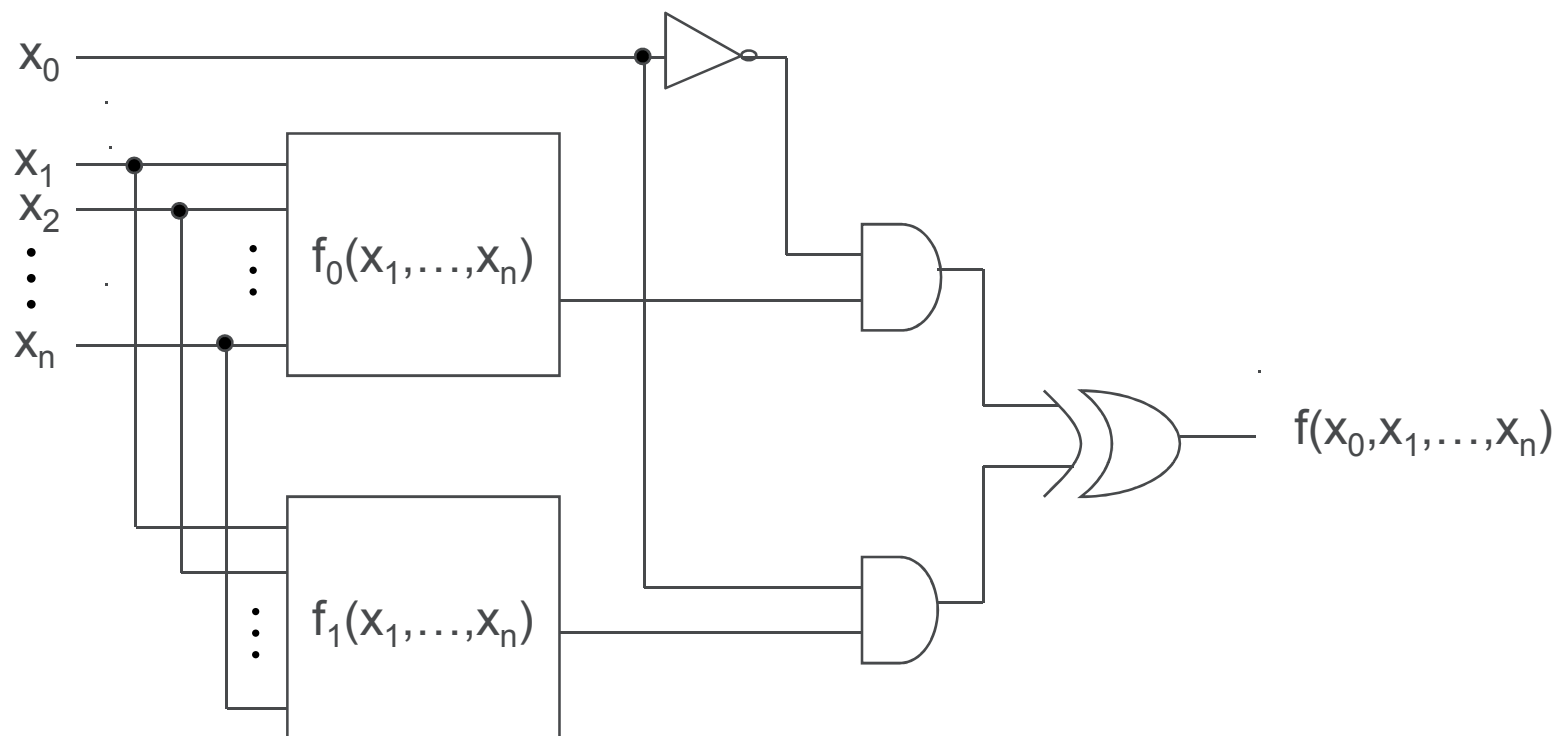
全加器 (FA) 线路

1. 基本的经典逻辑门与计算逻辑线路 (4)



Addition circuit for two three-bit integers, $x = x_2x_1x_0$ and $y = y_2y_1y_0$, using the elementary algorithm taught to school-children.

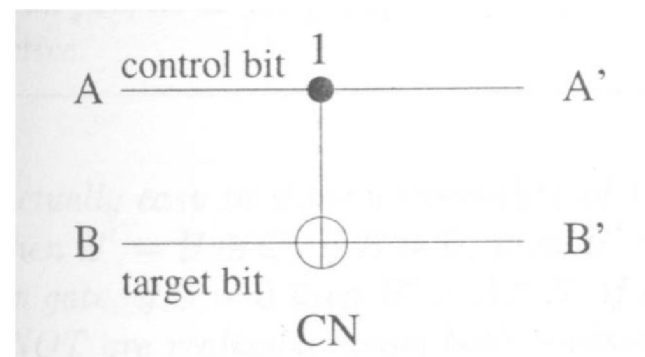
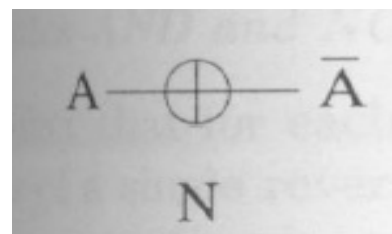
1. 基本的经典逻辑门与计算逻辑线路 (5)



递归构造计算任意布尔函数的线路

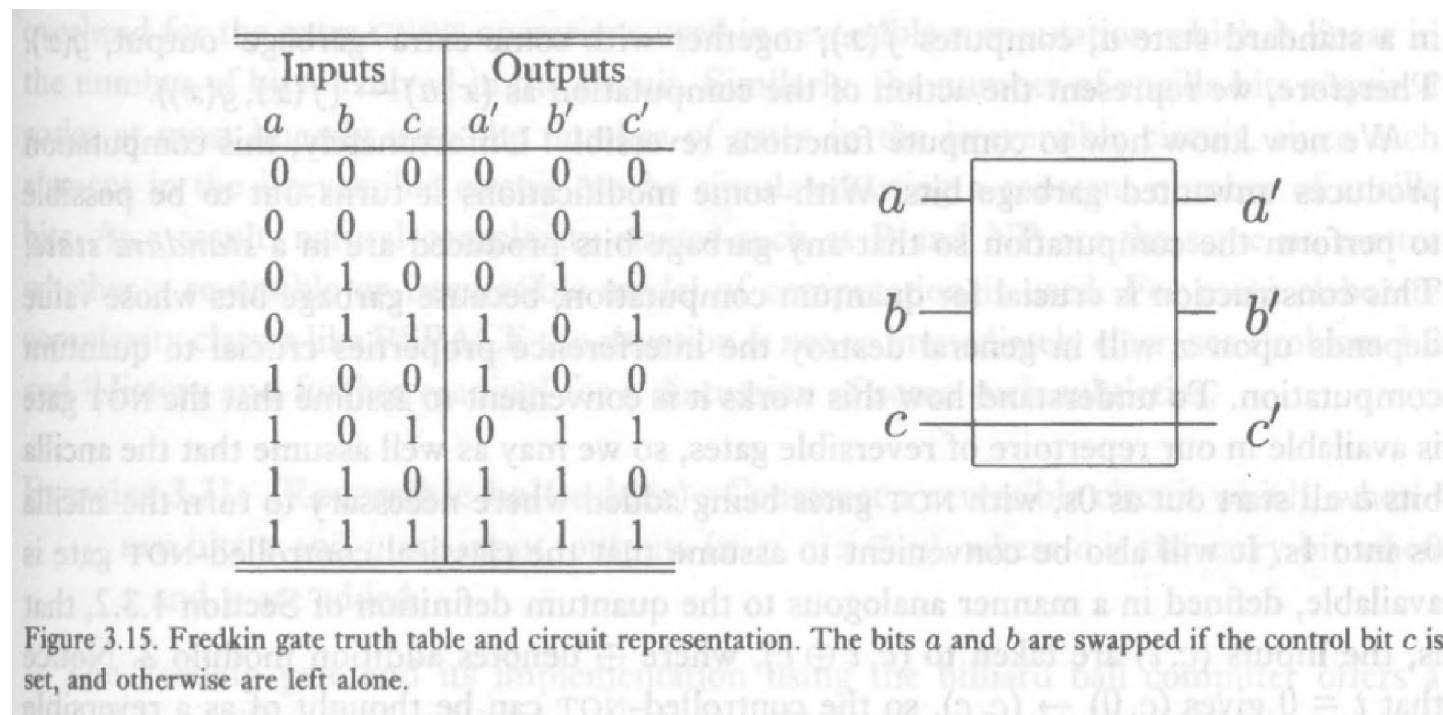
2. 基本的可逆逻辑门

基本的可逆逻辑门包括非门、受控非门、双控非门（Toffoli门）、受控交换门（Fredkin门）等。



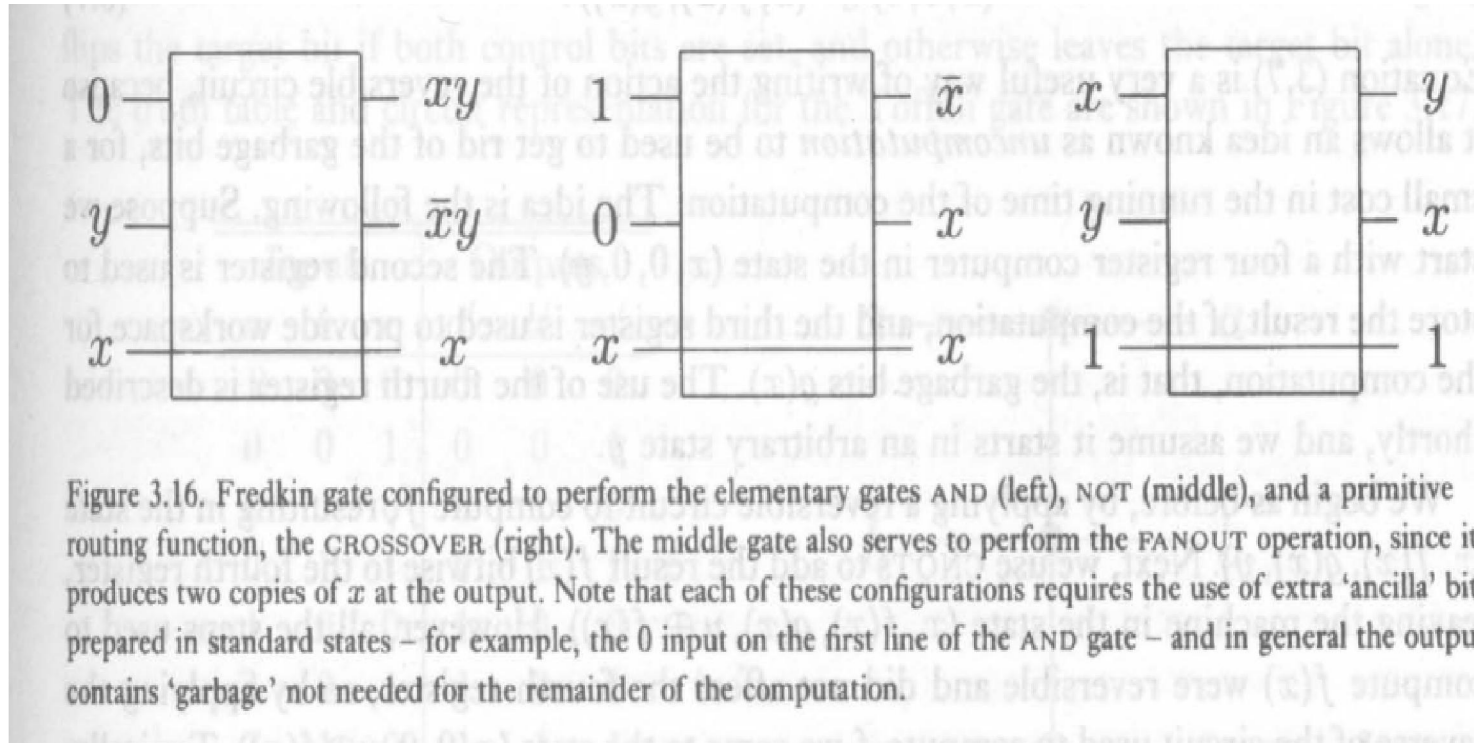
2. 基本的可逆逻辑门 (2)

Fredkin门的真值表:



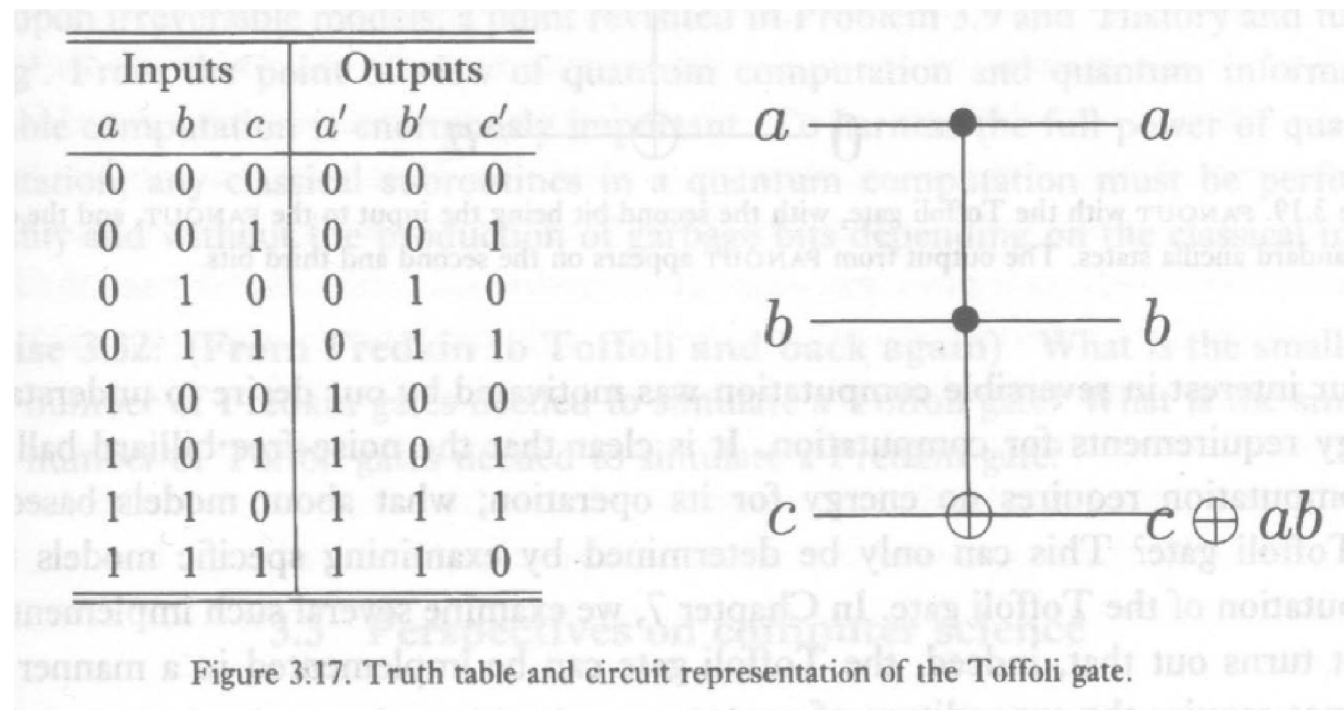
2. 基本的可逆逻辑门 (3)

Fredkin门是通用逻辑门：



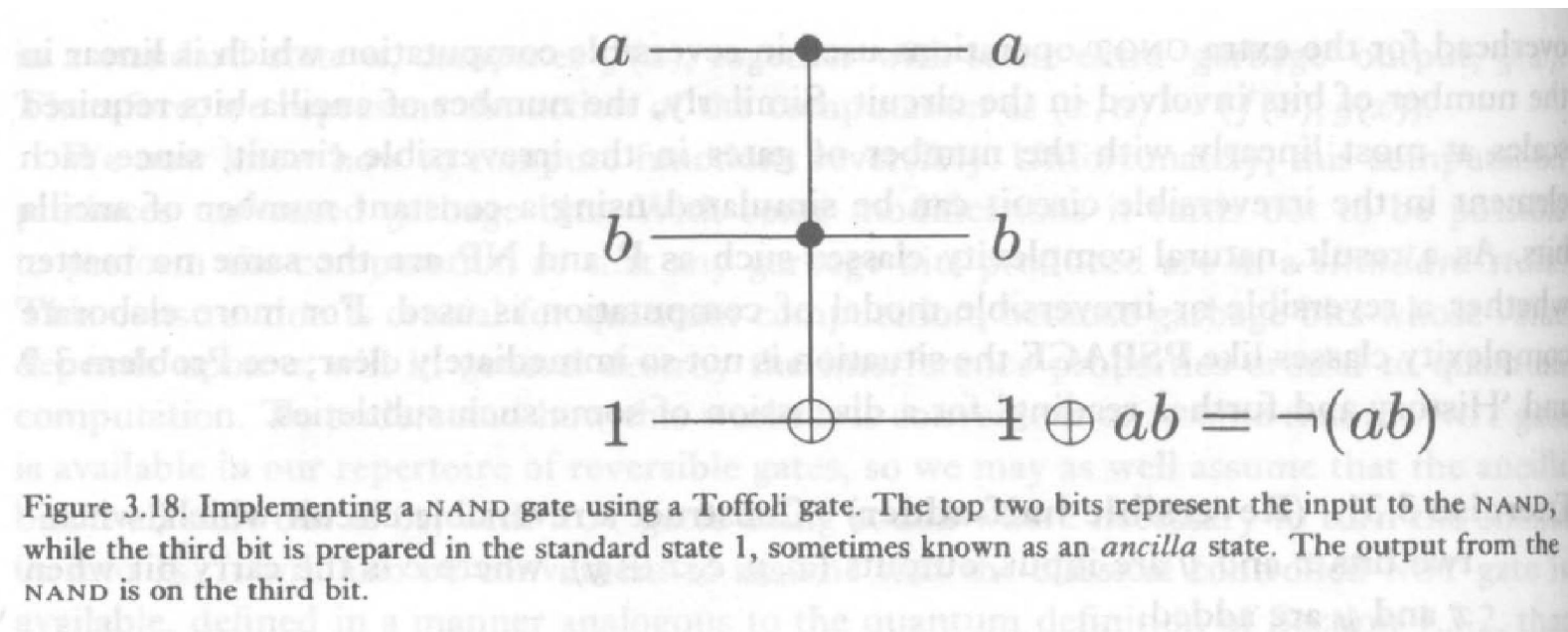
2. 基本的可逆逻辑门 (4)

Toffoli门的真值表:



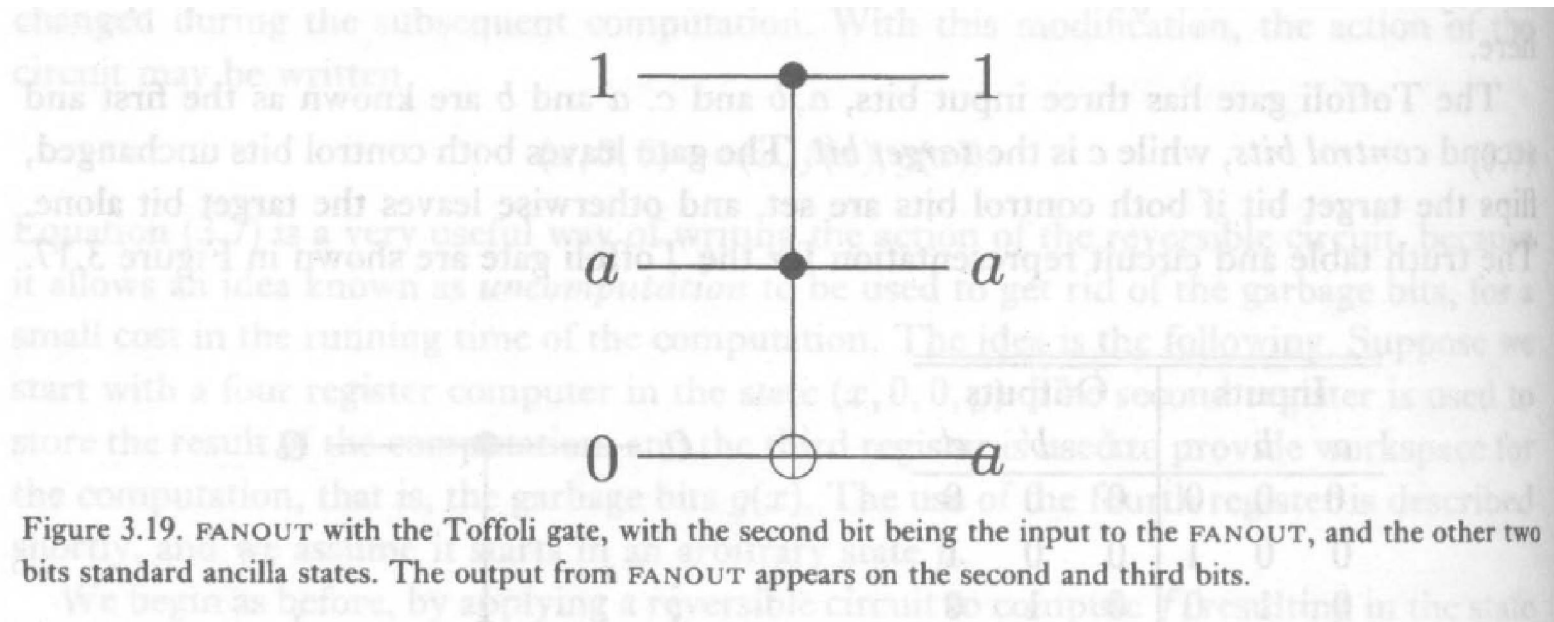
2. 基本的可逆逻辑门 (5)

Toffoli门是通用逻辑门—与非运算：



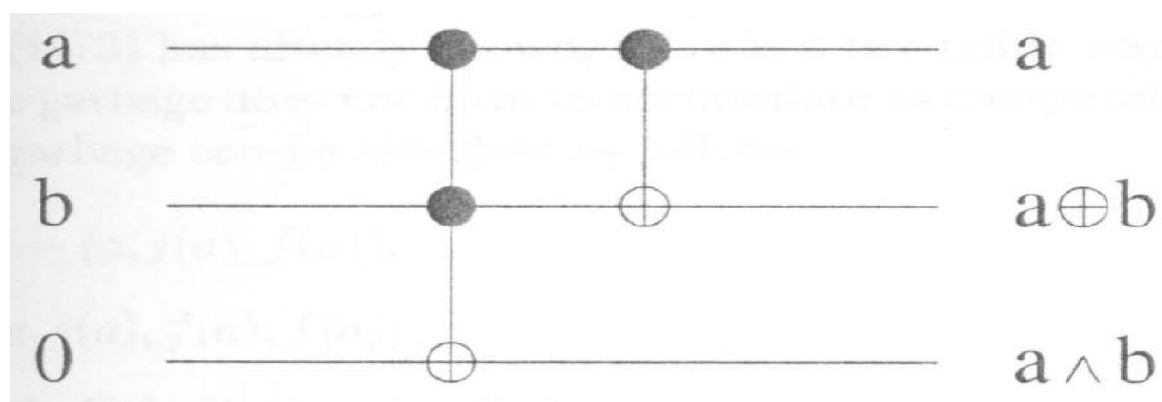
2. 基本的可逆逻辑门 (6)

Toffoli门是通用逻辑门—扇出运算：



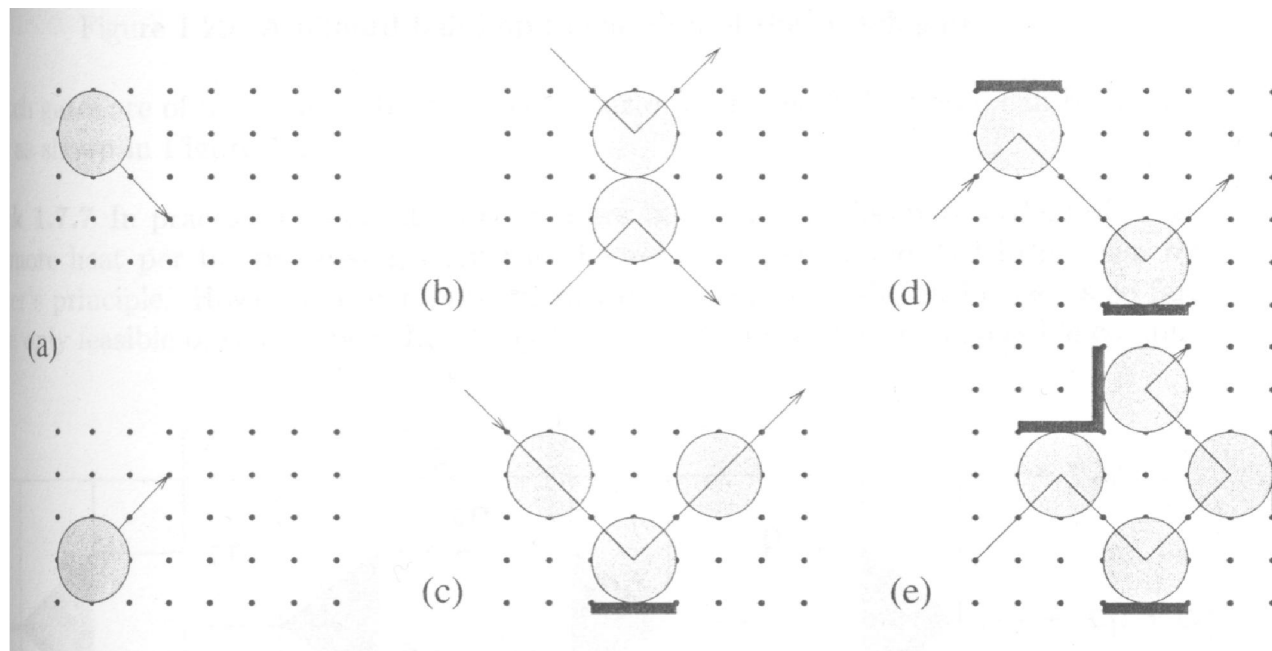
2. 基本的可逆逻辑门 (7)

基于Toffoli门的可逆两比特加法器 (HA) :



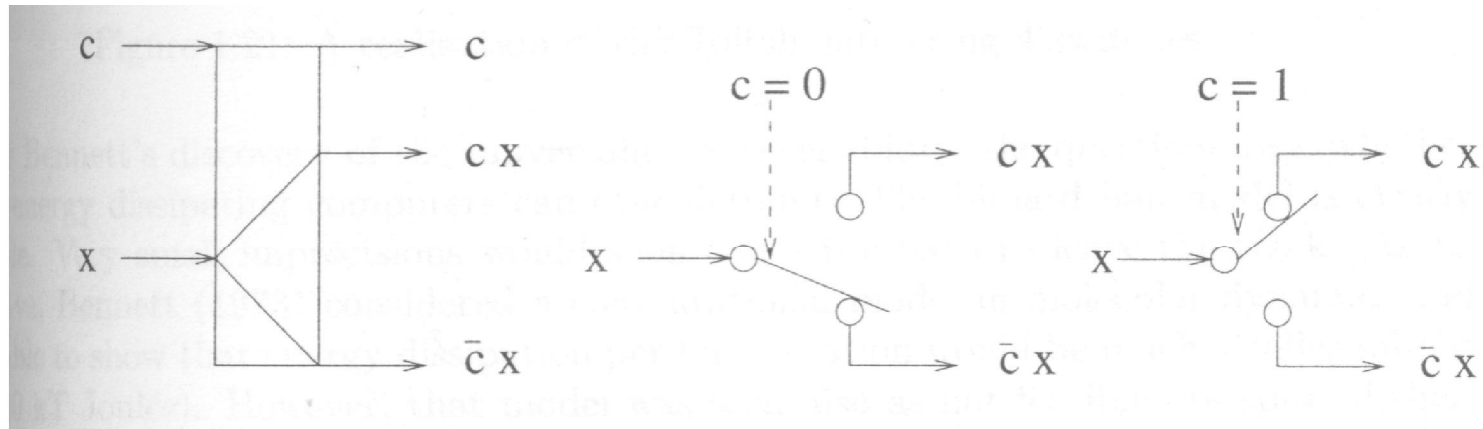
3. 可逆计算的硬球模型

◆ Billiard ball model of reversible computation:



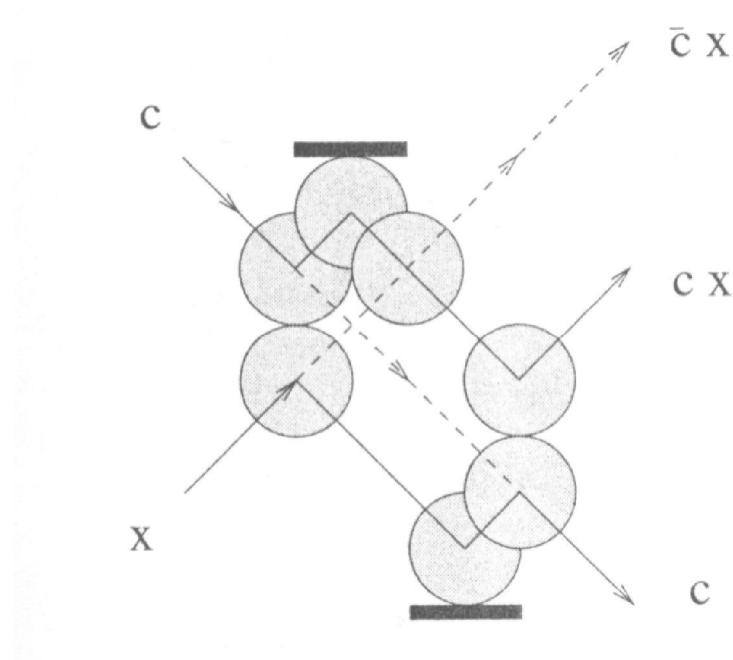
3. 可逆计算的硬球模型 (2)

◆ Switch gate:



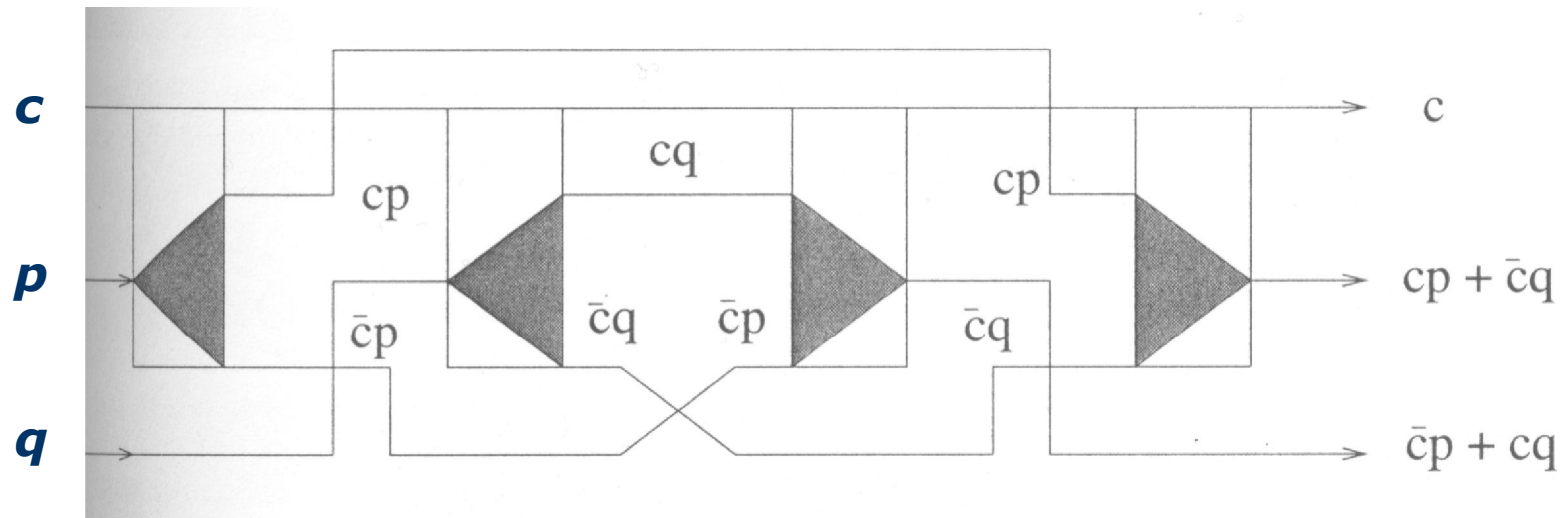
3. 可逆计算的硬球模型 (3)

◆ A billiard ball implementation of the switch gate:

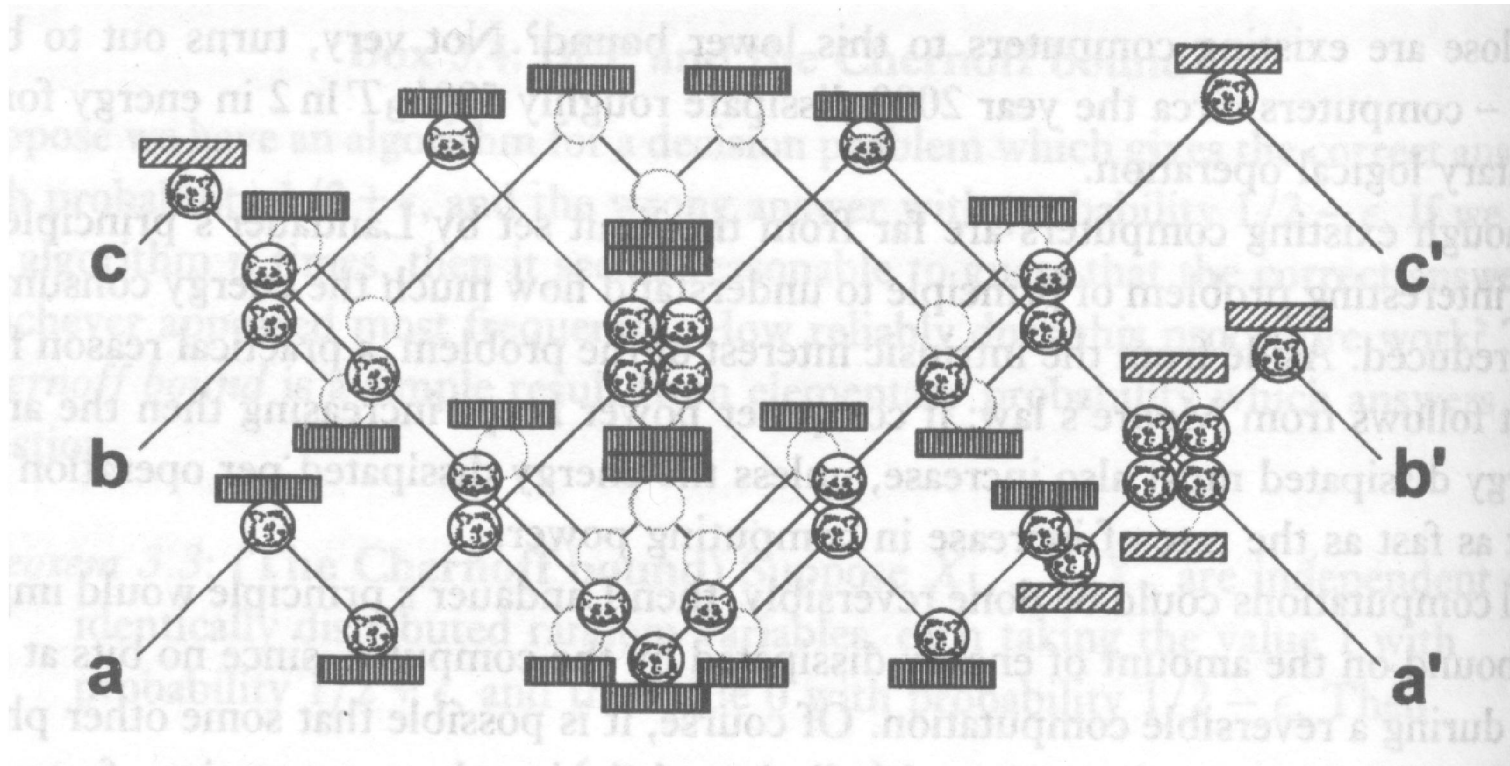


3. 可逆计算的硬球模型 (4)

◆ A realization of the (anti-)Fredkin gate using 4 switches:



3. 可逆计算的硬球模型 (5)

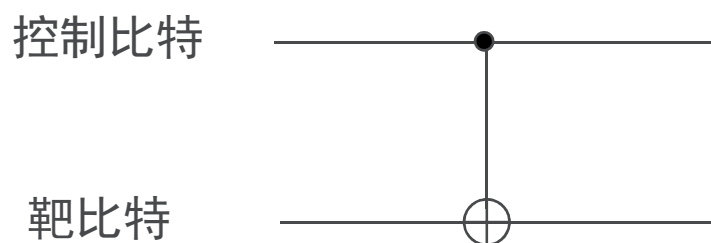


A realization of the Fredkin gate

4. 量子逻辑门

(1) 单量子比特门：可作用于量子比特（复二维向量空间）的两维酉变换， $\{I, X \equiv \sigma_x, Y \equiv \sigma_y, Z \equiv \sigma_z\}$ 为一组基。

(2) 量子 CNOT 门：可作用于量子叠加态的 CNOT 门。



$$|c\rangle|t\rangle \rightarrow |c\rangle|t \oplus c\rangle.$$

矩阵表示：

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

4. 量子逻辑门——单量子比特门的一般形式

◆ 单量子比特门可以写成如下的一般形式：

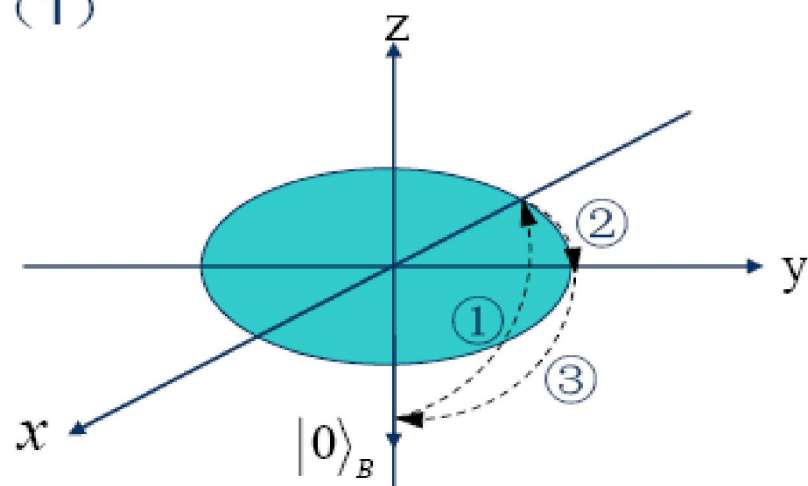
$$U = \begin{bmatrix} e^{i\left(\alpha - \frac{\beta}{2} - \frac{\delta}{2}\right)} \cos \frac{\gamma}{2} & -e^{i\left(\alpha - \frac{\beta}{2} + \frac{\delta}{2}\right)} \sin \frac{\gamma}{2} \\ e^{i\left(\alpha + \frac{\beta}{2} - \frac{\delta}{2}\right)} \sin \frac{\gamma}{2} & e^{i\left(\alpha + \frac{\beta}{2} + \frac{\delta}{2}\right)} \cos \frac{\gamma}{2} \end{bmatrix},$$

定理：对任意单量子比特的 U 变换，存在实参数 $\alpha, \beta, \gamma, \delta$ ，使得 $U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)$ ，其中

$$R_{\vec{n}}(\theta) \equiv e^{-i\theta \vec{n} \cdot \vec{\sigma}/2} = \cos \frac{\theta}{2} I - i \sin \frac{\theta}{2} (n_x X + n_y Y + n_z Z).$$

4. 量子逻辑门--CNOT门的物理实现（自旋qubit）

(1)



$$|0\rangle_A |0\rangle_B \rightarrow |0\rangle_A |0\rangle_B$$

A为控制位

CNOT门:

$$y\left(\frac{\pi}{2}\right) \oplus \tau \text{ 进动} \oplus x\left(-\frac{\pi}{2}\right),$$

其中: τ 进动沿 $-z$ 方向,

控制位 = $|0\rangle$, 进动 $\frac{\pi}{2}$;

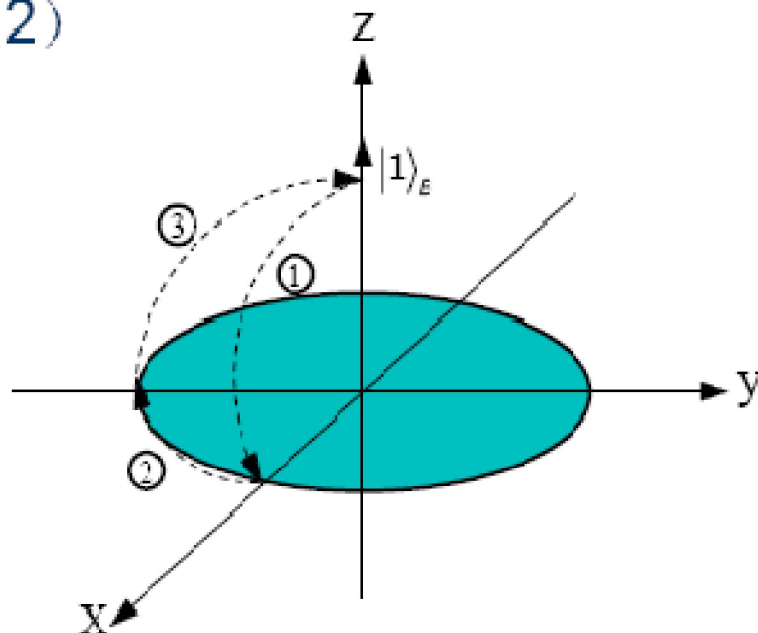
控制位 = $|1\rangle$, 进动 $\frac{3\pi}{2}$.

信息位: 自旋沿 $-Z$ 方向为 $|0\rangle$,

自旋沿 Z 方向为 $|1\rangle$.

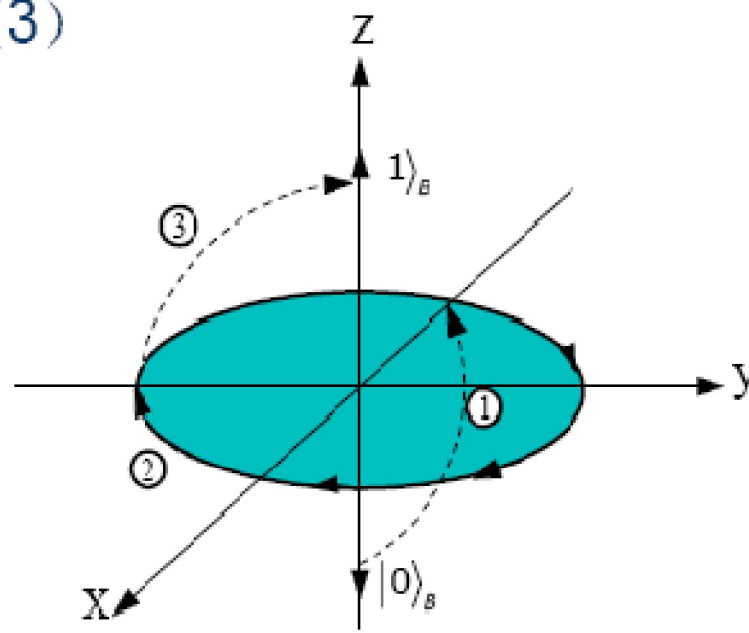
4. 量子逻辑门--CNOT门的物理实现 (自旋qubit)

(2)



$$|0\rangle_A |1\rangle_B \rightarrow |0\rangle_A |1\rangle_B$$

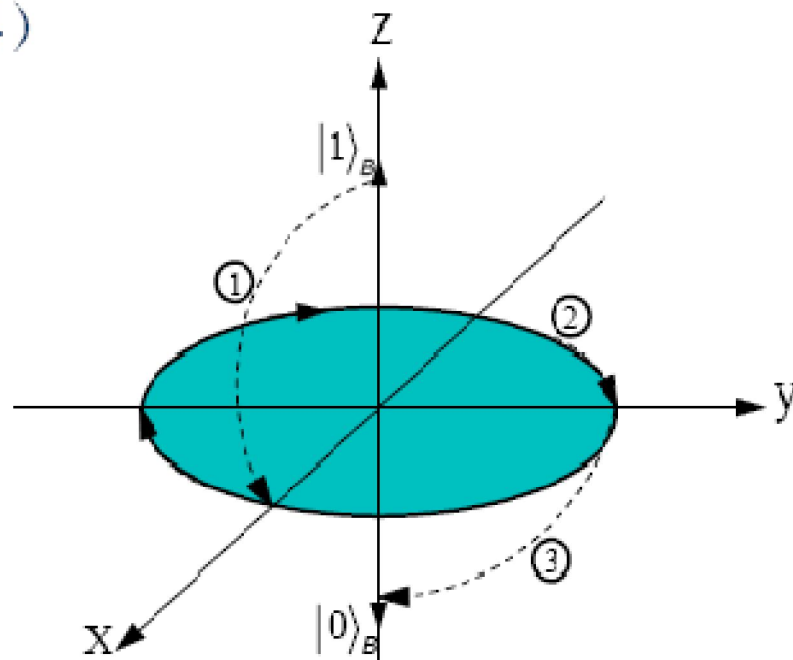
(3)



$$|1\rangle_A |0\rangle_B \rightarrow |1\rangle_A |1\rangle_B$$

4. 量子逻辑门--CNOT门的物理实现（自旋qubit）

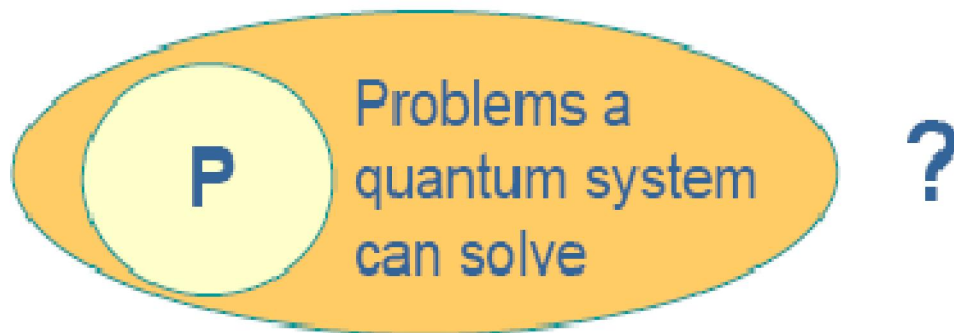
(4)



控制位处于相干叠加态
导致控制位和信息位纠缠的物理基础是定域相互作用。

$$\boxed{|1\rangle_A |1\rangle_B \rightarrow |1\rangle_A |0\rangle_B}$$

§ 3.4 简单量子算法



量子计算机可以有效求解任何P类问题，但已知其不能有效求解PSPACE类以外的问题。量子计算机可有效求解的问题类在P类和PSPACE类之间的什么位置还不清楚。该问题的解决很可能导致PSPACE类是否等于P类这个计算机科学重要问题的解决。



David
Deutsch

Quantum Parallelism

- ◆ Quantum parallelism is that feature of quantum computers which makes it possible to evaluate a function $f(x)$ on many different values of x simultaneously
- ◆ We will look at an example of quantum parallelism now – how to compute $f(0)$ and $f(1)$ for some function f all in one go!

Circuits for Boolean Functions

- ◆ It is known that, for any Boolean function

$$f : \{0,1\} \mapsto \{0,1\}$$

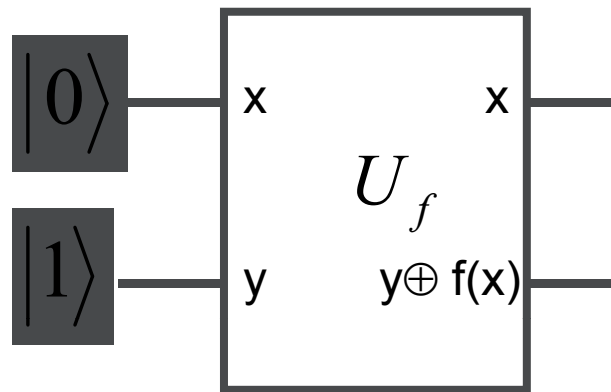
- ◆ it is possible to construct a quantum circuit U_f that computes it
- ◆ Specifically, to each binary function f corresponds a quantum circuit:

$$U_f : |x, y\rangle \mapsto |x, y \oplus f(x)\rangle$$

binary addition

Circuits for Boolean Functions (2)

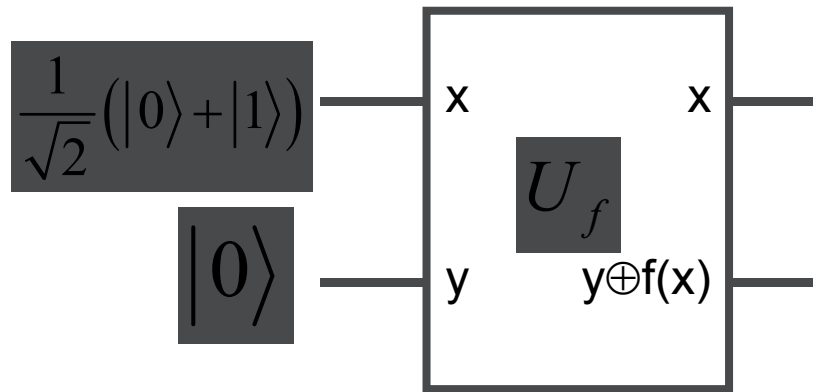
◆ What can this circuit U_f do? Example:



$$\begin{aligned} |\psi\rangle &= U_f (|0\rangle \otimes |1\rangle) \\ &= U_f |0, 1\rangle \\ &= |0, 1 \oplus f(0)\rangle \end{aligned}$$

Circuits for Boolean Functions (3)

◆ But what if the input is a superposition?



amazing! we've computed $f(0)$ and $f(1)$ at the same time!

$$\begin{aligned} |\psi\rangle &= U_f \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \cdot |0\rangle \right) \\ &= U_f \left(\frac{|00\rangle + |10\rangle}{\sqrt{2}} \right) \\ &= \frac{|0, 0 \oplus f(0)\rangle + |1, 0 \oplus f(1)\rangle}{\sqrt{2}} \\ &= \frac{|0, f(0)\rangle + |1, f(1)\rangle}{\sqrt{2}} \end{aligned}$$

Quantum Parallelism Summary

- ◆ So, a superposition of inputs will give a superposition of outputs!
- ◆ We can perform many computations simultaneously
- ◆ This is what makes famous quantum algorithms, such as Shor's algorithm for factoring, or Grover's algorithm for searching
- ◆ Simple algorithm: Deutsch's algorithm

Deutsch's Algorithm

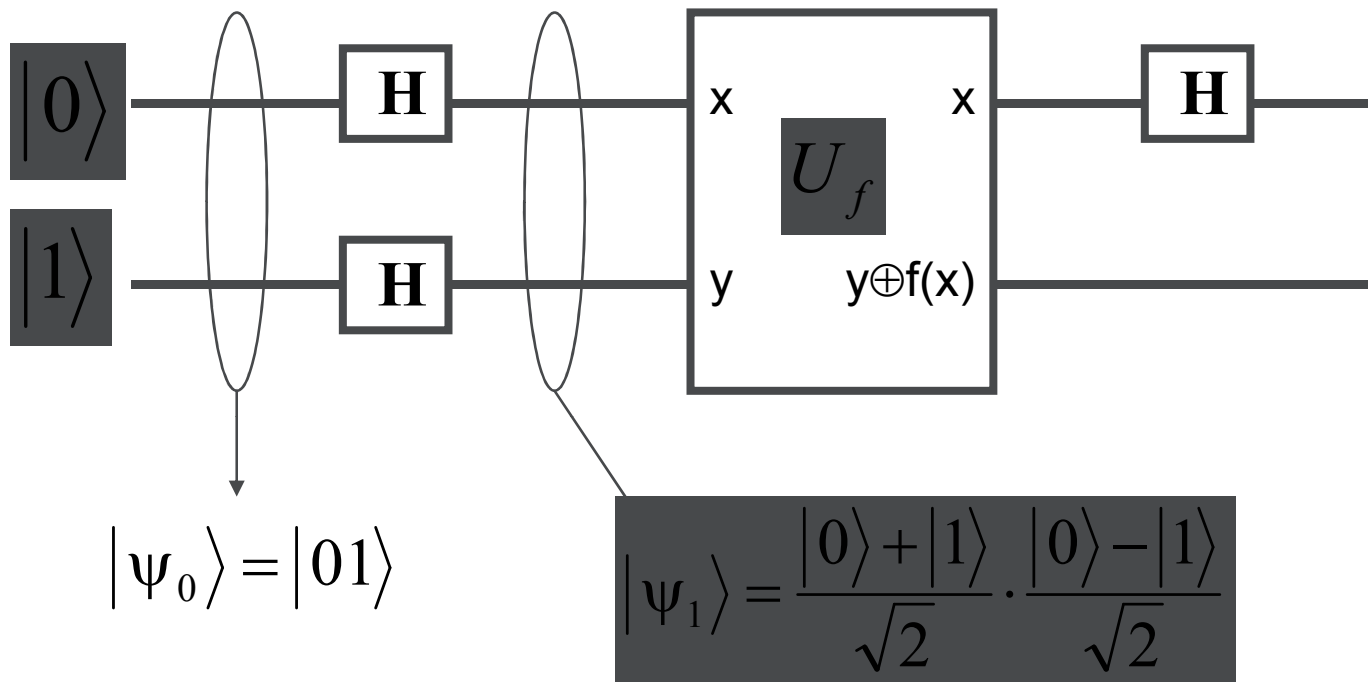
- ◆ David Deutsch: British physicist
- ◆ Deutsch's algorithm allows us to compute, in only one step, the value of

$$f(0) \oplus f(1)$$

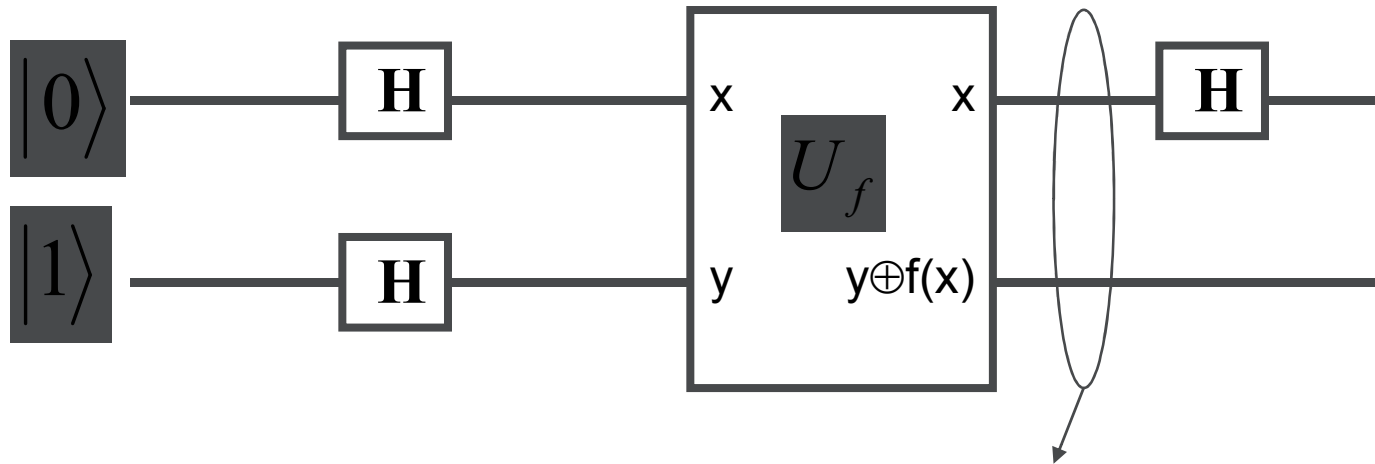
- ◆ To do this classically, you would have to:
 1. compute $f(0)$
 2. compute $f(1)$
 3. add the two results
- Remember:

$$f : \{0,1\} \mapsto \{0,1\}$$

Circuit for Deutsch's Algorithm

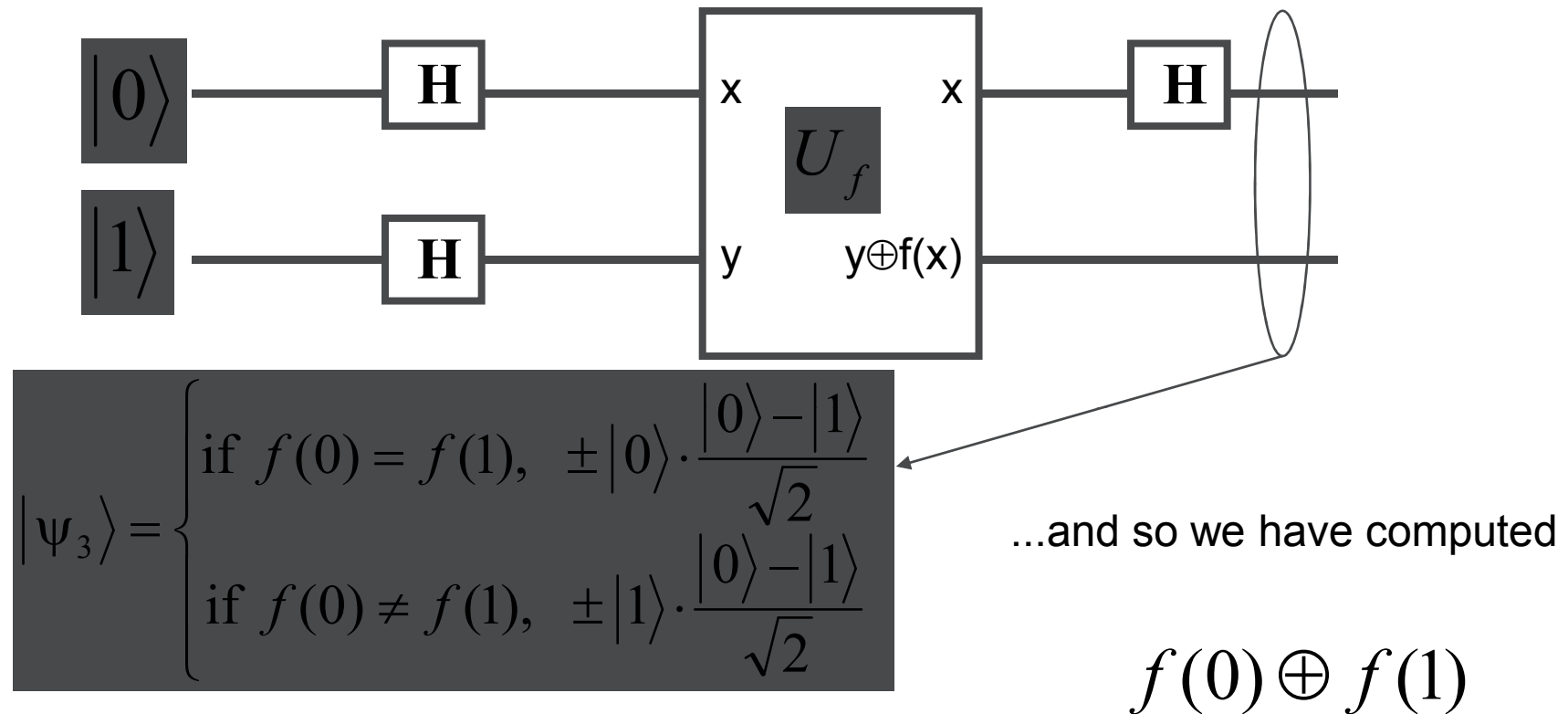


Circuit for Deutsch's Algorithm (2)



$$|\psi_2\rangle = \begin{cases} \text{if } f(0) = f(1), & \pm \frac{|0\rangle + |1\rangle}{\sqrt{2}} \cdot \frac{|0\rangle - |1\rangle}{\sqrt{2}} \\ \text{if } f(0) \neq f(1), & \pm \frac{|0\rangle - |1\rangle}{\sqrt{2}} \cdot \frac{|0\rangle - |1\rangle}{\sqrt{2}} \end{cases}$$

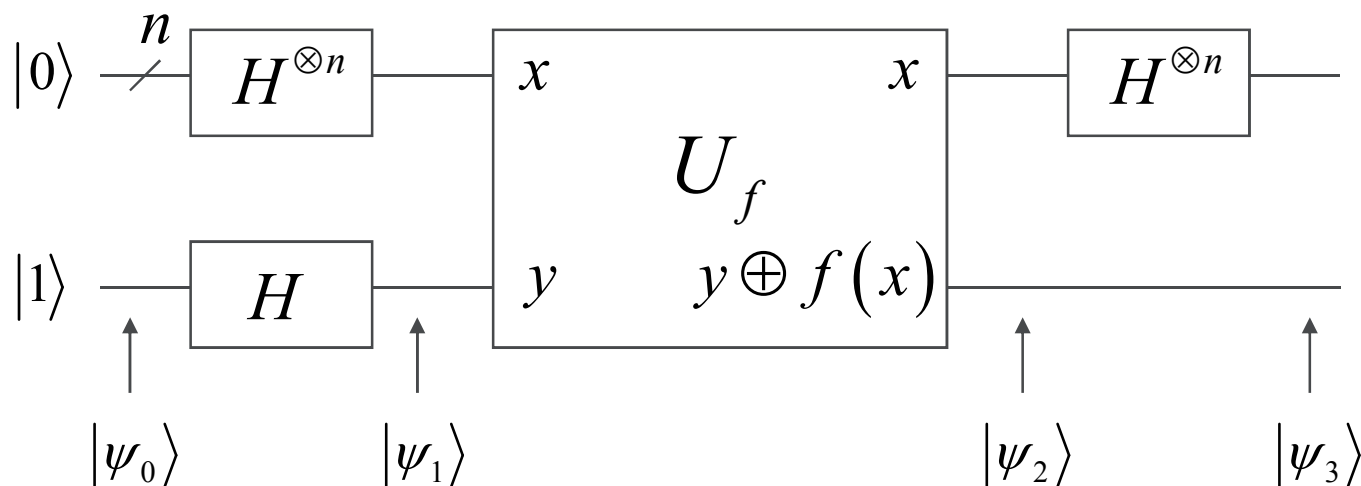
Circuit for Deutsch's Algorithm (3)



this simplifies to

$$|\psi_3\rangle = \pm |f(0) \oplus f(1)\rangle \cdot \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Deutsch-Jozsa算法



◆实现Deutsch-Jozsa算法的量子路线，类似于工程上通用的符号，带有斜杠 / 的线表示：通过此线的是一组量子比特。

$$|\psi_0\rangle = |0\rangle^{\otimes n} |1\rangle$$

$$|\psi_1\rangle = \sum_{x \in \{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$$

$$|\psi_2\rangle = \sum_x \frac{(-1)^{f(x)} |x\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$$

Deutsch-Jozsa 算法 (2)

$$H^{\otimes n} |x_1, \dots, x_n\rangle = \frac{\sum_{z_1, \dots, z_n} (-1)^{x_1 z_1 + \dots + x_n z_n} |z_1, \dots, z_n\rangle}{\sqrt{2^n}}$$

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

$$|\psi_3\rangle = \sum_z \sum_x \frac{(-1)^{x \cdot z + f(x)}}{2^n} |z\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$$

Deutsch-Jozsa算法 (3)

◆考虑对 x 的求和：

◆如果 $f(x)$ 是常数函数，则和为

$$(-1)^{f(x)} \left(\frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{x \cdot z} \right) = (-1)^{f(x)} \delta_{z,0}$$

◆这是因为 $z \neq 0$ 时， $(-1)^{x \cdot z}$ 有半数等于+1，半数等于-1，所以，测量这个 n 位寄存器，将以概率1得到 $z = 0$ 。

◆如果 $f(x)$ 是对称函数，对于 $z = 0$ 的态，有

$$\frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)} (-1)^{x \cdot z} = 0$$

这是因为函数 $(-1)^{f(x)}$ 对 $x = 0$ 到 $x = 2^n - 1$ 求和时，有一半为+1，一半为-1。所以 $f(x)$ 是对称函数时，测量这个 n 位寄存器，得到 $|z = 0\rangle$ 态的概率为零。

Deutsch-Jozsa算法总结

算法 Deutsch-Jozsa

输入 对 $x \in \{0, \dots, 2^n - 1\}$ 和 $f(x) \in \{0, 1\}$ 进行变换

$|x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$ 的黑箱 U_f , 已知 $f(x)$

对所有的 x 或者是常数 , 或者是平衡的

(即恰好对于所有可能的 x 的一半取1 , 另一半取0)

输出 当且仅当 f 是常数 , 输出为0。

运行时间 计算 U_f 一次 , 总是成功的。

Deutsch-Jozsa算法总结 (2)

过程

$$(1) |0\rangle^{\otimes n} |1\rangle$$

//状态初始化

$$(2) \rightarrow \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$$

//用Hadamard门
产生叠加

$$(3) \rightarrow \frac{1}{\sqrt{2^n}} \sum_x (-1)^{f(x)} |x\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$$

//用 U_f 计算函数 f

$$(4) \rightarrow \sum_z \sum_x \frac{(-1)^{x \cdot z + f(x)}}{2^n} |z\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$$

//进行Hadamard
变换

$$(5) \rightarrow z$$

//测量最终输出 z

◆ Bernstein-Vazirani问题

设 a 是一个 n 位串，假设量子黑箱可以计算函数

$$f_a : f_a(x) = a \cdot x \text{ 。 现在的问题是： } a = ?$$

经典算法确定 a ，必须运行黑箱 n 次，通过求解 n 元线性方程组得到 a 。 Bernstein-Vazirani设计的如下量子算法，只需要运行黑箱一次。

◆ 问题：如果只有经典黑箱（使用者不知 a ），能否构造量子黑箱？——考虑经典计算与量子计算的关系。

Bernstein-Vazirani算法 (2)

$$\begin{aligned} U_{f_a} &: \left[|x\rangle \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \right] \\ &= (-1)^{f_a(x)} |x\rangle \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \\ &= (-1)^{x \cdot a} |x\rangle \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \end{aligned}$$

$$\begin{aligned} U_{f_a} &\left[H^{(n+1)} |0\rangle^n |1\rangle \right] \\ &= \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} (-1)^{a \cdot x} |x\rangle \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \\ &\xrightarrow{\text{前 } n \text{ 位 } H^{(n)}} \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{a \cdot x} \sum_{y=0}^{2^n-1} (-1)^{x \cdot y} |y\rangle \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \end{aligned}$$

Bernstein-Vazirani算法 (3)

考虑对变量 x 的求和，由于

$$\frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{a \cdot x} (-1)^{x \cdot y} = \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{(a \oplus y) \cdot x} = \delta_{a,y}$$

即：

$$\begin{aligned} & \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{a \cdot x} \sum_{y=0}^{2^n-1} (-1)^{x \cdot y} |y\rangle \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \\ &= \sum_{y=0}^{2^n-1} \delta_{a,y} |y\rangle \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) = |a\rangle \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle), \end{aligned}$$

测量前 n 位寄存器将以概率1得到 a 。

◆ 设 f 为量子黑箱可计算函数，

$f: \{0,1\}^n \rightarrow \{0,1\}^m$ 是 $2 \rightarrow 1$ 的同态，

且对确定的 $a \in \{0,1\}^n$ ，有 $f(x \oplus a) = f(x)$ 。

经典方法求解 a ：最坏情形需要 $2^{n-1}+1$ 次运算。

利用量子黑箱可以通过 n 次运算求得 a 。

Simon算法 (2)

$$U_f \left[\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle |0\rangle \right] = \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle |f(x)\rangle$$

现在测量第二个寄存器，设结果为 $f(x_0)$,

由于仅 x_0 和 $x_0 + a$ 被映射为 $f(x_0)$,

所以知第一个寄存器的态为 $\frac{1}{\sqrt{2}}(|x_0\rangle + |x_0 \oplus a\rangle)$,

Simon算法 (3)

$$\begin{aligned} & H^{(n)} \frac{1}{\sqrt{2}} (|x_0\rangle + |x_0 \oplus a\rangle) \\ &= \frac{1}{2^{(n+1)/2}} \sum_{y=0}^{2^n-1} [(-1)^{x_0 \cdot y} + (-1)^{(x_0 \oplus a) \cdot y}] |y\rangle \\ &= \frac{1}{2^{(n-1)/2}} \sum_{y \cdot a = 0} (-1)^{x_0 \cdot y} |y\rangle \end{aligned}$$

测量第一个寄存器, 随机得到一个 $|y\rangle$, 满足 $a \cdot y = 0$

Simon算法 (4)

◆重复上面算法，可求得 n 个线性独立的 y 值，通过解方程组：

$$\begin{cases} y_1 \cdot a = 0, \\ y_2 \cdot a = 0, \\ \vdots \\ y_n \cdot a = 0. \end{cases}$$

可求得 a 。即使考虑到两次运行黑箱可能得到同一个 y 值，或者是与已得 y 值线性相关的值，重复运行黑箱的次数仍是 n 的多项式，可知量子算法获得了指数加速的效果。

量子信息与量子密码

[第4次课] 量子信息论与早期量子算

Q&A