

量子信息基础

第六章：量子计算

金潮渊

浙江大学信息与电子工程学院



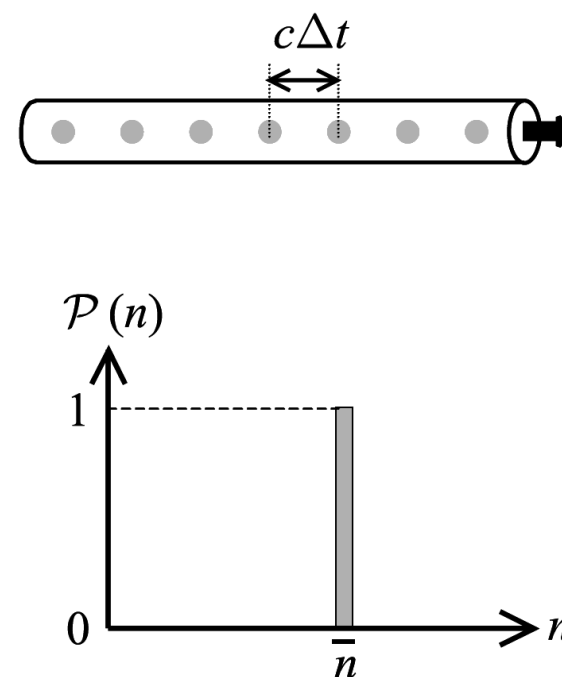
C6-1 量子比特和量子逻辑



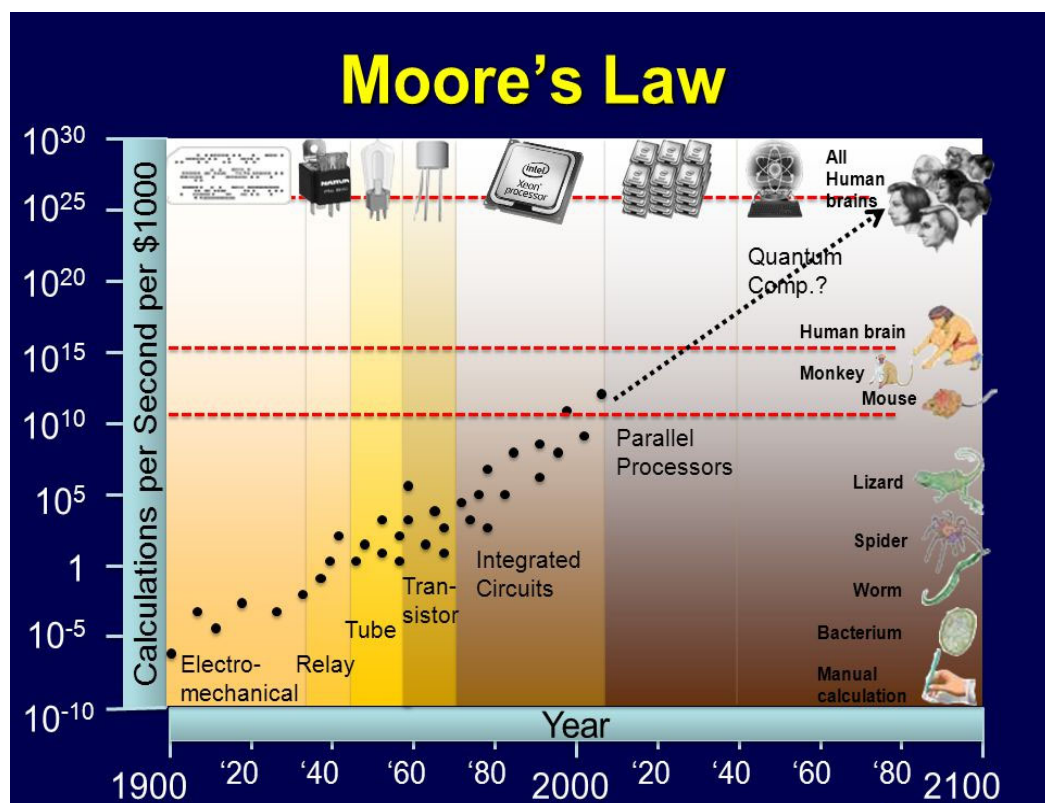
课程回顾

单光子源和量子中继：

- 由于光子的量子化特点，光子计数的波动范围遵循一定的统计规律。完美的相干光束遵循泊松光子统计；超泊松光源的典型代表是热光源；亚泊松光源的典型代表是单光子源。
- 量子中继通过在长距离通信链路中插入一系列中继节点，对量子信号进行放大和纠错，从而扩展量子通信的有效距离。量子通信网络的中继站分为量子中继和可信中继。
- 量子中继的关键技术包括：纠缠交换、纠缠纯化、量子存储。

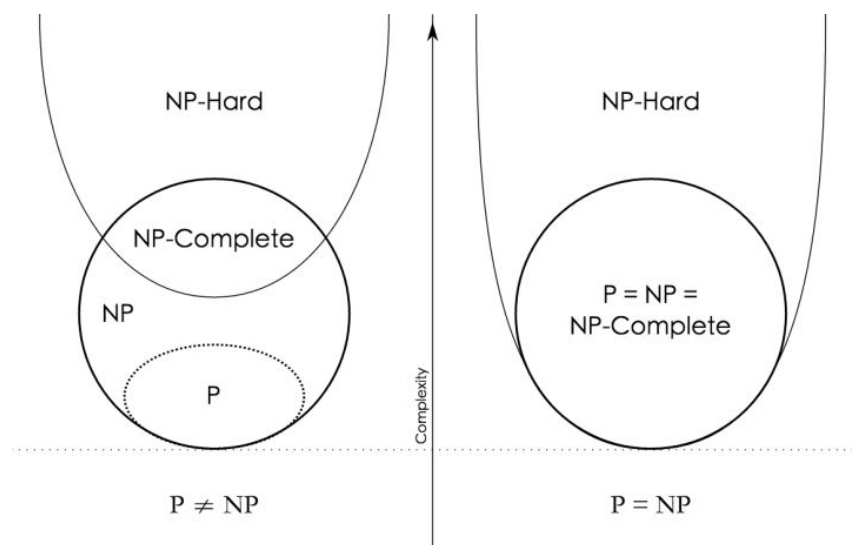


摩尔定律



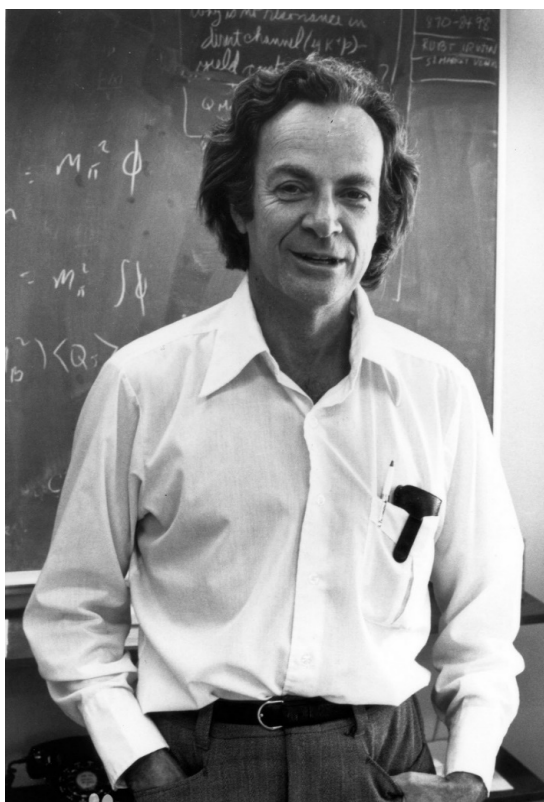
- 摩尔定律：集成电路上可容纳的晶体管数目，大约每隔两年便会增加一倍。由英特尔（Intel）创始人之一戈登·摩尔提出。
- 摩尔定律并非数学/物理定律，而是对发展趋势的一种分析预测。“摩尔定律”对整个世界意义深远。半导体芯片的集成化趋势，推动了整个信息技术产业的发展，进而给千家万户的生活带来变化。
- 摩尔定律走向终结：（1）器件尺寸的缩小带来了复杂的量子效应；（2）单个原子是器件可能的最小尺寸；（3）生产成本随着线宽走向极致而大幅度增加。

P=NP难题



- P问题：问题可以在多项式的时间复杂度内解决。例如：n个数的排序。
- NP问题：一个问题的解可以在多项式的时间被证实或证伪。例如：典型的子集求和问题，给定一个整数集合求是否存在一个非空子集它的和为零。如给定集合 $s=\{-1,3,2,-5,6\}$ ，很明显子集 $\{3,2,-5\}$ 能满足问题，并且验证该解只需要线性时间复杂度就能被证实。
- NP-complete问题：所有的NP问题都可以约化为的问题。
- NP-hard问题：那些至少和NP一样难的问题。
- NP问题求解的时间复杂度指数上升，导致传统计算方式在NP问题求解上失效。

量子计算机



- 理查德·费曼在1982年提出了量子计算机的概念。他提到，既然量子系统的计算随着系统复杂度的上升而变得难以进行，那我们何不利用量子规则来计算量子系统的演化。
- 1985年，牛津大学的David Deutsch提出量子图灵机（quantum Turing machine）的概念，也称为通用量子计算。量子计算才开始具备了数学的基本型式。
- 1994年，贝尔实验室的应用数学家Peter Shor提出，利用量子计算可以在短时间内将一个很大的整数分解成质因子的乘积。这个结论开启实用性量子算法的新阶段。
- 2011年，加拿大量子计算公司D-Wave正式发布了全球第一款商用型量子计算机“D-Wave One”。2019年底，谷歌发布了53个超导量子比特的量子计算机“Sycamore”，宣称实现了“量子霸权”。
- 2020年12月，中国科学技术大学发布了光量子计算原型机“九章”，成功演示了76个光子输出的玻色采样，宣称实现了“量子优越性”。这三款量子计算机不是真正意义上的通用量子计算机。



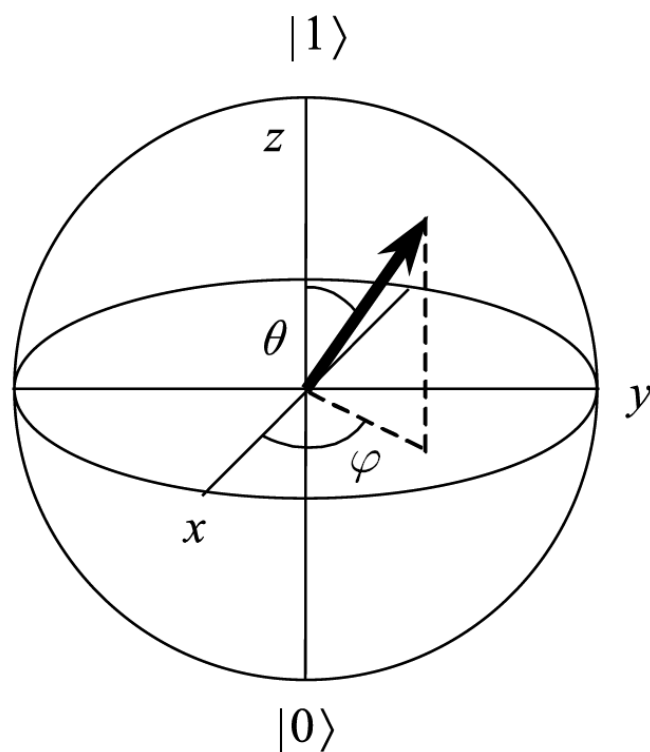
量子比特

- 传统计算机的信息处理依赖于比特（1或者0），是信息量的最小单位。相对应地，量子计算机的逻辑运算依赖于量子比特（quantum bits, qubits）。
- 量子比特不是1或者0，而是1态和0态的量子叠加 $|\psi\rangle = c_0|0\rangle + c_1|1\rangle$ ，其中 $|c_0|^2 + |c_1|^2 = 1$ 。一般情形下，我们要求 $\langle 0|1\rangle = 0$ 。
- 常见的量子比特有光子偏振、电子自旋、二能级原子、核自旋、约瑟夫森结、超导线圈等等。

Quantum system	Physical property	$ 0\rangle$	$ 1\rangle$
Photon	Linear polarization	Horizontal	Vertical
Photon	Circular polarization	Left	Right
Nucleus	Spin	Up	Down
Electron	Spin	Up	Down
Two-level atom	Excitation state	Ground state	Excited state
Josephson junction	Electric charge	N Cooper pairs	$N + 1$ Cooper pairs
Superconducting loop	Magnetic flux	Up	Down



布洛赫球



- 量子比特也可以通过所谓的布洛赫矢量来表示，即对于 $|\psi\rangle = c_0|0\rangle + c_1|1\rangle$ ，相应的布洛赫矢量系数为

$$c_0 = \sin(\theta/2)$$
$$c_1 = e^{i\varphi} \cos(\theta/2)$$

- 不难验证上式中的 φ 和 θ 对应于极坐标系中的方位角和天顶角。 $\theta = 0$ 和 $\theta = \pi$ 分别代表布洛赫球面上的北极点和南极点，即 $|1\rangle$ 和 $|0\rangle$ 。
- 布洛赫球面上的同一直径的两个端点所代表的态，在希尔伯特空间内正交。

量子寄存器

- N 个量子比特的集合被称作尺度为 N 的量子寄存器（quantum register）。
- 如果我们写下两个量子比特的量子寄存器。体系波函数是四种波函数可能组合的态。

$$|\psi\rangle = c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle$$

对于三个量子比特的量子寄存器，容易得到

$$|\psi\rangle = c_{000}|000\rangle + c_{001}|001\rangle + c_{010}|010\rangle + c_{011}|011\rangle + c_{100}|100\rangle + c_{101}|101\rangle + c_{110}|110\rangle + c_{111}|111\rangle$$

- 对于 N 个量子比特的量子寄存器，就存在 2^N 个0到1之间的线性叠加系数。可见随着量子比特数的增加，量子信息呈指数增长。
- 但是，每次测量之后量子寄存器都会丢失掉大部分信息。所以量子计算过程必须保证其相干性，独立于外界环境进行演化，这种演化代表了一种极高平行度的计算过程。



矩阵表示

- 量子比特也可以用矩阵的形式来表示

$$|\psi\rangle = \begin{pmatrix} c_0 \\ c_1 \end{pmatrix} \xrightarrow{\text{on the basis of}} \begin{matrix} |0\rangle \\ |1\rangle \end{matrix}$$

- 同理对于2个量子比特的量子寄存器，可以写作

$$|\psi\rangle = \begin{pmatrix} c_{00} \\ c_{01} \\ c_{10} \\ c_{11} \end{pmatrix} \xrightarrow{\text{on the basis of}} \begin{matrix} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{matrix}$$

逻辑门

- 经典计算机使用二进制逻辑门来进行信息的处理。包括非门、与门、或门、与非门、或非门等。其中包括单逻辑门和双逻辑门。

非门

\bar{A}

Input bit		Output bit
0		1
1		0

与门

$A \cdot B$

Input bits		Output bit
0	0	0
1	0	0
0	1	0
1	1	1

与非门

$\overline{A \cdot B}$

Input bits		Output bit
0	0	1
1	0	1
0	1	1
1	1	0

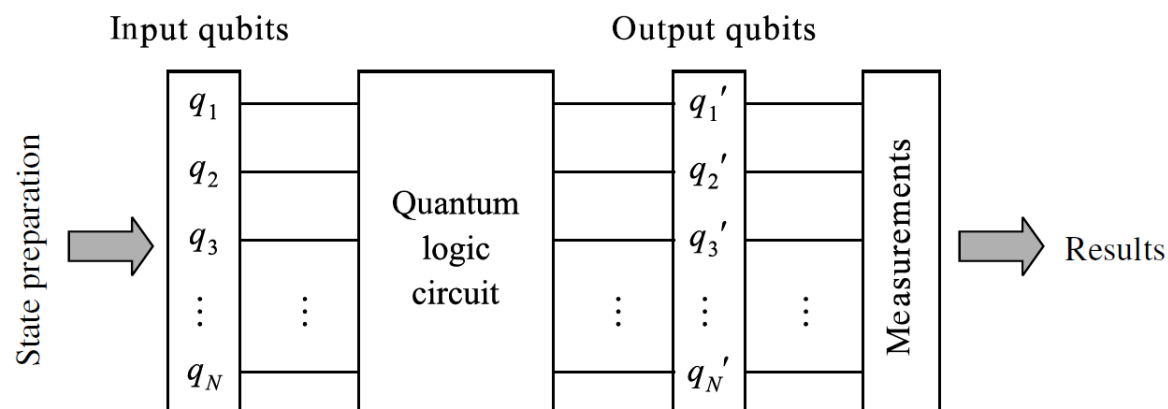
异或门

$A \oplus B$

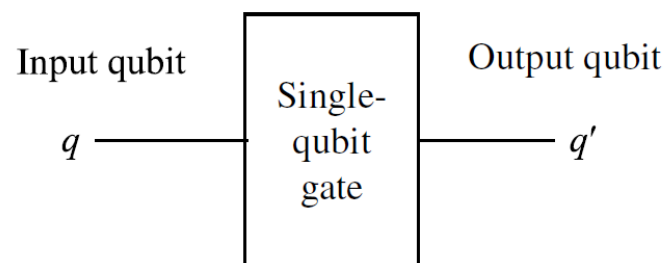
Input bits		Output bit
0	0	0
1	0	1
0	1	1
1	1	0

量子回路

- 量子计算机使用量子逻辑门（quantum logic gate）所组成的量子回路（quantum circuit）。量子计算的核心是量子回路和量子测量。
- 从 N 个量子比特组成的量子寄存器开始 $\{q_1, q_2, q_3, \dots, q_N\}$ ，经过量子逻辑回路的处理，得到一组新的量子寄存器 $\{q'_1, q'_2, q'_3, \dots, q'_N\}$ 。对最终量子寄存器的测量返回 N 个经典的比特。
- 在计算过程中，共有 2^N 个参数参与运算，但输入和输出是 N 个量子比特和 N 个经典比特。
- 和经典计算类似，通用量子逻辑回路中大量使用单量子比特门和双量子比特门。



单量子比特门



Quantum gate	Matrix representation
NOT (X)	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
Z	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
Hadamard (H)	$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

- 单量子比特门是输入一个量子比特 q 输出另一个量子比特 q' 的逻辑器件。可以把输入输出的波函数分别写作

$$|\psi\rangle = c_0|0\rangle + c_1|1\rangle \quad |\psi'\rangle = c'_0|0\rangle + c'_1|1\rangle$$

- 数学上可以使用 2×2 的运算矩阵 M 来表示这个过程，满足 $MM^\dagger = I$ ，所以 M 是么正矩阵。

$$\begin{pmatrix} c'_0 \\ c'_1 \end{pmatrix} = \begin{pmatrix} M_{11} & M_{12} \\ M_{21} & M_{22} \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \end{pmatrix}$$


- 三种最为常见逻辑门分别是 X 门、 Z 门和 H 门

$$X \cdot q = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \end{pmatrix} = \begin{pmatrix} c_1 \\ c_0 \end{pmatrix} \quad Z \cdot q = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \end{pmatrix} = \begin{pmatrix} c_0 \\ -c_1 \end{pmatrix}$$

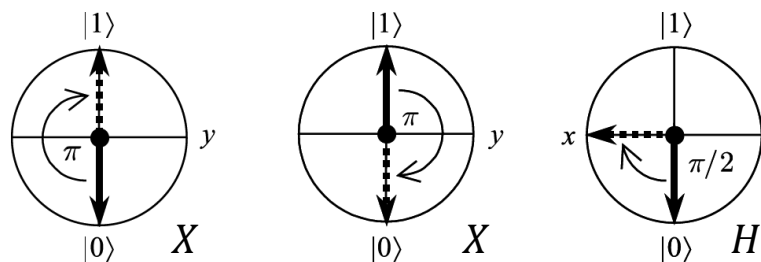
$$H \cdot q = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \end{pmatrix} = \begin{pmatrix} (c_0 + c_1)/\sqrt{2} \\ (c_0 - c_1)/\sqrt{2} \end{pmatrix}$$

单量子比特门的几何解释

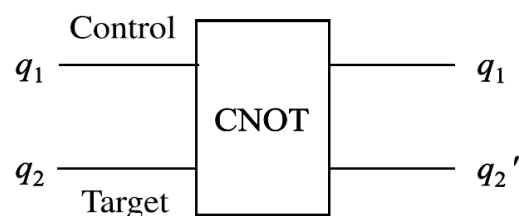
- 量子比特可以看作是布洛赫球上的布洛赫矢量，所以量子比特门也可以看作是布洛赫矢量在布洛赫球上的旋转操作。 X 门对应于相对于 x 轴旋转180度的操作。

$ 0\rangle \xrightarrow{X} 1\rangle$	<div style="text-align: center;"> 对应于布洛赫球上的变换  </div>	$(0,0,-1) \xrightarrow{X} (0,0,1)$
$ 1\rangle \xrightarrow{X} 0\rangle$		$(0,0,1) \xrightarrow{X} (0,0,-1)$
$(1/\sqrt{2})(0\rangle + 1\rangle) \xrightarrow{X} (1/\sqrt{2})(0\rangle + 1\rangle)$		$(1,0,0) \xrightarrow{X} (1,0,0)$
$(1/\sqrt{2})(0\rangle + i 1\rangle) \xrightarrow{X} (1/\sqrt{2})(i 0\rangle + 1\rangle)$		$(0,1,0) \xrightarrow{X} (0,-1,0)$

- Z 门对应于相对于 z 轴旋转180度的操作； H 门对应于相对于 z 轴旋转90度的操作。

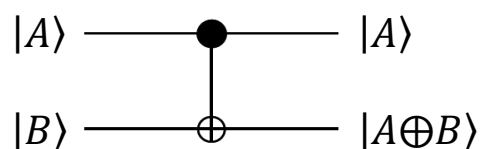


双量子比特门



- 任何量子逻辑都可以通过单量子比特门的组合来实现。一种典型的双量子比特门是所谓的CNOT门（可控非门）。CNOT门是可控么正变换门（C-U门）的一种特例。

$$|00\rangle \rightarrow |00\rangle \quad |01\rangle \rightarrow |01\rangle \quad |10\rangle \rightarrow |11\rangle \quad |11\rangle \rightarrow |10\rangle$$

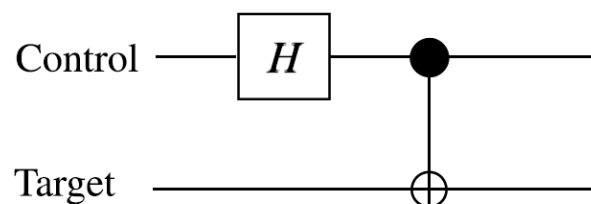


$$\hat{U}_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Input qubits		Output qubits	
Control	Target	Control	Target
$ 0\rangle$	$ 0\rangle$	$ 0\rangle$	$ 0\rangle$
$ 0\rangle$	$ 1\rangle$	$ 0\rangle$	$ 1\rangle$
$ 1\rangle$	$ 0\rangle$	$ 1\rangle$	$ 1\rangle$
$ 1\rangle$	$ 1\rangle$	$ 1\rangle$	$ 0\rangle$

$$\hat{U}_{CNOT} \cdot |\psi\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} c_{00} \\ c_{01} \\ c_{10} \\ c_{11} \end{pmatrix} = \begin{pmatrix} c_{00} \\ c_{01} \\ c_{11} \\ c_{10} \end{pmatrix}$$

量子逻辑



In	Out
$ 00\rangle$	$(00\rangle + 11\rangle)/\sqrt{2} \equiv \beta_{00}\rangle$
$ 01\rangle$	$(01\rangle + 10\rangle)/\sqrt{2} \equiv \beta_{01}\rangle$
$ 10\rangle$	$(00\rangle - 11\rangle)/\sqrt{2} \equiv \beta_{10}\rangle$
$ 11\rangle$	$(01\rangle - 10\rangle)/\sqrt{2} \equiv \beta_{11}\rangle$

- 让我们来看一个简单的量子逻辑的例子。一个 H 门和 CNOT 门的组合。
- 假设控制和目标量子比特都是 $|0\rangle$ ，控制比特经过 H 门后得到

$$H \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix}$$

- CNOT 门的输入波函数可以写作

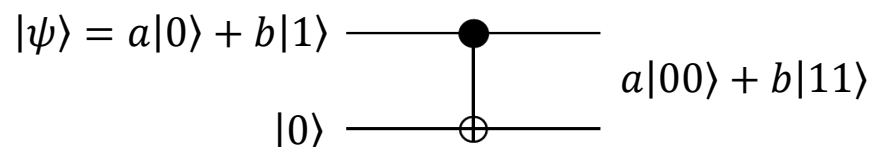
$$|\psi\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)|0\rangle = \frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |10\rangle$$

- 输出为

$$|\psi'\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \cdot \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

$$|\psi'\rangle = \frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle$$

克隆量子比特？



- 上面我们利用一个CNOT门，是否成功克隆了量子比特 $|\psi\rangle$ ？
- 答案是否定的。如果 $|\psi\rangle$ 处于本征态 $|0\rangle$ 或者 $|1\rangle$ ，CNOT门的确可以复制量子态。但是对于一个非平庸的线性叠加态 $|\psi\rangle$ 。克隆需要满足

$$|\psi\rangle|\psi\rangle = (a|0\rangle + b|1\rangle)(a|0\rangle + b|1\rangle) = a^2|00\rangle + ab|01\rangle + ab|10\rangle + b^2|11\rangle$$

参考文献

- 量子比特和量子逻辑主要参考：
 - Mark Fox, Quntum Optics – An Introduction, Oxford University Press (2006). 第13.1-13.3小节。
 - David A.B. Miller, Quantum Mechanics for Scientists and Engineers, Cambridge University Press (2008). 第18.4小节。
 - Michael A. Nielsen and Isaac L. Chuang, Quantum Computation and Quantum Information (10th anniversary edition), Cambridge University Press (2016). 第1.3小节。

