量子计算

杨易轩 罗昶恺 张质源

流程图

- 1.序论
- 2.量子门的物理基础
- 3.量子门电路
- 4.量子算法

简要历史

史蒂芬·魏施纳在1969年最早提出“基于量子力学的计算设备”，但早期多处于理论推导状态。1994年彼得·秀尔提出量子质因数分解算法后证明量子计算机能做出离散对数运算且速度远胜传统计算机。因为量子不像半导体只能记录0与1，可以同时表示多种状态，一次运算可以处理多种不同状况，因此，一个40位元的量子计算机，就能在很短时间内解开1024位元计算机花上数十年解决的问题。因其对于现在通行于银行及网络等处的RSA加密算法可以破解而构成威胁之后，量子计算机变成了热门的话题，除了理论之外，也有不少学者着力于利用各种量子系统来实现量子计算机。

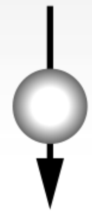
基本概念

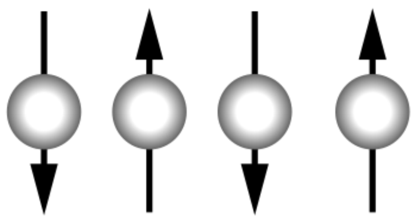
- 传统计算机即对输入信号序列按一定算法进行变换的机器，其算法由计算机的内部逻辑电路实现。
- 输入输出态都是传统信号，用量子力学的语言来描述，也即是：其输入态和输出态都是某一力学量的本征态。如输入二进制序列0110110，用量子记号，即|0110110>。所有输入态均相互正交，传统计算机不可能输入以下叠加态：$c_1|0110110\rangle+c_2|1001001\rangle$。
- 传统计算机内部的每一步变换都演化为正交态，而一般的量子变换没有这个性质，因此，传统计算机中的变换（或计算）只对应一类特殊集。

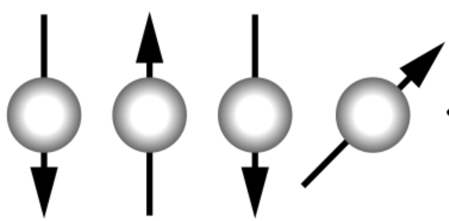
基本概念

- 量子计算机的输入用一个具有有限能级的量子系统来描述，如二能级系统（称为量子比特（qubits）），量子计算机的变换（即量子计算）包括所有可能的正变换。
- 量子计算机的输入态和输出态为一般的叠加态，其相互之间通常不正交；
- 量子计算机中的变换为所有可能的正变换。得出输出态之后，量子计算机对输出态进行一定的测量，给出计算结果。
- 量子计算对传统计算作了极大的扩充，最本质的特征为量子叠加性和量子相干性。量子计算机对每一个叠加分量实现的变换相当于一种经典计算，所有这些传统计算同时完成，并按一定的概率振幅叠加起来，给出量子计算机的输出结果。这种计算称为量子并行计算。

 $\Leftrightarrow |1\rangle$

 $\Leftrightarrow |0\rangle$

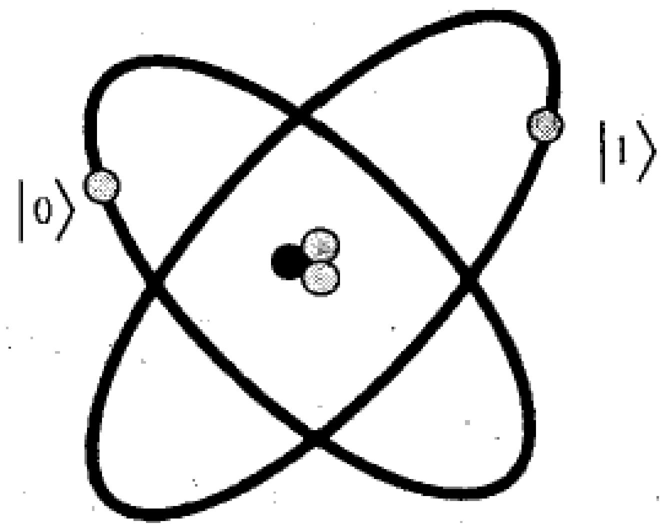
 $\Leftrightarrow |0101\rangle \Leftrightarrow |5\rangle$

 $\Leftrightarrow |4\rangle + |5\rangle$

量子信息

- 利用微观粒子的状态表示的信息就称为量子信息。量子信息学是指以量子力学基本原理为基础，通过量子系统相干特性（如量子并行、量子纠缠和量子不可克隆等），研究信息存储、编码、计算和传输等行为的理论体系。
- 量子信息的载体可以是任意两态的微观粒子系统。如光子的两个线偏振态或椭圆偏振态，恒定磁场中原子核的自旋，具有二能级的原子、分子或离子，围绕单一原子旋转的电子的两个状态。

量子信息



量子信息

- 量子态相干性：微观系统中量子间相互干涉的现象成为量子信息诸多不可思议特征的重要物理基础。

- 量子态纠缠性：N个量子在特定的（温度、磁场等）环境下可以处于稳定的量子纠缠状态，对其中某个子系统的局域操作会影响到其余子系统的状态。

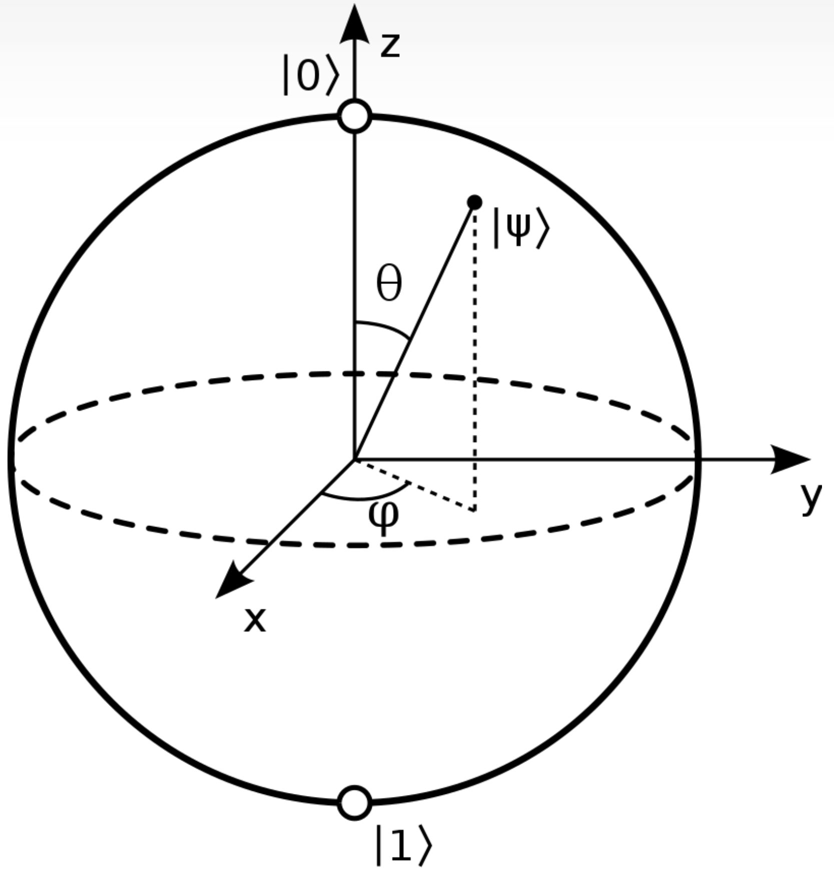
量子信息

- 量子态叠加性：量子状态可以叠加，因此量子信息也可以叠加，所以可以同时输入或操作N个量子比特的叠加态。
- 量子态不可克隆性：量子力学的线性特征确保对任意量子态无法实现精确的复制，量子不可克隆定理和测不准原理构成了量子密码技术的物理基础。
- 目前的量子信息主要是基于量子力学的相干特征，重构信息密码、信息计算和信息通信的基本原理。

量子信息

- 经典信息处理过程中，记录经典信息的二进制存储单元比特（bits）由经典状态1和0（如电压的高低）表示。从物理角度讲，比特是一个两态系统，它可以制备为两个可识别状态中的一个。
- 对于量子信息而言，记录量子信息的基本存储单元是量子比特（qubits）。一个量子比特的状态是一个二维复数空间的向量，两个极化状态对应于经典中的1和0.
- 量子比特的重要特性在于一个量子比特可以连续地、随机地存在于状态|0>和|1>的任意叠加状态上。

量子信息



量子态叠加与量子态纠缠

- 量子态的叠加源于微观粒子“波粒二象性”的波动“相干叠加性”（一个以上的信息状态累加在同一个微观粒子上的现象）；量子纠缠状态指的是两个或多个量子系统之间的非定域、非经典的关联，是量子系统内各子系统或各自由度之间关联的力学属性（一个以上的微观粒子因微观系统的特性相互交缠在一起的现象）。量子态可以叠加的物理特性是实现量子并行计算的基础，量子态能够纠缠是实现信息高速的不可破译通信的理论基础。它们都是量子信息理论中特有的概念。

量子态叠加与量子态纠缠

- 当量子态的叠加无法用各量子比特的张量积乘积表示时，这种叠加状态称为量子纠缠。
- 经典系统内的叠加反映在概率不相乘上，而量子态的叠加反映在概率幅不相乘上。
- 量子态叠加与并行处理。

量子计算

- 简单地说，量子计算就是利用量子态进行信息处理的方法，其实体设备称为量子计算机。量子计算机的基本原理是通过量子力学的运用，将微晶体管压缩到原子般大小，然后在极小的面积上放入数十亿颗量子微晶体管，进而利用量子态的叠加性和相干性进行信息运算、保存和处理。

PART ONE：物理实现

- 可能的实现方式：核磁共振，量子点，离子阱，半导体硅基，Josephson结，相移片......

- 以下的全部物理实现均以核磁共振为例

基本量子态

- 在弱静磁场下：

$$|1\rangle = |\downarrow\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$|0\rangle = |\uparrow\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

基本量子态

$\langle \varphi^* \vert \sigma_x \vert \varphi \rangle$	$\frac{1}{\sqrt{2}}(\vert 0\rangle \pm \vert 1\rangle)$
$\langle \varphi^* \vert \sigma_y \vert \varphi \rangle$	$\frac{1}{\sqrt{2}}(\vert 0\rangle \pm i\vert 1\rangle)$
$\langle \varphi^* \vert \sigma_z \vert \varphi \rangle$	$\vert 1\rangle / \vert 0\rangle$

- 操作示例：

$$U|1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}0\\ 1\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\ 1\end{bmatrix} = \frac{1}{\sqrt{2}}\left(|1\rangle + |0\rangle\right)$$

多qubit

$$|a_0\rangle\otimes|a_1\rangle\otimes|a_2\rangle\otimes|a_3\rangle\otimes\ldots\otimes|a_{n-1}\rangle=|a_0a_1\ldots a_{n-1}\rangle$$

- 置零态：

$$|0\rangle\rangle=|0\rangle\otimes|0\rangle\otimes\ldots\otimes|0\rangle$$

- 基准态：

$$U|0\rangle\rangle=\frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right)\otimes\frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right)\otimes\ldots\otimes\frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right)$$

$$=\frac{1}{\sqrt{2^n}}\left(|0\rangle\rangle+|1\rangle\rangle+\ldots+|n-1\rangle\rangle\right)=\frac{1}{\sqrt{2^n}}\sum_{q=0}^{n-1}|q\rangle\rangle$$

单qubit：U(a,φ)

$$|0\rangle \rightarrow \cos\alpha|0\rangle - ie^{i\varphi}|1\rangle$$

$$|1\rangle \rightarrow \cos\alpha|1\rangle - ie^{-i\varphi}|0\rangle$$

- 在X-Y平面加一个存在时间为τ的脉冲磁场

$$B = |B|(\cos\phi, \sin\phi, 0)$$

$$H\psi = i\hbar \frac{\partial \psi}{\partial t}$$

$$\psi = \exp(-\frac{iH}{\hbar}\tau)\psi_0 = \exp(-i\frac{\omega_L \tau}{2}\sigma \cdot e_B)\psi_0$$

- 数学小tips：

$$\exp(xA) = I + xA + \frac{1}{2!}(xA)^2 + \frac{1}{3!}(xA)^3 + \ldots$$

$$A = \sigma \cdot e_B = \sigma_x \cos\varphi + \sigma_y \sin\varphi$$

$$= \begin{bmatrix} 0 & \cos\varphi - i\sin\varphi \\ \cos\varphi + i\sin\varphi & 0 \end{bmatrix} = \begin{bmatrix} 0 & e^{-i\varphi} \\ e^{i\varphi} & 0 \end{bmatrix}$$

$$A^2 = I$$

$$\exp(-i\alpha\sigma\cdot e_B) = I\left[1+\frac{1}{2!}(-i\alpha)^2+\frac{1}{4!}(-i\alpha)^4+\ldots\right]$$

$$+\sigma\cdot e_B\left[(-i\alpha)+\frac{1}{3!}(-i\alpha)^3+\frac{1}{5!}(-i\alpha)^5+\ldots\right]$$

$$= I\cos\alpha - i\sin\alpha\begin{pmatrix} 0 & e^{-i\varphi} \\ e^{i\varphi} & 0 \end{pmatrix} = \begin{pmatrix} \cos\alpha & -i\sin\alpha e^{-i\varphi} \\ -i\sin\alpha e^{i\varphi} & \cos\alpha \end{pmatrix}$$

双qubit的量子态

$$|a\rangle \otimes |b\rangle$$

$$\frac{1}{\sqrt{2}}\left(|\uparrow\rangle + |\downarrow\rangle\right) \otimes |\uparrow\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

双qubit：CNOT

$$|00\rangle \rightarrow |00\rangle$$

$$|01\rangle \rightarrow |01\rangle$$

$$|11\rangle \rightarrow |10\rangle$$

$$|10\rangle \rightarrow |11\rangle$$

$$\hat{P}^0 = |0\rangle\langle 0| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$$\hat{P}^1 = |1\rangle\langle 1| = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$$U_{CN} = \hat{P}^0 \otimes \hat{1} + \hat{P}^1 \otimes \sigma_x = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

双qubit的物理实现

- 三氯甲烷：$CHCl_3$
- C，H各有一个自旋，二者自旋有耦合。
- Cl无自旋。

$$H_0=\frac{\omega_1}{2}z_1\otimes I_2+I_1\otimes\frac{\omega_2}{2}z_2+\frac{\pi J}{2}z_1\otimes z_2$$

$$=\frac{\omega_1}{2}Z_1+\frac{\omega_2}{2}Z_2+\frac{\pi J}{2}z_1\otimes z_2$$

$$\begin{pmatrix}
\frac{\omega_1}{2}+\frac{\omega_2}{2}+\frac{\pi J}{2} & 0 & 0 & 0 \\
0 & \frac{\omega_1}{2}-\frac{\omega_2}{2}-\frac{\pi J}{2} & 0 & 0 \\
0 & 0 & -\frac{\omega_1}{2}+\frac{\omega_2}{2}-\frac{\pi J}{2} & 0 \\
0 & 0 & 0 & -\frac{\omega_1}{2}-\frac{\omega_2}{2}+\frac{\pi J}{2}
\end{pmatrix}$$

$$H_{RF_i} = \frac{\Omega(t)}{2}\left(x_i \cos\left(\eta t + \phi(t)\right) + y_i \sin\left(\eta t + \phi(t)\right)\right)$$

$$H = H_0 + H_{RF_1} + H_{RF_2}$$

$$= \left(\frac{\Omega(t)}{2}\left(X_1 \cos\left(\eta t + \phi(t)\right) + Y_1 \sin\left(\eta t + \phi(t)\right)\right) + \frac{\omega_1}{2} Z_1\right)$$

$$+ \left(\frac{\Omega(t)}{2}\left(X_2 \cos\left(\eta t + \phi(t)\right) + Y_2 \sin\left(\eta t + \phi(t)\right)\right) + \frac{\omega_2}{2} Z_2\right)$$

$$+ \frac{\pi J}{2} z_1 \otimes z_2 = H_1 + H_2 + \frac{\pi J}{2} z_1 \otimes z_2$$

- 引入变换： $s=\exp\left(-i\frac{\eta t}{2}\sigma_z\right)$

$$i\hbar\frac{\partial\psi}{\partial t}=H\psi$$

$$\psi=S\tilde{\psi}$$

$$i\hbar\frac{\partial S\tilde{\psi}}{\partial t}=i\hbar S\frac{\partial\tilde{\psi}}{\partial t}+i\hbar\frac{\partial S}{\partial t}\tilde{\psi}=H\psi$$

$$S^{-1}\left(i\hbar S\frac{\partial\tilde{\psi}}{\partial t}+i\hbar\frac{\partial S}{\partial t}\tilde{\psi}\right)=S^{-1}H\psi=S^{-1}HS\tilde{\psi}$$

$$i\hbar\frac{\partial\tilde{\psi}}{\partial t}=\left(S^{-1}HS-i\hbar S^{-1}\frac{\partial S}{\partial t}\right)\tilde{\psi}$$

- 数学小tip：

$$\left(A\otimes B\right)\bullet\left(C\otimes D\right)=\left(A\bullet C\right)\otimes(B\bullet D)$$

$$S^{-1}HS=(s_1\otimes s_2)^{-1}H(s_1\otimes s_2)$$

$$=(s_1{}^{-1}\otimes s_2{}^{-1})(H_1+H_2+\frac{\pi J}{2}z_1\otimes z_2)(s_1\otimes s_2)$$

$$=(s_1{}^{-1}H_1s_1)\otimes(s_2{}^{-1}I_2s_2)+(s_1{}^{-1}I_1s_1)\otimes(s_2{}^{-1}H_2s_2)$$

$$+\frac{\pi J}{2}(s_1{}^{-1}z_1s_1)\otimes(s_2{}^{-1}z_2s_2)$$

$$=\tilde{H}_1+\tilde{H}_2+\frac{\pi J}{2}z_1\otimes z_2$$

$$H = -\mu \cdot B = \frac{1}{2}\hbar\omega_0\sigma_z + \frac{1}{2}\hbar\omega_1(\sigma_x \cos\eta t + \sigma_y \sin\eta t)$$

$$\tilde{H} = s^{-1}Hs = \frac{\hbar}{2}\begin{pmatrix} e^{\frac{i\eta t}{2}} & 0 \\ 0 & e^{-\frac{i\eta t}{2}} \end{pmatrix}\begin{pmatrix} \omega_0 & \omega_1 e^{-i\eta t} \\ \omega_1 e^{i\eta t} & -\omega_0 \end{pmatrix}\begin{pmatrix} e^{-\frac{i\eta t}{2}} & 0 \\ 0 & e^{\frac{i\eta t}{2}} \end{pmatrix}$$

$$= \frac{\hbar}{2}\begin{pmatrix} \omega_0 & \omega_1 \\ \omega_1 & -\omega_0 \end{pmatrix}$$

$$\frac{\partial s_j}{\partial t} = \frac{\partial \exp\left(-i\frac{\eta_j t}{2}\sigma_z\right)}{\partial t} = -i\frac{\eta_j}{2}\sigma_z s_i$$

$$S^{-1}\frac{\partial S}{\partial t} = \left(s_1^{-1} \otimes s_2^{-1}\right)\frac{\partial\left(s_1 \otimes s_2\right)}{\partial t}$$

$$= \left(s_1^{-1} \otimes s_2^{-1}\right)\left(\frac{\partial s_1}{\partial t} \otimes s_2 + s_1 \otimes \frac{\partial s_2}{\partial t}\right)$$

$$= -i\frac{\left(\eta_1 + \eta_2\right)}{2}\sigma_z\left(s_1^{-1} \otimes s_2^{-1}\right)\left(s_1 \otimes s_2\right) = -i\frac{\left(\eta_1 + \eta_2\right)}{2}\sigma_z$$

$$i\hbar\frac{\partial\tilde{\psi}}{\partial t}=\left(S^{-1}HS-i\hbar S^{-1}\frac{\partial S}{\partial t}\right)\tilde{\psi}$$

$$=\left(\tilde{H}_1+\tilde{H}_2+\frac{\pi J}{2}z_1\otimes z_2-\hbar\frac{(\eta_1+\eta_2)}{2}\sigma_z\right)\tilde{\psi}=\hat{H}\tilde{\psi}$$

其中每一项都不显含时间

$$\tilde{\psi}=\exp\left(-i\frac{\hat{H}t}{\hbar}\right)\psi_0$$

$$\psi=S\tilde{\psi}$$

$$ZZ90 = \exp(-\frac{\pi}{4} i z_1 \otimes z_2)$$

$$U_{Cphase} = Z_1(-90) \cdot Z_2(90) \cdot ZZ90 =$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & i & 0 \\ 0 & 0 & 0 & i \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -i & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -i \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & i & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$U_{CN} = Y_2(90) U_{Cphase} Y_2(-90)$$

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

$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

summary

- 如何用NMR方法做出
- U(α,φ)
- 相移门
- CNOT门

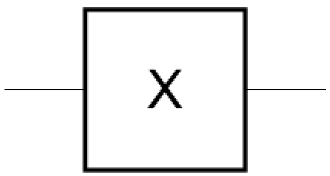
PART TWO：量子门电路

我们有什么？

- 单比特量子门：$\begin{cases} U(\alpha,\emptyset)门 \quad \begin{bmatrix} cos\alpha & -isin\alpha e^{-i\emptyset} \\ -isin\alpha e^{i\emptyset} & cos\alpha \end{bmatrix} \\ 相位偏移门 \quad \begin{bmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{bmatrix} （或：\begin{bmatrix} e^{-i\emptyset} & 0 \\ 0 & e^{i\emptyset} \end{bmatrix}） \end{cases}$

- 双比特量子门——$CNOT$门：$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$

基本量子门示意图



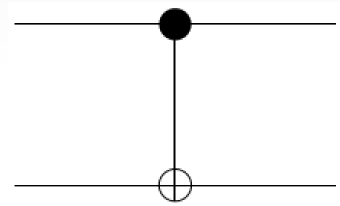
X可以是对单个比特进行操作的任意幺正矩阵（在不计入相位差的前提下）

例如——

X门：$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$　　H门：$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$

相位门：$\begin{bmatrix} e^{-i\emptyset} & 0 \\ 0 & e^{i\emptyset} \end{bmatrix}$

$U(\alpha,\emptyset)$门：$\begin{bmatrix} cos\alpha & -isin\alpha e^{-i\emptyset} \\ -isin\alpha e^{i\emptyset} & cos\alpha \end{bmatrix}$



两比特$CNOT$门，对应幺正矩阵为：

$$\hat{P}^0 \otimes I + \hat{P}^1 \otimes \sigma_x = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

计算机伪代码直观地表示为：

$$qubit_A = (qubit_B ?\, \sigma_x : I) * qubit_A$$

我们想要什么？
——N个量子位的任意幺正演化！

- N个量子位的所有可能状态对应2^N维空间，因而上述要求本质上在于利用量子逻辑门生成任意的2^N维幺正矩阵
- 波函数**整体**乘上任意的相位因子$e^{i\alpha}$不影响系统的演化，同时不造成任何可观测的效应，因而可以忽略
- 由于我们是最初涉猎量子计算，我们重点关注理论上的可行性，而不去考虑计算复杂度和实验噪声干扰

引理1

- 任意d维幺正变换都可以分解为一些（不超过$d(2d-1)$，实际上可以更少）2维幺正变换的乘积，而且这些幺正变换作用在同一组基底任意两个基矢张成的子空间

- 由此，我们可以把开头提到的任务转化为

i）生成任意具有上述性质的2维幺正矩阵

ii）加以组合得到任意2^N维幺正矩阵

引理2

- 利用单比特量子门和双比特量子门可以实现作用在任意两个基矢上的二维幺正变换

- 显然，若这两个基矢只有一个量子位存在差异则可以很容易地实现。例如$|0100110\rangle$和$|0110110\rangle$，只需对第3个量子位使用单比特门$U(\alpha, \emptyset)$和相位门即可实现所需的幺正变换

- 下面我们将要展示如何对存在多个量子位差异的两个基矢完成二维幺正变换

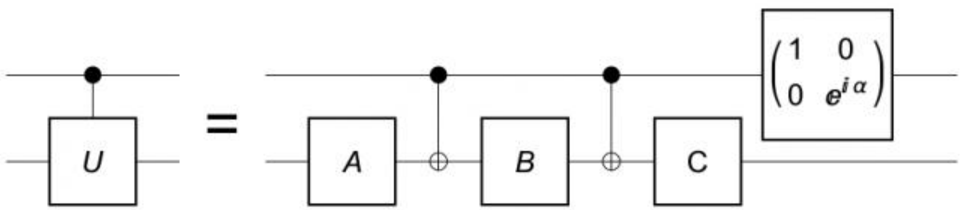
控制U门

——1量子位控制1量子位

- 为了实现任意的二维幺正变换，我们要做一些准备工作——先引入控制U门的概念，其对应的幺正变换如下：

$$I_1 \otimes P_1 + U \otimes P_2$$

- 也可以用伪代码表示为：$qubit_A = (qubit_B ? U : I) * qubit_A$

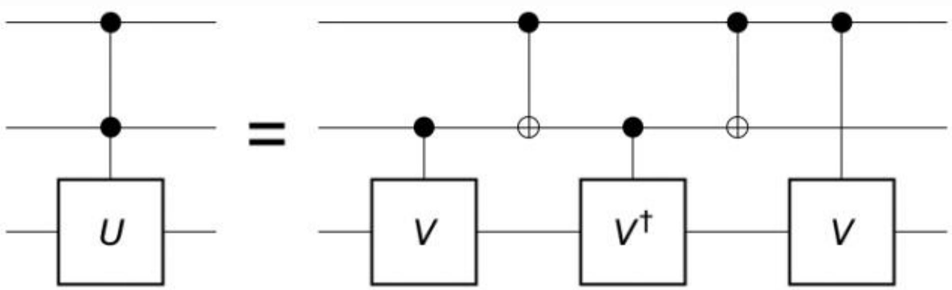


其中：$e^{i\alpha} = det(U)$，$U = e^{i\alpha} A\sigma_x B\sigma_x C$，$ABC = I$

A、B、C都是幺正矩阵，其存在性可由幺正矩阵的性质得到证明

$Toffoli$门

——2量子位控制1量子位



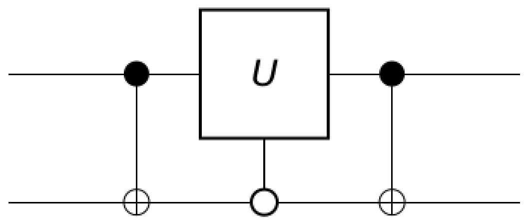
伪代码如下：$qubit_A = (qubit_B \&\& qubit_C ? U : I) * qubit_A$
矩阵表示为：$P_2 \otimes P_2 \otimes U + (I_2 \otimes I_2 - P_2 \otimes P_2) \otimes I_3$

$Toffoli$门由两个$CNOT$门和三个控制U门组成
由图中信息不难看出，若满足$V^2 = U$，则可实现伪代码

n量子位控制1量子位可以由此递归实现！！

两个量子位不同的情形

回到正题，我们要对$|00\cdots\rangle$和$|11\cdots\rangle$两个基矢张成的子空间进行幺正变换，该怎么办呢？？？量子电路如下：



$$\begin{array}{c} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{array} \xRightarrow{CNOT} \begin{array}{c} |\mathbf{00}\rangle \\ |01\rangle \\ |11\rangle \\ |\mathbf{10}\rangle \end{array} \xRightarrow[\text{和}|10\rangle\text{张成的子空间）}]{\text{控制}U\text{门（作用在}|00\rangle} \begin{array}{c} \boldsymbol{\alpha}|\mathbf{00}\rangle + \boldsymbol{\beta}|\mathbf{10}\rangle \\ |01\rangle \\ |11\rangle \\ \boldsymbol{\gamma}|\mathbf{10}\rangle + \boldsymbol{\delta}|\mathbf{00}\rangle \end{array} \xRightarrow{CNOT} \begin{array}{c} \boldsymbol{\alpha}|\mathbf{00}\rangle + \boldsymbol{\beta}|\mathbf{11}\rangle \\ |01\rangle \\ |10\rangle \\ \boldsymbol{\gamma}|\mathbf{11}\rangle + \boldsymbol{\delta}|\mathbf{00}\rangle \end{array}$$

多个量子位不同的情形

- 怎么办?
- 使用递归的办法!

  (以$|000\cdots\rangle$和$|111\cdots\rangle$为例，示意图见黑板)

- 综上，我们成功实现了在同一组基底任意两个基矢张成的子空间上的幺正变换，结合引理1（**任意d维幺正变换都可以分解为一些2维幺正变换的乘积，而且这些幺正变换作用在同一组基底任意两个基矢张成的子空间**），我们可以利用基本量子逻辑门实现对N个量子位的任意幺正演化!

Part2小结

- 尽管我们确实可以理论上利用基本量子门完成任意幺正演化，但这远远不是终点。因为 N 个量子位的所有可能状态对应 2^N 维空间，我们需要的基本逻辑门数量在2^{2N}量级，这样的复杂度显然是不可接受的，因而必须针对特定需求开发特定的电路构造

- 逻辑门起到了非常重要的承前启后的作用，它既是对量子计算机物理实现的抽象，又是进一步开发量子算法的基础
- 刚刚提到的逻辑门属于理想模型，但这也是不够的，量子计算机实际工作中必须考虑各种噪声的影响，具备纠错功能

量子算法

- NP问题
- 离散傅里叶变换（DFT）
- 大整数素数分解：Shor算法

量子纠错编码

- 经典代数纠错码
- 量子纠错编码的基本概念