

第十章 量子门与简单量子网络

前言——作为信息载体的量子态

一个纯量子态中各叠加成分的系数模值、内部相因子和纠缠模式都可以荷载人们设定的信息。不少混态也可以用来作为信息的载体。于是，对量子态的制备、操控、存储和传送，就开辟了量子信息论这一新领域。

量子信息论中用到量子系统许多特殊的不同于宏观系统的性质。它们包括：叠加性质——作为量子计算机细胞的量子位可以处于经典布尔态的任意复系数的线性组合态上

$$\alpha|true\rangle + \beta|false\rangle \quad (10.1)$$

并且，此叠加态的两个组分都能按同一个么正变换进行演化，这就形成了并行的计算路径；相干性质——这种叠加是相干叠加；塌缩性质——如果对这一叠加态进行测量，将出现向两个组分之一塌缩，这类塌缩是概率的、非定域的、不可逆的、切断相干性的；不可克隆性质——未知的量子信息态不可能以 100%成功的概率被精确克隆，并且观测时必定引入扰动；纠缠性质——例如，当整个存贮器处于一个确定的量子态时，其中某些量子位可以各自都不处于确定的量子态上。其中有些性质前面已叙述过，有些下面将阐述。

§10.1 量子逻辑门的构成与运行

1, 量子态的存贮——量子位与量子存贮器

i, 量子位(*quantum bit=qubit*)的实现和转动

【*bit*——*qubit* 对比】

	<i>Bit</i>	<i>Qubit</i>
构成	双稳态电子线路	光子极化状态、电子（或原子核）自旋状态
I 可取的状态	$ 0\rangle$ or $ 1\rangle$	$ 0\rangle, 1\rangle$ and $C_1 0\rangle + C_2 1\rangle$
测量影响	不受测量（读出）影响	叠加态将受测量（读出）影响

【*qubit* 物理实现举例】

【例 1】*qubit*=静磁场 ($-B_0\vec{e}_z$) 下原子核磁矩状态。调控手段则

是 x - y 平面内射频磁场脉冲 $\vec{B}(t)$ 。这里有两个磁场：弱静磁场用于定义两个布尔态，它所产生的演化称自由演化；射频磁场脉冲则是调控状态的手段。

【定义 1】鉴于 $H = -\vec{\mu} \cdot \vec{B}_0$ ，核磁矩顺静磁场取向状态为 $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ ，逆静磁场取向状态为 $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ 。注意，由于定义不同，各书的二维矩阵表示可能有所不同。

【定义 2】平均自旋矢量——极化矢量 $\vec{P} = \langle \varphi | \vec{\sigma} | \varphi \rangle$ 。它在外磁场中的进动运动符合经典图象。 $\vec{\sigma}$ 的本征态及相应 $\vec{P}$ 为

$$\begin{cases} \frac{1}{\sqrt{2}}(|1\rangle \pm |0\rangle), & \vec{P} = (\pm 1, 0, 0) \\ \frac{1}{\sqrt{2}}(|1\rangle \pm i|0\rangle), & \vec{P} = (0, \pm 1, 0) \\ |0\rangle, |1\rangle, & \vec{P} = (0, 0, \pm 1) \end{cases} \quad (10.2)$$

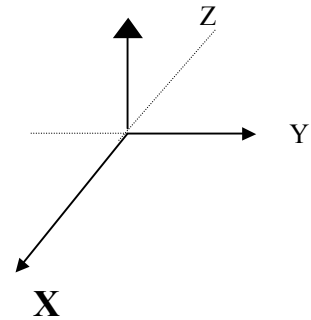
常常对单个 *qubit* 进行各种转动操作。这类转动操作的物理基础也各不相同。其中比如，自旋（磁矩）在外磁场中的进动。

转动操作举例：设转动前自旋状态为 $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ ，经受转动

$$R\left(\frac{\pi}{2} \vec{e}_y\right) = \exp\{-i(\pi/4)\sigma_y\} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \quad (10.3)$$

$$\begin{aligned} \therefore |\varphi\rangle_{\text{after Rotation}} &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \end{aligned} \quad (10.4)$$

成为叠加态，它在进行自旋分量测量时，将以相等的概率随机塌缩到 $|0\rangle$ or $|1\rangle$ 。



ii, 量子存储器及其置零态与初始态

设有 L 个 *qubit*, 组成一个量子存储器。于是, 一个数的二进制表示为

$$\begin{aligned} |a_0\rangle \otimes |a_1\rangle \otimes \cdots \otimes |a_{L-1}\rangle &= |a_0, a_1, \dots, a_{L-1}\rangle \\ (a_i &= 0, 1; \quad i = 0, 1, \dots, L-1) \end{aligned} \quad (10.5a)$$

若以十进制数表示, 这个态可记为:

$$|a\rangle \left(a = \sum_{i=0}^{L-1} a_i 2^i \right) \quad (10.5b)$$

“置零态”为

$$|0\rangle = |0\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle \quad (10.5c)$$

现对存储器(L 个 *qubit*)实行如下的旋转操作:

$$\begin{aligned} |0\rangle &\xrightarrow{R\left(\frac{\pi}{2}\vec{e}_y\right)} |0\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle \Rightarrow \\ &\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \cdots \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \\ &= \frac{1}{\sqrt{q}}\{|0\rangle + |1\rangle + |2\rangle + \cdots + |q-1\rangle\} = \frac{1}{\sqrt{q}} \sum_{n=0}^{q-1} |n\rangle, \quad (q = 2^L) \\ |initial\rangle &= \frac{1}{\sqrt{q}} \sum_{n=0}^{q-1} |n\rangle = \frac{1}{\sqrt{q}}\{|0\rangle + |1\rangle + |2\rangle + \cdots + |q-1\rangle\} \end{aligned} \quad (10.6)$$

这就是开始运算时存贮器的“初始状态”或“基准状态”。

这里预先指出, 此处 (10.6) 式已清楚地表明了量子计算的高度并行性。设有一个需要做的算法 f , 它对应到量子逻辑网络上, 翻译成对量子逻辑门的一系列么正变换的乘积, 最后总并为一个么正变换 $U(f)$ 。于是有

$$\begin{aligned} U(f)|initial\rangle &= U(f) \frac{1}{\sqrt{q}} \sum_{n=0}^{q-1} |n\rangle = \frac{1}{\sqrt{q}} \{U(f)|0\rangle + \cdots + U(f)|2^L - 1\rangle\} \\ &= \frac{1}{\sqrt{q}} \{f(0)|0\rangle + \cdots + f(n)|n\rangle + \cdots + f(2^L - 1)|2^L - 1\rangle\} \end{aligned} \quad (10.7)$$

这就是说, 由于量子态线性叠加性质, 算符对计算机中全部可能的自变数态, 一次性地将相应函数值全部计算出来, 只不过是相

干叠加着的，一旦测量便会塌缩到其中某一个函数值。所以真正要取出全部计算数据需要宏观数目的这类同样计算机同时工作。

2, 量子态的操控

量子态操控通过各种量子逻辑门来实现。量子逻辑门可用多种物理系统的多种物理过程实现。比如，核磁共振 (*NMR*)、量子点、离子阱、半导体硅基、*Josephson* 结等。下面用 *NMR* 方法来说明。

i, 单 *qubit* 量子门—— $U(\alpha, \varphi)$ 门

$U(\alpha, \varphi)$ 门	
输入	输出
$ 0\rangle$	$\cos \alpha 0\rangle - ie^{i\varphi} \sin \alpha 1\rangle$
$ 1\rangle$	$\cos \alpha 1\rangle - ie^{-i\varphi} \sin \alpha 0\rangle$

【物理实现】一个脉冲磁场，在(x-y)面内存在 τ 时间间隔：

$\vec{B} = |\vec{B}|(\cos \varphi, \sin \varphi, 0)$ ，它招致自旋绕磁场方向进动一定角度。设

$\vec{e}_B = \vec{B}/|\vec{B}|$ ， $\omega_L = \frac{2}{\hbar} |\vec{\mu}_n| |\vec{B}|$ 为拉摩进动频率， $\omega_L \tau$ 为进动转过的角度。这

个脉冲磁场使自旋态产生 $SU(2)$ 变换 ($\alpha = \frac{\omega_L \tau}{2}$)，

$$\begin{aligned}
 \exp \left\{ -\frac{i}{2} \vec{\sigma} \cdot \vec{e}_B \omega_L \tau \right\} &\equiv \exp \{ -i\alpha \vec{\sigma} \cdot \vec{e}_B \} \\
 &= \exp \{ -i\alpha (\sigma_x \cos \varphi + \sigma_y \sin \varphi) \} \\
 &= \begin{pmatrix} \cos \alpha & -i \sin \alpha e^{i\varphi} \\ -i \sin \alpha e^{-i\varphi} & \cos \alpha \end{pmatrix}
 \end{aligned} \tag{10.8}$$

特例 1: 非门 $U\left(\alpha = \frac{\pi}{2}, \varphi = 0\right) = \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ 。

特例 2: *Hadamard* 门是执行以下转动的单个 *qubit* 门，

$$|0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle); |1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{10.9}$$

这相当于 $e^{-i\pi\sigma_x/2}e^{-i\pi\sigma_y/4} = \frac{-i}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ (也见【4】中文译本 p.18、163)。

回忆第一章叙述可知，这个门也可以用半透片或者相移器来实现。

特例 3：两个特别的 $U(\alpha, \varphi)$ 相乘：一个非门乘一个 $U\left(\frac{\pi}{2}, \varphi\right)$ ，便可以构成相位门 $-i \begin{pmatrix} \exp(-i\varphi) & 0 \\ 0 & \exp(i\varphi) \end{pmatrix}$ 。

ii, 双 qubit 量子门——CNOT 可控非门

CNOT			
输入		输出 (mod2)	
控制 qubit	工作 qubit	控制 qubit	工作 qubit
$ 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$

由此真值表可知，CNOT 门实际上是个 mod2 的加法门（即工作位的输出是两个输入量子位数值的相加，逢 2 舍去—modulo2=mod2）。

【物理实现】NMR。三氯甲烷 $CHCl_3$ $\vec{B}_0 = -|\vec{B}_0|\vec{e}_z$ 。控制位 qubit A 为 $\vec{B}_0$ 下的 1H 原子核自旋 $\hat{I}_{zA}$ ；工作位 qubit B 为 $\vec{B}_0$ 下的 ^{13}C 原子核自旋 $\hat{I}_{zB}$ ；这个系统的 Hamiltonian 为

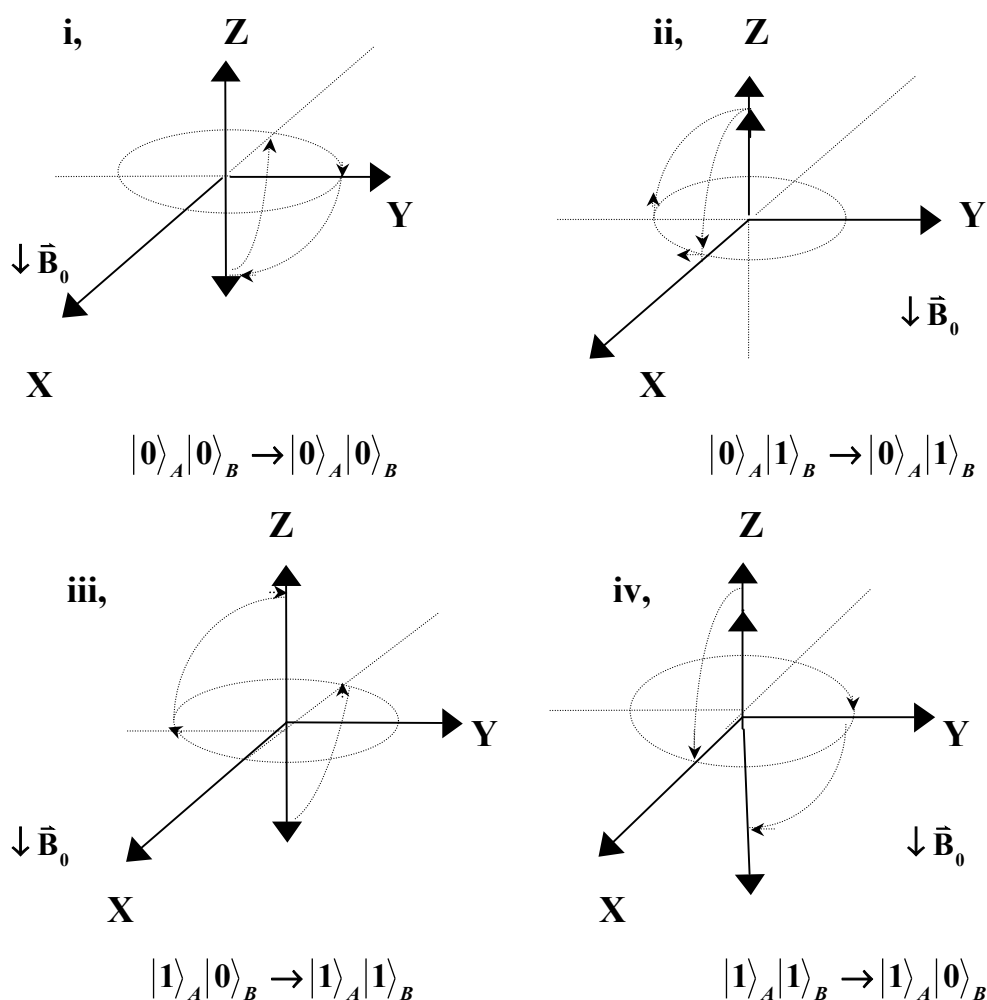
$$\hat{H} = \omega_A \hat{I}_{zA} + \omega_B \hat{I}_{zB} + 2\pi \hat{J}_{zA} \hat{I}_{zB} \quad (10.10)$$

在说明如何施加脉冲磁场对原子核自旋进行调控，以达到运算的目的之前，先分析一下这个 Hamiltonian。当外加交变磁场脉冲的频率正好等于某个原子核的固有频率时，该原子核的自旋将绕这个磁场方向作进动运动。进动频率就是 Lamor 频率（受磁场

大小决定), 进动时间就是该磁场脉冲存留的时间。这就是以共振方式所作的进动运动。在此磁场脉冲期间, 别的原子核自旋将不进动。为说明方便, 平移能量的原点: 当 I_{zA}, I_{zB} 向下时, 将它们量子数算作零, 相应附加能量均为零, 而朝上取向时, 量子数算作 1, 相应附加能分别为 $\hbar\omega_A, \hbar\omega_B$ 。

现在, 当控制位 A 原子自旋为零时, 工作位 B 原子进动频率是 ω_B ; 而当 A 位的自旋为 1 时, B 位自旋进动的频率加快了, 成为 $\omega_B + 2\pi J$ 。这就是下面所作分析的关键所在。

现在研究在 “ $Y(\frac{\pi}{2})$ —— τ 进动—— $X(-\frac{\pi}{2})$ ” 系列脉冲操作下 B 核自旋运动, 这些运动使工作位 B 核承当着 $CNOT$ 门的计算任务:



应当说明, 上面这些操控图解只是原理演示性质。因为这些图解叙述并未考虑这种 $CNOT$ 门工作中的误差问题和抗干扰问题。比如, 始终存在的恒定磁场对极化矢量进动一直有影响; 分子热运

动的影响；而当 *NMR* 技术中利用几何相——*Berry* 相位工作时，未表明如何划分几何相因子和动力学相因子，以及如何消除后者影响等问题。详细可见有关文献。比如，国内就有不少很好的工作【6、7、8、9】，可供参考。其中除【6】是关于离子阱双量子门的理论工作外，都是关于几何相量子门的理论或实验工作。

§10.2 量子门简单组合及量子网络分解

1, 量子门的简单组合

i, 逻辑门的作用与记号（为确定，依 σ_z 本征态的约定）

非门——单输入单输出 *NOT* 门：

$$\begin{cases} |x\rangle_{in} \rightarrow |\bar{x}\rangle_{out} \\ \alpha|0\rangle_{in} + \beta|1\rangle_{in} \rightarrow \alpha|1\rangle_{out} + \beta|0\rangle_{out} \end{cases}$$

与门——两输入单输出 *AND* 门：

$$\begin{cases} |x\rangle_1 \otimes |y\rangle_2 \rightarrow |x\rangle_1 \otimes |xy\rangle_2 \\ (\alpha|0\rangle_1 + \beta|1\rangle_1) \otimes |y\rangle_2 \rightarrow (\alpha|0\rangle_1 \otimes |0\rangle_2 + \beta|1\rangle_1 \otimes |y\rangle_2) \end{cases}$$

非与门——两输入单输出 *NAND* 门：

$$\begin{cases} |x\rangle_1 \otimes |y\rangle_2 \rightarrow |x\rangle_1 \otimes |\overline{xy}\rangle_2 \\ (\alpha|0\rangle_1 + \beta|1\rangle_1) \otimes |y\rangle_2 \rightarrow (\alpha|0\rangle_1 \otimes |1\rangle_2 + \beta|1\rangle_1 \otimes |\bar{y}\rangle_2) \end{cases}$$

或门——两输入单输出 *OR* 门：

$$\begin{cases} |x\rangle_1 \otimes |y\rangle_2 \rightarrow |x\rangle_1 \otimes |\bar{x} \cdot \bar{y}\rangle_2 \\ (\alpha|0\rangle_1 + \beta|1\rangle_1) \otimes |y\rangle_2 \rightarrow (\alpha|0\rangle_1 \otimes |y\rangle_2 + \beta|1\rangle_1 \otimes |1\rangle_2) \end{cases}$$

非或门——两输入单输出 *NOR* 门：

$$\begin{cases} |x\rangle_1 \otimes |y\rangle_2 \rightarrow |x\rangle_1 \otimes |\bar{x} \cdot \bar{y}\rangle_2 \\ (\alpha|0\rangle_1 + \beta|1\rangle_1) \otimes |y\rangle_2 \rightarrow (\alpha|0\rangle_1 \otimes |\bar{y}\rangle_2 + \beta|1\rangle_1 \otimes |0\rangle_2) \end{cases}$$

控制非门——两输入单输出 *XOR* 门：

$$\begin{cases} |x\rangle_1 \otimes |y\rangle_2 \rightarrow |x\rangle_1 \otimes |(x+y) \bmod 2\rangle_2 \\ (\alpha|0\rangle_1 + \beta|1\rangle_1) \otimes |y\rangle_2 \rightarrow (\alpha|0\rangle_1 \otimes |y\rangle_2 + \beta|1\rangle_1 \otimes |\bar{y}\rangle_2) \end{cases}$$

以图解表示为（注意，加法都是 $\bmod 2$ 的）：

▲ 例如 **XOR**：

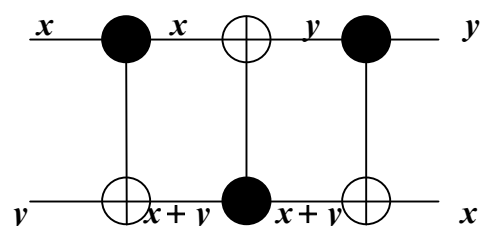
$$|x\rangle_1 |y\rangle_2 \rightarrow |x\rangle_1 |(x \oplus y) \bmod 2\rangle_2$$

平方等于恒等变换：

$$|x\rangle_1 |y\rangle_2 \rightarrow |x\rangle_1 |(x \oplus y) \bmod 2\rangle_2 \rightarrow |x\rangle_1 |y\rangle_2$$

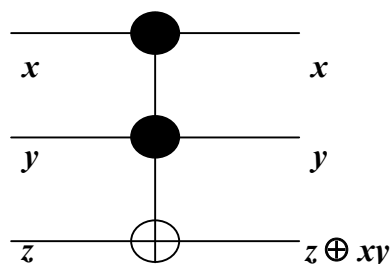
▲ 再比如三个门联合作用：也可记为

$$(x, y) \rightarrow (x, x \oplus y) \rightarrow (y, x \oplus y) \rightarrow (y, x)$$



▲ **Toffoli 门**——双可控非门：

$$\theta^{(3)}: (x, y, z) \rightarrow (x, y, z \oplus xy)$$



这里， x 位和 y 位是两个控制位，而 z 位是靶位。两个控制位输出总不变。当也只当 x 和 y 都有信号输入时，靶位将信号 z 反转为 $\bar{z}$ 输出。可以分析证实，如果将这个门的 z 端固定为1，就成为上面的非与门 **NAND**。

ii, 可逆两 *bit* 门与线性运算

为了构建通用的可逆的计算，单 *bit*、两 *bit* 的可逆逻辑门是不够的，至少需要三个 *bit*。为弄清这一点，注意到：其一，所有这些门都是线性的；其次，每个可逆两 *bit* 门，其作用都不外乎是如下的形式

$$\begin{pmatrix} x \\ y \end{pmatrix} \rightarrow \begin{pmatrix} x' \\ y' \end{pmatrix} = M \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} a \\ b \end{pmatrix} \quad (10.11a)$$

这里，常数 $\begin{pmatrix} a \\ b \end{pmatrix}$ 取四种可能中的一种，而 M 共有以下 6 种可逆矩阵

$$M = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \quad (10.11b)$$

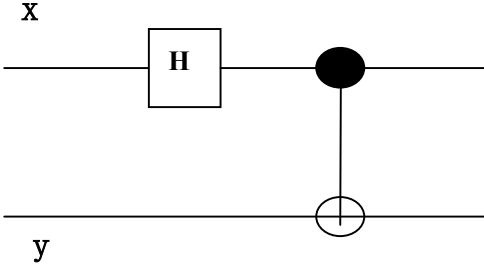
这 6 个 M 和 4 个 $\begin{pmatrix} a \\ b \end{pmatrix}$ 选择搭配，共组成 24 个不同的门（这里所有加法都执行 *mod2* 的运算）。这些 24 种搭配穷尽了所有可逆的 $2 \rightarrow 2$ 门的运算。这些全都是线性变换。而接连实行的线性变换，其结果仍旧是个线性变换。所以 24 种组合相乘最后一定还是个线性变换。因此由可逆两 *bit* 门组合的任何回路只能计算线性函数，而不能计算非线性函数。

但对于三个或更多个 *bit* 门组成的回路，可以包含非线性运算。比如 3*bit* 的 *Toffoli* 门，它当前两个门都是 1 时，才翻转第 3 个门的输入。它是它自己的逆，这一点如同 *CNOT* 门。不像可逆的两 *bit* 门，如果我们能提供固定的输入 *bits* 并且忽略输出的 *bits*，*Toffoli* 门就可以作 *Boolean* 逻辑运算的普适门。假如 z 初始为 1，于是 $x \uparrow y = 1 - xy$ 就在第 3 个门的输出处出现——这就执行了 *NAND* 操

作。假如我们固定 $x=1$ ，*Toffoli* 门的作用就像一个 *CNOT* 门。就下面意义而言，*Toffoli* 门是普适的：可以只用 *Toffoli* 门（假定能够固定输入 *bits* 并且忽略输出 *bits*）建造回路计算任何可逆的函数。详见文献【2、3、4】。

iii, 能够制备 4 个 *Bell* 基的量子回路

一个 *Hadamard* 门之后紧跟 *CNOT* 门，这种组合能产生 4 个 *Bell* 基【4】。结果是：如果将输入记为 $|xy\rangle$ ，则输出可以表示为：

$$|xy\rangle \Rightarrow \frac{1}{\sqrt{2}} \left(|0y\rangle + (-1)^x |1\bar{y}\rangle \right),$$


具体的真值表为：

$$\left\{ \begin{array}{l} |00\rangle \\ |10\rangle \\ |01\rangle \\ |11\rangle \end{array} \right\} \rightarrow \left\{ \begin{array}{l} |\varphi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ |\varphi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\ |\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\ |\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \end{array} \right\}$$

这是由于 *Hadamard* 门变换是（也见【4】中译本第 160、163 页）

$$H \equiv \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

这个门的第一列将 $|0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ ；而第二列将 $|1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ 。其平方为恒等变换 $H^2 = I$ 。现在，比如 $|10\rangle$ 态输入（ $x=1, y=0$ ），有

$$|xy\rangle = |10\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes |0\rangle \equiv \frac{1}{\sqrt{2}}(|00\rangle - |10\rangle) \xrightarrow{CNOT} \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

2, 量子网络的 *Deutsch* 分解定理

【*Deutsch* 定理(1985)】【2】

“对任意 d 维么正变换 U , 总可以将其分解为 $2d^2 - d$ 个二维么正变换的乘积(它们均是分别作用于各自一对基矢所张成的两维子空间, 即它们中每一个的各自余空间均不变)。

于是, 作用在任一组 *qubit* 上的任意么正变换均可以用一系列单 *qubit* 量子门 $U(\alpha, \varphi)$ 和双 *qubit* 量子门 *CNOT* 门依次作用来实现。”

【证明】取定基矢 $\{|e_1\rangle, |e_2\rangle, \dots, |e_d\rangle\}$ 所张成的 d 维空间。

首先, 可证用 $(d-1)$ 个 2 维么正变换将任意给定的 d 维矢量变为

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_d \end{pmatrix} \rightarrow \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \equiv |e_1\rangle \quad (10.12)$$

为此, 取 2 维么正变换 A_2 ,

$$A_2 = \frac{1}{\sqrt{|a_1|^2 + |a_2|^2}} \begin{pmatrix} a_1^* & a_2^* \\ a_2 & -a_1 \end{pmatrix} \quad (10.13a)$$

它仅作用于子空间 $\{|e_1\rangle, |e_2\rangle\}$, 对相应的余空间为恒等变换, 于是有

$$A_2 \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} \sqrt{|a_1|^2 + |a_2|^2} \\ 0 \end{pmatrix} \quad (10.13b)$$

再取 2 维么正变换 A_3 ,

$$A_3 = \frac{1}{\sqrt{|a_1|^2 + |a_2|^2 + |a_3|^2}} \begin{pmatrix} \sqrt{|a_1|^2 + |a_2|^2} & a_3^* \\ a_3 & -\sqrt{|a_1|^2 + |a_2|^2} \end{pmatrix} \quad (10.14a)$$

它仅对子空间 $\{|e_1\rangle, |e_3\rangle\}$ 作用, 对相应的余空间为恒等变换, 于是有

$$A_3 \begin{pmatrix} \sqrt{|a_1|^2 + |a_2|^2} \\ a_3 \\ 0 \end{pmatrix} = \begin{pmatrix} \sqrt{|a_1|^2 + |a_2|^2 + |a_3|^2} \\ 0 \end{pmatrix} \quad (10.14b)$$

如此继续即得 $(d-1)$ 个（依赖于给定矢量的）2 维幺正变换，使得

$$A_d \cdots A_3 A_2 \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_d \end{pmatrix} = \sqrt{|a_1|^2 + |a_2|^2 + \cdots + |a_d|^2} \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad (10.15)$$

其次，令 $|\Phi_1\rangle, |\Phi_2\rangle, \dots, |\Phi_d\rangle$ 是任意给定的 d 维幺正变换 U 的本征矢量（它们彼此正交），相应本征值分别为 $e^{i\Phi_1}, e^{i\Phi_2}, \dots, e^{i\Phi_d}$ 。

将上面步骤用于 $|\Phi_1\rangle$ 之后再乘以 $e^{i\Phi_1}$ ，就是说，

$$|\Phi_1\rangle \rightarrow e^{i\Phi_1} |e_1\rangle \quad (10.16)$$

然后将 $|e_1\rangle$ 逆映射为 $|\Phi_1\rangle$ ，于是有

$$\left(A_2^{(1)}\right)^{-1} \cdots \left(A_d^{(1)}\right)^{-1} \begin{pmatrix} e^{i\Phi_1} & 0 & & \\ 0 & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} A_d^{(1)} \cdots A_2^{(1)} |\Phi_1\rangle = e^{i\Phi_1} |\Phi_1\rangle \quad (10.17)$$

这里共有 $(d-1)+1+(d-1)=2d-1$ 个 2 维幺正变换。对每个本征矢量 $|\Phi_j\rangle$ 都重复如此作法，并注意，由于 $|\Phi_1\rangle$ 和 $|\Phi_j\rangle$ ($j=2, \dots, d$) 彼此正交，因而

$$\left(A_2^{(1)}\right)^{-1} \cdots \left(A_d^{(1)}\right)^{-1} \begin{pmatrix} e^{i\Phi_1} & 0 & & \\ 0 & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} A_d^{(1)} \cdots A_2^{(1)} |\Phi_j\rangle = |\Phi_j\rangle, (j=2, \dots, d) \quad (10.18)$$

这是由于列矢量 $A_d^{(1)} \cdots A_2^{(1)} |\Phi_j\rangle$ ($j \neq 1$) 中的第一个元素必定为零，而
为零则是因为此列矢量必须和 $A_d^{(1)} \cdots A_2^{(1)} |\Phi_1\rangle = |e_1\rangle$ 正交。

于是 U 就是这组 $d(2d-1)$ 个 2 维幺正变换的乘积。因为此乘积满足 U 的全部本征矢量的本征方程。

注意，由于 U 被分解为 d 的多项式个运算，按下面说法， U 的这种分解是有效算法。应当指出，后来【4】中有一个改进证明，表明 U 可以被表示成为 $d(d-1)/2$ 个 2 维幺正变换的乘积。显然， $d(d-1)/2 < d(2d-1)$ 。由此，作为特例，一个 n 个 *qubit* 的量子存储器将至多可以被分解为 $2^{n-1}(2^n-1)$ 个两维幺正矩阵的乘积。当然，对于特殊的矩阵，还可以找到更有效也即更少数目的分解。但分解为两维幺正矩阵乘积个数最少不能少于 $(d-1)$ 个(参见习题【9.1】)。采用所谓相邻 *qubit* 的 *Gray* 码，可以证明（参见【4】）：任何针对单个 *qubit* 或两个不同 *qubit* 之间的二维幺正变换，更直接说，任何作用在一组 N 个 *qubit* 上的二维幺正变换，均可用一系列 $U(\alpha, \varphi)$ 单量子门和 *CNOT* 双量子门的依序作用来实现。于是，就量子计算而言，这两个逻辑门是普适的。

3，分解举例

作为一个例子，现在分解 S 能级任意量子态 *Teleportation* 过程中的幺正变换算符 U_{AC} 。

在那里，利用 $L(> \log S)$ 个两能级 *EPR* 对实行单个 S 能级粒子态的超空间转移。而算符 U_{AC} 是表示 *Alice* 对她手中的 $L+1$ 个粒子所进行的局域联合的幺正变换。而这种变换通过 L 个量子通道，影响着 $2L+1$ 个粒子的状态。为了让操作成为可行，需要将多体操作转化为两体操作，即将 U_{AC} 分解为一系列两体幺正变换与单体幺正变换的先后作用。

可以发现，只需两种类型的幺正变换即可实现 U_{AC} 的这种分解。第一种是对 S 能级单个粒子 C 量子态的离散 *Fourier* 变换 DFT_S 。

根据基 $\{|m\rangle_C, m=0,1,\dots,S-1\}$ ，此变换定义为

$$DFT_S : |m\rangle_C \rightarrow \frac{1}{\sqrt{S}} \sum_{j=0}^{S-1} e^{i2mj\pi/S} |j\rangle_C, \quad m=0,1,\dots,S-1 \quad (10.19)$$

第二种类型的么正变换 U_{Ck} 作用在 C 粒子与 A_k 粒子上，它的定义是

$$U_{Ck} : |m\rangle_C |n_k\rangle_{A_k} \rightarrow |m\rangle_C |m_k \oplus n_k\rangle_{A_k}$$

这两种变换的么正性都是很容易证明的。于是由它们乘积所组成的任一算符也将是么正的。

下面证明，利用 U_{Ck} 和 DFT_S ，可以将 U_{AC} 分解为

$$U_{AC} = \left(\prod_{k=0}^{L-1} U_{Ck} \right) \cdot DFT_S \cdot \left(\prod_{k=0}^{L-1} U_{Ck} \right) \quad (10.20)$$

其中，因为 $[U_{Ck'}, U_{Ck}] = 0, (k, k' = 0, 1, \dots, L-1)$ ，所以上式中 U_{Ck} 的连乘积可以不分次序。

【证明】 下面证明记号引自【3】§ 9.5.2。由(9.22)式，

$$\begin{aligned} U_{AC} : |m\rangle_C |n\rangle_A &= \frac{1}{\sqrt{S}} \sum_{j=0}^{S-1} e^{i2mj\pi/S} |j\rangle_C |f^{(n)}(j, m)\rangle_A \\ &= \frac{1}{\sqrt{S}} \sum_{j=0}^{S-1} \left(e^{i2mj\pi/S} |j\rangle_C \prod_{k=0}^{L-1} |n_k \oplus m_k \oplus j_k\rangle_{A_k} \right) \\ &= \left(\prod_{k=0}^{L-1} U_{Ck} \right) \left\{ \left(\frac{1}{\sqrt{S}} \sum_{j=0}^{S-1} e^{i2mj\pi/S} |j\rangle_C \right) \left(\prod_{k=0}^{L-1} |n_k \oplus m_k\rangle_{A_k} \right) \right\} \\ &= \left(\prod_{k=0}^{L-1} U_{Ck} \right) \left\{ (DFT_S |m\rangle_C) \left(\prod_{k=0}^{L-1} |n_k \oplus m_k\rangle_{A_k} \right) \right\} \\ &= \left\{ \left(\prod_{k=0}^{L-1} U_{Ck} \right) \cdot DFT_S \cdot \left(\prod_{k=0}^{L-1} U_{Ck} \right) \right\} (|m\rangle_C |n\rangle_A) \end{aligned}$$

由于 $|m\rangle_C |n\rangle_A (m=0,1,\dots,S-1; n=0,1,\dots,L-1)$ 构成 $A+C$ 体系的完备基，所以得到上述 U_{AC} 的分解式。证毕。

作为特例，当 $S=3$ 时， U_{AC} 将依序分解为 $U_{C1}U_{C0}DFT_3U_{C0}U_{C1}$ 总共 5 个么正变换的连乘积。

§10.3 量子计算机及量子网络的 DiVincenzo 标准

下面分别介绍 *DiVincenzo* 关于量子计算机的 5 条标准,和关于量子网络的两条标准【6】。按照这些标准,便于对各种实验实现方案的潜在能力、现状和预期进展作出客观统一的评价。

1, 关于量子计算机的五条 *DiVincenzo* 标准:

- i, 具有较好特性的量子位和一定规模的量子位体系;
- ii, 可将全部量子位初始化为简单同一基准态的能力;
- iii, 相对于门的运算时间来说,有长得多的退相干时间;
- vi, 量子门彼此可作普适的插接;
- v, 对任何特定量子位进行测量的能力。

2, 关于量子计算机的量子网络功能附加的两条必要标准:

- i, 在飞行量子位和定态量子位之间的转换能力;
- ii, 在规定地点之间可信地传送飞行量子位的能力。

【练习题】

[10.1] 证明: 存在一个 $d \times d$ 的么正矩阵 U , 它不能被分解为少于 $d-1$ 个二维么正矩阵的乘积。

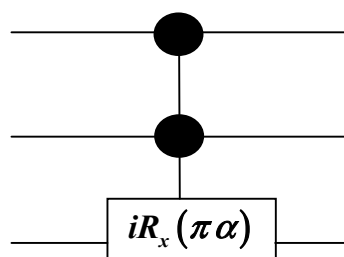
[10.2] 验证: $\frac{1}{2}$ 自旋的 $SU(2)$ 代数可用两模耦合谐振子来表示:

$$\left\{ \begin{array}{l} \sigma_z \rightarrow a^+a - b^+b \\ \sigma_x \rightarrow a^+b + ab^+; \quad \sigma_+ \rightarrow a^+b \\ \sigma_y \rightarrow -i(a^+b - ab^+); \quad \sigma_- \rightarrow ab^+ \end{array} \right.$$

这里 $\sigma_{\pm} = (\sigma_x \pm i\sigma_y)/2$ 。接着表明: 描述反射率为 $R \equiv \cos \theta$ 的量子

分束器 (*beamsplitter*) 作用的 *Hamiltonian* 为 $H_{bs} = i\theta(ab^+ - a^+b)$ 。

[10.3] 证明：下面回路确定的 3-qubit 门——称为 *G* 门或 *Deutsch* 门



当 α 是无理数时，对量子计算也是普适的。

【参考文献】

- 【1】 *A.Ekert, et.al., Rev.Mod.Phys., 68(1996)733.*
- 【2】 *J. Preskill, 《Lecture Notes for Physics 229: Quantum Information and Computation》, CIT, Sept. 1998, pp.242-245.*
- 【3】 张永德,《量子信息物理原理》,北京:科学出版社。2012年。
- 【4】 *M.A.Nielsen and I.L.Chuang,《Quantum Computation and Quantum Information》, Cambridge Univ. Press, pp.25-26. pp.159。中译本,清华大学出版社,2004年。*
- 【5】 *ibid. p.216, p.637.*
- 【6】 *A Quantum Information Science and Technology Roadmap, Part 1 : Quantum Computation, Appendix A-2, LA-UR-04-1778, April 2, 2004.*