量子比特系统和量子逻辑电路

吴晋渊

2021 年 10 月 28 日

1 量子比特系统

1.1 单量子比特

一个**单量子比特系统**是一个只有$|0\rangle$和$|1\rangle$两种状态的系统。正如经典比特系统非常简单，但是可以编码一切经典信息，量子比特系统也是量子计算的基础。单个量子比特也可以看成一个1/2自旋自由度，虽然未必有对应的对称性。

量子比特系统的密度矩阵是本征值之和为1、本征值大于等于零的全体2×2复厄米矩阵，容易验证这样的矩阵一定具有形式

$$\hat{\rho}=\frac{1+\boldsymbol{r}\cdot\hat{\boldsymbol{\sigma}}}{2}=\frac{1+x\hat{\sigma}_x+y\hat{\sigma}_y+z\hat{\sigma}_z}{2},\quad r=\sqrt{x^2+y^2+z^2}\leq 1. \tag{1}$$

这是因为泡利矩阵构成全体2×2厄米矩阵的一组基，于是一个2×2厄米矩阵一定可以写成

$$R(1+x\hat{\sigma}_x+y\hat{\sigma}_y+z\hat{\sigma}_z)$$

的形式。这样的矩阵的本征值为$R(1\pm r)$，而为了保证本征值之和为1必须取$R=1/2$，由本征值大于等于零就有$r\leq 1$，于是就得到(1)。

可以看出，$\boldsymbol{r}$的取值范围构成了一个半径为1的球，称为**Bloch球**。任何密度矩阵都可以表示成Block球上的一个点。当且仅当密度矩阵只有一个本征值非零时，它对应一个纯态，因此量子比特系统是纯态，当且仅当$r=1$，而$r<1$的情况都是混合态。实际上，通过计算冯诺依曼熵可以发现r越大熵越小，$r=0$时是完全混和态。于是Bloch球的球壳上是全部纯态，其内部为全部混合态。实际上，可以根据r计算纯度

$$\operatorname{tr}\hat{\rho}^2=\frac{1}{2}(1+r^2). \tag{2}$$

既然所有纯态都在Bloch球的球面，不失一般性地，以z轴和Bloch球的交点为$|0\rangle$，我们很快会发现$|1\rangle$对应的是$(x,y,z)=(0,0,-1)$，因此$|0\rangle$在Bloch球的北极，而$|1\rangle$在Bloch球的南极。显然，$|0\rangle$和$|1\rangle$没有任何特殊地位，因此我们得出结论：Bloch球球面上相对的两个点表示一对正交态。

在Bloch球上建立球坐标系，以(r,θ,φ)为球坐标。对$r=1$的点，即纯态，代入(1)，做特征分解可以得到

$$|\psi(\boldsymbol{r})\rangle=\cos\frac{\theta}{2}|0\rangle+\sin\frac{\theta}{2}\mathrm{e}^{\mathrm{i}\varphi}|1\rangle, \tag{3}$$

而与它正交、位于Bloch球另一边的$|\psi(-\boldsymbol{r})\rangle$是

$$|\psi(-\boldsymbol{r})\rangle=\sin\frac{\theta}{2}|0\rangle-\cos\frac{\theta}{2}\mathrm{e}^{\mathrm{i}\varphi}|1\rangle. \tag{4}$$

Bloch球以一种直观的方式展现了量子比特系统和经典比特系统的区别：一个经典比特系统只能够存储1 bit的信息，但是一个量子比特系统需要两个实数来描述，因此包含不可数无穷多个比特的信息。但是这里有一个微妙的地方：态矢量的分量系数并不是直接可以实验观察的，但一旦做了观测，量子比特系统就坍缩了。因此我们并不能将θ和φ直接读出来。

1.2 多量子比特

1.2.1 二量子比特

两个量子比特形成的系统的密度矩阵具有如下的一般形式：

$$\hat{\rho}_{AB}=\frac{1}{4}(1+\boldsymbol{a}\cdot\hat{\boldsymbol{\sigma}}\otimes 1_B+1_A\otimes\boldsymbol{b}\cdot\hat{\boldsymbol{\sigma}}+\sum_{jk}T_{jk}\hat{\sigma}_j\otimes\hat{\sigma}_k). \tag{5}$$

通过对这一密度矩阵做适当的求迹可以得到各个参数：

$$\begin{cases}\mathrm{tr}(\hat{\rho}_{AB}(\hat{\boldsymbol{\sigma}}\otimes 1_B))=\boldsymbol{a},\\ \mathrm{tr}(\hat{\rho}_{AB}(1_A\otimes\hat{\boldsymbol{\sigma}}))=\boldsymbol{b},\\ \mathrm{tr}(\hat{\rho}_{AB}(\hat{\sigma}_i\otimes\hat{\sigma}_j))=T_{ij}.\end{cases} \tag{6}$$

T_{jk}称为<u>关联矩阵</u>，因为它不能通过A或B的约化密度矩阵得到。直接计算可知，

$$\hat{\rho}_A=\mathrm{tr}_B(\hat{\rho}_{AB})=\frac{1}{2}(1+\boldsymbol{a}\cdot\hat{\boldsymbol{\sigma}}),\quad \hat{\rho}_B=\mathrm{tr}_A(\hat{\rho}_{AB})=\frac{1}{2}(1+\boldsymbol{b}\cdot\hat{\boldsymbol{\sigma}}), \tag{7}$$

即$\boldsymbol{a}$和$\boldsymbol{b}$为A和B对应的Bloch球矢量，而T_{jk}始终没有出现。因此，T_{jk}应该存储着描述两个比特之间的量子关联或者说量子纠缠的信息。（量子纠缠有可观测的实际效应，见第2节）如果$\hat{\rho}_{AB}$是两个系统的状态的直积，那么

$$T_{jk}=a_jb_k,\quad \det T_{jk}=0.$$

对二系统组成的纯态，纠缠熵是好的度量纠缠大小的量。我们下面计算最大纠缠态。对二量子比特系统做Schmidt分解。每个量子比特的希尔伯特空间为二维的，因此Schmidt分解可以将一个任意的二量子比特系统的态矢量写成一个二维希尔伯特空间中的矢量。显然，这个二维希尔伯特空间的基底可以是$\{|00\rangle,|11\rangle\}$或是$\{|01\rangle,|10\rangle\}$。于是我们只需求解优化问题

$$|\psi\rangle=a|00\rangle+b|11\rangle\quad\text{or}\quad a|01\rangle+b|10\rangle,\quad |a|^2+|b|^2=1.$$

以上优化问题的一组解为所谓<u>贝尔态</u>，它们是

$$\begin{aligned}|\Phi^+\rangle&=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle),\quad |\Phi^-\rangle=\frac{1}{\sqrt{2}}(|00\rangle-|11\rangle),\\ |\Psi^+\rangle&=\frac{1}{\sqrt{2}}(|01\rangle+|10\rangle),\quad |\Psi^-\rangle=\frac{1}{\sqrt{2}}(|01\rangle-|10\rangle).\end{aligned} \tag{8}$$

它们之间彼此线性无关，因此构成了二量子比特系统的一组基。

最大纠缠态是很多量子关联问题中最优解的实现方式。例如，在量子关联中，最大纠缠态通常会带来最大的关联。

1.3 量子比特系统的制备

2 量子关联

本节讨论量子比特系统展现出的一些纠缠特性。虽然态矢量本身并不是一个可以直接使用观测结果定义的量，但是一些现象强烈地表明，如果不引入可以直积、叠加——从而可以形成纠缠态的——态矢量，将很难描述一些现象。

2.1 CHSH游戏

CHSH游戏指的是这样一个过程：一个真随机数发生器产生一对均匀分布、彼此无关的比特x和y，将它们分别提供给Alice和Bob，两人相距一段距离，彼此不能联系，然后Alice和Bob分别产生一个比特，记作a和b，如果

$$x \wedge y = a \oplus b, \tag{9}$$

游戏就成功了。

当然，Alice和Bob可以采取不同的策略来增大游戏成功的概率，不过显然游戏成功的概率有一个小于1的上限。我们将指出，如果量子力学实际上是错误的，也即，可以用局域的隐变量模拟各种量子现象，那么游戏成功的概率的上限要小于量子力学实际上成立时的概率上限。这意味着量子力学的一部分不同诠释实际上有可观察的效应。

由于x和y是均匀分布且彼此独立的，有

$$\begin{aligned} P_{\text{win}} &= \sum_{a,b,x,y} V(x,y,a,b) p_{AB|XY}(a,b|x,y) p_{XY}(x,y) \\ &= \frac{1}{4} \sum_{a,b,x,y} V(x,y,a,b) p_{AB|XY}(a,b|x,y). \end{aligned} \tag{10}$$

其中$V(x,y,a,b)$是指示函数，在游戏成功时为1，否则为0。现在要做的就是分析$p_{AB|XY}(a,b|x,y)$的形式。

2.1.1 隐变量理论的上限

Alice和Bob在分开之前可能有某种约定，从而导致它们在分开之后看起来还是有远距离关联，这是隐变量理论模拟量子纠缠的思路。我们取一个非常一般化的形式：设有隐变量为Λ，且

$$p_{AB|XY}(a,b|x,y) = \int \mathrm{d}\lambda \, p_\Lambda(\lambda) p_{A|\Lambda X}(a|\lambda,x) p_{B|\Lambda Y}(b|\lambda,b).$$

由于Alice和Bob分开之后才根据x,y决定a,b，a和b的产生是彼此独立的，因此我们有上式的形式。这样

$$\begin{aligned} P_{\text{win}} &= \int \mathrm{d}\lambda \, p_\Lambda(\lambda) \frac{1}{4} \sum_{a,b,x,y} V(x,y,a,b) p_{A|\Lambda X}(a|\lambda,x) p_{B|\Lambda Y}(b|\lambda,b) \\ &\leq \frac{1}{4} \sum_{a,b,x,y} V(x,y,a,b) p_{A|\Lambda X}(a|\lambda^*,x) p_{B|\Lambda Y}(b|\lambda^*,b), \end{aligned}$$

不等号是因为对λ的积分无非是一种平均值，因此只需要适当调节λ^*就可以让被积函数大于最后的积分值，且等号可以取到。这意味着隐变量其实在此处并没有什么意义——最有效的策略中隐变量是定死的。更进一步，我们可以发现让只有x,y,a,b能够胜利时概率取1其它情况取0能够获得最大胜率，因此胜率最大的策略中a是x的函数，而b是y的函数。这意味着我们需要让

$$0 = a_1 \oplus b_0, \quad 0 = a_0 \oplus b_1, \quad 0 = a_0 \oplus b_0, \quad 1 = a_1 \oplus b_1$$

尽可能成立。这四个式子不能都成立，最多只能成立三个，否则会产生矛盾，于是我们会发现P_{win}最大为3/4。

2.1.2 量子关联的胜率上限

另一方面，如果标准的量子力学的纠缠态是可以实现的，我们将会获得比3/4更大的胜率上界。这里不再使用隐变量来编码Alice和Bob的关联，而是真的认为Alice和Bob组成的系统由一个密度矩阵$\hat{\rho}$描述。这覆盖了隐变量的机制，同时还允许真正的量子纠缠，即所谓密度矩阵的非对角部分。

由于x, y是给定的，Alice和Bob可以根据他们得到的确定的x, y值来分别决定给出什么输出。唯一能够试图利用他们之间的关联的方法是通过测量$\hat{\rho}$，于是

$$p_{AB|XY}(a,b|x,y) = \mathrm{tr}(\hat{\rho}\hat{\Pi}_a^{(x)} \otimes \hat{\Pi}_b^{(y)}),$$

其中诸$\hat{\Pi}$均为正定算符，是POVM成员，且满足归一化条件。（Alice和Bob的POVM成员可能是不一样的，使用指标x和y区分它们）最大值肯定是在$\hat{\rho}$为纯态时取到的，因为POVM成员都是正定的。因此接下来我们讨论纯态的情况，即

$$p_{AB|XY}(a,b|x,y) = \langle\phi|\hat{\Pi}_a^{(x)} \otimes \hat{\Pi}_b^{(y)}|\phi\rangle\,.$$

在(x,y)为01，10或00时游戏成功意味着$a=b$，此时赢的概率为

$$\langle\phi|\hat{\Pi}_0^{(x)} \otimes \hat{\Pi}_0^{(y)}|\phi\rangle + \langle\phi|\hat{\Pi}_1^{(x)} \otimes \hat{\Pi}_1^{(y)}|\phi\rangle\,,$$

而输的概率为

$$\langle\phi|\hat{\Pi}_1^{(x)} \otimes \hat{\Pi}_0^{(y)}|\phi\rangle + \langle\phi|\hat{\Pi}_1^{(x)} \otimes \hat{\Pi}_0^{(y)}|\phi\rangle\,,$$

于是赢的概率减去输的概率为

$$\langle\phi|(\hat{\Pi}_0^{(x)} - \hat{\Pi}_1^{(x)}) \otimes (\hat{\Pi}_0^{(y)} - \hat{\Pi}_1^{(y)})|\phi\rangle\,.$$

类似的，(x,y)为11时赢的概率减去输的概率为

$$-\langle\phi|(\hat{\Pi}_0^{(x)} - \hat{\Pi}_1^{(x)}) \otimes (\hat{\Pi}_0^{(y)} - \hat{\Pi}_1^{(y)})|\phi\rangle\,.$$

设

$$\hat{A}^{(x)} = \hat{\Pi}_0^{(x)} - \hat{\Pi}_1^{(x)}, \quad \hat{B}^{(y)} = \hat{\Pi}_0^{(y)} - \hat{\Pi}_1^{(y)},$$

并定义

$$\hat{C}_{AB} = \hat{A}^{(0)} \otimes \hat{B}^{(0)} + \hat{A}^{(0)} \otimes \hat{B}^{(1)} + \hat{A}^{(1)} \otimes \hat{B}^{(0)} - \hat{A}^{(1)} \otimes \hat{B}^{(1)},$$

通过贝叶斯公式可以得到

$$P_{\mathrm{win}} - P_{\mathrm{lose}} = \frac{1}{4}\langle\phi|\hat{C}_{AB}|\phi\rangle\,.$$

通过一些代数计算可以得到

$$\hat{C}_{AB}^2 = 41_{AB} - [\hat{A}^{(0)}, \hat{A}^{(1)}] \otimes [\hat{B}^{(0)}, \hat{B}^{(1)}]\,,$$

使用无穷范数，有

$$\begin{aligned}\|\hat{C}_{AB}^2\| &\le 4 + \|[\hat{A}^{(0)}, \hat{A}^{(1)}]\|\|[\hat{B}^{(0)}, \hat{B}^{(1)}]\| \\ &\le 4 + (\|\hat{A}^{(0)}\hat{A}^{(1)}\| + \|\hat{A}^{(1)}\hat{A}^{(0)}\|)(\|\hat{B}^{(0)}\hat{B}^{(1)}\| + \|\hat{B}^{(1)}\hat{B}^{(0)}\|) \\ &= 4 + 2\cdot 2 = 8,\end{aligned}$$

考虑到无穷范数的定义我们就有

$$P_{\text{win}} - P_{\text{lose}} = \frac{1}{4}\langle\phi|\hat{C}_{AB}|\phi\rangle \leq \frac{\sqrt{2}}{2}.$$

由于

$$P_{\text{win}} + P_{\text{lose}} = 1,$$

我们得到

$$P_{\text{win}} \leq \frac{2+\sqrt{2}}{4}, \tag{11}$$

这个不等式的等号是可以取到的，为此我们尝试令$|\phi\rangle$取最大纠缠态。不失一般性地我们设

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle)$$

取到等号。所谓的**Tsirelson不等式**。

因此，如果量子纠缠真的是物理可实现的，我们将会观察到胜率高于3/4的情况；如果观察到了$(2+\sqrt{2})/2$的胜率，那么量子理论也是不足够的，需要引入超越量子理论的关联。

2.2 贝尔实验

CHSH游戏可以一般化为这样一个场景：

2.3 混合态的量子关联

在总维数小于6时，使用部分转置可以判断一个态是不是可分离态。当且仅当将总密度算符对每个子空间做部分转置后得到半正定算符，总密度算符是可分离态。

3 量子电路模型

正如基于经典比特系统的经典逻辑电路可以实现经典计算机，基于量子比特系统的**量子电路**也可以实现量子计算机。此处“电路”一词并不代表我们使用电子系统实现量子比特，而只是为了和经典构成对比。

一个量子电路模型通常可以分为三步：

1. 制备量子态，包括但不限于根据（可能是经典的）输入制备量子比特和引入辅助位；这些量子态称为**量子寄存器**。
2. 幺正演化，即让量子比特经过一系列幺正矩阵（**量子逻辑门**）的变换。
3. 测量。我们通常将测量放在最后，因为可以根据**推迟测量原则**，受控门和测量算符对易，于是任何在计算过程中发生的测量都可以推迟到线路的最后。

3.1 量子逻辑门

3.1.1 单量子比特门

单比特操作是非常容易实现的，但是显然是不够的，因为多量子比特系统经过单比特操作之后一定会得到直积态，而不能产生纠缠态。

最容易想到的量子门包括泡利矩阵，我们分别用X,Y,Z指代三个方向上的泡利矩阵，这样就获得了三个门。很容易看出X实际上就是非门。除此以外还有更多的门，如**Hadamard门**是指

$$H=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}, \tag{12}$$

它可以用于实现态叠加。 **相位门**是指

$$S=\begin{pmatrix}1 & 0\\ 0 & \mathrm{i}\end{pmatrix}, \tag{13}$$

它可以在单个量子比特的两种可能本征态之间产生一个$\pi/2$的相对相位。有了$\pi/2$相位当然还可以有别的相位，如**T门**或者$\pi/8$门

$$T=\begin{pmatrix}1 & 0\\ 0 & \exp(\mathrm{i}\pi/4)\end{pmatrix}. \tag{14}$$

单量子比特逻辑门有通用的构造方法。我们有**旋转**

$$R_x(\theta)=\exp\left(-\frac{\mathrm{i}\theta X}{2}\right)=\begin{pmatrix}\cos\frac{\theta}{2} & -\mathrm{i}\sin\frac{\theta}{2}\\ -\mathrm{i}\sin\frac{\theta}{2} & \cos\frac{\theta}{2}\end{pmatrix}, \tag{15}$$

$$R_y(\theta)=\exp\left(-\frac{\mathrm{i}\theta Y}{2}\right)=\begin{pmatrix}\cos\frac{\theta}{2} & -\sin\frac{\theta}{2}\\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2}\end{pmatrix}, \tag{16}$$

$$R_z(\theta)=\exp\left(-\frac{\mathrm{i}\theta Z}{2}\right)=\begin{pmatrix}\mathrm{e}^{-\frac{\mathrm{i}\theta}{2}} & \\ & \mathrm{e}^{\frac{\mathrm{i}\theta}{2}}\end{pmatrix}. \tag{17}$$

这些操作被称为旋转是因为将它们作用在一个态上就相当于将这个态在Bloch球上做了对应的旋转。例如，我们有

$$R_y(\alpha)\begin{pmatrix}\cos\frac{\theta}{2}\\ \mathrm{e}^{\mathrm{i}\varphi}\sin\frac{\theta}{2}\end{pmatrix}=\mathrm{e}^{-\frac{\mathrm{i}\alpha}{2}}\begin{pmatrix}\cos\frac{\theta}{2}\\ \mathrm{e}^{\mathrm{i}(\varphi+\alpha)}\sin\frac{\theta}{2}\end{pmatrix},$$

正好就是绕着z轴转动了α角度。实际上，更加一般的，绕着轴$\boldsymbol{n}$的旋转门为

$$R_{\boldsymbol{n}}(\theta)=\cos\frac{\theta}{2}I-\mathrm{i}\sin\frac{\theta}{2}\boldsymbol{n}\cdot\hat{\boldsymbol{\sigma}}. \tag{18}$$

可以证明，任何一个单比特幺正变换均形如

$$U=\mathrm{e}^{\mathrm{i}\alpha}R_z(\beta)R_y(\gamma)R_z(\delta)=\begin{pmatrix}\mathrm{e}^{\mathrm{i}(\alpha-\beta/2-\delta/2)}\cos\frac{\gamma}{2} & -\mathrm{e}^{\mathrm{i}(\alpha-\beta/2+\delta/2)}\sin\frac{\gamma}{2}\\ \mathrm{e}^{\mathrm{i}(\alpha+\beta/2-\delta/2)}\sin\frac{\gamma}{2} & \mathrm{e}^{\mathrm{i}(\alpha+\beta/2+\delta/2)}\cos\frac{\gamma}{2}\end{pmatrix}, \tag{19}$$

因此写出了单量子比特变换之后可以用三个旋转门连同一个一般的相位门来实现它。这个一般形式没有用到R_x门，但是这并没有什么奇怪的——实际上它就是欧拉角。上式的分解有一个简单的变形。设

$$A=R_z(\beta)R_y\left(\frac{\gamma}{2}\right),\quad B=R_y\left(-\frac{\gamma}{2}\right)R_z\left(-\frac{\delta+\beta}{2}\right),\quad C=R_z\left(\frac{\delta-\beta}{2}\right), \tag{20}$$

则

$$U=\mathrm{e}^{\mathrm{i}\alpha}AXBXC,\quad ABC=I. \tag{21}$$

这个结论在实现受控U门时可以用到。

我们有以下简单的逻辑门恒等式：

$$H=(X+Z)/\sqrt{2}, \tag{22}$$

$$HXH=Z,\quad HZH=X, HYH=-Y. \tag{23}$$

3.1.2 受控门

最为平凡的二量子比特门可能是两个单量子比特门直积得到的（注意张量积不可交换，虽然$A \otimes B \simeq B \otimes A$）。仅仅靠门的直积不能得到所有可能的量子逻辑门，因为这样不能产生纠缠态。因此我们需要横跨多个量子比特的量子门。

稍微复杂一些的二量子比特门是所谓**受控操作**，即只有在某个量子比特（称为**控制位**）为1时才对另一个量子比特（称为**目标位**）做操作。物理地说，受控门的作用是产生纠缠，原因是显然的——它对应量子比特之间的相互作用。 CNOT是一个典型的受控门，它形如

$$C = \mathrm{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{24}$$

CNOT门满足以下恒等式：

$$CX_1C = X_1X_2, \quad CY_1C = Y_1X_2, \quad CZ_1C = Z_1, \tag{25}$$

更加一般的，设U是任意一个操作，被单个量子比特控制的**受控U门**可以验证为[1]

$$\begin{pmatrix} 1 & 0 & \\ 0 & 1 & \\ & & U \end{pmatrix}, \tag{26}$$

进一步，多量子比特上，一个有n个控制位的受控U门可以定义为

$$C^n(U) \left|x_1, x_2, \ldots, x_n\right\rangle \left|\psi\right\rangle = \left|x_1, x_2, \ldots, x_n\right\rangle U^{x_1x_2\ldots x_n} \left|\psi\right\rangle. \tag{27}$$

特别的，Toffoli门就是CCNOT门。

此外，没有什么要求我们一定要在控制位为1时对目标位做操作，例如完全可以在控制位为0时对目标位做操作。总之，“在一些量子比特满足某些条件时对另一些量子比特做操作”的量子门统称**广义受控门**。不失一般性地设控制位排在目标位前面，受控位满足条件的状态的投影算符为P_{cond}，不满足条件的状态的投影算符为P_{other}，则广义受控门为

$$U = P_{\mathrm{other}} \otimes I + P_{\mathrm{cond}} \otimes \tilde{U}, \tag{28}$$

其中$\tilde{U}$是目标位在满足条件时做的操作。从这个通式出发，(26)就是显然的。

广义受控门总是可以使用普通受控门配合一些单量子比特门实现，因为我们可以用一个单量子比特门将控制位在满足特定条件时转化为1，然后使用普通受控门，然后再使用之前那个单量子比特门的逆来恢复控制位。

实际上，二量子比特的一切量子门都可以使用CNOT配合单量子比特门实现实现。任何一个二量子比特量子门都可以分解为(20)，而我们有

$$C(U) = \tag{29}$$

因为如果控制位为0，

$$C(U) = ABC = I,$$

[1] 请注意分块对角矩阵并不是两个矩阵的直积！

而如果控制位为1，

$$C(U) = \mathrm{e}^{\mathrm{i}\alpha} AXBXC = U,$$

于是我们就实现了$C(U)$门。这个结论实际上和量子线路模型的通用性密切相关，我们将在第3.1.3节中系统地讨论这一点。

3.1.3 通用量子门

下面的问题是，给定一个任意的n比特系统上的幺正操作U，怎样使用一组通用的量子门（允许直积上适当的恒等变换）的乘积构造它们？这种构造可以是完全准确的，也可以是近似的。

two level unitary transformation是指只对两个分量做非平凡操作的幺正变换。任何$d \times d$的幺正变换U可以写成k个two level unitary的乘积，其中$k \leq d(d-1)/2$。对这件事的证明是构造性的：设需要分解的幺正变换为U，则我们可以用一系列two level unitary transformation左乘到U上，这相当于对U施加某种特殊的高斯消元法，然后最后把U变换为最后两个量子比特上的变换直积上一个恒等变换，而由于U本身是幺正的，左乘到它上面的矩阵也是幺正的，最后的二量子比特变换也是幺正的，这就完成了分解。于是，全体two level unitary transformation构成通用量子门。

实际上，CNOT配合单量子比特门也构成通用量子门。我们知道任何二量子比特门都可以用CNOT配合单量子比特门实现。two level unitary transformation并不是单量子比特门和恒等变换的直积，它能够使用CNOT配合单量子比特门实现吗？实际上是可以的。请注意一个two level unitary transformation实际上就是某个广义受控门的行和列打乱之后的结果。另一方面，注意到广义CNOT门可以交换两个仅仅在某一位有差别的态，而通过**Gray编码**——即一系列相邻两个编码只差一位的编码串——可以使用广义CNOT门交换任意两个态，因此广义CNOT门配合一个单一的广义受控门就可以实现任意的two level unitary transformation。 Gray编码不是唯一的，并且最后一位是1变成0还是0变成1都无关紧要。最后，任意的广义CNOT门都可以使用CNOT门和单量子比特门实现，这是因为

使用这样的方法，使用单量子比特门和CNOT实现一个任意的n比特量子门最多需要量级为$\mathcal{O}(n^2 4^n)$的操作——一个任意的n比特量子门是一个2^n阶的方阵，

上面提到的量子门的集合都是连续的，如单量子比特门可以连续地调节，这当然也是正确的，因为量子线路模型中可以有相位变换而这是一种连续的操作。还有一种思路是，不要求精确地构造任何可能的幺正变换，而要求可能任意精确地逼近一个幺正变换。这就是近似通用量子门，可以用一个离散的集合做近似通用量子门。例如，

Hadamard, phase, CNOT, T gates (approximate)

使用∞-范数体现两个算符的差异。设

$$E(R_{\boldsymbol{n}}(\alpha), R_{\boldsymbol{n}}(\theta)^k) < \frac{\epsilon}{3} \tag{30}$$

实际上，这种逼近不仅是可能的，还是比较高效的。**Solovay-Kitaev定理**说，通过Hadamard门和T门对任何一个单量子比特门做精度ϵ的近似可以通过最多

$$N \sim \mathcal{O}(\log^c(1/\epsilon)) \tag{31}$$

个量子门实现，其中c大约是2。

通用量子门的存在意味着量子电路模型的表现力是非常强大的，可以覆盖任何实际的计算任务。

3.2 测量

用对单比特做测量得到的结果来做经典受控门，和用测量后的比特（塌缩到了$|0\rangle$或$|1\rangle$中的某一个上面）做控制位做量子受控门是等价的，因为它们产生一样的密度矩阵。

3.2.1 测量一个算符

设要用投影算符M_0和M_1做单比特测量，设

$$M_0 = I + U, \quad M_1 = I - U, \tag{32}$$

则

$$V = (H \otimes I)C(U)(H \otimes I) \tag{33}$$

principle of implicit measurement

测量只依赖于子系统的约化密度矩阵，因此自始至终未被测量的量子比特可以当成已经测量的，原因也是显而易见的：

$$\mathrm{tr}(\hat{\rho}(\hat{E} \otimes \hat{I})) = \mathrm{tr}(\hat{\rho}_A \hat{E}). \tag{34}$$

这个结论当然应该是正确的，否则就有信息的超距传播了。

principle pf deferred measurement

$$\sum_i \hat{M}_i \hat{C} \hat{\rho} \hat{C} \hat{M}_i^\dagger = \hat{C}$$

4 量子算法

4.1 量子傅里叶变换

量子傅里叶变换是指如下变换：

$$|j\rangle \longrightarrow \frac{1}{\sqrt{N}} \sum_k \mathrm{e}^{2\pi \mathrm{i} jk/N} |k\rangle, \tag{35}$$

其中N是$|i\rangle$的个数。我们通常将数值编码为二进制，从而设数据位数为n，则$N = 2^n$。通过直接展开可以发现上式可以在量子比特的框架下被写成

$$|j_1 j_2 \cdots j_n\rangle \longrightarrow 2^{n/2}(|0\rangle + \mathrm{e}^{2\pi \mathrm{i} 0.j_n}|1\rangle) \cdots (|0\rangle + \mathrm{e}^{2\pi \mathrm{i} 0.j_1 j_2 \cdots j_n}|1\rangle), \tag{36}$$

其中$0.j_n j_{n-1} \cdots$表示二进制小数，$j_1 j_2 \cdots$表示二进制整数；在推导上式时要注意到$\mathrm{e}^{2\pi \mathrm{i}}$的整数倍是1。

(36)可以比较容易地使用量子线路实现，具体步骤为实现的关键在于意识到j_1只需要被使用一次，所以一开始就可以直接在它上面做操作，而j_2需要被使用两次，所以需要等j_1上的操作完成了才能在j_2上做操作，等等。其时间复杂度为$\mathcal{O}(n^2)$。作为对比，经典傅里叶变换的时间复杂度为量子傅里叶变换尚未有效实现的主要原因是难以制备那么多量子比特，并且也很难测量相位——如果要精确测量，需要制备大量同样的量子态，这本身需要指数次操作。

4.2 量子相位估计

设某个量子寄存器$|u\rangle$是某个幺正操作的本征态，有

$$\hat{U}\left|u\right\rangle = \mathrm{e}^{2\pi \mathrm{i}\varphi}\left|u\right\rangle, \quad 0 < \varphi < 1. \tag{37}$$

现在需要设计一种算法来估计φ的前n位。

$$t = \tag{38}$$

4.3 order finding

对任意给定的、和整数N互质的整数x，满足以下条件的最小r定义为x的**order**：

$$x^r = 1 \mod N. \tag{39}$$

4.4 量子搜索

设我们有一个黑盒子$f(x)$，它是某个问题的oracle，即如果x是这个问题的解那么$f(x)$为1，否则为零。显然，可以构造一个量子门来获得oracle：

$$\left|x\right\rangle\left|q\right\rangle \xrightarrow{O} \left|x\right\rangle\left|q \oplus f(x)\right\rangle, \tag{40}$$

其中q为oracle qubit。容易验证，

$$\left|x\right\rangle \otimes \frac{\left|0\right\rangle - \left|1\right\rangle}{\sqrt{2}} \xrightarrow{O} (-1)^{f(x)}\left|x\right\rangle \frac{\left|0\right\rangle - \left|1\right\rangle}{\sqrt{2}}. \tag{41}$$

因此这是一个“相位的谕示”。

5 量子通信

6 混合态和量子操作

实际的量子系统都是有噪声的，应用混合态表示，而时间演化也不总是幺正的。噪声可以有好几种形式。例如，我们有完全经典的0和1之间的跃迁：

$$\begin{pmatrix} p_0(t+\Delta t) \\ p_1(t+\Delta t) \end{pmatrix} = \begin{pmatrix} 1-p & p \\ p & 1-p \end{pmatrix} \begin{pmatrix} p_0(t) \\ p_1(t) \end{pmatrix}, \tag{42}$$

这是一个马尔可夫过程，因为不同时间点的噪声是彼此独立的。作用在量子比特系统上的噪声可以写成“在一定的经典概率之下做某个操作”的形式，这称为**量子操作**。 Kraus分解定理告诉我们，一个量子操作可以写成

$$\hat{\rho}' = \sum_k \hat{E}_k \hat{\rho} \hat{E}_k^\dagger,$$

如果环境的初态为纯态，那么

$$\hat{E}_k = \left\langle \mathrm{env}_k \right| \hat{U} \left| \mathrm{env}_i \right\rangle,$$

其中$\hat{U}$为系统和环境共同的时间演化算符，$|\mathrm{env}_i\rangle$为环境初始状态。

密度矩阵的一般性时间演化都可以看成作用了一个量子操作。系统受到扰动是一个量子操作，对系统做观测是一个量子操作，对系统以一定的成功率做一个量子门也是一个量子操作。

我们下面将要频繁地讨论两个态之间的“距离”。常用的判据包括迹距离，定义为

$$D(\hat{\rho},\hat{\varrho})=\frac{1}{2}|\hat{\rho}-\hat{\varrho}|\,,$$

其中

$$|\hat{A}|=\sqrt{\hat{A}\hat{A}^{\dagger}}.$$

可以证明在保持迹不变、完备的量子操作下迹距离不会增大。另一个常用的判据是**fidelity**，定义为

$$F(\hat{\rho},\hat{\varrho})=\left(\mathrm{tr}\sqrt{\hat{\rho}^{\frac{1}{2}}\hat{\varrho}\hat{\rho}^{\frac{1}{2}}}\right)^{2}=\left(\mathrm{tr}\sqrt{\hat{\varrho}^{\frac{1}{2}}\hat{\rho}\hat{\varrho}^{\frac{1}{2}}}\right)^{2},$$

如果其中一个是纯态，则

$$F(\,|\psi\rangle\langle\psi|\,,\hat{\rho})=\langle\psi|\hat{\rho}|\psi\rangle\,.$$

Fidelity在保迹量子操作

6.1 Bloch球上的操作

本节讨论单量子比特上的量子操作。一般的幺正变换不会减少一个态的纯度，但是量子操作可以，因此一般的幺正变换只是对Bloch球做旋转，而量子操作还可以让它伸缩、平移，变成一个椭球。量子操作也可以破坏纠缠。

例如我们有

$$\frac{1}{4}(X\rho X+Y\rho Y+Z\rho Z+\rho)=\frac{1}{2}I, \tag{43}$$

即我们将一个任意的混合态变换成一个经典$1/2-1/2$概率的态。

如果两个态其中有一个是纯态，那么我们有

$$F(\hat{\rho},\hat{\varrho})= \tag{44}$$

6.1.1 比特翻转

比特翻转是一种简单的量子操作，也是一种噪声的形式。

6.1.2 态的间距

6.2 量子表征

7 量子纠错

量子纠错的一个挑战在于不可克隆定理，从而，不可能通过朴素的冗余比特来做到纠错。测量还会不可避免地破坏量子态，因此需要想出一种办法来“诊断”什么样的错误发生了。最后，环境噪声会造成连续的变化（因为量子态的各个分量是连续变化的），因此错误本身就很难辨别。但这并不意味着量子纠错是不可能的。本节将指出，只要有足够多的量子比特，量子纠错理论上总是可行的。

7.1 比特翻转纠错

本节讨论一种能够纠正比特翻转的量子纠错编码。假定系统中的主要扰动是比特翻转，我们将用三个物理比特代表一个逻辑比特，即

$$|1_{\mathrm{L}}\rangle = |111\rangle\,, \quad |0_{\mathrm{L}}\rangle = |000\rangle\,. \tag{45}$$

我们假定凡不是$|000\rangle$和$|111\rangle$的态都是$|000\rangle$和$|111\rangle$经过单次比特翻转而产生的。（如果多次翻转非常常见，那么需要更多物理比特）因此，我们可以用下面的算符做一次投影测量：

$$P_0 = |000\rangle\langle 000| + |111\rangle\langle 111|\,, \tag{46}$$

测量并不会将逻辑比特的信息抹除，但是可以估计是否发生了比特翻转，以及发生在了哪里，因此被称为**症状测量**。然后根据测量结果做纠正即可。症状测量还带来了一个额外的好处。例如，如果比特翻转为

$$|0\rangle \longrightarrow a\,|0\rangle + b\,|1\rangle\,,$$

则经过测量后它塌缩到$|0\rangle$上（此时无需进一步操作）或者塌缩到$|1\rangle$上（此时需要纠错，但是待纠正的错误是一个离散的错误，即0被翻转为1）。

因此，通过症状测量，量子纠错的三个困难全部被克服了：我们无需真的复制任意的比特，只需要能够制备冗余的比特即可；症状测量可以避免破坏逻辑比特；症状测量可以将连续的错误转化为离散的。

比特翻转纠错的一种