量子信息与量子密码

Quantum Information & Quantum Cryptology

[第6次课] 量子纠错码

授课教师：杨理

授课时间：2021年4月11日

内容概要

一、 编码理论基本概念

二、 量子纠错码

一、 编码理论基本概念

1. 编码过程 $\mathcal{E}$ 是 m 位二进制数到 n 位二进制数的转换：

$\mathcal{E}$： $B^m \to B^n$ ，译码过程为 $\mathcal{D}$： $B^n \to B^m$ 。

$W=(w_1,w_2,\cdots w_n)$ 是 n 位二元码，即 $w_i \in \{0,1\}$， 接收端收到的是 $R=r_1,r_2,\cdots r_n$， 设 $R=W\oplus E$，（$\oplus$：模2加法）。

这里使用的加法是“按位加”，其中 $E=e_1,e_2,\cdots e_n$． 显然：

$$e_i=\begin{cases}0, & w_i=r_i \\ 1, & w_i\neq r_i\end{cases}.$$

易知：$W=R\oplus E$，其中 $E=W\oplus R$ 为错误矢量。

编码理论基本概念

设 $A=a_1,a_2,\cdots a_n\in \mathrm{B}^n$ ，$B=b_1,b_2,\cdots,b_n\in \mathrm{B}^n$

令 $W(A)$ 为 A 的权(Hamming重量)，即：为1的分量的个数。

$d(A,B)=w(A\oplus B)$ 称为 A 与 B 的距离（Hamming距离）。

引理：若 $A,B,C\in \mathrm{B}^n$，则

(1) $d(A,B)=d(B,A)$

(2) $d(A,C)\le d(A,B)+d(B,C)$ （+：普通加法）

证(1) $d(A,B)=w(A\oplus B)=w(B\oplus A)=d(B,A)$.

编码理论基本概念

(2) 定义 $d(a_i,b_i)=\begin{cases}0, & b_i=a_i\\ 1, & b_i\neq a_i\end{cases}$;

则 $d(a_i,c_i)\leq d(a_i,b_i)+d(b_i,c_i)$

所以有 $d(A,C)=\sum_{i=1}^{n}d(a_i,c_i)\leq\sum_{i=1}^{n}d(a_i,b_i)+\sum_{i=1}^{n}d(b_i,c_i)$

$$=d(A,B)+d(B,C)$$

编码理论基本概念

定理： 一组码可以检出 k 个错误的充要条件是这组码的码字间最短距离至少为 $k+1$.

证：$\varepsilon : \mathrm{B}^m \to \mathrm{B}^n, A \in \mathrm{B}^n$ 是码字，传输后接收到 R，$E = A \oplus R$，$w(E) = d(A,R)$. 错误 E 可被检出的充要条件：R 不是码字。因此, $w(E) \le k$ 的所有误差可被检出的充要条件是不存在码字 $B \neq A$ 满足：

$$d(A,B) \le k.$$

即：任意两个不同码字间的距离 d 至少为 $k+1$.

编码理论基本概念

定理：已知一组编码的任意两码字的最短距离为 $2k+1$，则所有权不超过 k 的误差可得到纠正。

证：设 A 是一个码字，在传输过程中发生误差，接收到的为 R， $d(A,R)\le k$.

如果有码字 B 在传输过程中也接收到 R ,且 $d(B,R)\le k$,

则有 $d(A,B)\le d(A,R)+d(B,R)\le k+k<2k+1$,

编码理论基本概念

即： 两码字 A 和 B 之间的距离小于 $2k+1$，与定理假设矛盾，故知：不可能在权不超过 k 的误差下，两不同码字在接收端相同。所以，所有权不超过 k 的误差可得到纠正。

（注意：考虑信道发生随机错误时，此处优先考虑较大概率事件。思考题：为什么？）

编码理论基本概念

2. 线性码

生成矩阵和校验矩阵。

取矩阵 $G=\left(g_{ij}\right)_{mn}$， 取编码过程为 $\mathcal{E}: W = AG$，

其中 $A=\left(a_1,a_2,\cdots,a_m\right)\in \mathrm{B}^m$， 则称 G 为生成矩阵。

例如：

$$G=\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}, A=\left(0\,1\,1\right),$$

编码理论基本概念

对应有码字：

$$W=(0\,1\,1)\begin{pmatrix}1&0&0&1&1&0\\0&1&0&0&1&1\\0&0&1&1&0&1\end{pmatrix}=(0\,1\,1\,1\,1\,0).$$

特别是，若取生成矩阵

$$G=\begin{pmatrix}1&0&0&\cdots&0&g_{1,m+1}&g_{1,m+2}&\cdots&g_{1,n}\\0&1&0&\cdots&0&g_{2,m+1}&g_{2,m+2}&\cdots&g_{2,n}\\0&0&1&\cdots&0&g_{3,m+1}&g_{3,m+2}&\cdots&g_{2,n}\\\vdots&\vdots&\vdots&\ddots&\vdots&\vdots&\vdots&\ddots&\vdots\\0&0&0&\cdots&1&g_{m,m+1}&g_{m,m+2}&\cdots&g_{m,n}\end{pmatrix},$$

编码理论基本概念

则有码字：

$$W = AG = (a_1, a_2, \cdots, a_m)\begin{pmatrix} 1 & 0 & \cdots & 0 & g_{1,m+1} & \cdots & g_{1,n} \\ 0 & 1 & \cdots & 0 & g_{2,m+1} & \cdots & g_{2,n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & g_{m,m+1} & \cdots & g_{m,n} \end{pmatrix}$$

$$= (w_1, w_2, \cdots, w_n).$$

显然有：(1) $w_1 = a_1, w_2 = a_2, \cdots, w_m = a_m$.

(2) $w_j = a_1 g_{1,j} + \cdots + a_m g_{m,j}$.

编码理论基本概念

由(1)、(2)有： $$w_{m+j}=g_{1,m+j}w_1+g_{2,m+j}w_2+\cdots+g_{m,m+j}w_m \qquad (3)$$

$$j=1,\cdots,n-m,$$

码字的各位满足上述关系，可用于校验。

码字： n 位 $=$ m 位 $+$ $n-m$ 位

（信息位）（校验位，偶校验）

例如：$G=\begin{pmatrix}1&0&0&1&1&0\\0&1&0&0&1&1\\0&0&1&1&0&1\end{pmatrix}$, $\left(a_1,a_2,a_3\right)G=\left(w_1,w_2,\cdots,w_6\right)$

编码理论基本概念

则有
$$\begin{cases} w_1 + w_3 + w_4 = 0 \quad (w_4 = w_1 + w_3) \\ w_1 + w_2 + w_5 = 0 \\ w_2 + w_3 + w_6 = 0 \end{cases}$$

可得：
$$\begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_6 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

编码理论基本概念

一般情况有

$$\left.\begin{aligned}
g_{1,m+1}w_1 + g_{2,m+1}w_2 + \cdots + g_{m,m+1}w_m + w_{m+1} &= 0 \\
g_{1,m+2}w_1 + g_{2,m+2}w_2 + \cdots + g_{m,m+2}w_m + w_{m+2} &= 0 \\
\cdots\cdots \\
g_{1,n}\ w_1 + g_{2,n}\ w_2 + \cdots + g_{m,n}\ w_m + w_n &= 0
\end{aligned}\right\} \quad \text{(即 (3) 式)}$$

编码理论基本概念

可写成：$HW^T = 0$，其中$W = AG$，

$$H = \begin{pmatrix} g_{1,m+1} & g_{2,m+1} & \cdots & g_{m,m+1} & 1 & 0 & 0 & \cdots & 0 \\ g_{1,m+2} & g_{2,m+2} & \cdots & g_{m,m+2} & 0 & 1 & 0 & \cdots & 0 \\ & \cdots & \cdots & & \vdots & & & \ddots & 0 \\ g_{1,n} & g_{2,n} & \cdots & g_{m,n} & 0 & 0 & 0 & \cdots & 1 \end{pmatrix}_{(n-m)\times n}$$

H 称为对应于生成矩阵 G 的校验矩阵。已知 G 可求得 H，反之亦然。

编码理论基本概念

校验矩阵 H 可用于纠正一位错误。例如：

$$H=\begin{pmatrix}1&0&1&1&0&0\\1&1&0&0&1&0\\0&1&1&0&0&1\end{pmatrix}, R=\begin{pmatrix}1&0&0&1&0&1\end{pmatrix}.$$

则 $HR^T=\begin{pmatrix}0\\1\\1\end{pmatrix}\neq\begin{pmatrix}0\\0\\0\end{pmatrix}$, R 不是码字，设 $R=W+E$，则：

$$HR^T=HW^T+HE^T=HE^T,$$

编码理论基本概念

若 $E = \underbrace{(0 \cdots 0\,1\,0 \cdots 0)}_{\text{第i个为1，其余为0}}$，则 HE^T 必是矩阵 H 的第 i 列，

故根据 $HE^T = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$， 知第二位出错，纠正得 $W = (110101)$， 取

信息位得 $A = (110)$.

若出现两个错误，则不能正确译码。

编码理论基本概念

译码步骤：接收到 $R=(r_1,r_2,\cdots,r_n)$.

(1) 计算校正子 $s=HR^T$.

(2) 若 $s=0$, 确认原信息即为 $(r_1,r_2,\cdots,r_m)$.

若 $s\neq 0$, 则进行(3)。

(3) 若 s 是 H 的第 i 列，则认为 R 在第 i 位出错，可纠正得 R_1 ,

取 R_1 的前 m 位作为信息。

若 s 不为 H 的某一列，则认为至少出现两个错误，不能正确译码。

编码理论基本概念

定理： 校验矩阵 $H=\left(h_{ij}\right)_{(n-m)\times n}$ 能纠正一个错误的充要条件是 H 的各列互不相同且非零。

证： 充分性显然成立，现证必要性。

① 若 H 的第 i 列为零向量，对于第 i 位出错的情形，有 $H\left(W+E\right)^T=HE^T=0$，不能正确译码。

② 若 H 的第 i 列和第 j 列相同，则第 i 位和第 j 位的错误将无法区分，而且，两位都出错时，将误以为传输正确。

编码理论基本概念

定理： 设 $A=\left(a_{ij}\right)_{m\times(n-m)}$ 是 $(0,\ 1)$矩阵，若以矩阵 $G=\left(I_m \vdots A\right)$ 为生成矩阵，则对应的校验矩阵为 $H=\left(A^T \vdots I_{n-m}\right)$，其中 I_m 为 m 维的单位矩阵。

编码理论基本概念

3. Hamming码（1950年）

编译码器简单，构造容易，使用普遍。

构造 $(n-m)\times n$ 校验矩阵 $H=(h_{ij})$ 如下：

令 $l=n-m$ 为列向量的维数（即行数），则可得 2^l-1 个不同的非零列向量，将其排成 $(n-m)\times n$ 矩阵 H_l，使后面 l 列恰好构成 I_l。这种校验矩阵对应的纠错码即为Hamming码。

问：Hamming码的生成矩阵如何构造？

编码理论基本概念

例如：

$$H_3=\begin{pmatrix}0&1&1&1&1&0&0\\1&0&1&1&0&1&0\\1&1&0&1&0&0&1\end{pmatrix}.\quad A_{4\times3}\to G_{4\times7}$$，把4位编成7位.

$$H_4=\begin{pmatrix}1&1&1&0&0&0&1&1&1&0&1&1&0&0&0\\1&0&0&1&1&0&1&1&0&1&1&0&1&0&0\\0&1&0&1&0&1&1&0&1&1&1&0&0&1&0\\0&0&1&0&1&1&0&1&1&1&1&0&0&0&1\end{pmatrix}$$

$A_{11\times4}\to G_{11\times15}$把11位编成15位.

作业：①生成矩阵 $G=?$　②可纠正几位错误？

编码理论基本概念

以上我们讲到了纠错编码的基本思想（一致检验），和基本的方法（生成矩阵、校验矩阵），现在来介绍编码理论的几个概念：

1、**完全码**：一个极小距离为 $2k+1$ 的码称为完全码，如果每个向量都恰与一个码字之间的距离 $\leq k$。

Hamming码是完全码。

2、**线性码**：一个线性码 C 是一个线性子空间。若 C 的维数是 m，则说 C 是一个$[n,m]$码。

编码理论基本概念

线性码的生成矩阵 G 是一个$m\times n$ 矩阵，其行向量是 C 的一组基。

如果 $G=\left(I_m, A\right)$，则称 G是标准型的。

3、对偶码： 设 C是 $[n,m]$ 码，我们定义对偶码 $C^{\perp}$ 为：

$$C^{\perp}\equiv\left\{y\,\middle|\,y\in F_2^{(n)}\text{ satisfies: for any }x\in C,\,x_1y_1\oplus x_2y_2\oplus\cdots\oplus x_ny_n=0\right\}.$$

当 $C=C^{\perp}$ 时，我们称 C 是自对偶码。

若 $G=\left(I_m, A\right)$是码 C 的标准型生成矩阵，那么 $H=\left(A^T, I_{n-m}\right)$ 是 $C^{\perp}$ 的生成矩阵。

二、 量子纠错码

1. 所面临的问题

(1) 错误类型不同：除比特反转外，还有相位反转：

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|0\rangle - \beta|1\rangle .$$

(2) 纠错过程不能直接对数据态进行测量，也不能简单复制。

2. 一个简单的例子：纠正一位比特反转错误的方法

$$|\psi\rangle \rightarrow \left(\alpha|0\rangle + \beta|1\rangle\right)|0\rangle|0\rangle \rightarrow \alpha|000\rangle + \beta|111\rangle$$

量子纠错码

可通过测量 $y \oplus z$ 和 $x \oplus z$ 来确定反转的比特，然后加以纠正（解决第二个问题）。

关键：由于 $|000\rangle$ 和 $|111\rangle$ 两叠加分量的每一位均相反，因而当取两位做加法时，不同叠加分量的结果一定相同，不论是否出错。这使我们可以纠正叠加态的错误。从下面的图中可看到这一点：

量子纠错码

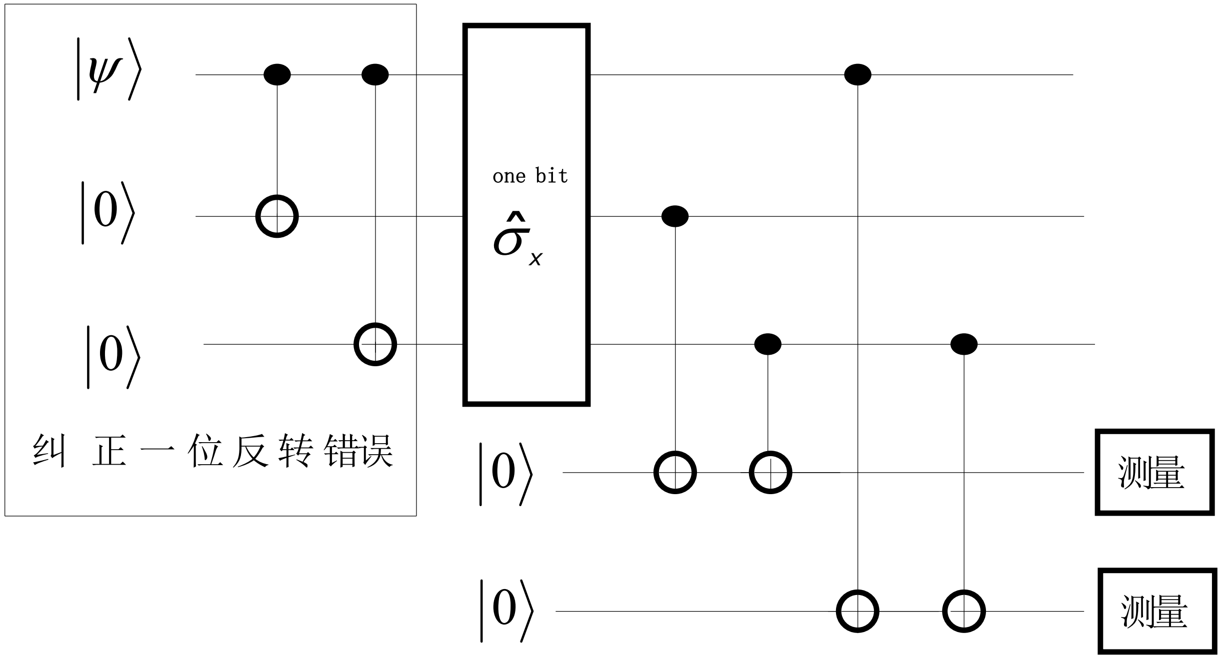
校验子——经典纠错码理论

$\lvert xyz\rangle$	$y\oplus z$	$x\oplus z$	出错位
$\lvert 000\rangle$	0	0	0
$\lvert 100\rangle$	0	1	1
$\lvert 010\rangle$	1	0	2
$\lvert 001\rangle$	1	1	3
$\lvert 111\rangle$	0	0	0
$\lvert 011\rangle$	0	1	1
$\lvert 101\rangle$	1	0	2
$\lvert 110\rangle$	1	1	3

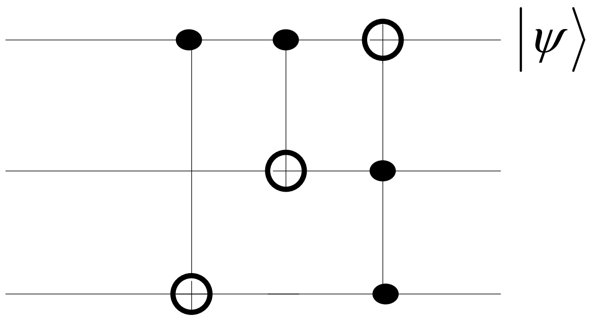
量子纠错码

编译码量子线路

编码线路



量子纠错码



恢复线路（不必依据前面测量结果）

量子纠错码

前述译码线路实现了：

① 第一位错误：$\alpha|100\rangle+\beta|011\rangle$

$$\rightarrow\alpha|011\rangle+\beta|111\rangle=\left(\alpha|0\rangle+\beta|1\rangle\right)|11\rangle,$$

② 第二位错误：$\alpha|010\rangle+\beta|101\rangle$

$$\rightarrow\alpha|010\rangle+\beta|110\rangle=\left(\alpha|0\rangle+\beta|1\rangle\right)|10\rangle,$$

③ 第三位错误：$\alpha|001\rangle+\beta|110\rangle$

$$\rightarrow\alpha|001\rangle+\beta|101\rangle=\left(\alpha|0\rangle+\beta|1\rangle\right)|01\rangle.$$

④ 无错误：$\alpha|000\rangle+\beta|111\rangle$

$$\rightarrow\alpha|000\rangle+\beta|100\rangle=\left(\alpha|0\rangle+\beta|1\rangle\right)|00\rangle.$$

量子纠错码

3、纠正相位错误 $\alpha|000\rangle+\beta|111\rangle$

$$\xrightarrow{H^{(3)}}\frac{1}{2\sqrt{2}}\Big[\alpha\big(|\bar{0}\rangle+|\bar{1}\rangle\big)\big(|\bar{0}\rangle+|\bar{1}\rangle\big)\big(|\bar{0}\rangle+|\bar{1}\rangle\big)$$

$$+\beta\big(|\bar{0}\rangle-|\bar{1}\rangle\big)\big(|\bar{0}\rangle-|\bar{1}\rangle\big)\big(|\bar{0}\rangle-|\bar{1}\rangle\big)\Big],$$

送入信道，第一位相位反转 $\rightarrow\frac{1}{2\sqrt{2}}\Big[\alpha\big(|\bar{0}\rangle-|\bar{1}\rangle\big)\big(|\bar{0}\rangle+|\bar{1}\rangle\big)\big(|\bar{0}\rangle+|\bar{1}\rangle\big)$

$$+\beta\big(|\bar{0}\rangle+|\bar{1}\rangle\big)\big(|\bar{0}\rangle-|\bar{1}\rangle\big)\big(|\bar{0}\rangle-|\bar{1}\rangle\big)\Big]$$

$$\xrightarrow{H^{(3)}}\alpha|100\rangle+\beta|011\rangle.$$

$$\xrightarrow{\text{译码线路}}\big(\alpha|0\rangle+\beta|1\rangle\big)|11\rangle$$

量子信道错误：系统与环境纠缠；对抗量子信道错误：以纠缠对抗纠缠。问题：如何同时对抗反转错误和相位错误？

量子纠错码

Shor 码：

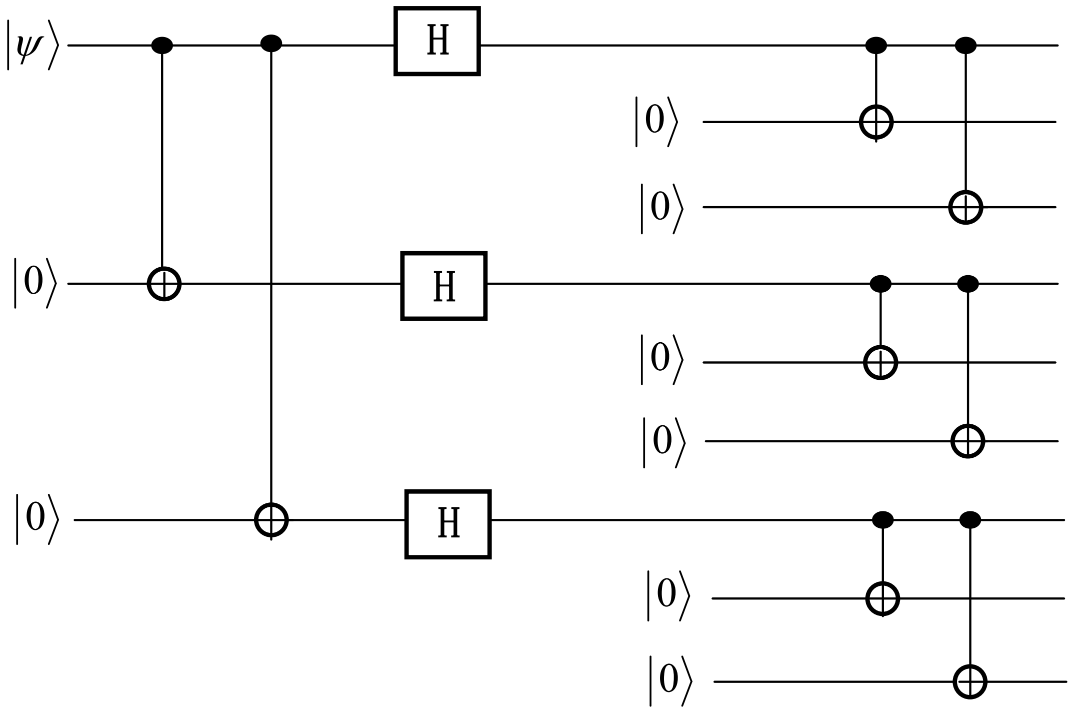
$$\alpha|0\rangle+\beta|1\rangle\rightarrow\alpha|0_L\rangle+\beta|1_L\rangle,$$

$$其中|0_L\rangle\equiv\frac{(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)}{2\sqrt{2}}$$

$$|1_L\rangle\equiv\frac{(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)}{2\sqrt{2}}$$

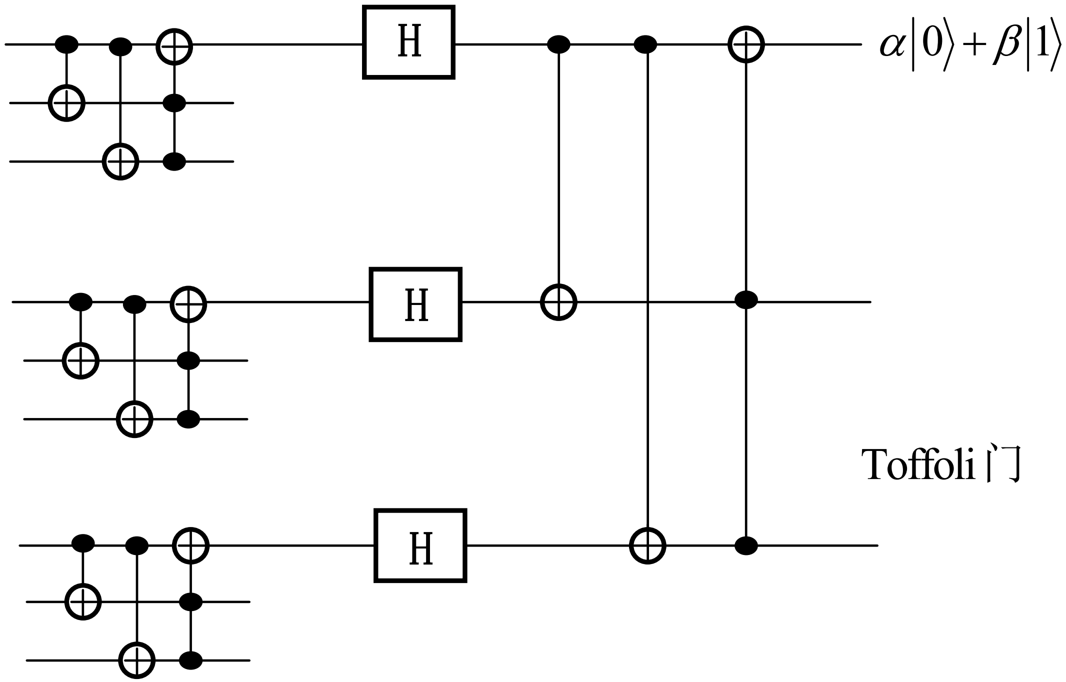
量子纠错码

Shor码的编码线路：



量子纠错码

Shor 码的译码线路：



量子纠错码

CSS量子纠错码

基：$\begin{cases}|0\rangle \\ |1\rangle\end{cases}$

共轭基：$\begin{cases}|\bar{0}\rangle \\ |\bar{1}\rangle\end{cases}$.　　对偶码：$G, H$ 互换生成的码。

1、定理：在一组基下经典线性纠错码 C 的所有码字的等权重叠加态，是其共轭基下 C 的对偶码 $C^{\perp}$ 的所有码字的等权重叠加态。

量子纠错码

主要用到：

$$H^{(n)}|x\rangle = \frac{1}{2^{n/2}}\sum_{y=0}^{2^n-1}(-1)^{x\cdot y}|y\rangle .$$

易见：

$$\sum_{x=0}^{2^n-1}(-1)^{x\cdot y} = \begin{cases} 2^n, & 当\ \ y=(0,\cdots,0). \\ 0, & 当\ \ y\neq(0,\cdots,0). \end{cases}$$

证明： 练习题。

量子纠错码

定理证明：基 $\{|0\rangle,|1\rangle\}$ 下码 C 等权重叠加：$|C\rangle=\dfrac{1}{2^{m/2}}\sum\limits_{v\in c}|v\rangle$.

在共轭基 $\{|\bar{0}\rangle,|\bar{1}\rangle\}$ 下，

$$|s\rangle=H^{(n)}|C\rangle=\frac{1}{2^{m/2}}\sum_{v\in C}H^{(n)}|v\rangle$$

$$=\frac{1}{2^{m/2}}\sum_{v\in C}\frac{1}{2^{n/2}}\sum_{w=0}^{2^n-1}(-1)^{v\cdot w}|w\rangle$$

$$\overset{\text{利用}v=aG}{=}\frac{1}{2^{(n+m)/2}}\sum_{w=0}^{2^n-1}\sum_{a=0}^{2^m-1}(-1)^{(aG)\cdot w}|w\rangle,$$

量子纠错码

$$(aG)\cdot w = aGw^T = a\cdot\left(Gw^T\right)^T$$

由于 G 是 $C^\perp$ 的校验矩阵，故知 $Gw^T = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ 当且仅当 $w \in C^\perp$.

所以有 $|s\rangle = \dfrac{1}{2^{(n+m)/2}} \sum_{w\in C^\perp} 2^m |w\rangle = \dfrac{1}{2^{(n-m)/2}} \sum_{w\in C^\perp} |w\rangle$.

即：$|s\rangle$ 在共轭基下看是 $C^\perp$ 中各码字的等权重叠加。

量子纠错码

2、 CSS码

$C_2 \subset C_1$， C_1, C_2 为线性码，C_2 为 C_1 的 K 阶子码，即 C_2 在 C_1 中不同陪集的 数目有 2^K 个。

对偶码：由校验矩阵作为生成矩阵所生成的码。维数 $n-m$.

量子纠错码

构造CSS码，涉及四个经典纠错码：

$$\begin{array}{ccc} C_2\left(n, m-K, \geq d_1\right) & \subset & C_1\left(n, m, d_1\right) \\ \updownarrow \perp & & \updownarrow \perp \\ C_2^{\perp}\left(n, n-m+K, d_2\right) & \supset & C_1^{\perp}\left(n, n-m, \geq d_2\right) \end{array}$$

可编码 K 量子位。

$$\left|C_w\right\rangle = \frac{1}{2^{(n-m)/2}} \sum_{v \in C_1^{\perp}} \left|w+v\right\rangle, \quad w \in C_2^{\perp} \setminus C_1^{\perp}.$$

量子纠错码

① 由于 $\{|C_w\rangle\}$ 都是由 $C_2^{\perp}$ 中的码字对应的量子态叠加而成，故可纠正 $\frac{1}{2}(d_2-1)$ 个位反转错误；只有当 $w=(0,\cdots,0)$ 时，$|C_w\rangle$ 才是由 $C_1^{\perp}$ 中元素对应的量子态叠加而成，其它情况都是 $C_1^{\perp}$ 的某个陪集中的元素所对应的量子态叠加而成。

② 由于在共轭基下 $|C_w\rangle=\frac{1}{2^{m/2}}\sum_{v\in C_1}(-1)^{w\cdot v}|v\rangle$

故在共轭基下 $\{|C_w\rangle\}$ 又可看成是由 C_1 中码字对应的量子态叠加而成，故可纠正 $\frac{1}{2}(d_1-1)$ 个相位反转错误。

量子纠错码

$$C_2 \subset C_1$$

$$\downarrow ?$$

$$C_2^{\perp} \supset C_1^{\perp}$$

即：由 $C_2 \subset C_1$ 可推出 $C_2^{\perp} \supset C_1^{\perp}$?

证明：由 $C_2 \subset C_1$ 知 $H_1 (a\, G_2)^T = 0$ 即：$H_1\, G_2^T\, a^T = 0$,

由 a 的任意性，知 $H_1\, G_2^T = 0$, 而 $C_1^{\perp}$ 中码字为 $b\, G_1^{\perp} = b\, H_1$,

故知 $H_2^{\perp} (b\, H_1)^T = G_2\, H_1^T\, b^T = \left(H_1\, G_2^T \right)^T b^T = 0$,

即： $C_1^{\perp}$ 中码字都属于 $C_2^{\perp}$， $C_1^{\perp}$ 是 $C_2^{\perp}$ 的子码。

量子纠错码—— CSS 码

$$C_2[7,3,4] \subset C_1[7,4,3]$$

$$\Updownarrow\perp \qquad\qquad \Updownarrow\perp$$

$$C_2^{\perp}[7,4,3] \supset C_1^{\perp}[7,3,4]$$

极特殊： $C_2^{\perp}=C_1$，$C_1^{\perp}=C_2$，可纠一位错。

$$\left|\bar{0}\right\rangle_L=\frac{1}{2^{3/2}}\Big(|0000000\rangle+|0011101\rangle+|0100111\rangle+|0111010\rangle$$

$$+|1001110\rangle+|1010011\rangle+|1101001\rangle+|1110100\rangle\Big),$$

为偶重码字对应的量子态之和。

量子纠错码—— CSS 码

$$\left|\bar{1}\right\rangle_L = \frac{1}{2^{3/2}}\left(\left|1111111\right\rangle + \left|1100010\right\rangle + \left|1011000\right\rangle + \left|1000101\right\rangle\right.$$

$$\left. + \left|0110001\right\rangle + \left|0101100\right\rangle + \left|0010110\right\rangle + \left|0001011\right\rangle\right).$$

为奇重码字对应的量子态之和——作关于w=(1111111)的陪集，故：

共轭基下 $$\left|1\right\rangle_L = \frac{1}{\sqrt{2^4}}\sum_{v\in C_1}(-1)^{w\cdot v}\left|v\right\rangle = \frac{1}{4}\sum_{v\in C_1}(-1)^{\sum_i v_i}\left|v\right\rangle$$

$$= \frac{1}{4}\left(\sum_{v\in C_1,\text{偶重}}\left|v\right\rangle - \sum_{v\in C_1,\text{奇重}}\left|v\right\rangle\right).$$

量子纠错码—— CSS 码

$$|0\rangle_L = \frac{1}{4}\sum_{v\in C_1}|v\rangle = \frac{1}{4}\left(\sum_{v\in C_1,\text{偶重}}|v\rangle + \sum_{v\in C_1,\text{奇重}}|v\rangle\right)$$

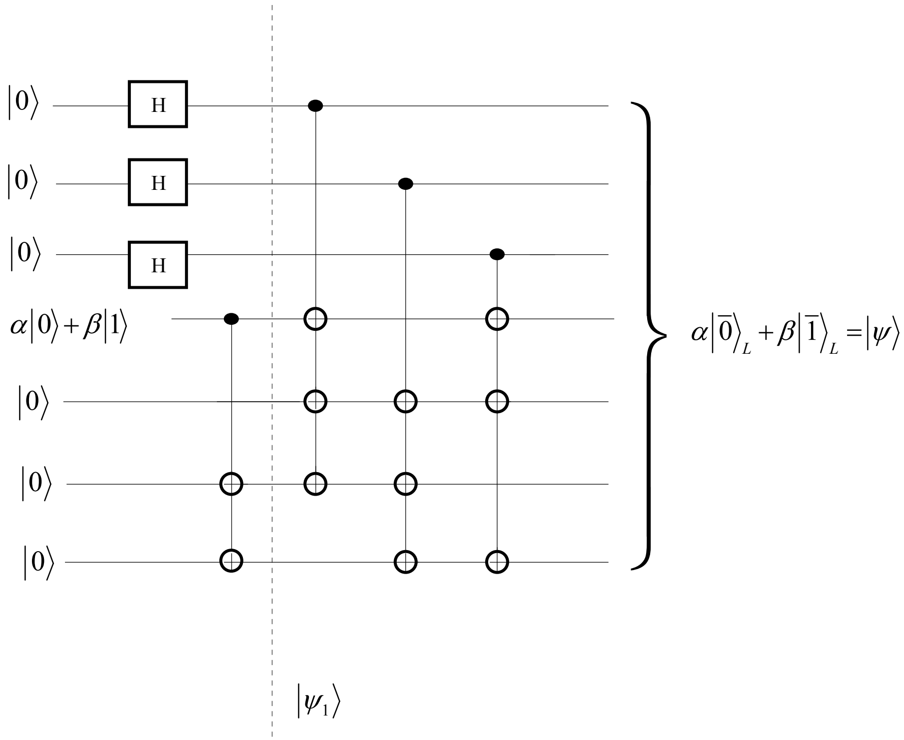
即：$|0\rangle_L = \frac{1}{\sqrt{2}}\left(|\overline{0}\rangle_L + |\overline{1}\rangle_L\right), |1\rangle_L = \frac{1}{\sqrt{2}}\left(|\overline{0}\rangle_L - |\overline{1}\rangle_L\right).$

量子纠错码—— Steane 码

编码线路

$$
\begin{aligned}
&|000\rangle\left(\alpha|0\rangle+\beta|1\rangle\right)|000\rangle\\
&\left.\begin{aligned}
&\to\frac{1}{2\sqrt{2}}\alpha\left|(0+1)(0+1)(0+1)0000\right\rangle\\
&+\frac{1}{2\sqrt{2}}\beta\left|(0+1)(0+1)(0+1)1011\right\rangle
\end{aligned}\right\}|\psi_1\rangle\\
&\to\alpha\left|\overline{0}\right\rangle_L+\beta\left|\overline{1}\right\rangle_L .
\end{aligned}
$$

量子纠错码—— Steane 码



量子纠错码—— Steane 码

编码线路的解释：

$$
\begin{aligned}
|\psi\rangle &= \alpha\left|\overline{0}\right\rangle_L + \beta\left|\overline{1}\right\rangle_L \\
&= \alpha \sum_{v\in C[7,3,4]} |v\rangle + \beta \sum_{v\in\ C[7,3,4]\text{在}C[7,4,3]\text{中的陪集}} |v\rangle
\end{aligned}
$$

量子纠错码—— Steane 码

因此必须生成一个在 $C[7,4,3]$ 中但不在 $C[7,3,4]$ 中的码字。

线路中后面三列控制变换对应于

$$G[7,3,4]=\begin{bmatrix}1&0&0&1&1&1&0\\0&1&0&0&1&1&1\\0&0&1&1&1&0&1\end{bmatrix}$$

的三行，将态 $(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)|0\rangle|0\rangle|0\rangle|0\rangle$ 变换为 $\sum_{v\in C[7,3,4]}|v\rangle$，

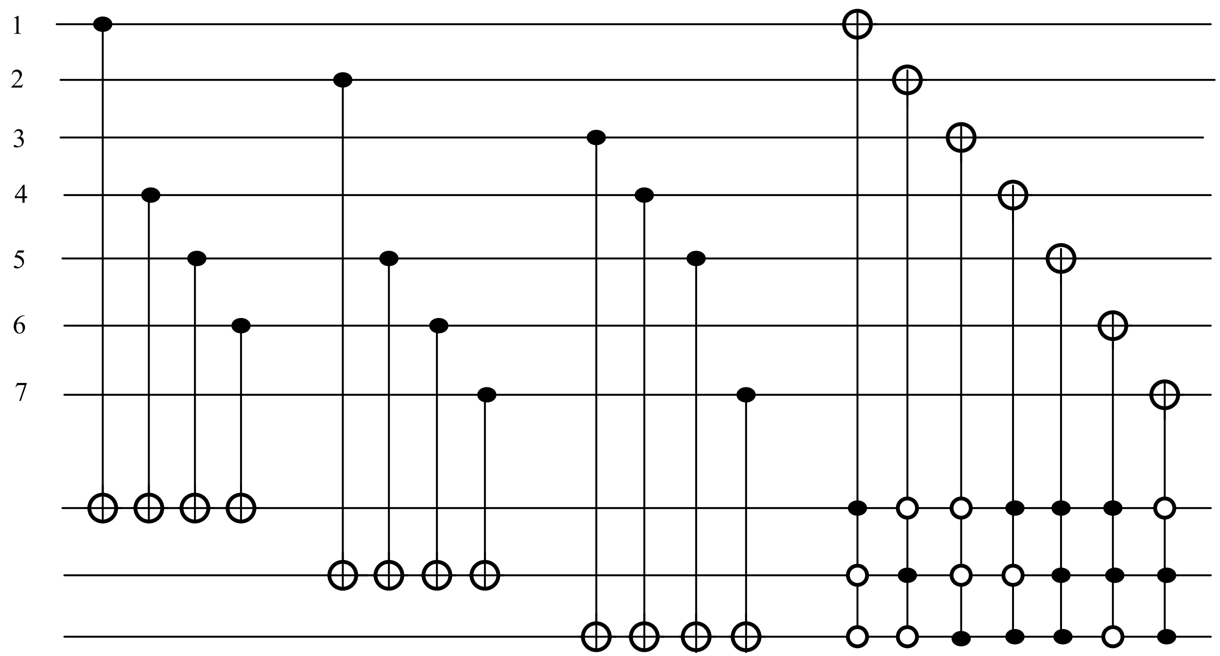
将态 $(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)|1011\rangle$ 变换为

$$\sum_{v\in C[7,3,4]}\left|v\oplus(0001011)\right\rangle=\sum_{\substack{v\in C[7,3,4]\text{在}C[7,4,3]\text{中的}\\ \text{由}0001011\text{生成的陪集}}}|v\rangle,$$

量子纠错码——CSS码的译码线路

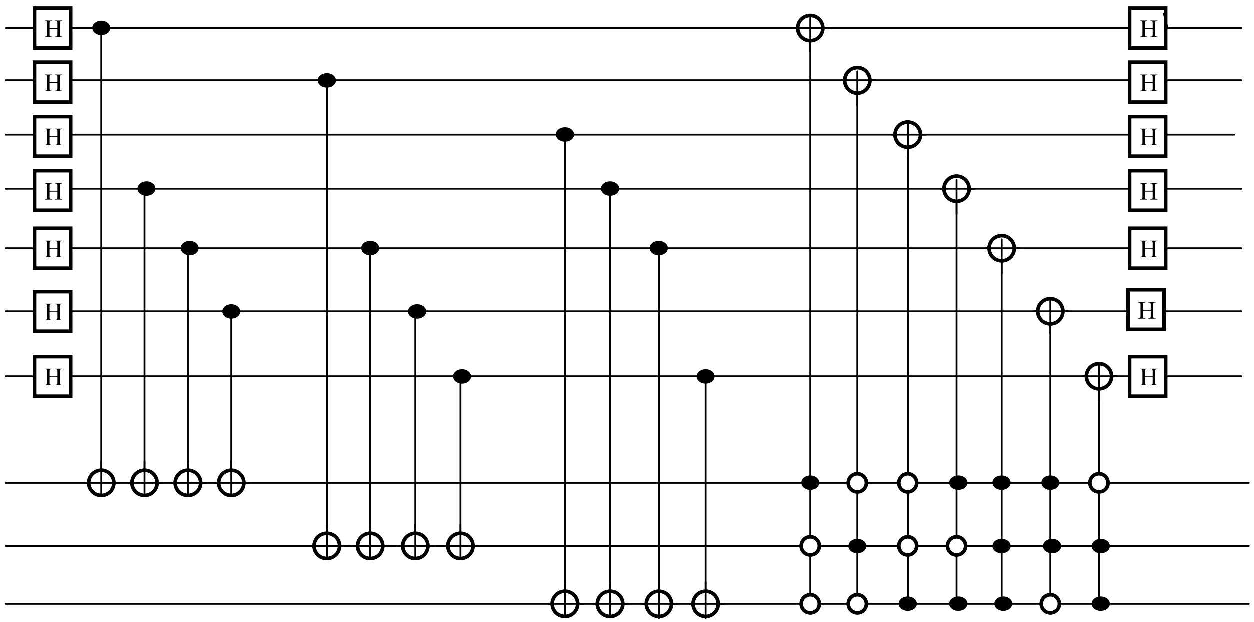
Steane码的译码线路（不考虑容错问题）：

(1)在基 $\{|0\rangle,|1\rangle\}$ 下，纠位反转错误。利用 C_1 码，$H(7,4,3)=\begin{bmatrix}1001110\\0100111\\0011101\end{bmatrix}$



量子纠错码——CSS码的译码线路

(2)在共轭基下纠相位反转错误：利用 $C_2^{\perp}[7,4,3]$ 的 $H(7,4,3)=\begin{bmatrix}1001110\\0100111\\0011101\end{bmatrix}$.



量子纠错码——CSS码的译码线路

(3)编码线路逆用： $G(7,3,4)=\begin{bmatrix}1001110\\0100111\\0011101\end{bmatrix}.$

$$|C_w\rangle=\frac{1}{2^{(n-m)/2}}\sum_{v\in C_1^{\perp}}|w+v\rangle$$

$$\to H^{(n)}|C_w\rangle=\frac{1}{2^{(n-m)/2}}\sum_{v\in C_1^{\perp}}\frac{1}{2^{n/2}}\sum_{w'=0}^{2^n-1}(-1)^{(w+v)\cdot w'}|w'\rangle$$

$$=\frac{1}{2^{(n-m)/2}}\cdot\frac{1}{2^{n/2}}\sum_{w'=0}^{2^n-1}(-1)^{w\cdot w'}\sum_{a=0}^{2^{(n-m)}-1}(-1)^{(aH_1)\cdot w'}|w'\rangle=\frac{1}{2^{(n-m)/2}}\cdot\frac{1}{2^{n/2}}\cdot\sum_{w'\in C_1}(-1)^{w\cdot w'}2^{n-m}|w'\rangle$$

$$=\frac{2^{(n-m)/2}}{2^{n/2}}\sum_{v\in C_1}(-1)^{w\cdot v}|v\rangle=\frac{1}{2^{m/2}}\sum_{v\in C_1}(-1)^{w\cdot v}|v\rangle.$$

此式为CSS码的基础！

量子纠错码——CSS码的译码线路

上式推导中利用了H_1为$C_1^{\perp}$的生成矩阵；H_1为C_1的校验矩阵；

$(a H_1)\cdot w' = a H_1 w'^T = a\cdot\left(w' H_1^T\right)$。

总之，CSS码思想为：在一组基及其共轭基下，分别纠正比特反转和相位反转错误。

问题：基 $\{|0\rangle,|1\rangle\}$ 下的$|C_w\rangle = \frac{1}{2^{(n-m)/2}}\sum_{v\in C_1^{\perp}}|w+v\rangle$ 在共轭基下是什么？

量子纠错码——CSS码的译码线路

在共轭基下为: $\boxed{\left|C_w\right\rangle = \frac{1}{2^{m/2}}\sum_{v\in C_1}(-1)^{w\cdot v}\left|v\right\rangle}$ ，等概率但不是等系数.

特例: $w=0$

$$\left|C_0\right\rangle = \frac{1}{2^{m/2}}\sum_{v\in C_1}\left|v\right\rangle$$ 等系数叠加.

$$=\frac{1}{\sqrt{2}}\left(\frac{1}{2^{(n-m)/2}}\sum_{v\in C_1,\text{偶重}}\left|v\right\rangle+\frac{1}{2^{(n-m)/2}}\sum_{v\in C_1,\text{奇重}}\left|v\right\rangle\right)$$

$w=\left|1111111\right\rangle$ 时,

$$\left|C_w\right\rangle=\frac{1}{\sqrt{2}}\left(\frac{1}{2^{(n-m)/2}}\sum_{v\in C_1,\text{偶重}}\left|v\right\rangle-\frac{1}{2^{(n-m)/2}}\sum_{v\in C_1,\text{奇重}}\left|v\right\rangle\right)$$

第五章 量子纠错码

Q&A