量子纠错码

林雨轩

February 2025

1 量子纠错的基本思路

三大困难：不可克隆，错误连续，测量破坏量子信息

从测量的角度出发：为了使得测量不破坏信息，必须让发生错误与不发生错误的态分别进入不同测量值的本征空间，这样可以通过测量结果知道进入了哪个子空间，并且不破坏信息，再进行对应的恢复即可。

纠错分为两步：错误探测，恢复

2 Shor 编码

Shor 编码是一种利用 9 个比特维护 1 个逻辑比特 ($|0_L\rangle, |1_L\rangle$) 的编码，可以对抗单量子比特上的任意错误。也就是说，当且仅当这 9 个比特中的某一个发生了某种错误，这套编码能够在整体的信息不被破坏的条件下 ($|0_L\rangle, |1_L\rangle$ 前的系数被维护)，通过错误探测和恢复两个步骤，找出错误的比特并进行改正，使得这 9 个比特回到完美编码状态。

本节中，我们先说明 Shor 编码的有效性，之后将从更深刻的角度理解 Shor 编码。(包括为什么需要 9 个比特，编码空间为什么是 2 维的，为什么针对于单量子比特错误有效等)

2.1 比特翻转

考虑将 $a|0\rangle + b|1\rangle$ 完美编码成 $a|000\rangle + b|111\rangle$。当某一位发生比特翻转错误时 (比如第 1 位)，量子态变为 $a|100\rangle + b|011\rangle$。

如果使用如下四种投影算子进行测量 (投影算子 P 需要满足 $P^2 = I$):

$P_0 = |000\rangle\langle 000| + |111\rangle\langle 111|$; $P_1 = |100\rangle\langle 100| + |011\rangle\langle 011|$;

$P_2 = |010\rangle\langle 010| + |101\rangle\langle 101|$; $P_3 = |001\rangle\langle 001| + |110\rangle\langle 110|$;

当发生第 1 位比特翻转时，测量 P_0, P_2, P_3 的结果均为 0，而测量 P_1 的结果为 1，并且测量后量子态仍然保持为 $a|100\rangle + b|011\rangle$ (注意该测量并没有揭示 a，b 的信息，因而逻辑比特上的信息被维护)。根据测量结果，我们可以推断出是第 1 位比特发生了翻转，进行恢复只需要将第 1 个比特进行翻转 (作用 X 门) 即可。

以上的四个投影算子是我们基于错误的影响构造出来的，事实上我们可以仅使用 2 个由熟悉的逻辑门所构造的测量算符 Z_1Z_2, Z_2Z_3 便能达到相同的目的。

$Z_1Z_2 = (|00\rangle\langle 00| + |11\rangle\langle 11|) \otimes I - (|01\rangle\langle 01| + |10\rangle\langle 10|) \otimes I$

$Z_2Z_3 = I \otimes (|00\rangle\langle 00| + |11\rangle\langle 11|) - I \otimes (|01\rangle\langle 01| + |10\rangle\langle 10|)$

若 Z_1Z_2 的测量结果为 1，则说明前两个比特相同；若 Z_1Z_2 的测量结果为-1，则说明前两个比特相反。再结合 Z_2Z_3 的测量结果，就可以准确定位出究竟发生了何种错误。并且不同测量结果所对应的本征空间完全罩住可能发生错误的量子态，因而有用的信息（a,b）仍然不被破坏。

2.2 相位翻转

相位翻转错误指的是 $a|0\rangle + b|1\rangle$ 变为 $a|0\rangle - b|1\rangle$。

考虑用 $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}, |-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$ 来代替 $|0\rangle, |1\rangle$,

则 $a|0\rangle + b|1\rangle = \frac{a+b}{\sqrt{2}}|+\rangle + \frac{a-b}{\sqrt{2}}|-\rangle, a|0\rangle - b|1\rangle = \frac{a-b}{\sqrt{2}}|+\rangle + \frac{a+b}{\sqrt{2}}|-\rangle$

于是相位翻转错误被转换为了比特翻转错误，同理可知需要相应地将测量算子 Z_1Z_2, Z_2Z_3 改为 X_1X_2, X_2X_3。($X = |0\rangle\langle 1| + |1\rangle\langle 0| = \frac{|+\rangle+|-\rangle}{\sqrt{2}}\frac{\langle+|-\langle-|}{\sqrt{2}} + \frac{|+\rangle-|-\rangle}{\sqrt{2}}\frac{\langle+|+\langle-|}{\sqrt{2}} = |+\rangle\langle+| - |-\rangle\langle-|$)

事实上，我们可以看出以上两个信道是等价的。如果一个信道作用 U 之后再作用 $U^\dagger$ 就成为另一个信道，则称两个信道是酉等价的。以上的 U 实际上就是 H 门，因而恢复信息的操作也应该相应地由 X 门变为 $HXH = Z$。

2.3 Shor 编码

作为一种朴素的直觉，如果将以上两种编码级联起来（先使用相位翻转编码，再把每一位复制 3 遍用以对抗比特翻转错误），则理论上来说，新的编码应该能够同时对抗比特翻转错误和相位翻转错误。

$|0_L\rangle = \frac{(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)}{2\sqrt{2}}, |1_L\rangle = \frac{(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)}{2\sqrt{2}}$

测量算子 $Z_1Z_2, Z_2Z_3, Z_4Z_5, Z_5Z_6, Z_7Z_8, Z_8Z_9$，可以定位出有无比特翻转错误。

对于相位翻转错误，需要注意的是，此时（1,2,3）位，（4,5,6）位，（7,8,9）位中的某一位相位翻转对编码的影响是相同的，因此我们只需定位出前 3 个，中间 3 个以及后 3 个中哪一部分存在相位翻转即可。

测量算子 $X_1X_2X_3X_4X_5X_6, X_4X_5X_6X_7X_8X_9$，可以定位出哪一部分存在相位翻转。

对于某一位同时发生相位翻转与比特翻转的情况，以上操作同样有效。

有意思的是，Shor 编码不仅可以对抗单比特上的 X，Z，XZ 错误，理论上它能够对抗单比特上的任意错误，但是逻辑上略有不同。

任意的单量子错误可以表述为 $E = e_0I + e_1X + e_2Z + e_3XZ$，则被污染的态（假设为第一位）可以表述为 $|\psi\rangle, X_1|\psi\rangle, Z_1|\psi\rangle, X_1Z_1|\psi\rangle$ 的叠加态。

注意此时的 $|\psi\rangle$ 指的是未被污染的态，即 $|\psi\rangle = a|0_L\rangle + b|1_L\rangle$。

当进行 Z_1Z_2 测量时，如果测量结果为 1，则只有在投影算子 $(|00\rangle\langle 00| + |11\rangle\langle 11|) \otimes I$ 所罩住的空间内的信息被保留了下来，亦即只有 $|\psi\rangle, Z|\psi\rangle$ 被保留下来，而 $Z|\psi\rangle, XZ|\psi\rangle$ 全部丢失。而如果测量结果为-1，则 $Z|\psi\rangle, XZ|\psi\rangle$ 被保留，而 $|\psi\rangle, Z|\psi\rangle$ 丢失。

在第一次测量后的态上再进行 $X_1X_2X_3X_4X_5X_6$ 测量，综合两次的测量结果，如果为（1,1）则最终留下的是 $|\psi\rangle$; 如果为（1，-1）则最终留下的是 $Z|\psi\rangle$; 如果为（-1，1）则最终留下的是 $X|\psi\rangle$; 如果为（-1，-1）则最终留下的是 $XZ|\psi\rangle$。根据测量结果进行相应的恢复即可得到完美编码的 $|\psi\rangle$。

3 量子纠错理论

分析 Shor 编码，我们可以确定出一套纠错的程序：

1、确定一套离散的错误，可以表出其他任意错误。

2、这套特殊的离散的错误具有性质：发生不同的错误进入不同的正交子空间。

3、找到这些正交子空间对应的投影算子，各个同构且正交，每个对应一种类型的错误。

一般性的纠错理论可以表述为：$(\mathcal{R}\circ\mathcal{E})\rho\propto\rho$。

其中，$\mathcal{R}$ 表示纠错量子操作，$\mathcal{E}$ 表示错误，ρ 为密度矩阵。

3.1 量子纠错条件

定理： C 是一组量子编码，P 是映射到编码 C 上的投影算子。假设 $\{E_i\}$ 表示错误，则该错误能被编码 C 纠正的充要条件是

$$PE_i^\dagger E_jP=\alpha_{ij}P$$

其中 α 组成一个复元素的厄米矩阵。

利用这个定理，我们可以检查一套编码 C 是否能够有效地对抗错误 $\{E_i\}$，下面来看定理的证明。

充分性：由 $PE_i^\dagger E_jP=\alpha_{ij}P$ 可以构造出相应的 $\mathcal{R}$。

由于厄米矩阵一定可以被酉对角化，故 $d=u^\dagger\alpha u$，其中 u 是酉矩阵。

定义 $F_k=\sum\limits_i u_{ik}E_i$, 由于 u 是酉矩阵，故 $\{E_i\}$，$\{F_k\}$ 表示相同的量子操作 $\mathcal{E}$。

$PF_k^\dagger F_lP=\sum\limits_{i,j}u_{ki}^\dagger u_{jl}PE_i^\dagger E_jP=\sum\limits_{i,j}u_{ki}^\dagger u_{jl}\alpha_{ij}P=d_{kl}P$，其中 d_{kl} 是对角的。

故 $PF_k^\dagger F_kP=d_{kk}P$，极分解得到 $F_kP=\sqrt{d_{kk}}U_kP$，其中 U_k 是酉矩阵。

针对每一种错误 F_k 的投影算子可以构造为 $P_k=U_kPU_k^\dagger=\frac{F_kPU_k^\dagger}{\sqrt{d_{kk}}}, P_kP_l=P_k^\dagger P_l=\frac{U_kPF_k^\dagger}{\sqrt{d_{kk}}}\frac{F_lPU_l^\dagger}{\sqrt{d_{ll}}}$。

故当 $k\neq l$ 时，$P_kP_l=0$，即 P_k 相互正交；而 $P_kP_k=\frac{U_kd_{kk}PU_k^\dagger}{\sqrt{d_{kk}}\sqrt{d_{kk}}}=P_{kk}$，说明的确是投影算子。

故投影算子是 P_k，而恢复通过 $U_k^\dagger$ 实现。

具体地，假设发生了错误 F_k，进行测量 P_l 得到 $P_lF_kP|\psi\rangle=\frac{U_lPF_l^\dagger F_kP}{\sqrt{d_{kk}}}|\psi\rangle$。当 $k\neq l$ 时结果为 0，而当 $k=l$ 时，$P_kF_kP|\psi\rangle=\sqrt{d_{kk}}U_kP|\psi\rangle$，继续作用 $U_k^\dagger$，则回到完美编码 $P|\psi\rangle$ 上。

必要性： 说明 α 是厄米矩阵。

如果操作 $\mathcal{R}$ 能将错误探测并恢复，则 $R_jE_iP|\psi\rangle=c_{ji}P|\psi\rangle$, 即 $R_jE_iP=c_{ji}P$，其中 c_{ji} 是复数。

故 $PE_i^\dagger R_j^\dagger=c_{ji}^*P$ $PE_i^\dagger R_j^\dagger R_jE_kP=c_{ji}^*c_{jk}P$。

求和得到 $\sum\limits_j PE_i^\dagger R_j^\dagger R_jE_kP=\sum\limits_j c_{ji}^*c_{jk}P=\alpha_{ik}P$。

其中 $\alpha_{ik}\equiv\sum\limits_j c_{ji}^*c_{jk}, \alpha_{ki}\equiv\sum\limits_j c_{jk}^*c_{ji}=\alpha_{ik}^*$，说明 α 是厄米矩阵。

3.2 错误的离散化

量子纠错条件可以帮助检查编码是否对某一套错误 $\{E_i\}$ 有效，但实际情况下，我们需要编码能够对抗的错误是连续的一大类，而下面的定理将帮助我们扩充可纠正的错误。

定理： C 是一套量子编码，错误 $\{E_i\}$ 可以被操作 $\mathcal{R}$ 所纠正。则其他可以表述为 $\{E_i\}$ 线性组合的错误 $\{F_i\}$，即 $F_j = \sum_i m_{ji} E_i$（m_{ji} 是一个复数矩阵），都可以被 $\mathcal{R}$ 纠正。

证明：恰当选取 $\{E_i\}$，使得 $PE_i^\dagger E_j P = d_{ij} P$，其中 d 是对角阵。

$U_k^\dagger P_k F_j P |\psi\rangle = \sum_i m_{ji} U_k^\dagger P_k E_i P |\psi\rangle = \frac{\sum_i m_{ji} P E_k^\dagger E_i P}{\sqrt{d_{kk}}} |\psi\rangle = \sqrt{d_{kk}} m_{jk} P |\psi\rangle$，因而错误 $\{F_i\}$ 也可以被 $\mathcal{R}$ 纠正。

利用该定理，容易知道只要能纠正泡利矩阵 $\sigma_0, \sigma_1, \sigma_2, \sigma_3$，则可以纠正任意单量子比特错误。

3.3 量子汉明界

假设一个量子编码将 k 个量子比特编码成 n 个量子比特，而且能够纠正不超过 t 个比特任意组合上的错误（每个比特上的错误有 X,Y,Z 三种可能），则不同错误的可能总数为：$\sum_{j=0}^{t} \binom{n}{j} 3^j$。由于每个错误需要对应一个正交的 2^k 维子空间，于是需要满足条件 $\sum_{j=0}^{t} \binom{n}{j} 3^j 2^k \leq 2^n$。

特别地，对于将 1 个量子比特编码到 n 个量子比特上的情况，则需要满足 $2(1+3n) \leq 2^n$，为满足该条件，至少需要满足 $n \geq 5$，即至少需要使用 5 个量子比特进行编码。

需要注意的是，由于量子编码的简并性（发生不同错误可能不影响编码，如 Shor 编码中的相位翻转），量子汉明界并不是严格的，但是可以起到经验法则的作用。

4 稳定子

所谓稳定子，指的是一种用算子来描述量子态与量子纠错理论的语言。本节中，将先介绍稳定子的形式与具体性质，进而从稳定子的角度更加深刻地理解此前的量子纠错编码。

4.1 稳定子形式

考虑量子态 $|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$，发现 $X_1 X_2 |\psi\rangle = |\psi\rangle, Z_1 Z_2 |\psi\rangle = |\psi\rangle$，则称 $|\psi\rangle$ 被 $X_1 X_2, Z_1 Z_2$ 稳定。

事实上，在很多情况下用算子 $X_1 X_2, Z_1 Z_2$ 代替 $|\psi\rangle$ 来描述更加方便。这种不改变量子态的算子集合称之为稳定子 S，而被这些稳定子所稳定的空间称为稳定子空间 V_S。下面我们从更数学的角度解释。

引入泡利群 $G = \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}$。（引入 $\pm 1, \pm i$ 的目的在于使泡利群对乘法封闭。）

稳定子 S 是泡利群 G 的子集。注意到泡利矩阵之间要么对易要么但对易，因而 S 的元素之间也满足要么对易，要么反对易。

容易看出，V_S 非平凡可以推出 $-I \notin S$，且 S 的元素之间两两对易。

（$MN = -NM, M|\psi\rangle = |\psi\rangle, N|\psi\rangle = |\psi\rangle, MN|\psi\rangle = |\psi\rangle = NM|\psi\rangle = -MN|\psi\rangle$，矛盾。）

进一步引入生成子的概念，要求 S 中的元素相互独立，即 S 中的元素可以被 $g_1, g_2...g_l$ 的乘积生成，记为 $S =< g_1, g_2...g_l >$。

注意到泡利算子的特征值总是 ± 1，而稳定子空间取得是其中特征值为 $+1$ 的那一半。每多一个独立的生成子，稳定子空间就被裁掉一半。

4.2 校验矩阵

我们使用七比特 Steane 码作为具体例子：

$|0_L\rangle = \frac{1}{\sqrt{8}}(|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle + |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle)$

$|1_L\rangle = \frac{1}{\sqrt{8}}(|1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle + |1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle)$

而用以下 6 个生成子则可以表示产生 Steane 码的稳定子：

g_1	I	I	I	X	X	X	X
g_2	I	X	X	I	I	X	X
g_3	X	I	X	I	X	I	X
g_4	I	I	I	Z	Z	Z	Z
g_5	I	Z	Z	I	I	Z	Z
g_6	Z	I	Z	I	Z	I	Z

可以检验 $|0_L\rangle, |1_L\rangle$ 被 $g_1, g_2...g_6$ 所稳定，即 $g_i |\psi\rangle = |\psi\rangle$。

进一步，需要知道 g_i 之间的独立性与对易性，引入校验矩阵。

校验矩阵：用长度为 2n 的 01 串 $r(g)$ 来表示 g_i，用第 k 个和第 n+k 个来共同表出 g_{ik}。

其中的对应规则为：I:(0,0) , X:(1,0) , Z:(0,1) , Y:(1,1)。

则 Steane 码的校验矩阵可以写作：

g_1	0	0	0	1	1	1	1	0	0	0	0	0	0	0
g_2	0	1	1	0	0	1	1	0	0	0	0	0	0	0
g_3	1	0	1	0	1	0	1	0	0	0	0	0	0	0
g_4	0	0	0	0	0	0	0	0	0	0	1	1	1	1
g_5	0	0	0	0	0	0	0	0	1	1	0	0	1	1
g_6	0	0	0	0	0	0	0	1	0	1	0	1	0	1

记 $\Lambda = \begin{bmatrix} 0 & I \\ I & 0 \end{bmatrix}$，其中 I 为 $n \times n$ 单位矩阵。

命题 1： g ，g' 对易 $\iff r(g)\Lambda r(g')^T = 0$。

（注意有关校验矩阵的运算定义在 Z_2 域上，即需要对 2 取模。）

证明：$r(g) = \begin{bmatrix} r_1 & r_2 \end{bmatrix}, \Lambda r(g')^T = \begin{bmatrix} r'_1 \\ r'_2 \end{bmatrix}, r(g)\Lambda r(g')^T = r_1 r'_2 + r_2 r'_1$。

注意到 $I \to (0\ 0), X \to (1\ 0), Z \to (0\ 1), Y \to (1\ 1)$。

我们只需说明算子之间的对易关系与相应的两个矩阵的转置再内积（并且模 2）的结果相符即可。

容易知道 I 与所有算子均对易，而 $r_1 = r_2 = 0 \Rightarrow r_1 r'_2 + r_2 r'_1 = 0$。

同时各个算符与自身均对易，比如 $XX = XX$, 对应于 $\begin{bmatrix} 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = 0$。（注意后面的转置）

而泡利算符之间是反对易的，$XY = -YX$，对应于 $\begin{bmatrix} 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = 1$。

同时，当有偶数个比特位反对易时，两个算子整体仍然是对易的，这与奇偶性的性质相似，相当于不同比特位之间的直积关系被表述为了校验矩阵中不同位置之间的求和关系。

命题 2： $g_1, g_2 ... g_l$ 相互独立 $\iff$ $r(g_i)$ 不线性相关，亦即 $r(g)$ 矩阵满秩。

证明：只需证 $r(gg') = r(g) + r(g')$，注意当我们取校验矩阵时，并不在意系数 $\pm 1, \pm i$。

$II = I, IX = X$ 对应于 $\begin{bmatrix} 0 & 0 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$。

$XX = YY = ZZ = I$ 对应于 $\begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}$。

$XY \propto Z, YZ \propto X, ZX \propto Y$ 对应于 $\begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 1 \\ 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{bmatrix}$。

均符合条件，可以看出生成子之间的乘积关系与校验矩阵的求和关系相对应，因而生成子独立性（无法用乘积表出）对应于校验矩阵的行线性无关（即满秩）。

命题 3： 存在 $g \in G_n$（n 比特泡利群），使得 g 与某个 g_i 反对易，而与其他 g_j 对易，其中 $g_1, g_2 ... g_l$ 是一组相互独立的生成子。

证明：由于校验矩阵 G 满秩，则总可以找到长度为 $2n$ 的列向量 X，使得方程 $G\Lambda X = e_i$ 成立，其中 e_i 是只有第 i 个元素不为 0 的列向量。那么列向量 X 所对应的算符即为所求的 g。

命题 4： $n-k$ 个生成子（相互独立，相互对易），所对应的稳定子空间 V_S 是 2^k 维的。

（该命题相当于建立了一组 n 个比特与 k 个比特之间的对应关系，注意此时我们还没有涉及到任何纠错相关的内容，理解时不要与纠错理论混淆起来。）

证明：x 是长度为 $n-k$ 的 01 串，定义算子 $P(x) = \frac{\prod_{i=1}^{n-k} (I + (-1)^{x_i} g_i)}{2^{n-k}}$。我们首先说明 $P(x)$ 是相互正交的投影算子，这就表示不同的 01 串对应于不同的正交子空间。

$P(x)P(x) = \frac{\prod_{i=1}^{n-k} (I + (-1)^{x_i} g_i)}{2^{n-k}} \frac{\prod_{i=1}^{n-k} (I + (-1)^{x_i} g_i)}{2^{n-k}}$，注意到 g_i 之间互相对易，故可以随意交换顺序，又 $\frac{I \pm g}{2} \frac{I \pm g}{2} = \frac{I + g^2 \pm 2g}{4} = \frac{I \pm g}{2}$，故 $P(x)P(x) = P(x)$。

对于正交性，仍可以任意调换顺序，找到 01 串中不同的那一位，有 $\frac{I+g}{2} \frac{I-g}{2} = 0$，因而 $P(x_1)P(x_2) = 0$。

下面说明各个投影算子对应的子空间维数相同，即各个子空间同构。

由命题 3 可知，对于 01 串 $(0, 0 ... 0)$ 与 $(1, 0, 0 ... 0)$ 而言，总可以找到 g 与 g_1 反对易而与其他的 $g_2 ... g_{n-k}$ 对易。

此时，$g(\frac{I+g_1}{2}) = \frac{g+gg_1}{2} = \frac{g-g_1 g}{2} = \frac{I-g}{2} g_1$。于是 $gP_0 = P_1 g$，即 $gP_0 g^\dagger = P_1$。推广可知，所有的 $P(x)$ 同构。

同时，$I=\sum_x P(x)$，说明所有投影子空间的和是总空间，利用维数相同可以得到每个投影算子对应的总空间的维度是 $\frac{2^n}{2^{n-k}}=2^k$。

4.3 规范子

考虑稳定子空间内的量子 $|\psi\rangle$ 态经历了某种酉变化 U，有 $U|\psi\rangle=Ug|\psi\rangle=UgU^\dagger U|\psi\rangle$。

这说明状态 $U|\psi\rangle$ 被算子 $UgU^\dagger$ 所稳定，则向量空间 UV_S 被群 $USU^\dagger$ 稳定。

对于一些特别的酉变换，新的稳定子可以与之前的稳定子具有特定的关系（比如相同或包含），这将使得在对应的酉变换作用下，量子态仍然处于稳定子空间中。

作为具体的例子，有 $HXH^\dagger=Z, HYH^\dagger=-Y, HZH^\dagger=X$。

假设 U 是受控非门，有 $UX_1U^\dagger=X_1X_2, UX_2U^\dagger=X_2, UZ_1U^\dagger=Z_1, UZ_2U^\dagger=Z_1Z_2$。

我们验证其中的第一个:

$$UX_1U^\dagger=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}\begin{bmatrix}0&0&1&0\\0&0&0&1\\1&0&0&0\\0&1&0&0\end{bmatrix}\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}\begin{bmatrix}0&0&0&1\\0&0&1&0\\1&0&0&0\\0&1&0&0\end{bmatrix}$$

$$=\begin{bmatrix}0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0\end{bmatrix}=X_1X_2$，其他四个式子同理。$$

相位门 $S=\begin{bmatrix}1&0\\0&i\end{bmatrix}$，容易得到 $SXS^\dagger=Y, SYS^\dagger=X, SZS^\dagger=Z$。

对于一个任意的酉变换，如果它将 G_n 中的元素变换到 G_n 中的另一个元素，则这样的 U 的集合称之为 G_n 的规范子，记为 $N(G_n)$，从如下的定理中我们可以看到，规范子可以由少数几种门来构成。

命题： G_n 的规范子可以由 $O(n^2)$ 个 H 门，受控非门，相位门外加一个可能的全局相位构成。

证明：首先证明 H 门和 S 门可以被用来实现单量子比特上的任意规范子操作。

注意到规范子操作实际上描述的是将 X,Y,Z 转变为 X,Y,Z 的另一种排列，而 H 门代表按顺序移动一位，S 门代表交换 X,Y，容易看出仅通过这两种操作可以生成 X,Y,Z 的全排列。

假设 $U\in N(G_{n+1})$，而对 G_n 中的元素 g,g' 有 $UZ_1U^\dagger=X_1\otimes g, UX_1U^\dagger=Z_1\otimes g'$。那么可以构造 $U=(I\otimes U')(U_{g'})(H\otimes I)(U_g)$，其中 $U_g,U_{g'}$ 表示受控操作。

下面验证该构造有效，我们不妨取 $|0\rangle\otimes|\psi\rangle, |1\rangle\otimes|\psi\rangle$ 态分别对 Z_1 与 X_1 算子进行检验。

（注意可以选取 g,g' 为厄米矩阵且相互对易，且满足 $U'gU'^\dagger=g', U'g'U'^\dagger=g$。）

$UZ_1U^\dagger(|0\rangle\otimes|\psi\rangle)=U'U_{g'}H_1U_gZ_1U_gH_1U_{g'}U'^\dagger(|0\rangle\otimes|\psi\rangle)=U'U_{g'}H_1U_gZ_1U_gH_1U_{g'}(|0\rangle\otimes U'^\dagger|\psi\rangle)$

$=U'U_{g'}H_1U_gZ_1U_g(\frac{|0\rangle+|1\rangle}{\sqrt2}\otimes U'^\dagger|\psi\rangle)=U'U_{g'}H_1U_gZ_1(\frac{|0\rangle}{\sqrt2}\otimes U'^\dagger|\psi\rangle+\frac{|1\rangle}{\sqrt2}\otimes gU'^\dagger|\psi\rangle)$

$=U'U_{g'}H_1U_g(\frac{|0\rangle}{\sqrt2}\otimes U'^\dagger|\psi\rangle-\frac{|1\rangle}{\sqrt2}\otimes gU'^\dagger|\psi\rangle)=U'U_{g'}H_1(\frac{|0\rangle}{\sqrt2}\otimes U'^\dagger|\psi\rangle-\frac{|1\rangle}{\sqrt2}\otimes ggU'^\dagger|\psi\rangle)$

$=U'U_{g'}(|1\rangle\otimes U'^\dagger|\psi\rangle)=|1\rangle\otimes U'g'U'^\dagger|\psi\rangle=|1\rangle\otimes g|\psi\rangle$

$UZ_1U^\dagger(|1\rangle\otimes|\psi\rangle)=U'U_{g'}H_1U_gZ_1U_gH_1U_{g'}U'^\dagger(|1\rangle\otimes|\psi\rangle)=U'U_{g'}H_1U_gZ_1U_gH_1U_{g'}(|1\rangle\otimes U'^\dagger|\psi\rangle)$

$=U'U_{g'}H_1U_gZ_1U_g(\frac{|0\rangle-|1\rangle}{\sqrt2}\otimes g'U'^\dagger|\psi\rangle)=U'U_{g'}H_1U_gZ_1(\frac{|0\rangle}{\sqrt2}\otimes g'U'^\dagger|\psi\rangle-\frac{|1\rangle}{\sqrt2}\otimes gg'U'^\dagger|\psi\rangle)$

$= U'U_{g'}H_1U_g(\frac{|0\rangle}{\sqrt{2}} \otimes g'U'^{\dagger}|\psi\rangle + \frac{|1\rangle}{\sqrt{2}} \otimes gg'U'^{\dagger}|\psi\rangle) = U'U_{g'}H_1(\frac{|0\rangle}{\sqrt{2}} \otimes g'U'^{\dagger}|\psi\rangle + \frac{|1\rangle}{\sqrt{2}} \otimes ggg'U'^{\dagger}|\psi\rangle)$

$= U'U_{g'}(|0\rangle \otimes g'U'^{\dagger}|\psi\rangle) = |0\rangle \otimes U'g'U'^{\dagger}|\psi\rangle = |0\rangle \otimes g|\psi\rangle$

于是 $UZ_1U^{\dagger} = X_1 \otimes g$ 成立。

$UX_1U^{\dagger}(|0\rangle \otimes |\psi\rangle) = U'U_{g'}H_1U_gX_1U_gH_1U_{g'}U'^{\dagger}(|0\rangle \otimes |\psi\rangle) = U'U_{g'}H_1U_gX_1U_gH_1U_{g'}(|0\rangle \otimes U'^{\dagger}|\psi\rangle)$

$= U'U_{g'}H_1U_gX_1U_g(\frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes U'^{\dagger}|\psi\rangle) = U'U_{g'}H_1U_gX_1(\frac{|0\rangle}{\sqrt{2}} \otimes U'^{\dagger}|\psi\rangle + \frac{|1\rangle}{\sqrt{2}} \otimes gU'^{\dagger}|\psi\rangle)$

$= U'U_{g'}H_1U_g(\frac{|1\rangle}{\sqrt{2}} \otimes U'^{\dagger}|\psi\rangle + \frac{|0\rangle}{\sqrt{2}} \otimes gU'^{\dagger}|\psi\rangle) = U'U_{g'}H_1(\frac{|1\rangle}{\sqrt{2}} \otimes gU'^{\dagger}|\psi\rangle + \frac{|0\rangle}{\sqrt{2}} \otimes gU'^{\dagger}|\psi\rangle)$

$= U'U_{g'}(|0\rangle \otimes gU'^{\dagger}|\psi\rangle) = |0\rangle \otimes U'gU'^{\dagger}|\psi\rangle = |0\rangle \otimes g'|\psi\rangle$

$UX_1U^{\dagger}(|1\rangle \otimes |\psi\rangle) = U'U_{g'}H_1U_gX_1U_gH_1U_{g'}U'^{\dagger}(|1\rangle \otimes |\psi\rangle) = U'U_{g'}H_1U_gX_1U_gH_1U_{g'}(|1\rangle \otimes U'^{\dagger}|\psi\rangle)$

$= U'U_{g'}H_1U_gX_1U_g(\frac{|0\rangle-|1\rangle}{\sqrt{2}} \otimes g'U'^{\dagger}|\psi\rangle) = U'U_{g'}H_1U_gX_1(\frac{|0\rangle}{\sqrt{2}} \otimes g'U'^{\dagger}|\psi\rangle - \frac{|1\rangle}{\sqrt{2}} \otimes gg'U'^{\dagger}|\psi\rangle)$

$= U'U_{g'}H_1U_g(\frac{|1\rangle}{\sqrt{2}} \otimes g'U'^{\dagger}|\psi\rangle - \frac{|0\rangle}{\sqrt{2}} \otimes gg'U'^{\dagger}|\psi\rangle) = U'U_{g'}H_1(\frac{|1\rangle}{\sqrt{2}} \otimes gg'U'^{\dagger}|\psi\rangle - \frac{|0\rangle}{\sqrt{2}} \otimes gg'U'^{\dagger}|\psi\rangle)$

$= U'U_{g'}(-|1\rangle \otimes gg'U'^{\dagger}|\psi\rangle) = -|1\rangle \otimes U'g'gg'U'^{\dagger}|\psi\rangle = -|1\rangle \otimes g'|\psi\rangle$

于是 $UX_1U^{\dagger} = Z_1 \otimes g'$ 成立。

n+1 个比特与 n 个比特之间多引入了 $O(2n)$ 个门（2 组 n 比特受控门），因而 n 比特稳定子操作需要用 $O(n^2)$ 个 H 门，受控非门，相位门外加一个可能的全局相位构成。

需要特别注意的是，只有很少一部分逻辑门在规范子的范围内（比如 Toffoli 门和 $\frac{\pi}{8}$ 就并非如此）。但幸运的是，稳定子的编码、解码等操作都只需要用到属于规范子的逻辑门即可实现。

4.4 稳定子形式中的测量

考虑在稳定子 $< g_1, g_2 \dots g_n >$ 描述的状态 $|\psi\rangle$ 下进行测量 $g, g \in G_n$ 且是厄米的。

（利用 4.2 中的命题 4 可知此时的稳定子空间 V_S 是一维的。）

g 可以取如下两种情况：

若 g 与 $< g_1, g_2 \dots g_n >$ 均对易，则有 $gg_i|\psi\rangle = g_ig|\psi\rangle = g|\psi\rangle$ 均成立，故 $g|\psi\rangle = c|\psi\rangle$，其中 c 为复系数。

又 $g^2 = I$，故 $c = \pm 1$，不妨取正，则说明 g 也是稳定子，所以测量 g 将以概率 1 获得 $+1$ 的结果，并且不影响量子态本身，因而稳定子维持不变。

若 g 不与 $< g_1, g_2 \dots g_n >$ 全部对易，不失一般性地，假设 g 与 g_1 反对易，与 $g_2, g_3 \dots g_n$ 对易。

g 的特征值为 ± 1，对应的投影算子为 $\frac{I \pm g}{2}$，测量的概率为：

$p(+1) = tr(\frac{I+g}{2}|\psi\rangle\langle\psi|), p(-1) = tr(\frac{I-g}{2}|\psi\rangle\langle\psi|)$。

$p(+1) = tr(\frac{I+g}{2}|\psi\rangle\langle\psi|) = tr(\frac{I+g}{2}g_1|\psi\rangle\langle\psi|) = tr(g_1\frac{I-g}{2}|\psi\rangle\langle\psi|) = tr(\frac{I-g}{2}|\psi\rangle\langle\psi|g_1) = p(-1) = \frac{1}{2}$，

其中倒数第二个等号利用了求迹的循环特性。

于是系统以 $\frac{1}{2}$ 概率得到结果 $+1$，新的状态为 $|\psi^+\rangle = \frac{I+g}{\sqrt{2}}|\psi\rangle$，对应的稳定子为 $< g, g_2 \dots g_n >$；以 $\frac{1}{2}$ 概率得到结果 -1，新的状态为 $|\psi^-\rangle = \frac{I-g}{\sqrt{2}}|\psi\rangle$，对应的稳定子为 $< -g, g_2 \dots g_n >$。

Gottesman-Knill 定理： 假设量子计算中只涉及以下操作：计算基下的状态制备、H 门、相位门、受控非门、泡利门，与泡利群中可观测量对应的测量，以及基于量子测量结果的经典控制，则这种量子计算可以被经典计算机有效模拟。

4.5 稳定子编码的构造

对于一套由 $n-k$ 个生成子描述的稳定子 $S=<g_1,g_2\dots g_{n-k}>$，其稳定子空间 V_S 的维度为 2^k，我们需要构造的就是这样一套从 n 个比特到 k 个比特上的编码。

原则上，这种编码可以随意选取，只要能够生成规模为 2^k 的标准正交基即可。但我们打算用一套更有意义的方式系统地实现这一点：寻找算子 $\bar{Z}_1,\bar{Z}_2\dots\bar{Z}_k$，使得 $g_1,g_2\dots g_{n-k},\bar{Z}_1,\bar{Z}_2\dots\bar{Z}_k$ 整体相互独立且对易，那么此时 $\bar{Z}_j$ 将起到第 j 个逻辑比特上泡利 Z 算子的作用。因而计算基矢态 $|x_1,x_2\dots x_k\rangle_L$ 被定义为稳定子 $<g_1,g_2\dots g_{n-k},(-1)^{x_1}\bar{Z}_1,(-1)^{x_2}\bar{Z}_2\dots(-1)^{x_k}\bar{Z}_k>$ 所描述的量子态。

在此之前，我们都还未涉及到错误的影响，接下来我们考虑噪声 $E\in G_n$ 对编码的影响。

首先从定性的角度去思考：如果噪声 E 与稳定子中的至少 1 个反对易，该噪声会将编码空间 V_S 变到一个与之正交的空间上去，那么通过合适的投影测量就能够探测并恢复错误；如果 $E\in S$，则噪声不会对编码态产生影响。真正造成影响的是那些与 S 中所有元素都对易却不在 S 中的 E，这将导致我们的编码状态在 V_S 空间中发生了某种转动，从而造成了所维护的信息的丢失。不难看出这样的 E 所对应的集合实际上就是 $N(S)-S$。

由此，我们可以给出稳定子编码的量子纠错条件：

稳定子编码的量子纠错条件： S 是稳定子，$C(S)$ 为对应编码，如果错误 $\{E_i\}(E_i\in G_n)$ 满足对所有的 j,k 均有 $E_j^\dagger E_k\notin N(S)-S$，那么 $\{E_i\}$ 对于纠错码 $C(S)$ 是一组可纠正错误。

证明：不失一般性地，我们只考虑那些厄米的噪声 $E_i=E_i^\dagger$。

若 $E_iE_j\in S$，则 $PE_iE_jP=P$，满足量子纠错条件。

若 $E_iE_j\in G_n-N(S)$，则其至少于 S 生成子中的 1 个反对易，不妨设为 g_1。

$P=\frac{\prod^{n-k}(I+g_l)}{2^{n-k}},E_iE_jP=\frac{1}{2^{n-k}}E_iE_j(I+g_1)\prod_{l=2}^{n-k}(I+g_l)=\frac{1}{2^{n-k}}(I-g_1)E_iE_j\prod_{l=2}^{n-k}(I+g_l)$。

$PE_iE_jP=\frac{1}{2^{n-k}}\prod_{l=2}^{n-k}(I+g_l)(I+g_1)\frac{1}{2^{n-k}}(I-g_1)E_iE_j\prod_{l=2}^{n-k}(I+g_l)=0$。$((I-g_1)(I+g_1)=0)$

我们引入距离 d 和权重 w 的概念，其中 w 指的是张量积中非单位矩阵的数量，而一套编码 $C(S)$ 的 d 指的是 $N(S)-S$ 中元素的最小权重。而一个距离至少为 $2t+1$ 的编码可以纠正 t 个量子比特上的任意错误。

以上我们给出了稳定子编码纠错的理论依据，但未给出具体构造，我们将通过具体的示例来深入体会：

4.5.1 三量子比特的比特翻转编码

错误集合 $\{I,X_1,X_2,X_3\}$，其中两项的乘积为 $I,X_1,X_2,X_3,X_1X_2,X_1X_3,X_2X_3$ 都与稳定子对应生成子 $<Z_1Z_2,Z_2Z_3>$ 中的至少一项反对易。

具体到纠错过程，我们测量生成子 Z_1Z_2,Z_2Z_3，如果发生错误 X_1，则稳定子变成 $<-Z_1Z_2,Z_2Z_3>$，对应的测量结果为 $-1,+1$。其他的几种错误可以按照相同程序探测并恢复。

4.5.2 九量子比特 Shor 编码

g_1	Z	Z	I	I	I	I	I	I	I
g_2	I	Z	Z	I	I	I	I	I	I
g_3	I	I	I	Z	Z	I	I	I	I
g_4	I	I	I	I	Z	Z	I	I	I
g_5	I	I	I	I	I	I	Z	Z	I
g_6	I	I	I	I	I	I	I	Z	Z
g_7	X	X	X	X	X	X	I	I	I
g_8	I	I	I	X	X	X	X	X	X
$\bar{Z}$	X	X	X	X	X	X	X	X	X
$\bar{X}$	Z	Z	Z	Z	Z	Z	Z	Z	Z

不难验证 $\bar{Z}, \bar{X}$ 之间反对易，且与 $g_1, g_2 \dots g_9$ 之间都对易，代入之前的编码形式可以验证 $\bar{Z}, \bar{X}$ 的确是逻辑 Z, X 门。

下面验证可以纠正任意单量子比特错误：

若 $E_i E_j = I$，则其在稳定子当中。

若 $E_i E_j = X_i, Y_i$，则至少与 $g_1 \dots g_6$ 中的一个反对易；若 $E_i E_j = Z_i$，则与 g_7, g_8 中的 1 个反对易。

若 $E_i E_j = X_i R_{j(j\neq i)}, Y_i R_{j(j\neq i)}$，则至少与 $g_1 \dots g_6$ 中的一个反对易。

若 $E_i E_j = Z_i Z_j$，若 i, j 同属于前三个，中间三个或后三个，则其在稳定子当中。若否，则至少于 g_7, g_8 中的 1 个对易。

我们也可以从 Shor 编码对应的生成子去写出逻辑比特 $|0_L\rangle, |1_L\rangle$。

注意到 $|000000000\rangle$ 在稳定子空间内，让它作为 $|0_L\rangle$ 的一部分，又所有生成子和 $\bar{Z}$ 作用在 $|0_L\rangle$ 的任意部分的结果仍然在 $|0_L\rangle$ 中，于是依次得到：

$|111111000\rangle, |000111111\rangle, |111000111\rangle, |111111111\rangle, |111000000\rangle, |000111000\rangle, |000000111\rangle$。

归一化可得：$|0_L\rangle = \frac{(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)}{2\sqrt{2}}, |1_L\rangle = \bar{X}|0_L\rangle = |0_L\rangle = \frac{(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)}{2\sqrt{2}}$。

4.5.3 五量子比特码

g_1	X	Z	Z	X	I
g_2	I	X	Z	Z	X
g_3	X	I	X	Z	Z
g_4	Z	X	I	X	Z
$\bar{Z}$	Z	Z	Z	Z	Z
$\bar{X}$	X	X	X	X	X

我们先来验证这个五量子比特编码确实能够处理任意单量子比特错误，更特别地，只需验证可以对抗错误 I, X, Z：

若 $E_i E_j = X_i, Z_i$，由于 $g_1 \dots g_4$ 这四个算子中的 Z, X 覆盖了每个比特至少 1 次，因此此时必然与之反对易。

若 $E_iE_j = X_iX_j$，g_1 与除了 $X_1X_4, X_1X_5, X_4X_5, X_2X_3$ 之外的反对易；g_2 与 X_2X_3, X_1X_4, X_4X_5 反对易，g_3 与 X_1X_5 反对易，故满足条件，对于 $E_iE_j = Z_iZ_j$ 同理。

若 $E_iE_j = X_iZ_j$,不妨设 $i < j$,g_1 可解决 $(1,4),(2,3),(2,5),(3,5)$,g_2 可解决 $(1,2),(1,5),(2,5)^*,(3,4)$,$g_3$ 可解决 $(1,3),(2,3)^*,(4,5)$，g_4 可解决 $(2,4),(3,4)^*,(1,3)^*,(1,5)^*$，对于 $i > j$ 的情况同理。

综上，由这四个生成子维护的编码可以纠正任何单比特错误。

仿照上一小节的做法，给出对应的 $|0_L\rangle, |1_L\rangle$。

$|0_L\rangle$ 中包含 $|00000\rangle, |10010\rangle, |01001\rangle, |10100\rangle, |01010\rangle, -|11011\rangle, -|00110\rangle, -|11000\rangle, -|11101\rangle,$ $-|00011\rangle, -|11110\rangle, -|01111\rangle, -|10111\rangle, -|10001\rangle, -|01100\rangle, |00101\rangle$。

$|0_L\rangle = \frac{1}{4}(|00000\rangle - |11000\rangle - |01100\rangle - |00110\rangle - |00011\rangle - |10001\rangle + |10100\rangle + |10010\rangle + |01010\rangle + |01001\rangle + |00101\rangle - |01111\rangle - |10111\rangle - |11011\rangle - |11101\rangle - |11110\rangle)$。

$|1_L\rangle = \bar{X}|0_L\rangle = \frac{1}{4}(|11111\rangle - |00111\rangle - |10011\rangle - |11001\rangle - |11100\rangle - |01110\rangle + |01011\rangle + |01101\rangle + |10101\rangle + |10110\rangle + |11010\rangle - |10000\rangle - |01000\rangle - |00100\rangle - |00010\rangle - |00001\rangle)$。

实际上编码内部有规律性，以 $|0_L\rangle$ 为例，只能有偶数个 1，并且相邻 1 的数目为奇数对时需添加负号。

我们由此可以看出用稳定子表述的简洁性，同时这种五比特编码也将会带来一些疑问。在 Shor 编码中，我们清晰地知道每一个生成子所对应的含义，比如某两位是否存在比特翻转，或者说某两部分是否存在相位翻转；但在五比特编码的生成子中，这两种效应纠缠在了一起，比如说 g_1 的测量结果告诉我们第 2 个比特和第 3 个比特之间存在比特翻转与第 1 个比特和第 4 个比特之间存在相位翻转这两件事是同时成立（不成立）还是只有其中的某 1 个成立，这种纠缠造成了我们直观上思考每个测量的作用时的困难。

4.6 稳定子编码的标准形式

在先前的讨论中，我们总是用多个量子比特来维护 1 个量子比特，这使得逻辑 Z, X 门的构造较为简单。对于一般情形而言，使用稳定子编码的标准形式有助于写出所有的逻辑 Z, X 门。

$[n,k]$ 编码的校验矩阵：$[G_1|G_2]$。

G_1 的秩为 r，做高斯消元并进行必要的比特交换：

		r	$n-r$	r	$n-r$
r		I	A	B	C
$n-k-r$		0	0	D	E

对 E 高斯消元并做必要的比特交换：

		r	$n-r-s-k$	$s+k$	r	$n-r-s-k$	$s+k$
r		I	A_1	A_2	B	C_1	C_2
$n-r-s-k$		0	0	0	D_1	I	E_1
s		0	0	0	D_2	0	0

我们要求生成子之间相互对易，即前 r 个与后 s 个之间相互对易，当且仅当 $D_2 = 0$ 时成立。

又编码是独立的，故校验矩阵满秩，则 $s = 0$。

注意到对 E 高斯消元并不会影响到 C_1，因而可以先通过线性组合使得 $C_1 = 0$。

于是我们得到校验矩阵的标准形式：

$$\begin{array}{c|cccccc} & r & n-k-r & k & r & n-k-r & k \\ r & I & A_1 & A_2 & B & 0 & C \\ n-k-r & 0 & 0 & 0 & D & I & E \end{array}$$

现在我们给出 k 个逻辑 Z 算子的校验矩阵的构造，并验证如下条件：

1. 这些逻辑 Z 算子之间互相对易，且互相独立。

2. 这些逻辑 Z 算子与生成子互相对易，且互相独立。

k 个逻辑 Z 算子的校验矩阵的构造为：$G_z = [000|A_2^T 0 I]$。

由于全部由 Z 组成，因此相互对易，同时最后一个部分为 $k \times k$ 单位阵，故各行线性无关。

$I \times (A_2^T)^T + A_2 = 0$，说明与前 r 个生成子对易，而后 $n-k-r$ 个生成子仅有 Z 组成，故对易性要求满足。

由于逻辑 Z 算子仅由 Z 构成，故与前 r 个生成子独立，又后 $n-k-r$ 个生成子的中间 $n-k-r$ 列并不全为 0，故与逻辑 Z 校验矩阵行线性无关，说明互相独立，故独立性要求也满足。

逻辑 X 算子的校验矩阵的构造为：$G_x = [0E^T I|C^T 00]$，需要验证其满足如下条件：

1. 这些逻辑 X 算子之间互相对易，且互相独立。

2. 这些逻辑 X 算子与生成子互相对易，且互相独立。

3.$\bar{X}_i$ 与 $\bar{Z}_i$ 之外的 $\bar{Z}_j$ 都对易，并于 $\bar{Z}_i$ 反对易。

$0 \times (C^T)^T + (E^T) \times 0 + I \times 0 = 0$，说明相互对易，而其中具有单位矩阵 I 说明行线性无关，因此相互独立。

$I \times (C^T)^T + C = 0$，说明与前 r 个生成子对易，$E^T + E^T = 0$ 说明与后 $n-k-r$ 个生成子对易。

前 r 个生成子前 r 列组成单位矩阵而逻辑 X 算子对应列均为 0，故行线性无关；后 $n-k-r$ 个生成子均由 Z 算子构成，而逻辑 X 算子的左半部分最后 k 列为单位矩阵，故行线性无关，因而独立性得到满足。

$G_z \Lambda G_x = I \times I = I$，说明仅有对于编号的逻辑算子反对易，而其余情况均对易。

下面以 Steane 码为具体样例，给出操作流程：

$$\begin{array}{cccccccccccccccc} g_1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \\ g_2 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \\ g_3 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \\ g_4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \\ g_5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & \\ g_6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & \end{array} \Rightarrow r = 3$$

交换比特 1 和 4：

$$\begin{array}{cccccccccccccc} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{array}$$

交换比特 3 和 4：

$$\begin{matrix}1&0&0&0&1&1&1&0&0&0&0&0&0&0\\0&1&0&1&0&1&1&0&0&0&0&0&0&0\\0&0&1&1&1&0&1&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&1&0&0&0&1&1&1\\0&0&0&0&0&0&0&0&1&0&1&0&1&1\\0&0&0&0&0&0&0&0&0&1&1&1&0&1\end{matrix}$$

交换比特 6 和 7:

$$\begin{matrix}1&0&0&0&1&1&1&0&0&0&0&0&0&0\\0&1&0&1&0&1&1&0&0&0&0&0&0&0\\0&0&1&1&1&1&0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&1&0&0&0&1&1&1\\0&0&0&0&0&0&0&0&1&0&1&0&1&1\\0&0&0&0&0&0&0&0&0&1&1&1&1&0\end{matrix}$$

$4 \to 4+6$（表示第六行加到第四行上）:

$$\begin{matrix}1&0&0&0&1&1&1&0&0&0&0&0&0&0\\0&1&0&1&0&1&1&0&0&0&0&0&0&0\\0&0&1&1&1&1&0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&1&0&1&1&0&0&1\\0&0&0&0&0&0&0&0&1&0&1&0&1&1\\0&0&0&0&0&0&0&0&0&1&1&1&1&0\end{matrix}$$

$5 \to 5+6$:

$$\begin{matrix}1&0&0&0&1&1&1&0&0&0&0&0&0&0\\0&1&0&1&0&1&1&0&0&0&0&0&0&0\\0&0&1&1&1&1&0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&1&0&1&1&0&0&1\\0&0&0&0&0&0&0&0&1&1&0&1&0&1\\0&0&0&0&0&0&0&0&0&1&1&1&1&0\end{matrix}$$

$6 \to 6+4+5$:

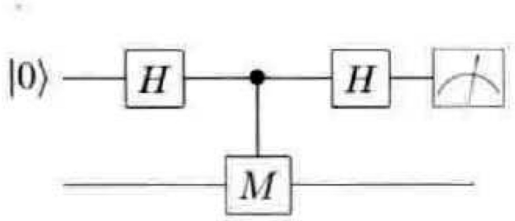
$$\begin{matrix}1&0&0&0&1&1&1&0&0&0&0&0&0&0\\0&1&0&1&0&1&1&0&0&0&0&0&0&0\\0&0&1&1&1&1&0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&1&0&1&1&0&0&1\\0&0&0&0&0&0&0&0&1&1&0&1&0&1\\0&0&0&0&0&0&0&1&1&1&0&0&1&0\end{matrix}$$

$A_2 = 110, G_z = 00000001100001, \Rightarrow \bar{Z}' = Z_1Z_2Z_7$

换回之前的比特，$\bar{Z}'' = Z_2Z_4Z_6$，又 $g_6 = Z_1Z_3Z_5Z_7 \Rightarrow \bar{Z} = g_6\bar{Z}'' = Z_1Z_2Z_3Z_4Z_5Z_6Z_7$。

4.7 纠错的量子电路

我们仔细考量先前探测错误征状时的具体操作，对于一个 n 个比特上的操作，我们要通过一步测量 M，使得我们能够凭借测量结果知道量子态进入了哪个投影空间中。这在理论上来说是显然的，但在搭建具体量子电路时，我们需要引入辅助比特通过如下结构来实现该操作：

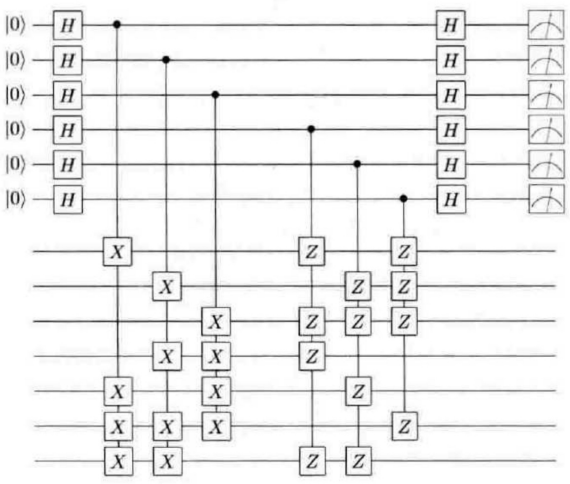


该量子程序的具体过程为：

$|0\rangle \otimes |\psi\rangle \to \frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes |\psi\rangle \to \frac{1}{\sqrt{2}} |0\rangle \otimes I |\psi\rangle + \frac{1}{\sqrt{2}} |1\rangle \otimes M |\psi\rangle \to \frac{|0\rangle+|1\rangle}{2} \otimes I |\psi\rangle + \frac{|0\rangle-|1\rangle}{2} \otimes M |\psi\rangle$
$\to |0\rangle \otimes \frac{I+M}{2} |\psi\rangle + |1\rangle \otimes \frac{I-M}{2} |\psi\rangle$

当辅助量子态处于 $|0\rangle$ 时，计算态进入 $P(+1)$ 投影空间；当辅助量子态处于 $|1\rangle$ 时，计算态进入 $P(-1)$ 投影空间。

对于七比特 Steane 编码，我们给出如下量子电路，注意我们使用的是标准形式下的生成子：



作为之前的补充，我们考虑不同测量结果所对应的错误征状：

首先定性来看，前半部分由 X 门组成，用以探测是否存在相位翻转错误；后半部分由 Z 门组成，用以探测是否存在比特翻转错误。

从数量关系上看，要定位出 7 个比特中哪一个出错，总共有 8 种可能（包含无错误），而三次测量结果正好对应于 8 个测量结果。

事实上，这个过程与我们称量 3 次判断 8 个砝码中哪一个是坏的砝码的步骤类似。

$1,4,5,7$	$2,4,6,7$	$3,4,5,6$
$1(2,3,6)$	$1(3)$	$1(0)$
$1(2,3,6)$	$1(3)$	$-1(3)$
$1(2,3,6)$	$-1(2,6)$	$1(2)$
$1(2,3,6)$	$-1(2,6)$	$-1(6)$
$-1(1,4,5,7)$	$1(1,5)$	$1(1)$
$-1(1,4,5,7)$	$1(1,5)$	$-1(5)$
$-1(1,4,5,7)$	$-1(4,7)$	$1(7)$
$-1(1,4,5,7)$	$-1(4,7)$	$-1(4)$

根据对应的测量结果，可以进行错误恢复。

5 容错量子计算

在前面章节中，我们忽略了量子纠错码的解码部分，这是因为在容错量子计算的逻辑下，可以在合理编码后的量子态上直接进行量子计算。需要注意的是，错误会在电路中传播与积累，并且纠错程序本身也会引入错误，因此必须小心地设计电路，才可以保证错误一直在可纠正范围内。

从理解上来说，前文讲述的几种编码都只能用以对抗单比特错误，但如果使用了跨界在多个比特上的门，那么错误将会传递到其他比特上，从而使得原先的编码不再有效。比如 X 错误发生在作用受控非门前的第一个量子比特上，有 $UX_1 = UX_1U^\dagger U = X_1X_2U$，相当于先作用完美受控非门，再在两个比特上同时发生 X 错误，可见造成了错误的传播。因此在设计编码时，必须使得错误只能扩展到一小部分区域。

5.1 阈值定理

一个容错的过程定义为：这个过程的一个组成部分发生错误，那么这个错误在过程最后输出的每一个编码量子比特区块中至多产生一个错误。

从而在只有一个单组成部分以最大概率 p 发生错误时，测量结果发生错误的概率为 $O(p^2)$。

一个没有经过容错程序的门的错误概率为 p，而经过了容错程序的门错误概率为 cp^2，这个 c 代表的含义可以理解为所有造成两个错误的情况数，由于编码的庞大，这个 c 可能比预计的大，比如 Steane 编码的 c 大概在 10^4，因而我们至少需要 $p < \frac{1}{c}$ 才可以使得容错程序起效果。

我们可以通过级联编码使得容错程序的效果指数级别放大，$p_{(k)} = cp_{(k-1)}^2 \Rightarrow cp_{(k)} = c^2p_{(k-1)}^2 \Rightarrow p_{(k)} = \frac{(cp)^{2^k}}{c}$，当达到精度要求时，$\frac{(cp)^{2^k}}{c} \approx \frac{\epsilon}{p(n)}$，其中 $p(n)$ 代表要实现的逻辑门个数，ϵ 代表目标精度。

于是电路的规模 $d^k = (2^k)^{log\ d} \approx (\frac{log(\frac{c\epsilon}{p(n)})}{log(cp)})^{log\ d} = O(P(log(\frac{p(n)}{\epsilon}))$，即电路规模只放大了多项式倍。

以上就是所谓的阈值定理：当电路的单个部分的错误概率低于某个阈值时，可以在电路规模扩大多项式倍的情况下达到任意的精度（逼近精度的速度是指数的）。

5.2 容错量子逻辑门

5.2.1 规范子

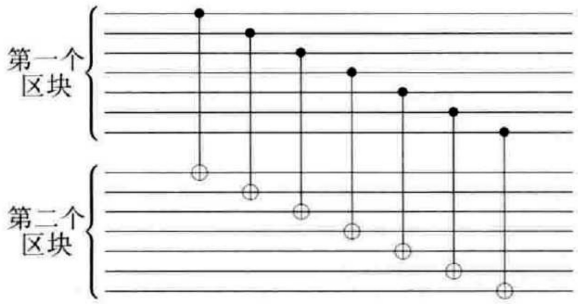
一个很朴素的想法是，如果某一种操作可以由编码的各个比特逐位完成（称为满足横向性），那么一个比特上的错误必然只会发展到一个比特上，幸运的是，许多逻辑门都是如此。

我们以 Steane 编码为例，$\bar{Z} = Z_1Z_2Z_3Z_4Z_5Z_6Z_7, \bar{X} = X_1X_2X_3X_4X_5X_6X_7$，要构造 $\bar{H}$ 门满足 $\bar{H}\bar{Z}\bar{H}^\dagger = \bar{X}, \bar{H}\bar{X}\bar{H}^\dagger = \bar{Z}$, 只需要 $\bar{H} = H_1H_2H_3H_4H_5H_6H_7$ 即可。

我们分析具体操作，实际上只要使得我们所涉及的逻辑门能够实现与单比特 Z, X 算子上的变换相同的逻辑比特上的门变换即可。

$SZS^\dagger = Z, SXS^\dagger = Y = iXZ$，因而 $S_1S_2S_3S_4S_5S_6S_7$ 使得 $\bar{Z} \to \bar{Z}, \bar{X} \to i^7\bar{X}\bar{Z} = -i\bar{X}\bar{Z}$, 因此实现 $\bar{S}$ 的操作为逐位作用 ZS 门，$\bar{S} = Z_1Z_2Z_3Z_4Z_5Z_6Z_7S_1S_2S_3S_4S_5S_6S_7$。

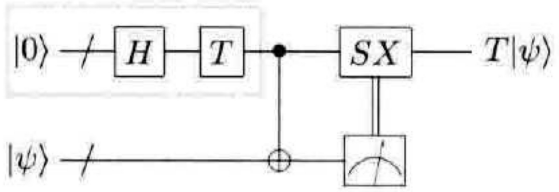
现在考虑受控非门，这似乎不可避免地会使得一个比特上的错误发展到两个比特上。但事实并没有这么糟糕，因为我们作用受控非门，总是对于两个逻辑比特而言的，如果说两个逻辑比特之间的受控非门可以像如下情况一样被实现，那么实际上单个区块中的错误还是只有一个，即我们每一套编码内部还是满足可纠错的条件的，具体情况可以参考下方 Steane 码所对应的量子线路：



以上，我们证明了任意的规范子操作都可以被容错实现，接下来我们需要构造出更多的容错门。

5.2.2 $\frac{\pi}{8}$ 门与 Toffoli 门

$\frac{\pi}{8}$ 门的构造需要使用到容错测量，其中的具体细节将在下一小节给出，我们此处先假设容错测量可以被实现。下面我们来看具体的构造：



注意，传输线上的斜线代表这是七量子比特，双传输线代表测量结果控制门操作。注意左上虚线部分中包含 T 门并非真的作用 T 门，而仅仅只是指示需要辅助态 $|\Theta\rangle = \frac{|0\rangle + e^{\frac{i\pi}{4}}|1\rangle}{\sqrt{2}}$，至于该辅助态如何容

错制备我们将使用另外的方法单独讨论。

首先分析该电路的作用：$a\left|0\right\rangle+b\left|1\right\rangle\rightarrow a\left|0\right\rangle+e^{\frac{i\pi}{4}}b\left|1\right\rangle$

具体地，借助辅助态 $\left|\Theta\right\rangle$，可以得到：$\left|\Theta\right\rangle\otimes\left|\psi\right\rangle\rightarrow\frac{1}{\sqrt{2}}\left|0\right\rangle\otimes(a\left|0\right\rangle+b\left|1\right\rangle)+\frac{1}{\sqrt{2}}e^{\frac{i\pi}{4}}\left|1\right\rangle\otimes(a\left|1\right\rangle+b\left|0\right\rangle)\rightarrow\frac{a|0\rangle+be^{\frac{i\pi}{4}}|1\rangle}{\sqrt{2}}\otimes\left|0\right\rangle+\frac{b|0\rangle+ae^{\frac{i\pi}{4}}|1\rangle}{\sqrt{2}}\otimes\left|1\right\rangle$

如果第二个比特的状态为 $\left|0\right\rangle$，则第一个量子比特保持不变，输出为 $\frac{a|0\rangle+be^{\frac{i\pi}{4}}|1\rangle}{\sqrt{2}}\propto T\left|\psi\right\rangle$。

如果第二个比特的状态为 $\left|1\right\rangle$,则第一个量子比特需作用 SX 门得到 $SX\frac{b|0\rangle+ae^{\frac{i\pi}{4}}|1\rangle}{\sqrt{2}}=S\frac{b|1\rangle+ae^{\frac{i\pi}{4}}|0\rangle}{\sqrt{2}}=\frac{ib|1\rangle+ae^{\frac{i\pi}{4}}|0\rangle}{\sqrt{2}}=\frac{e^{\frac{i\pi}{4}}}{\sqrt{2}}T\left|\psi\right\rangle\propto T\left|\psi\right\rangle$

而辅助态 $\left|\Theta\right\rangle$ 可以用容错测量的方式制备：

由于 $\left|\Theta\right\rangle=TH\left|0\right\rangle=THZ\left|0\right\rangle,THZHT^{\dagger}\left|\Theta\right\rangle=THZHT^{\dagger}TH\left|0\right\rangle=THZ\left|0\right\rangle=\left|\Theta\right\rangle,$

因此 $\left|\Theta\right\rangle$ 是算子 $THZHT^{\dagger}=TXT^{\dagger}=e^{-\frac{i\pi}{4}}SX$ 的特征值为 1 的特征向量，于是制备 $\left|\Theta\right\rangle$ 态可以通过不断测量 $e^{-\frac{i\pi}{4}}SX$ 直至出现结果 1 做到。

进一步地，我们希望用某一个容错操作将上述特征值为-1 的特征向量转成我们想要的 $\left|\Theta\right\rangle$，发现 $ZSXZ=-ZSZX=-ZZSX=-SX$，因此作用容错 Z 门既可以实现该操作。

总结来说，容错制备的过程为：容错测量算子 $e^{-\frac{i\pi}{4}}SX$，如果结果为 $+1$，则对应的态为 $\left|\Theta\right\rangle$，如果测量结果为-1，则作用容错 Z 门后得到目标态 $\left|\Theta\right\rangle$。

以上我们并没有给出这么设计的逻辑所在，现在给出设计思路，并希望将之运用于 Toffoli 门的设计上：

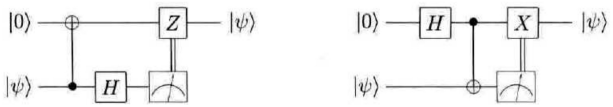
1. 构造能将将计算态 $\left|\psi\right\rangle$ 转移到辅助态上的量子电路。

2. 在计算态上作用特定门等价于在第 1 步电路的辅助态上作用该门。

3. 利用已经获得的容错门以及相互之间的等价关系，可以将最后的目标门转移到辅助态的前序电路上。

4. 利用设计好的容错测量操作代替作用在辅助态上的目标门操作。

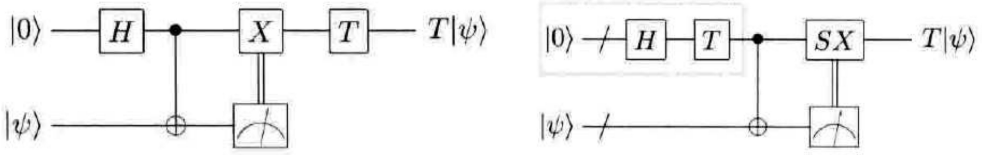
我们首先给出两个能够实现第 1 步的电路：



左图：$\left|0\right\rangle\otimes(a\left|0\right\rangle+b\left|1\right\rangle)\rightarrow a\left|00\right\rangle+b\left|11\right\rangle\rightarrow a\left|0\right\rangle\otimes\frac{|0\rangle+|1\rangle}{\sqrt{2}}+b\left|1\right\rangle\otimes\frac{|0\rangle-|1\rangle}{\sqrt{2}}=\frac{a|0\rangle+b|1\rangle}{\sqrt{2}}\otimes\left|0\right\rangle+\frac{a|0\rangle-b|1\rangle}{\sqrt{2}}\otimes\left|1\right\rangle\rightarrow\frac{a|0\rangle+b|1\rangle}{\sqrt{2}}\propto\left|\psi\right\rangle$。

右图：$\frac{|0\rangle+|1\rangle}{\sqrt{2}}\otimes(a\left|0\right\rangle+b\left|1\right\rangle)\rightarrow\frac{1}{\sqrt{2}}\left|0\right\rangle\otimes(a\left|0\right\rangle+b\left|1\right\rangle)+\frac{1}{\sqrt{2}}\left|1\right\rangle\otimes(a\left|1\right\rangle+b\left|0\right\rangle)=\frac{a|0\rangle+b|1\rangle}{\sqrt{2}}\otimes\left|0\right\rangle+\frac{a|1\rangle+b|0\rangle}{\sqrt{2}}\otimes\left|1\right\rangle\rightarrow\frac{a|0\rangle+b|1\rangle}{\sqrt{2}}\propto\left|\psi\right\rangle$

进而证明如下两个电路等价：



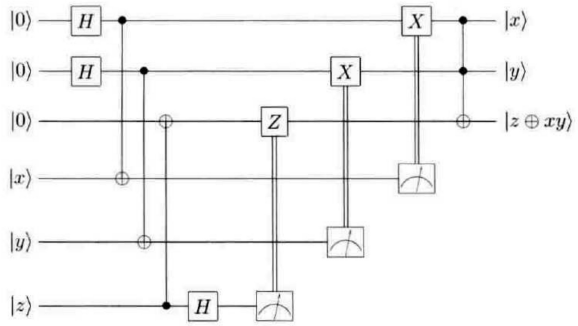
(a) (b)

当第二个比特测量结果为 1 时，双传输线控制的门不起作用，因而左图的 T 可以移动到 X 前方。

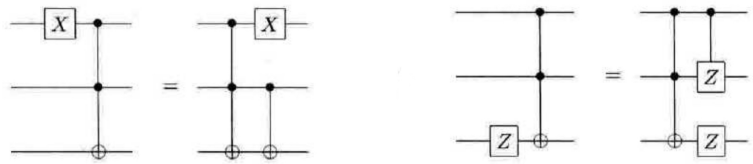
当第二个比特测量结果为-1 时，有 $TXT^\dagger = e^{-\frac{i\pi}{4}}SX \Rightarrow TX \propto SXT$，故可以将 T 移动至前序位置上。（注意作用门的方式从左往右，先作用的门在列表达式时要写在右边）

又 $T_1U = UT_1$，T 门与受控非门可交换，故左右两图等价。

下面进行 Toffoli 门的设计，首先完成步骤 1,2：



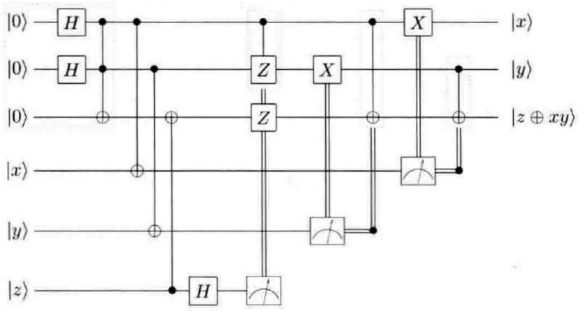
然后将最后的 Toffoli 门前移，移动过程需要使用如下两个电路，我们先进行证明：



左图：只需验证前两比特的特殊态 01 与 10，代入发现 01 都对应第三比特翻转，11 对应第三比特不翻转（翻转两次）。

右图：只需验证前两比特的特殊态 10 与 11：代入发现 10 对应前两比特不变，第三比特仅坐拥 Z 门；左侧 $|110\rangle \to |111\rangle$，右侧 $|110\rangle \to |1\rangle \otimes (-|1\rangle) \otimes (-|1\rangle) = |111\rangle$（注意相位是全局的，三个比特共同的）；左侧 $|111\rangle \to -|110\rangle$，右侧 $|111\rangle \to -|110\rangle$。

于是乎我们可以将电路图改造为：



注意第三个辅助比特的两次翻转并不因为前后关系而影响，因而可以将前三个辅助比特上的 Toffoli 门前置。

可以看到除了左上角的部分需要利用容错制备以外，其余部分均由规范子组成，因而整个电路是容错的。

5.2.3 容错测量

我们先前已经介绍了测量 M 的测量电路，除了其中的受控 M 门之外，电路是容错的。如果说我们只使用 1 个辅助比特，那么这个比特上的错误会传播到其余比特上造成错误累积，因此我们需要与编码比特数量相同的辅助比特来一一跨接受控 M 门，这同时意味着我们需要先制备猫态 $\frac{|00\ldots0\rangle+|11\ldots1\rangle}{\sqrt{2}}$，接下来考虑如何容错地制备并验证猫态。