

第十二章 量子误差纠正与保真度计算

§12.1 量子误差与纠正

1, 量子误差的来源和类型

i, 量子误差及其来源

和经典信息论的情况一样，由于量子位、量子门和量子存储器受环境和别的量子器件的相互作用影响，肯定会发生不希望量子纠缠，这些纠缠造成所考虑信息的退相干。于是，在任何量子信息计算或存储过程中，总会有一定的概率出现失误。防止这些失误的一种办法是改进硬件。然而这会很费钱费事耗时，并且也不是任何情况下都能办得到。*Shannon* 指出了这样一种途径：如其化力气在硬件上避免发生误差，不如化力气在软件上纠正误差会更好一些。纠正误差的基本思路是：由于信息在处理过程中存在各种产生误差的机制，于是通过附加某种冗余 (*redundent*) 信息，用添加额外多余位信息的办法，以增加信息的抗干扰能力，便于信息的正确编辑、存储、传递和读出。

ii, 量子误差的类型

从误差发生的部位来区分，误差的种类分为：

存储误差 (*memory errors*)

运算误差 (*operation errors*)

前者发生在所存储的信息上，不管这时有没有进行操作，这一般是静态型误差；后者是在操作期间发生的，是动态型误差。

从误差的性质来区分，误差的类型分为：

位翻转误差—— σ_x 型；

相位翻转误差—— σ_z 型；

混合型误差—— σ_y 型。

本讲集中讲述存储误差。因为这时相应的纠正手续易于理解。另一方面，它们不仅在量子计算中占据着重要地位，而且在量子通讯和量子信息中也如此。只有当人们了解了怎样纠正存储误差之后，作一些与传递过程及时间相关的修改，人们就能了解怎样去纠正操作运行中的动态型误差。下面先简明地说一下经典计算机中纠正误差的最直接的方法，然后再谈量子计算机中怎样做。

另外显然，发生误差的概率和存储的持续时间 τ 有关，记为 $P(\tau)$ 。通常假定 $P(0)=0$ 。

2，简单的经典误差纠正码【1】

i，码符与纠正前的失误概率

纠正误差的主要方法是基于“冗余码 (redundent code)”的办法。比如，用 3 个 *bit* 联合起来，共同表示“0”*bit* 和“1”*bit*。即

$$0_L = 000, \quad 1_L = 111$$

每个“逻辑位 (logical bit)”——称作码符 (code word)，实际上是由 3 个 *bit* 联合构成的。

于是，对任一逻辑位的信息，在存储 τ 时间之后，无误差的概率为 $[1-P(\tau)]^3$ 。发生 1 位 (1 个 *bit*) 误差，比如原先是 000，后

来误成 100 或 010 或 001 中的任一种，其概率为 $3P(\tau)[1-P(\tau)]^2$ 。发生 2 位（2 个 *bit*）误差，比如原先是 000，后来是 110、011、101 中的任一种，其概率为 $3P(\tau)^2[1-P(\tau)]$ 。发生 3 位——3 个 *bit* 全发生误差的概率为 $3P(\tau)^3$ 。这时原先是 000，后来是 111。

ii, 误差纠正和纠正后的失误概率；长时间的纠正

误差纠正由如下测量所组成：假如 3 个 *bit* 全在同一状态上，就不做操作；假如它们在不同态上，我们就采用多数表决的原则去翻转、纠正那个处于少数的不同状态的 *bit*。例如，这些纠正为：010→000、110→111 等等。

现在来看纠正后失误的概率。纠正以后 τ 时刻，得到维持在正确状态的概率为

$$P(\tau)_c = [1-P(\tau)]^3 + 3P(\tau)[1-P(\tau)]^2 = 1-3P(\tau)^2+2P(\tau)^3 \quad (12.1)$$

于是若要求 $P(\tau)_c > 1-P(\tau)$ ，则须 $P(\tau) < \frac{1}{2}$ 。因此，若已经是完全随机的 $P(\tau)=1/2$ ，这种“添加冗余位并用多数表决”的办法是行不通的。

假如要求将态保持一个长的时间 t ，就必须执行足够频密的测量。设在 t 时间内测量次数 N 足够大，以致间隔 $\tau=t/N$ 足够短，这时可设 $P(\tau) \approx c\tau$ 。于是在执行纠正之后的 t 时刻，保有正确态的概率将是

$$P_N^C(t) = \left[1 - 3\left(\frac{ct}{N}\right)^2 + 2\left(\frac{ct}{N}\right)^3 \right]^N \xrightarrow{N \rightarrow \infty} 1 \quad (12.2)$$

只要 $N \gg ct$ 足够大，这个概率可以与 1 接近到所希望的程度。这

就是利用量子 Zeno 效应所得的结果。

iii, 推广

以上叙述可以推广到一般情况：要求存储 k 个逻辑位（比如，对中文方块字编码时所需要的二进制编码的位数）并容许在 T 时间内有 l 位（ $l \leq t$, t 为设计中最大允许的误差位数）误差。例如，用 5 个 *bit*（按下面记号为 $n=5$ ）记录两个逻辑位（ $k=2$ ）

$$0_L = 00000; 1_L = 11111$$

容许有 2 个 *bit*——不能再多，否则就不是正确的多数位去纠正错误的少数位了。这种情况相应于（ $l \leq t=2$ ）。等等。

3, 简单的量子误差纠正码——自旋翻转型

i, 自旋翻转误差的纠正与码符

首先研究发生单一类型误差情况。设任务是存储某一单 *qubit* 上如下未知态到 T 时刻

$$|\psi(0)\rangle = c_0|0\rangle + c_1|1\rangle \quad (12.3)$$

称这个 *qubit* 为一个“逻辑 *qubit*”。假定在 τ 时刻后它有概率 $1-P(\tau)$ 仍保持不变，而有 $P(\tau)$ 的概率变成为

$$|\psi(\tau)\rangle = c_0|1\rangle + c_1|0\rangle \quad (12.4)$$

这种误差可称作自旋翻转误差，可用 σ_x 对 *qubit* 态作用表示。

采用冗余码办法可以纠正上面这类误差。例如，可以用 3 个 *qubit* 来对表示一个逻辑 *qubit*：

$$|\bar{0}\rangle_L = |000\rangle; |\bar{1}\rangle_L = |111\rangle \quad (5a)$$

于是上面的态（12.3）式成为

$$|\Psi\rangle_L = c_0|\bar{0}\rangle_L + c_1|\bar{1}\rangle_L = c_0|000\rangle + c_1|111\rangle \quad (12.5b)$$

由 (12.5) 式中两个态所撑开的子空间称为码符子空间。当然，有许多不同方式标记“逻辑零”位和“逻辑 1”位，比如有：

$$\begin{cases} |\bar{0}\rangle_L = \left\{ \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \right\}^{\otimes 3} \\ |\bar{1}\rangle_L = \left\{ \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle) \right\}^{\otimes 3} \end{cases} \quad (12.6)$$

这里，每一个“逻辑”位的基矢态都是 3 重直积的 3-qubit 的 *Schrodinger* 猫态【1】，等等。

ii, 纠正前后失误的概率

纠正前，在 τ 时间后，有：

无误差的概率为 $[1-P(\tau)]^3$ （态将仍然是 $|\Psi\rangle_L$ ）；

一位误差 $3P(\tau)[1-P(\tau)]^2$ （态变为 $\sigma_x^1|\Psi\rangle_L; \sigma_x^2|\Psi\rangle_L; \sigma_x^3|\Psi\rangle_L$ ）；

两位误差 $3P(\tau)^2[1-P(\tau)]$ （ $\sigma_x^1\sigma_x^2|\Psi\rangle_L; \sigma_x^1\sigma_x^3|\Psi\rangle_L; \sigma_x^2\sigma_x^3|\Psi\rangle_L$ ）；

三位有误差 $P(\tau)^3$ （态变为 $\sigma_x^1\sigma_x^2\sigma_x^3|\Psi\rangle_L$ ）。

误差纠正——如同经典情况：测量三个位是否在同一个态上。如果它们是在同一个态上，那就什么也不做；如果它们处在不同态上，就按照多数决定的原则去改变那个单独处在不同态上的 qubit。

注意，对于现在量子情况，所有这些测量必须以不破坏 (12.3) 式的相干叠加的方式进行。对于逻辑位为 (12.5b) 式的情况，用测量发现并纠正某个 qubit 位翻转误差的手续是：首先测量如下投影算符 (*projector*)

$$P_0 = |000\rangle\langle 000| + |111\rangle\langle 111| \quad (12.7)$$

这是个投影算符 $P_0^2 = P_0$ ，本征值是 (0,1)（比如设计力学量 P_0 为 $P_0 = \frac{1}{2^3}(\sigma_z^{(1)} + I^{(1)})(\sigma_z^{(2)} + I^{(2)})(\sigma_z^{(3)} + I^{(3)}) - \frac{1}{2^3}(\sigma_z^{(1)} - I^{(1)})(\sigma_z^{(2)} - I^{(2)})(\sigma_z^{(3)} - I^{(3)})$ ）。假如得到 1，表明原态 (12.5b) 未发生误差，就放下这个量子逻辑位不动；假如得到 0，就对它作下面测量，试探是否发生在第一个 *qubit*,

$$P_1 = |100\rangle\langle 100| + |011\rangle\langle 011|$$

此时若得到 1 就施加局域么正算符 σ_x^1 ；若不是，再试探第二个 *qubit*,

$$P_2 = |010\rangle\langle 010| + |101\rangle\langle 101|$$

此时如得到 1 就施加局域么正算符 σ_x^2 ；而如果不是 1，就可以直接对第三个 *qubit* 施加局域么正变换 σ_x^3 ，对其进行纠错(注意此时已不必作测量 $P_3 = |001\rangle\langle 001| + |110\rangle\langle 110|$ ，但假如还想作，将肯定得到 1)。总之，这样手续的结果是，若没有误差或是一位误差，这个量子逻辑位将被纠正；但如果存在两位或多位误差，将不能得到纠正。

在如此纠正之后，得到正确态的概率为：

$$P(\tau)_c = [1 - P(\tau)]^3 + 3P(\tau)[1 - P(\tau)]^2 = 1 - 3P(\tau)^2 + 2P(\tau)^3 \quad (12.8)$$

于是结果和经典情况的 (12.1) 式一样。

长时间纠正问题。可以采用量子 *Zeno* 效应来保持一个量子态不受扰动到任意长的时间。也可以推广到一般情况：有 k 个逻辑位，每个逻辑位由 n 位 *qubit* 组成，并容许误差为 l 位 *qubit*。

4, 简单的量子误差纠正码——位相翻转型

i, 位相翻转误差的纠正与码符

再研究发生另一类单一误差情况。设发生位相翻转误差：

$$|\psi\rangle = c_0|0\rangle - c_1|1\rangle \quad (12.9)$$

这个误差也称作自旋翻转误差，因为它可以表示为由 σ_z 作用在 *qubit* 上造成的。

这时，方便的做法是用 σ_x 本征态

$$|\pm\bar{e}_x\rangle \equiv |\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2} \quad (12.10)$$

来代替 $|0\rangle$ 态和 $|1\rangle$ 态。理由是，这时产生 σ_z 型位相误差将导致基矢的翻转 $|+\rangle \leftrightarrow |-\rangle$ 。于是问题就等价于前面已经分析过的基矢翻转情况。特别是，正确的编码方法现在应当是

$$|0\rangle_L = |+++ \rangle; \quad |1\rangle_L = |-- - \rangle \quad (12.11)$$

于是不需要再复述。

显然，在实际情况中，鉴别实际发生的误差究竟属于这两类误差中哪一类是重要的。这样才有针对性地进行编码设计。

5, 量子误差纠正码——一般情况【1】

i, 任意误差。以上讲的单一类型误差的纠正具有经典性质，原则上也适用于经典情况。现在叙述量子情况下经常发生的任意类型误差。由下面 (12.14) 式量子 *Hamming* 界限可知，情况要复杂得多。

设“逻辑量子位”由 k 个 *qubit* 组成，它们是需要用编码的办法来保护以防止发生误差丢失的被编码量子位。一般办法是以

冗余的方式，附加 $n-k$ 个 *qubit* 来存储 k 个逻辑 *qubit* 信息，用以增加可靠性来抵抗干扰，使得被编码的信息相对地不易遭受破坏。于是，一个量子误差纠正码（*quantum error-correcting code*——*QECC*）是量子态空间的一种扩张型线性映射，它是在设定要求下将 k 个 *qubit* 态空间（维数 2^k ）向 n （ $n > k$ ）个 *qubit* 态空间（维数 2^n ）映射。其任务是用 n 个 *qubit* 编码 k 个逻辑位的量子信息，以保证在 T 时刻内，即使 n 个 *qubit* 中最多有 t 个 *qubit* 发生任意类型量子误差，仍然能够予以纠正。

下面寻找能够完成这个任务的码符并说明误差纠正手续。

所谓任意量子误差是指，在第 j 个 *qubit* 上发生了相当于施加一个任意算符的变换。注意，不同 *qubit* 间也可能存在相互干扰。任意误差算符在分解之后，对第 j 个 *qubit* 二维态空间的作用总可以再分解为 $\{\sigma_0^j, \sigma_x^j, \sigma_y^j, \sigma_z^j\}$ 的线性组合。因此，发生在第 $j_1, j_2, \dots, j_l$ 位总共 l 个 *qubit* 上的一个任意误差算符 $A_l^{j_1 j_2 \dots j_l}$ 可表示为

$$\left\{ \begin{aligned} A_l^{j_1 j_2 \dots j_l} &= \sum_{\alpha_1} \sum_{\alpha_2} \dots \sum_{\alpha_l} c_{\alpha_1, \alpha_2, \dots, \alpha_l} \sigma_{\alpha_1}^{j_1} \sigma_{\alpha_2}^{j_2} \dots \sigma_{\alpha_l}^{j_l} \equiv \sum_{\alpha_1} \sum_{\alpha_2} \dots \sum_{\alpha_l} c_{\alpha_1, \alpha_2, \dots, \alpha_l} E_{\alpha_1 \alpha_2 \dots \alpha_l}^{j_1 j_2 \dots j_l} \\ E_{\alpha_1 \alpha_2 \dots \alpha_l}^{j_1 j_2 \dots j_l} &\equiv \sigma_{\alpha_1}^{j_1} \sigma_{\alpha_2}^{j_2} \dots \sigma_{\alpha_l}^{j_l} \end{aligned} \right. \quad (12.12)$$

这里，系数 c 是一些复常数， $\alpha_i = 0, x, y, z$ 。为了简便当 $\alpha_i = 0$ 时，

$\sigma_0^{j_1} = \sigma_0^{j_1} = \dots = \sigma_0^{j_l}$ 是各个 *qubit* 的单位算符。

ii, **误差纠正**。量子误差纠正方案的思想是：

其一，码符。考虑用 n 个 *qubit*（*Hilbert* 空间 H 维数是 2^n 维）去对 k 个逻辑 *qubit* 进行编码（码符子空间 H_L 是 2^k 维）。显然，

(12.12) 式误差算符 $A_l^{j_1 j_2 \dots j_l}$ 中，除可能有的叠加系数外，自旋乘积算符 $E_{\alpha_1 \alpha_2 \dots \alpha_l}^{j_1 j_2 \dots j_l}$ 会将子空间 H_L 变换到 H 的下述对应子空间中

$$E_{\alpha_1 \alpha_2 \dots \alpha_l}^{j_1 j_2 \dots j_l} : H_L \rightarrow H_{\alpha_1 \alpha_2 \dots \alpha_l}^{j_1 j_2 \dots j_l} \in H \quad (12.13)$$

但由于算符 E 是幺正的，不会改变作用空间的维数，于是与每一个算符 E 对应的这个子空间的维数仍然是 2^k 。但 E 中所含相关 *qubit* 自旋算符(以及可能包含的叠加系数)可能对原先 H_L 的基矢产生变换。

显然，码符子空间 H_L 应当如此设计，使得在全部误差作用下，码符子空间 H_L 中原有正交态仍然继续保持彼此正交。这个条件对所需的 *qubit* 数目 n 设下了下限。因为所有这些正交子空间都必须镶嵌在整个 H 中。

现在计算 n 的这个下限——量子 *Hamming* 界限。为此，先必须数出不同的误差算符 E 的个数，这些 E 全都包含总数不超过 t 个(各自分别作用在 n 个 *qubit* 中的一部份 *qubit* 上) *Pauli* 算符。首先计算只包含 l 个 *Pauli* 算符的那些算符，然后再考虑 $l=0 \rightarrow t$ 求和。对于其中只含 l 个 *Pauli* 算符的情况，由于从 n 个 *qubit* 中选出 l 个 *qubit* 的组合数为 $n!/[l!(n-l)!]$ ，在这 l 个 *qubit* 中的每一个又都有三个可能的 *Pauli* 算符，所以一共有 $3^l n!/[l!(n-l)!] = 3^l \binom{n}{l}$ 个误差算符。于是总数不超过 t 个 *qubit* 上出现误差算符的总个数是 $l=0 \rightarrow t$ 的求和 ($l=0$ 对应于全部 n 个 *qubit* 上无差错情况)。为了以非简并编码方式编码 k 个逻辑 *qubit*，这些差错中的每一个都必须对应于一个 2^k 维子空间。与

此同时，误差算符作用结果虽使态矢出了原先的 H_L 空间，但所有这些子空间，都仍然包含在 H 中。所以必须有

$$2^k \sum_{l=0}^t 3^l \binom{n}{l} < 2^n \quad (12.14)$$

这就是量子 *Hamming* 界限。例如，由此式可知，当 $k=1$ 时，只对 $t=1$ ，所需最小位数为 $n=5$ 。只有这样，至少用 5 个 *qubit* 来编码一个 *qubit*，才能容许 5 个 *qubit* 中的任一个 *qubit* 发生(包括全部三类误差的)任意类型的量子误差，还能纠正。详细参见最后例算。

提个醒，如果只发生一种误差（比如经典情况下常见的位翻转类型 $\sigma_x: 0 \leftrightarrow 1$ ），对于 $k=t=1$ ，只需 $n=3$ 。

其二，一般手续。 设 n 已满足量子 *Hamming* 界限，并且已经按要求编好了纠正码。于是，首先实行向全体子空间 (12.13) 的测量投影（这些子空间是由全部 $E_{\alpha_1 \alpha_2 \dots \alpha_l}^{j_1 j_2 \dots j_l}$ 作用所造成的）。因为这些子空间已经编码设计为彼此正交，只有一个投影会给出为 1，并且系统的态将被投影到相应的子空间 $H_{\alpha_1 \alpha_2 \dots \alpha_l}^{j_1 j_2 \dots j_l}$ 。然后，施加么正变换 $E_{\alpha_1 \alpha_2 \dots \alpha_l}^{j_1 j_2 \dots j_l}$ 。手续的第一部分相当于探测误差。而第二部分则相当于纠正误差。显然，这样做事实上纠正了 (12.12) 式形式的所有 $l \leq t$ 的误差。下面证明：

【证明】 给定码符子空间中任意态 $|\psi\rangle \in H_L$ ，假如产生了 (12.12) 式形式的一个误差，态将成为 $A_l |\psi\rangle$ ，这是所有子空间 (12.13) 的直和。测量将把这个态投影到这些子空间中的一个。使得在测量之后态成为

$$E_{\alpha^1 \alpha^{2L} \alpha^l}^{j^1 j^{2L} j^l} |\psi\rangle \quad (12.15)$$

由于 $(E_{\alpha^1 \alpha^{2L} \alpha^l}^{j^1 j^{2L} j^l})^2 = 1$ ，纠正将会产生正确的态 $|\psi\rangle$ 。证毕。

现在，总的任务是寻找这样的纠正码，它们能够纠正 n 个 $qubit$ 中有 t 个发生任意误差。这个任务归结为：寻找正确的 2^k 维码符号子空间 H_L ，使得在所有误差算符 E 的作用下，码符号子空间基矢的相互正交性仍然保持。

iii, 码稳定子

这里主要考虑怎样去构造码符，使得能够用 n 个 $qubit$ 编码 k 个逻辑位（设 n 已满足 *Hamming* 界限）。

回忆 *Pauli* 算符的一些性质：

$$\begin{aligned} [\sigma_x^i, \sigma_y^j] &= 2i\sigma_z^i & \{\sigma_x^i, \sigma_y^j\} &= 0 & [\sigma_x^i, \sigma_y^j] &= 0 (i \neq j) \\ [\sigma_z^i, \sigma_x^j] &= 2i\sigma_y^i & \{\sigma_z^i, \sigma_x^j\} &= 0 & [\sigma_z^i, \sigma_x^j] &= 0 (i \neq j) \\ [\sigma_y^i, \sigma_z^j] &= 2i\sigma_x^i & \{\sigma_y^i, \sigma_z^j\} &= 0 & [\sigma_y^i, \sigma_z^j] &= 0 (i \neq j) \end{aligned}$$

一些由 *Pauli* 算符乘积构成的组合算符的群性质。设 n 个 $qubit$ 的全部 *Pauli* 算符乘积组成一个集合：

$$G_1 = (g_1, g_2, \dots) \quad (12.16)$$

比如， $g_1 = \sigma_x^1 \sigma_y^3 \sigma_z^4 \sigma_x^5$, $g_2 = \sigma_y^1 \sigma_x^2 \sigma_y^3 \sigma_y^5$, $g_3 = \sigma_z^1 \sigma_y^2 \sigma_x^3 \sigma_x^4 \sigma_x^5, \dots$ 。这个集合共有 4^n 元素。记 $G_+ = G_1 \cup (-G_1)$; $G_- = iG_+$ 。于是集合

$$G = G_+ \cup G_- \quad (12.17)$$

是阶数为 4^{n+1} 的有限群，称作 *Pauli 群*。这个集合有如下性质：

——由于 $(\sigma_\alpha^i)^2 = 1$ ，并且不同 $qubit$ 的 *Pauli* 算符都对易，所以 G_+ 所有元素的平方均为 1，并且都是厄米的和么正的。而 G_-

的所有元素的平方均为-1，并且都是反厄米的和么正的。

——假如 A 和 $B \in G$ ，于是 $AB = \pm BA$ ，就是说，要么是 $[A, B] = 0$ ，要么是 $\{A, B\} = 0$ 。比如，

$$\begin{aligned} g_1 g_2 &= (\sigma_x^1 \sigma_y^1) \sigma_x^2 (\sigma_y^3 \sigma_y^3) \sigma_z^4 (\sigma_x^5 \sigma_y^5) = g_2 g_1 \\ g_1 g_3 &= (\sigma_x^1 \sigma_z^1) \sigma_y^2 (\sigma_y^3 \sigma_x^3) (\sigma_z^4 \sigma_x^4) (\sigma_x^5 \sigma_x^5) = -g_3 g_1 \end{aligned}$$

当 A 和 B 中每个 *qubit* 的不同自旋算符出现的总次数都是偶数时，有 $[A, B] = 0$ ；当每个 *qubit* 不同自旋算符出现的总次数是奇数时，有 $\{A, B\} = 0$ 。

码符和稳定子（也见【3】p.453）。记 H_L 为 2^k 维码符子空间。

【定义】 码符子空间 H_L 的稳定子 S 是 G 中各个 *qubit* 的 *Pauli* 算符乘积组成的一组算符，它们能够保持码符子空间 H_L 态不变：

$$S = \{M \in G, M|\psi\rangle = |\psi\rangle, \forall |\psi\rangle \in H_L\} \quad (12.18)$$

稳定子 S 有以下性质：

——**可对易性**。 S 是有限且可对易的。若 $M, N \in S$ ，则 $[M, N] = 0$ 。就是说，是个有限的 *Abel* 群，证明很简单： $\because M, N \in G$ ，它俩不是对易就是反对易，将它俩的对易子和反对易子作用到 H_L 的任一态 $|\psi\rangle$ 上，就知道不可能是反对易的。

——**群性质**。 H_L 的不变变换的 S 是 G 的一个子群。由于 G 是有限群，按 *Lagrange* 定理（【3】附录 B）， S 元素（容许重复）可以生成全部 G 元素。

—— S 任一元素的平方必为 1。因为按 G 元素的性质，平方不是 +1，就是 -1。现在 $\because M^2|\psi\rangle = |\psi\rangle$ ， $\therefore M^2 = 1$ 。

——和 $(Z_2)^\alpha$ 同构。这里 Z_2 是在 XOR (等价于 $\text{mod} 2$ 的加法) 运算下由元素 0 和 1 构成的 2 阶循环群 ($Z_m = (0, 1, \dots, m-1, \text{mod } m)$ 为 m 阶循环群)。既然 S 是一个元素平方均为 1 的 $Abel$ 群, S 必定和给定正整数 α (阶数) 的 2 循环群的直积群 $(Z_2)^\alpha$ 同构。这为下面寻找 S 的元素提供了依据。

——生成元。给定这个同构下, 存在 S 的一组元素, 使得

a) S 的所有元素都可以写成这组元素的乘积;

b) 它们是最少的。就是说, 不存在另一组个数较少的元素, 也能将 S 所有元素表示成乘积形式。记这组生成元为 $M_1, M_2, \dots, M_\alpha$ 。

—— H_L 的维数。 H_L 的维数必定为 $2^{n-\alpha}$, α 是 S 生成元个数。这可如下看出: 所有生成元都对易, 并且有本征值 (及本征态) ± 1 。 α 个生成元必定撑开 2^α 维子空间。接着, 可以将 $Hilbert$ 空间 H 按这些生成元的本征值分解成一些正交本征子空间, 每个子空间都是由全体生成元的本征值表征。所以每个子空间维数是 $2^{n-\alpha}$ 。其中, 对应本征值全为 +1 的子空间就是 H_L 。由此得到

$$k = n - \alpha, \quad \dim H_L = 2^k$$

【举例】3quits, $n=3$, $S = \{I, \sigma_z^1 \sigma_z^2, \sigma_z^2 \sigma_z^3, \sigma_z^1 \sigma_z^3\} = S = \{I, \sigma_z^1 \sigma_z^2, \sigma_z^2 \sigma_z^3\}$ 。这里, 第三个元素 $\sigma_z^1 \sigma_z^3$ 由前两者乘积构成, 不独立, 不予考虑。 $\sigma_z^1 \sigma_z^2$ 所固定的子空间由 $\{|000\rangle, |001\rangle, |110\rangle, |111\rangle\}$ 所张成, $\sigma_z^2 \sigma_z^3$ 所固定的子空间由 $\{|000\rangle, |100\rangle, |011\rangle, |111\rangle\}$ 所张成。显然, $\{|000\rangle, |111\rangle\}$ 是 S 元素共有的不变子空间, 它们撑开 $k=1$ 的 2^k 维子空间 H_L 。

误差算符保持正交性问题。记 E_1 和 E_2 为 (12.12) 式中的两个任意误差算符。按照上面量子 *Hamming* 界限思想，应当有：“当且仅当对所有 $|\psi\rangle, |\phi\rangle \in H_L$ ， $E_1|\psi\rangle$ 和 $E_2|\phi\rangle$ 都相互垂直，误差纠正才是可能的”。

接着可以证明：如果算符 E_1E_2 和稳定子 S 中至少一个元素 M 反对易，这个条件就将自动得到满足。

【证明】

$$\langle \phi | E_1 E_2 | \psi \rangle = \langle \phi | E_1 E_2 M | \psi \rangle = -\langle \phi | M E_1 E_2 | \psi \rangle = -\langle \phi | E_1 E_2 | \psi \rangle \quad (12.19)$$

这导致 $\langle \phi | E_1 \cdot E_2 | \psi \rangle = 0$ 。

注意，除了 S 本身元素外， G 中任一个 E 算符（包括 $E = E_1 E_2$ ）总会和 S 中某个或某些元素反对易。这可以用反证法推知。因为，否则 E 将和 S 所有元素都对易，这导致 G 是有限的 *Abel* 群。这和原先的假设相悖。证毕。

于是现在的问题就变成为：寻找一个子空间 H_L 和一个稳定子 S ，使得 G 中每一个长度不超过 $2t$ （ $\because$ 每个 E 的长度不超过 t ）的（非平庸的）误差算符和 S 中某一元素反对易。

iv, 纠正手续，怎样确定码稳定子及 H_L

纠正手续。现在问题归结为，寻找一个子空间 H_L 和稳定子 S 。为此首先要找到由 *Pauli* 算符乘积作为元素所组成的这个 *Abel* 群——二阶循环群 S ，使得 G 中所有长度直到 $2t$ 的非平庸的误差算符和 S 中某元素反对易。一旦稳定子 S 知道了，就能找到 H_L ，也就是说，就能找到码符。

怎样确定码的稳定子。为确定 $\alpha = n - k$ 个生成元，如下进行：

——对于一个给定的生成元 $M \in S \in G$ ，定义自变数 N （ G 中全部 *Pauli* 自旋算符）的一个函数，【定义 $f_M(N): G \rightarrow Z_2$ 】所有与 M 对易的 N ，函数值为 0；和 M 反对易的 N ，函数值为 1，

$$f_M(N) = \begin{cases} 0, & \text{if } [M, N] = 0 \\ 1, & \text{if } \{M, N\} = 0 \end{cases} \quad (12.20)$$

若 S 由 $M_1, M_2, \dots, M_\alpha$ ($\alpha = n - k$) 所组成，扩充定义 $f: G \rightarrow (Z_2)^\alpha$ 为

$$f(N) = [f_{M_1}(N) f_{M_2}(N) \cdots f_{M_\alpha}(N)] \quad (12.21)$$

下面将把 $f(N)$ ，也就是 (12.21) 式的右边写为一个 α 位的二进制序列。例如， $f(I) = 00 \cdots 0$ ，这里 $I = I^1 I^2 \cdots I^n$ 是单位算符。

——希望如此挑选 S ，以便对长度一直到 $2t$ 的所有 E ， $f(E) \neq f(I)$ ，即总是非零的（于是所有 E 必定和某个或某些 M 反对易）。为保证如此，办法是记 $E = E_1 E_2$ ， E_1 和 E_2 长度 $\leq t$ ，只须

$$f(E) \neq 0 \quad \text{if} \quad f(E_1) \neq f(E_2)$$

【这里是说， f 与 E 同态 (*homomorphism*) $f(AB) = f(A)f(B)$ ；另一方面，在 Z_2 的操作是 *XOR*。于是，当且仅当 $f(A) \neq f(B)$ 时， $f(A)f(B)$ 不为 $00 \cdots 0$ 】。这样，只需要如此建立起 S ，使得 $f(E_i)$ 对长度不超过 t 的每个 E_i 都相异，就可以了。

——实现的具体办法之一是，为长度不超过 t 的每个可能误差 E ，按照同态结构遵从如下一些限制条件来选用有 α 位的一组数（ $\neq 00 \cdots 0$ ），然后由此找到生成元。例如

$$f(\sigma_y^i) = \text{XOR}[f(\sigma_x^i), f(\sigma_z^i)] \quad (12.22)$$

怎样确定 H_L 。已知生成元后，就可以在种子态——逻辑 *qubit*

态 $|i\rangle_L$ (二进制记号) 基础上构造

$$|\psi^i\rangle \propto \sum_{M \in S} M|i\rangle_L \quad (12.23)$$

假如结果不是零, 这个态就属于 H_L , 并且能够纠正最多 t 个 *qubit* 任意误差的抗干扰态。因为, 如果对态 $|\psi\rangle$ 施加任一算符 $M' \in S$, 就相应于重排求和式子 (S 是个有限群)。这就是说, 求和式 $\sum_{M \in S} M$ 所相应的算符对于乘任何 $M, \forall M \in S$ 是不变的,

$$M_1|\psi\rangle = M_2|\psi\rangle = |\psi\rangle$$

于是, 人们可以用各个种子态 $|00\cdots 00\rangle_L, \cdots$ 去尝试, 一直到找出全部 k 个正交态为止。作为一组正交不变基, 它们共同撑开码符号子空间 H_L , 并且能够纠正 *Hamming* 界限 n 个 *qubit* 中不超过 t 个 *qubit* 任意误差算符 E 的作用。

v, 【例算】单个 *qubit* 中一种误差的纠正【1】

a) 现在的问题和误差。考虑 $k=t=1, n=5$ 情况。这时 $\alpha=n-k=4$, 误差算符是 16 个: 每个 *qubit* 有 3 个 *Pauli* 算符, 5 个 *qubit* 共 15 个, 再加一个单位算符。

b) α 位数。对每个 E 算符选一个 4 位数 (α 位), 它们必须是不一样的, 并且符合约束条件 $f(\sigma_y^i) = \text{XOR}[f(\sigma_x^i), f(\sigma_z^i)]$ 。由于是 *XOR* 操作, 同一个 i (同一个 *qubit*) 不同 (x, y, z) 并位于相同位上的三个数都是 *mod2* 加法关系。于是只能三个全为 0、一个 0 二个 1, 不会出现三个数中有两个 0, 或者三个都为 1 的情况。例如, 可以选择:

$$\begin{array}{lll}
\sigma_x^1:0110, & \sigma_z^1:1000, & \sigma_y^1:1110, \\
\sigma_x^2:0001, & \sigma_z^2:0100, & \sigma_y^2:0101, \\
\sigma_x^3:0111, & \sigma_z^3:1010, & \sigma_y^3:1101, \\
\sigma_x^4:1011, & \sigma_z^4:0010, & \sigma_y^4:1001, \\
\sigma_x^5:0011, & \sigma_z^5:1100, & \sigma_y^5:1111,
\end{array} \quad (12.24)$$

这里每一行内同一位数字都存在约束条件，表现为它们之间有 $\text{mod}2$ 加法关系，但实际上，依据 S 和 $(Z_2)^\alpha$ 同构定理，这种 XOR 操作决定着 *Pauli* 自旋算符的代数表示。

c) **生成元**。比如 (12.24) 式第一行，是 5 个 *qubit* 中第一个 *qubit* 的三个自旋量 $\sigma_x^1, \sigma_z^1, \sigma_y^1$ ，相应有三个 4 位数。第 1 个生成元 M_1 的决定：第一个 *qubit* 三组数的第 1 位数合起来决定 M_1 中应含第一个 *qubit* 的哪个自旋算符；第二个 *qubit* 三组数的第 1 位数合起来决定 M_1 中应含第二个 *qubit* 的哪个自旋算符；等等。现在， $\sigma_x^1, \sigma_z^1, \sigma_y^1$ 的三个第 1 位数合起来是 011，按 (12.20) 式，有 $[M_1, \sigma_x^1] = 0$ ， $\{M_1, \sigma_z^1\} = 0$ ， $\{M_1, \sigma_y^1\} = 0$ 。这就决定了 M_1 包含 σ_x^1 。接着继续去决定 M_1 包含第 2 个 *qubit* 的哪个自旋 $\sigma_x^2, \sigma_z^2, \sigma_y^2$ 。由于第 2 个 *qubit* 三组数的第 1 位三个数全都为 0， M_1 只含第 2 个 *qubit* 的单位算符 σ_0^2 （常略写）。如此等等，汇合起来成为 $M_2 = \sigma_x^1 \sigma_x^3 \sigma_z^4 \sigma_x^5$ 。再比如，决定 M_2 ：它包含第 1 个 *qubit* 的哪个自旋，要看相应的 $\sigma_x^1, \sigma_z^1, \sigma_y^1$ 三组数中处于第 2 位的三个数，它们合起来为 (101)，这个 0 属于 σ_z^1 ，于是 M_2 含 σ_z^1 。接着看 M_2 含第 2 个 *qubit* 的哪个自旋算符。这由相应的 $\sigma_x^2, \sigma_z^2, \sigma_y^2$ 三组数中处于第 2 位数上的三个数 (011) 决定，这个 0 属于 σ_x^2 ，于是 M_2 含 σ_x^2 ；

第 3 个 *qubit* 的第 2 位的三个数是 (101)，应含 σ_z^3 ；第 4 个 *qubit* 的第 2 位的三个数为 (000)，只含单位算符 σ_0^4 ；第 5 个 *qubit* 的第 2 位数是 (011)，应含 σ_x^5 。汇合起来成为 $M_2 = \sigma_z^1 \sigma_x^2 \sigma_z^3 \sigma_x^5$ 。总之最后得到：

$$\begin{aligned} M_1 &= \sigma_x^1 \sigma_x^3 \sigma_z^4 \sigma_x^5 \\ M_2 &= \sigma_z^1 \sigma_x^2 \sigma_z^3 \sigma_x^5 \\ M_3 &= \sigma_z^1 \sigma_y^3 \sigma_y^4 \sigma_z^5 \\ M_4 &= \sigma_z^2 \sigma_z^3 \sigma_z^4 \sigma_z^5 \end{aligned} \quad (12.25)$$

显然，它们彼此全都对易。

d) 码符。从两个种子态之一的 $|00000\rangle$ 态出发，作为方程 (12.23) 中的 $|m\rangle$ 态，经过 (12.25) 式 4 个生成元算符（以乘积方式）生成 S 的全部算符，包括 4 个 M_i 和单位算符

$M_0 = \sigma_0^1 \sigma_0^2 \sigma_0^3 \sigma_0^4 \sigma_0^5$ ，以及

$$\begin{aligned} M_1 M_2 &= -\sigma_y^1 \sigma_x^2 \sigma_y^3 \sigma_z^4; & M_1 M_3 &= -\sigma_y^1 \sigma_z^3 \sigma_x^4 \sigma_y^5; & M_1 M_4 &= -\sigma_x^1 \sigma_z^2 \sigma_y^3 \sigma_y^5; \\ M_2 M_3 &= -\sigma_x^2 \sigma_x^3 \sigma_y^4 \sigma_y^5; & M_2 M_4 &= -\sigma_z^2 \sigma_y^3 \sigma_z^4 \sigma_y^5; & M_3 M_4 &= -\sigma_z^1 \sigma_z^2 \sigma_x^3 \sigma_x^4; \\ M_1 M_2 M_3 &= -\sigma_x^1 \sigma_x^2 \sigma_x^4 \sigma_z^5; & M_1 M_2 M_4 &= -\sigma_y^1 \sigma_y^2 \sigma_x^3 \sigma_z^5; \\ M_2 M_3 M_4 &= -\sigma_y^2 \sigma_y^3 \sigma_x^4 \sigma_x^5; & M_1 M_3 M_4 &= -\sigma_y^1 \sigma_z^2 \sigma_z^4 \sigma_y^5; \\ M_1 M_2 M_3 M_4 &= \sigma_x^1 \sigma_y^2 \sigma_z^3 \sigma_y^4 \end{aligned}$$

共同组成群 S 。将它们向种子态 $|0\rangle_L = |00000\rangle$ 作用并求和，由

$|0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ ，每个 *qubit* 的自旋算符对态作用分别为 $\sigma_x|0\rangle = |1\rangle$ ，

$\sigma_y|0\rangle = -i|1\rangle$ ， $\sigma_z|0\rangle = -|0\rangle$ 。算得各项并经求和，即得下式态

$$\begin{aligned} |0\rangle\rangle &\equiv |0\rangle_L = |6\rangle + |17\rangle + |23\rangle + |0\rangle \\ &\quad - |4\rangle - |11\rangle - |13\rangle - |26\rangle \end{aligned} \quad (12.26)$$

这里，态中 *qubit* 编号自左往右为第 1 号 *qubit* 到第 5 号 *qubit*。

与此同时，采用另一个种子态 $|1\rangle_L = |11111\rangle$ ，类似做法得到

另一个能够抵抗发生单 *qubit* 任意误差的表示（别忘了单位元素作用到种子态时将保留种子态，现在它算是 $|1\rangle$ 态）：

$$\begin{aligned} |1\rangle\rangle \equiv |1\rangle_L = & |1\rangle + |10\rangle + |16\rangle + |20\rangle \\ & + |22\rangle + |29\rangle - |7\rangle - |27\rangle \end{aligned} \quad (12.27)$$

这样就找到了采用 5 个 *qubit* 编码，能够纠正任一单 *qubit* 发生任意误差的一种编码方案。而 (12.26)、(12.27) 两式便是撑开单 *qubit* 码符空间 H_L 的两个逻辑位——能够经受任一单 *qubit* 的任意误差而仍保持正交性，因而能作误差纠正的——码符子空间的两个基矢。

参考文献

- 【1】 *The Lecture Notes of Innsbruck University, Innsbruck, Austria, 1998.*
- 【2】 *J.Preskill, Lecture Notes for Physics 229: Quantum Information and Computation, CIT, Chapter 7, 2001.*
- 【3】 *M.A.Nielsen and I. L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, 2000.*