量子信息导论
PHYS5251P

中国科学技术大学
物理学院/合肥微尺度物质科学国家研究中心

陈凯

2025.12

第五章 量子纠错

1. **量子纠错的基本理论**
2. 比特翻转量子码
3. 纠单比特错误量子码，Shor码
4. 量子错误刻画
5. 纠缠纯化与量子纠错
6. 量子码的构造（经典线性码，CSS码）
7. 稳定子码(Stabilizer Codes)
8. 普适量子计算

一、量子纠错基本理论

(一)量子纠错的作用：保护信息免受噪声干扰

(二) 量子纠错与经典纠错的区别

(1) **量子态不可复制。**经典信息：通过克隆的方式，加入冗余信息来编码消息，例如

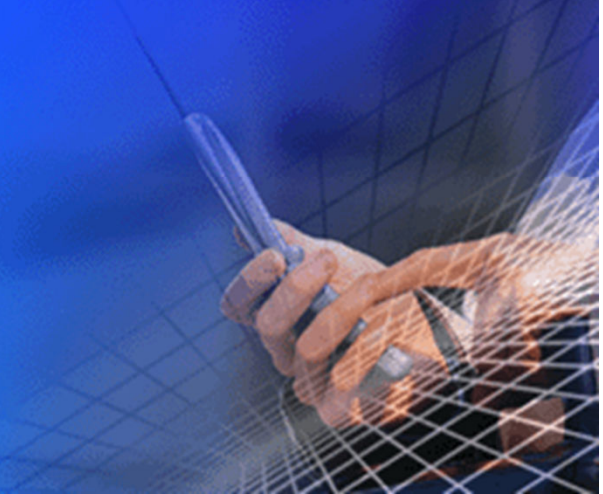
一、量子纠错基本理论

例如经典码

$0 \longrightarrow 000$

$1 \longrightarrow 111$

如果发生错误的概率为P，加入纠错码后发生错误的概率由 $p \longrightarrow 3p^2-2p^3$



量子信息：将单量子比特编码

$$\alpha|0\rangle+\beta|1\rangle \longrightarrow \alpha|000\rangle+\beta|111\rangle$$

（原量子比特）　　（通过3个量子比特编码后）

注：量子比特的编码方式不是克隆而是直接制造，比如上述量子态编码可以通过3光子纠缠来实现。

（2）**差错连续性**。经典信息的错误是分立的，而量子位态取值与一个二维的Hilbert空间的任意态失，所以量子信息的错误可以是连续的。比如在一个量子门的操作下一个量子位态应由

$$\alpha|0\rangle+\beta|1\rangle \longrightarrow \alpha|0\rangle+\beta e^{\varphi i}|1\rangle$$

但是由于误差，使得

$$\alpha|0\rangle+\beta e^{\varphi i}|1\rangle \longrightarrow \alpha|0\rangle+\beta e^{i(\varphi+\delta)}|1\rangle$$

虽然δ是一个小量，但依然是错误的量子态，随着时间的推移，这些小量会积累起来变成大错。

（3）**不可测量性**。由于不可观测的量子特性，使得纠错过程出现两个难题：

1是否出错？

2出现什么错误？

Shor码

第五章 量子纠错

1. 量子纠错的基本理论
2. **比特翻转量子码**
3. 纠单比特错误量子码，Shor码
4. 量子错误刻画
5. 纠缠纯化与量子纠错
6. 量子码的构造（经典线性码，CSS码）
7. 稳定子码(Stabilizer Codes)
8. 普适量子计算

比特翻转量子码

方法1

P_0= |000><000| + |111><111|无差错

P_1= |100><100| + |011><011|第一比特翻转

P_2= |010><010| + |101><101|第二比特翻转

P_3= |001><001| + |110><110|第三比特翻转

例如第一比特翻转时，比特状态为：

$$\alpha |100\rangle + \beta |011\rangle$$

这时测量状态φ时，$\langle\varphi|P_1|\varphi\rangle=1$

测量并不会引起状态的改变，测量前后比特状态都为$\alpha |100\rangle + \beta |011\rangle$，通过测量只得到了φ的差错信息，并不会得知α，β的值

方法2

由$Z_1 Z_2$与$Z_2 Z_3$ 代替 P_0 P_1 P_2 P_3

Z_1Z_2测量目的是比较第1量子比特与第2量子比特

$$Z_1 Z_2 = (|00\rangle\langle 00| + |11\rangle\langle 11|) \otimes I - (|01\rangle\langle 01| + |10\rangle\langle 10|) \otimes I,$$

若1与2相同，则给出+1，若不同给出-1

Z_2Z_3测量目的是比较第2量子比特与第3量子比特

若2与3相同，则给出+1，若不同给出-1

由此，可以判断出错误类型，却不测量有关编码后量子状态的幅值α，β

第五章 量子纠错

1. 量子纠错的基本理论
2. 比特翻转量子码
3. **纠单比特错误量子码，Shor码**
4. 量子错误刻画
5. 纠缠纯化与量子纠错
6. 量子码的构造（经典线性码，CSS码）
7. 稳定子码(Stabilizer Codes)
8. 普适量子计算

纠单比特错误量子码

$$|0\rangle_L = |000\rangle$$
$$|1\rangle_L = |111\rangle$$

code states

$$|\psi\rangle = \alpha|000\rangle + \beta|111\rangle$$

$\alpha|000\rangle + \beta|111\rangle$ **Even Even**

No error $I \otimes I \otimes I$

Bit flip on first qubit $X \otimes I \otimes I$

$\alpha|100\rangle + \beta|011\rangle$

Odd Even

Parity of pairs 12 and 23

$Z \otimes Z \otimes I$ and $I \otimes Z \otimes Z$

Error syndrome

Bit flip on second qubit $I \otimes X \otimes I$

Bit flip on third qubit $I \otimes I \otimes X$

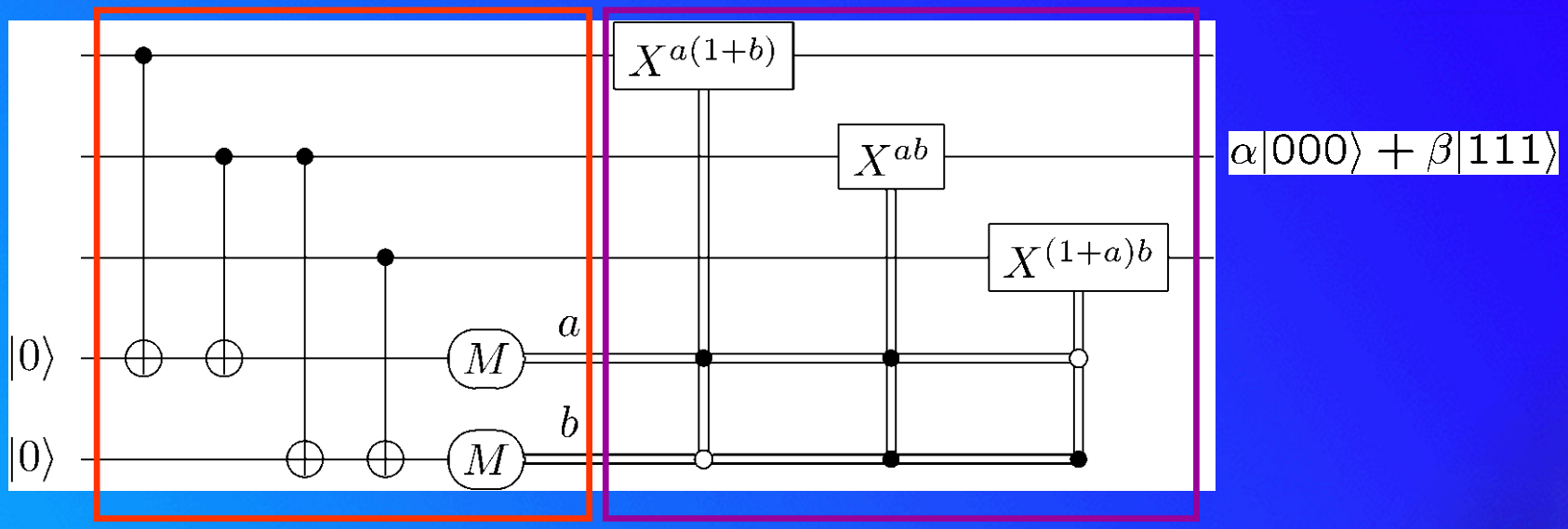
$\alpha|010\rangle + \beta|101\rangle$

Odd Odd

$\alpha|001\rangle + \beta|110\rangle$ **Even Odd**

Quantum error correction

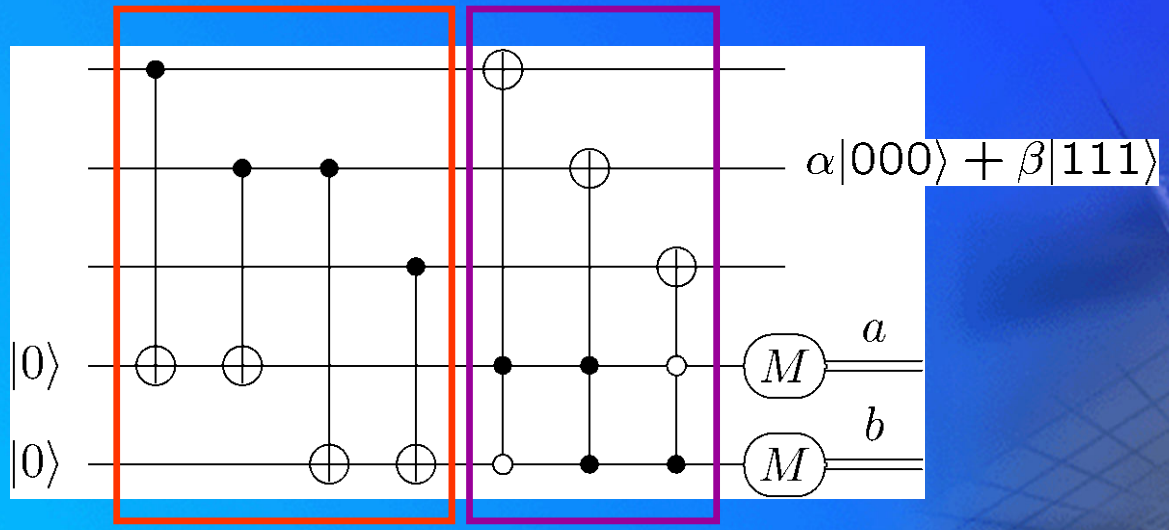
Single bit flip correction circuit



Syndrome measurement

Error correction

Coherent version



From Caves

相位翻转

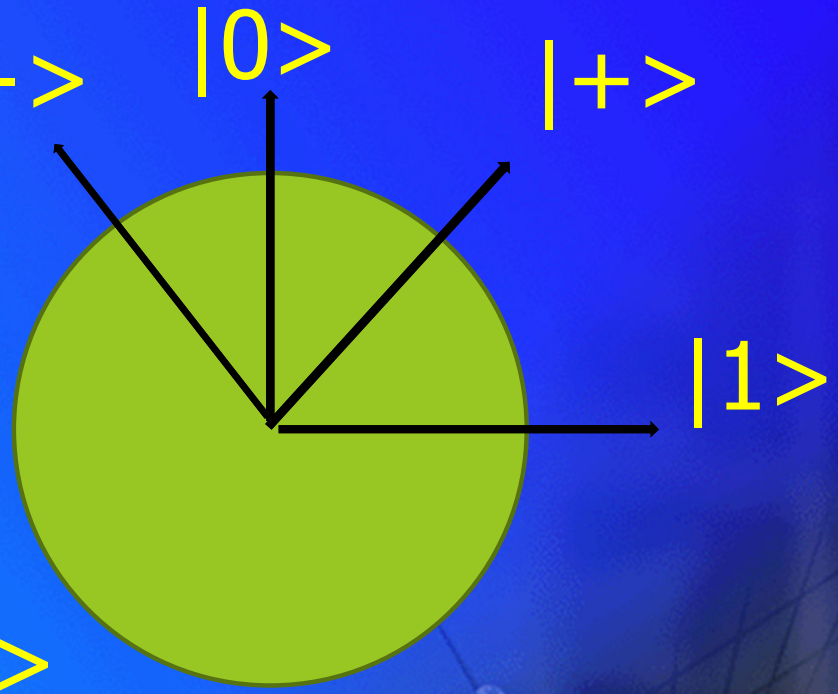
由$\alpha|0\rangle+\beta|1\rangle \longrightarrow \alpha|0\rangle-\beta|1\rangle$（相位翻转）

处理方式：将相位翻转转化为比特翻转

设

$$|+\rangle \equiv (|0\rangle + |1\rangle)/\sqrt{2},$$

$$|-\rangle \equiv (|0\rangle - |1\rangle)/\sqrt{2}.$$



得出

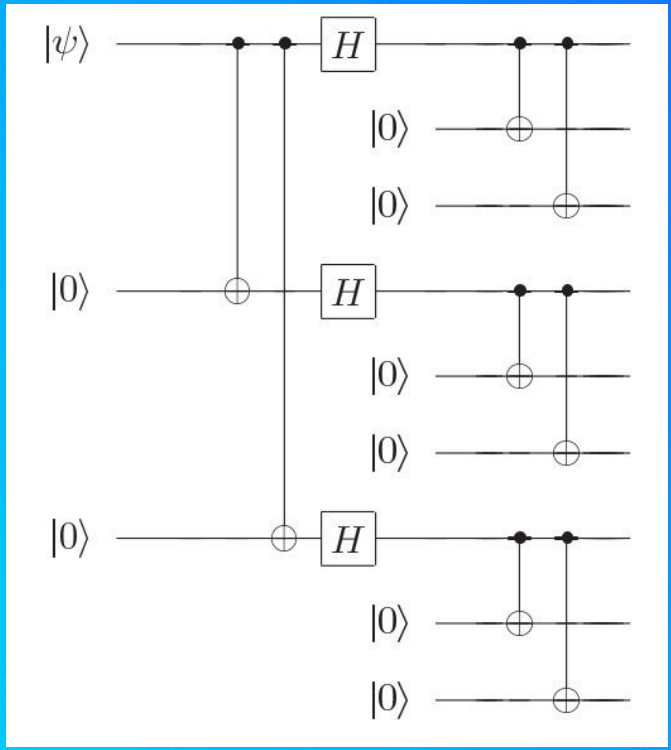
$|0_L\rangle=|000\rangle$ $|0_L\rangle=|+++\rangle$

$|1_L\rangle=|111\rangle$ $|1_L\rangle=|---\rangle$

Shor量子码：
三量子比特 相位翻转码与比特翻转码的组合

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

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



Shor码编码线路

Hadamard门可以实现|0>，|1>基与|+>，|−>之间的转换

(四) Shor码推广--可对完全任意的差错进行保护

设噪声为$\{E_i\}$,编码后的量子比特态为

$$|\psi\rangle = \alpha|0_L\rangle + \beta|1_L\rangle$$

噪声$\{E_i\}$作用后:

$$\mathcal{E}(|\psi\rangle\langle\psi|) = \sum_i E_i|\psi\rangle\langle\psi|E_i^\dagger$$

假设把纠错集中到一个单项式 $E_i|\psi\rangle\langle\psi|E_i^\dagger$

量子状态$E_i|\psi\rangle$可以写成

$|\psi\rangle$，$X_1|\psi\rangle$，$Z_1|\psi\rangle$，$X_1Z_1|\psi\rangle$的叠加

测量差错症状会将这个叠加结果

塌缩到上述4个状态之一

恢复过程由相应的逆运算而执行，

并成功恢复状态$|\psi\rangle$，

这种方法对于所有运算元E_i都是正确的

第五章 量子纠错

1. 量子纠错的基本理论
2. 比特翻转量子码
3. 纠单比特错误量子码，Shor码
4. **量子错误刻画**
5. 纠缠纯化与量子纠错
6. 量子码的构造（经典线性码，CSS码）
7. 稳定子码(Stabilizer Codes)
8. 普适量子计算

量子错误描述

A general quantum error is a superoperator that is of form:

$$\rho \rightarrow \Sigma\, A_k\, \rho\, A_k^{\dagger}$$

Examples of single-qubit errors:

Bit Flip X: $X|0\rangle = |1\rangle,\ X|1\rangle = |0\rangle$

Phase Flip Z: $Z|0\rangle = |0\rangle,\ Z|1\rangle = -|1\rangle$

Complete dephasing: $\rho \rightarrow (\rho + Z\rho Z^{\dagger})/2$ (decoherence)

Depolarizing channel : $\rho \rightarrow ((1-p)\rho + p/3(X\rho X + Y\rho Y + Z\rho Z)$

Rotation: $R_\theta|0\rangle = |0\rangle,\ R_\theta|1\rangle = e^{i\theta}|1\rangle$

Correcting Continuous Rotation

Let us rewrite continuous rotation

$R_\theta |0\rangle = |0\rangle$, $R_\theta |1\rangle = e^{i\theta} |1\rangle$

$$R_\theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} = e^{i\theta/2} \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix}$$

$$= \cos(\theta/2)\, I - i \sin(\theta/2)\, Z$$

$$R_\theta^{(k)} |\psi\rangle = \cos(\theta/2) |\psi\rangle - i \sin(\theta/2)\, Z^{(k)} |\psi\rangle$$

($R_\theta^{(k)}$ is R_θ acting on the *k*th qubit.)

From Gottesman

Correcting Continuous Rotations

How does error correction affect a state with a continuous rotation on it?

$$R_\theta^{(k)} |\psi\rangle = \cos(\theta/2) |\psi\rangle - i \sin(\theta/2) Z^{(k)} |\psi\rangle$$

$$\longrightarrow \quad \cos(\theta/2) |\psi\rangle |I\rangle - i \sin(\theta/2) Z^{(k)} |\psi\rangle \; |Z^{(k)}\rangle$$

Error syndrome

Measuring the error syndrome collapses the state:

Prob. $\cos^2(\theta/2)$: $|\psi\rangle$ (no correction needed)

Prob. $\sin^2(\theta/2)$: $Z^{(k)} |\psi\rangle$ (corrected with $Z^{(k)}$)

From Gottesman

Correcting All Single-Qubit Errors

Theorem: If a quantum error-correcting code (QECC) corrects errors A and B, it also corrects $\alpha A + \beta B$.

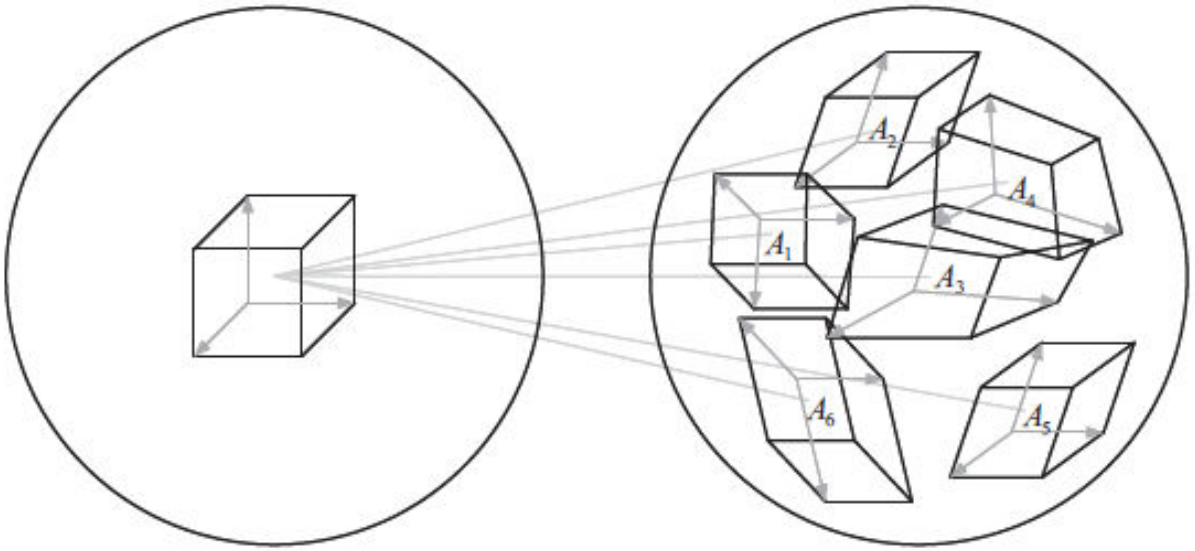
Any 2x2 matrix can be written as $\alpha I + \beta X + \gamma Y + \delta Z$.

A general single-qubit error $\rho \rightarrow \sum A_k \rho A_k^\dagger$ acts like a mixture of $|\psi\rangle \rightarrow A_k |\psi\rangle$, and A_k is a 2x2 matrix.

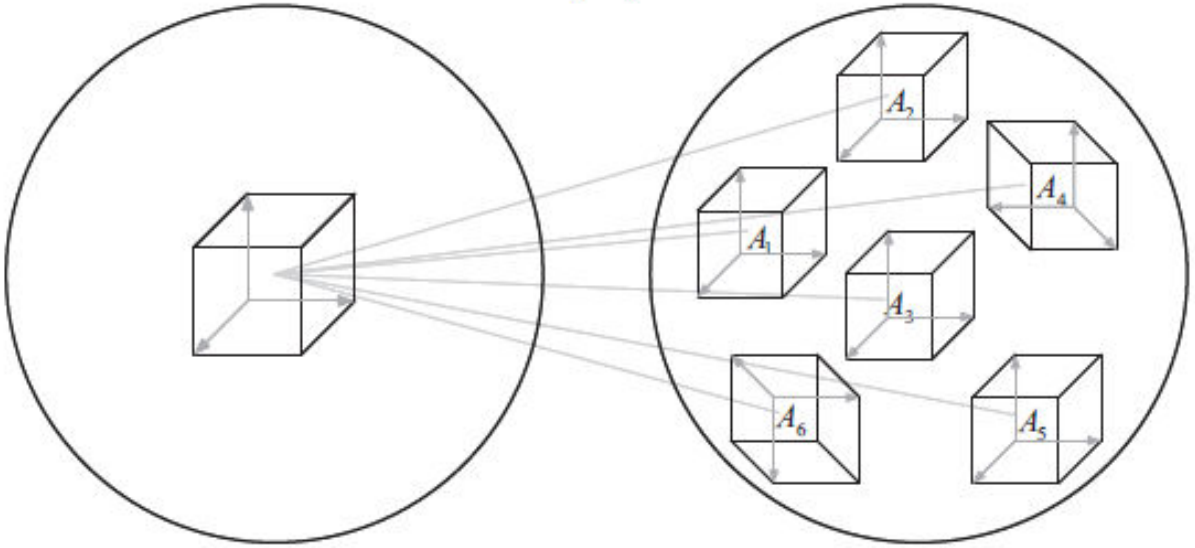
Any QECC that corrects the single-qubit errors X, Y, and Z (plus I) corrects every single-qubit error.

Correcting all t-qubit X, Y, Z on t qubits (plus I) corrects all t-qubit errors.

From Gottesman



(A)



(B)

Figure 10.5. The packing of Hilbert spaces in quantum coding: (A) bad code, with non-orthogonal, deformed resultant spaces, and (B) good code, with orthogonal (distinguishable), undeformed spaces.

量子纠错一般性

假定：噪声是由量子运算$\mathcal{E}$所描述，整个纠错方法（纠错运算）由保迹量子运算$\mathcal{R}$承担

量子纠错条件：令C为一个量子码，P为到C的投影算子设$\mathcal{E}$为具有运算元$\{E_i\}$的量子运算，则纠正C上的$\mathcal{E}$纠错运算$\mathcal{R}$存在的充分必要条件为，对某个复数Hermitian矩阵α成立

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

称为$\{E_i\}$组成一个可纠错的差错集合

假设$\{F_j\}$为噪声E_i的线性组合，即对某个复数矩阵m_{ji}有 $F_j = \sum_i m_{ji} E_i$ 那么纠错运算$\mathcal{R}$也可以对噪声F进行纠错。

如果用 $\{|\overline{k}\rangle\}$ 表示码空间的一组标准正交基，则纠错条件可以表示为:

$$\langle \overline{k} | E_i^\dagger E_j | \overline{l} \rangle = \alpha_{ij} \delta_{kl}$$

$\alpha_{ij} = \langle \overline{k} | E_i^\dagger E_j | \overline{k} \rangle$ 是一个与k无关的厄米矩阵

每个运算元$\{E_i\}$都可以被写成Pauli矩阵的线性组合。所以只需要满足

$$P\sigma_i^1\sigma_j^1P = \alpha_{ij}P,$$

便可以确定Shor码可以对单量子比特进行纠错

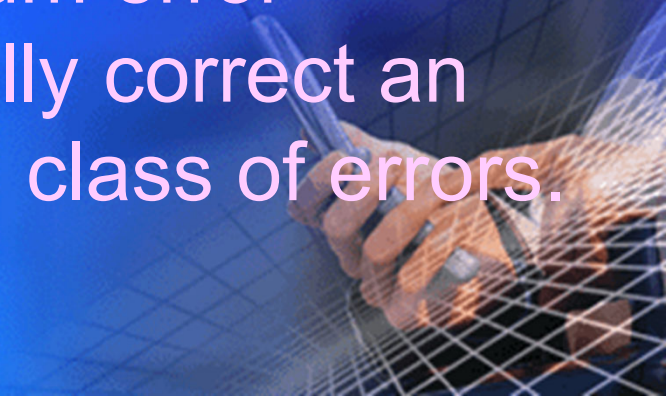
量子纠错的实质：如何构造码空间C以及相应的纠错运算R

Discretization of the errors

Any QECC that corrects the single-qubit errors X, Y, and Z (plus I) corrects every single-qubit error.

Correcting all t-qubit X, Y, Z on t qubits (plus I) corrects all t-qubit errors.

This is a fundamental and deep fact about quantum error-correction, that by correcting just a discrete set of errors – the bit flip, phase flip, and combined bit–phase flip, in this example – a quantum error-correcting code is able to automatically correct an apparently much larger (continuous!) class of errors.



简并编码与Hamming界

简并编码优势
- 优势：能够储存更多的信息
- 劣势：某些经典纠错技术失效

Hamming界适用于非简并编码，但它映射出一般界的可能性。举例来说：

有k个数目的量子比特，用非简并编码将k量子比特编码为n量子比特，如果出现j个差错（j≤t,t为差错数上限）总共有 $\binom{n}{j}$ 种差错可能出现的位置，每种差错又实际是三个Pauli矩阵线性作用的结果，所以总共有3^j个可能的差错，所以在t个量子比特上出现的差错最多为 $\sum_{j=0}^{t}\binom{n}{j}3^j$ 个。

如果以非简并的方式对k个量子比特进行编码，
条件:(1)每个差错要对应一个正交的2^k维子空间
(2)所有纠错子空间置于n个量子比特可利用的整个2^n 空间中。

建立不等式:

$$\sum_{j=0}^{t}\binom{n}{j}3^j 2^k \le 2^n$$

这就是量子Hamming界

如果用n个量子比特对一个量子比特进行编码，则量子Hamming界为

$$2(1+3n) \le 2^n.$$

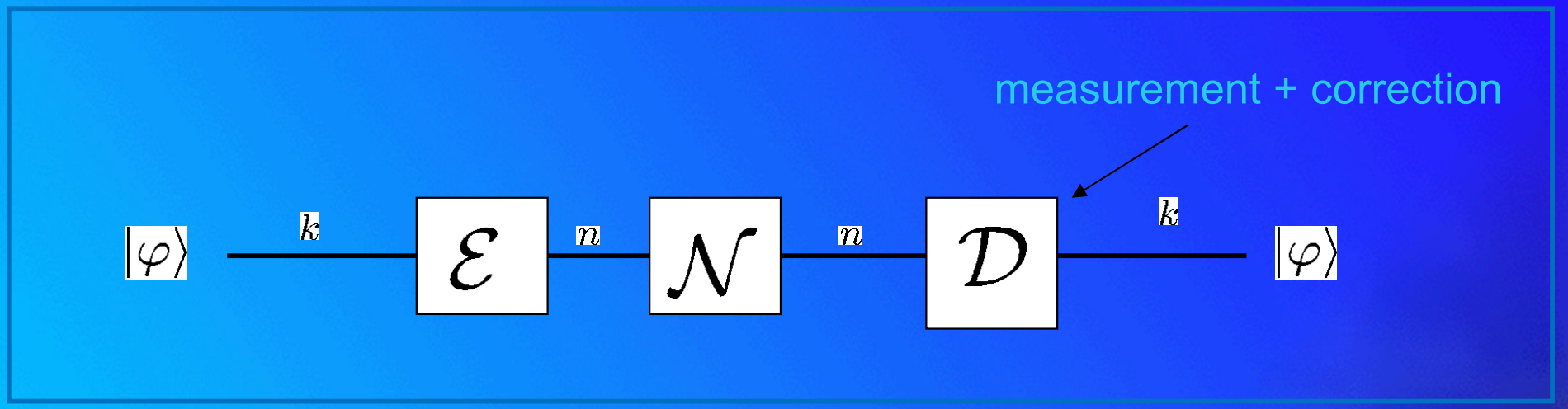
当n≥5时等式成立，所以不存在用少于5个量子比特对一个量子比特编码的非简并码

第五章 量子纠错

1. 量子纠错的基本理论
2. 比特翻转量子码
3. 纠单比特错误量子码，Shor码
4. 量子错误刻画
5. **纠缠纯化与量子纠错**
6. 量子码的构造（经典线性码，CSS码）
7. 稳定子码(Stabilizer Codes)
8. 普适量子计算

量子纠错过程

[[n,k]] quantum error correcting code



纠缠纯化与量子纠错

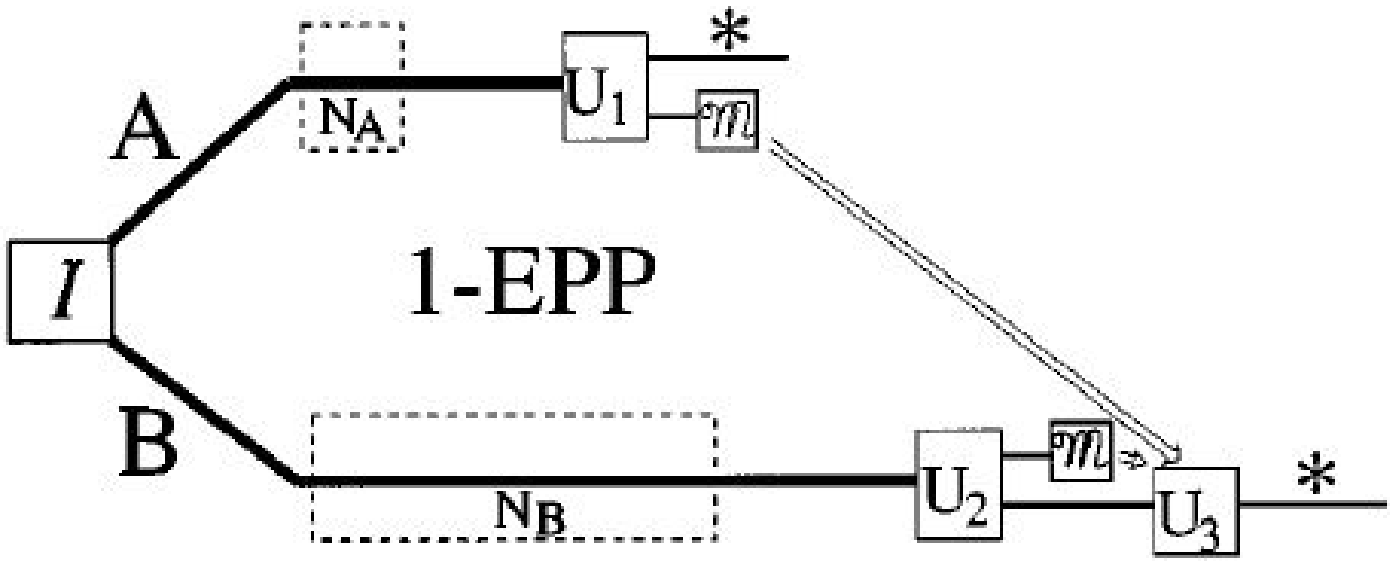


FIG. 3. One-way entanglement purification protocol (1-EPP). In 1-EPP there is only one stage; after unitary transformation U_1 and measurement $\mathcal{M}$, Alice sends her classical result to Bob, who uses it in combination with his measurement result to control a final transformation U_3. The unidirectionality of communication allows the final, maximally entangled state (*) to be separated both in space and in time.

纠缠纯化与量子纠错

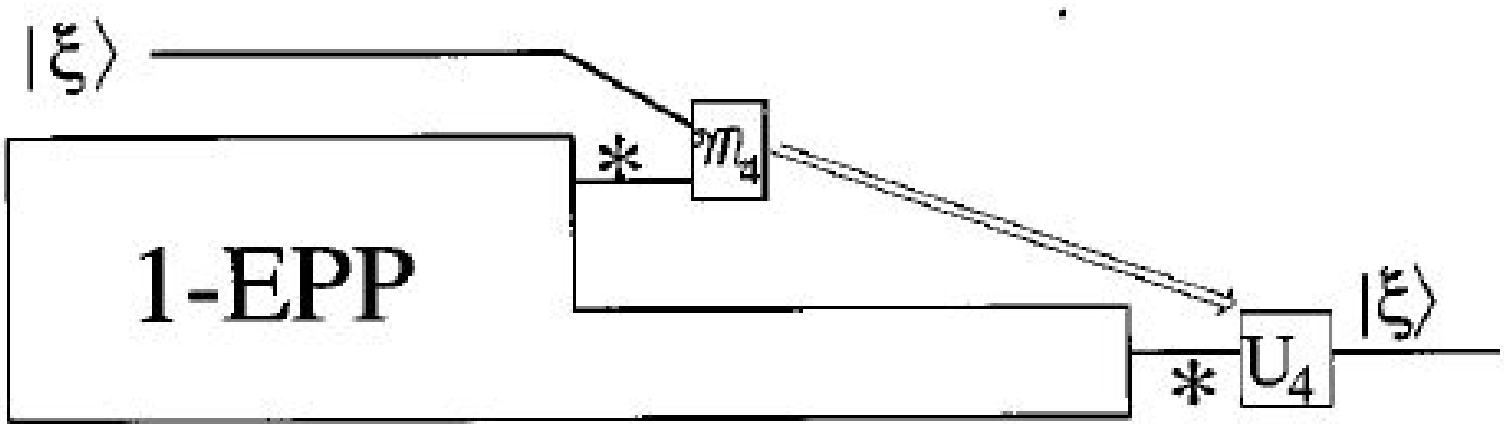


FIG. 4. If the 1-EPP of Fig. 3 is used as a module for creating time-separated EPR pairs (*), then by using quantum teleportation [5], an arbitrary quantum state $|\xi\rangle$ may be recovered exactly after U_4, despite the presence of intervening noise. This is the desired effect of a quantum error-correcting code (QECC).

纠缠纯化与量子纠错

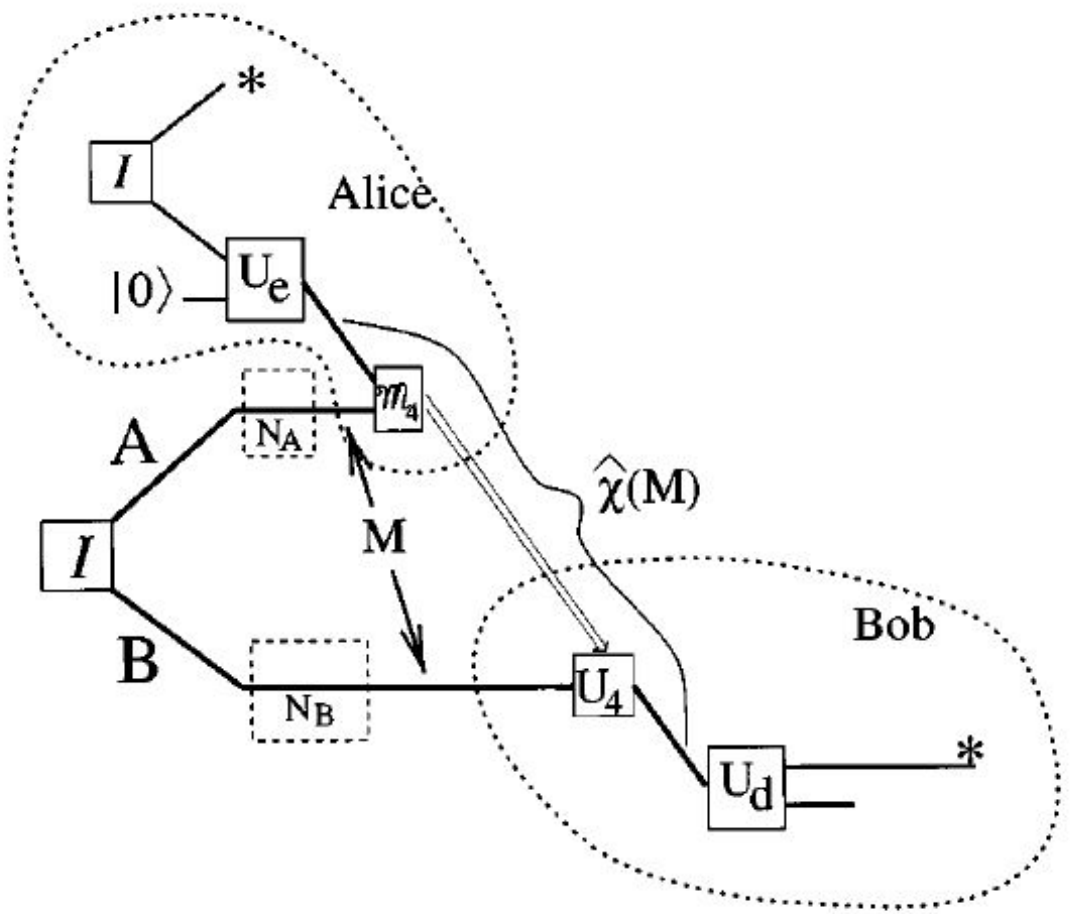


FIG. 14. A QECC can be transformed into a 1-EPP. Teleporting (M_4, U_4) via a mixed state M defines the noisy channel $\hat{\chi}(M)$. If a quantum error-correcting code $\{U_e, U_d\}$ can correct the errors in this channel, the code and channel can be used to share pure entanglement between Alice and Bob (*). This establishes inequality (52), viz., $\forall_M D_1(M) \geqslant Q(\hat{\chi}(M))$.

纠缠纯化与量子纠错

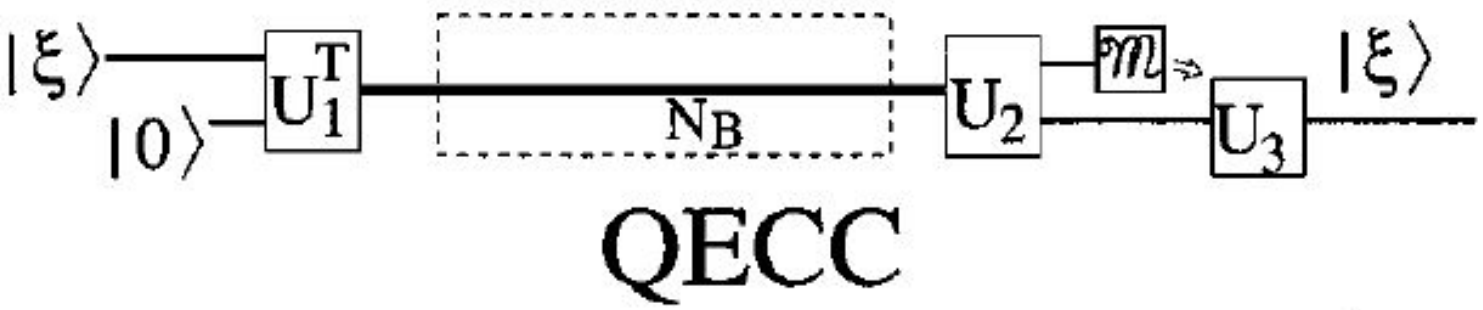


FIG. 16. The one-way purification protocol of Fig. 4 may be transformed into the quantum-error-correcting-code protocol shown here. In a QECC, an arbitrary quantum state $|\xi\rangle$, along with some qubits which are originally set to $|0\rangle$, are encoded in such a way by U_1^T that, after being subjected to errors N_B, decoding U_2 followed by measurement $\mathcal{M}$, followed by final rotation U_3, permits an exact reconstruction of the original state $|\xi\rangle$.

第五章 量子纠错

1. 量子纠错的基本理论
2. 比特翻转量子码
3. 纠单比特错误量子码，Shor码
4. 量子错误刻画
5. 纠缠纯化与量子纠错
6. **量子码的构造（经典线性码，CSS码）**
7. 稳定子码(Stabilizer Codes)
8. 普适量子计算

量子码的构造

经典线性码

n by *k generator matrix G* whose entries are all elements of Z_2, that is, zeroes and ones.

The matrix *G* maps messages to their encoded equivalent. Thus the *k* bit message *x* is encoded as *Gx*

例如[6, 2] code

$$G = \begin{bmatrix} 1 & 0 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \\ 0 & 1 \end{bmatrix}$$

$$G(0,0) = (0,0,0,0,0,0); \quad G(0,1) = (0,0,0,1,1,1);$$
$$G(1,0) = (1,1,1,0,0,0); \quad G(1,1) = (1,1,1,1,1,1),$$

经典线性码

- A code that encodes k bits in n bits ($n>k$) is called an *[n,k] code*.
- A general code encoding k bits in n bits requires 2^k codewords of length n to specify the encoding.
- A *linear* code C encodes k bits of information into an n bit code space specified by an n by k generator matrix $\boldsymbol{G}$ with elements in Z_2.
- A linear code only requires kn bits to specify the encode.

线性编码

- We encode a k bits codeword x, into a n bits codeword c using a [*n* by k] generator matrix ***G*** as follows:

$$c \equiv G \bullet x$$

- Error correction for linear codes is done using a [(*n-k*) by *n*] *parity matrix*.

Parity Check 过程

- Parity check matrix ***H*** is such that:

$$\boldsymbol{H c = 0} \quad \text{and} \quad \boldsymbol{H G = 0}$$

- The receiver gets the codeword ***r***, which incorporates an error ***e***:

$$\boldsymbol{r = c + e}$$

- Then, the syndrome ***s*** is given by:

$$\boldsymbol{s = H r = H e}$$

Error Correction & Recovery

- Once we detect the syndrome ***s***, we can find the error that occurred ***e***.
- Now we can correct the error as:

$$c = r - e$$

- And finally one can recover the original message

量子码的构造

经典线性码

优势为节省资源：用n个比特编码k个比特

线性码：kn 个比特 刻画生成矩阵

一般码：$n2^k$ 个比特 刻画生成矩阵

奇偶检验矩阵：Hx=0 (H)为奇偶检验矩阵

H矩阵为(n-k)×n

H与G之间可进行相互转换，例如

$$H \equiv \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

n-k

n

奇偶检验矩阵使差错检测和恢复变得十分明显

H与G之间可进行相互转换

奇偶检验矩阵具体的运作方式

设　编码消息x ⟶ y=Gx

对y造成影响的噪声 ⟶ e

出错后的码字 ⟶ y′=y+e　(+为模二加)

Hy=0 ⟶ Hy′=He

Hy′为差错症状。
- 当没有差错出现的情况下为0
- 当差错出现在第j个比特时为He_j

假设最多只会出现一个比特的错误，则通过比较Hy′与 He_j 的值，确定哪个比特需要被纠正。

Hamming距离

距离标示可执行线性纠错码

设 x和y为n比特的字，

则d(x,y)为差异位置数目 ➡ Hamming距离

举例：d((1,1,0,0),(0,1,0,1))=2

Wt(x)=d(x,0)为X中非零位置数目➡Hamming权重

$$d(x,y)=Wt(x+y)$$

距离的重要性在于，对某个整数t，简单的通过解码变坏的编码消息y′为满足d(y,y′)≤t的唯一码字y，具有距离至少为2t+1的一个码就能纠正最多t个比特上的差错。

Hamming码，可以纠正任意单比特错误

设r≥2为一个整数，H为一个矩阵

H矩阵列的长度为2^r-1 （不全为0）

Hamming码 ⟶ [2^r-1 , 2^r-r-1]

当r=3时， Hamming码 ⟶ [7,4]码

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

这个码的距离为3，可以纠正任意单比特上的差错。

Gilbert–Varshamov界

Gilbert–Varshamov界

对于大n，必存在对某个k防止t比特上差错的[n,k]纠错码

$$\frac{k}{n} \geq 1 - H\left(\frac{2t}{n}\right)$$

其中 $H(x) \equiv -x\log(x) - (1-x)\log(1-x)$ 为二元Shannon熵

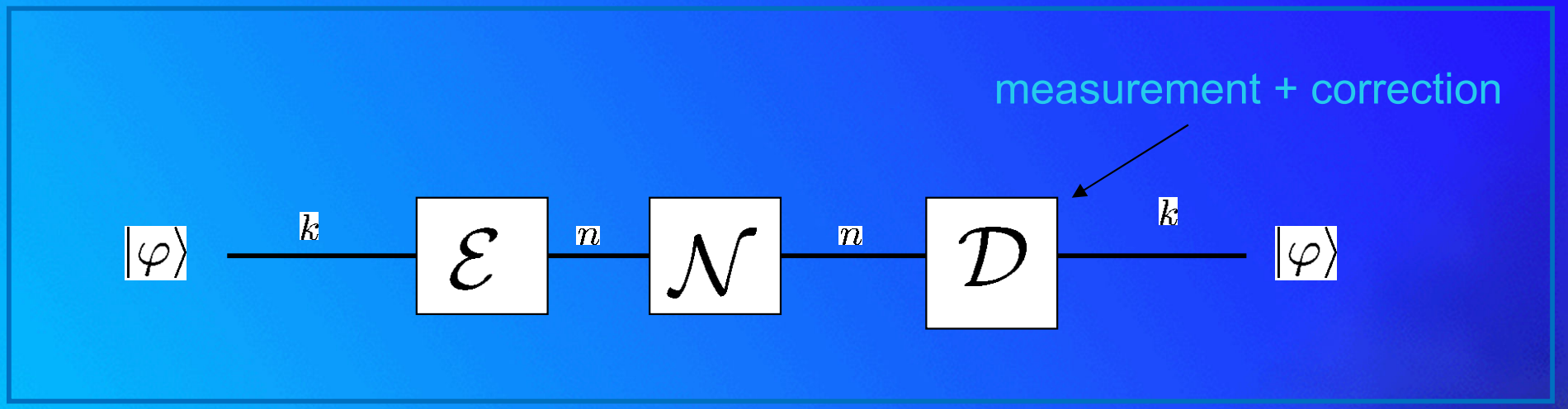
Gilbert–Varshamov界的重要性在于，k较小n较大时，有好码存在

量子纠错码特征

- Quantum Error Correction Codes are characterized by the triplet [n,k,d], where:
  - n is the length of the resulting codeword.
  - k is the number of qubits to be encoded.
  - d is the *minimum distance*.
- Data redundancy implies $n>k$
- A code with minimal distance $d=2t+1$ is able to correct errors on up to t bits.

量子纠错过程

[[n,k]] quantum error correcting code



Basic framework for quantum error correction

After encoding the code is subjected to noise, following which a syndrome measurement is performed to diagnose the type of error which occurred, that is, the error syndrome. Once this has been determined, a recovery operation is performed, to return the quantum system to the original state of the code. The basic picture is illustrated in Figure 10.5: different error syndromes correspond to undeformed and orthogonal subspaces of the total Hilbert space. The subspaces must be orthogonal, otherwise they couldn't be reliably distinguished by the syndrome measurement. Furthermore, the different subspaces must be undeformed versions of the original code space, in the sense that the errors mapping to the different subspaces must take the (orthogonal) codewords to orthogonal states, in order to be able to recover from the error.

检测错误，而不是量子信息

Through the information from the error syndromes, one can determine whether there is an error and where it is:

E.g., measurements of Z_1Z_2 and Z_2Z_3 for $\alpha|010\rangle + \beta|101\rangle$ give syndrome 11, which means the second bit is different. Correct it with a X operation on the second qubit. Note that the syndrome does not depend on α and β.

We have learned about the error without learning about the data, so quantum superpositions are still alive!

Calderbank–Shor–Steane codes

Suppose C_1 and C_2 are $[n, k_1]$ and $[n, k_2]$ classical linear codes such that $C2 \subset C1$ and C_1 and $C_2^{\perp}$ both correct t errors. We will define an $[n, k_1 - k_2]$ quantum code $CSS(C_1, C_2)$ capable of correcting errors on t qubits, the CSS code of C_1 over C_2.

Suppose $x \in C_1$ is any codeword in the code C_1. Then we define the quantum state $|x + C_2\rangle$ by

$$|x + C_2\rangle \equiv \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x + y\rangle$$

The quantum code $\mathrm{CSS}(C_1, C_2)$ is defined to be the vector space spanned by the states $|x + C_2\rangle$ for all $x \in C_1$. The number of cosets of C_2 in C_1 is $|C_1|/|C_2|$ so the dimension of $\mathrm{CSS}(C_1, C_2)$ is $|C_1|/|C_2| = 2^{k_1 - k_2}$, and therefore $\mathrm{CSS}(C_1, C_2)$ is an $[n, k_1 - k_2]$ quantum code.

Calderbank–Shor–Steane codes

Bit flip errors detection and correction

Suppose the bit flip errors are described by an n bit vector e_1 with 1s where bit flips occurred, and 0s elsewhere, and the phase flip errors are described by an n bit vector e_2 with 1s where phase flips occurred, and 0s elsewhere. If $|x+C_2\rangle$ was the original state then the corrupted state is:

$$\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{(x+y)\cdot e_2} |x + y + e_1\rangle$$

Introducing an ancilla and taking

$$|x + y + e_1\rangle |H_1(x + y + e_1)\rangle = |x + y + e\rangle |H_1 e_1\rangle$$

one has

$$\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{(x+y)\cdot e_2} |x + y + e_1\rangle |H_1 e_1\rangle$$

Calderbank–Shor–Steane codes

Bit flip errors detection and correction

Error-detection for the bit flip errors is completed by measuring the ancilla to obtain the result $H_1 e_1$ and discarding the ancilla, giving the state

$$\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{(x+y)\cdot e_2} |x + y + e_1\rangle$$

Knowing the error syndrome $H_1 e_1$ we can infer the error e1 since C_1 can correct up to t errors, which completes the error-detection. Recovery is performed simply by applying gates to the qubits at whichever positions in the error e_1 a bit flip occurred, removing all the bit flip errors and giving the state

$$\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{(x+y)\cdot e_2} |x + y\rangle$$

Calderbank–Shor–Steane codes

Phase flip errors detection and correction

To detect phase flip errors we apply Hadamard gates to each qubit, taking the state to

$$\frac{1}{\sqrt{|C_2|2^n}} \sum_z \sum_{y \in C_2} (-1)^{(x+y)\cdot(e_2+z)} |z\rangle$$

where the sum is over all possible values for *n* bit *z*. Setting $z' \equiv z + e_2$, this state may be rewritten:

$$\frac{1}{\sqrt{|C_2|2^n}} \sum_{z'} \sum_{y \in C_2} (-1)^{(x+y)\cdot z'} |z' + e_2\rangle$$

Supposing $z' \in C_2^{\perp}$ it is easy to see that $\sum_{y \in C_2} (-1)^{y \cdot z'} = |C_2|$, while if $z' \notin C_2^{\perp}$ then $\sum_{y \in C_2} (-1)^{y \cdot z'} = 0$. Thus the state may be rewritten:

$$\frac{1}{\sqrt{2^n/|C_2|}} \sum_{z' \in C_2^{\perp}} (-1)^{x \cdot z'} |z' + e_2\rangle ,$$

Calderbank–Shor–Steane codes

Phase flip errors detection and correction

The last formula looks just like a bit flip error described by the vector e_2! As for the error-detection for bit flips we introduce an ancilla and reversibly apply the parity check matrix H_2 for $C_2^{\perp}$ to obtain $H_2 e_2$, and correct the 'bit flip error' e_2, obtaining the state

$$\frac{1}{\sqrt{2^n/|C_2|}} \sum_{z' \in C_2^{\perp}} (-1)^{x \cdot z'} |z'\rangle$$

The error-correction is completed by again applying Hadamard gates to each qubit. Since the Hadamard gate is self-inverse this takes us back to the state

$$\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x + y\rangle$$

Quantum Gilbert–Varshamov bound

In the limit as n becomes large, an [n, k] quantum code protecting against errors on up to t qubits exists for some k such that

$$\frac{k}{n} \geq 1 - 2H\left(\frac{2t}{n}\right)$$

Thus, good quantum error-correcting codes exist, provided one doesn't try to pack too many qubits k into an n qubit code.

第五章 量子纠错

1. 量子纠错的基本理论
2. 比特翻转量子码
3. 纠单比特错误量子码，Shor码
4. 量子错误刻画
5. 纠缠纯化与量子纠错
6. 量子码的构造（经典线性码，CSS码）
7. **稳定子码(Stabilizer Codes)**
8. 普适量子计算

The Pauli Group

The general Pauli group G_n on n qubits is defined to consist of all n-fold tensor products of up to n operators I, X, Y, or Z with overall phase $\pm 1, \pm i$

For a single quantum bit

$$G_1 \equiv \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}$$

that G_1 is closed under multiplication, and thus forms a legitimate group.

Any pair M, N of Pauli operators either commutes (MN = NM) or anticommutes (MN = -NM).

The Pauli Group G_n on n qubits is given by the n-fold tensor product of Pauli matrices.

The Pauli group spans the set of all n-qubit errors.

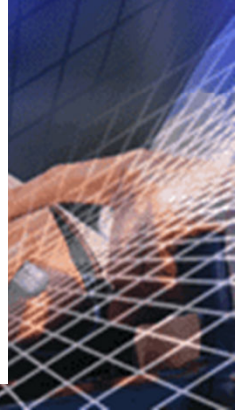
Quantum Error Correction Sonnet

We cannot clone, perforce; instead, we split
Coherence to protect it from that wrong
That would destroy our valued quantum bit
And make our computation take too long.

Correct a flip and phase – that will suffice.
If in our code another error's bred,
We simply measure it, then God plays dice,
Collapsing it to X or Y or zed.

We start with noisy seven, nine, or five
And end with perfect one. To better spot
Those flaws we must avoid, we first must strive
To find which ones commute and which do not.

With group and eigenstate, we've learned to fix
Your quantum errors with our quantum tricks.
– 'Quantum Error Correction Sonnet', by Daniel Gottesman



Stabilizer

Suppose S is a subgroup of G_n and define V_S to be the set of n qubit states which are fixed by every element of S.

V_S is the *vector space stabilized by* S, and S is said to be the *stabilizer* of the space V_S, since every element of V_S is stable under the action of elements in S.

Properties of a Stabilizer

The stabilizer is a group:

If $M|\psi\rangle = |\psi\rangle$ and $N|\psi\rangle = |\psi\rangle$, then $MN|\psi\rangle = |\psi\rangle$.

The stabilizer is Abelian:

If $M|\psi\rangle = |\psi\rangle$ and $N|\psi\rangle = |\psi\rangle$, then

$$(MN-NM)|\psi\rangle = MN|\psi\rangle - NM|\psi\rangle = 0$$

(For Pauli matrices) ⟹ $MN = -NM$

Stabilizer 例子

The EPR state of two qubits

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

It is easy to verify that this state satisfies the identities

$$X_1 X_2 |\psi\rangle = |\psi\rangle$$
$$Z_1 Z_2 |\psi\rangle = |\psi\rangle$$

We say that the state |ψ> is *stabilized* by the operators X_1X_2 and Z_1Z_2.
In addition, the state |ψ> is the unique quantum state (up to a global phase) which is stabilized by these operators X_1X_2 and Z_1Z_2.

Stabilizer 例子

- Such a state is *unique*, as it is the only one (up to a global phase) to be stabilized by both X_1X_2 and Z_1Z_2.
- The basic idea of using the stabilizer group is to work with the stabilizer operators as group generators rather than with the states.
- The *group theoretical formalism* of the stabilizer codes offers a more compact description of the quantum error correction codes.

Stabilizer 例子

For the classical repetition code, one can see the error syndromes

first two bits have even parity (an even number of 1's), and similarly for the 2nd and 3rd bits, with correctly-encoded state 000 or 111

For state with error on one of the first two bits: odd parity for the first two bits.

One can rephrase this by observing that a codeword is a +1 eigenvector of $Z \otimes Z \otimes I$ and that a state with an error on the 1st or 2nd bit is a -1 eigenvector of $Z \otimes Z \otimes I$.

典型的错误探测

For the three-qubit phase error correcting code, a codeword has eigenvalue +1 for X⊗X⊗I, whereas a state with a phase error on one of the first two qubits has eigenvalue -1 for X⊗X⊗I.

Measuring Z⊗Z detects bit flip (X) errors, and measuring X⊗X detects phase (Z) errors.

Measuring enough operators find locations of errors.

Error Correction Conditions

Theorem: Let *S* be the stabilizer of the stabilizer code *C(S)*. Suppose $\{E_i\}$ is a set of operators in G_n such that:

$$E_j^\dagger E_k \notin N(S) - S$$

for all j and k. Then, $\{E_i\}$ is a correctable set of errors for the code *C(S)*.

The normalizer of *S*, denoted *N*(*S*), which is defined to consist of all elements *E* of G_n such that $EgE^\dagger \in S$ for all $g \in S$.

Error Detection

- Suppose $g_1,\ldots,g_{n-k}$ is the set of generators for the stabilizer of an [n,k] stabilizer code, and that $\{E_j\}$ is the set of correctable errors for the code.
- Error detection is performed by measuring the generators of the stabilizer in turn, to obtain the error syndrome, which consists of the results of the measurements $\beta_1,\ldots,\beta_{n-k}$.
- If the error E occurred then the error syndrome is given by β_l such that:

$$E g_l E^\dagger = \beta_l g_l$$

Recovery (1)

- In the case where E is the unique error operator having this syndrome, recovery is done by applying $E^{\dagger}$.
- In the case where there there are two distinct errors E and E' giving rise to the same error syndrome, it follows that:

  $EPE^{\dagger} = E'PE'^{\dagger}$ and then $E^{\dagger}E'PE'^{\dagger}E = P$

  and therefore $E^{\dagger}E'$ is part of S.

Recovery (2)

- Thus applying $E^{\dagger}$ after the error E' has occurred results in a successful recovery.
- Thus, for each possible error syndrome we simply pick out a single error E with that syndrome, and apply $E^{\dagger}$ to achieve recovery when that syndrome is observed.

How to construct a quantum error correction code?

An [n,k,d] quantum error correction code *C(S)* is the vector space V_S stabilized by a subgroup *S* of G_n such that $-I \notin S$ and *S* has *n-k* independent and commuting generators:

$$S = \langle g_1, \ldots, g_{n-k} \rangle$$

and logical states stabilized by:

$$\langle g_1, \ldots, g_{n-k}, (-1)^{x_1} \overline{Z}_1, \ldots, (-1)^{x_k} \overline{Z}_k \rangle$$

which can correct a set of correctable error operators $\{E_i\}$ in G_n such that, for all *j* and *k*:

$$E_j^\dagger E_k \notin N(S) - S$$

Design Goals for QECCs

Several requiremens:

- High rate (high value of both k/n and d/n).
- Efficient decoding (for a general QECC, determining the exact error can take exponentially long in n).
- Efficient encoding (all stabilizer codes can be encoded using $O(n^2)$ operations, but O(n) is better).
- Specific error models (we can sometimes be more efficient if don't insist on correcting all t-qubit errors).
- Many symmetries (useful for fault-tolerance and sometimes other constructions).
- Other application-specific properties

From Gottesman

The three qubit bit flip code

Consider the familiar three qubit bit flip code spanned by the states $|000\rangle$ and $|111\rangle$, with stabilizer generated by Z_1Z_2 and Z_2Z_3. By inspection we see that every possible product of two elements from the error set $\{I, X_1, X_2, X_3\}$ – $I, X_1, X_2, X_3, X_1X_2, X_1X_3, X_2X_3$ – anti-commutes with at least one of the generators of the stabilizer (except for I, which is in S), and thus by Theorem 10.8 the set $\{I, X_1, X_2, X_3\}$ forms a correctable set of errors for the three qubit bit flip code with stabilizer $\langle Z_1Z_2, Z_2Z_3\rangle$.

Error-detection and correction

Z_1Z_2	Z_2Z_3	Error type	Action
+1	+1	no error	no action
+1	−1	bit 3 flipped	flip bit 3
−1	+1	bit 1 flipped	flip bit 1
−1	−1	bit 2 flipped	flip bit 2

The three qubit bit flip code

g_1	Z	Z	I
g_2	I	Z	Z
$\overline{X}$	X	X	X
$\overline{Z}$	Z	Z	Z

The nine qubit Shor code

Name	Operator
g_1	$ZZIIIIIII$
g_2	$IZZIIIIII$
g_3	$IIIZZIIII$
g_4	$IIIIZZIII$
g_5	$IIIIIIZZI$
g_6	$IIIIIIIZZ$
g_7	$XXXXXXIII$
g_8	$IIIXXXXXX$
$\bar{Z}$	$XXXXXXXXX$
$\bar{X}$	$ZZZZZZZZZ$

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

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

The nine qubit Shor code

Name	Operator
g_1	$ZZIIIIIII$
g_2	$IZZIIIIII$
g_3	$IIIZZIIII$
g_4	$IIIIZZIII$
g_5	$IIIIIIZZI$
g_6	$IIIIIIIZZ$
g_7	$XXXXXXIII$
g_8	$IIIXXXXXX$
$\bar{Z}$	$XXXXXXXXX$
$\bar{X}$	$ZZZZZZZZZ$

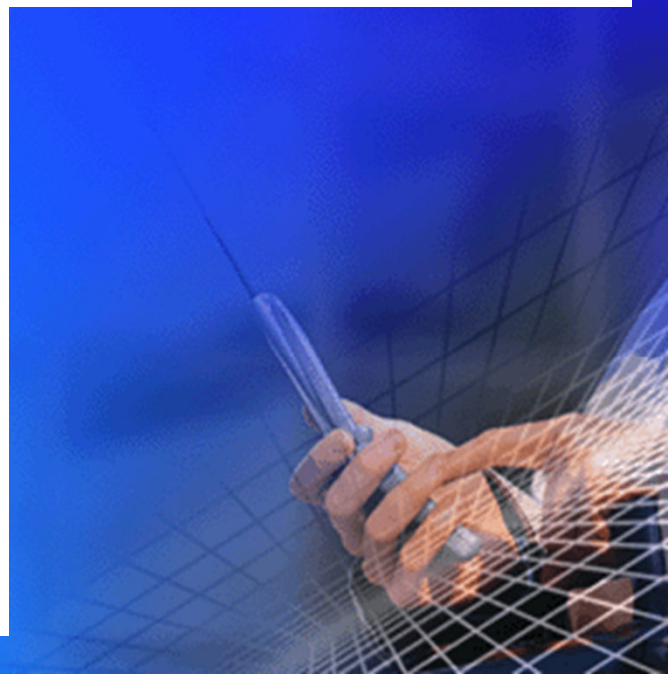
$g_1, g_2, \ldots, g_8$ generate a group, the *stabilizer* of the code, consisting of all Pauli operators M with the property that $M|\psi\rangle = |\psi\rangle$ for all encoded states $|\psi\rangle$.

The five qubit code

Name	Operator
g_1	$XZZXI$
g_2	$IXZZX$
g_3	$XIXZZ$
g_4	$ZXIXZ$
$\bar{Z}$	$ZZZZZ$
$\bar{X}$	$XXXXX$

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

$$|1_L\rangle = \frac{1}{4}\Big[|11111\rangle + |01101\rangle + |10110\rangle + |01011\rangle + |10101\rangle - |00100\rangle - |11001\rangle - |00111\rangle - |00010\rangle - |11100\rangle - |00001\rangle - |10000\rangle - |01110\rangle - |10011\rangle - |01000\rangle + |11010\rangle\Big]$$



CSS Codes

Define a quantum error-correcting code by choosing two classical linear codes C_1 and C_2, and replacing the parity check matrix of C_1 with Z's and the parity check matrix of C_2 with X's.

[[7,1,3]] QECC

Name	Operator
g_1	$IIIXXXX$
g_2	$IXXIIXX$
g_3	$XIXIXIX$
g_4	$IIIZZZZ$
g_5	$IZZIIZZ$
g_6	$ZIZIZIZ$

C_1: [7,4,3] Hamming

C_2: [7,3,4] Hamming

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

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

Calderbank-Shor-Steane Codes

- CSS codes are a subclass of stabilizer codes.
- They construct quantum error correction codes from classical linear codes.
- As a general rule, to detect *X* errors, CSS take a classical parity check matrix *P*, replaces 1 by *Z* and I's elsewhere.
- To detect *Z* errors, replace *X's* instead of *Z's* in the matrix.

CSS codes

- If C_1 and C_2 are orthogonal then we can combine these two codes. This means that the dual code of each code must be a subset of the other code.

- Combining a $C_1[n,k_1,d_1]$ with a $C_2[n,k_2,d_2]$ yields a $CSS(C_1,C_2)[n,|k_1-k_2|,d_3]$ with $d_3 = min\{d_1,d_2\}$.

CSS codes and the seven qubit code

- The 7-qubit Steane code is the most popular CSS code.
- It is created with a classical Hamming code [7,4,3] which is self dual.
- The matrix C_1 is taken as the classical parity check matrix H.
- The matrix C_2 is taken as the transposed of its generator G^T.

CSS codes and the seven qubit code

Define a check matrix with the form

$$\left[\begin{array}{c|c} H(C_2^{\perp}) & 0 \\ 0 & H(C_1) \end{array}\right]$$

- The 7-qubit Steane code is the most popular CSS code.
- It is created with a classical Hamming code [7,4,3] which is self dual.
- The matrix C_1 is taken as the classical parity check matrix H.

More about Stabilizer

The stabilizer is a group:

The stabilizer is Abelian:

Given any Abelian group S of Pauli operators, define a code space $T(S) = \{ |\psi\rangle \text{ s.t. } M|\psi\rangle = |\psi\rangle \ \forall\ M \in S\}$. Then T(S) encodes k logical qubits in n physical qubits when S has n-k generators (so size 2^{n-k}).

Stabilizer Elements Detect Errors

Suppose $M \in S$ and Pauli error E anticommutes with M. Then:

$$M (E |\psi\rangle) = - EM |\psi\rangle = - E |\psi\rangle,$$

so $E |\psi\rangle$ has eigenvalue -1 for M.

Conversely, if M and E commute for all $M \in S$,

$$M (E |\psi\rangle) = EM |\psi\rangle = E |\psi\rangle \quad \forall M \in S,$$

so $E |\psi\rangle$ has eigenvalue +1 for all M in the stabilizer.

The eigenvalue of an operator M from the stabilizer detects errors which anticommute with M.

From Gottesman

Distance of a Stabilizer Code

Let S be a stabilizer, and let T(S) be the corresponding QECC. Define

$$N(S) = \{N \in P_n \text{ s.t. } MN=NM \ \forall \ M \in S\}.$$

Then the distance d of T(S) is the weight of the smallest Pauli operator N in N(S) \ S.

The code detects any error not in N(S) \ S (i.e., errors which commute with the stabilizer are not detected).

Why minus S? "Errors" in S leave all codewords fixed, so are not really errors. (Degenerate QECC.)

From Gottesman

Error Syndromes and Stabilizers

To correct errors, we must accumulate enough information about the error to figure out which one occurred.

The error syndrome is the list of eigenvalues of the generators of S: If the error E commutes with M $\in$ S, then M has eigenvalue +1; if E and M anticommute, M has eigenvalue -1.

We can then correct a set of possible errors if they all have distinct error syndromes.

From Gottesman

Stabilizer Codes Correct Errors

Theorem: The code corrects errors for which $E^\dagger F \notin N(S) \setminus S$ for all possible pairs of errors (E, F).

E and F have same error syndrome $\Leftrightarrow$

E and F commute with same elements of S

$\Leftrightarrow$ $E^\dagger F \in N(S)$

$E^\dagger F \in S$ $\Leftrightarrow$ $E^\dagger F |\psi\rangle = |\psi\rangle$ $\Leftrightarrow$ $F |\psi\rangle = E |\psi\rangle$

E and F act the same, so we need not distinguish.

A stabilizer code with distance d corrects $\lfloor (d-1)/2 \rfloor$ errors (i.e., to correct t errors, we need d = 2t+1):

From Gottesman

Stabilizer Codes Summary

- Choose an Abelian subgroup of the Pauli group. This will be the stabilizer S of the QECC.
- The codewords: $\{ |\psi\rangle \text{ s.t. } M|\psi\rangle = |\psi\rangle \ \forall M \in S\}$
- If S has r generators on n qubits, the QECC has k = n-r encoded qubits.
- The codes corrects errors if $E^\dagger F \notin N(S) \setminus S$ for all pairs (E, F) of possible errors. The distance d is the minimum weight of $N(S) \setminus S$.

From Gottesman

Summary: Stabilizer Codes

- We can describe a quantum stabilizer code by giving its stabilizer, an Abelian subgroup of the Pauli group.
- By looking at the stabilizer, we can learn all of the most interesting properties of a QECC, including the set of errors it can correct.
- One interesting and useful class of stabilizer codes is the family of CSS codes, derived from two classical codes. The 7-qubit code is the smallest example.

From Gottesman

Application: 5-Qubit Code

We can generate good codes by picking an appropriate stabilizer. For instance:

$$X \otimes Z \otimes Z \otimes X \otimes I$$

$$I \otimes X \otimes Z \otimes Z \otimes X$$

$$X \otimes I \otimes X \otimes Z \otimes Z$$

$$Z \otimes X \otimes I \otimes X \otimes Z$$

n = 5 physical qubits

- 4 generators of S

k = 1 encoded qubit

Distance d of this code is 3.

Notation: [[n,k,d]] for a QECC encoding k logical qubits in n physical qubits with distance d. The five-qubit code is a non-degenerate [[5,1,3]] QECC.

From Gottesman

第五章 量子纠错

1. 量子纠错的基本理论
2. 比特翻转量子码
3. 纠单比特错误量子码，Shor码
4. 量子错误刻画
5. 纠缠纯化与量子纠错
6. 量子码的构造（经典线性码，CSS码）
7. 稳定子码(Stabilizer Codes)
8. **普适量子计算**

The Gottesman-Knill Theorem

Theorem: Suppose a quantum computation is performed which involves only the following elements: state preparations in the computational basis, Hadamard gates, phase gates, controlled-NOT gates, Pauli gates, and measurements of observables in the Pauli group (which includes measurement in the computational basis as a special case), together with the possibility of classical control conditioned on the outcome of such measurements. Such a computation may be efficiently simulated on a classical computer.

Quantum Computing Simulations

- The Gottesman-Knill theorem shows that some quantum computations involving highly entangled states may be simulated *efficiently* (in polynomial time complexity) on classical computers.
- These computations include quantum teleportation and superdense coding.
- However, *not all* types of entanglement can be described efficiently with the stabilizer formalism.

Universal quantum computation?

In order to perform truly universal quantum computation, even a single gate outside of N(G) can be sufficient. For instance, the Toffoli gate (a three-qubit gate which flips the third qubit iff both of the first two qubits are |1>) along with N(G) suffices for universal computation.

The set of U such that $UAU^{\dagger} \in G$ for all $A \in G$ is the normalizer N(G) of G in U(n).

Also for the single-qubit π/8 rotation gate

Summary of QECCs

- Quantum error-correcting codes exist which can correct very general types of errors on quantum systems.
- A systematic theory of QECCs allows us to build many interesting quantum codes.
- Quantum error correction can be formalized in terms of quantum states and projectors, stabilizer subspaces or the stabilizer group.
- All these formalizations are equivalent.
- The theory of quantum error correction is quite elegant and simple.
- The implementation is really a nontrivial task.

参考书目和文献

- Quantum computation and quantum information by M.A. Nielsen and I.L. Chuang

谢谢

中国科学技术大学 陈凯