Lecture 6: Criteria for QECC

6.1 a simple classical ECC:

repetition code

encoding: $C': \{0,1\} \to \{0,1\}^3$

$$x \mapsto xxx$$

send every bit (symbol) three times (or n times)

error correction step:

- compare all received symbols $\vec{y} = (y_1, \ldots, y_n)$
- use the most frequent as the decoding result

for $n = 3$: 1 error can be corrected

$n = 2t+1$ t errors can be corrected

assumption: a small number errors is more likely than many errors

rate of the encoding: $\frac{1}{n}$

number of errors per symbol $\frac{t}{2t+1} \to \frac{1}{2}$

2

A direct analogue of the repetition code does not work for quantum information since

1. unknown quantum states cannot be replicated
2. multiple copies of a quantum state, some of which might be corrupted, cannot be compared (without destroying them)

6.2 A first quantum code

bad idea: encoding $|\phi\rangle \mapsto |\phi\rangle^{\otimes n}$

good idea: take copies of the basis states:

$$C:\quad \mathbb{C}^2 \longrightarrow (\mathbb{C}^2)^{\otimes 3}$$

$$|0\rangle \mapsto |000\rangle$$

$$|1\rangle \mapsto |111\rangle$$

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle \mapsto \alpha|000\rangle + \beta|111\rangle$$

	state	error operator	space
no error	$\alpha\|000\rangle + \beta\|111\rangle$	$I \otimes I \otimes I$	$\mathcal{C}_0$
σ_x on 1st position	$\alpha\|100\rangle + \beta\|011\rangle$	$\sigma_x \otimes I \otimes I$	$\mathcal{C}_1$
σ_x on 2nd position	$\alpha\|010\rangle + \beta\|101\rangle$	$I \otimes \sigma_x \otimes I$	$\mathcal{C}_2$
σ_x on 3rd position	$\alpha\|001\rangle + \beta\|110\rangle$	$I \otimes I \otimes \sigma_x$	$\mathcal{C}_3$

$$\mathcal{C}_0 = \langle |000\rangle, |111\rangle \rangle$$

$$\mathcal{C}_1 = \langle |100\rangle, |011\rangle \rangle = (\sigma_x \otimes I \otimes I)\, \mathcal{C}_0$$

$$\mathcal{C}_2 = \langle |010\rangle, |101\rangle \rangle = (I \otimes \sigma_x \otimes I)\, \mathcal{C}_0$$

$$\mathcal{C}_3 = \langle |001\rangle, |110\rangle \rangle = (I \otimes I \otimes \sigma_x)\, \mathcal{C}_0$$

$$(\mathbb{C}^2)^{\otimes 3} = \mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \mathcal{C}_2 \oplus \mathcal{C}_3$$

decomposition of $(\mathbb{C}^2)^{\otimes 3}$ into 4 mutually orthogonal subspaces $\mathcal{C}_i$

This code can correct one „bit-flip error" σ_x, but cannot even detect a single „sign-flip error" σ_z

A code correcting one σ_z-error (but no σ_x-error):

The Hadamard transform $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ interchanges σ_x and σ_z, i.e.

$$H \sigma_x H = \sigma_z$$

Using the code $(H \otimes H \otimes H) \mathcal{C}_0$, we can correct one sign-flip error

$$(H \otimes H \otimes H)|000\rangle = \frac{1}{\sqrt{8}} \sum_{x \in \{0,1\}^3} |x\rangle$$

$$(H \otimes H \otimes H)|111\rangle = \frac{1}{\sqrt{8}} \sum_{x \in \{0,1\}^3} (-1)^{x_1+x_2+x_3} |x_1 x_2 x_3\rangle$$

different bases

$$|0\rangle \mapsto \sum_{\mathrm{wgt}(x)\ \mathrm{even}} |x\rangle$$

$$|1\rangle \mapsto \sum_{\mathrm{wgt}(x)\ \mathrm{odd}} |x\rangle$$

$\mathrm{wgt}(x)$ = number of non-zero elements

first "full" quantum error-correcting code (QECC)
by Peter Shor:

combine two levels of these simple codes,
one correcting σ_x-errors, the other level
correcting σ_z-errors

$\Rightarrow$ nine qubit code correcting one "general"
error (more details later)

6.3 QECC conditions by Knill & Laflamme 97

Let $\mathcal{C} \leq \mathcal{H}$ be a subspace of the Hilbert space $\mathcal{H}$ and let $\{A_i : i \in \mathcal{I}_Q\}$ be the errors of a quantum channel Q on $\mathcal{H}$.

Furthermore, let $\{|c_i\rangle : i \in \mathcal{I}_\mathcal{C}\}$ be an orthonormal basis of $\mathcal{C}$.

Then $\mathcal{C}$ is a quantum error-correcting code for the channel Q, iff

(i) $\forall k,l \in \mathcal{I}_Q \; \forall i \neq j \in \mathcal{I}_\mathcal{C} : \quad \langle c_i | A_k^\dagger A_l | c_j \rangle = 0$

(ii) $\forall k,l \in \mathcal{I}_Q \; \forall i,j \in \mathcal{I}_\mathcal{C} : \langle c_i | A_k^\dagger A_l | c_i \rangle = \langle c_j | A_k^\dagger A_l | c_j \rangle$
$= \alpha_{kl}$

Equivalently, if $P_\mathcal{C}$ denotes the projection onto $\mathcal{C}$, then

(iii) $\forall k,l \in \mathcal{I}_Q : \; P_\mathcal{C} A_k^\dagger A_l P_\mathcal{C} = \alpha_{kl} P_\mathcal{C}$

6.4 Lemma:

The error-correction conditions 6.3 are linear in the error operators.

Proof: $A = \sum \lambda_k A_k \qquad B = \sum \mu_\ell A_\ell$

a) $\langle c_i | A^\dagger B | c_j \rangle = \langle c_i | \left(\sum \lambda_k^* A_k^\dagger\right)\left(\sum \mu_\ell A_\ell\right) | c_j \rangle$

$= \sum \lambda_k^* \mu_\ell \langle c_i | A_k^\dagger A_\ell | c_j \rangle \overset{(i)}{=} 0$

b) similarly: $\langle c_i | A^\dagger B | c_i \rangle \overset{(ii)}{=} \langle c_j | A^\dagger B | c_j \rangle$

Consequence: It is sufficient to test/fulfill the conditions 6.3 for a vector space basis of all error operators of the channel.

"Constructive" proof of the QECC conditions 6.3

in the conditions, we have inner products of the (unnormalized) states $A_k |c_i\rangle$

	$A_1 \mathcal{C}$	$A_2 \mathcal{C}$	...	$A_k \mathcal{C}$	
$\mathcal{V}_0$	$A_1 \lvert c_0\rangle$	$A_2 \lvert c_0\rangle$	....	$A_k \lvert c_0\rangle$	...
$\mathcal{V}_1$	$A_1 \lvert c_1\rangle$	$A_2 \lvert c_1\rangle$	...	$A_k \lvert c_1\rangle$	...
	$\vdots$				
$\mathcal{V}_i$	$A_1 \lvert c_i\rangle$	$A_2 \lvert c_i\rangle$	...	$A_k \lvert c_i\rangle$	
					$\ddots$

Condition (i): the spaces $\mathcal{V}_i$ are mutually orthogonal, i.e $\mathcal{V}_i \perp \mathcal{V}_j$

consider the vector space $\mathcal{V}_0 = \{ A_k |c_0\rangle : k \in I_Q \}$

perform a Gram-Schmidt orthogonalisation in $\mathcal{V}_0$

for $j \in I_Q$ do

$$|b_j^{(i)}\rangle \leftarrow A_j |c_i\rangle$$

$$|b_j^{(i)}\rangle \leftarrow |b_j^{(i)}\rangle - \sum_{l<j} \langle b_l^{(i)} | b_j^{(i)}\rangle \cdot |b_l^{(i)}\rangle$$

if $|b_j^{(i)}\rangle \neq 0$

$$|b_j^{(i)}\rangle \leftarrow \frac{1}{\sqrt{\langle b_j^{(i)} | b_j^{(i)}\rangle}} \cdot |b_j^{(i)}\rangle$$

end if

end for

$\Rightarrow$ ONB for the space $\mathcal{V}_i$

$$|b_j^{(i)}\rangle = \sum_{k \in I_Q} \lambda_{jk}^{(i)} A_k |c_i\rangle$$

The coefficients $\lambda_{jk}^{(i)}$ depend only on the inner products of the vectors $A_k |c_i\rangle$ in $\mathcal{V}_i$, i.e. on

$$\langle c_i | A_l^\dagger A_k | c_i\rangle \overset{(i)}{=} \alpha_{lk}$$

$\Rightarrow$ They are independent of the state $|c_i\rangle$.

Instead of taking linear combinations of the basis states in $\mathcal{V}_i$, we replace the operators A_k by linear combinations, i.e

$$\tilde{A}_j := \sum_{k \in I_Q} \lambda_{jk} A_k$$

$\Rightarrow$ new scheme:

	$\tilde{A}_1 \mathcal{C}$	$\tilde{A}_2 \mathcal{C}$	$\ldots$	$\tilde{A}_K \mathcal{C}$
$\mathcal{V}_0$	$\tilde{A}_1 \vert c_0\rangle$	$\tilde{A}_2 \vert c_0\rangle$	$\ldots$	$\tilde{A}_K \vert c_0\rangle$
$\mathcal{V}_1$	$\tilde{A}_1 \vert c_1\rangle$	$\tilde{A}_2 \vert c_1\rangle$		$\tilde{A}_K \vert c_1\rangle$
$\vdots$				
$\mathcal{V}_i$	$\tilde{A}_1 \vert c_i\rangle$	$\tilde{A}_2 \vert c_i\rangle$		$\tilde{A}_K \vert c_i\rangle$

$\Rightarrow$ now the spaces $\tilde{A}_k \mathcal{C}$ and $\tilde{A}_\ell \mathcal{C}$ for $k \neq \ell$ are mutually orthogonal

$\rightarrow$ There exists a measurement which projects onto onto one of these spaces and yields information on the error $\tilde{A}_k$.