What if errors occur on more than one qubit?

Some – but not all – errors are corrected:

E.g.: $X_1 X_4$: correctable.

$Z_1 Z_2$: trivial (no error)

But: $X_1 X_2$: breaks code $\frac{1}{2}$

$Z_1 Z_4$: breaks code $\frac{1}{2}$

$\Rightarrow$ Concatenate codes or use better codes.

3. Quantum error correction conditions & properties of Quantum Error Correcting Codes (QECC)

QECC: Defined by code space C (containing codewords); choose basis $|\bar{i}\rangle$.

Noise model: CPTP map

$$\mathcal{E}(\rho) = \sum E_\alpha \rho E_\alpha^\dagger \; ; \; \sum E_\alpha^\dagger E_\alpha = \mathbb{1}$$

(i.e.: error E_α w/ prob. $\mathrm{tr}(E_\alpha^\dagger E_\alpha \rho)$; e.g. $E_\alpha \propto$ pauli's.)

Want: Recovery procedure: Measurement + correction

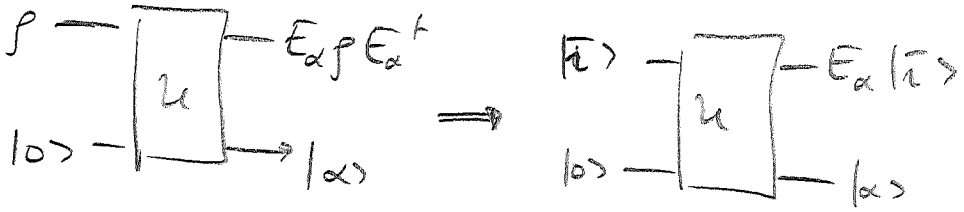
$\longleftrightarrow$ CP map $\mathcal{R}(\rho) = \sum_k R_k \rho R_k^\dagger$.

Require that $\mathcal{R}(\mathcal{E}(\rho)) = \rho$ for all $\rho \in C$.

Under which conditions on C & $\mathcal{E}$ does this hold, i.e., we can correct $\mathcal{E}$?

Intuition:

$\rho \mapsto \mathcal{E}(\rho)$ $\longleftrightarrow$ Chapter I: Stinespring dilation



Necessary condition for error correction:

(i) environment carries no information about ρ for any ρ in the codespace (!)

$\Rightarrow$ $\underbrace{\langle \tilde{i} | E_\alpha^\dagger E_\alpha | \tilde{i} \rangle}_{\text{prob. for } \alpha.} = C_\alpha$

(ii) orthogonal states must remain orthogonal (otherwise we cannot undo error):

$\mathcal{E}(|i\rangle\langle i|) \perp \mathcal{E}(|j\rangle\langle j|)$ for $\langle i | j \rangle = 0$

↑ supported on $\perp$ space!

$$\Rightarrow \delta_{ij} \propto \mathrm{tr}\left(\mathcal{E}(|i\rangle\langle i|)\, \mathcal{E}(|j\rangle\langle j|) \right)$$

$$= \sum_{\alpha\beta} \mathrm{tr}\left(E_\alpha |i\rangle\langle i| E_\alpha^\dagger E_\beta |j\rangle\langle j| E_\beta^\dagger \right)$$

$$= \sum_{\alpha\beta} \left| \langle j| E_\beta^\dagger E_\alpha |i\rangle \right|^2$$

$$\Rightarrow \boxed{\langle j| E_\beta^\dagger E_\alpha |i\rangle = c_{\alpha\beta}\, \delta_{ij}} \qquad c_{\alpha\beta} = c_{\beta\alpha}^*$$

Quantum Error Correction Condition

Sufficiency: Construct explicit recovery operation $\mathcal{R} = \sum R_\beta \cdot R_\beta^\dagger$

Step 1: Use gauge degree of freedom in $\mathcal{E}$:

$$\sum E_{\alpha\beta} E_\alpha^\dagger = \sum F_\gamma \rho F_\gamma^\dagger \quad \text{if } F_\gamma = \sum_\alpha V_{\gamma\alpha} E_\alpha, \; V \text{ isometry}$$

Choose V s.t. $V_{\alpha\varepsilon}^* c_{\alpha\beta} V_{\beta\gamma} = \lambda_\varepsilon \delta_{\varepsilon\gamma}$: diagonal

$$\Rightarrow \langle i| F_\alpha^\dagger F_\beta |j\rangle = \lambda_\alpha \delta_{\alpha\beta} \delta_{ij}$$

I.e.: Different α can be distinguished by measurement!

Step 2: Measure α & undo error F_α.

Want R_β s.th. $R_\beta F_\alpha |\bar{\imath}\rangle = \delta_{\alpha\beta} |\bar{\imath}\rangle$

Choose $R_\beta = \frac{1}{\lambda_\beta} \sum_j |\bar{\jmath}\rangle\langle\bar{\jmath}| F_\beta^\dagger$

$$\Rightarrow R_\beta F_\alpha |\bar{\imath}\rangle = \frac{1}{\lambda_\beta} \sum_j |\bar{\jmath}\rangle \underbrace{\langle\bar{\jmath}| F_\beta^\dagger F_\alpha |\bar{\imath}\rangle}_{\lambda_\alpha \delta_{ij}\delta_{\alpha\beta}} = \delta_{\alpha\beta} |\bar{\imath}\rangle .$$

$$\Rightarrow \mathcal{R}(\mathcal{E}(\rho)) = \sum R_\beta F_\alpha \rho F_\alpha^\dagger R_\beta^\dagger = \rho \quad \forall \rho \in \mathcal{C}.$$

Note: For any single-qubit error E_α, we have

$$E_\alpha = \sum_{k,p} w_{\alpha k p}\, \sigma_{k,p}$$

($\sigma_{k,p}$: Pauli Gates on site p)

I.e.: $\langle\bar{\jmath}| \sigma_{kp}^\dagger \sigma_{qi} |\bar{\imath}\rangle \propto \delta_{ij} \Rightarrow \langle\bar{\jmath}| E_\beta^\dagger E_\alpha |\bar{\imath}\rangle \propto \delta_{ij}$

I.e.: Err. Corr. Cond. holds for Paulis $\Rightarrow$ err. corr.

Conds hold for any single-qubit error!

(In part.: Robust to depol. channel $\mathcal{E}(\rho) = p\rho + \frac{(1-p)}{3}[X_\rho X + Y_\rho Y + Z_\rho Z]$
$\Rightarrow$ robust to any channel!)

Examples: 3qubit, 9qubit code $\longrightarrow$ Homework!

Properties of QECC:

We focus on *binary codes*: Encode k qubits into $n > k$ qubits.

Distance d: Smallest # of Paulis ($\neq I$) in E_α s.th.

$$\langle \bar{j} | E_\alpha | \bar{i} \rangle \neq \lambda_\alpha \delta_{ij}.$$

(E.g.: 9-qubit code: Distance $d=3$, e.g. $E_\alpha = Z_1 Z_4 Z_7$.
Note: $E_\alpha = Z_1 Z_2$ maps $|\bar{i}\rangle$ to ~~itself~~!)

Notation: $[\![n, k, d]\!]$ code

- n: phys. qubits
- k: enc. qubits
- d: distance

How many single-qubit errors, t, can a distance d code correct? E_α, E_β: $\leq t$ Paulis $\Longrightarrow$

$$\langle \bar{j} | \underbrace{E_\beta^\dagger E_\alpha}_{\leq 2t \text{ Paulis}} | \bar{i} \rangle \overset{?}{=} c_{\alpha\beta} \delta_{ij} \Longleftrightarrow \underline{\underline{2t+1 \leq d}}$$

Note: If we know the location of the t errors, then

$E_\beta^\dagger E_\alpha$ has t Paulis $\Rightarrow$ $\underline{t+1 \leq d}$.

$\Rightarrow$ C can correct t errors in arbitrary locations $\Rightarrow$ t can correct $2t$ errors in known locations.

Are there constraints on $[[n,k,d]]$?

> Def.: A code is called non-degenerate if different Pauli errors lead to different states, $\langle \bar{j} | E_\beta^\dagger E_\alpha | \bar{i} \rangle \propto \delta_{\alpha\beta}$.
>
> E.g. the 9-qubit code is degenerate, since $Z_1, Z_2 Z_1, Z_3$ have same syndrome.

Hamming bound: For non-deg. codes,

$$\sum_{j=0}^{t} 3^j \binom{n}{j} \leq 2^{n-k} \qquad ; \; 2t+1 = d,$$

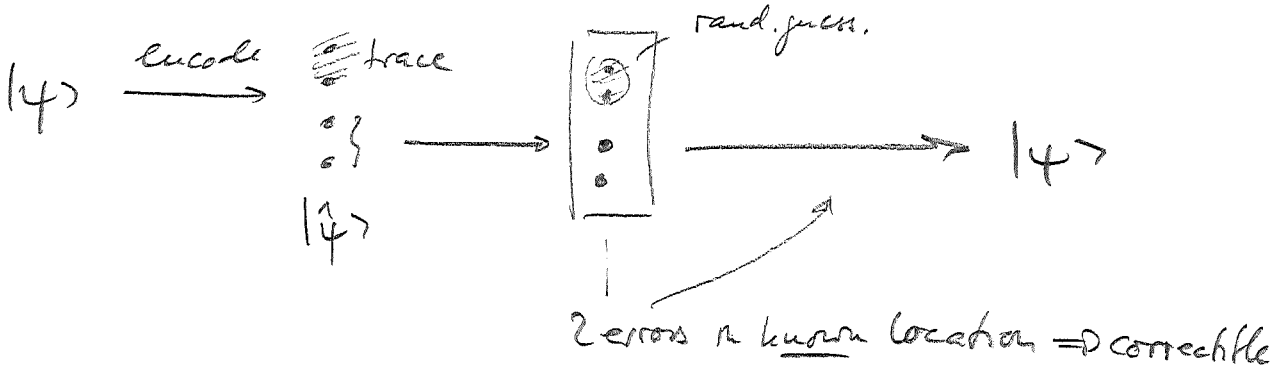
(Proof via counting $\Rightarrow$ Homework)

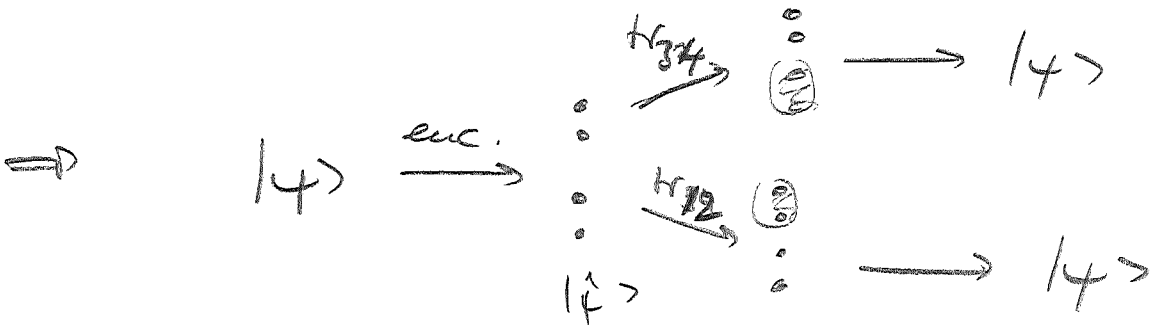
For $k=1$, $t=1$ $(d=3)$ – encode 1 qubit, correct 1 error:

$$\underline{n \geq 5}.$$

Could there be a degenerate $[\![4,1,3]\!]$ code?

No:





↯ violates no-cloning!

$\Rightarrow$ $[\![5,1,3]\!]$ code optimal!

4. Classical codes

$[n,k,d]$ code: encode k bits in n bits, distance d.

Consider linear codes:

$\underline{a} = (a_1, \dots, a_k) \in \{0,1\}^k$ encoded in

$\underline{v}(\underline{a}) = \sum_i a_i \underline{v}_i$; $\underline{v}_i \in \{0,1\}^n$ (all mod 2!)

Define generator matrix $G = \begin{pmatrix} \underline{v}_1 \\ \vdots \\ \underline{v}_k \end{pmatrix}$; $k \times n$ matrix.

Encoding: $\underline{a} \longmapsto \underline{v}(\underline{a}) = \underline{a} G$

Alternative characterization:

Parity check matrix H: $(n-k) \times n$ matrix.

equiv. def.:
- rows of $H \perp$ rows of G
- $H \underline{v}^T = 0 \ \forall \underline{v} \in C$
- $\ker H = \operatorname{im} G^T$

Errors: Bit flips, given by $\underline{e} = \{0,1\}^n$:

$$\underline{v} \longrightarrow \underline{v} + \underline{e}$$

Detect error with H: $\underline{v} \in$ code:

$$H(\underline{v} + \underline{e})^T = \underbrace{H \underline{v}^T}_{=0} + H \underline{e}^T = \underbrace{H \underline{e}^T}$$

syndrome of $\underline{e}$.

Set of possible errors:

Recovery possible iff all e_i have different syndromes,

i.e.: $H e_i^T = H e_j^T \Rightarrow e_i = e_j$.