ITO

$$\Pi_{C_1} S_1 \Pi_{C_1} = \frac{1}{2}(\mathbb{1} + S_1) S_2$$

commute!

$$\mathrm{tr}\left(\frac{1}{2}(\mathbb{1} + S_1) S_2\right) = 0 \quad (\text{as } S_1, S_2 \neq \pm I)$$

$\Rightarrow$ $\frac{1}{2}(\mathbb{1} + S_1) S_2$ has eq. # of ± 1 eigenvalues

(whose eigenvectors span C_1)

$\Rightarrow$ $\dim C_2 = \dim C_1/2 = 2^{n-2}$ ... etc, inductively,

Dimension of code space: $\underline{\dim C = 2^{n-k}}$

What about error correcting conditions?

Pauli errors E_α: 3 possibilities for $E_\beta^\dagger E_\alpha$:

(i) $E_\beta^\dagger E_\alpha$ anti-comm. w/ some $S \in \mathcal{S}$:

$$\langle \bar{j} | E_\beta^\dagger E_\alpha | \bar{i} \rangle = \langle \bar{j} | E_\beta^\dagger E_\alpha S | \bar{i} \rangle =$$

$$= - \langle \bar{j} | S E_\beta^\dagger E_\alpha | \bar{i} \rangle = \langle \bar{j} | E_\beta^\dagger E_\alpha | \bar{i} \rangle$$

$\Rightarrow \langle \bar{j} | E_\beta^\dagger E_\alpha | \bar{i} \rangle = 0.$ ✓

(ii). $E_\beta^\dagger E_\alpha \in \mathcal{S}$:

$$\langle \bar{j} | \underbrace{E_\beta^\dagger E_\alpha}_{\in \mathcal{S}} | \bar{i} \rangle = \langle \bar{j} | \bar{i} \rangle = \delta_{ij}$$

Case (i) & (ii) satisfy EC Cond. $\Rightarrow$ error correctable.

(iii) $E_\beta^\dagger E_\alpha$ comm. w/ all $S \in \mathcal{S}$, but $E_\beta^\dagger E_\alpha \notin \mathcal{S}$:

$\Rightarrow E_\beta^\dagger E_\alpha$ acts non-triv. on code space

$\Rightarrow$ <u>Logical operator</u> $\Rightarrow$ not correctable.

<u>Example:</u> 3-qubit code

$$\left.\begin{aligned} S_1 &= ZZI \\ S_2 &= ZIZ \end{aligned}\right\} \quad \mathcal{S} = \{III, ZZI, ZIZ, IZZ\}$$

$k = 3-2 = 1 \Rightarrow$ 1 encoded qubit

Single-qubit X errors: $E_\alpha = III, IIX, IXI, XII$

$\Rightarrow E_\beta^\dagger E_\alpha = III, IIX, IXI, XII, XXI, XIX, IXX$

$\Leftrightarrow$ Anti-comm. w/ S_1, S_2, $S_1 S_2$, or $\in \mathcal{S}$.

$\Rightarrow$ correctable.

<u>Single-qubit Z errors:</u> $E_\beta^\dagger E_\alpha = ZII$ possible.

ZII comm. w S_1, S_2 but $ZII \notin \mathcal{S}$ ↯

$\Rightarrow$ 2 errors not correctable!

Logical operators:

- $\hat{Z} = ZII$ (or any $\hat{Z}' = \hat{Z} \cdot S$, $S \in \mathcal{S}$, e.g. $\hat{Z}' = IZI, ZZZ, \ldots$)
- $\hat{X} = XXX$, or e.g. $\hat{X}' = XXX \cdot ZZI = YYI, \ldots$

Normalizer + logical operators:

Normalizer $\mathcal{N}$ of $\mathcal{S}$: $P^\dagger = P \; \forall P \in \mathcal{G}$

$$\mathcal{N} = \{P \in \mathcal{G} \mid S = PSP^\dagger \; \forall S \in \mathcal{S}\} = \underbrace{\{P \in \mathcal{G} \mid PS = SP \; \forall S \in \mathcal{S}\}}_{\text{Centralizer}}$$

i.e.: all $N \in \mathcal{N}$ leave $\mathcal{C}$ invariant.

$\mathcal{S} \subset \mathcal{N}$: trivial operators (no error)

$\mathcal{N} - \mathcal{S}$: non-trivial logical operators

Note: $N \in \mathcal{N}$ and NS, $S \in \mathcal{S}$, act equivalently.

$\Rightarrow$ Logical space $\hat{=}$ quotient $\mathcal{N}/\mathcal{S}$.

Distance of code = "shortest" non-trivial logical operator

= "shortest" element in $\mathcal{N} - \mathcal{S}$.

Examples:

3-qubit phase flip code:

$S_1 = XXI$

$S_2 = IXX$

$\hat{X} = XII$

$\hat{Z} = ZZZ$

9-qubit Shor code:

$S_1 = ZZIIIIIII$

$S_2 = IZZIIIIII$

$S_3 = IIIZZIIII$

$S_4 = IIIIZZIII$

$S_5 = IIIIIIZZI$

$S_6 = IIIIIIIZZ$

$S_7 = XXXXXXIII$

$S_8 = IIIXXXXXX$

8 stabilizers = 1 enc. qubit

Logical X of 3-qubit code!

Logical operators:

$\hat{Z} = ZZZZZZZZZ$

$\hat{X} = XXXXXXXXX$

odd # of Z / X; commute w/ S!

simple $\hat{Z}, \hat{X}$: $\hat{Z}' = ZII\,ZII\,ZII = \hat{Z} \cdot S_2 S_4 S_6$

$\hat{X}' = XXVIII\,III = \hat{X} \cdot S_8$

⇒ meas. 3 qubit enough to meas. encoded qubit in X/Z basis.

(Note: $\hat{X}$ & $\hat{Z}$ together must use at least 5 qubits

→ classy argument!)

Degenerate code: $\underbrace{ZZIIIIIII}_{} = S_1 \in \mathcal{S}$

possible $E_\beta^\dagger E_\alpha$ for 1 qubit.

(i.e.: 1 qubit code degen ⟺ $\exists\, S \in \mathcal{S}$ w/ 2 Paulis)

$\mathcal{N} = \{\bar{Z} \cdot S, \bar{X} \cdot S, \bar{X} \cdot \bar{Z} \cdot S \mid S \in \mathcal{S}\}$

Distance $d = 3$ (e.g. $\hat{Z}'$ or $\hat{X}'$ above!)

Steane code: Homework!

Note: For all CSS codes, with $H = \begin{pmatrix} \underline{\omega}_1 \\ \vdots \\ \underline{\omega}_r \end{pmatrix}$:

$S_1 = X^{\omega_{1,1}} \cdot X^{\omega_{1,2}} \cdots$

$S_2 = X^{\omega_{2,1}} \cdot X^{\omega_{2,2}} \cdots$

$\vdots$

$S_{r+1} = Z^{\omega_{1,1}} Z^{\omega_{2,2}} \cdots$

$\vdots$

I.e.: For CSS codes, the S_i consist of 2 groups — only with X only & one w/ Z only (and they are identical!)

The 5-qubit code

$$S_1 = X\,Z\,Z\,X\,I$$
$$S_2 = I\,X\,Z\,Z\,X$$
$$S_3 = X\,I\,X\,Z\,Z$$
$$S_4 = Z\,X\,I\,X\,Z$$
$$(S_5 = Z\,Z\,X\,I\,Z)$$

Encodes 1 qubit.

Note: $S_5 = ZZXIX = S_1 S_2 S_3 S_4$

Cyclic code: $S_1, \ldots, S_5$ cyclic perms of S_1 ⇒ cyclic code. words ok!

Corrects any 1-qubit error:

$E_\beta^\dagger E_\alpha$ = Prod. of 2 Paulis

⇒ anti-comm. w/ at least one S_i!

(E.g. via: each col. has one I ⇔ that S_i fixes the other Pauli error ⇒ both Pauli errors fixed by two S_i ⇒ ✓)

⇒ Distance $d \geq 3$ (and $d \leq 3$ because of cloning!)

Syndromes: (1 ≡ anti-com.)

	X error a					Y error a					Z error a				
	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
S_1	0	1	1	0	0	1	1	1	1	0	1	0	0	1	0
S_2	0	0	1	1	0	0	1	1	1	1	0	1	0	0	1
S_3	0	0	0	1	1	1	0	1	1	1	1	0	1	0	0
S_4	1	0	0	0	1	1	1	0	1	1	0	1	0	1	0
(S_5)	1	1	0	0	0	1	1	1	1	0	1	0	0	1	0	1

⇒ each error has different syndrome ⇒ non-degen.

and all 2^4-1 syndromes appear!

Logical operators:

$\hat{Z} = ZZZZZ$ } $\in \mathcal{N}$, and $\notin \mathcal{S}$, since all
$\hat{X} = XXXXX$ } S_i have even # of X & Z.

or, simply: $\hat{Z}' = \hat{Z} \cdot S_3 = -YZYII$

$\hat{X}' = \hat{X} \cdot S_2 = -XIYYI$

⇒ distance $d = 3$.

and: we can read out logical info in $\hat{Z}/\hat{X}$ basis by meas. 3 qubits only.

Syndrome measurement + correction can be done only w/ (Controlled-NOT, H, and ancillas

⟹ Homework!

Clifford gates:

The Clifford group $\mathcal{C}$ consists of all gates which map Paulis to Paulis:

$$\mathcal{C} = \{ C \mid C(P_1 \otimes \dots \otimes P_n) C^\dagger = P_1' \otimes \dots \otimes P_n' \}$$

Theorem:

$$\mathcal{C} \equiv \{ \text{all circuits built from CNOT, } S = \begin{pmatrix} 1 & \\ & i \end{pmatrix}, \text{ and } H. \}$$

(Impact: Any C which maps Paulis to Paulis is of this form!)

Note: Only $T = \begin{pmatrix} 1 & \\ & e^{i\pi/4} \end{pmatrix}$ missing for a universal gate set!

How to apply gates on encoded qubits?

→ Decode / Apply / Encode: Bad idea — info not protected!

→ Try to apply gates to encoded qubits!

Stabilizer codes: Clifford gates can be applied to encoded qubits:

Clifford gates on logical qubits

⇓

maps Paulis to Paulis (logical)

⇓ logical Paulis are prods. of physical Paulis!

maps Paulis to Paulis (physical)

⇓

Clifford gate on physical qubits.

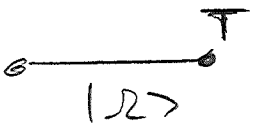
E.g.: 5-qubit code $\hat{H}$ gate:

$\hat{X} = XXXXX$
$\hat{Z} = ZZZZZ$
$\hat{H}\hat{X}\hat{H} = \hat{Z}$

} find Clifford s.th. $XXXXX \hookrightarrow ZZZZZ$ & stabilizers are preserved!

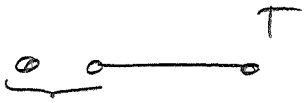
Can we also realize non-Clifford gates (e.g. $T = \begin{pmatrix} 1 & \\ & e^{i\pi/4} \end{pmatrix}$) in a robust way?

Our idea: Gate teleportation:

Prepare $|X\rangle$ = 

↑ ME state $|\Omega\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

+ "teleport" through $|X\rangle$



Bell meas.

↳ Outcome $|\Omega\rangle$: result is $T|X\rangle$

→ otherwise: different outcome, but can be transformed to T w/ Clifford (→ HW!)

& $|X\rangle$ can be prepared (+ tested) beforehand in an encoded state

& telep. circuit consists of Cliffords + meas. in Z basis.