V. Quantum Error Correction

1. Introduction

a) Setting & Problem

- Coupling to environment induces errors (i.e., uncontrolled behavior).
- Classical computers: Information stored in "macroscopic" properties → errors unlikely.
- Quantum computers:
  - need qubits = "single" quantum systems, and must store general superposition, not just $|0\rangle$ and $|1\rangle$

    → fragile!
  - should be well isolated to protect qubits, but also need coupling to "environment" (experimental apparatus) to control the computation (gates, measurements).

Q: Can we protect quantum information from noise?

Classical error correction:

copy information, e.g. encode 1 bit in 3 bits:

$$0 \longmapsto \hat{0} := 000 \qquad\qquad \text{"encoding"}$$

$$1 \longmapsto \hat{1} := 111$$

Error model: Bit flip w/ some (small) probability p (independently on all bits):

$\Longrightarrow$ typically 0 or 1 bits flipped.

Error correction ("decoding") by majority vote:

$$000, 001, 010, 100 \longmapsto 000$$

$$111, 110, 101, 011 \longmapsto 111$$

Probability for a "logical error" (i.e. on encoded bit):

$$p_{\text{error}} = \text{prob}(\geq 2 \text{ flips}) = p^3 + 3p^2(1-p)$$

$$= \underset{\text{error quadratically suppressed!}}{3p^2} - 2p^3 < p \quad \text{for } p < 1/2.$$

$\Longrightarrow$ effective error probability decreased.

Can be improved by:

- using more bits: $0 \mapsto 00\cdots0$, $1 \mapsto 11\cdots1$
- nesting ("concatenating") codes
- using smarter codes (i.e. encode several bits at once)

Quantum Error Correction:

Several potential problems when trying to generalize classical error correction codes:

- cannot copy qubits
- even if we could: what would be the "majority vote"?
- different types of errors exist,

  e.g. X (bit flip)

  or Z ("phase flip")
- errors can be continuous: there is an infinity of errors!
- measuring qubits destroys quantum information!

6) The 3-qubit bit flip code

Copy qubits in computational basis:

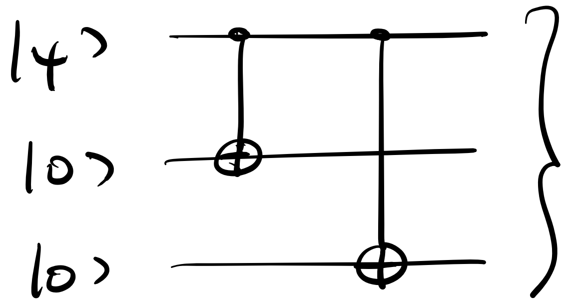
$$|0\rangle \longmapsto |\hat{0}\rangle = |000\rangle$$

$$|1\rangle \longmapsto |\hat{1}\rangle = |111\rangle$$

i.e., the encoding is a linear map

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \xmapsto{\text{encoding}} \alpha|000\rangle + \beta|111\rangle$$

Possible encoding circuit:



$$|\hat{\psi}\rangle = \alpha|000\rangle + \beta|111\rangle$$

Now consider bit flip error on qubit i:

$$|\hat{\psi}\rangle \xmapsto{\text{error}} X_i|\hat{\psi}\rangle$$

Can we correct for one bit flip error on an unknown qubit i?

Problem: Measuring the qubits in comp. basis reveals i, but also destroys superposition!

$\Rightarrow$ Need a measurement which only returns information about position i of error – indep. of encoded state $|\psi\rangle$!

Define "syndrome measurement" with outcomes $0,1,2,3$, and projectors:

0 = "no flip": $P_0 = |000\rangle\langle 000| + |111\rangle\langle 111|$

1 = "1st qubit flipped": $P_1 = |100\rangle\langle 100| + |011\rangle\langle 011|$

2 = "2nd qubit flipped": $P_2 = |010\rangle\langle 010| + |101\rangle\langle 101|$

3 = "3rd qubit flipped": $P_3 = |001\rangle\langle 001| + |110\rangle\langle 110|$

(This defines a complete measurement, as $\sum P_i = I$)

The outcome is called the "error syndrome".

Measurement of $\{P_\alpha\}$ reveals only 2 bits of info.

$\Rightarrow$ one qubit of information untouched!

By direct inspection: The information obtained is the location of the bit flip, e.g.

$$\alpha|000\rangle + \beta|111\rangle \xmapsto[\text{on qubit 2}]{\text{bit flip}} \alpha|010\rangle + \beta|101\rangle$$

$\Rightarrow$ measurement always returns P_2, with post-measurement state

$$\alpha|010\rangle + \beta|101\rangle \xmapsto[\text{flip qubit 2}]{\text{recovery:}} \alpha|000\rangle + \beta|111\rangle \,!$$

$\Rightarrow$ Bit flip corrected!

Works for any single bit flip in unknown location and no flip, and for all states $|\psi\rangle$

$\Rightarrow$ suppression of error $p \rightsquigarrow 3p^2 - 2p^3$, as classically.

By linearity, this also works for part of a larger entangled state:

$$\alpha|0\rangle|a\rangle + \beta|1\rangle|b\rangle \xmapsto{\text{encode}} \alpha|000\rangle|a\rangle + \beta|111\rangle|b\rangle$$

$$\xmapsto[X_1]{\text{error:}} \alpha|100\rangle|a\rangle + \beta|011\rangle|b\rangle \xmapsto[\text{correct: } X_1]{\text{meas.: } P_1} \alpha|000\rangle|a\rangle + \beta|111\rangle|b\rangle$$

What about continuous errors, e.g.

$$|\hat{\psi}\rangle \longmapsto e^{i\vartheta X_i}|\hat{\psi}\rangle = \left(\cos\vartheta\, I + i\sin\vartheta\, X_i\right)|\hat{\psi}\rangle \;?$$

$$|\hat{\psi}\rangle = \alpha|000\rangle + \beta|111\rangle \xmapsto[\text{e.g. } X_3]{\text{error,}} \alpha\left(\cos\vartheta|000\rangle + i\sin\vartheta|001\rangle\right) + \beta\left(\cos\vartheta|111\rangle + i\sin\vartheta|110\rangle\right)$$

$$= \underset{\substack{\uparrow \\ \text{prob.: } |\cos\vartheta|^2}}{\cos\vartheta}\underbrace{\left(\alpha|000\rangle + \beta|111\rangle\right)}_{\text{syndrome } P_0} + \underset{\substack{\uparrow \\ \text{prob.: } |\sin\vartheta|^2}}{i\sin\vartheta}\underbrace{\left(\alpha|001\rangle + \beta|110\rangle\right)}_{\text{syndrome } P_3}$$

Syndrome measurement collapses state into:

$p = \cos^2\vartheta$: result P_0,

post-meas. state $\alpha|000\rangle + \beta|111\rangle$,

$0 \equiv$ no correction : OK ✓

$p = \sin^2\vartheta$: result P_3,

post-meas. state $\alpha|001\rangle + \beta|110\rangle$,

$3 \equiv$ correction: flip bit 3:

$\Longrightarrow \alpha|000\rangle + \beta|111\rangle$: OK ✓

Measurement of error syndrome $\{P_\alpha\}$ collapses continuous error onto one of the 4 correctable discrete errors:

- measurement "digitalizes" error
- sufficient to study discrete (distinguishable) errors (will be formalized later)

A different perspective on syndrome measurement & correction (the "stabilizer formalism" – more later):

$|000\rangle, |111\rangle$: +1 eigenstates of $Z_1 Z_2$ and $Z_2 Z_3$
("stabilizers")

Measure $\underbrace{Z_1 Z_2}$ and $\underbrace{Z_2 Z_3}$:

compare qubits 1&2 and 2&3

$(+1, +1)$: no error

$(-1, +1)$: qubit 1 flipped

$(+1, -1)$: qubit 3 flipped

$(-1, -1)$: qubit 2 flipped

More formally:

encoded state $|\hat{\psi}\rangle = \alpha|000\rangle + \beta|111\rangle$:

$$\Longrightarrow Z_1 Z_2 |\hat{\psi}\rangle = |\hat{\psi}\rangle \; , \; Z_2 Z_3 |\hat{\psi}\rangle = |\hat{\psi}\rangle$$

Bit flip error, e.g. X_1:

X_1 anti-commutes with $Z_1 Z_2$

$$\Longrightarrow \langle\hat{\psi}| X_1 Z_1 Z_2 X_1 |\hat{\psi}\rangle = - \langle\hat{\psi}| Z_1 Z_2 |\hat{\psi}\rangle$$

$$= -1$$

Thus:

Outcome -1 for $Z_1 Z_2$ $\Longleftrightarrow$ an error which anti-commutes with $Z_1 Z_2$ has occurred.

The correction operation must satisfy the <u>same</u> anti-commutation relations (and some further properties) → <u>later!</u>

Have focused on X errors.

But what about Z <u>errors</u>?

$$\alpha|000\rangle + \beta|111\rangle \xmapsto[\text{on qubit 1}]{\text{Z error}} \alpha|000\rangle - \beta|111\rangle$$

This is still a state in the <u>code space</u>

(i.e., a valid encoded state $|\hat{\psi}\rangle$)

$\Rightarrow$ error <u>not detectable</u>, but it <u>has changed</u> <u>$|\hat{\psi}\rangle$</u>. After decoding, the error acts as

$$\alpha|0\rangle + \beta|1\rangle \longmapsto \alpha|0\rangle - \beta|1\rangle,$$

i.e. as a <u>logical Z operator</u>.

"logical operator" = operator on encoded qubit.

$\Rightarrow$ 3-qubit bit flip code <u>cannot protect</u> <u>against</u> single <u>"phase flip error"</u> Z_i.

Stabilizer picture:

Error Z_i commutes with stabilizers $Z_1 Z_2$ & $Z_2 Z_3$

$\Longrightarrow$ it cannot be detected.

But: Z_i cannot be expressed as a product of the stabilizers $Z_1 Z_2$ & $Z_2 Z_3$ $\Longrightarrow$ logical error!

c) The 3-qubit phase-flip code

Can we correct against Z errors?

$$Z|+\rangle = |-\rangle, \quad Z|-\rangle = |+\rangle$$

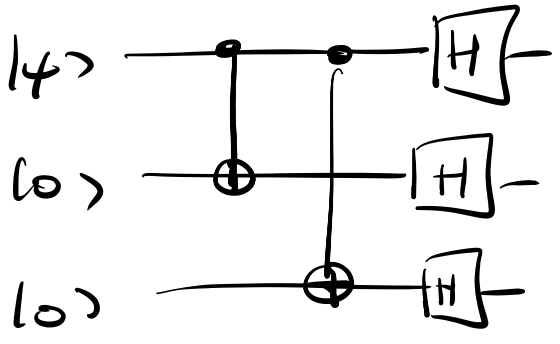
$\Longrightarrow$ Z error $\hat{=}$ bit flip error in $|\pm\rangle$-basis.

Use encoding $\alpha|0\rangle + \beta|1\rangle \longmapsto \alpha|\hat{0}\rangle + \beta|\hat{1}\rangle$,

with $|\hat{0}\rangle := |{+}{+}{+}\rangle$, $|\hat{1}\rangle = |{-}{-}{-}\rangle$:

Will protect against single Z errors!

Encoding:



Syndrome measurement:

$$\tilde{P}_\alpha \stackrel{!}{=} H^{\otimes 3} P_\alpha H^{\otimes 3}$$

(or via stabilizers $X_1 X_2$ & $X_2 X_3$).

Recovery operation:

$$H X_i H = Z_i$$

(anti-com. with stabilizers).

Problem:

Now, there is no protection against bit flip errors X_i

— and X_i acts as a logical Z operator!

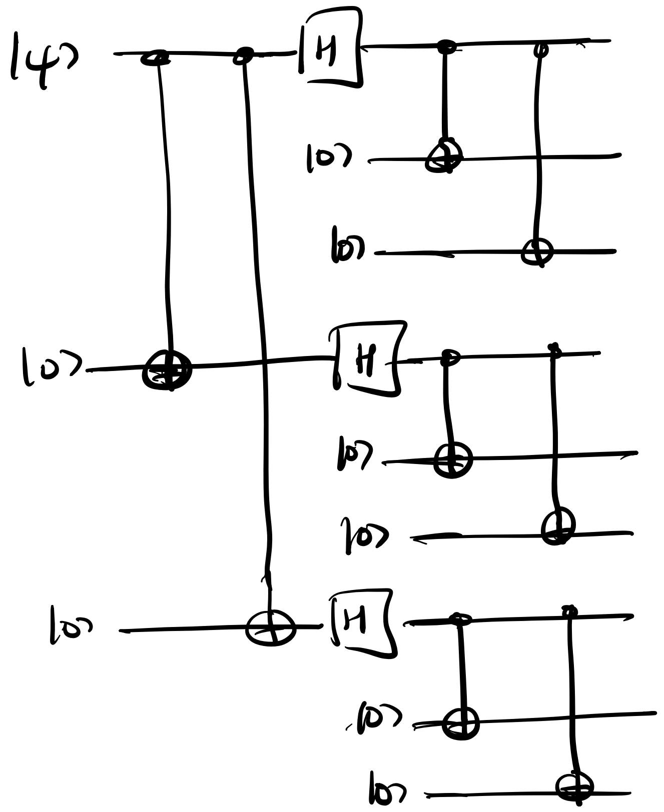
2. The 9-qubit Shor code

Solution: Concatenate (= nest) 3-qubit bit flip code and 3-qubit phase flip code:

$$|0\rangle \longmapsto |+\rangle|+\rangle|+\rangle \longmapsto \frac{(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)}{2\sqrt{2}}$$

$$|1\rangle \longmapsto |-\rangle|-\rangle|-\rangle \longmapsto \frac{(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)}{2\sqrt{2}}$$

Encoding circuit:



$\boxed{\text{9-qubit Shor code}}$

Shor code protects against <u>arbitrary</u> single-qubit errors!

Sufficient to focus on X, Z, and $Y \propto XZ$ errors:

Any general error $E = \alpha I + \sum \beta_i \sigma_i$ will collapse to one of these (if done right).

— More on this later! —

<u>Intuitively</u>:

(i) Errors X_i are corrected on "inner" layer.

(ii) Z_i error =

= <u>logical</u> error on qubit encoded on inner layer

= Z error on outer layer in one position

$\Longrightarrow$ correctable!

(iii) $Y_i \propto X_i Z_i$:

Correct X_i on inner layer.

then as in (ii): only Z error left!

More formally: <u>Stabilizers</u>

Code is +1 eigenstate of

$Z_1 Z_2, \quad Z_2 Z_3$ ← 1st inner layer

$Z_4 Z_5, \quad Z_5 Z_6$

$Z_7 Z_8, \quad Z_8 Z_9$

and of

X on intermediate qubits

$X_{(123)} X_{(456)}$

$\Downarrow \quad \alpha|000\rangle + \beta|111\rangle$

$X_{(456)} X_{(789)}$,

$X_{(123)} = X_1 X_2 X_3$

$\Longrightarrow$

$X_1 X_2 X_3 X_4 X_5 X_6$

$X_4 X_5 X_6 \; X_7 X_8 X_9$

These are 8 commuting operators: Measuring gives 8 bits of information ⟹ 1 qubit untouched!

Analysis of errors:

Bit flip error X_i:

e.g. X_1 anti-comm. w/ $Z_1 Z_2$

or X_2 anti-com. w/ $Z_1 Z_2$ & $Z_2 Z_3$

⇒ meas. of all 6 $Z_k Z_l$ reveals position of X_i

⇒ can be corrected!

Phase flip error Z_i:

E.g.: Z_1: anti-com. w/ $X_1 X_2 X_3 X_4 X_5 X_6$

But: same holds for Z_2 or Z_3!

Yet: Z_1, Z_2, and Z_3 act identically on encoded state $|\hat{\psi}\rangle$ – can be seen by inspection, or since

$$Z_2 |\hat{\psi}\rangle = Z_1 \underbrace{(Z_2 Z_1) |\hat{\psi}\rangle}_{= |\hat{\psi}\rangle \text{ (stabilizer!)}} = Z_1 |\hat{\psi}\rangle!$$

(The 9-qubit code is a degenerate code: different errors have the same syndrome!)

Y errors Y_i:

E.g. $Y_2 \propto Z_2 X_2$

anti-comm. w/ $Z_1 Z_2$

$Z_2 Z_3$

$X_1 X_2 X_3 X_4 X_5 X_6$

$\rightarrow$ correction e.g. via $Z_2 X_2$, or $Z_1 X_2$, ...

All single-qubit errors can be corrected!

What if errors occur on more than one qubit?

Some – but not all! – can be corrected:

e.g. $X_1 X_4$: correctable.

$Z_1 Z_2$: trivial = no error

but: $X_1 X_2$: breaks inner code ↯

$Z_1 Z_4$: breaks outer code ↯

3. The Quantum Error Correction Conditions

Definition: Given $\mathcal{H} = (\mathbb{C}^2)^{\otimes n}$, a Quantum Error Correction Code (QECC) on $\mathcal{H}$ is a subspace $\mathcal{C} \subset \mathcal{H}$ (the code space, with $|\psi\rangle \in \mathcal{C}$ codewords).

We denote by $|\hat{i}\rangle$ an (arbitrary, but fixed) basis of $\mathcal{C}$.

Definition: A noise model on $\mathcal{H}$ is a CP map

$$\mathcal{E}(\rho) = \sum E_\alpha \rho E_\alpha^\dagger \, ; \quad \sum E_\alpha^\dagger E_\alpha \underline{\underline{\le}} I \, , \; !$$

(i.e., error E_α occurs w/ prob. $\operatorname{tr}(E_\alpha^\dagger E_\alpha \rho)$,

e.g. $E_\alpha \propto$ single-qubit Paulis.)

Note: This is only the part of the noise which we want to correct – thus $\sum E_\alpha^\dagger E_\alpha \le I$. The total noise is

$$\mathcal{N}(\rho) = \mathcal{E}(\rho) + \underbrace{\sum N_\gamma \rho N_\gamma^\dagger}_{\longleftarrow \text{ not correctable noise.}} , \quad \sum E_\alpha^\dagger E_\alpha + \sum N_\gamma^\dagger N_\gamma = I \, .$$

Definition: We say that a QECC $\mathcal{C}$ can correct for an error $\mathcal{E}$ if there exists a recovery map $\mathcal{R}$, i.e. a CP map $\mathcal{R}$ such that

$$\mathcal{R}(\mathcal{E}(\rho)) \propto \rho \qquad \forall \rho = |\hat{\psi}\rangle\langle\hat{\psi}|, \ |\hat{\psi}\rangle \in \mathcal{C}$$

Note: $\mathcal{R}$ must correct the error deterministically, i.e., $\mathcal{R}$ must be trace-preserving on states supported on the image of $\mathcal{C}$ under $\mathcal{E}$, i.e., on states obtained by noise from a code state.)

Theorem (Quantum Error Correction Condition):

Given $\mathcal{C}$ and $\mathcal{E}(\cdot) = \sum E_\alpha \cdot E_\alpha^\dagger$, there exists a recovery $\mathcal{R}$ (i.e. $\mathcal{C}$ can correct for $\mathcal{E}$) if and only if

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

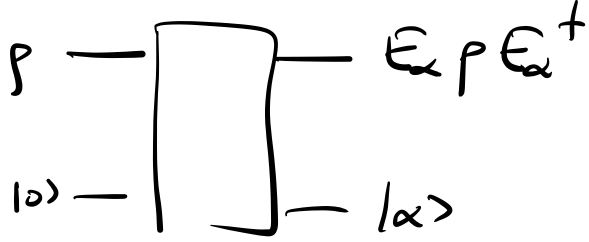
for some ONB $\{|\hat{i}\rangle\}$ $(\langle \hat{i} | \hat{j} \rangle = \delta_{ij})$ of $\mathcal{C}$.

Intuition:

① Orthogonal states remain orthogonal (R cannot make states *more* orthogonal!)

② Environment learns nothing about state:

Stinespring:



$$\mathrm{prob}(\alpha) = \left(\sum \bar{a}_i \langle \hat{i}|\right) E_\alpha^\dagger E_\alpha \left(\sum a_j |\hat{j}\rangle\right)$$

$$= \underbrace{\sum |a_i|^2}_{=1} c_{\alpha\alpha} = c_{\alpha\alpha} \text{ indep. of state.}$$

Proof:

'existence of $R \Longrightarrow \circledast$':

Lemma: $\sum_\tau K_\tau |\psi\rangle\langle\psi| K_\tau^\dagger \propto |\psi\rangle\langle\psi| \quad \forall |\psi\rangle \in \mathcal{C}$

$\Longrightarrow K_\tau |\psi\rangle = a_\tau |\psi\rangle$

with a_τ indep. of $|\psi\rangle$.

Proof: $\sum_\tau K_\tau |\psi\rangle\langle\psi| K_\tau^\dagger \propto |\psi\rangle\langle\psi|$

Choose any $|\chi\rangle$ s.th. $\langle\chi|\psi\rangle = 0$

$$\Rightarrow \sum_\tau \underbrace{\langle\chi|K_\tau|\psi\rangle\langle\psi|K_\tau^\dagger|\chi\rangle}_{\geq 0} \propto \langle\chi|\psi\rangle\langle\psi|\chi\rangle = 0$$

$$\Rightarrow \langle\chi|K_\tau|\psi\rangle = 0 \quad \forall \tau$$

$$\Rightarrow K_\tau|\psi\rangle = a_\tau(|\psi\rangle)\,|\psi\rangle.$$

What if $a_\tau(|\psi\rangle)$ dep. on $|\psi\rangle$? Choose $|\psi_1\rangle, |\psi_2\rangle$ s.th. $a_\tau(|\psi_1\rangle) \neq a_\tau(|\psi_2\rangle)$. Then,

$$K_\tau(|\psi_1\rangle + |\psi_2\rangle) = a_\tau(|\psi_1\rangle)|\psi_1\rangle + a_\tau(|\psi_2\rangle)|\psi_2\rangle$$

$$\not\propto |\psi_1\rangle + |\psi_2\rangle$$ ↯

$$\Rightarrow a_\tau(|\psi\rangle) = a_\tau$$

$$\Rightarrow K_\tau|\psi\rangle = a_\tau|\psi\rangle.$$ ∎

Let $R(\cdot) = \sum R_\gamma \cdot R_\gamma^\dagger$.

Then: $R(\mathcal{E}(|\psi\rangle\langle\psi|)) \propto |\psi\rangle\langle\psi| \quad \forall |\psi\rangle \in \mathcal{C}$

Lemma

$$\Longrightarrow \quad R_\gamma E_\alpha |\psi\rangle = a_{\gamma\alpha} |\psi\rangle \quad \forall |\psi\rangle \in \mathcal{C}$$

ONB $|\hat{i}\rangle, |\hat{j}\rangle$:

$$\Longrightarrow \quad \sum_\gamma \langle \hat{i} | E_\alpha^\dagger R_\gamma^\dagger R_\gamma E_\beta | \hat{j} \rangle = \sum_\gamma \bar{a}_{\gamma\alpha} a_{\gamma\beta} \langle \hat{i} | \hat{j} \rangle$$

$$=: c_{\alpha\beta} \, \delta_{\hat{i}\hat{j}}$$

$$\Longrightarrow \quad \langle \hat{i} | E_\alpha^\dagger \underbrace{\Big(\sum_\gamma R_\gamma^\dagger R_\gamma \Big)}_{= I \text{ on image of } \mathcal{C} \text{ under } \mathcal{E}.} E_\beta | \hat{j} \rangle = c_{\alpha\beta} \, \delta_{ij}$$

$$\Longrightarrow \quad \langle \hat{i} | E_\alpha^\dagger E_\beta | \hat{j} \rangle = c_{\alpha\beta} \, \delta_{ij} \qquad ∎$$

„⊛ ⟹ existence of $\mathcal{R}$":

Construct explicit recovery channel $\mathcal{R}(\cdot) = \sum R_\gamma \cdot R_\gamma^\dagger$.

Step 1: Use gauge degree of freedom in E_α:

$$\mathcal{E}(\rho) = \sum E_\alpha \rho E_\alpha^\dagger = \sum F_\beta \rho F_\beta^\dagger$$

if & only if $F_\beta = \sum_\alpha V_{\beta\alpha} E_\alpha$, V isometry.

Choose V unitary s.th. $\sum_{\alpha\beta} \overline{V_{\varepsilon\alpha}} \, c_{\alpha\beta} \, V_{\tau\beta} = \lambda_\varepsilon \, \delta_{\varepsilon\tau}$ diagonal

$$\circledast \Rightarrow \langle \hat{i} | F_\varepsilon^\dagger F_\tau | \hat{j} \rangle = \sum_{\alpha,\beta} \langle \hat{i} | \overline{V_{\varepsilon\alpha}}\, E_\alpha^\dagger E_\beta V_{\tau\beta} | \hat{j} \rangle$$

$$= \sum_{\alpha,\beta} \overline{V_{\varepsilon\alpha}}\, V_{\tau\beta} \langle \hat{i} | E_\alpha^\dagger E_\beta | \hat{j} \rangle$$

$$= \sum_{\alpha\beta} \overline{V_{\varepsilon\alpha}}\, V_{\tau\beta}\, c_{\alpha\beta}\, \delta_{ij}$$

$$= \lambda_\varepsilon\, \delta_{\varepsilon\tau}\, \delta_{ij}$$

$\Rightarrow$ Different errors F_ε can be distinguished by a projective measurement!

Note that $\sum_\varepsilon \lambda_\varepsilon = \sum_\varepsilon \underbrace{\langle \hat{i} | F_\varepsilon^\dagger F_\varepsilon | \hat{i} \rangle}_{=\lambda_\varepsilon :\ \text{prob. of error } \varepsilon} \leq \langle \hat{i} | I | \hat{i} \rangle = 1.$

Step 2: Measure ε and undo error F_ε.

Want R_γ s.th. $R_\gamma F_\varepsilon | \hat{i} \rangle = \sqrt{\lambda_\varepsilon}\, \delta_{\gamma\varepsilon} | \hat{i} \rangle$!

prob. of error F_ε.

Choose $R_\gamma := \frac{1}{\sqrt{\lambda_\varepsilon}} \sum_j | \hat{j} \rangle\langle \hat{j} | F_\gamma^\dagger$.

If $\lambda_\varepsilon = 0$, then $R_\gamma = 0$ is a solution.

$$\Rightarrow R_\gamma F_\varepsilon | \hat{i} \rangle = \frac{1}{\sqrt{\lambda_\varepsilon}} \sum_j | \hat{j} \rangle \underbrace{\langle \hat{j} | F_\gamma^\dagger F_\varepsilon | \hat{i} \rangle}_{= \lambda_\varepsilon \delta_{\gamma\varepsilon} \delta_{ij}} = \sqrt{\lambda_\varepsilon}\, \delta_{\gamma\varepsilon} | \hat{i} \rangle.$$

$$\Rightarrow R_\gamma F_\varepsilon |\hat{\varphi}\rangle = \sqrt{\lambda_\varepsilon}\, \delta_{\gamma\varepsilon} |\hat{\varphi}\rangle \quad \forall |\hat{\varphi}\rangle \in \mathcal{C}$$

$$\Rightarrow \mathcal{R}(\mathcal{E}(|\hat{\varphi}\rangle\langle\hat{\varphi}|)) = \sum_{\gamma,\varepsilon} R_\gamma F_\varepsilon |\hat{\varphi}\rangle\langle\hat{\varphi}| F_\varepsilon^\dagger R_\gamma^\dagger$$

$$= \sum_\varepsilon \lambda_\varepsilon |\hat{\varphi}\rangle\langle\hat{\varphi}| \propto |\hat{\varphi}\rangle\langle\hat{\varphi}| \quad \forall |\hat{\varphi}\rangle \in \mathcal{C},$$

and $\mathrm{tr}(\mathcal{R}(\mathcal{E}(|\hat{\varphi}\rangle\langle\hat{\varphi}|))) = \sum \lambda_\varepsilon =$

$$= \sum \langle\hat{\varphi}| F_\varepsilon^\dagger F_\varepsilon |\hat{\varphi}\rangle = \mathrm{tr}(\mathcal{E}(|\hat{\varphi}\rangle\langle\hat{\varphi}|)),$$

i.e. $\mathcal{R}$ is trace-preserving on the image of $\mathcal{C}$ under $\mathcal{E}$. ☒

Definition: single-qubit errors correspond to an error model with noise operators of the form

$$E_\alpha = \sum_{k,s} w_{\alpha,k,s}\, \sigma_s^k \leftarrow$$ k'th Pauli matrix on qubit s.

Observation: A QECC can correct for any single-qubit error if it can correct for any single-qubit Pauli error.

Proof: Code can correct for any single Pauli error $\Rightarrow$

$$\langle \hat{i} | \sigma_s^k \sigma_r^l | \hat{j}\rangle = c_{skrl}\, \delta_{ij} \Rightarrow$$

$$\Rightarrow \langle \hat{i} | E_\alpha^\dagger E_\beta | \hat{j}\rangle = \tilde{c}_{\alpha\beta}\, \delta_{ij} \Rightarrow$$ can correct of any single-qubit error. ☒

In particular: A QECC which can correct for single-qubit depolarizing noise

$$\mathcal{E}(\rho) = (1-p)\rho + \frac{p}{3}\left(X\rho X + Y\rho Y + Z\rho Z\right)$$

on any one of k qubits – i.e. a noise

$$\mathcal{E}(\rho) = (1-kp)\,\rho + \sum_{i=1}^{k} \frac{p}{3}\left(X_i\rho X_i + Y_i\rho Y_i + Z_i\rho Z_i\right)$$

is also robust against any single-qubit error!

Corollary: To check for robustness against arbitrary single-qubit errors, it is sufficient to check the error model with

$$\{E_\alpha\} \propto \{I, X_1, X_2, \ldots, Y_1, Y_2, \ldots, Z_1, Z_2, \ldots\}$$

E_α up to prefactors

The analogous result holds for k-qubit errors vs. k-qubit Paulis.

Exercise suggestion: Check q. error correction condition for 3-qubit & 9-qubit code!

4. Basic properties of QECCs

Focus on "*binary codes*":

encode k qubits in $n > k$ qubits

Definition: The *distance* d of a QECC is the smallest number of Paulis $\{P_{i_k} \neq I\}_{k=1}^{d}$ s.th.

$$\langle \hat{i} | F | \hat{j} \rangle \neq \lambda \delta_{ij} \quad \text{for } \underline{\text{some}} \ |\hat{i}\rangle, |\hat{j}\rangle \in \mathcal{C}, \ \langle \hat{i} | \hat{j} \rangle = \delta_{ij}.$$

where $F := P_{i_1} \otimes I \otimes \dots \otimes P_{i_2} \otimes I \otimes \dots \otimes$

(*i.e.*: The smallest # of sites where we have to apply a Pauli to change a code state into another.)

Notation: A binary code encoding k qubits in n qubits with distance d is denoted

$$\boxed{[\![n,k,d]\!]\text{-code}}$$

phys. qubits

logical qubits

distance

How many one-qubit errors can a distance-d code correct for?

Can focus on Pauli errors.

For E_α, E_β with $\leq t$ Paulis each:

$$\langle \hat{i} | \underbrace{E_\alpha^\dagger E_\beta}_{\leq 2t \text{ Paulis}} | \hat{j} \rangle \overset{?}{=} c_{\alpha\beta} \delta_{ij} \quad \forall E_\alpha, E_\beta$$

$$\Longleftrightarrow \quad 2t + 1 \leq d$$

Result: A distance-d code can correct t general single-qubit errors if & only if

$$\boxed{2t + 1 \leq d}$$

E.g. with a $d=3$-code, we can correct any single-qubit error.

If the location of the error is known — that is, we additionally learn that a specific noise channel $\mathcal{E}_{\text{location}}(\cdot) = \sum \tilde{E}_\alpha \rho \tilde{E}_\alpha^\dagger$

has been applied:

$$\langle \hat{i} | \underbrace{\tilde{E}_\alpha^\dagger \tilde{E}_\beta}_{\text{Paulis in same location}} | \hat{j} \rangle$$

$\Rightarrow$ $\tilde{E}_\alpha^\dagger \tilde{E}_\beta$ has $\leq t$ Paulis

$\Rightarrow$ correctable for $\boxed{t+1 \leq d}$

Result: QECC can correct t errors in unknown locations $\Longleftrightarrow$ QECC can correct 2t errors in known locations.

What are constraints on $[n,k,d]$?

Definition: A code is called non-degenerate if different Pauli errors result in orthogonal states, i.e. are distinguishable,

$$\langle \hat{j} | E_\alpha^\dagger E_\beta | \hat{i} \rangle \propto \delta_{\alpha\beta}$$

for all E_α w/ at most t $(2t+1 \leq d)$ Paulis.

Theorem (Hamming bound):

For non-degenerate codes,

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

Proof: via counting possibilities.

E.g.: For $k=1$, $t=1$ $(d=3)$ — i.e. encodes 1 qubit, can correct for one error:

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

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

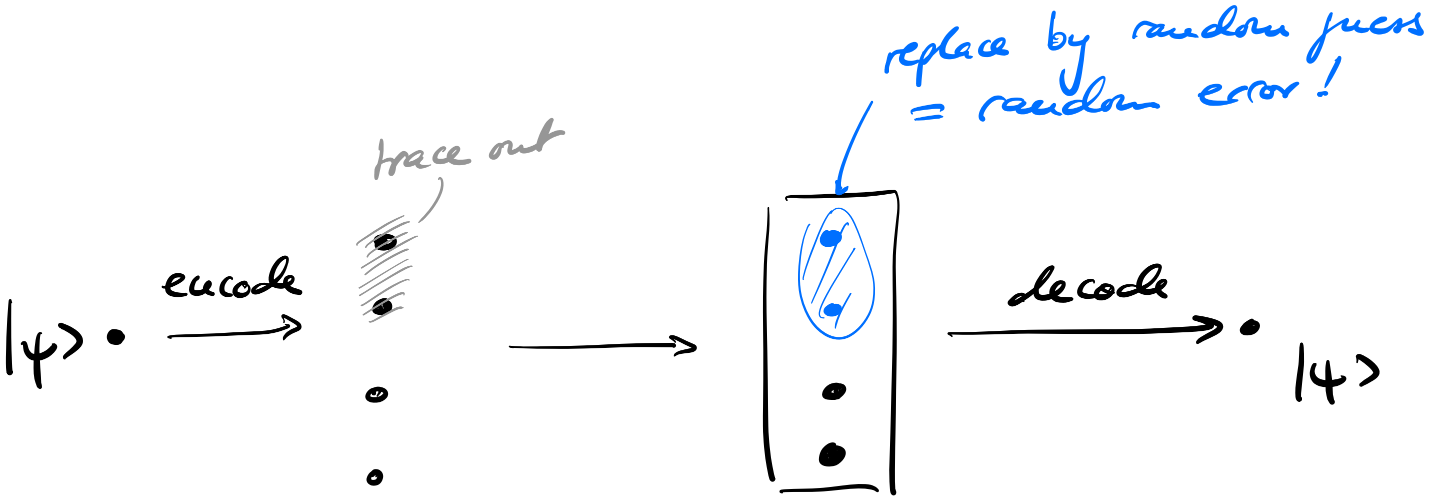
NO!

Proof:

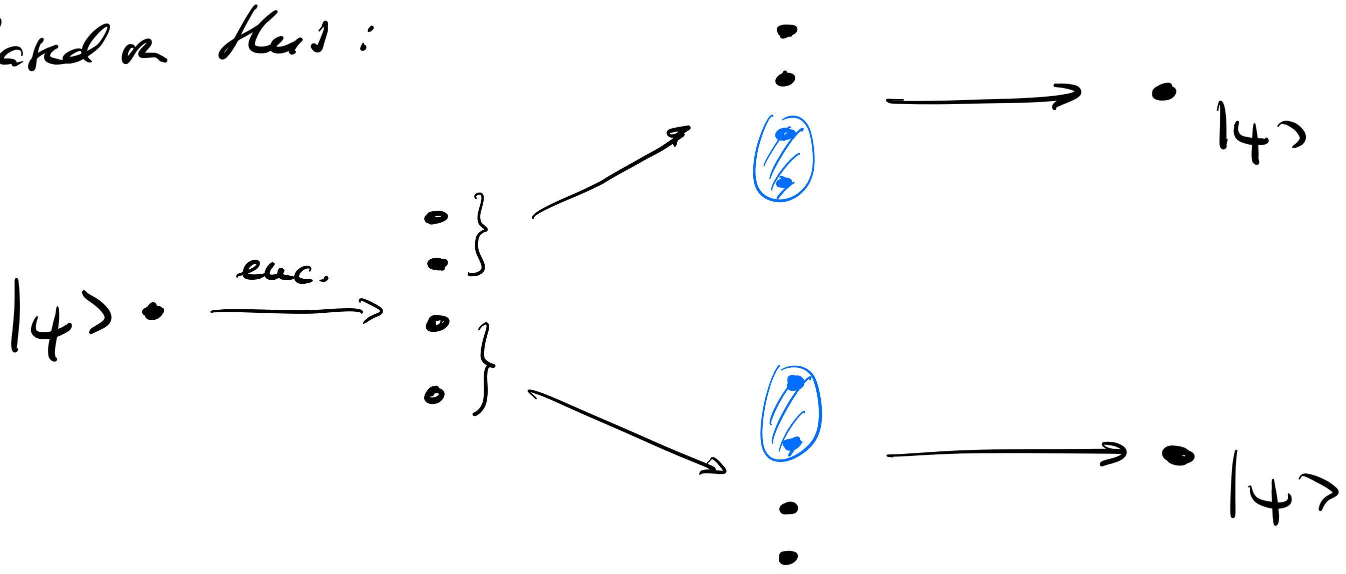
$d=3$: Can correct for unknown 1-qubit error

⇒ can correct for 2 errors on known location

Can use it to recover 2 lost qubits:



Based on this:



↳ have built a quantum cloner!

→ No $[[4,1,3]]$ code can exist,

a $[[5,1,3]]$ code would be optimal!

5. Stabilizer codes

Have seen, e.g. for 3-qubit / 9-qubit code:

code space = joint +1 eigenspace of Paulis

error & correction ⟷ anti-comm. pattern

→ General framework?

a) Definition

Definition: The Pauli group $\mathcal{G} \equiv \mathcal{G}_n$ on n qubits is

$$\mathcal{G} := \{ i^\ell P_1 \otimes \ldots \otimes P_n \mid P_i = I, X, Y, Z ; \ell = 0, \ldots, 3 \}$$

Note: Any two $S_1, S_2 \in \mathcal{G}$ either commute or anti-commute.

Definition (Stabilizer group, stabilizer code)

A subgroup $\mathcal{S} \subset \mathcal{G}$ with $-I \notin \mathcal{S}$ is called a stabilizer group $\mathcal{S}$. Since $-I \notin \mathcal{S} \Rightarrow S_1, S_2 \in \mathcal{S}$ commute (else $S_1 S_2 S_1^{-1} S_2^{-1} = -I$); this also implies $S = \pm \otimes P_i \quad \forall S \in \mathcal{S}$.

The elements $S \in \mathcal{S}$ are called *stabilizers*.

$\mathcal{S}$ defines a subspace $\mathcal{C} \subset (\mathbb{C}^2)^{\otimes n}$,

$$\mathcal{C} := \{ |\psi\rangle \mid |\psi\rangle = S|\psi\rangle \ \forall S \in \mathcal{S} \},$$

the *code space* of a *stabilizer code*.

$\mathcal{S}$ can also be characterized by a minimal set of generators $S_1, \dots, S_r \in \mathcal{S}$.

Lemma: dim $\mathcal{C} = 2^{n-r}$.

Proof: (sketch!)

i) S_1 has same # of ± 1 eigenvalues (as tr $S_1 = 0$)

$\Rightarrow$ split space in half.

$\Pi_1 = \frac{1}{2}(I + S_1)$: proj. on $+1$ eigenspace of S_1.

ii) $\Pi_1 S_2 = S_2 \Pi_1$ (as $S_1 S_2 = S_2 S_1$),

and $\underbrace{\Pi_1 S_2 \Pi_1} = \frac{1}{2}(I + S_1) S_2$

± 1 - eigensp. of S_2 on $+1$ - eigenspace of S_1

(0 on -1 - eigensp. of S_1)

$$\mathrm{tr}\left(\tfrac{1}{2}(I+S_1)S_2\right) = \tfrac{1}{2}\Big(\underbrace{\mathrm{tr}(S_1)}_{=0} + \underbrace{\mathrm{tr}(S_1S_2)}_{=0\text{: indep. set of gen-s}}\Big)$$

$$= 0$$

$\Rightarrow$ S_2 has eq. # of $+1/-1$ eigenvals

on $+1$ - eigenspace of S_1

$\Rightarrow$ split again in half.

iii) continue inductively! ☒

b) Error correction conditions for stabilizer codes

What about error corr. conditions?

E_α Pauli errors.

$E_\alpha^\dagger E_\beta$ have three possibilities:

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

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

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

$$\Rightarrow \quad \langle \hat{i} | E_\alpha^{+} E_\beta | \hat{j} \rangle = 0$$

$\Rightarrow$ QECC satisfied $\Rightarrow$ error correctable!

ii) $E_\alpha^{+} E_\beta \in \mathcal{S}$:

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

$\Rightarrow$ QECC satisfied $\Rightarrow$ error correctable!

iii) $E_\alpha^{+} E_\beta$ comm. with all $S \in \mathcal{S}$,

but $E_\alpha^{+} E_\beta \notin \mathcal{S}$:

$\Rightarrow$ $E_\alpha^{+} E_\beta$ acts non-trivially on code space:

it is a logical operator

In particular: $E_\alpha^{+} E_\beta \, \mathcal{C} \subset \mathcal{C}$, but

$\exists |\hat{j}\rangle$ s.th. $E_\alpha^{+} E_\beta |\hat{j}\rangle \neq c \cdot |\hat{j}\rangle$

(else $E_\alpha^{+} E_\beta \in \mathcal{S}$)

$\Rightarrow \langle \hat{i} | E_\alpha^\dagger E_\beta | \hat{j} \rangle \neq 0$ for some $i \neq j$.

$\Rightarrow$ not correctable! ↯ (as QEC cond. violated)

(Diff. intuition: Cannot tell w/ certainty if after error state is $E_\alpha |\hat{i}\rangle$ or $E_\beta |\hat{j}\rangle$, and – unlike (ii) – it does matter which of them occurred $\Rightarrow$ not correctable!)

How does the error correction work?

Correctable error model w/ errors $\{E_a\}$,

E_α = product of Paulis.

Assume some error E_β (unknown!) occurred.

$$|\hat{\psi}\rangle \xmapsto{\text{error}} E_\beta |\hat{\psi}\rangle$$

Let $\sigma_i = \pm 1$ denote the commutator of S_i and E_β,

$$S_i E_\beta = E_\beta S_i \sigma_i \quad (\text{as } S_i|\hat{\psi}\rangle = |\hat{\psi}\rangle).$$

Step 1: Measure all S_i, $i = 1, \dots, r$. Using the (anti)commutation, we find that the result is deterministically σ_i: $S_i E_\beta |\hat{\psi}\rangle = \sigma_i E_\beta S_i |\hat{\psi}\rangle = \sigma_i E_\beta |\hat{\psi}\rangle$

(measurement can be done using CNOTs & single-qubit rotations.)

Step 2: Pick some E_γ from $\{E_\alpha\}$ with same commutation properties, $S_i E_\gamma = \sigma_i E_\gamma S_i$.

Step 3: Apply $E_\gamma^\dagger$ as a correction:

$$E_\beta|\hat{\psi}\rangle \xrightarrow{\text{corr.}} E_\gamma^\dagger E_\beta|\hat{\psi}\rangle.$$

Since $S_i E_\gamma^\dagger E_\beta = E_\gamma^\dagger E_\beta S_i$, we have (from (ii)) that

$E_\gamma^\dagger E_\beta|\hat{\psi}\rangle = |\hat{\psi}\rangle$ ⟹ error corrected.

Note: If case (iii) exists, the correction could induce a logical error!

Key question: Given a stabilizer code, what is the shortest $E_\alpha^\dagger E_\beta$ (= Pauli product) of that type (here, "short" refers to # of non-trivial Paulis)

(→ distance of code!)

c) Example: 3-qubit code

$$\mathcal{C} = \text{span}\{|000\rangle, |111\rangle\}$$

$$\left.\begin{aligned} S_1 &= ZZI \\ S_2 &= ZIZ \end{aligned}\right\} \Longrightarrow \mathcal{S} = \{III, ZZI, ZIZ, \overset{S_1S_2}{\overset{\shortparallel}{IZZ}}\}$$

$k = \underset{n}{\underset{\shortparallel}{3}} - \underset{r}{\underset{\shortparallel}{2}} = 1 \Rightarrow$ 1 encoded qubit

<u>Single-qubit X errors:</u>

$E_\alpha = III, IIX, IXI, XII$ (up to prefactor $\sqrt{p_a}$)

$E_\alpha^\dagger E_\beta = III, IIX, IXI, XII,$

XXI, XIX, IXX

$\Rightarrow$ anti-commu. w/ S_1, S_2, both S_1 & S_2,

or an element of $\mathcal{S}$ (for III).

$\Rightarrow$ correctable!

<u>Single-qubit Z errors:</u>

$E_\alpha = III, IIZ, IZI, ZII$

$E_\alpha^\dagger E_\beta = ZII$ is one possibility

<u>But:</u> ZII commu. w/ S_1, S_2, but $\underline{ZII \notin \mathcal{S}}$!

$\Rightarrow$ <u>Z errors not correctable!</u>

Logical operators:

(at the same time: uncorrectable $E_\alpha^\dagger E_\beta$!)

$\hat{\cdot}$ ≡ logical Z operator

- $\hat{Z} = \underbrace{ZII}_{\text{distance 1 ↯}}$

  - or any $\hat{Z}' = \hat{Z} \cdot S$, $S \in \mathcal{S}$, e.g. IZI, ZZZ, ...

- $\hat{X} = XXX$

  - or e.g. $\hat{X}' = XXX \cdot ZZI = -YYX$, etc ...

Note: $\hat{X}\hat{Z} = -\hat{Z}\hat{X}$ — and this is all we have to require from the logical Pauli operators!

Error detection and correction:

X error E_α can be detected by anti-comm. pattern.

e.g.: • XII anti-comm. w/ ZIZ, ZZI $\in \mathcal{S}$.

• can be measured: $ZZI|\psi\rangle \overset{?}{=} \pm|\psi\rangle$ etc.

⇒ allows to detect error (up to a T s.th.

$TS = ST$ $\forall S \in \mathcal{S}$, and thus $T \in \mathcal{S}$ for correctable errors).

d) More examples:

3-qubit phase flip code:

$$S_1 = XXI$$

$$S_2 = IXX$$

$$\hat{X} = XII$$

$$\hat{Z} = ZZZ$$

9-qubit Shor code:

$$\left.\begin{aligned}
S_1 &= ZZI\ III\ III\\
S_2 &= IZZ\ III\ III\\
S_3 &= III\ ZZI\ III\\
S_4 &= III\ IZZ\ III\\
S_5 &= III\ III\ ZZI\\
S_6 &= III\ III\ IZZ\\
S_7 &= XXX\ XXX\ III\\
S_8 &= III\ \underbrace{XXX}\ \underbrace{XXX}
\end{aligned}\right\} \begin{array}{c}\text{8 indep. stabilizers}\\ \| \\ \text{1 encoded qubit}\end{array}$$

logical X of 3-qubit code!

Logical operators:

e.g.:

$\hat{Z} = ZZZ\ ZZZ\ ZZZ$

$\hat{X} = XXX\ XXX\ XXX$

— these comm. w/ S_i, as those have even # of X/Z, but are $\notin S$, since they have odd # of X/Z.

simpler ("shorter") logical ops:

e.g. $\hat{Z} = ZII\ ZII\ ZII$

$\hat{X} = XXX\ III\ III$

($\Rightarrow$ distance 3!)

Also means that $\hat{X}$ and $\hat{Z}$ can be measured by measuring only 3 qubits!
(**But**: Meas. a general function of $\hat{X}$ & $\hat{Z}$ requires at least 5 qubits because of no-cloning argument!)

Note: 9-qubit code is degenerate:

$E_1 = ZIIIIIIII$ and

$E_2 = IZIIIIIII$

have same syndrome, since

$E_1 E_2 = ZZIIIIIII \in S$.

e) The 5-qubit code

Consider the stabilizer code on 5 qubits w/ generators

$$\left.\begin{aligned} S_1 &= XZZXI \\ S_2 &= IXZZX \\ S_3 &= XIXZZ \\ S_4 &= ZXIXZ \end{aligned}\right\}$$

encodes $5-4=1$ qubit

cyclic code: $S_1, \dots, S_5$ are cyclic permutations.

$\Rightarrow$ cyclic codewords!

$(S_5 = ZZXIX = S_1 S_2 S_3 S_4)$

Corrects any 1-qubit error:

$E_\alpha^\dagger E_\beta$ = product of ≤ 2 Paulis

⟹ anti-comm. w/ at least one S_i, $i=1,\dots,5$

(Why? Fix pos. of 1st Pauli; pick S_k which has I there. Then, 2nd Pauli must agree with that on S_k; and conversely. But: can check that those choices won't commute w/ some other S_i.)

⟹ correctable ⟹ $d \geq 3$.

(And $d \leq 3$ from no-cloning: $[[5,1,3]]$-QECC!)

Error syndromes ($1 \equiv$ anti-comm. = eigenval. -1)

	X error on qubit					Z error on					Y error on				
	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
S_1	0	1	1	0	0	1	0	0	1	0	1	1	1	1	0
S_2	0	0	1	1	0	0	1	0	0	1	0	1	1	1	1
S_3	0	0	0	1	1	1	0	1	0	0	1	0	1	1	1
S_4	1	0	0	0	1	0	1	0	1	0	1	1	0	1	1
S_5	1	1	0	0	0	0	0	1	0	1	1	1	1	0	1

15 errors, 15 syndromes ⟹ non-degenerate.

All possible $2^4 - 1 = 15$ syndromes appear.

Logical operators:

$$\left.\begin{aligned} \hat{Z} &= ZZZZZ \\ \hat{X} &= XXXXX \end{aligned}\right\}$$ comm. w/ all S_i (even # of X & Z in S_i), but for same reason $\notin S$!

simpler choices:

e.g. $\hat{Z}' = \hat{Z} \cdot S_3 = -YZYII$

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

$\Longrightarrow$ distance $d = 3$

& logical info in $\hat{Z}$ or $\hat{X}$ basis can be obtained by meas. only 3 qubits!

(Note: General feature of distance-d code!)

Syndrome meas. + correction can be done using only CNOT, H, X (for corr.), and ancillas.

(Again: gen. feature of stabilizer code: need to compute parity of X & Z eigenvalues.)