V.3 Quantum Error Correction Conditions

Quantum Error Correcting Code (QECC):

Defined by code space C (elements: "codewords").
Choose basis $|\hat{i}\rangle$.

Noise model: CPTP map

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

Recovery procedure: Measurement + recovery
$\leftrightarrow$ another CP map $\mathcal{R}$.

Require that $\mathcal{R}(\mathcal{E}(\rho)) = \rho$ for all $\rho = |\psi\rangle\langle\psi|, |\psi\rangle \in C$

Under which conditions on C & $\mathcal{E}$ does such an $\mathcal{R}$ exist?

Necessary conditions:

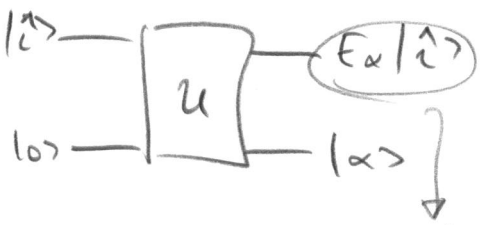
(i) Environment carries no information about ρ

for any $\rho = \sum \rho^{ij} |\hat{i}\rangle\langle\hat{j}|$ in C:

Linearity $\Rightarrow$ $\underbrace{\langle \hat{i} | E_\alpha^\dagger E_\alpha | \hat{j} \rangle}_{= \text{prob}(\alpha)} = c_\alpha$ (indep. of i)

.. recall:

$|\hat{i}\rangle\langle\hat{i}| \mapsto \mathcal{E}(|\hat{i}\rangle\langle\hat{i}|) \iff$



Ch. II: Stinespring dilation!

output for env. state $|\alpha\rangle$.

(ii) orthogonal states must remain orthogonal ($\mathcal{R}$ cannot make states more orthogonal!)

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

↑ orth. support!

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

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

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

(i) + (ii) $\Rightarrow$

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

Quantum Error Correction Condition

This is also sufficient:

Use gauge deg. of freedom:

$$\sum E_\alpha \rho E_\alpha^\dagger = \sum F_\beta \rho F_\beta^\dagger \quad \text{w/} \quad F_\beta = \sum V_{\beta\alpha} E_\alpha$$

(V: isometry)

to choose F_β s.t. $c_{\alpha\beta}$ becomes diagonal,

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

i.e.: Different α can be distinguished by measurement and undone:

$$\left(\frac{1}{\lambda_\beta} \sum_{\hat{i}} |\hat{i}\rangle\langle\hat{i}| F_\beta^\dagger \right) F_\alpha |\hat{j}\rangle = \delta_{\alpha\beta} |\hat{j}\rangle$$

$$= \lambda_\alpha \delta_{\alpha\beta} \delta_{ij}$$

Kraus op. of recovery map

Note: For a single-qubit error,

$$E_\alpha = \sum_{k,s} \omega_{\alpha,k,s} \, \sigma_s^k$$

(σ^k: Pauli on qubit s)

i.e: $\langle \hat{i} | (\sigma_k^s)^\dagger \sigma_\ell^r | \hat{j} \rangle \propto \delta_{ij} \Rightarrow \langle \hat{i} | E_\alpha^\dagger E_\beta | \hat{j} \rangle \propto \delta_{ij}$.

i.e.: Err. Corr. Cond. for Paulis ⇒ err. corr. cond. for any single-qubit error!

In particular: Robust to depolarizing channel

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

on every qubit ⇒ robust to any 1-qubit error

... and similar for k-qubit errors & k-fold Pauli products!

Basic properties of QECC:

Focus: "binary codes": encode k qubits in $n > k$ qubits.

"Distance" d: Smallest # of Paulis ($\neq I$) in $E_\alpha = P \otimes I \otimes \ldots \otimes P \otimes \ldots$ s.th.

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

Notation: $[\![n, k, d]\!]$ – code

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

How many 1-qubit errors t can a distance d code correct?

For E_α, E_β with $\leq t$ Paulis:

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

i.e.: For $d=3$, we can correct all 1-qubit errors.

Note: If location of errors is known, $E_\alpha^\dagger E_\beta$ has $\leq t$ Paulis

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

Or: Code can correct t errors in unknown locations

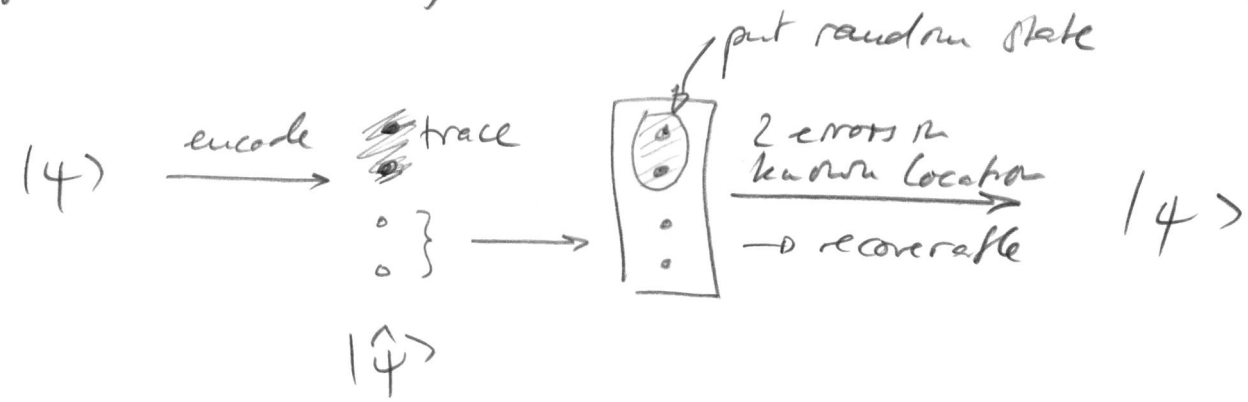
$\iff$ t can correct $2t$ errors in known locations

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

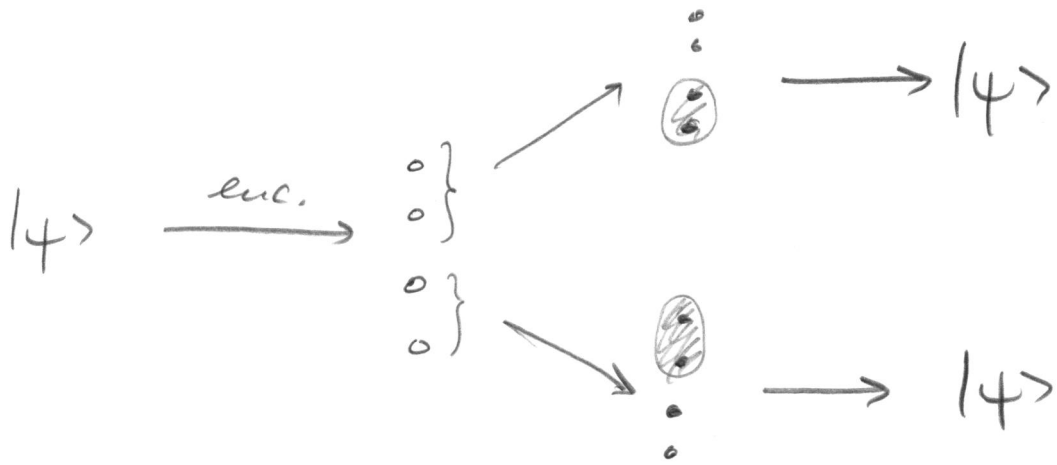
Simplest case: $k=1$, $d=3$. What is minimal n?

Claim: $n \geq 5$!

Proof via no-cloning:



So...



↯ violates no-cloning!

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

Will see: it exists!

V.4 Stabilizer codes

Consider the Pauli group on n qubits

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

Two elements $S_1, S_2 \in \mathcal{G}$ either commute or anticommute.

Let $S_1, \dots, S_r \in \mathcal{G}$ be a lin. indep. set of commuting S_i (i.e., no S_i is a product of other S_j)

Then, $S_1, \dots, S_r$ generate a subgroup

$$\mathcal{S} = \langle S_1, \dots, S_r \rangle, \text{ the } \underline{\text{stabilizer group}} \text{ of } \mathcal{S}.$$

$\mathcal{S}$ defines subspace C:

$$|\psi\rangle \in C :\Leftrightarrow |\psi\rangle = S|\psi\rangle \quad \forall S \in \mathcal{S}.$$

C forms the code space of a stabilizer code.
$S \in \mathcal{S}$ are called stabilizers.

(Techn. pt: This req. $-I \notin \mathcal{S}$, or $S_i = \pm \otimes P_i$).

We have $\dim C = 2^{n-r}$ – each lin. indep. stabilizer removes half the space!

What about err. corr. conditions?

Pauli errors $\Rightarrow E_\alpha^\dagger E_\beta$ Pauli product.

3 possibilities:

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

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

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

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

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

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

Cases (i) & (ii): error correctable!

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

$\Rightarrow E_\alpha^\dagger E_\beta$ acts non-trivially on code space:

it is a logical operator.

$\Rightarrow$ not correctable.

Q: What is shortest $E_\alpha^\dagger E_\beta$ of that type?

Example: 3-qubit code.

$C = \mathrm{span}\{|000\rangle, |111\rangle\}$.

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

qubits must be pairwise equal

$\rightarrow \alpha|000\rangle + \beta|111\rangle$

$k = 3 - 2 = 1$

$\Rightarrow$ 1 encoded qubit

Single-qubit X errors:

$$\mathcal{E}_\alpha = III, IIX, IXI, XII$$

$$\mathcal{E}_\alpha^\dagger \mathcal{E}_\beta = \underline{III}, \underline{IIX}, \underline{IXI}, \underline{XII}, IXX, XIX, XXI$$

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

$\Rightarrow$ correctable!

Single-qubit Z errors:

$\mathcal{E}_\alpha^\dagger \mathcal{E}_\beta = ZII$ possible.

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

$\Rightarrow$ 2 errors not correctable!

Logical operators (or uncorrectable errors...)

- $\hat{Z} = \underbrace{ZII}_{\text{distance 1}}$ (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. $\hat{X}' = XXX \cdot ZZI = YYX, \ldots$

Error detection / correction:

X error E_X can be identified by anti-com. pattern:

e.g.: XII anticom. w/ $ZZI, ZIZ \in \mathcal{S}$.

$\Rightarrow$ allows to (i) correct error

(ii) even: uniquely identify error ("non-degenerate" code).

More examples:

3-qubit phase flip code:

$$S_1 = XXI$$

$$S_2 = IXX$$

$$\hat{X} = XII$$

$$\hat{Z} = ZZZ$$

9-qubit Shor code

3-qubit 1:
$S_1 = ZZI\ III\ III$
$S_2 = IZZ\ III\ III$

3-qubit 2:
$S_3 = III\ ZZI\ III$
$S_4 = III\ IZZ\ III$

3-qubit 3:
$S_5 = III\ III\ ZZI$
$S_6 = III\ III\ IZZ$

$S_7 = XXX\ XXX\ III$
$S_8 = III\ XXX\ XXX$

8 stabilizers = 1 encoded qubit!

$XXX\ XXX\ XXX$ ↑ logical X on 3-qubit code.

Logical operators: e.g.

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

} odd # of Z/X: cannot be in S!

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

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

$\hat{X}$ and $\hat{Z}$ can be measured by meas. only 3 qubits.

(Note: meas. a general function of $\hat{X}$ & $\hat{Y}$ must require at least 5 qubits: no cloning argument!)

$\Rightarrow \hat{X}, \hat{Z}$ shortest possible $\Rightarrow d = 3$ code!

(Note: Degenerate code: $\overbrace{ZII\ III\ III}^{=:S_1}$ and $\overbrace{IZI\ III\ III}^{=:S_2}$

have same syndrome, since $S_1 S_2 = ZZI\ III\ III \in \mathcal{S}$.)

The 5-qubit-code:

$$\left.\begin{aligned} S_1 &= X Z Z X I \\ S_2 &= I X Z Z X \\ S_3 &= X I X Z Z \\ S_4 &= Z X I X Z \end{aligned}\right\}$$

Encodes $5-4 = 1$ qubit

Cyclic code: $S_1, \dots, S_5$ are cyclic permutations: cyclic codewords!

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

Corrects any 1-qubit error:

$E_\alpha^+ E_\beta$ = prod. of 2 Paulis:

$\Rightarrow$ anti-commut. w/ at least one S_i!

(E.g.: each col. has one $I \Rightarrow$ that S_i fixed other Pauli error $\Rightarrow$ both Paulis fixed by 2 $S_i \Rightarrow \not\in$)

$\Rightarrow$ Distance $d \geq 3$ (and $d \leq 3$ from no-cloning)

$\Rightarrow$ $[\![5,1,3]\!]$ QECC!

Non-degen. code, and: $\underbrace{5+5+5}_{X,Y,Z \text{ on each qubit}} = 15$ errors,

and $S_i = \pm 1 \Rightarrow 2^4 - \underset{\uparrow}{1} = 15$ syndromes!
triv.

1-to-1 relation!

Logical operators:

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

Note: Syndrome meas. + correction can be done using only CNOT, H, X, & ancillas!

General note: There is a general framework to work w/ stabilizers by using arithmetics mod 2.

(Matrices w/ $1 = Z$ or $1 = X$, e.g. for 5-qubit code:

$$\begin{array}{c} S_1 \\ S_2 \\ S_3 \\ S_4 \end{array} \left(\begin{array}{ccccc|ccccc} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{array} \right)$$

X operators Z operators.