

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.t.

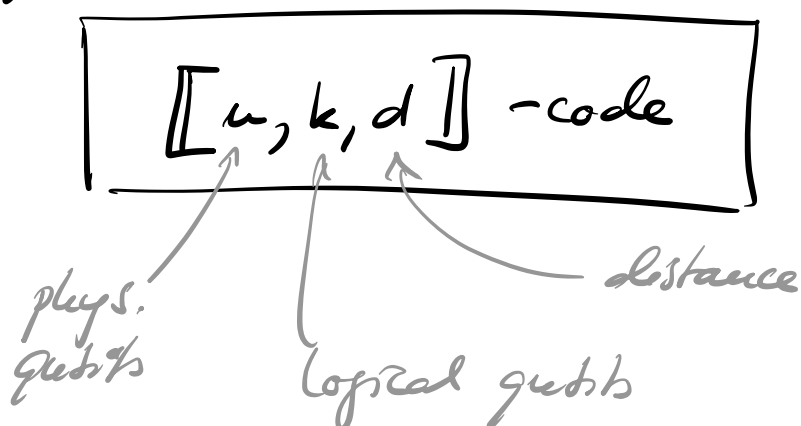
$$\langle \hat{i} | F | \hat{j} \rangle \neq \lambda \delta_{ij} \quad \text{for some } |\hat{i}\rangle, |\hat{j}\rangle \in \mathcal{C},$$

$$\langle \hat{i} | \hat{j} \rangle = \delta_{ij}.$$

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

(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



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

Can focus on Pauli errors.

For E_α, E_β with $\leq t$ Pauli's each:

$$\langle \hat{i} | \underbrace{E_\alpha^\dagger E_\beta}_{\leq 2t \text{ Pauli's}} | \hat{j} \rangle \stackrel{?}{=} c_{\alpha\beta} \delta_{ij} \quad \forall E_\alpha, E_\beta$$

$$\iff 2t + 1 \leq d$$

Result; A distance- d code can correct t multiple one-qubit errors if & only if

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

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

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

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

Paulis in same location

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

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

Result: QECC can correct t errors in

unknown locations $\Leftrightarrow$ 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,

$$\langle \hat{j} | E_a^\dagger E_b | \hat{i} \rangle \propto \delta_{ab}$$

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

Theorem (Hamming bound):

For non-degenerate codes,

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

Proof: na 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? Chapter V, pg 31

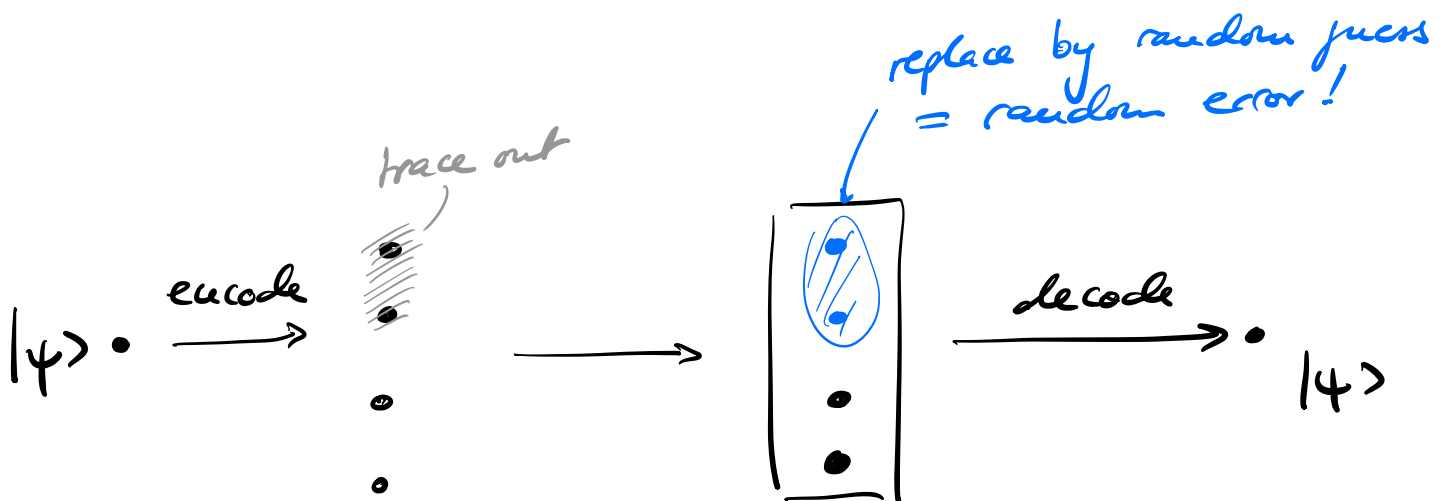
NO!

Proof:

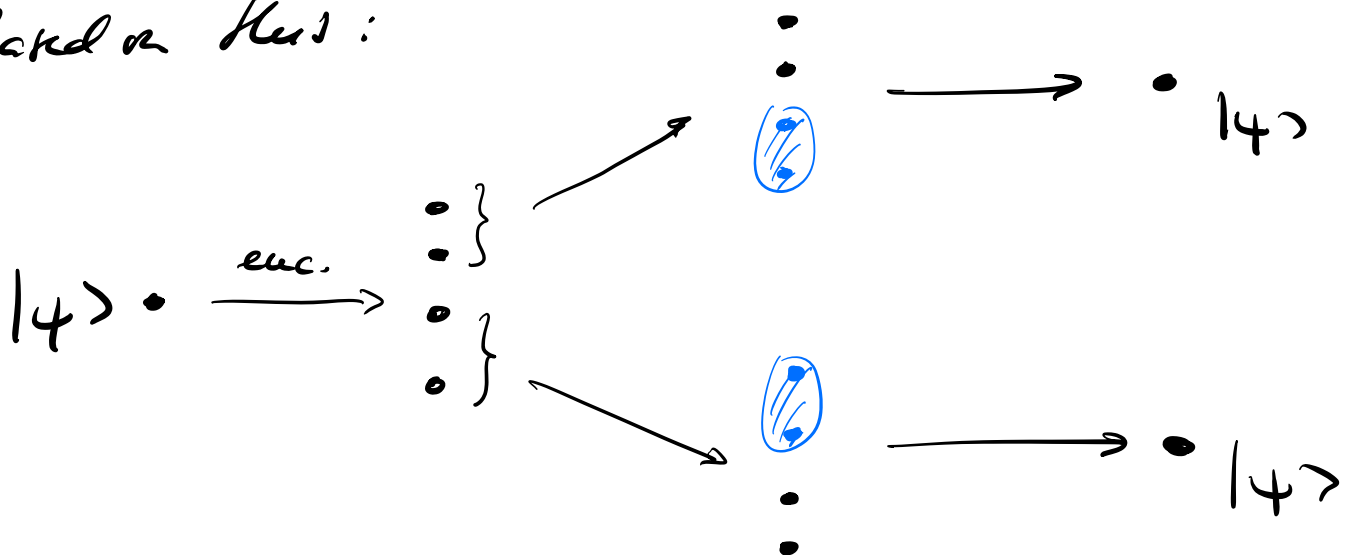
$d=3$: Can correct for unknown 1-qubit error

$\Rightarrow$ can correct for 2 errors in known location

Can use it to recover 2 lost qubits:



Back on this:



↳ have built a quantum clone!

→ No $[[4, 1, 3]]$ code can exist,
a $[[5, 1, 3]]$ code would be optimal!