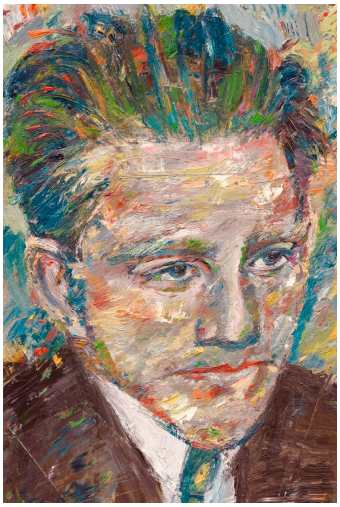
Norbert Schuch

QUANTUM ERROR CORRECTION

Wintersemester 2024

Transcribed and Typeset by
Maximilian Fettinger



University of Vienna

1 Introduction

1.1 Setting and Problem

- Coupling to **environment** induces **errors**
- Classical computer: Information stored in *macroscopic* properties → errors unlikely
- Quantum computers:
  - need qubits = *single* quantum systems, and must store general superpositions, 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).

Question: Can we protect quantum information from noise?

Classical Error Correction

Copy information (*encoding*), e.g encode 1 bit in 3 bits:

$$0 \mapsto \hat{0} := 000$$
$$1 \mapsto \hat{1} := 111$$

Error Model: Bit flip with some (small) probability p (independently for all bits) $\Longrightarrow$ typically 0 or 1 bits flipped.

Error correction (*decoding*) by majority vote:

$$000, 001, 010, 100 \mapsto 000$$
$$111, 110, 101, 011 \mapsto 111$$

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

$$p_{\text{error}} = \Pr(\geq 2 \text{ flips}) = p^3 + 3p^2(1-p)$$
$$= 3p^2 - 2p^3 < p \quad \text{for } p < \frac{1}{2}$$

Error quadratically suppressed → effective error probability **decreased**.

Can be improved by:

- using more bits: $0 \mapsto 00\ldots0, 1 \mapsto 11\ldots1$
- 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!

1.2 The 3-qubit bit flip code

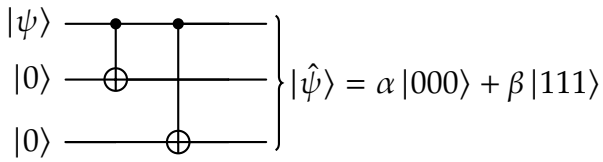
Copy qubits in computational basis:

$$|0\rangle \mapsto |\hat{0}\rangle = |000\rangle$$
$$|1\rangle \mapsto |\hat{1}\rangle = |111\rangle$$

i.e., the encoding is a linear map

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

Possible **encoding circuit**:



Now consider **bit flip error** on qubit i:

$$|\hat{\psi}\rangle \overset{\text{error}}{\longmapsto} X_i\,|\hat{\psi}\rangle$$

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

Problem: Measuring the qubits in computational basis reveals i, but also **destroys superposition!**

$\Longrightarrow$ Need a measurement which **only** returns information about **position** i **of error** – independently 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 gets flipped*****:**	$P_1 = \|100\rangle\langle 100\| + \|011\rangle\langle 011\|$
2 = ***2nd qubit gets flipped*****:**	$P_2 = \|010\rangle\langle 010\| + \|101\rangle\langle 101\|$
3 = ***3rd qubit gets flipped*****:**	$P_3 = \|001\rangle\langle 001\| + \|110\rangle\langle 110\|$

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

The outcome is called the *error syndrome*.

Measurement of $\{P_\alpha\}$ reveals only **2 bits of information** $\Longrightarrow$ one qubit of information **untouched**!

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

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

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

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

$\Longrightarrow$ Bit flip **corrected**!

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

$\Longrightarrow$ suppression of error $p \to 3p^2 - 2p^3$, 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.

$$|\hat{\psi}\rangle \mapsto e^{i\vartheta X_1}|\hat{\psi}\rangle = (\cos\vartheta I + i\sin\vartheta X_1)|\hat{\psi}\rangle?$$

$$|\hat{\psi}\rangle = \alpha|000\rangle + \beta|111\rangle \xmapsto[\text{e.g. } X_3]{\text{error}} \alpha(\cos\vartheta|000\rangle + i\sin\vartheta|001\rangle) + \beta(\cos\vartheta|111\rangle + i\sin\vartheta|110\rangle)$$
$$= \cos\vartheta \underbrace{(\alpha|000\rangle + \beta|111\rangle)}_{\text{syndrome } P_0} + i\sin\vartheta \underbrace{(\alpha|001\rangle + \beta|110\rangle)}_{\text{syndrome } P_3}$$

Syndrome measurement collapses state into:

Prob.: $|\cos\vartheta|^2$:
result P_0, post-measurement state $\alpha|000\rangle + \beta|111\rangle$, $0 \equiv$ no correction: ✓

Prob.: $|\sin\vartheta|^2$:
result P_3, post-measurement state $\alpha|001\rangle + \beta|110\rangle$, $3 \equiv$ correction: flip bit 3:
$\Rightarrow \alpha|000\rangle + \beta|111\rangle$: ✓

Measurement of error syndrome P_α collapses **continuous error** into one of the 4 **discrete errors**:

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

We have focused on X errors, but what about **Z errors**?

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

This is still a state in the **code space** (i.e. a valid encoded state $|\hat{\psi}\rangle$)

$\Longrightarrow$ error **not detectable**, but it **has changed** $|\hat{\psi}\rangle$. After decoding, the error acts as

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

i.e. as a **logical Z operation** (*logical operator* = operation on encoded qubit).

$\Longrightarrow$ 3-qubit bit flip code **cannot protect against** single ***phase flip error*** Z_i.

1.3 The 3-qubit phase flip code

Can we correct against Z errors?

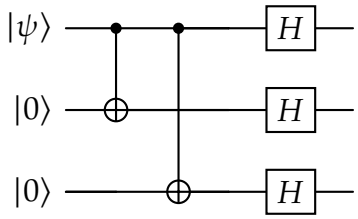
$$Z|+\rangle = |-\rangle\,,\; Z|-\rangle = |+\rangle$$

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

Use encoding $\alpha|0\rangle + \beta|1\rangle \mapsto \alpha|\hat{0}\rangle + \beta|\hat{1}\rangle$, with $|\hat{0}\rangle := |+++\rangle$, $|\hat{1}\rangle := |---\rangle$:

Will protect against single Z errors!

Encoding:



Syndrome measurement:

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

Recovery operation:

$$HX_iH = Z_i$$

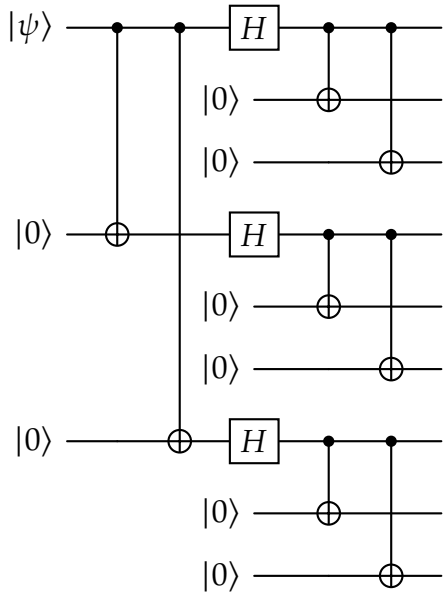
Problem: Now there is no protection against bit flip errors X_i – and X_i acts as a logical Z operator!

2 The 9-qubit Shor code

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

$$|0\rangle \mapsto |+\rangle|+\rangle|+\rangle \mapsto \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}}$$
$$|1\rangle \mapsto |-\rangle|-\rangle|-\rangle \mapsto \frac{(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}}$$

Encoding circuit:



Shor code protects against **arbitrary** single qubit errors! Sufficient to focus on X, Z, and $Y \propto XZ$ errors:

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

— More on this later! —

Intuitively:

(i) Errors X_i are corrected on *inner code* layer.

(ii) Z_i error =
= **logical** error on qubit encoded in 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!

What if errors occur on **more than one qubit**?

Some – but not all! – can be corrected, e.g.

$$X_1 X_4 : \text{ correctable}$$
$$Z_1 Z_2 : \text{ trivial = no error}$$

but:

$$X_1X_2: \text{ breaks inner code } \lightning$$
$$Z_1Z_4: \text{ breaks outer code } \lightning$$

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 $C \subset \mathcal{H}$ (the **code space**, with $|\psi\rangle \in C$ **codewords**). We denote by $|\hat{i}\rangle$ an (arbitrary, but fixed) basis of C.

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

$$\mathcal{E}(\rho) = \sum E_\alpha \rho E_\alpha^\dagger; \quad \sum E_\alpha^\dagger E_\alpha \leq I$$

(i.e., error E_α occurs with probability $\mathrm{tr}(E_\alpha E_\alpha^\dagger \rho)$, e.g. $E_\alpha \propto$ single-qubit Paulis.)

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

$$\mathcal{N}(\rho) = \mathcal{E}(\rho) + \underbrace{\sum N_\gamma \rho N_\gamma^\dagger}_{\text{non correctable noise}}, \quad \sum E_\alpha E_\alpha^\dagger + \sum N_\gamma^\dagger N_\gamma = I.$$

Definition. We say that a QECC 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

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

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

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

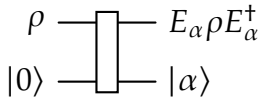
$$\langle\hat{i}|E_\alpha^\dagger E_\beta|\hat{j}\rangle = c_{\alpha\beta}\delta_{ij} \qquad (*)$$

Intuition

1. Orthogonal states remain orthogonal ($\mathcal{R}$ cannot make states *more* orthogonal!)

2. Environment learns nothing about the state:

Stinespring:



$$\begin{aligned}\Pr(\alpha) &= \left(\sum \overline{a_i}\,\langle \hat{\imath}|\right) E_\alpha^\dagger E_\alpha \left(\sum a_j\,|\hat{\jmath}\rangle\right) \\ &= \underbrace{\sum |a_i|^2\, c_{\alpha\alpha}}_{=1} = c_{\alpha\alpha} \quad \text{(independent of state)}\end{aligned}$$

Lemma. *If $\sum_\tau K_\tau |\psi\rangle\langle\psi| K_\tau^\dagger \propto |\psi\rangle\langle\psi|$ for all $|\psi\rangle \in C$, then $K_\tau |\psi\rangle = a_\tau |\psi\rangle$, with a_τ independent of $|\psi\rangle$.*

Proof. **Existence of $\mathcal{R} \Rightarrow (*)$:**

Let $\mathcal{R}(\cdot) = \sum R_\gamma \cdot R_\gamma^\dagger$. Then :

$$\begin{aligned}&\mathcal{R}(\mathcal{E}(|\psi\rangle\langle\psi|)) \propto |\psi\rangle\langle\psi| \quad \forall |\psi\rangle \in C \\ &\xrightarrow{\text{Lemma}} R_\gamma E_\alpha |\psi\rangle = a_{\gamma\alpha}|\psi\rangle \quad \forall |\psi\rangle \in C \\ &\xrightarrow{\text{ONB } |\hat{\imath}\rangle, |\hat{\jmath}\rangle} \sum_\gamma \langle \hat{\imath}|E_\alpha^\dagger R_\gamma^\dagger R_\gamma E_\beta|\hat{\jmath}\rangle = \sum_\gamma \overline{a_{\gamma\alpha}} a_{\gamma\beta}\langle \hat{\imath}|\hat{\jmath}\rangle =: c_{\alpha\beta}\delta_{ij} \\ &\Longrightarrow \langle \hat{\imath}|E_\alpha^\dagger \Big(\underbrace{\sum_\gamma R_\gamma^\dagger R_\gamma}_{=I \text{ on image of } C \text{ under } \mathcal{E}}\Big) E_\beta|\hat{\jmath}\rangle = c_{\alpha\beta}\delta_{ij} \\ &\Longrightarrow \langle \hat{\imath}|E_\alpha^\dagger E_\beta|\hat{\jmath}\rangle = c_{\alpha\beta}\delta_{ij}\end{aligned}$$

□

$(*) \Rightarrow$ 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:

$$\begin{aligned}\mathcal{E}(\rho) &= \sum E_\alpha \rho E_\alpha^\dagger = \sum F_\beta \rho F_\beta^\dagger \\ &\Leftrightarrow F_\beta = \sum_\alpha V_{\beta\alpha} E_\alpha \quad \text{with } V \text{ isometry.}\end{aligned}$$

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

$$\begin{aligned}
\overset{(*)}{\Longrightarrow} \langle \hat{\imath} | F_\varepsilon^\dagger F_\tau | \hat{\jmath} \rangle &= \sum_{\alpha,\beta} \langle \hat{\imath} | \overline{V_{\varepsilon\alpha}} E_\alpha^\dagger E_\beta V_{\tau\beta} | \hat{\jmath} \rangle \\
&= \sum_{\alpha,\beta} \overline{V_{\varepsilon\alpha}} V_{\tau\beta} \langle \hat{\imath} | E_\alpha^\dagger E_\beta | \hat{\jmath} \rangle \\
&= \sum_{\alpha,\beta} \overline{V_{\varepsilon\alpha}} V_{\tau\beta} c_{\alpha\beta} \delta_{ij} = \lambda_\varepsilon \delta_{\varepsilon\tau} \delta_{ij}
\end{aligned}$$

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

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

Step 2: Measure ε and undo error F_ε

Want R_γ s.t. $R_\gamma F_\varepsilon |\hat{\imath}\rangle = \underbrace{\sqrt{\lambda_\varepsilon}}_{\text{prob. of error } F_\varepsilon} \delta_{\gamma\varepsilon} |\hat{\imath}\rangle$!

Choose $R_\gamma := \underbrace{\frac{1}{\sqrt{\lambda_\varepsilon}}}_{\text{If } \lambda_\varepsilon=0\text{, then } R_\gamma=0 \text{ is a solution.}} \sum_j |\hat{\jmath}\rangle \langle \hat{\jmath}| F_\gamma^\dagger$.

$$\Longrightarrow R_\gamma F_\varepsilon |\hat{\imath}\rangle = \frac{1}{\sqrt{\lambda_\varepsilon}} \sum_j |\hat{\jmath}\rangle \underbrace{\langle \hat{\jmath}| F_\gamma^\dagger F_\varepsilon |\hat{\imath}\rangle}_{=\lambda_\varepsilon \delta_{\gamma\varepsilon} \delta_{ij}} = \sqrt{\lambda_\varepsilon} \delta_{\gamma\epsilon} |\hat{\imath}\rangle .$$

$$\Longrightarrow R_\gamma F_\varepsilon |\hat{\psi}\rangle = \sqrt{\lambda_\varepsilon} \delta_{\gamma\epsilon} |\hat{\psi}\rangle \quad \forall |\hat{\psi}\rangle \in C$$

$$\begin{aligned}
\Longrightarrow \mathcal{R}(\mathcal{E}(|\hat{\psi}\rangle \langle \hat{\psi}|)) &= \sum_{\gamma,\varepsilon} R_\gamma F_\varepsilon |\hat{\psi}\rangle \langle \hat{\psi}| F_\varepsilon^\dagger R_\gamma^\dagger \\
&= \sum_\varepsilon \lambda_\varepsilon |\hat{\psi}\rangle \langle \hat{\psi}| \propto |\hat{\psi}\rangle \langle \hat{\psi}| \quad \forall |\hat{\psi}\rangle \in C
\end{aligned}$$

and

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

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

Definition. Single-qubit errors correspond to an error model with noise operators of the form

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

with σ_s^k meaning the 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

$$\implies \langle \hat{i} | \sigma_s^k \sigma_r^l | \hat{j} \rangle = c_{skrl} \delta_{ij} \implies$$
$$\implies \langle \hat{i} | E_\alpha^\dagger E_\beta | \hat{j} \rangle = \tilde{c}_{\alpha\beta} \delta_{ij} \implies \text{can correct for any single-qubit error}$$

□

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

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

on any one of k qubits – i.e. a noise

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

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*

$$\{E_\alpha\} \underbrace{\propto}_{\substack{E_\alpha \text{ up to projectors}}} I, X_1, X_2, \ldots, Y_1, Y_2, \ldots, Z_1, Z_2, \ldots$$

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

4 Base properties of QECCs

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

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

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

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

(I.e.: The smallest number of qubits 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 as

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

with n denoting the physical qubits, k the logical qubits and d the 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:

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

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

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

$$2t + 1 \leq d$$

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:

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

$$\implies \tilde{E}_\alpha + \tilde{E}_\beta \text{ has } \leq t \text{ Paulis}$$

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

Result: QECC can correct **t errors** in **unknown locations** if and only if QECC can correct **2t errors** in **known locations**.

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

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

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

for all E_α with 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. Via counting possibilities. □

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

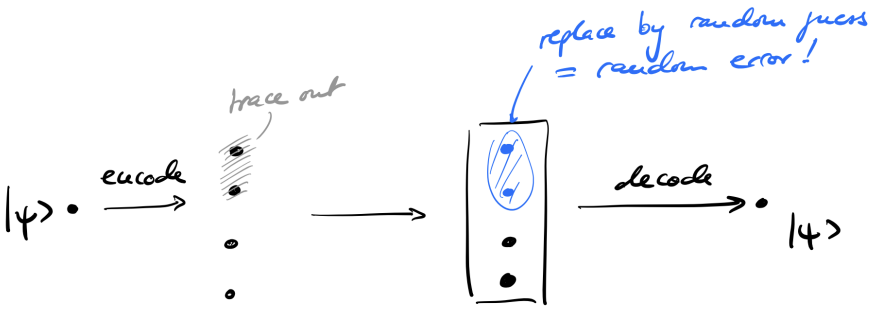
$$n \geq 5$$

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

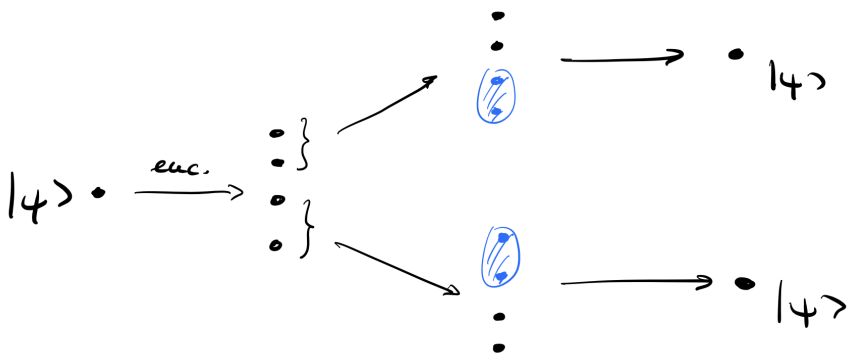
NO!

Proof. $d = 3$: Can correct for unknown 1-qubit error $\Longrightarrow$ can correct for **2 errors** in **known locations**

Can use it to recover 2 lost qubits:



Based on that:



↯ **have built a quantum cloner!**

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