V. Quantum error correction

1) Introduction

- Coupling to environment → errors
- Class. systems: macroscopic → errors unlikely
- Quantum comp: - need single qubits (= quantum syste)
  → fragile!
  - need coupling to realize gates!

Can we protect q. information from noise?

Classical error correction:

copy information.

e.g.: assume indep. bit flip errors w. prob. p.

encode 1 bit in 3:

$0 \longrightarrow \hat{0} = 000$

$1 \longrightarrow \hat{1} = 111$

Correction: majority vote:

$000, 001, 010, 100 \xrightarrow{\text{Correct to}} 000$

$111, 110, 101, 011 \longrightarrow 111$

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

for $p < 1/2$!

$\Rightarrow$ effective error prob decreased!

To obtain better robustness:

- concatenate codes
- use more bits
- use smarter codes

Quantum error correction:

Several problems:

- cannot clone qubits (and if we could, we couldn't compare them!)
- different types of errors exist, e.g. X (bit flip) and Z (phase flip)
- errors can be continuous
- measuring qubits destroys quantum info

a) The 3-qubit bit flip code

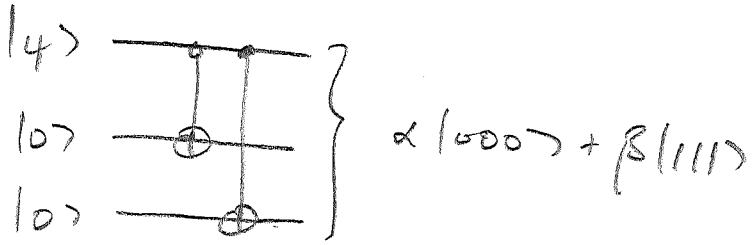
Try to copy a fixed (computat.) basis:

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

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

i.e.: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \xrightarrow{\text{encoding}} \alpha|000\rangle + \beta|111\rangle$

Encoding circuit:



Consider bit flip error $|\psi\rangle \longmapsto X|\psi\rangle$.

Want: Correction procedure which can correct one bit flip error.

But: Meas. all qubits would destroy quantum info!

⟹ Need to measure only info about error (i.e., which bit has been flipped)!

POVM elements ("syndrome measurement")

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

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

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

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

→ only 2 bits of information acquired!
(namely the error syndrome)

E.g. consider

$$\alpha|000\rangle + \beta|111\rangle \xrightarrow[\text{qubit 1}]{\text{bit flip on}} \alpha|100\rangle + \beta|011\rangle.$$

⇒ meas. result P_1, post-meas. state

$$\alpha|100\rangle + \beta|011\rangle$$

⇒ recovery operation: flip qubit 1: $X_1 \longrightarrow \alpha|000\rangle + \beta|111\rangle$.

Note: Since this works for any state, it also works for parts of an entangled state (already!)

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

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

What about arbitrary (continuous) errors, e.g.

$$|\phi\rangle \longmapsto e^{i\vartheta X}|\phi\rangle = (\cos\vartheta\,\mathbb{1} + i\sin\vartheta X)|\phi\rangle ?$$

$$\alpha|000\rangle + \beta|111\rangle \xrightarrow{\text{error}} \cos\theta\,(\alpha|000\rangle + \beta|111\rangle) + i\sin\theta\,(\alpha|100\rangle + \beta|011\rangle)$$

<u>syndrome meas.</u>: collapse onto:

$p = \cos^2\vartheta$: $P_0 \Rightarrow \alpha|000\rangle + \beta|111\rangle$: no corr. necessary ✓

$p = \sin^2\vartheta$: $P_1 \longrightarrow \alpha|100\rangle + \beta|011\rangle \xrightarrow[X_1]{\text{correction}}$ ✓

<u>Meas. of error syndrome P_i</u>: <u>collapses error</u> onto no error or bit flip error:

Cont. error is mapped to <u>discrete error</u> ("digital error").

Different perspective on syndrome meas. + correction:

$|000\rangle, |111\rangle$: $+1$-eigenstates of Z_1Z_2 & Z_2Z_3. ("stabilizer")

Measure Z_1Z_2 & Z_2Z_3 (i.e., compare $1 \leftrightarrow 2$ & $2 \leftrightarrow 3$):

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

$(-1, +1)$: error on qubit 1

$(+1, -1)$: ——— 3

$(-1, -1)$: ——— 2

More formally:

X_1 anti-com. w $Z_1 Z_2$:

$|\psi\rangle = \alpha|000\rangle + \beta|111\rangle$, $Z_1 Z_2 |\psi\rangle = |\psi\rangle$:

$$\langle\psi| X Z_1 Z_2 X |\psi\rangle = -\langle\psi| Z_1 Z_2 |\psi\rangle = -1.$$

$\Rightarrow (-1)$: error anti-comm. w/ $Z_1 Z_2$ occurred.

Correction operation $\leftrightarrow$ satisfies same anti-comm. relations!

... more on this later!

6) 3-qubit phase flip code

What about Z errors?

$$\alpha|000\rangle + \beta|111\rangle \xrightarrow[\text{one qubit}]{\text{Z error on}} \alpha|000\rangle - \beta|111\rangle.$$

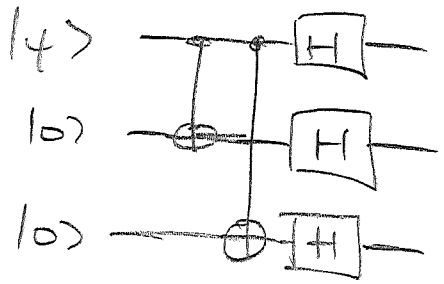
$\rightarrow$ still in code space (i.e., valid state) $\Rightarrow$ error not detectable!

(cf: error comm. w. $Z_1 Z_2$ & $Z_2 Z_3$)

Recall: $Z|+\rangle = |-\rangle$; $Z|-\rangle = |+\rangle$

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

Encoding $|\hat{0}\rangle = |+++\rangle$, $|\hat{1}\rangle = |---\rangle$ and protect against 2 error!



Syndrome measurements: $H^{\otimes 3} P_k H^{\otimes 3}$, or via stabilizers X_1X_2 and X_2X_3.

Recovery: $HX_i H = Z_i$ (anti-com. w. stabilizers).

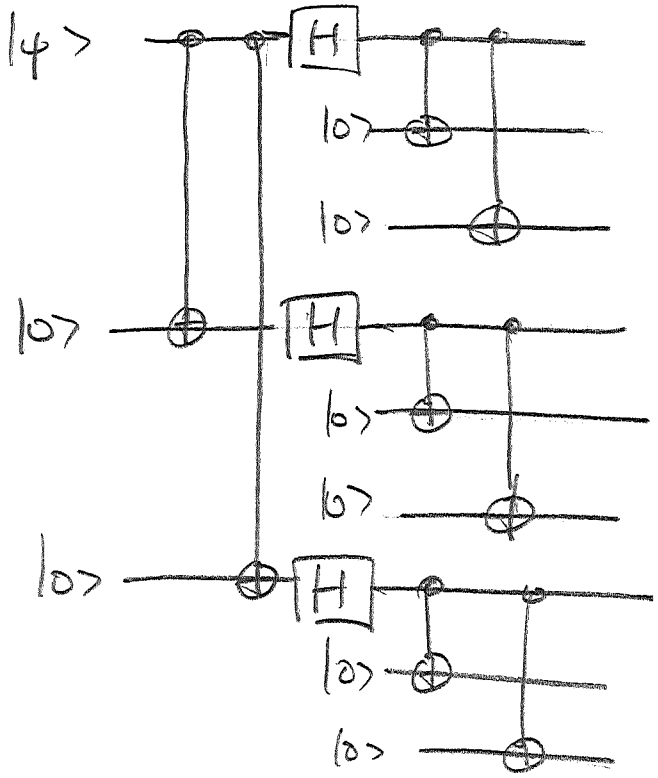
Problem: Now no protection against bit flip (X) errors!

2. The 9-qubit Shor code

Solution: Concatenate 3-qubit bit flip w/ 3-qubit phase flip code!

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

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



9-qubit Shor code

Shor code protects against arbitrary single-qubit errors.

Focus on X, Z, and $XZ \hat{=} Y$ errors (all err. collapse to these)

Syndrome meas. + correction:

Bit-flip (X error):

meas. $Z_1 Z_2$, $Z_2 Z_3$

$Z_4 Z_5$, $Z_5 Z_6$

$Z_7 Z_8$, $Z_8 Z_9$

E.g.: Bit flip X_1 : $\langle Z_1 Z_2 \rangle = -1$, rest $= +1$

(also follows from comm. relations).

Correction: Apply corresp. X_i (anti-com. w/ all stabilizers S w/ $\langle S \rangle = -1$).

Single phase flip (Z error):

phase flip: $|000\rangle \pm |111\rangle \longleftrightarrow |000\rangle \mp |111\rangle$.

$\Rightarrow$ syndrome = compare phase of adjacent encoded blocks,

"$X_{123} X_{456}$" and "$X_{456} X_{789}$":

Stabilizers are

$X_1 X_2 X_3 X_4 X_5 X_6$

$X_4 X_5 X_6 X_7 X_8 X_9$

(Note: These act as "$X_{123} X_{456}$" & "$X_{456} X_{789}$" on the encoded qubits.)

$\Rightarrow$ corrected by any anti-comm. operation!

E.g.: Z error on 4: $|000\rangle + |111\rangle \longleftrightarrow |000\rangle - |111\rangle$

$\left.\begin{array}{l} \langle X_1 X_2 X_3 X_4 X_5 X_6 \rangle = -1 \\ \langle X_4 X_5 X_6 X_7 X_8 X_9 \rangle = -1 \end{array}\right\}$ Z error on 4, 5, or 6

Correction: Z_4, Z_5, Z_6, or $Z_4 Z_5 Z_6$.

Note: All X & Z stabilizers commute;

- 9 qubits, 8 indep. stabilizers $\Rightarrow$ fix 2-dim qubit space!
- can be measured simultaneously
- correction must anti-com. w/ all stabilizers w/ $\langle S \rangle = -1$, and commute w/ all w/ $\langle S \rangle = 1$.

9-qubit code also protects against Y errors:

E.g.: $Y_2 \propto Z_2 X_2$

Anti-com. w/ $X_1 X_2 X_3 X_4 X_5 X_6$

——— " ——— $Z_1 Z_2$ & $Z_2 Z_3$

$\Rightarrow$ Correction $Z_2 X_2$, or $Z_1 Z_2 Z_3 X_2$.

$\Rightarrow$ error fully corrected (up to global phase).

In fact: protection against arb. errors

$$e^{i\theta \vec{n}\cdot\vec{\sigma}} = \cos\theta\, \mathbb{1} + i \sin\theta\, \vec{n}\cdot\vec{\sigma}$$

$\Rightarrow$ syndrome meas. projects onto (anti-)comm. error, i.e., Pauli error X, Y, or Z.

What if errors occur on <u>more than one qubit</u>?

Some – but not all – errors are corrected:

<u>E.g.:</u> $X_1 X_4$: correctable.

$Z_1 Z_2$: trivial (no error)

<u>But:</u> $X_1 X_2$: breaks code ↯

$Z_1 Z_4$: breaks code ↯

⇒ <u>Concatenate codes</u> or <u>use better codes.</u>

3. Quantum error correction conditions & properties of Quantum Error Correcting Codes (QECC)

<u>QECC:</u> Defined by <u>code space C</u> (containing <u>codewords</u>); choose basis $|\bar{i}\rangle$.

<u>Noise model:</u> CPTP map

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

(<u>i.e.:</u> error E_α w/ prob. $\mathrm{tr}(E_\alpha^\dagger E_\alpha \rho)$; e.g. $E_\alpha \propto$ Paulis.)

Want: Recovery procedure: Measurement + correction

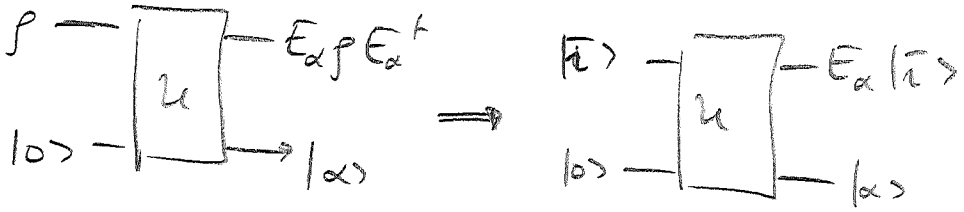
$\longleftrightarrow$ CP map $\mathcal{R}(\rho) = \sum_k R_k \rho R_k^\dagger$.

Require that $\mathcal{R}(\mathcal{E}(\rho)) = \rho$ for all $\rho \in C$.

Under which conditions on C & $\mathcal{E}$ does this hold, i.e., we can correct $\mathcal{E}$?

Intuition:

$\rho \mapsto \mathcal{E}(\rho)$ $\longleftrightarrow$ Chapter I: Stinespring dilation



Necessary condition for error correction:

(i) environment carries no information about ρ for any ρ in the codespace (!)

$\Rightarrow$ $\underbrace{\langle \tilde{i} | E_\alpha^\dagger E_\alpha | \tilde{i} \rangle}_{\text{prob. for } \alpha.} = C_\alpha$

(ii) orthogonal states must remain orthogonal (otherwise we cannot undo error):

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

↑ supported on $\perp$ space!

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

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

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

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

Quantum Error Correction Condition

Sufficiency: Construct explicit recovery operation $\mathcal{R} = \sum R_\beta \cdot R_\beta^\dagger$

Step 1: Use gauge degree of freedom in $\mathcal{E}$:

$$\sum E_{\alpha\beta} E_\alpha^\dagger = \sum F_\gamma \rho F_\gamma^\dagger \quad \text{if } F_\gamma = \sum_\alpha V_{\gamma\alpha} E_\alpha, \; V \text{ isometry}$$

Choose V s.t. $V_{\alpha\varepsilon}^* c_{\alpha\beta} V_{\beta\gamma} = \lambda_\varepsilon \delta_{\varepsilon\gamma}$: diagonal

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

I.e.: Different α can be distinguished by measurement!

Step 2: Measure α & undo error F_α.

Want R_β s.th. $R_\beta F_\alpha |\bar{\imath}\rangle = \delta_{\alpha\beta} |\bar{\imath}\rangle$

Choose $R_\beta = \frac{1}{\lambda_\beta} \sum_j |\bar{\jmath}\rangle\langle\bar{\jmath}| F_\beta^\dagger$

$$\Rightarrow R_\beta F_\alpha |\bar{\imath}\rangle = \frac{1}{\lambda_\beta} \sum_j |\bar{\jmath}\rangle \underbrace{\langle\bar{\jmath}| F_\beta^\dagger F_\alpha |\bar{\imath}\rangle}_{\lambda_\alpha \delta_{ij}\delta_{\alpha\beta}} = \delta_{\alpha\beta} |\bar{\imath}\rangle .$$

$$\Rightarrow \mathcal{R}(\mathcal{E}(\rho)) = \sum R_\beta F_\alpha \rho F_\alpha^\dagger R_\beta^\dagger = \rho \quad \forall \rho \in \mathcal{C}.$$

Note: For any single-qubit error E_α, we have

$$E_\alpha = \sum_{k,p} w_{\alpha k p}\, \sigma_{k,p}$$

($\sigma_{k,p}$: Pauli Gates on site p)

I.e.: $\langle\bar{\jmath}| \sigma_{kp}^\dagger \sigma_{qi} |\bar{\imath}\rangle \propto \delta_{ij} \Rightarrow \langle\bar{\jmath}| E_\beta^\dagger E_\alpha |\bar{\imath}\rangle \propto \delta_{ij}$

I.e.: Err. Corr. Cond. holds for Paulis $\Rightarrow$ err. corr.

Conds hold for any single-qubit error!

(In part.: Robust to depol. channel $\mathcal{E}(\rho) = p\rho + \frac{(1-p)}{3}[X_\rho X + Y_\rho Y + Z_\rho Z]$
$\Rightarrow$ robust to any channel!)

Examples: 3qubit, 9qubit code $\longrightarrow$ Homework!

Properties of QECC:

We focus on *binary codes*: Encode k qubits into $n > k$ qubits.

Distance d: Smallest # of Paulis ($\neq I$) in E_α s.th.

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

(E.g.: 9-qubit code: Distance $d=3$, e.g. $E_\alpha = Z_1 Z_4 Z_7$.
Note: $E_\alpha = Z_1 Z_2$ maps $|\bar{i}\rangle$ to ~~itself~~!)

Notation: $[\![n, k, d]\!]$ code

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

How many single-qubit errors, t, can a distance d code correct? E_α, E_β: $\leq t$ Paulis $\Longrightarrow$

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

Note: If we know the location of the t errors, then

$E_\beta^\dagger E_\alpha$ has t Paulis $\Rightarrow$ $\underline{t+1 \leq d}$.

$\Rightarrow$ C can correct t errors in arbitrary locations $\Rightarrow$ t can correct $2t$ errors in known locations.

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

> Def.: A code is called non-degenerate if different Pauli errors lead to different states, $\langle \bar{j} | E_\beta^\dagger E_\alpha | \bar{i} \rangle \propto \delta_{\alpha\beta}$.
>
> E.g. the 9-qubit code is degenerate, since $Z_1, Z_2 Z_1, Z_3$ have same syndrome.

Hamming bound: For non-deg. codes,

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

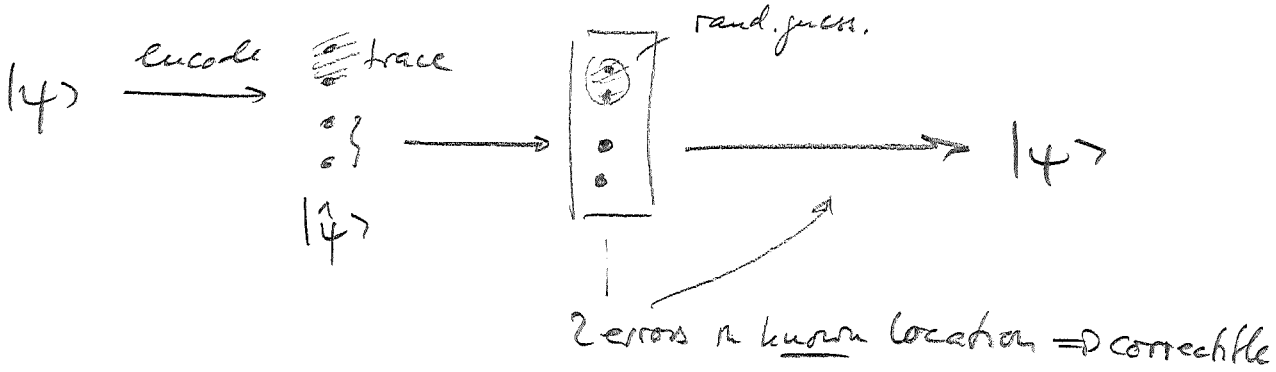
(Proof via counting $\Rightarrow$ Homework)

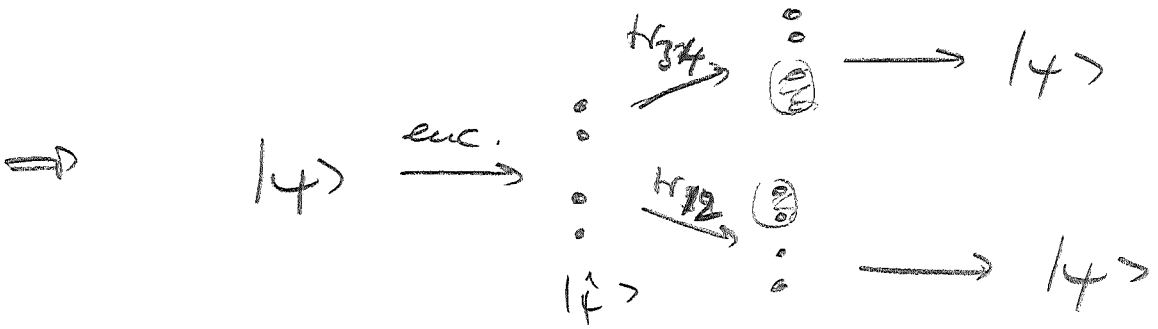
For $k=1$, $t=1$ $(d=3)$ – encode 1 qubit, correct 1 error:

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

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

No:





↯ violates no-cloning!

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

4. Classical codes

$[n,k,d]$ code: encode k bits in n bits, distance d.

Consider linear codes:

$\underline{a} = (a_1, \dots, a_k) \in \{0,1\}^k$ encoded in

$\underline{v}(\underline{a}) = \sum_i a_i \underline{v}_i$; $\underline{v}_i \in \{0,1\}^n$ (all mod 2!)

Define <u>generator matrix</u> $G = \begin{pmatrix} \underline{v}_1 \\ \vdots \\ \underline{v}_k \end{pmatrix}$; $k \times n$ matrix.

<u>Encoding</u>: $\underline{a} \longmapsto \underline{v}(\underline{a}) = \underline{a} G$

Alternative characterization:

<u>Parity check matrix</u> H: $(n-k) \times n$ matrix.

equiv. defs.
- rows of $H \perp$ rows of G
- $H \underline{v}^T = 0 \quad \forall \underline{v} \in C$
- $\ker H = \operatorname{im} G^T$

<u>Errors</u>: Bit flips, given by $\underline{e} = \{0,1\}^n$:

$$\underline{v} \longrightarrow \underline{v} + \underline{e}$$

<u>Detect error with H</u>: $\underline{v} \in$ code:

$$H(\underline{v}+\underline{e})^T = \underbrace{H \underline{v}^T}_{=0} + H \underline{e}^T = \underbrace{H \underline{e}^T}$$

<u>syndrome</u> of $\underline{e}$.

Set of possible errors:

Recovery possible iff all e_i have different syndromes,

i.e.: $H \underline{e}_i^T = H \underline{e}_j^T \Rightarrow \underline{e}_i = \underline{e}_j$.

Distance d of code $\Leftrightarrow$ $\underline{v}(\tilde{a})$ with smallest Hamming weight $|\underline{v}(\tilde{a})|$ ($=$ # of 1's).

(Equiv.: $\underline{e}$ w/ smallest Ham. wght. s.th. $\underline{v}+\underline{e}=\underline{w}$, $\underline{v},\underline{w}\in C$)

We have:

$$\underline{e}_1+\underline{e}_2=\underline{v}(\tilde{a}) \Leftrightarrow 0 = H(\underline{e}_1+\underline{e}_2)^T = H\underline{e}_1^T + H\underline{e}_2^T \Leftrightarrow H\underline{e}_1^T = H\underline{e}_2^T$$

$\Leftrightarrow$ errors indistinguishable.

$\Rightarrow$ Can correct up to t errors, $2t+1 \le d$.

Dual codes:

Code C: G: $k\times n$ matrix, H: $(n-k)\times n$ matrix } orth. rows

Dual code $C^\perp$: $G^\perp = H$ $(n-k)\times n$ matrix

$H^\perp = G$ $k \times n$ matrix

I.e.: The codewords of C & $C^\perp$ are orth. + span $\{0,1\}^n$.

Important identity: $u \notin C^\perp \Rightarrow \sum_{v\in C} (-1)^{v\cdot u} = 0$,

since $\sum_{v\in C} (-1)^{v\cdot u} = \frac{1}{2}\left(\sum_{v\in C}\left[(-1)^{v\cdot u} + (-1)^{(v+v_0)\cdot u}\right]\right)$ for any $v_0 \in C$,

and there exists v_0 s.th. $v_0\cdot u = 1 \Rightarrow (-1)^{v\cdot u} + (-1)^{(v+v_0)\cdot u} = 0$.

Example: Hamming code $[n, k, d] = [7, 4, 3]$

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \quad ; \ (n-k) \times n$$

columns $\equiv$ binary $1 \ldots 8$

$k = 4, \ n = 7$

$d = ?$

$H \cdot (1110000)^T = 0 \Rightarrow d \leq 3$

H can correct any 1-bit error:

$$e_k = (0, \ldots, \underset{k}{1}, 0, \ldots)$$

$\Rightarrow$ $H e_k^T$ = k in binary! $\Rightarrow$ syndrome allows to infer k!

$\Rightarrow t \geq 1 \Rightarrow d \geq 2t + 1 \geq 3$

$\Rightarrow d = 3.$

5. CSS (Calderbank-Shor-Steane) codes

General procedure to convert classical into QECC.

C_1 class. lin. code w/ $(n-k_1)\times n$ parity check H_1.

C_2 subcode of C_1, i.e., $C_2 \subset C_1$:

$(n-k_2)\times n$ parity check H_2,

first $(n-k_1)$ rows of $H_2 = H_1$: $H_2 = \left(\begin{array}{c} H_1 \\ \hline * \end{array}\right)$

C_2 defines equivalence relation on C_1:

$u, v \in C_1$: $u \sim v :\Leftrightarrow u = v + w$, $w \in C_2$

equiv. classes $\{u \mid u \sim v\} = v + C_2$: cosets of C_2 in C_1.

CSS code: $[\![n, k_1 - k_2, ?]\!]$ code:

Code space: $|\bar{v}\rangle = \frac{1}{2^{k_2/2}} \sum_{w \in C_2} |v+w\rangle \equiv |v + C_2\rangle$

$2^{k_1-k_2}$ cosets $\Rightarrow$ $2^{k_1-k_2}$ codewords $|\bar{v}\rangle$, and

$\langle \bar{v} | \bar{v}' \rangle = \begin{cases} 1, & v \text{ and } v' \text{ in same coset, } v - v' \in C_2 \\ 0 & \text{if } v, v' \text{ in different cosets} \end{cases}$

Let Code C_1 have distance $d_1 \geq 2t_1 + 1$

$C_2^\perp$ have dist. $d_2^\perp \geq 2t_2^\perp + 1$

Bit flip error: $|v\rangle \longmapsto |v+e\rangle$, $\underbrace{|e|}_{\text{wgt.}} \leq t_1$

$$\Rightarrow |\bar{v}\rangle = \frac{1}{2^{k_2/2}} \sum_{w \in C_2} \underbrace{|v+w+e\rangle}_{\text{codewords in } C_1 \Rightarrow \text{error can be corrected!}}$$

Correction procedure:

Map $|v\rangle|0\rangle \longmapsto |v\rangle \underbrace{|H_1 v\rangle}_{\text{measure syndrome + correct error.}}$

Phase flip error (w. wgt $t_2^\perp$):

$\longleftrightarrow$ bit flip error in Hadamard basis.

$$H^{\otimes n}|\bar{v}\rangle = \frac{1}{2^{n/2}} \sum_u \frac{1}{2^{k_2/2}} \underbrace{\sum_{w \in C_2} (-1)^{u\cdot w} (-1)^{u\cdot v}}_{= 0,\ u \notin C_2^\perp;\ = 2^{k_2},\ u \in C_2^\perp} |u\rangle$$

$$= \frac{1}{2^{(n-k_2)/2}} \sum_{u \in C_2^\perp} (-1)^{u\cdot v} |u\rangle$$

$H^{\otimes n}|\bar{v}\rangle$ superpos. of states in $C_2^\perp$

$\Rightarrow$ bit flip error (= phase flip error in $|\bar{v}\rangle$) correctable if weight $\leq t_2^\perp$.

$\Rightarrow$ Can correct both bit flip, phase flip, & joint errors.

Distance of CSS code: $d \geq \min(d_1, d_2^\perp)$.

Example: The 7-qubit Steane code

Use 7-bit Hamming code $[7,4,3] = C_1$.

$$H_1 = \begin{pmatrix} 1&0&1&0&1&0&1 \\ 0&1&1&0&0&1&1 \\ 0&0&0&1&1&1&1 \end{pmatrix} \Longleftarrow \text{codewords of } C_1^\perp.$$

$$G_1 = \left[\begin{pmatrix} 1&0&1&0&1&0&1 \\ 0&1&1&0&0&1&1 \\ 0&0&0&1&1&1&1 \\ 1&1&1&0&0&0&0 \end{pmatrix}\right] = H_1 ! \Longleftarrow \text{codewords of } C_1$$

Choose C_1 = Hamming code; $C_2 = C_1^\perp$ (as $C_1^\perp \subset C_1$)

$\Rightarrow C_2^\perp = C_1 \Rightarrow$ Same H for bit + phase flip!

$k_1 = 4;\ k_2 = 3 \Rightarrow$ encodes 1 qubit

Distance $d = \min(d_1, d_2^\perp) = d_1 = 3.$

$\Rightarrow$ $\underline{[\![7, 1, 3]\!]}$ code.

Codewords: $\Rightarrow$ Homework!

6. Stabilizer codes

Have seen (e.g. 3-qubit / 7-qubit code):

code space $\equiv +1$ eigenspace of Paulis.

$\rightarrow$ General framework?

Pauli group:

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

$\mathcal{G} \equiv$ all Pauli products (+ phase)

Stabilizer subgroup:

Abelian subgroup $\mathcal{S} \subset \mathcal{G}$; $-I \notin \mathcal{S}$.

(i.e.: $\mathcal{S}$ contains only commuting elements of the form $\pm P_1 \otimes \dots \otimes P_n$, i.e. all $S \in \mathcal{S}$ have eigenvals ± 1)

$\mathcal{S}$ defines subspace C:

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

C : stabilizer code

Use minimal set of generators to describe $\mathcal{S}$:

$$\mathcal{S} = \langle S_1, \dots, S_r \rangle$$

s.th. (i) any $S \in \mathcal{S}$ is a product of the S_i

(ii) $S_1, \dots, S_r$ is minimal: no S_i is a product of other S_j's.

What is $\dim C$?

$S_i = \pm P_1 \otimes \dots \otimes P_n$: eigenvalues ± 1.

$\operatorname{tr} S_i = 0 \Rightarrow S_i$ has eq. # of $+1$ & -1 eigenvalues.

$\Rightarrow C_1 = \{|\psi\rangle \mid S_1|\psi\rangle = |\psi\rangle\}$ has $\dim C_1 = 2^{n-1}$

Projector onto C_1 is $\Pi_{C_1} = \frac{1}{2}(\mathbb{1} + S_1)$.

Add constraint $S_2|\psi\rangle = |\psi\rangle$:

$$C_2 = \{|\psi\rangle \mid S_1|\psi\rangle = S_2|\psi\rangle = |\psi\rangle\} = \{|\psi\rangle \mid |\psi\rangle \in C_1, S|\psi\rangle = |\psi\rangle\}$$

$$= \{|\psi\rangle \mid \Pi_{C_1} S_2 \Pi_{C_1} |\psi\rangle = |\psi\rangle\} = +1\text{-eigenspace of } \Pi_{C_1} S \Pi_{C_1}.$$

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.

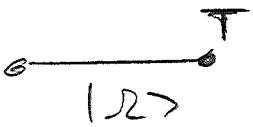
E.g.: 5-qubit code $\hat{H}$ gate:

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

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

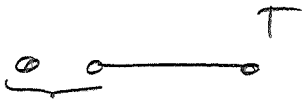
Can we also realize non-Clifford gates (e.g. $T = \begin{pmatrix} 1 & \\ & e^{i\pi/4} \end{pmatrix}$) in a robust way?

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.