QIC 890 / CO781 / CS 867, W22

Lec 2 : Basics of Quantum error correction

- Classical intuition

Binary symmetric channel : a bit x is flipped with prob p

3-bit repetition code : $x=0 \rightarrow 000 \xrightarrow{N} \xrightarrow[\text{decoding}]{\text{majority}} y$

$x=1 \rightarrow 111 \xrightarrow{N} \xrightarrow[\text{decoding}]{\text{majority}} y$

Then $x=y$ if no more than 1 bit flip.

If $\underbrace{N = BSC^{\otimes 3}}_{\text{① independence}}$, then $\text{prob}(x \neq y) = 3p^2(1-p) + p^3 \ll p$ if $p \ll \frac{1}{3}$.

① independence

①+② ⇒ ③ : improvement

② $BSC \approx I$

- Quantum problems

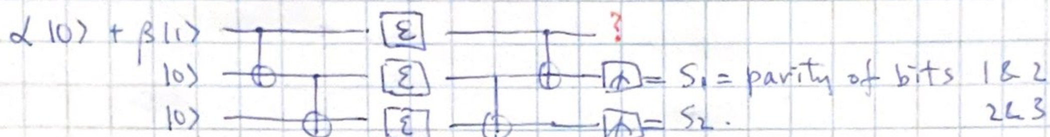
① No cloning $|\psi\rangle \not\rightarrow |\psi\rangle^{\otimes 3}$
② Cannot measure unknown Q info for majority decoding
③ Continuum of errors to correct

- Quantum ideas

① Repetition → linear constraints in codes.
② Measure syndrome, not Q info.
③ Discretize errors

- Quantum bit flip channel: $\mathcal{E}(\rho) = (1-p)\rho + p X\rho X \qquad \left(X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right)$

Quantum 3-bit repetition code:



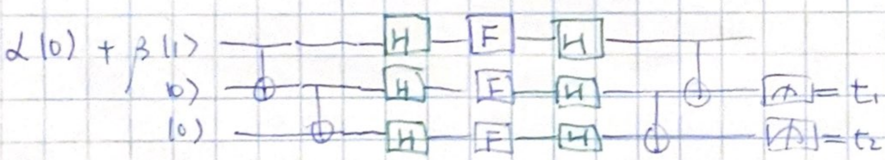
$\alpha|000\rangle + \beta|111\rangle$

		$S_1 S_2$
$\alpha|000\rangle + \beta|111\rangle$	if no error	0 0
$\alpha|100\rangle + \beta|011\rangle$	if X error on 1st qubit	1 0
$\alpha|010\rangle + \beta|101\rangle$	if – – – 2nd – –	1 1
$\alpha|001\rangle + \beta|110\rangle$	– – 3rd	0 1

1st qubit in state $\alpha|0\rangle + \beta|1\rangle$ if $S_1S_2 = 00,\ 11,\ 01$
$\alpha|1\rangle + \beta|0\rangle$ if $S_1S_2 = 10$, apply X gives $\alpha|0\rangle + \beta|1\rangle$

Output $\alpha|0\rangle + \beta|1\rangle$ if at most 1 X error.

- Quantum phase flip channel: $F(\rho) = (1-p)\rho + p Z\rho Z \qquad \left(Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \right)$



$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$

$\alpha|{+}{+}{+}\rangle + \beta|{-}{-}{-}\rangle$

if $|{+}{+}\rangle$ or $|{-}{-}\rangle$ on qubits 1, 2, $t_1 = 0$
$|{+}{-}\rangle$ $\quad |{-}{+}\rangle$ $\qquad\qquad\qquad\qquad 1$

$\therefore\ -\boxed{H}-\boxed{F}-\boxed{H}- \;=\; -\boxed{\mathcal{E}}-$, apply X to 1st qubit if $t_1t_2 = 10$
gives $\alpha|0\rangle + \beta|1\rangle$ if at most 1 Z error.

NB $\rho -\boxed{H}-\boxed{F}-\boxed{H}-\quad (1-p)\, H\, H\rho H\, H + p\, H Z H \rho H Z H = (1-p)\rho + X\rho X$
$(\because HH = I) \quad (\because HZH = X)$

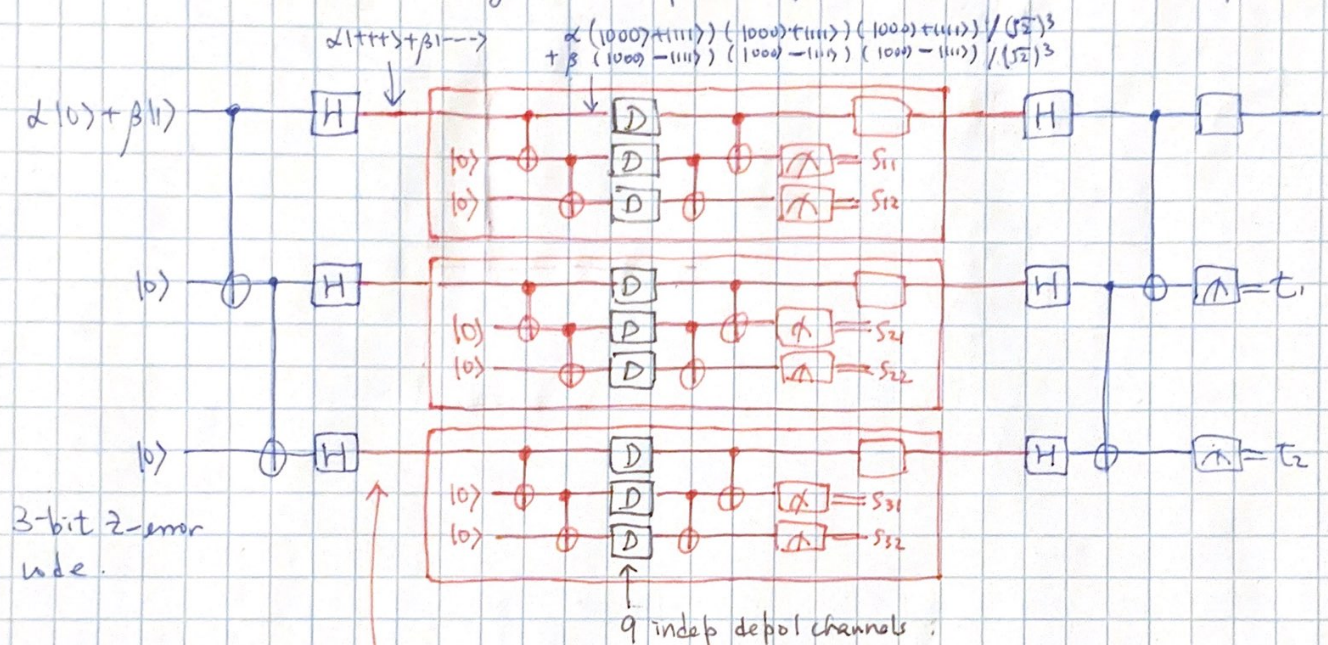
$H\rho H \qquad (1-p)\, H\rho H + p\, Z H\rho H Z$

- Redundancy: restrict logical space to satisfy linear constraints (eg. parities of subsets of bits) so that errors can be identified by "wrong" parities.

Solves no cloning problem & enables meas of "syndrome" not the logical state.

- Qubit depolarizing channel: $D(\rho) = (1-p)\rho + \frac{p}{3}(X\rho X + Z\rho Z + Y\rho Y) = \left(1-\frac{4p}{3}\right)\rho + \frac{4p}{3}\left(\frac{I}{2}\right)$

9-bit Shor code (concatenating 3-bit rep code for X errors with 3-bit rep code for Z errors):



Each qubit in the 3-bit Z-error code is encoded into a 3-bit X-error code.

$$D^{\otimes 9}(\rho) = (1-p)^9\rho + (1-p)^8\tfrac{p}{3}\, XIIIIIIII\,\rho\, XIIIIIIII + (1-p)^8\tfrac{p}{3}\, YIIIIIIII\,\rho\, YIIIIIIII + (1-p)^8\tfrac{p}{3}\, ZIIIIIIII\,\rho\, ZIIIIIIII$$
$$+ \vdots + (1-p)^8\tfrac{p}{3}\, IIIIIIIIX\,\rho\, IIIIIIIIX + (1-p)^8\tfrac{p}{3}\, IIIIIIIIY\,\rho\, IIIIIIIIY + (1-p)^8\tfrac{p}{3}\, IIIIIIIIZ\,\rho\, IIIIIIIIZ + O(p^2)$$

- If 0 or 1 X error occurs, it happens to "one of the red blocks" which corrects it.
- If 0 or 1 Z error occurs, it happens to "one of the red blocks" which outputs a qubit with Z error. This Z error is corrected by the 3-bit Z-error code.
- $Y = iX \cdot Z$ so if 0 or 1 Y error occurs, it will be corrected.

NB. Z error on qubit 1 or 2 or 3 gives the same syndrome $(S_{11} S_{12} \dots S_{32}, t_1 t_2)$ but they have the same correction procedure, so no need to distinguish them

The 9-bit code is called a "degenerate code".

NB. What happens if we first encode in the 3-bit rep code for X errors and further encode each qubit in the 3-bit rep code for Z errors?

(a) Write down the code words

(b) Can this code correct all single qubit Pauli error?

(c) Is this code spanning the same "code space" as the one we just saw?

NB. Instead of $D^{\otimes 9}$, consider a continuous set of error

$$E_\theta = R_Z(\theta) \otimes I^{\otimes 8}$$

$$\uparrow$$

$$e^{-i\theta Z} = \begin{bmatrix} e^{-i\theta} & 0 \\ 0 & e^{i\theta} \end{bmatrix} = \cos\theta \, I - i \sin\theta \, Z$$

The encoded state $|\bar{\Psi}\rangle = \left[\alpha\,(|000\rangle + |111\rangle)^{\otimes 3} + \beta\,(|000\rangle - |111\rangle)^{\otimes 3}\right] \cdot 2^{-3/2}$

becomes $E_\theta |\bar{\Psi}\rangle = \underbrace{\cos\theta\, |\bar{\Psi}\rangle}_{} \underbrace{- i \sin\theta \;\; Z \otimes I \cdots I \, |\bar{\Psi}\rangle}_{}$.

- leads to all 0 meas. outcomes
- and no corrections

- leads to $t_1 = 1$
- and a correction that removes the error.

Both terms are corrected, continuous parameter goes into prob of I or Z error and we still only have 2 errors to distinguish.

"Discretization" of errors (physical error turned to discrete errors by QECC).

Def of a QECC:

Many similar possibilities, want to capture
1. code space
2. what errors are corrected
3. encoded operations

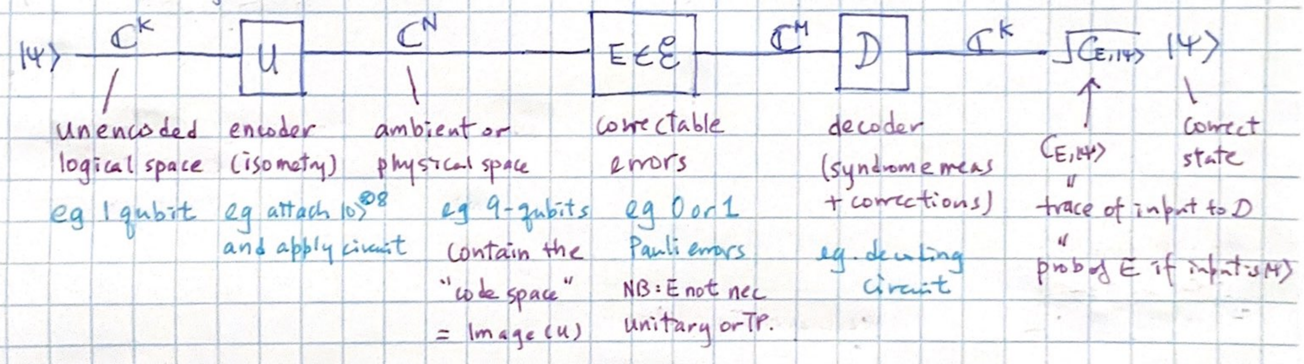
1: fundamental, 2, 3: useful.

Def: A QECC is given by a pair $(U, \mathcal{E})$ where
- U is an isometry from $\mathbb{C}^K$ to $\mathbb{C}^N$ for some $K \le N$
- $\mathcal{E}$: set of linear operators $E: \mathbb{C}^N \to \mathbb{C}^M$

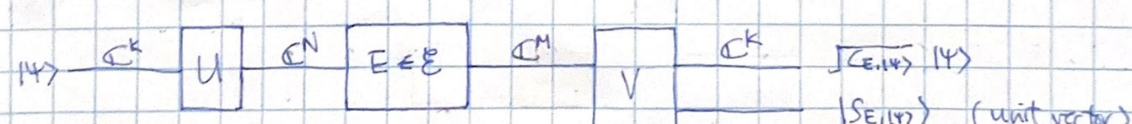
s.t. $\exists$ TCP map $\mathcal{D}: B(\mathbb{C}^M) \to B(\mathbb{C}^K)$

$$\forall E \in \mathcal{E},\ \forall |\psi\rangle \in \mathbb{C}^K,\ \mathcal{D}(EU|\psi\rangle\langle\psi|U^\dagger E^\dagger) = c_{E,|\psi\rangle}\, |\psi\rangle\langle\psi|$$

In circuit diagram:



- $(U, \mathcal{E})$ is QECC $\Rightarrow$ $\exists V$ s.t. $\forall |\psi\rangle \in \mathbb{C}^K$, $\forall E$



eg. $|S_{E,|\psi\rangle}\rangle = |S_{11} S_{21} \cdots S_{32} t_1 t_2\rangle$ for 9-bit code.
indep of $|\psi\rangle$, either ortho or identical for diff E

$c_{E,|\psi\rangle}$ = indep of $|\psi\rangle$ for 9-bit code.

} general...

Observation: set of correctable errors $\mathcal{E}$ depends only on code space (Image(U)) but not on U.

<u>Lemma:</u> for $U_1, U_2 : \mathbb{C}^K \to \mathbb{C}^N$ with Image(U_1) = Image(U_2)

$(U_1, \mathcal{E})$ is a QECC $\iff$ $(U_2, \mathcal{E})$ is a QECC.

<u>Pf:</u> $\exists$ unitary W on $\mathbb{C}^K$ s.t. $U_2 = U_1 W$.

To see this, let $|e_1\rangle, \ldots, |e_K\rangle$ be an orthonormal basis for Image (U_1).

$\exists$ $|f_1\rangle \ldots |f_K\rangle \in \mathbb{C}^K$ s.t. $U_1 |f_i\rangle = |e_i\rangle$

$\exists$ $|g_1\rangle \ldots |g_K\rangle \in \mathbb{C}^K$ s.t. $U_2 |g_i\rangle = |e_i\rangle$

We can take $W = \sum_i |f_i\rangle\langle g_i|$.

NB $\{|f_i\rangle\}$ o.n because U_i is an isometry. Same for $\{|g_i\rangle\}$.

Suppose $(U_1, \mathcal{E})$ QECC,

Then $\exists$ D s.t. $\forall |\psi\rangle \in \mathbb{C}^K$, $\forall E \in \mathcal{E}$, $D(E U_1 |\psi\rangle\langle\psi| U_1^\dagger E^\dagger) = \sqrt{c_{(E,|\psi\rangle)}}\, |\psi\rangle\langle\psi|$

$$\begin{aligned} &\| \\ &D(E U_1 W W^\dagger |\psi\rangle\langle\psi| W W^\dagger U_1^\dagger E^\dagger) \\ &\| \\ &D(E U_2 |\phi\rangle\langle\phi| U_2^\dagger E^\dagger), \text{ where } |\phi\rangle = W^\dagger |\psi\rangle \end{aligned}$$

Conjugating both sides by $W^\dagger$: $W^\dagger D(E U_2 |\phi\rangle\langle\phi| U_2^\dagger E) W = \sqrt{c_{(E, W|\phi\rangle)}}\, |\phi\rangle\langle\phi|$

Above includes all $|\phi\rangle \in \mathbb{C}^K$ [$\because$ $|\phi\rangle = W^\dagger (\underbrace{W|\phi\rangle}_{|\psi\rangle \in \mathbb{C}^K})$]

Take $\tilde{D}(\rho) = W^\dagger D(\rho) W$ as decoder shows $(U_2, \mathcal{E})$ is a QECC.

[Similar proof for $(U_2, \mathcal{E})$ QECC $\Rightarrow$ $(U_1, \mathcal{E})$ QECC.]

NB: Encoding map <u>does</u> affect what are the logical ops.

Following theorem enables QECC for continuous set of errors / discretization of errors.

Thm: If $(\mathcal{U}, \mathcal{E})$ is a QECC
then $(\mathcal{U}, \mathrm{span}(\mathcal{E}))$ is a QECC.

linear span of $\mathcal{E}$, containing linear combinations of elements of $\mathcal{E}$.

ie if E, F correctable, so is $\alpha E + \beta F$ (E, F need not have distinct or identical syndromes)

Pf: $\exists V$ s.t. $\forall |\psi\rangle$,
$$VE\mathcal{U}|\psi\rangle = \sqrt{C_{E,|\psi\rangle}}\, |\psi\rangle \otimes |S_{E,|\psi\rangle}\rangle$$
$$VF\mathcal{U}|\psi\rangle = \sqrt{C_{F,|\psi\rangle}}\, |\psi\rangle \otimes |S_{F,|\psi\rangle}\rangle$$

$\therefore \forall \alpha, \beta \in \mathbb{C}$,
$$V(\alpha E + \beta F)\mathcal{U}|\psi\rangle = |\psi\rangle \otimes \left(\alpha\sqrt{C_{E,|\psi\rangle}}\, |S_{E,|\psi\rangle}\rangle + \beta\sqrt{C_{F,|\psi\rangle}}\, |S_{F,|\psi\rangle}\rangle\right)$$
$$= \sqrt{\underbrace{C_{\alpha E+\beta F,|\psi\rangle}}_{\left\| \alpha\sqrt{C_{E,|\psi\rangle}}\, |S_{E,|\psi\rangle}\rangle + \beta\sqrt{C_{F,|\psi\rangle}}\, |S_{F,|\psi\rangle}\rangle \right\|^2}}\, |\psi\rangle \otimes |S_{\alpha E+\beta F,|\psi\rangle}\rangle$$

$\therefore \alpha E + \beta F$ is correctable.

eg: 9-bit code corrects $R_Z(\theta) \otimes I^{\otimes 8}$ since it corrects $I^{\otimes 9}$ and $Z \otimes I^{\otimes 8}$.

Corollary: A QECC that corrects Pauli operators of weight $\leq t$ corrects <u>any</u> t-qubit error channel.

Pf sketch: Express channel in Kraus rep. analyse output of decoder for each Kraus operator

Recall that the set of correctable error depends only on the code space.

Let $(\mathcal{U}, \mathcal{E})$ be a QECC, $\mathcal{U}: \mathbb{C}^k \to \mathbb{C}^N$.

Let $\mathcal{C}$ denote the code space $\mathrm{Image}(\mathcal{U})$.

Let $P \in B(\mathbb{C}^N)$ be the projector onto $\mathcal{C}$. [Ex: check that $P = \mathcal{U}\mathcal{U}^\dagger$]

A necessary and sufficient condition for QECC is:

Thm $(\mathcal{U}, \mathcal{E})$ QECC $\Leftrightarrow$ $\forall E_i, E_j \in \mathcal{E}$, $P E_i^\dagger E_j P = c_{ij} P$ $\leftarrow (*)$

where $c_{ij} = (i,j)$ entry of matrix $C \geq 0$, $P = \mathcal{U}\mathcal{U}^\dagger$.

Remark:

- Proving $[\Leftarrow]$ establishes RHS as sufficient condition for QECC.
  We need to use the algebraic conditions to find a decoder.

  (Proof is constructive.)

- Proving $[\Rightarrow]$ says that correctable errors must act uniformly on code space

- $(*)$ easier to verify for small discrete $\mathcal{E}$. Once established, we have $(\mathcal{U}, \mathcal{E})$ QECC than we also have $(\mathcal{U}, \mathrm{span}(\mathcal{E}))$ QECC.

Pf [$\Leftarrow$] $\because C \geq 0$, take spectral decomposition

$\therefore C = W d W^{\dagger}$ where W unitary

d diagonal with nonnegative entries

Let $F_k = \sum_j W_{jk} E_j$ — $\circledast$ $\quad$ (W_{jk} = (j,k) entry of W)

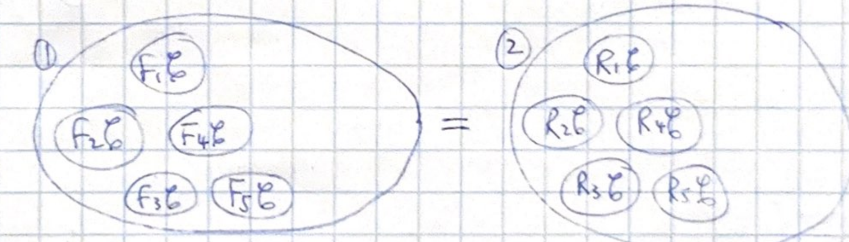
Then
$$P F_l^{\dagger} F_k P \overset{\circledast}{=} \sum_{ij} (W_{il})^{\dagger} W_{jk} P E_i^{\dagger} E_j P$$
$$\overset{\#}{=} \sum_{ij} (W_{il})^{\dagger} C_{ij} W_{jk} P$$
$$= [W^{\dagger} C W]_{lk} \cdot P$$
$$= d_{kk} \delta_{kl} P.$$

① Orthogonality condition:

if $k \neq l$, F_k, F_l take $\mathcal{C}$ to orthogonal spaces

$\forall |\psi\rangle, |\varphi\rangle \in \mathcal{C}$, $\quad \langle \varphi | F_l^{\dagger} F_k | \psi \rangle$

$= \langle \varphi | P F_l^{\dagger} F_k P | \psi \rangle = 0$



② Nondeformation condition:

Apply polar decomposition to $F_k P$:

$F_k P = R_k \sqrt{P F_k^{\dagger} F_k P} \overset{\circledast}{=} R_k \sqrt{d_{kk}} \cdot P$

R_k: unitary

ie F_k acts like some unitary R_k on $\mathcal{C}$.

Idea to correct $\{F_k\}$: find which F_k occurs

then revert using $R_k^{\dagger}$.

(3) Construct decoder for $(U, \{F_k\})$:

(i) Syndrome measurement with projectors $P_k = R_k P R_k^\dagger$ (if $d_{kk} \neq 0$)

$$P_k P_l = R_k P R_k^\dagger R_l P R_l^\dagger$$

$$= R_k \frac{P F_k^\dagger}{\sqrt{d_{kk}}} \frac{F_l P}{\sqrt{d_{ll}}} R_l^\dagger = 0 \text{ if } k \neq l$$

$\therefore$ these projectors are orthogonal. can be completed to a meas.

(ii) if syndrome is "k", apply $R_k^\dagger$

(iii) Apply $U^\dagger$ to decode.

$\therefore$ $(U, \{F_k\})$ is a QECC.

(4) Since W unitary, (*) can be reverted

$\therefore$ Each E_j is a linear combination of F_k's.

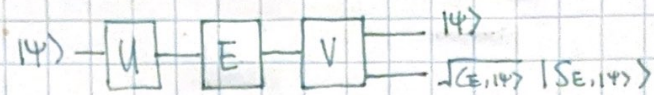
By Thm (on discretization), $(U, \mathcal{E})$ is also a QECC.

NB $\{F_k\}$ easier to correct.
We correct each E_i by correcting each F_k term in E_i.

Example?

Pf [⇒]

Intuition:



neither should depend on $|\psi\rangle$
else we gain info about $|\psi\rangle$ without disturbance

But E is not a TCP map.
So cannot just invoke the operational argument.
Try: enter 2 different states and analyse the ancilla.

Pf: Take $|\psi\rangle, |\phi\rangle \in \mathbb{C}^K$ linear indep.

$$(U,\mathcal{E})\ \text{QECC} \Rightarrow \exists V \text{ s.t. } \forall E \in \mathcal{E},\ \left.\begin{aligned} VEU|\psi\rangle &= \sqrt{C_{E,|\psi\rangle}}\ |\psi\rangle|S_{E,|\psi\rangle}\rangle \\ VEU|\phi\rangle &= \sqrt{C_{E,|\phi\rangle}}\ |\phi\rangle|S_{E,|\phi\rangle}\rangle \end{aligned}\right\} \circledast$$

- Let $\eta(|\psi\rangle+|\phi\rangle)$ be a unit vector.

$$VEU\,\eta(|\psi\rangle+|\phi\rangle) = \sqrt{C_{E,\eta(|\psi\rangle+|\phi\rangle)}}\ \eta(|\psi\rangle+|\phi\rangle)\,|S_{E,\eta(|\psi\rangle+|\phi\rangle)}\rangle \qquad \text{(QECC cond)}$$

- Cancel η, sub $\circledast$ into LHS:

$$\sqrt{C_{E,|\psi\rangle}}\ |\psi\rangle|S_{E,|\psi\rangle}\rangle + \sqrt{C_{E,|\phi\rangle}}\ |\phi\rangle|S_{E,|\phi\rangle}\rangle = \sqrt{C_{E,\eta(|\psi\rangle+|\phi\rangle)}}\,(|\psi\rangle+|\phi\rangle)\,|S_{E,\eta(|\psi\rangle+|\phi\rangle)}\rangle$$

- $\because |\psi\rangle, |\phi\rangle$ lin indep, $\therefore |S_{E,|\psi\rangle}\rangle \propto |S_{E,\eta(|\psi\rangle+|\phi\rangle)}\rangle$, $|S_{E,|\phi\rangle}\rangle \propto |S_{E,\eta(|\psi\rangle+|\phi\rangle)}\rangle$

By normalization, the 3 vectors differ by phases. (ie $|S_{E,|\psi\rangle}\rangle \sim |S_{E,|\phi\rangle}\rangle$!)

$$\therefore \sqrt{C_{E,|\psi\rangle}}\ |\psi\rangle e^{i\theta_\psi} + \sqrt{C_{E,|\phi\rangle}}\ |\phi\rangle e^{i\theta_\phi} = \sqrt{C_{E,\eta(|\phi\rangle+|\psi\rangle)}}\ (|\psi\rangle+|\phi\rangle)$$

$$\because |\psi\rangle, |\phi\rangle \text{ lin indep}, \sqrt{C_{E,|\psi\rangle}}\, e^{i\theta_\psi} = \sqrt{C_{E,|\phi\rangle}}\, e^{i\theta_\phi} = \sqrt{C_{E,\eta(|\phi\rangle+|\psi\rangle)}}$$

$\therefore \theta_\psi = \theta_\phi = 0$, $C_{E,|\psi\rangle} = C_{E,|\phi\rangle}$ which says $|S_{E,|\psi\rangle}\rangle = |S_{E,|\phi\rangle}\rangle$.

- Now we know, $\forall |\psi\rangle$, $VEU|\psi\rangle = \sqrt{C_E}\ |\psi\rangle|S_E\rangle$

(NB our relax def of QECC is useful, so is the above inferred extra condition.)

- To show (#): $\forall |\psi\rangle, |\phi\rangle \in \mathbb{C}_K$, $\forall E_i, E_j \in \mathcal{E}$: $\langle\phi|U^\dagger E_i^\dagger V^\dagger V E_j U|\psi\rangle = \sqrt{C_{E_i}}\sqrt{C_{E_j}}\ \langle\phi|\psi\rangle\,\langle S_{E_i}|S_{E_j}\rangle$

or $\langle\phi|U^\dagger P E_i^\dagger E_j P U|\psi\rangle = C_{ij}\ \langle\phi|U^\dagger P U|\psi\rangle$

$$\therefore \; P E_i^{+} E_j P = c_{ij} P \quad \text{where} \quad c_{ij} = \sqrt{c_{E_i}}\sqrt{c_{E_j}}\, \langle S_{E_i} | S_{E_j} \rangle$$

$$= \left(\sqrt{c_{E_i}}\, \langle S_{E_i} | \right) \left(\sqrt{c_{E_j}}\, | S_{E_j} \rangle \right)$$

$$= (i,j) \text{ entry of a Gram matrix } C \geq 0.$$

QECC condition and non-degenerate vs degenerate QECC:

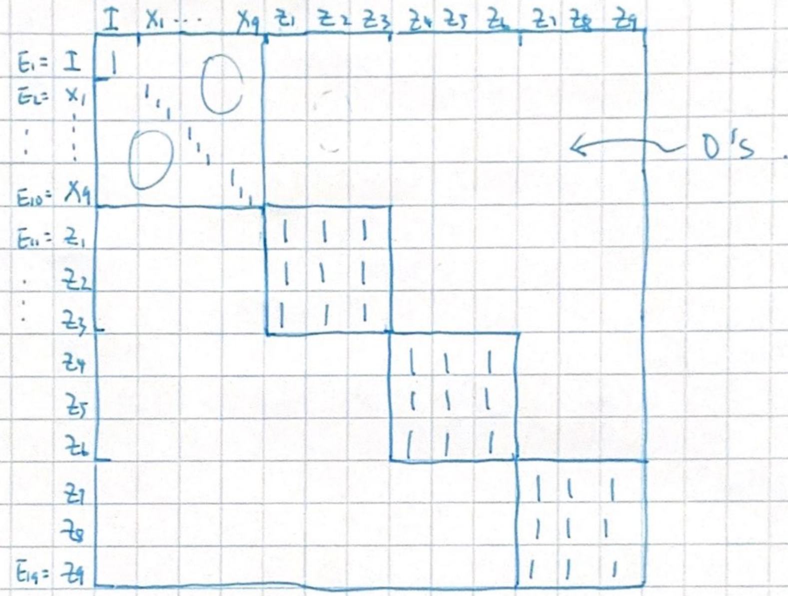
Consider 9-bit code and $\mathcal{E} = \{ I^{\otimes 9}, X_1, X_2, \ldots, X_9, Z_1, Z_2, \ldots, Z_9 \}$

where X_i = X error on i-th qubit $= I^{\otimes i-1} \otimes X \otimes I^{\otimes 9-i}$

$Z_i = Z \ldots$

What is C_{ij} ?

$C = 19 \times 19$



- All E unitary so $C_E = 1$ independent of E.
- $|S_{11} S_{12} S_{21} S_{22} S_{31} S_{32} t_1 t_2\rangle$ corresponds to $|S_E\rangle$

So $\langle S_E | S_F \rangle = \begin{cases} 1 & \text{if } E, F \text{ degenerate errors.} \\ 0 & \text{-- -- -- distinguishable errors.} \end{cases}$

- Transformation to the F_i's : $F_i = E_i$ for $i = 1, \ldots, 10$

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & w & w^2 \\ 1 & w^2 & w \end{bmatrix} \begin{bmatrix} 1 & & \\ & 0 & \\ & & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 \\ 1 & w^2 & w \\ 1 & w & w^2 \end{bmatrix}$$

$\therefore$ $F_{11} = E_{11} + E_{12} + E_{13}$

$F_{12} = E_{11} + w E_{12} + w^2 E_{13}$

$F_{13} = E_{11} + w^2 E_{12} + w E_{13}$

F_{11}: one of Z_1, Z_2, Z_3 occurs but we don't care which.

F_{12}, F_{13} : annihilates the code space, never occur.

Similarly for $F_{14} \cdots F_{19}$.

Ex: find C for $\mathcal{E}$ = 0 or 1 Pauli errors, $|\mathcal{E}| = 1 + 3 \times 7 = 28$.

Def: $(\mathcal{U}, \mathcal{E})$ degenerate code if C matrix in thm does not have full rank.

(ie if some $E_i P$ is a linear comb of other $E_j P$'s)

NB: Why not use the minimal set $\{F_k\}$ instead of $\mathcal{E}$?

$\mathcal{E}$ is often physically motivated eg all 0 or 1 qubit Pauli errors.

Def: Distance of subspace: $\min\{ wt(F) : PFP \neq cP, c \in \mathbb{C} \}$ (P = projector onto subspace)

eg 9-bit code, $PFP = cP$ if $F = I$

F = 1-qubit Pauli's (QECC cond)

F = 2- . . . . . . (QECC cond)

$\therefore$ 9-bit code space has distance 3.

Cor: A distance d subspace is the code space for some QECC that corrects ($t = \lfloor (d-1)/2 \rfloor$)-qubit errors.

Pf: Let $\mathcal{E}$ = set of Pauli errors with $wt \le t$.

If $E_i, E_j \in \mathcal{E}$, then $wt(E_i^\dagger E_j) \le 2t \le d-1$

$\therefore \; P E_i^\dagger E_j P = \underset{\substack{\uparrow \\ \text{depends on } i,j}}{cP} = c_{ij} P$ by hypothesis.

Take $|\psi\rangle$ in the subspace so $P|\psi\rangle = |\psi\rangle$.

$\langle\psi| P E_i^\dagger E_j P |\psi\rangle = c_{ij} \langle\psi|P|\psi\rangle = c_{ij}$ $\therefore$ c_{ij} = (i,j) entry of a Gram matrix C

$\therefore C \geq 0$.