Stabilizers and stabilizer codes:

Def Let $\mathcal{C}$ be a nontrivial subspace of $\mathbb{C}^{2^n}$.

The stabilizer of $\mathcal{C}$ is $\Sigma(\mathcal{C}) = \{ Q \in P_n : Q|\psi\rangle = |\psi\rangle \ \forall |\psi\rangle \in \mathcal{C} \}$

eg: The 8 Pauli's used for syndrome meas for 9-bit code (page ④) are elements of the stabilizer of the 9bit code

Proposition: ⓐ $-I \notin \Sigma(\mathcal{C})$
ⓑ $\Sigma(\mathcal{C})$ is a group
ⓒ $\Sigma(\mathcal{C})$ abelian

Pf: ⓐ ∵ $\mathcal{C}$ nontrivial, take $|\psi\rangle \neq 0$, $|\psi\rangle \in \mathcal{C}$.

(*) Pf by contradiction → If $-I \in \Sigma(\mathcal{C})$, $(-I)|\psi\rangle = |\psi\rangle \Rightarrow |\psi\rangle = 0$ contradiction.

∴ $-I \notin \Sigma(\mathcal{C})$.

ⓑ If $Q, R \in \Sigma(\mathcal{C})$,

then $\forall |\psi\rangle \in \mathcal{C}$, $QR|\psi\rangle = Q|\psi\rangle = |\psi\rangle$
($R \in \Sigma(\mathcal{C})$, $Q \in \Sigma(\mathcal{C})$)

∴ $QR \in \Sigma(\mathcal{C})$

∴ $\Sigma(\mathcal{C})$ is a group.

ⓒ If $Q, R \in \Sigma(\mathcal{C})$, Q, R either commute or anti commute.
suffices to prove this part

(*) Pf by contradiction → Suppose $QR = -RQ$. Take $|\psi\rangle \neq 0$, $|\psi\rangle \in \mathcal{C}$

Then $QR|\psi\rangle = -RQ|\psi\rangle$

$|\psi\rangle$ $\qquad$ $-|\psi\rangle$ $\quad$ ∵ $R, Q \in \Sigma(\mathcal{C})$

∵ $|\psi\rangle \neq 0$ we reach a contradiction

∴ $QR \neq -RQ$ ∴ Q, R commute.

Saw: $\mathcal{C} \to \Sigma(\mathcal{C})$ (code to stabilizer)
Next: $T(S) \leftarrow S$ (stabilizer to code)

Def: Let $S \subseteq P_n$ be an abelian group, $-I \notin S$.
$T(S) = \{|\psi\rangle : M|\psi\rangle = |\psi\rangle \ \forall M \in S\}$

Qn: $\mathcal{C} \to \Sigma(\mathcal{C}) \to T(\Sigma(\mathcal{C}))$.

How is $T(\Sigma(\mathcal{C}))$ related to $\mathcal{C}$?

Ex: check that $\mathcal{C} \subseteq T(\Sigma(\mathcal{C}))$

Containment can be strict:

eg. $\mathcal{C} = \text{span}\{|00\rangle, (|01\rangle + |10\rangle)/\sqrt{2}\}$ (Chuang & Yamamoto 96)

$|00\rangle$: inv under II, IZ, ZI, ZZ ; $(|01\rangle + |10\rangle)/\sqrt{2}$: inv under $II, XX, -ZZ, YY$.

$\therefore \Sigma(\mathcal{C}) = \langle II \rangle$

$\therefore T(\Sigma(\mathcal{C})) = \mathbb{C}^4 \supsetneq \mathcal{C}$

Given $\mathcal{C}$,
Def: If $\mathcal{C} = T(\Sigma(\mathcal{C}))$, then $\mathcal{C}$ is called a stabilizer code.

Qn: $S \to T(S) \to \Sigma(T(S))$

How is $\Sigma(T(S))$ related to S?

Obs: once again $S \subseteq \Sigma(T(S))$.

To see this, take def of $T(S)$, so $\forall M \in S \ \forall |\psi\rangle \in T(S), \ M|\psi\rangle = |\psi\rangle$
← this say $M \in \Sigma(T(S))$ →

Proposition: $S = \Sigma(T(S))$ (Given: S abel subgroup of P_n, $-I \notin S$)

↑ $-I \notin S$ correction!

Pf: Suffices to show that if $M \notin S$ then $M \notin \Sigma(T(S))$.

Divide into 2 cases: (a) M anticom with some $Q \in S$
(b) M commutes with all $Q \in S$.

Case (a): take $|\psi\rangle \in T(S)$, $Q \in S$, Q, M anticom.

then $M|\psi\rangle = MQ|\psi\rangle = -QM|\psi\rangle$

$\therefore \quad -(M|\psi\rangle) = Q(M|\psi\rangle)$

$\therefore \quad M|\psi\rangle \notin T(S)$

$\therefore \quad M \notin \Sigma(T(S))$

Case (b): since $M \notin S$, M commutes with all $Q \in S$

S cannot be maximal. Let $Q_1, \ldots, Q_m$ be generators, $m < n$.

By Lin alg lemma, there are 2^{2n-m-1} Pauli's in $\hat{P}_n$ commuting with all Q_i's and anticommuting with M.

Pick such N outside of S. $(\because 2^{2n-m-1} > 2^m)$

$$T(\langle S, N\rangle) \subseteq T(S)$$

(more constraints)

$$\Sigma(T(\langle S, N\rangle)) \supseteq \Sigma(T(S))$$

more constraints

Apply idea of case (a) to $\langle S, N\rangle \Rightarrow M \notin \Sigma(T(\langle S, N\rangle))$ $(\because \{N, M\} = 0)$

$\therefore \quad M \notin \Sigma(T(S))$

- Moral: start with S, $T(S)$ is a stabilizer code

since $\Sigma(T(S)) = S$ from Prop.

taking $T(\Sigma(T(S))) = T(S)$ $\therefore$ $T(S)$ is stabilizer code by def.

eg 5-qubit code:

Let $Q_1 = X Z Z X I$
$Q_2 = I X Z Z X$
$Q_3 = X I X Z Z$
$Q_4 = Z X I X Z$

(Note $Q_1 Q_2 Q_3 Q_4 = Z Z X I X$) ∴ ✓

① Check commutivity (Suffices to check $c(Q_1, Q_i) = 0$ for $i = 2,3,4$).

② Check independence (Suffices to check $Q_i \neq Q_2^{a_2} Q_3^{a_3} Q_4^{a_4}$ $\forall a_{2,3,4} \in \{0,1\}$)

③ Let S be the abelian group generated multiplicatively by $Q_1, \ldots, Q_4$. ∵ Q_i's com., $Q_i^2 = I$

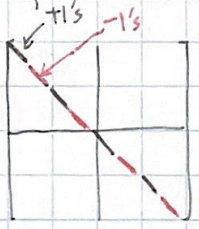
∴ $S = \{ Q_1^{a_1} Q_2^{a_2} Q_3^{a_3} Q_4^{a_4} : a_1 a_2 a_3 a_4 \in \{0,1\}^4 \}$

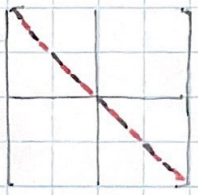
④ What is $T(S)$?

First derive the projector, P, onto $T(S)$.

NB ∵ Q_i has $\frac{1}{2}$ evals $+1$, $\frac{1}{2}$ evals -1

Since $Q_1, \ldots, Q_4$ commute, can simultaneously diagonalize in some basis:

$Q_1 = \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & -1 & \\ & & & -1 \end{bmatrix}$, $Q_2 = \begin{bmatrix} 1 & & & \\ & -1 & & \\ & & 1 & \\ & & & -1 \end{bmatrix}$, $Q_3 =$ 

, $Q_4 =$ 

∵ $\mathrm{tr}\, Q_1 = 0$ ∴ ← half → ← half →

Also: $\frac{I+Q_1}{2} = \begin{bmatrix} 1 & & & \\ & \ddots & & \\ & & 0 & \\ & & & 0 \end{bmatrix}$

Here $\mathrm{tr}\left(\frac{I+Q_1}{2}\right) \cdot Q_2 = a - b$

$= \frac{1}{2}(\mathrm{tr}\, Q_2 + \mathrm{tr}\, Q_1 Q_2)$

$= 0$ ∴ $a = b$.

∴ $c = d$ (∵ $\mathrm{tr}\, Q = 0$)

Black segments = $\left(\frac{I+Q_3}{2}\right)$ (the top "black" segment)

Black segments = $\left(\frac{I+Q_4}{2}\right)$

∴ P = Projector onto simultaneous $+1$ eigenspace of $Q_1, \ldots, Q_4 = \left(\frac{I+Q_1}{2}\right)\left(\frac{I+Q_2}{2}\right)\left(\frac{I+Q_3}{2}\right)\left(\frac{I+Q_4}{2}\right)$.

$= \frac{1}{2^4} \sum_{a_1 \ldots a_4} Q_1^{a_1} Q_2^{a_2} Q_3^{a_3} Q_4^{a_4}$

$= \frac{1}{2^4} \sum_{M \in S} M$.

Dim $(T(S)) = \mathrm{tr}\, P = \frac{1}{2^4} \mathrm{tr}\, I = 2$.

∴ this encodes 1 qubit.

Note with S we only specify the code space $T(S)$ but not the encoding map nor the codewords.

How to specify $|\bar{0}\rangle$, $|\bar{1}\rangle$ and/or logical operations?

- Characterization of logical operations (for all codes, not just stabilizer codes)

  Let $\mathcal{C}$ be a codespace, P projector onto $\mathcal{C}$.

  Then U is a logical operation iff $\forall |\psi_L\rangle \in \mathcal{C}$, $U|\psi_L\rangle \in \mathcal{C}$ (a)

  iff $\forall |\psi_L\rangle \in \mathcal{C}$, $PU|\psi_L\rangle = U|\psi_L\rangle$ (b)

  iff $U^\dagger P U = P$ (c)

  Pf: (a) $\Leftrightarrow$ (b) immediate.

  - Suppose (b) is true. Note $U^\dagger P U$ and P are both projectors; their images have equal dimensions.

    (b) $\Rightarrow (U^\dagger P U)|\psi_L\rangle = |\psi_L\rangle$ $\forall |\psi_L\rangle \in \mathcal{C}$

    $\therefore$ Both $U^\dagger P U$, P projects onto $\mathcal{C}$ $\therefore U^\dagger P U = P \Rightarrow$ (c)

  - Suppose (c) is true. Then $PU = UP$

    $\therefore \forall |\psi_L\rangle \in \mathcal{C}$, $PU|\psi_L\rangle = UP|\psi_L\rangle = U|\psi_L\rangle \Rightarrow$ (b).

- Sufficient conditions for U to be a logical operation for stabilizer codes:

  (d) $USU^\dagger = S$ $\left(\because P = \frac{1}{|S|}\sum_{M \in S} M,\ USU^\dagger = S \Rightarrow UPU^\dagger = P\right)$

  (e) $c(U, Q_i) = 0$ $\forall$ generator Q_i $\left(\because UMU^\dagger = M\ \forall M \in S \therefore UPU^\dagger = P\right)$

For 5-qubit code

(1) $ZZZZZ$ commutes with each generator $Q_1, \ldots Q_4$ ∴ logical op

(2) $(ZZZZZ)^2 = IIIII$

(3) $ZZZZZ \notin S$

(4) By (3) $\exists |\phi\rangle \in \mathcal{C}$ s.t. $\underbrace{(IIIII - ZZZZZ)|\phi\rangle}_{} \neq 0$

(a) Renormalize to $|\mu\rangle$ (note $|\mu\rangle \in \mathcal{C}$)

$ZZZZZ|\mu\rangle = -|\mu\rangle$.

(b) Note $XXXXX$ also commutes with $Q_1, \ldots Q_4$
∴ also a logic op.

Let $|\nu\rangle = XXXXX|\mu\rangle \in \mathcal{C}$

$ZZZZZ|\nu\rangle = (ZZZZZ)(XXXXX)|\mu\rangle$

$= -(XXXXX)(ZZZZZ)|\mu\rangle$

$= (XXXXX)|\mu\rangle = |\nu\rangle$

∴ We can take $|\nu\rangle = |\bar{0}\rangle$, $|\mu\rangle = |\bar{1}\rangle$

$ZZZZZ = \bar{Z}$, $XXXXX = \bar{X}$!!

(5) More generally: by Lin alg lemma,

elmts in $\hat{P}_5$ commuting w/ $Q_1, \ldots, Q_4 = 2^{2\cdot 5 - 4} = 2^6$,

including 2^4 elmts in S.

∴ $\frac{2^6}{2^4}$ distinct logical operations, pick one not in S as $\bar{Z}$ (e.g. $ZZZZZ$)

Then 2 distinct logical ops anti-com with $\bar{Z}$, com to $\bar{X}$ & $\bar{Y}$!! (e.g. $XXXXX$)

(6) But not knowing $|\phi\rangle \in \mathcal{L}$ in (4) ....

Pick instead any state $|\psi\rangle \in \mathbb{C}^{25}$, eg $|100000\rangle$

Then $|\bar{0}\rangle \propto |\bar{0}\rangle\langle\bar{0}|\psi\rangle \propto \left(\frac{I+Z}{2}\right) \cdot P\,|\psi\rangle$

- unless $|\psi\rangle$ = +1 eigenvector of one of the generators, $P|\psi\rangle \neq 0$
- $|\psi\rangle = |0\cdots0\rangle$ good since not eigenvec of the X's, and no − signs from Z's.
- Also gives usual basis for CSS codes.

P commute

$$= P \cdot \left(\frac{I+Z}{2}\right) |100000\rangle$$

$$= P \cdot |100000\rangle$$

$$\propto (I+Q_1)(I+Q_2)(I+Q_3)(I+Q_4)\,|100000\rangle$$

(Q_4: $ZXIXZ$)

$$= (I+Q_1)(I+Q_2)(I+Q_3)\,|100000\rangle + |01010\rangle$$

(Q_3: $XIXZZ$)

$$= (I+Q_1)(I+Q_2)\left(\begin{matrix}|100000\rangle + |01010\rangle \\ |10100\rangle - |11110\rangle\end{matrix}\right)$$

$$= \text{-----}$$

$|\bar{1}\rangle \propto (XXXXX) \cdot$ above.

What errors are corrected by the 5-qubit code?

Prop: The 5-qubit code has distance 3.

Pf: Exhaustive search verifies $\forall M \in \hat{P}_n$ with $wt(M) \leq 2$, $c(M, Q_i) = 1$ for some i.

Then $\forall |\psi\rangle \in \mathcal{Z}$,

$$\left(\frac{I+Q_i}{2}\right) \cdot M |\psi\rangle = M \left(\frac{I-Q_i}{2}\right) |\psi\rangle = 0$$

$$\therefore \quad P \cdot M |\psi\rangle = 0$$

$$\therefore \quad P \cdot M \cdot P = 0 = 0 \cdot P$$

Recall distance $= \min \{ wt(F) : PFP \neq cP, \; c \in \mathbb{C} \}$

$\therefore$ distance of 5-qubit code ≥ 3.

Distance $= 3$. eg. $\bar{Z} Q_1 = YIIYZ$, $P(\bar{Z}Q_1)P = P\bar{Z}P \neq cP$

Cor: 5-qubit code corrects all 1-qubit error channel (those with Kraus op in span of 0- or 1-qubit errors).

More concretely, applying the proof for QECC criterion,

we can get decoder.

Let $\mathcal{E} = \{ I, X_1, \ldots, X_5, Y_1, \ldots, Y_5, Z_1, \ldots, Z_5 \}$
$\quad E_1 \; E_2 \; \cdots \quad E_{16}$

$\because PE_iE_jP = 0$, $F_i = E_i$

$\because E_i$ unitary, $R_i = E_i$.

To meas syndrome, let $P_i = E_i P E_i^\dagger$

$$= E_i \frac{1}{2^4} \prod_{k=1}^{4} (I + Q_k) E_i^\dagger$$

$$= \frac{1}{2^4} \prod_{k=1}^{4} \Big[I + \underbrace{\big(1 - 2c(E_i, Q_k)\big)}_{\substack{-1 \text{ if } \{E_i, Q_k\} = 0 \\ +1 \text{ if } [E_i, Q_k] = 0}} Q_k \Big]$$

Note that the meas with (ortho) projector $P_1, \ldots, P_{16}$ is equivalent to measuring Q_1, Q_2, Q_3, Q_4. (Important $\because$ # generators $\approx \log$(# E_i's).)

eg. if E_i anticommutes with Q_2, Q_3, $P_i = \frac{1}{16} (I + Q_1)(I - Q_2)(I - Q_3)(I + Q_4)$.

If E_i occurs, meas $Q_1, \ldots, Q_4$ gives $+ - - +$.

Ex Complete the following table and check that each of $E_1 \ldots E_{16}$ has a distinct 4-bit syndrome!

$\forall \lvert\psi\rangle \in \mathcal{C}$: meas outcome of	$\lvert\psi\rangle$	$X_1\lvert\psi\rangle$	$X_2\lvert\psi\rangle$	$\cdots$	$Y_3\lvert\psi\rangle$	$\cdots$	$Z_5\lvert\psi\rangle$
$Q_1 = XZZXI$	+	+	−		−		+
$Q_2 = IXZZX$	+	+	+		−		−
$Q_3 = XIXZZ$	+	+	+		−		+
$Q_4 = ZXIXZ$	+	−	+		+		+

General recipe for constructing a stabilizer code & its properties

① Pick block length n

② Pick $m \leq n$ commuting, indep Pauli's $\in \hat{P}_n$ (use def in picture).

$Q_1, Q_2 \ldots, Q_m$ (stabilizer generators)

Use them to generate S multiplicatively (note $|S| = 2^m$)

↑ stabilizer / stabilizer group, $M \in S$: stabilizer element.

③ $T(S)$ has 2^{n-m} dims, encodes $K = n-m$ qubits.

④ Pick $\bar{Z}_1, \bar{Z}_2, \ldots, \bar{Z}_K$ from $\hat{P}_n$ s.t. $Q_1, \ldots, Q_m, \bar{Z}_1, \ldots, \bar{Z}_K$ is a max, indep, commuting set.

⑤ Pick $\bar{X}_1, \ldots, \bar{X}_n \in \hat{P}_n$ s.t. $\bar{X}_1$ commutes with $\bar{Z}_2 \cdots \bar{Z}_K, Q_1 \ldots Q_m$
anticom with $\bar{Z}_1$

$\bar{X}_2$ commutes with $\bar{X}_1, \bar{Z}_1, \bar{Z}_3, \ldots \bar{Z}_K, Q_1 \ldots Q_m$
anticom with $\bar{Z}_2$

$\bar{X}_3$ commutes with $\bar{X}_1, \bar{Z}_1, \bar{X}_2, \bar{Z}_2, \bar{Z}_4, \ldots \bar{Z}_K, Q_1 \ldots Q_m$
anticom with $\bar{Z}_3$

$\vdots$

$\bar{X}_K$ commutes with $\bar{X}_1 \bar{Z}_1 \cdots \bar{X}_{K-1} \bar{Z}_{K-1}, Q_1 \ldots Q_m$
anticom with $\bar{Z}_K$.

NB: We could have imposed that $\bar{X}_1 \cdots \bar{X}_K \bar{Z}_1 \cdots \bar{Z}_K Q_1 \ldots Q_m$ indepedent.
But the conditions in ⑤ automatically implies independence.

NB # options for $\bar{X}_1$: $2^{2n-n} = 2^n \rightarrow 2^{n-m} = 2^K$ options "mod S"
options for $\bar{X}_2$: $2^{2n-(n+1)} = 2^{n-1} \rightarrow 2^{K-1}$ options
$\vdots$ $\vdots$
options for $\bar{X}_K$: $2^{2n-(n+K-1)} = 2^{n-K+1} \rightarrow$ (2) options ($\bar{X}_K, \bar{Z}_K$)

Recall $\forall M \in S$, $\forall i$, $\bar{X}_i M$ & $\bar{X}_i$ act identically on $T(S)$.

(6) $T(S)$ has projector $P = \frac{1}{2^m}(I+Q_1)\cdots(I+Q_m)$

$$|\bar{0}\,\bar{0}\cdots\bar{0}\rangle \propto \frac{1}{2^n}(I+\bar{Z}_1)\cdots(I+\bar{Z}_k)(I+Q_1)\cdots(I+Q_m)\,|100\cdots0\rangle$$

($|\bar{0}\,\bar{0}\cdots\bar{0}\rangle$: $\leftarrow k \rightarrow$; $|100\cdots0\rangle$: $\leftarrow n \rightarrow$)

$$|\bar{b}_1\,\bar{b}_2\cdots\bar{b}_k\rangle = \bar{X}_1^{b_1}\bar{X}_2^{b_2}\cdots\bar{X}_k^{b_k}\,|\bar{0}\,\bar{0}\cdots\bar{0}\rangle, \quad b_i\in\{0,1\}$$

(7) How to characterize a valid logical operation U?

(covered earlier) Several equivalent conditions:

ⓐ $U\,T(S) = T(S)$ (def)

[$T(S) \to T(S)$ but $|\psi\rangle \in T(S)$ can be helped to $|\phi\rangle \in T(S)$, $|\phi\rangle \neq |\psi\rangle$]

$U^\dagger P U = P$ $\Leftrightarrow$ ⓑ $UPU^\dagger = P$

$U^\dagger S U = S$ $\Leftrightarrow$ ⓒ $USU^\dagger = S$

$\Uparrow$ because

ⓘ $P = \frac{1}{2^m}\sum_{M\in S} M$

or

ⓘⓘ $\Sigma(U\mathcal{E}) = U\,\Sigma(\mathcal{E})\,U^\dagger$ (proved next lecture)

$\Updownarrow$

ⓓ $UQ_iU^\dagger \in S \quad \forall i = 1,\ldots,m$

(8) Special class of logical operations:

Normalizer of S: $N(S) = \{L \in \hat{P}_n : \underbrace{C(L,M) = 0 \ \forall M\in S}_{\text{so } \forall M\in S,\ LML^\dagger = M}\}$ much more stringent than ⓒ

Obs: ⓐ $S \subseteq N(S)$.

$\uparrow$ set of Pauli implementing $\bar{I}$

ⓑ $N(S)$ is a group.

ⓒ $\because L_1, L_2$ act identically on $T(S)$ if $L_1 = ML_2$ for some $M\in S$

$\therefore$ Consider $N(S)/S$.

ⓓ $|N(S)| = 2^{2n-m}$ (lin alg lemma)

$|N(S)/S| = 2^{2n-2m} = 2^{2k}$

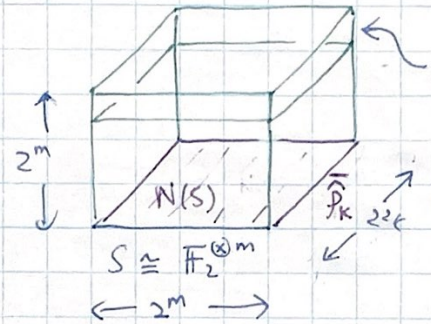
(e) Note $\bar{X}_1, \bar{Z}_1, \ldots, \bar{X}_k, \bar{Z}_k \in N(S)$

In fact, they are distinct elements in $N(S)/S$.

By the group structure of $N(S)$, $\overline{\hat{P}_k} \subseteq N(S)/S$

By the cardinality of both sides, $\overline{\hat{P}_k} \cong N(S)/S$.

(g) The code construction from (2)-(5) restructure $\hat{P}_n$ as:



Each layer: $A \in \hat{P}_n$ with same syndrome

ie fixed $c_i = c(A, Q_i)$ for $i = 1, \ldots m$.

$$\left[\forall |\psi\rangle \in T(S) \quad Q_i A|\psi\rangle = c_i A Q_i|\psi\rangle = c_i A|\psi\rangle\right]$$

Summary:

- A, B logically equivalent if $A = BM$ for some $M \in S$
- A, B indistinguishable error if $A = BM$ for some $M \in N(S)$

Intuition:

- $(T(S), \mathcal{E})$ QECC if $\forall E_i, E_j \in \mathcal{E}$, they're distinguishable or logically equivalent

abusing notation

ie $E_i E_j^\dagger \notin N(S)$

or $E_i E_j^\dagger \in S$

ie $E_i E_j^\dagger \notin N(S) - S$.

↑ set difference

eg if each $F \in N(S) - S$ has wt $\geq 2t+1$ then $\mathcal{E}$ can be all Pauli's of wt $\leq t$.

$\therefore \hat{P}_n / N(S)$ consists of cosets (layers) each labelled by m-bit string $c_1 \ldots c_m$

Each coset contains Paulis with same syndrome.

NB. $|\hat{P}_n| = 2^{2n}$, $|N(S)| = 2^{2n-m}$

$\therefore |\hat{P}_n / N(S)| = 2^m$ matching # syndromes.

(syndrome := m-bit meas outcome of $Q_1 Q_2 \ldots Q_m$)

(10) Distance of $T(S) = \min\{ wt(A) : A \in N(S) - S \}$

Pf: Distance of $T(S) = \min\{ wt(F) : PFP \neq cP \}$

Since F = linear combination of Pauli's in $\hat{P}_n$, consider $E \in \hat{P}_n$ first.

Case 1: $E \in S$, then $PEP = P$

Case 2: $E \notin N(S)$, then $\forall |\eta\rangle \in \mathbb{C}^{2^n}$

anticom with F

$$\begin{aligned} PEP|\eta\rangle &= PEQ_iP|\eta\rangle \\ &= -PQ_iEP|\eta\rangle \\ &= -PEP|\eta\rangle \end{aligned}$$

$\therefore PEP|\eta\rangle = 0 \quad \therefore PEP = 0 = c \cdot P$.

Case 3: $E \in N(S) - S$.

- Let $F = \sum_{E_i \in S} a_i E_i + \sum_{E_j \in N(S) - S} b_j E_j + \sum_{E_k \notin N(S)} h_k E_k$. attains min in dist of $T(S)$.

- We have $PFP = \sum_{E_i \in S} a_i P + \sum_{E_j \in N(S) - S} b_j PE_jP$

- Cannot have $b_j = 0 \ \forall j$ else $PFP = c \cdot P$ contradiction

$\therefore wt(F) \geq \min_{E_j \in N(S) - S} wt(E_j)$

- Meanwhile $\forall E_j \in N(S) - S$, $PE_jP \neq cP$

$\therefore$ Dist $T(S) = \min\{ wt(A) : A \in N(S) - S \}$

+P8-12

If not in N(S).

If in S, $E_i P = E_j P$

eg. $n=4$, $m=2$. $g_1 = XXXX$, $g_2 = ZZZZ$

Encodes 2-qubits.

Let $\bar{Z}_1 = ZZII$, $\bar{Z}_2 = ZIZI$

Let $\bar{X}_1 = XIXI$, $\bar{X}_2 = IIXX$

(Ex: find all possible $\bar{X}_1$ verify the # choices then take $\bar{X}_1 = XIXI$ find all possible $\bar{X}_2$ verify the # choices).

$|\bar{0}\bar{0}\rangle \propto \frac{1}{16}(IIII+ZZII)(IIII+ZIZI)(IIII+XXXX)(IIII+ZZZZ)|0000\rangle$

$|\bar{0}\bar{0}\rangle = \frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle)$ (trick: more Z's to the right!)

$|\bar{0}\bar{1}\rangle = \bar{X}_2|\bar{0}\bar{0}\rangle = \frac{1}{\sqrt{2}}(|0011\rangle + |1100\rangle)$

$|\bar{1}\bar{0}\rangle = \bar{X}_1|\bar{0}\bar{0}\rangle = \frac{1}{\sqrt{2}}(|1010\rangle + |0101\rangle)$

$|\bar{1}\bar{1}\rangle = \bar{X}_1\bar{X}_2|\bar{0}\bar{0}\rangle = \frac{1}{\sqrt{2}}(|1001\rangle + |0110\rangle)$

$S = \{IIII, XXXX, ZZZZ, YYYY\}$.

$N(S)/S = \{\bar{I}\bar{I}, \bar{I}\bar{X}, \bar{I}\bar{Z}, \bar{I}\bar{Y}, \bar{X}\bar{I}, \bar{X}\bar{X}, \bar{X}\bar{Y}, \bar{X}\bar{Z}, \bar{Z}\bar{I}, \bar{Z}\bar{X}, \bar{Z}\bar{Z}, \bar{Z}\bar{Y}, \bar{Y}\bar{I}, \bar{Y}\bar{X}, \bar{Y}\bar{Y}, \bar{Y}\bar{Z}\}$.

Ex: find the 4 coset reps for $\hat{P}_4 / N(S)$.

Distance = 2 since all wt 1 Pauli anti com with g_1 or g_2.

• CSS codes (Calderbank-Shor-Steane)

Note that if $Q_1, Q_2, \ldots, Q_m$ generate S
then $Q_1Q_2, Q_2, \ldots, Q_m$ also generate S.

A stabilizer code $T(S)$ is a CSS code
if $\exists$ set of stabilizer generators each is either tensor product of I, X or I, Z

eg. Shor 9-bit code (6 Z-generators, 2 X-generators)

eg. 4-bit code (1 Z-generator, 1 X-generator).

These 2 generators have the same form

eg. Steane 7-bit code:

Stabilizer generators:

$Q_1 = I\ I\ I\ X\ X\ X\ X$
$Q_2 = I\ X\ X\ I\ I\ X\ X$
$Q_3 = X\ I\ X\ I\ X\ I\ X$

parity check matrix for 7-bit Hamming code

$Q_4 = I\ I\ I\ Z\ Z\ Z\ Z$
$Q_5 = I\ Z\ Z\ I\ I\ Z\ Z$
$Q_6 = Z\ I\ Z\ I\ Z\ I\ Z$

The same, so these locate where an X-error occurs

Note that we need $HH^T = 0$ (self dual) for the Hamming code for these generators to commute.

if a Z-error occurs on the ith qubit, and $s_1s_2s_3$ is the binary rep of i then meas outcome: $(-1)^{s_1}\ (-1)^{s_2}\ (-1)^{s_3}$

This is a wonderful code for fault-tolerance — it has nice encoded operations.

eg. 5-bit code is NOT CSS.
Pf: Ex.

eg Hypergraph product codes (QLDPC codes) (see lecture 5).

Intuition: CSS codes correct X & Z errors separately.

(See eg Nielsen & Chuang Sec 10.4.2, C_2 there is C_2 here.)

In general, take 2 classical linear codes C_1, C_2 of equal length n with parity check matrices H_1, H_2. WLOG, H_i has r_i rows with $r_2 \geq r_1$.

Turn H_2 to X-generators (correct z errors), $\Pi_1, \ldots, \Pi_{r_2}$

H_1 z- (X - -), $\Pi_{r_2+1}, \ldots, \Pi_{n-r_2}$

Generators commute $\Leftrightarrow$ $H_1 H_2^T = 0$ $\Leftrightarrow$ $H_2 H_1^T = 0$

$\because H_1 G_1 = 0$, $H_2 G_2 = 0$, (G_i generator matrix for C_i)

If H_2^T is a submatrix of G_1, we have a proper stabilizer.

If C_i has distance d_i, resulting CSS code has distance $\geq \min(d_1, d_2)$.

↑ can be correct eg 9-bit code

Encodes $n - r_1 - r_2$ logical qubits, with a simple logical basis:

$$|\bar{0}\bar{0}\cdots\bar{0}\rangle \propto \prod_{i=1}^{r_1+r_2} (I + \Pi_i) \, |00\cdots0\rangle = \prod_{i=1}^{r_2} (I + \Pi_i) \, |0\cdots0\rangle$$

$\leftarrow n - r_1 - r_2 \rightarrow$ (= k) $\quad \leftarrow n \rightarrow \quad \leftarrow n \rightarrow$

↑ z generators do nothing ↑ X generators from H_2

$$= \sum_{c \in C_2^\perp} |c\rangle$$

↖ code with generator matrix H_2^T, a subcode of C_1

$\because H_2^T$ submatrix of C_1.

$$|\bar{b}_0 \bar{b}_2 \cdots \bar{b}_k\rangle \propto \prod_{l=1}^{k} (I + W_l)^{b_k} \, |\bar{0}\bar{0}\cdots\bar{0}\rangle \propto \sum_{c \in C_2^\perp} |m + c\rangle, \quad m \in C_1 / C_2^\perp.$$

$G_1 =$  . Turn l-th column of G_1 to W_l (tensor prod of Z, X).