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 (P_4) are elements of the stabilizer of the 9bit code.

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

Pf: (a) $\because \mathcal{C}$ 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.

$\therefore -I \notin \Sigma(\mathcal{C})$.

(b) If $Q, R \in \Sigma(\mathcal{C})$,

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

$\therefore QR \in \Sigma(\mathcal{C})$

$\therefore \Sigma(\mathcal{C})$ is a group.

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

(*) Suppose $QR = -RQ$.

Then take $|\psi\rangle \neq 0$, $|\psi\rangle \in \mathcal{C}$.

$QR|\psi\rangle = -RQ|\psi\rangle$ due to (*)

$|\psi\rangle = -|\psi\rangle$ $\because R$ and Q are in $\Sigma(\mathcal{C})$.

So we reach a contradiction $\therefore$ (*) cannot hold

$\therefore Q$ & R must commute.

Saw: $\mathcal{C} \to \Sigma(\mathcal{C})$

Next: $T(S) \leftarrow S$

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:

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

↑ inv under II, IZ, ZI, ZZ ↑ inv under $II, XX, -ZZ, YY$.

$\therefore \Sigma(\mathcal{C}) = \mathcal{I}\mathcal{I}$

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

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: $S = \Sigma(T(S))$

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} Paulis in $\hat{P}_n$ commuting with all Q_i's and anticommuting with M.

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

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

(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 $Q_1 = X\,Z\,Z\,X\,I$
$Q_2 = I\,X\,Z\,Z\,X$
$Q_3 = X\,I\,X\,Z\,Z$
$Q_4 = Z\,X\,I\,X\,Z$

① Check commutivity

② Check independence

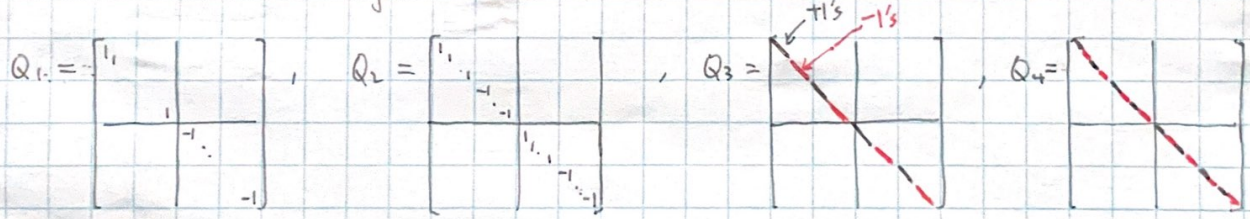
③ Let S be the abelian group (generated) multiplicatively by $Q_1,\dots,Q_4$. $\because Q_i$'s com., $Q_i^2 = I$

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

④ What is $T(S)$?

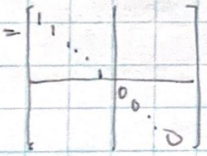
First derive the projector, P, onto $T(S)$.

Since $Q_1,\dots,Q_4$ diagonal in some basis :



$\because \mathrm{tr}\, Q_1 = 0 \;\therefore$ ←half→←half→

Also: $\frac{I+Q_1}{2} =$



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

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

$= 0 \quad \therefore a = b.$

$\therefore c = d.$

Black segments $= \left(\frac{I+Q_3}{2}\right)$

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

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

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

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

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

$\therefore$ this encodes 1 qubit.

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

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

Note that $\bar{Z} = |\bar{0}\rangle\langle\bar{0}| - |\bar{1}\rangle\langle\bar{1}|$

$\forall M \in S$,
$$\bar{Z}M = |\bar{0}\rangle\langle\bar{0}|M - |\bar{1}\rangle\langle\bar{1}|M = |\bar{0}\rangle\langle\bar{0}| - |\bar{1}\rangle\langle\bar{1}|$$
$$M\bar{Z} = M|\bar{0}\rangle\langle\bar{0}| - M|\bar{1}\rangle\langle\bar{1}| = |\bar{0}\rangle\langle\bar{0}| - |\bar{1}\rangle\langle\bar{1}|$$

i.e. $\bar{Z}$ commute with all elents of S.

But $\bar{Z} \notin S$ i.e. $\bar{Z}$ indep of $Q_1, \ldots, Q_4$

(*) One option: $\bar{Z} = ZZZZZ$

$$|\bar{0}\rangle\langle\bar{0}| = \left(\frac{1+\bar{Z}}{2}\right) \cdot P$$
$$|\bar{1}\rangle\langle\bar{1}| = \left(\frac{1-\bar{Z}}{2}\right) \cdot P.$$
} specify $|\bar{0}\rangle$, $|\bar{1}\rangle$ up to 2 separate phases.

(*) Relate these 2 phases by picking $\bar{X}$:

it has to commute with $Q_1 \ldots, Q_4$, anticom with $\bar{Z}$

By linalg lemma, 2^5 options in $\hat{P}_n$:
up to multiplication by the 2^4 elements in S (logically trivial), 2 distinct options
One option $\bar{X} = XXXXX$. ↑ $\bar{X}, \bar{Y}$

Finally, pick any state in $\mathbb{C}^{2^5}$ eg $|00000\rangle$

Then $|\bar{0}\rangle \propto \left(\frac{1+\bar{Z}}{2}\right) P |00000\rangle \propto \ldots$

$$|\bar{1}\rangle = \bar{X}|\bar{0}\rangle$$

Detail: see CO481 notes, file co481-w2019-topic-09-3b.pdf, P15-22.
beware of typos in the $\pm$ signs!

What errors are corrected by the 5-qubit code?

Proposition: The 5-qubit code has distance 3.

Pf: By exhaustive search, any $M \in \hat{P}_n$ with $wt(M) \le 2$ anticommutes with at least one of Q_1, Q_2, Q_3, Q_4.

(Using symmetry, this search is not too long; see CO481 notes. ... topic-09-3b.pdf p13-14.)

$\forall |\psi\rangle \in T(S)$,

$M|\psi\rangle = M Q_i |\psi\rangle = -Q_i M |\psi\rangle$

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

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

$\therefore P M P = 0 = 0 \cdot P$ ↓ $\sum_{\{|\psi\rangle\}}$ basis for $T(S)$ $P M |\psi\rangle\langle\psi|$

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 possible 1-qubit errors. (or 1 qubit erasure)

(This follows from Cor on P14, lec 2.)

Alternative, direct, proof of cor: compute the table: $\forall |\psi\rangle \in T(S)$

	$\|\psi\rangle$	$X_1\|\psi\rangle$	$X_2\|\psi\rangle$	⋯	$X_5\|\psi\rangle$	$Y_1\|\psi\rangle$ ⋯	$Y_5\|\psi\rangle$	$Z_1\|\psi\rangle$, ⋯, $Z_5\|\psi\rangle$
meas outcome of Q_1	+	+	−					+
Q_2	+	+	+			⋯		−
Q_3	+	+	+					+
Q_3	+	−	+					+

and check that each error of wt ≤ 1 has a distinct 4-bit syndrome.

General recipe for constructing a stabiliyr code & its properties

① Pick blocklength n

② Pick $m \leq n$ commuting, indep Pauli's from $\hat{P}_n$:

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

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

S: stabiliyr / stabiliyrgroup, $M \in S$: stabiliyr 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 $\bar{X}_1 \cdots \bar{X}_K \bar{Z}_1 \cdots \bar{Z}_K Q_1 \ldots Q_m$ independt. 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

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

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

$|\underbrace{\bar{0}\,\bar{0}\cdots\bar{0}}_{\leftarrow k \rightarrow}\rangle \propto \frac{1}{2^n}(1+\bar{Z}_1)\cdots(1+\bar{Z}_k)(1+Q_1)\cdots(1+Q_m)\,|\underbrace{00\cdots0}_{\leftarrow n \rightarrow}\rangle$

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

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

Several equivalent conditions:

(a) $U\,T(S) = T(S)$ (def)

$\approx$ (b) $UPU^\dagger = P$

(c) $USU^\dagger = S$

(d) $UQ_iU^\dagger \in S \quad \forall i = 1,\dots,m$

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

⇑ because

(i) $P = \frac{1}{2^m}\sum_{M\in S} M$

or

(ii) $\Sigma(U\mathcal{E}) = U\,\Sigma(\mathcal{E})\,U^\dagger$

(8) Special class of logical operations:

$N(S) = \{L \in \hat{P}_n : \underbrace{C(L,M) = 0 \quad \forall M \in S}\}$

so $\forall M \in S$, $LML^\dagger = M$ much more stringent than (c)

Obs: (a) $S \subseteq N(S)$.

↑ set of Pauli implementing $\bar{I}$

(b) $N(S)$ is a group.

(c) ∵ L_1, L_2 act identical on $T(S)$ iff $L_1 = ML_2$ for some $M \in S$

∴ Consider $N(S)/S$.

(d) $|N(S)| = 2^{2n-m}$ (lin alg lemma)

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

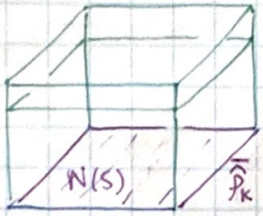
(e) Note $\bar{X}_1, \bar{Z}_1, \ldots, \bar{X}_k, \bar{Z}_k \in N(S)$

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:



$S \cong \mathbb{F}_2^{\otimes m}$

← Paulis that anticom with some Q_i

Let $C_i = C(A, Q_i)$.

$\forall |\psi\rangle \in T(S)$

$Q_i A|\psi\rangle = C_i A Q_i |\psi\rangle = C_i A|\psi\rangle$

∴ if an error A occurs, when we meas eigenvalue of $Q_1, \ldots, Q_m$ we get $c_1, c_2, \ldots, c_m$.

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

Each coset contains Paulis with same syndrome.

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

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

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

Summary:

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

Intuition:

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

  ie $E_i E_j^\dagger \neq M \quad \forall M \in N(S)$

  or $E_i E_j^\dagger = M$ for some $M \in S$'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 Paulis of wt $\leq t$.