QIC 890 / CO781 / CS867, W22

Lec 7: tracking evolution under Clifford unitaries & Pauli meas

① Evolution under Clifford unitary U:

ⓐ Suppose initial state $|\psi\rangle$ is a stabilizer state

(i.e. $|\psi\rangle \in T(S)$ where S maximal, ie with n generators in n qubits)

eg. $|0\rangle^{\otimes n}$ (S generated by $Z_1, Z_2, \ldots, Z_n$)

eg. $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ (S generated by XX, ZZ)

$\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ ($\cdots$ $XX, -ZZ$) ← this is allowed.

$\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$ ($\cdots$ $-XX, ZZ$)

$\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ ($\cdots$ $-XX, -ZZ$)

From P1 Lecture 6, if U acts on $|\psi\rangle \in T(S)$,

then new stabilizer $S' = \{UMU^\dagger : M \in S\} =: USU^\dagger$.

More succinctly,

$Q_1 \longrightarrow UQ_1U^\dagger$

$Q_2 \longrightarrow UQ_2U^\dagger$

$\vdots$ $\vdots$

$Q_n \longrightarrow UQ_nU^\dagger$

generators of S generators of S'

eg. $U = CNOT$. $|\psi\rangle = |00\rangle$,

$Z_1 \longrightarrow Z_1 \sim Z_1$

$Z_2 \longrightarrow Z_1Z_2 \sim Z_2$ ← can multiply generators to get new generator.

Of course, $CNOT|00\rangle = |00\rangle$!

eg. $U = CNOT$, $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

$-XX \longrightarrow -X1$

$ZZ \longrightarrow 1Z$. Indeed, $CNOT|\psi\rangle = |+\rangle|0\rangle$.

(b) For unrestricted states,

eg. $|0\rangle \to U|0\rangle$ So $|0\rangle\langle 0| = \frac{1}{2}(I+Z) \to U|0\rangle\langle 0|U^\dagger = U\frac{1}{2}(I+Z)U^\dagger = \frac{1}{2}(I+UZU^\dagger)$

$|1\rangle \to U|1\rangle$ $|1\rangle\langle 1| = -$ $U|1\rangle\langle 1|U^\dagger$ $-$ $-$

$|+\rangle \to U|+\rangle$ $|\pm\rangle\langle\pm| = \frac{1}{2}(I \pm X) \to U|\pm\rangle\langle\pm|U^\dagger = \frac{1}{2}(I \pm UXU^\dagger)$

$|-\rangle \to U|-\rangle$

So $X_i \to UX_iU^\dagger$

$Z_i \to UZ_iU^\dagger$ for $i=1,2,\ldots,n$ in general.

(c) Most general case: Stabilizer code encoding k qubits in n

Suppose $U \in C_n$ is applied,

- the stabilizer generators evolve as: $Q_i \to UQ_iU^\dagger$, $i=1,2,\ldots,n-k$
- the encoded Pauli's evolve as: $\overline{X}_i \to U\overline{X}_iU^\dagger$, $i=1,\ldots,k$

  $\overline{Z}_i \to U\overline{Z}_iU^\dagger$, $i=1,\ldots,k$

  (inherit com/anticom rel'n)
- Case (a) $k=0$, case (b) $k=n$.

Examples:

code 1	→	code 2
$XZZXI$	→	$ZXXZI$
$IXZZX$	→	$IZXXZ$
$XIXZZ$	→	$ZIZXX$
$ZXIXZ$	→	$XZIZX$
$\overline{X} = XXXXX$	→	$ZZZZZ$
$\overline{Z} = ZZZZZ$	→	$XXXXX$

- 7 qubit code, $U = H^{\otimes 7}$, or $R_{\frac{\pi}{4}}^{\otimes 7}$, or $CNOT^{\otimes 7}$:

Permute stabilizer generators but preserves stabilizer.
⇒ logical Pauli's as logical Clifford gates.

② Evolution under measurement of $P \in \hat{P}_n$.

3 Cases:
- ⓐ $\pm P \in S$ (syndrome measurements)
- ⓑ $P \in N(S) - S$ (measuring encoded Pauli's)
- ⓒ $P \notin N(S)$ (taking encoded state out of codespace)

Case ⓐ: State is an eigenstate of P, so unchanged by meas.
∴ Stabilizer & encoded Paulis unchanged.

Measurement outcome: $\begin{cases} +1 & \text{if } P \in S \\ -1 & \text{if } -P \in S \end{cases}$

eg meas XX on $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$, get -1, Bell state unchanged.

Case ⓑ: $P \in N(S) - S$

P com with all $M \in S$

Pauli com with half of $N(S)/S$.

If encoded state is $|\psi\rangle$, $\text{prob}(b = \pm) = \text{tr}\left[\left(\frac{I \pm P}{2}\right)|\psi\rangle\langle\psi|\right]$. (outcome)

Distribution of b depends on $|\psi\rangle$.

State change: $|\psi\rangle \longrightarrow \frac{1}{2}(I + b \cdot P)|\psi\rangle$

Suppose $S \to S'$, $N(S) \to N(S')$. How to relate S, S', $N(S)$, $N(S')$?

(i) $S \subseteq S'$. Pf: $\forall M \in S$,

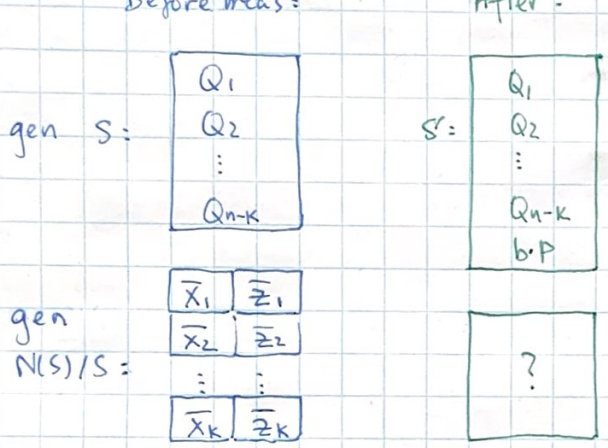
$$M\left(\tfrac{1}{2}(I + b\cdot P)|\psi\rangle\right) = \tfrac{1}{2}(I + b\cdot P) M|\psi\rangle \quad (\because M, P \text{ com})$$
$$= \tfrac{1}{2}(I + b\cdot P)|\psi\rangle \quad (\because M \in S)$$

∴ M stabilizes $\frac{1}{2}(I + b\cdot P)|\psi\rangle$.

Intuitively: P compatible with all $M \in S$.
Also meas encoded Pauli is a logical op which preserves the code space.

(ii) $b \cdot P \in S'$. (Meas reduces the encoded space.)

(iii) How does $N(S)$ transform to $N(S')$?



All elements in $N(S')$ commute with all elements in S', so elements in $N(S)$ that anticommute with P have to learn.

Procedure: ① At least one of $\bar{X}_1, \bar{X}_2 \ldots, \bar{X}_k, \bar{Z}_1, \ldots, \bar{Z}_k$ anticom with P.

For concreteness, say $c(\bar{X}_1, P) = 1$.

② For each of $\bar{X}_2, \ldots \bar{X}_k, \bar{Z}_2, \ldots, \bar{Z}_k$
If it anticommutes with P, multiply $\bar{X}_1$ to it. Else do nothing.
Call the resulting ops $\bar{X}_2', \ldots, \bar{X}_k', \bar{Z}_2', \ldots, \bar{Z}_k'$.

③ $N(S')/S'$:

$\bar{X}_2'$	$\bar{Z}_2'$
$\bar{X}_3'$	$\bar{Z}_3'$
⋮	
$\bar{X}_k'$	$\bar{Z}_k'$

- Let $F \in \{\bar{X}_2', \bar{X}_3', \ldots, \bar{Z}_2', \ldots, \bar{Z}_k'\}$.
- F commutes with $Q_1, Q_2 \ldots, Q_{n-k}$.
- if $c(E,P) = 1$, then $c(E\bar{X}_1, P) = c(E,P) + c(\bar{X}_1, P) = 0$.
  ∴ Procedure ② ensures F com with P.
- Since $\bar{X}_1$ com with all of $\bar{X}_2, \ldots, \bar{X}_k, \bar{Z}_2 \ldots \bar{Z}_k$, the com/anticom rel'ns in $\bar{X}_2, \ldots \bar{X}_k, \bar{Z}_2 \ldots, \bar{Z}_k$ stay in $\bar{X}_2', \bar{X}_3', \ldots, \bar{X}_k', \bar{Z}_2', \bar{Z}_3', \ldots \bar{Z}_k'$.

Overall effect = $b \cdot P$ promoted to S'
Only $K-1$ encoded qubits remain.

Remaining encoded Paulis can be permuted

$\bar{i}_1 |\psi\rangle \longrightarrow \frac{1}{2}(I + bP)|\psi\rangle$

encoded Clifford

(If P anticom with N instead of $\bar{X}_1$, similar procedure using N instead of $\bar{X}_1$.)

eg. $S: \begin{cases} Q_1 = XXXX \\ Q_2 = ZZZZ \end{cases}$

$N(S)/S: \begin{cases} \bar{X}_1 = XX11, & \bar{Z}_1 = 1Z1Z \\ \bar{X}_2 = X1X1, & \bar{Z}_2 = 11ZZ \end{cases}$

$P = YY11, \quad b = +$

- We find $\bar{X}_2$ anticom with P, use $\bar{X}_2$ as special op in step ②
- Going over all $\bar{X}_i, \bar{Z}_i$ for $i \neq 2$,
  here, checking $\bar{X}_1, \bar{Z}_1$:
  - $\bar{X}_1$ com with P ; $\bar{X}_1' = \bar{X}_1 = XX11$
  - $\bar{Z}_1$ anti com with P ; $\bar{Z}_1' = \bar{Z}_1 \cdot \bar{X}_2 = (1Z1Z)\cdot(X1X1) = XZXZ$.

  NB: $\bar{X}_1', \bar{Z}_1'$ com with Q_1, Q_2, P, anti-com with one another.
- $S': \begin{cases} Q_1 = XXXX \\ Q_2 = ZZZZ \\ P = YY11 \end{cases}$
- $N(S')/S': \begin{cases} \bar{X}_1' = XX11 \\ \bar{Z}_1' = XZXZ \end{cases}$

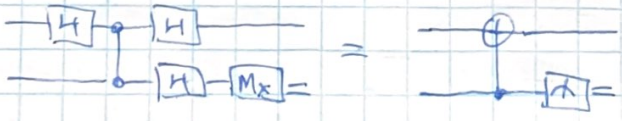
Of course, $\bar{X}_2, \bar{Z}_2$ now removed from $N(S')/S'$.

- What encoded operation has been achieved?

  $\bar{X}_1 \to \bar{X}_1$
  $\bar{Z}_1 \to \bar{Z}_1\bar{X}_2$
  $\bar{X}_2, \bar{Z}_2$ gone
  $YY11 = \bar{X}_1\bar{Z}_2 Q_2$ meas

Compare:

$\bar{X}_1$	$\bar{Z}_1$	$\bar{Z}_1$	$\bar{X}_1$
$\bar{Z}_1$	$\bar{X}_1$	$\bar{X}_1\bar{Z}_2$	$\bar{Z}_1\bar{X}_2$
$\bar{X}_2$	$\bar{X}_2$	$\bar{Z}_1\bar{X}_2$	$\bar{X}_1\bar{Z}_2$
$\bar{Z}_2$	$\bar{Z}_2$	$\bar{Z}_2$	$\bar{X}_2$
$\bar{H}I$		Controlled $-\bar{Z}$	$\bar{H}\bar{H}$

Encoded circuit: 

Case ⑤ $P \notin N(S)$

- Then $c(P, Q_i) = 1$ for some i
- $\forall |\psi\rangle \in T(S)$, Prob(meas outcome $= \pm$)

$$= \mathrm{Tr}\left[|\psi\rangle\langle\psi| \tfrac{1}{2}(I \pm P)\right]$$

$$= \tfrac{1}{2} \pm \tfrac{1}{2}\langle\psi|P|\psi\rangle, \quad \text{but } \langle\psi|P|\psi\rangle = \langle\psi|PQ_i|\psi\rangle$$

$$= -\langle\psi|Q_iP|\psi\rangle$$

$$= -\langle\psi|P|\psi\rangle = 0.$$

$\therefore$ outcome is random and indep of $|\psi\rangle$.

Let outcome $= b \in \{+, -\}$. $\therefore bP \in S'$.

Reorganize S and $N(S)/S$ as follows.

$\forall j \neq i$, if $c(Q_j, P) = \begin{cases} 0 \\ 1 \end{cases}$ then $\begin{matrix} Q_j' = Q_j \\ Q_j' = Q_jQ_i \end{matrix}$

$\forall j = 1, \ldots, k$ if $c(\bar{X}_j, P) = \begin{cases} 0 \\ 1 \end{cases}$ then $\begin{matrix} \bar{X}_j' = \bar{X}_j \\ \bar{X}_j Q_i \end{matrix}$

if $c(\bar{Z}_j, P) = \begin{cases} 0 \\ 1 \end{cases}$ then $\begin{matrix} \bar{Z}_j' = \bar{Z}_j \\ \bar{Z}_j Q_i \end{matrix}$

S: $Q_1', \ldots, Q_{i-1}, \boxed{Q_i}, Q_{i+1}', \ldots, Q_{n-k}$ —meas P→ S': $Q_1', \ldots, Q_{i-1}, \boxed{b \cdot P}, Q_{i+1}', \ldots, Q_{n-k}$

$N(S)/S$: $\bar{X}_1', \ldots, \bar{X}_k', \bar{Z}_1', \ldots, \bar{Z}_k'$ → $N(S')/S'$: $\bar{X}_1', \ldots, \bar{X}_k', \bar{Z}_1', \ldots, \bar{Z}_k'$.

↑ all but Q_i com with P!

Recipe:
- Starting from S, find Q_i anti-com with P.
- For any Q_j, $j \neq i$ or encoded Pauli, if anti com w/ P multiply Q_i to it.
- Replace Q_i by $b \cdot P$

eg. 5 qubit code, meas $P = XZ111$

$Q_1 = XZZXI$
$Q_2 = IXZZX$
$Q_3 = XIXZZ$
$Q_4 = ZXIXZ$

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

Q_1 anticom with P. Use Q_1 as "Q_1 in the recipe".

$C(Q_1, P) = 1$
$C(Q_2, P) = 1$
$C(Q_3, P) = 1$
$C(Q_4, P) = 0$
$C(\bar{X}, P) = 0$
$C(\bar{Z}, P) = 1$

$\therefore S' = \{ bP = b \cdot XZ111,\ Q_2' = Q_2 Q_1 = XYIYX,\ Q_3' = Q_3 Q_1 = IZYYZ,\ Q_4' = Q_4 = ZXIXZ \}$

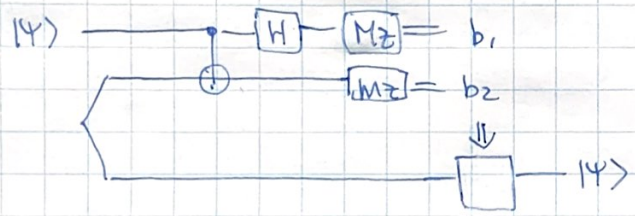
$N(S')/S' = \{ \bar{X}' = \bar{X} = XXXXX,\ \bar{Z}' = \bar{Z} Q_1 = YIIYZ \}$

In case ©, meas $P \notin N(S)$ changes the "code".

Gottesman–Knill theorem: Given initial stabilizer state, circuit of m Clifford operations, and Pauli measurements, outcome statistics can be simulated in $O(n^3 \cdot m)$ time.

Can improve to $O(n^2 m)$ time.

Final example: teleportation. $n=3$



S: $Q_1 = 1XX$, $Q_2 = 1ZZ$ $\xrightarrow{CNOT_{12}}$ $1XX$, ZZZ $\xrightarrow{H_1}$ $1XX$, XZZ

N(S)/S: $\bar{X} = X11$, $\bar{Z} = Z11$ → $XX1$, $Z11$ → $ZX1$, $X11$ } anticom with $Z11$

↓ meas $Z11$, take $Q_i = XZZ$

b_2 $1Z1$, b_1 $Z11$ ← meas $1Z1$, take $Q_i = 1XX$ ← $1XX$, $b_1 \cdot Z11$

$11X \sim Z1X = (ZX1)(1XX)$ → $ZX1$

$11Z \sim 1ZZ$ → $1ZZ$

∴ "Encoded" qubit ⊗ $\frac{1}{\sqrt{2}}(|100\rangle + |111\rangle) \rightarrow |b_1\rangle |b_2\rangle \otimes$ "Encoded" qubit.