QIC 890 / CO781 / CS 867, W22

Lec 6 Clifford group

Consider a stabilizer S, any $|\psi\rangle \in T(S)$, U unitary.

Qn: What operators stabilize $U|\psi\rangle$? (Call the set S'')

Let $S' = \{ UMU^{+} : M \in S \}$ (Abelian group, $|S| = |S'|$)

$$\forall M \in S, \quad (UMU^{+}) \cdot (U|\psi\rangle) = UM|\psi\rangle = U|\psi\rangle \quad \therefore S' \subseteq S''.$$

· Nice if S' consists of Pauli's; even nicer if U conjugates Paulis to Paulis.

Def [Clifford group on n qubits]:

$$\mathcal{C}_n = \{ U \in U(2^n) : UPU^{+} \in \mathcal{P}_n \ \forall P \in \mathcal{P}_n \}$$

Obs: For a stabilizer $S \subseteq \mathcal{P}_n$, $U \in \mathcal{C}_n$, $\Sigma[U(T(S))] = S' =: USU^{+}$

Stabilizer of space after U acts on codespace defined by S

Pf: We saw $S' \subseteq \Sigma[U(T(S))]$ above.

$$|S| = |S'| \leq |\Sigma[U(T(S))]|$$

Now apply U^{+} to $U(T(S))$, so the revised stabilizer is S.

By the same argument $|\Sigma[U(T(S))]| \leq |S|$.

$\therefore$ Both inequalities must be equalities.

Ex: Check that the Clifford "group" is a group.

Consider the mapping on $\mathcal{P}_n$ due to conjugation by $U \in U(2^n)$:

$$M_U : \mathcal{P}_n \to U(2^n)$$
$$P \mapsto U P U^\dagger$$

Properties of M_U:

① Homomorphic: $PQ \mapsto U(PQ)U^\dagger = (UPU^\dagger)(UQU^\dagger)$

② Injective: $UPU^\dagger = UQU^\dagger \Rightarrow P = Q$

$\therefore$ Restricting the range $\mathcal{P}_n \to U\mathcal{P}_n U^\dagger$ gives a bijection.

Cor: For $U \in \mathcal{C}_n$, M_U is a permutation on $\mathcal{P}_n$.

③ Preserves $c(P,Q)$: If $QP = c(P,Q)\, PQ$

then $UQU^\dagger UPU^\dagger = UQPU^\dagger = c(P,Q)\, UPQU^\dagger$
$= c(P,Q)\, UPU^\dagger UQU^\dagger$

<u>Remarks</u>:

- Because of ①, M_U is determined by its action on the generators of $\mathcal{P}_n$.
- Because of ③, the action on the generators are restricted.

* Conversely, a map for the generators respecting com/anticom relations specifies a unitary U (up to a phase) s.t. M_U extends the map. (See page)

* Condition ① $\Rightarrow$ indep of the images for the generators but indep is not explicitly needed as a hypothesis for the above converse.

Examples of Clifford group gates:

eg1 $\forall n, \forall \theta, \quad e^{i\theta} I \in C_n$

eg2 $\forall n, \quad P_n \subseteq C_n$.

Def: $\hat{C}_n := C_n / \{e^{i\theta} I\}$

$\check{C}_n := \hat{C}_n / \hat{P}_n$

When $V \in P_n$, $M_V(Q) = \pm Q$.
Each $U \in C_n$ can be a two step process:
① Picking $M_W(G_i) \in \hat{P}_n$ for generators G_i of P_n where $W \in \check{C}_n$
② Picking signs of each $M_W(G_i)$, which is effected by conjugation by some $V \in \hat{P}_n$.

So $U = VW$. (See page ---)

eg3 $n=1$, $H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} = \frac{1}{\sqrt{2}}(X+Z)$

Then $\left.\begin{array}{l} HXH = Z \\ HZH = X \end{array}\right\} (*)$

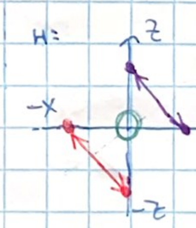
And $HYH = H(iXZ)H = i\, HXH\, HZH = iZX = -Y$ determined by $(*)$

NB: If we want $UXU^\dagger = Z$
$UXU^\dagger = -X$

take $U = ZH$.

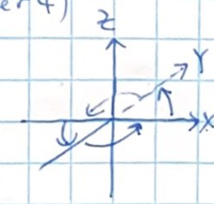
Then $UXU^\dagger = Z\underline{HXH}Z = ZZZ = Z$
$UZU^\dagger = Z\underline{HZH}Z = ZXZ = -X$

Again $UYU^\dagger$ fixed, $UYU^\dagger = Y$.



(order 2)

(order 4)

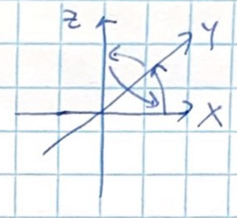


eg4. $n=1$, $U = R_{\frac{\pi}{4}} = e^{-i\frac{\pi}{4}Z}$

Then $UXU^\dagger = Y$
$UZU^\dagger = Z$

And $UYU^\dagger = U(iXZ)U^\dagger = i\, UXU^\dagger\, UZU^\dagger = iYZ = -X$

eg 5 We will see $\exists U$ s.t. $UXU^\dagger = Y$
$(n=1)$ $UYU^\dagger = Z$
$UZU^\dagger = X$

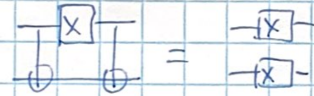
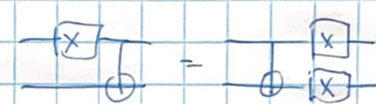


order 3.

eg 6 $n=2$. $U = CNOT_{12} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Z$.

$$\left.\begin{aligned} U\,X1\,U^\dagger &= XX \\ U\,Z1\,U^\dagger &= Z1 \\ U\,1X\,U^\dagger &= 1X \\ U\,1Z\,U^\dagger &= ZZ \end{aligned}\right\} (*)$$

time $\rightarrow$

Useful later:  means 

ie CNOT propagate X error from control to target.

CNOT . . . Z error from target to control.

Notation: (*) often written as:
$X1 \to XX$
$Z1 \to Z1$
$1X \to 1X$
$1Z \to ZZ$

note also still anti com

and each in first group com with each in 2nd group.

eg 7 $n=2$, $U = SWAP$, $U \in C_2$.
$X1 \to 1X$
$Z1 \to 1Z$
$1X \to X1$
$1Z \to Z1$

eg 8 $n=2$, $U = \text{controlled-}Z = \begin{bmatrix} 1 & & & 0 \\ & 1 & & \\ & & 1 & \\ 0 & & & -1 \end{bmatrix}$.
$U = (I \otimes H)\, CNOT_{12}\, (I \otimes H)$
$(\because Z = HXH)$.

$$\therefore \begin{array}{lllll} X1 & \xrightarrow{IH} X1 & \xrightarrow{CNOT_{12}} XX & \xrightarrow{IH} & XZ \\ Z1 & \longrightarrow Z1 & \longrightarrow Z1 & \longrightarrow & Z1 \\ 1X & \longrightarrow 1Z & \longrightarrow ZZ & \longrightarrow & ZX \\ 1Z & \longrightarrow 1X & \longrightarrow 1X & \longrightarrow & 1Z \end{array}$$

(in fact, C-Z diagonal, com with Z1)

(again, C-Z com with 1Z).

Thm. Let $f : \mathcal{P}_n \to U(2^n)$ be a gp homomophism

$\forall i = 1, 2, \ldots, n$, Let $X_i = I^{\otimes i-1} \; X \; I^{\otimes n-i}$
$Z_i = I^{\otimes i-1} \; Z \; I^{\otimes n-i}$

$\bar{X}_i = f(X_i)$, $\bar{Z}_i = f(Z_i)$

If $\forall i, j$, $c(\bar{X}_i, \bar{X}_j) = c(\bar{Z}_i, \bar{Z}_j) = 0$
$c(\bar{X}_i, \bar{Z}_j) = \delta_{ij}$

Then $\exists U \in U(2^n)$ s.t. $\forall P \in \mathcal{P}_n$, $f(P) = UPU^\dagger$.

Furthermore, we can determine U up to an overall phase.

NB: it means, $\underbrace{\text{2n images}}_{\bar{X}_i, \bar{Z}_i}$ with correct com/anticom relations specify

a unitary whose conjugation map realizes the gp homo.

Lemma: Let $U, V \in U(2^n)$
If $\forall P \in \mathcal{P}_n$, $UPU^\dagger = VPV^\dagger$
then $U = e^{i\theta} V$ for some θ.

Pf: Let $W = V^\dagger U$. It suffices to show if $\forall P \in \mathcal{P}_n$, $WPW^\dagger = P$ $\leftarrow (*)$
then $W = e^{i\theta} I$.

From $(*)$, $\forall P \in \mathcal{P}_n$, $P^\dagger W P = W$ $\leftarrow (\ddagger)$

But for any 2×2 matrix M, $M + XMX + YMY + ZMZ \propto I$
$\therefore$ for any $2^n \times 2^n$ matrix M, $\sum_{P \in \mathcal{P}_n} P^\dagger M P \propto I$.

So $\sum_{P \in \mathcal{P}_n} P^\dagger W P \propto I$
$\parallel$
W by $(\ddagger)$ $\quad \therefore W \propto I \quad \therefore W = e^{i\theta} I$ for some θ.

$\therefore$ Uniqueness in Thm is proved.

Pf (thm):

- Procedure to determine U:

① Define $|\Psi_0\rangle \propto \prod_{i=1}^{n} \left(\frac{I+\bar{Z}_i}{2}\right) |\alpha\rangle$, for any $|\alpha\rangle$ s.t. RHS $\neq 0$. Take $\| |\Psi_0\rangle \| = 1$.

② Let $b = b_1 b_2 \cdots b_n$ be an n-bit string. Let $\tilde{X}(b) = \prod_{i=1}^{n} (\bar{X}_i)^{b_i}$.

③ Let $|\Psi_b\rangle = \tilde{X}(b) |\Psi_0\rangle$.

④ Let $U = \sum_b |\Psi_b\rangle\langle b|$.

- Intuition:

$$\begin{tikzcd}
\prod_{i=1}^{n}\left(\frac{I+Z_i}{2}\right)|\beta\rangle \propto |0\rangle^{\otimes n} \arrow[r, "\prod_{i=1}^{n}(X_i)^{b_i}"] \arrow[d, "U"] & |b\rangle \arrow[d, "U"] \\
\prod_{i=1}^{n}\left(\frac{I+\bar{Z}_i}{2}\right)|\alpha\rangle \propto |\Psi_0\rangle \arrow[r, "\prod_{i=1}^{n}(\bar{X}_i)^{b_i}"] & |\Psi_b\rangle
\end{tikzcd}$$

- Verifying $\sum_b |\Psi_b\rangle\langle b|$ is a valid U:

ⓐ U is unitary iff $\{|\Psi_b\rangle\}$ is an orthonormal basis.

(i) If $b \neq b'$ $\exists j$ s.t. $b_j \neq b'_j$.

Then
$$\begin{aligned}
\langle \Psi_b | \Psi_{b'} \rangle &= \langle \Psi_0 | \prod_{i=1}^{n} (\bar{X}_i)^{b_i + b'_i} |\Psi_0\rangle \\
&= \langle \Psi_0 | \prod_{i=1}^{n} (\bar{X}_i)^{b_i + b'_i} \bar{Z}_j |\Psi_0\rangle \\
&= (-1) \langle \Psi_0 | \bar{Z}_j \prod_{i=1}^{n} (\bar{X}_i)^{b_i + b'_i} |\Psi_0\rangle \\
&= (-1) \langle \Psi_0 | \prod_{i=1}^{n} (\bar{X}_i)^{b_i + b'_i} |\Psi_0\rangle = 0
\end{aligned}$$

$\therefore$ The $|\Psi_b\rangle$'s are mutually orthogonal.

(ii) Also, $\bar{X}(b)$ unitary $\therefore \| |\Psi_b\rangle \| = \| |\Psi_0\rangle \| = 1 \quad \forall b$.

$\therefore \{|\Psi_b\rangle\}_b$ is an orthonormal set.

(b) Verify $U X_i U^\dagger = \overline{X}_i$, $U Z_i U^\dagger = \overline{Z}_i$.

(i) $\forall b$, $U Z_i U^\dagger |\psi_b\rangle = U Z_i |b\rangle = (-1)^{b_i} U|b\rangle = (-1)^{b_i} |\psi_b\rangle$

$$\overline{Z}_i |\psi_b\rangle = \overline{Z}_i \tilde{X}(b) |\psi_0\rangle = (-1)^{b_i} \tilde{X}(b) \overline{Z}_i |\psi_0\rangle = (-1)^{b_i} \tilde{X}(b) |\psi_0\rangle = (-1)^{b_i} |\psi_b\rangle$$

$\because$ $U Z_i U^\dagger$ and $\overline{Z}_i$ act the same on a basis, $U Z_i U^\dagger = \overline{Z}_i$.

The case for $U X_i U^\dagger = \overline{X}_i$: exercise.

Obs: For any $2n$ bits $a_1 a_2 \cdots a_n\ b_1 b_2 \cdots b_n$
the group homomorphism defined by: $X_i \mapsto (-1)^{a_i} X_i$
$Z_i \mapsto (-1)^{b_i} Z_i$

can be implemented by $M_W : P \mapsto W P W^\dagger$ for $W = \bigotimes_{j=1}^{n} X_j^{b_j} Z_j^{a_j}$.

Cor: For $U \in \hat{C}_n$, we can specify M_U by

① $\overline{X}_i, \overline{Z}_i \in \hat{P}_n$ for $i = 1, 2, \ldots, n$ (implemented by $V \in \check{C}_n$)
② $a_1, \ldots, a_n, b_1, \ldots b_n \in \{0, 1\}$ (implemented by $W \in \hat{P}_n$)

Then $U = VW$.

NB Step ① in procedure requires $\overline{Z}_i$'s be commuting.
② $\overline{X}_i$'s

Unitarity of U requires $\{X_i, Z_j\} = \delta_{ij}$.

NB Specifying $U \in \hat{C}_n$ in Cor takes $2n^2 + 2n$ bits $\ll$ size of U $(2^n \times 2^n)$.

Encoded Clifford gates for stabilizer codes:

Recall a valid logical operation U satisfies $U Q U^\dagger \in S$ $\forall$ generator Q

$U S U^\dagger = S$

Logical Clifford: can permute elements within S

also permute elements in $N(S)/S$.

$N(S)$: each N commutes with each $M \in S$.

$\therefore N M N^\dagger = M$

ie fixes each M by conjugation

S: each $M \in S$ fixes each $|\psi\rangle \in T(S)$

But $N(S)/S \cong$ logical Pauli's.

$\therefore$ contains N that do not fix the state $|\psi\rangle \in T(S)$

When proposing logical Clifford gates $\bar{U}$ for a stabilizer code, check:

① $\bar{U} Q \bar{U}^\dagger \in S$ $\forall Q$ generator for S

② $\bar{U} \bar{X}_i \bar{U}^\dagger$, $\bar{U} \bar{Z}_i \bar{U}^\dagger$ transform according to the Clifford gate eg 1 5-qubit code

$$G_1 = X\ Z\ Z\ X\ 1$$
$$G_2 = 1\ X\ Z\ Z\ X$$
$$G_3 = X\ 1\ X\ Z\ Z$$
$$G_4 = Z\ X\ 1\ X\ Z$$

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

$$\bar{H} \stackrel{?}{=} U = H\ H\ H\ H\ H$$

Unfortunately no. $U \bar{X} U^\dagger = \bar{Z}$, $U \bar{Z} U^\dagger = \bar{X}$

but $U G_1 U^\dagger = Z\ X\ X\ Z\ 1$

Ex: show that no $a_1\ a_2\ a_3\ a_4$ make $G_1^{a_1} G_2^{a_2} G_3^{a_3} G_4^{a_4} = Z X X Z 1$

So $U G_1 U^\dagger \notin S$ $\therefore$ $U = H^{\otimes 5}$ does not preserve the code space

$\therefore$ not a valid logical operator, despite the action on $N(S)/S$ is correct.

eg 7-qubit code

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

$Q_4 = I\ I\ I\ Z\ Z\ Z\ Z$
$Q_5 = 1\ Z\ Z\ 1\ 1\ Z\ Z$
$Q_6 = Z\ 1\ Z\ 1\ Z\ 1\ Z$

$\bar{X} = X\ X\ X\ X\ X\ X\ X$

$\bar{Z} = Z\ Z\ Z\ Z\ Z\ Z\ Z$

- Consider $U = H^{\otimes 7}$, $HXH = Z$, $HZH = X$

Then $UQ_1U^+ = Q_4$, $UQ_4U^+ = Q_1$
$UQ_2U^+ = Q_5$, $UQ_5U^+ = Q_2$
$UQ_3U^+ = Q_6$, $UQ_6U^+ = Q_3$ $\therefore \forall i\ UQ_iU^+ \in S$

$\therefore$ U is an encoded operation.

Also $U\bar{X}U^+ = \bar{Z}$, $U\bar{Z}U^+ = \bar{X}$.

By Thm, $U = \bar{H}$ up to an overall phase.

- Consider $U = R_{\frac{\pi}{4}}^{\otimes 7}$, $UXU^+ = Y$, $UZU^+ = Z$ $(Y = iXZ)$

Then $UQ_1U^+ = 1\ 1\ 1\ Y\ Y\ Y\ Y$

$= 1\ 1\ 1\ (iXZ)\ (iXZ)\ (iXZ)\ (iXZ)$

$= (1\ 1\ 1\ X\ X\ X\ X)\ (1\ 1\ 1\ Z\ Z\ Z\ Z) = Q_1 Q_4$

Similarly $UQ_2U^+ = 1\ Y\ Y\ 1\ 1\ Y\ Y = Q_2 Q_5$
$UQ_3U^+ = Y\ 1\ Y\ 1\ Y\ 1\ Y = Q_3 Q_6$

$UQ_iU^+ = Q_i$ for $i = 4, 5, 6$.

$\therefore \forall i\ UQ_iU^+ \in S$, and U is an encoded operation.

$U\bar{X}U^+ = Y^{\otimes 7} = (iXZ)^{\otimes 7} = i^7\,\bar{X}\bar{Z} = -i\bar{X}\bar{Z} = -i\bar{Y}$
$U\bar{Z}U^+ = Z^{\otimes 7} = \bar{Z}$.

$\therefore U = \bar{R}_{\frac{\pi}{4}}^{\,+} = \bar{R}(-\frac{\pi}{4})$.

- Before analyzing $CNOT^{\otimes 7}$, how to encode 2 qubits into 2 blocks of 7-qubit codes?

  What is the stabilizer, and the encoded Paulis?

- General proposition:

  Consider a stabilizer S with generators $Q_1, Q_2, \ldots, Q_r$ encoding k qubits into n qubits ($k = n - r$), with encoded Pauli's $\bar{X}_i, \bar{Z}_i$ for $i = 1, 2, \ldots, k$.

  Consider a stabilizer S' with generators $G_1, G_2, \ldots, G_{r'}$ encoding k' qubits into n' qubits ($k' = n' - r'$), with encoded Pauli's $\bar{X}'_j, \bar{Z}'_j$ for $j = 1, 2, \ldots, k'$.

  Then the combined code encodes $k + k'$ qubits into $n + n'$ qubits, with stabilizer generated by $r + r'$ generators:

$$
\begin{array}{ll}
Q_1 \otimes I^{\otimes n'}, & I^{\otimes n} \otimes G_1 \\
Q_2 \otimes I^{\otimes n'}, & I^{\otimes n} \otimes G_2 \\
\vdots & \vdots \\
Q_r \otimes I^{\otimes n'}, & I^{\otimes n} \otimes G_{r'}
\end{array}
$$

  and encoded Pauli group generated by:

$$
\begin{array}{ll}
\bar{X}_1 \otimes I^{\otimes n'}, & I^{\otimes n} \otimes \bar{X}'_1 \\
\vdots & \vdots \\
\bar{X}_k \otimes I^{\otimes n'}, & I^{\otimes n} \otimes \bar{X}'_{k'} \\
 & \\
\bar{Z}_1 \otimes I^{\otimes n'}, & I^{\otimes n} \otimes \bar{Z}'_1 \\
\vdots & \vdots \\
\bar{Z}_k \otimes I^{\otimes n'}, & I^{\otimes n} \otimes \bar{Z}'_{k'}
\end{array}
$$

For 2 blocks of 7 qubit code, stabilizer generators are:

$Q_1 \otimes I^{\otimes 7} = 111XXXX\ 1111111 = J_1$ $\qquad \bar{X}_1 = X^{\otimes 7} \otimes I^{\otimes 7}$

$Q_2 \otimes I^{\otimes 7} = 1XX11XX\ 1111111 = J_2$ $\qquad \bar{X}_2 = I^{\otimes 7} \otimes X^{\otimes 7}$

$Q_3 \otimes I^{\otimes 7} = X1X1X1X\ 1111111 = J_3$ $\qquad \bar{Z}_1 = Z^{\otimes 7} \otimes I^{\otimes 7}$

$Q_4 \otimes I^{\otimes 7} = 111ZZZZ\ 1111111 = J_4$ $\qquad \bar{Z}_2 = I^{\otimes 7} \otimes Z^{\otimes 7}$

$Q_5 \otimes I^{\otimes 7} = 1ZZ11ZZ\ 1111111 = J_5$

$Q_6 \otimes I^{\otimes 7} = Z1Z1Z1Z\ 1111111 = J_6$

$I^{\otimes 7} \otimes Q_1 = 1111111\ 111XXXX = J_7$

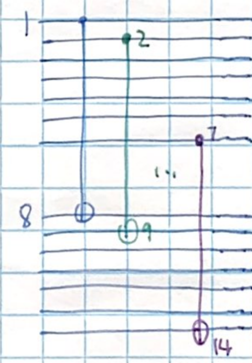
$I^{\otimes 7} \otimes Q_2 = 1111111\ 1XX11XX = J_8$

$I^{\otimes 7} \otimes Q_3 = 1111111\ X1X1X1X = J_9$

$I^{\otimes 7} \otimes Q_4 = 1111111\ 111ZZZZ = J_{10}$

$I^{\otimes 7} \otimes Q_5 = 1111111\ 1ZZ11ZZ = J_{11}$

$I^{\otimes 7} \otimes Q_6 = 1111111\ Z1Z1Z1Z = J_{12}$



- Let $U = CNOT_{18} \otimes CNOT_{29} \otimes \cdots \otimes CNOT_{7\,14}$

Then $U J_1 U^{+} = 111XXXX\ 111XXXX = J_1 J_7$

recall CNOT X1 CNOT = XX

$U J_2 U^{+} = J_2 J_8$

$U J_3 U^{+} = J_3 J_9$

$U J_i U^{+} = J_i$ for $i = 4, 5, 6, 7, 8, 9$.

$U J_{10} U^{+} = 111ZZZZ\ 111ZZZZ = J_4 J_{10}$

CNOT 1Z CNOT = ZZ

$U J_{11} U^{+} = J_5 J_{11}$

$U J_{12} U^{+} = J_6 J_{12}$ $\qquad \therefore U$ is a encoded operator.

Also $U \bar{X}_1 U^{+} = X^{\otimes 7} \otimes X^{\otimes 7} = \bar{X}_1 \bar{X}_2$, $\quad U \bar{Z}_1 U^{+} = Z^{\otimes 7} \otimes I^{\otimes 7} = \bar{Z}_1$

$U \bar{X}_2 U^{+} = I^{\otimes 7} \otimes X^{\otimes 7} = \bar{X}_2$, $\quad U \bar{Z}_2 U^{+} = Z^{\otimes 7} \otimes Z^{\otimes 7} = \bar{Z}_1 \bar{Z}_2$

$\therefore U = \overline{CNOT}_{\bar{1}\bar{2}}$.

Summary: for the 7-qubit code, encoded X, Z, $R_{\frac{\pi}{4}}^{-1}$, H, CNOT can be performed transversally (crucial for fault-tolerance).

Def: a transversal operation does not interact different qubits within a code block.

Obs: ① These operations are "bitwise", being tensor power of a physical op, which is symmetric over the qubits in the code block.

This may have implementation / cryptographic advantages.

② $R_{\frac{\pi}{4}}$, H, CNOT generate the Clifford group!

Thm: If $U \in C_n$, then $U \in \langle e^{i\theta} I, H_i, R_{\frac{\pi}{4}i}, \mathrm{CNOT}_{ij\,(i<j)} \rangle$.

which qubit(s) the gates act on

ie the Clifford group is generated (multiplicatively) by H, $R_{\frac{\pi}{4}}$, CNOT.

Pf idea: Note that $R_{\frac{\pi}{4}}^2 \propto Z$, so, H, $R_{\frac{\pi}{4}}$ generate the Pauli subgroup.

Recall $\hat{C}_n = C_n / \langle e^{i\theta} I \rangle$, $\check{C}_n = \hat{C}_n / \hat{P}_n$, focus on $\check{C}_n$.

specify $U \in \hat{C}_n$ by $f(X_i) = U X_i U^\dagger$, $f(Z_i) = U Z_i U^\dagger$, $i = 1, \ldots, n$.

Switch to symplectic rep: $v_{f(X_i)} = (x_{f(X_i)}, z_{f(X_i)})$

$v_{f(Z_i)} = (x_{f(Z_i)}, z_{f(Z_i)})$

The map f (from $\hat{P}_n$ to $\hat{P}_n$) induces a linear transf on $(\mathbb{Z}_2)^{2n}$:

$$\begin{array}{c} n \\ n \end{array} \left[\begin{array}{c|c} x_{f(X_i)} & x_{f(Z_i)} \\ \hline z_{f(X_i)} & z_{f(Z_i)} \end{array}\right] \begin{bmatrix} x_p \\ z_p \end{bmatrix} = \begin{bmatrix} x_{UPU^\dagger} \\ z_{UPU^\dagger} \end{bmatrix}$$

$\leftarrow n \rightarrow \quad \leftarrow n \rightarrow$

ith col $= v_{f(X_i)}$ ith col $= v_{f(Z_i)}$

eg H_1 is represented by : $\left[\begin{array}{c|c|c|c} 0 & 0 \cdots 0 & 1 & 0 \cdots 0 \\ \hline 0 & & 0 & \\ \vdots & I & \vdots & O \\ 0 & & 0 & \\ \hline 1 & 0 \cdots 0 & 0 & 0 \cdots 0 \\ \hline 0 & & 0 & \\ \vdots & O & \vdots & I \\ 0 & & 0 & \end{array}\right]$ (swaps X_1 & Z_1 leaves the rest invariant)

$(R_{\frac{\pi}{4}})_1$ is represented by : $\left[\begin{array}{c|c|c} 1 & 0 \cdots 0 & \\ \hline 0 & & \\ 0 & I & O \\ \vdots & & \\ 0 & & \\ \hline 1 & 0 \cdots 0 & \\ \hline 0 & & I \\ 0 & O & \\ \vdots & & \\ 0 & & \end{array}\right]$ (takes X_1 to iX_1Z_1 leaves the rest invariant)

$(CNOT)_{12}$ is rep by : $\left[\begin{array}{c|c|cc|c} 1 & 0 \cdots 0 & & & \\ \hline 1 & & & & \\ 0 & I & & & O \\ \vdots & & & & \\ 0 & & & & \\ \hline 0 & 0 \cdots 0 & 1 & 1 & 0 0 \cdots \\ 0 & & 0 & 1 & 0 0 \cdots \\ \vdots & O & 0 & 0 & \\ & & \vdots & \vdots & I \\ 0 & & 0 & 0 & \end{array}\right]$ (takes X_1 to X_1X_2, Z_2 to Z_1Z_2 leaves the rest inv)

- Call the symplectic rep of $U \in \check{C}_n$ $\mathbb{S}(U)$.
- Columns of $\mathbb{S}(U)$ satisfy symplectic inner product governed by (anti) com relations of the Pauli's.
- Left multiplications by $\mathbb{S}(H_i)$, $\mathbb{S}(R_{\frac{\pi}{4}i})$, $\mathbb{S}(CNOT_{ij})$ corr to special row operations, right multiplication corr to column operations.
- $\mathbb{S}(U) \cdot \mathbb{S}(V) = \mathbb{S}(UV)$
- These row / col operations preserve the full rank of $\mathbb{S}(U)$, but can be chosen to strictly reduce the # of 1's.
- $\exists$ a sequence of these row / col operations to transform $\mathbb{S}(U)$ to I_{2n}.
  $\therefore \exists$ a sequence of $H, R, CNOT$ that left / right multiply to U resulting in $I \in \check{C}_n$.
  $O(n^2)$ of them

- $I \in \check{C}_n$ correspond to an operator $P \in \hat{P}_n$.

$\therefore$ $V_1 V_2 \ldots V_t \, U \, V_{t+1} \ldots V_r = P$ with $r \sim O(n^2)$

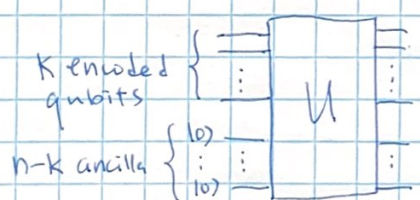
$\therefore$ $$U = V_t^\dagger \ldots V_2^\dagger V_1^\dagger P \, V_r^\dagger \, V_{r-1}^\dagger \ldots V_{t+1}^\dagger$$

where each V_k is H, $R_{\frac{\pi}{4}}$ or CNOT.

Remarks:

① Proof of thm is constructive

② We can obtain encoding circuit for any stabilizer code.
Say blocklength $= n$, # encoded qubits $= k$, $Q_1, Q_2 \ldots Q_{n-k}$ generate S.
$\bar{X}_i, \bar{Z}_i$ are logical Pauli's.



Want: $U X_i U^\dagger = \bar{X}_i$
$U Z_i U^\dagger = \bar{Z}_i$ for $i = 1, 2 \ldots k$

$U Z_j U^\dagger = Q_{j-k}$ for $j = k+1, k+2, \ldots, n$

Augment: $U X_j U^\dagger$ for $j = k+1, k+2, \ldots n$, preserving needed com/anticom relations.

Take $U X_i U^\dagger$, $U Z_i U^\dagger$ for $i = 1, \ldots, n$ and apply Thm to get sequence of R, H, CNOT.

Observation: $\mathcal{C}_n$ is not universal (it's a finite, discrete, group)

Thm (Nebe, Rains, Sloane, arXiv:math/0001038):

Add any $G \notin \mathcal{C}_n$ into $\mathcal{C}_n$ generates a dense set in $\mathcal{U}(2^n)$

ie $\{G, R_{\frac{\pi}{4}}, H, CNOT\}$ universal.

The C^k hierarchy:

Let $C^1 = \bigcup_n P_n$

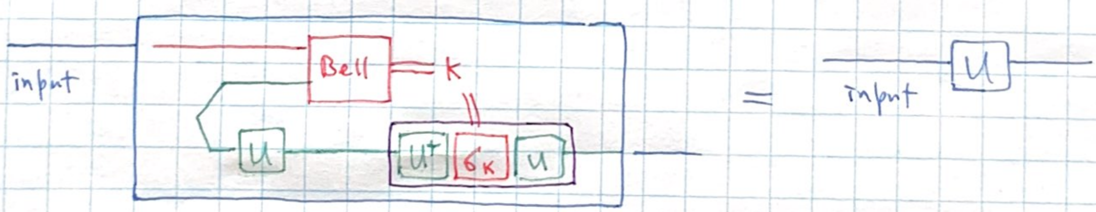
Let $C^2 = \bigcup_n \{U \in \mathcal{U}(2^n) : U P_n U^\dagger \subseteq P_n\} = \bigcup_n \{U \in \mathcal{U}(2^n) : U P_n U^\dagger \subseteq C^1\}$

Let $C^3 = \bigcup_n \{U \in \mathcal{U}(2^n) : U P_n U^\dagger \subseteq \mathcal{C}_n\} = \bigcup_n \{U \in \mathcal{U}(2^n) : U P_n U^\dagger \subseteq C^2\}$

$\vdots$

$C^k = \bigcup_n \{U \in \mathcal{U}(2^n) : U P_n U^\dagger \subseteq C^{k-1}\}$

Teleporting a C^3 gate:



① This box teleports, then apply U

② This box can be implemented with

ⓘ State $I \otimes U$ (max entangled state) ← Will learn more in part II

✓ ⓘⓘ Bell measurement (XX, ZZ)

✓ ⓘⓘⓘ $U \sigma_k U^\dagger$ which is Clifford!

More efficient schemes exist for CNOT, $R_{\frac{\pi}{8}}$, etc (1-bit teleportation)