Lec 6  Clifford group

Consider a stabilizer \( S \), any \( |14\rangle \in T(S) \), \( U \) unitary.

Qn: What operators stabilize \( U|14\rangle \)? (all the set \( S' \))

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

\[ \forall M \in S, \ (UMU^+)(U|14\rangle) = UMU|14\rangle = U|14\rangle \vdash S' \leq S''. \]

\( \vdash \) Nice if \( S' \) consists of Paulis; even nicer if \( U \) conjugates Paulis to Paulis.

Def: [Clifford group on \( n \) qubits]:

\[ C_n = \{ U \in U(2^n) : UPU^+ \in \mathbb{P}_n \ \forall P \in \mathbb{P}_n \} \]

Obs: For a stabilizer \( S \leq \mathbb{P}_n \), \( U \in C_n \), \( \Sigma U(T(S)) = S' = : USU^+ \)

[Stabilizer of space after \( U \) acts on codespace defined by \( S \)]

Pf: We saw \( S' \leq \Sigma U(T(S)) \) above.

\[ |S'| = |S'_{\Sigma} | \leq | \Sigma U(T(S)) | \]

Now apply \( U^* \) to \( U(T(S)) \), so the revised stabilizer is \( S' \).

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

Both inequalities must be equalities.

Ex: Check that the Clifford "group" is a group.
Consider the mapping on $\mathbb{P}_n$ due to conjugation by $U \in U(2^n)$:

$$\begin{align*}
\text{Mu: } \mathbb{P}_n & \rightarrow U(2^n) \\
\mathcal{P} & \rightarrow U \mathcal{P} U^* 
\end{align*}$$

Properties of Mu:

1. Homomorphic: $\mathcal{P} \mathcal{Q} \mapsto U(\mathcal{P} \mathcal{Q}) U^* = (U \mathcal{P} U^*) (U \mathcal{Q} U^*)$

2. Injective: $U \mathcal{P} U^* = U \mathcal{Q} U^* \Rightarrow \mathcal{P} = \mathcal{Q}$

.: Restricting the range $\mathbb{P}_n \rightarrow U \mathcal{P} U^*$ gives a bijection.

Cor: For $U \in C_n$, Mu is a permutation on $\mathbb{P}_n$.

3. Preserves $c(\mathcal{P}, \mathcal{Q})$: If $\mathcal{Q} \mathcal{P} = c(\mathcal{P}, \mathcal{Q}) \mathcal{P} \mathcal{Q}$

then $U \mathcal{Q} U^* U \mathcal{P} U^* = U \mathcal{Q} U \mathcal{P} U^* = c(\mathcal{P}, \mathcal{Q}) U \mathcal{P} U^* U \mathcal{Q} U^*$

Remarks:

- Because of (1), Mu is determined by its action on the generators of $\mathbb{P}_n$.
- Because of (3), the action on the generators are restricted.

* Conversely, a map for the generators respecting comm/anti-comm relations specifies a unitary $U$ (up to a phase) s.t. Mu 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:

eg.1 \( \forall n, \forall g, \ \ e^{i\theta} I \in C_n \)

eg.2 \( \forall n, \ P_n \subseteq C_n. \)

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

\( \gamma_n := \hat{C}_n / \hat{P}_n \)

When \( \forall g \in P_n, \ M_g(Q) = \pm Q \),

Each \( \forall N \in C_n \) can be a two step process:
1. Picking \( M_g(G_i) \in P_n \) for generators \( G_i \) of \( P_n \) where \( \forall g \in C_n \)
2. Picking signs of each \( M_w(G_i) \), which is affected by conjugation by some \( \forall v \in P_n \).

So \( U = U \in C_n \) (See page ... )

eg.3. \( n=1, \ H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}} (X+Z) \)

Then \( HXH = Z \quad HZH = X \)

And \( HYH = H (iXZ) H = \begin{pmatrix} 0 & iXZ \\ iXZ & 0 \end{pmatrix} \)

\( HXH HZH = iZX = -Y \) determined by (8)

NB. \( \forall \) we want \( UXU = Z \)

\( UXU^T = -X \)

Take \( U = X \)

Then \( UXU^T = UXZU^T = Z \)

\( UXU^T = -X \)

Again \( UXU^T \) fixed, \( UXU^T = Y \)

eg.4. \( n=1, \ U = R_{45} = e^{-i\pi/2} \)

Then \( UXU^T = Y \)

\( UXU^T = Z \)

And \( UXU^T = U(\frac{iXZ}{U})U^T = \frac{i}{U} UXU^T \frac{U}{U} = iYZ = -X \)
eg 5. We will see $U \in U_{st}$. $U X U^T = Y$
\[ (n=1) \]
$U Y U^T = \hat{Z}$
$U Z U^T = X$

eg 6. $n=2$. $U = CNOT_3 = 10 \times 01 \times I + 11 \times 11 \times Z$

\[
\begin{align*}
U X_1 U^T &= XX \\
U 21 U^T &= \hat{Z}1 \\
U 1X U^T &= \hat{1}X \\
U 12 U^T &= \hat{Z}2
\end{align*}
\]
Useful notations:
\[
\begin{align*}
\begin{array}{c}
\text{X} \\
\text{O}
\end{array} & = -iX \\
\text{O} & = \frac{1}{2}X
\end{align*}
\]
means:
\[
\begin{align*}
\begin{array}{c}
\text{X} \\
\text{O} \\
\text{X}
\end{array} & = \frac{1}{2}X \\
\text{O} & = \frac{1}{2}X
\end{align*}
\]

ie CNOT propagate X error from control to target.

\[
\begin{align*}
\begin{array}{c}
\text{O} \\
\text{O} \\
\text{X}
\end{array} & = \frac{1}{2}X
\end{align*}
\]
CNOT - - - 2 error from target to control.

Notation: $\otimes$ often written as:
\[
\begin{align*}
X 1 & \rightarrow XX \\
21 & \rightarrow \hat{Z}1 \\
1X & \rightarrow \hat{1}X \\
12 & \rightarrow \hat{Z}2
\end{align*}
\]

\[\text{Note also still want, com} \]
\[\text{and each in first group com} \]
\[\text{with each in 2nd group.} \]

eg 7. $n=2$, $U$: SWAP. $U \in U_2$.
\[
\begin{align*}
X 1 & \rightarrow X \\
21 & \rightarrow 12 \\
1X & \rightarrow X1 \\
12 & \rightarrow 21
\end{align*}
\]

eg 8. $n=2$, $U$: Controlled - $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$. 
$U = (I \otimes H) \ CNOT_{12} \ (I \otimes H) \\
\implies Z = HXH$.
\[
\begin{align*}
\begin{array}{c}
X \\
\text{H} \\
\text{X}
\end{array} & \rightarrow X \rightarrow XX \rightarrow X \hat{Z} \\
21 & \rightarrow 21 \rightarrow 21 \rightarrow 21 \\
1X & \rightarrow 12 \rightarrow 22 \rightarrow \hat{Z}X \\
12 & \rightarrow 1X \rightarrow 1X \rightarrow 12
\end{align*}
\]
\[\text{In fact, C2 diagonal, com with 21} \]
\[\text{again, C2 com with 12.} \]
Thm. Let \( f : \mathbb{P}_n \to U(2^n) \) be a cp homomorphism.

\[
\forall i = 1, 2, \ldots, n, \quad \text{let } X_i = I^{\otimes n-1} \otimes I^{\otimes n-1} \\
\overline{X}_i = (I^{\otimes n-1} \otimes I^{\otimes n-1}) \chi_i,
\]

\[
\overline{X}_i = f(x_i), \quad \overline{X}_i = f(z_i).
\]

If \( \forall i, j, \quad C(\overline{X}_i, \overline{X}_j) = C(\overline{X}_i, \overline{X}_j) = 0 \)
\[
C(\overline{X}_i, \overline{X}_j) = \delta_{ij}
\]

Then \( \exists U \in U(2^n) \) s.t. \( \forall P \in \mathbb{P}_n, \quad f(P) = UPU^* \).

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

NB: it means, 2\( n \) images with correct com/anticom relations specify a unitary whose conjugation map realizes the cp homo.

Lemma: Let \( U, V \in U(2^n) \)

If \( \forall P \in \mathbb{P}_n, \quad UPU^* = VPV^* \)

then \( U = e^{i\theta} V \) for some \( \theta \).

Pf: Let \( W = V^*U \). It suffices to show if \( \forall P \in \mathbb{P}_n, \quad WPW^* = P \quad \Box \)

then \( W = e^{i\theta} I \).

From \( \Box \), \( \forall P \in \mathbb{P}_n, \quad P^*WP = W \quad \Box \)

But for any \( 2^{\otimes 2^n} \) matrix \( M \), \( M + WMX + YMY + 2M^2 \leq I \)

\( \forall P \in \mathbb{P}_n \)

\[
\sum_{P \in \mathbb{P}_n} P^*WP \leq I
\]

So \( \sum_{P \in \mathbb{P}_n} P^*WP \leq I \)

By \( \Box \), \( I, W \leq I \)

\( W = e^{i\theta} I \) for some \( \theta \).

Uniqueness in Thm is proved.
Pf (Thm):

- Procedure to determine \( U \):
  1. Define \( |\psi_0\rangle \propto \prod_{i=1}^{n} \left( \frac{1 + \hat{x}_i}{2} \right) |\chi_i\rangle \), for any \( |\chi_i\rangle \) st. \( \text{RHS} \neq 0 \). Take \( \| |\psi_0\rangle \| = 1 \).
  2. Let \( b = b_1 b_2 \ldots b_n \) be an \( n \)-bit string. Let \( \hat{x}^{(b)} = \prod_{i=1}^{n} (\hat{x}_i)^{b_i} \).
  3. Let \( |\psi\rangle = \hat{x}^{(b)} |\psi_0\rangle \).
  4. Let \( U = \sum_{b} |\psi\rangle \langle b| \).

- Intuition:
  \[
  \prod_{i=1}^{n} \left( \frac{1 + \hat{x}_i}{2} \right) |\psi_0\rangle \propto 10^{\text{high}} \prod_{i=1}^{n} (\hat{x}_i)^{b_i} |\psi_0\rangle \]
  \[
  \downarrow \quad U \quad \downarrow \quad U
  \]
  \[
  \prod_{i=1}^{n} \left( \frac{1 + \hat{x}_i}{2} \right) |\psi_0\rangle \propto |\psi\rangle \prod_{i=1}^{n} (\hat{x}_i)^{b_i} |\psi_0\rangle \]

- Verifying \( \sum_{b} |\psi\rangle \langle b| \) is a valid \( U \):
  A. \( U \) is unitary \( \iff \{ |\psi_b\rangle \} \) is an orthonormal basis.

- (i) If \( b \neq b' \) \exists \ j \text{ st } b_j \neq b'_j,
  \[
  \text{Then } \langle \psi_b | \psi_{b'} \rangle = \langle \psi_0 | \prod_{i=1}^{n} (\hat{x}_i)^{b_i + b'_i} |\psi_0\rangle \]
  \[
  = \langle \psi_0 | \prod_{i=1}^{n} (\hat{x}_i)^{b_i} |\psi_0\rangle \prod_{i=1}^{n} (\hat{x}_i)^{b'_i} |\psi_0\rangle \]
  \[
  = (-1) \langle \psi_0 | \prod_{i=1}^{n} \hat{x}_j |\psi_0\rangle \prod_{i=1}^{n} \hat{x}_i |\psi_0\rangle \]
  \[
  = (-1) \langle \psi_0 | \prod_{i=1}^{n} (\hat{x}_i)^{b_i + b'_i} |\psi_0\rangle = 0.
  \]
  \( \therefore \) The \( |\psi_b\rangle \)'s are mutually orthogonal.

- (ii) Also, \( \hat{x}^{(b)} \) unitary \( \iff \| |\psi_b\rangle \| = 1 \), \( |\psi_b\rangle \| = 1 \iff b \).
  \( \therefore \{ |\psi_b\rangle \}_{b} \) is an orthonormal set.
6. Verify $UX_i U^\dagger = \bar{x}_i$, $U_2 U^\dagger = \bar{z}_i$.

(i) $\forall b, ~ U_2 U^\dagger 14_b = U_2 U^\dagger 1b = (\pm 1_i 1_b) U 1_b = (\pm 1_i 1_b) 14_b$

$\bar{z}_i 14_b = \bar{z}_i \tilde{x}(b) 14_b = (\pm 1_i \tilde{x}(b)) \bar{z}_i 14_b = (\pm 1_i \tilde{x}(b)) 14_b = (\pm 1_i 14_b)$

"$U_2 U^\dagger \text{ and } \bar{z}_i \text{ act the same on a basis, } U_2 U^\dagger = \bar{z}_i$.

The case for $UX_i U^\dagger = \bar{x}_i$: exercise.

Obs.: For any $2n$ bits $a_1 a_2 \ldots a_n b_1 b_2 \ldots b_n$

the group homomorphism defined by $X_i \mapsto (\pm 1_i X_i)$
$\bar{z}_i \mapsto (\pm 1_i \bar{z}_i)$

can be implemented by $M_W : P \mapsto WPW^\dagger$ for $W = \oplus_{j=1}^{n} a_j b_j \bar{z}_j$.

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

1. $X_i, \bar{z}_i \in \hat{P}_n$ for $i = 1, 2, \ldots, n$ (implemented by $V \in \hat{C}_n$)
2. $a_1, \ldots, a_n, b_1, \ldots, b_n \in \{0, 1\}$

Then $U = V W$.

NB. Step 1 in procedure requires $\bar{z}_i$'s be commuting.

Unitarity of $U$ requires $(X_i, \bar{z}_j) = \delta_{ij}$.

NB. Specifying $U \in \hat{C}_n$ in Cor takes $2n^2 + 2n$ bits < size of $U$ ($2^n \times 2^n$).
Encoded Clifford gates for stabilizer codes:

Recall a valid logical operation $U$ satisfies $U \in S \iff U^* U = S$, $U$ a generator of $S$.

- $U^* U = S$
- Logical Clifford: can permute elements within $S$
  - Also permute elements in $N(S)/S$.

$$N(S):$$
- Each $N$ commutes with each $M \in S$.
  - $N M N^* = M$
  - $N$ fixes each $M$ by conjugation.

$S$: each $M \in S$
- Fixes each $\langle \psi \rangle \in T(S)$

But $N(S)/S \cong \text{logical Pauli's}$.
- $S$ contains $N$ that do not fix the state $\langle \psi \rangle \in T(S)$

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

1. $\tilde{U} U \tilde{U}^* \in S$, $U \in$ generator for $S$
2. $\tilde{U} X; \tilde{U}^*$, $\tilde{U} Z; \tilde{U}^*$ transform according to the Clifford gate
Eq. 1 5-qubit code

\[ G_1 = X \otimes Z \otimes Z \otimes X \]
\[ G_2 = I \otimes Z \otimes Z \otimes X \]
\[ G_3 = X \otimes I \otimes Z \otimes Z \]
\[ G_4 = Z \otimes X \otimes I \otimes Z \]

\[ \hat{x} = XX_X \]
\[ \hat{z} = ZZ_Z \]

\[ H = U = HHHHH \]

Unfortunately no \( U\hat{x}U^+ = \hat{x} \), \( U\hat{z}U^+ = \hat{x} \)

But \( UG_i U^+ = Z \otimes X \otimes Z \otimes I \)

Ex: Show that no \( a, a_2, a_3, a_4 \) make \( G_1 a_1 G_2 a_2 G_3 a_3 G_4 a_4 = 2 \otimes X \otimes Z \)

So \( UG_i U^+ \notin S \) i.e. \( U = U^{\otimes 5} \) does not preserve the code space

\( Z \) not a valid logical operator, despite the action on \( N(S)/S \) is correct.
7-qubit code

\[ Q_i = \begin{cases} 1 & i \in I \\ I & \text{otherwise} \end{cases} \]

\[ X_i = \begin{cases} I & i \in I \\ X & \text{otherwise} \end{cases} \]

Consider \( U = H^\otimes 7 \), \( H \in H = Z \), \( H \in H = X \)

Then \( UQ_iU^+ = Q_i \), \( UQ_4U^+ = Q_1 \), \( UQ_5U^+ = Q_2 \), \( UQ_6U^+ = Q_3 \), \( UQ_7U^+ = Q_4 \), \( U, V \in UQ_iU^+ \in S \)

\( S \) is an encoded operation.

Also \( UX_iU^+ = Z \), \( U \in U^+ \in X \).

By Thm, \( U = \overline{H} \) up to an overall phase.

Consider \( U = R_{\frac{\pi}{4}} \otimes 7 \), \( UX_iU^+ = Y \), \( UZ_iU^+ = Z \) \( (Y = iXZ) \)

Then \( UQ_iU^+ = 1 1 1 1 1 1 1 \)

\[ = \begin{cases} 1 & (iXZ) \in I \\ 1 & (iXZ) \in X \end{cases} \]

\[ = \begin{cases} 1 1 1 & (iXZ) \in I \\ 1 1 1 & (iXZ) \in X \end{cases} \]

\[ = (1 1 1 \times X) \times (1 1 1 \times X) = Q_1 \times Q_4 \]

Similarly \( UQ_4U^+ = Y Y Y Y Y Y = Q_2 \times Q_5 \)

\[ UQ_5U^+ = Y Y Y Y Y Y = Q_3 \times Q_6 \]

\[ UQ_iU^+ = Q_i \quad i = 4, 5, 6 \]

\( \bar{U} = UQ_iU^+ \in S \), and \( U \) is an encoded operation.

\[ UX_iU^+ = Y \otimes 7 = (iXZ)^\otimes 7 = iZ \overline{X} \overline{Z} = -i\overline{Y} \]

\[ UZ_iU^+ = Z \otimes 7 = \overline{Z} \]

\( \bar{U} = \overline{R_{\frac{\pi}{4}}} = R_{\frac{\pi}{4}} \cdot \overline{Z} \)
Before analyzing CNOT, 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 $Q_1, Q_2, ..., Q_r$ encoding $K$ qubits into $N$ qubits ($K=N-r$), with encoded Pauli's $\overline{X}_1, \overline{Z}_1$ for $i=1,2,...,K$.

Consider a stabilizer $S'$ with generators $Q'_1, Q'_2, ..., Q'_r'$ encoding $K'$ qubits into $N'$ qubits ($K'=N'-r'$), with encoded Pauli's $\overline{X}'_j, \overline{Z}'_j$ for $j=1,2,...,K'$.

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

$$Q_1 \otimes I^{n'}, \quad I^{n} \otimes Q'_1$$
$$Q_2 \otimes I^{n'}, \quad I^{n} \otimes Q'_2$$
$$\vdots$$
$$Q_r \otimes I^{n'}, \quad I^{n} \otimes Q'_r$$

and encoded Pauli group generated by:

$$\overline{X}_1 \otimes I^{n'}, \quad I^{n} \otimes \overline{X}'_1$$
$$\overline{X}_2 \otimes I^{n'}, \quad I^{n} \otimes \overline{X}'_2$$
$$\vdots$$
$$\overline{X}_K \otimes I^{n'}, \quad I^{n} \otimes \overline{X}'_K$$
$$\overline{Z}_1 \otimes I^{n'}, \quad I^{n} \otimes \overline{Z}'_1$$
$$\overline{Z}_2 \otimes I^{n'}, \quad I^{n} \otimes \overline{Z}'_2$$
$$\vdots$$
$$\overline{Z}_K \otimes I^{n'}, \quad I^{n} \otimes \overline{Z}'_K$$
For 2 blocks of 7 qubit code, stabilizer generators are:

\( Q_1 \otimes I^{\otimes 7} = 111 \times \times \times 1111111 = J_1 \)
\( Q_2 \otimes I^{\otimes 7} = 1 \times x 11 \times 1111111 = J_2 \)
\( Q_3 \otimes I^{\otimes 7} = 111 \times \times 1 \times 1111111 = J_3 \)
\( Q_4 \otimes I^{\otimes 7} = 111 2 2 2 2 2 1111111 = J_4 \)
\( Q_5 \otimes I^{\otimes 7} = 12 2 1 1 2 2 2 1111111 = J_5 \)
\( Q_6 \otimes I^{\otimes 7} = 21 2 1 2 1 2 1111111 = J_6 \)
\( I^{\otimes 7} \otimes Q_1 = 1111111111 \times \times xx = J_7 \)
\( I^{\otimes 7} \otimes Q_2 = 1111111111 \times \times xx = J_8 \)
\( I^{\otimes 7} \otimes Q_3 = 1111111111 \times \times xx = J_9 \)
\( I^{\otimes 7} \otimes Q_4 = 1111111111 2 2 2 2 2 = J_{10} \)
\( I^{\otimes 7} \otimes Q_5 = 1111111122 2 2 2 = J_{11} \)
\( I^{\otimes 7} \otimes Q_6 = 1111111121 2 2 2 = J_{12} \)

Let \( U = CNOT_{12} \otimes CNOT_{29} \otimes \ldots \otimes CNOT_{714} \)

Then \( U J_i U^\dagger = 111 \times \times \times 111 \times \times xx = J_i J_j \)

\( H \text{call CNOT } x1 \text{ CNOT } x2 \)

\( U J_2 U^\dagger = J_2 J_8 \)

\( U J_3 U^\dagger = J_3 J_9 \)

\( U J_7 U^\dagger = J_7 \) for \( i = 4, 5, 6, 7, 8, 9. \)

\( U J_{10} U^\dagger = 111 2 2 2 2 2 111 2 2 2 = J_{14} J_{10} \)

\( CNOT_{12} \otimes CNOT_{22} = 2 \times \times \times \)

\( U J_4 U^\dagger = J_4 J_6 \)

\( U J_{12} U^\dagger = J_6 J_{12} \)

\( J_i U \) is a encoded operator.

Also \( U \bar{X}_1 U^\dagger = X^{\otimes 7} \otimes X^{\otimes 7} = \bar{X}_1 \bar{X}_2 \)
\( U \bar{Z}_1 U^\dagger = Z^{\otimes 7} \otimes Z^{\otimes 7} = \bar{Z}_1 \)
\( U \bar{X} U^\dagger = Z^{\otimes 7} \otimes Z^{\otimes 7} = \bar{X}_2 \)
\( U \bar{Z} U^\dagger = Z^{\otimes 7} \otimes Z^{\otimes 7} = \bar{Z}_2 \)

\( U = \text{CNOT}_{12} \)
Summary: for the 7-qubit code, encoded X, Z, \( R_{y}^{-1} \), 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. \( R_{x}^{\pi 2}, H, CNOT \) generate the Clifford group.

Thm: If \( U \in Cn \), then \( U \in \langle e^{i\theta} I, H, R_{x}^{\pi 2}, CNOT_{i\in\{1,2\}} \rangle \).

which qubits the gates act on.

\( Cn \) the Clifford group is generated (multiplicatively) by \( H, R_{x}^{\pi 2}, CNOT \).

Pf idea: Note that \( R_{x}^{\pi 2} \cong Z \), so, \( H, R_{x}^{\pi 2} \) generate the Pauli subgroup.

Recall \( \hat{Cn} = Cn / \langle e^{i\theta} I \rangle \), \( \hat{Cn} = \hat{Cn} / \hat{Pn} \), focus on \( \hat{Cn} \).

Specify \( W \in \hat{Cn} \) by \( f(x_i) = UX_i U^{+}, f(z_i) = UZ_i U^{+}, i = 1, \ldots, n \).

Switch to symplectic rep: \( \Sigma f(x_i) = (X f(x_i), Z f(x_i)) \)

\( \Sigma f(z_i) = (X f(z_i), Z f(z_i)) \)

The map \( f \) (from \( Pn \) to \( Pn \)) induces a linear transp on \((Z_2)^{2n}\):

\[ \begin{array}{c|c|c|c|c|c} \hline & Xf(x_1) & Xf(x_2) & \cdots & Xf(x_n) & \cr \hline \text{ith} \text{col.} & f(x_1) & f(x_2) & \cdots & f(x_n) & \cr \hline \text{ith} \text{row.} & f(x_1) & f(x_2) & \cdots & f(x_n) & \cr \hline \end{array} \]
19. $R_{12}$ is represented by:

\[
\begin{bmatrix}
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0
\end{bmatrix}
\]

(takes $x_1$ to $-i x_2$, leaves the rest invariant)

20. $(R_{12})^2$ is represented by:

\[
\begin{bmatrix}
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0
\end{bmatrix}
\]

(takes $x_1$ to $x_1 x_2$

\[
\begin{bmatrix}
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0
\end{bmatrix}
\]

leaves the rest invariant)

- Call the symplectic rep of $U \in \mathbb{C}^n$ $S(U)$.

- Columns of $S(U)$ satisfy symplectic inner product governed by (anti)comm relations of the Pauli's.

- Left multiplications by $S(H_i)$, $S(R_{12})$, $S(CNOT_{ij})$ are to special row operations, right multiplications are to column operations.

- $S(U) \cdot S(V) = S(UV)$

- These row/column operations preserve the full rank of $S(U)$, but can be chosen to strictly reduce the # of 1's.

- Exist a sequence of these row/column operations to transform $S(U)$ to $I_n$.

  - Exist a sequence of $H_i R_i CNOT$ that left/right multiply to $U$ resulting in $I \in \mathbb{C}^n$.

  - $O(n^2)$ of them
1. If \( \mathcal{C} \) correspond to an operator \( P \in \hat{S}_n \),
2. \( V_1, V_2, \ldots, V_r = P \) \( \text{with} \) \( r \sim O(n^2) \)
3. \( U = V_e^+ \ldots V_i V_i^+ P V_r^+ V_r^+ \ldots V_{r+1}^+ \)

where each \( V_d \) is \( H, \text{RZ}, \text{or CNOT} \).

Remarks:

1. Proof of thin is constructive.
2. We can obtain encoding circuit for any stabilizer code.
   Say block length \( n \), \# encoded qubits \( k \), \( \sigma_i \)'s generate \( S \).
   \( x_i, z_i \) are logical Pauli's.

\[ \begin{array}{c|cc}
   k \text{ encoded qubits} & \vdots & \vdots \\
   n-k \text{ ancilla} & \vdots & \vdots \\
   \end{array} \]

Want: \( U X_i U^+ = \overline{x_i} \)
\( U Z_i U^+ = \overline{z_i} \) \( \text{for} \) \( i = 1, 2, \ldots, k \)
\( U Z_j U^+ = \sigma_{j-k} \) \( \text{for} \) \( j = k+1, k+2, \ldots, n \)

Augment: \( U X_j U^+ \) \( \text{for} \) \( j = k+1, k+2, \ldots, n \), preserving needed \( \text{com/anti} \) \( \text{com} \) relations.

Take \( U X_i U^+ \), \( U Z_i U^+ \) \( \text{for} \) \( i = 1, \ldots, n \) and apply Thin to get sequence of \( R, H, \text{CNOT} \).
Observation: \( C_n \) is not universal (it's a finite, discrete, group).

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

Add any \( G \neq C_n \) into \( C_n \) generates a dense set in \( \mathcal{U}(2^n) \)

i.e. \( \{ G, R, Z, H \} \) (NOT's universal).

The \( C^k \) hierarchy:

Let \( C^1 = \bigcup \mathcal{P}_n \)

Let \( C^2 = \bigcup \mathcal{P}_n \{ U \in \mathcal{U}(2^n) : U P_n U^\dagger \subseteq \mathcal{P}_n \} = \bigcup \mathcal{P}_n \{ U \in \mathcal{U}(2^n) : U P_n U^\dagger \subseteq C^1 \} \)

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

\[ \vdots \]

\[ C^k = \bigcup \mathcal{P}_n \{ U \in \mathcal{U}(2^n) : U P_n U^\dagger \subseteq C^{k-1} \} \]

Teleporting a \( C^3 \) gate:

1. This box teleports, then apply \( U \)
2. This box can be implemented with
   - \( G \) state to \( U \) (max entangled state) \( \Leftarrow \) Will learn more in part II
   - Bell measurement \( \langle XX + ZZ \rangle \)
   - \( U \) and \( U^\dagger \) which is Clifford!

More efficient schemes exist for \( (\text{NOT, } R_{\frac{\pi}{2}}, \text{etc) (1-bit teleportation)} \)