QIC 890 / CO781 / CS 867, W24

Lec 4 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 $S' = \{ UMU^\dagger : M \in S \}$ (Abelian group, $|S| = |S'|$)

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

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

<u>Def</u> [Clifford group on n qubits]:

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

<u>Obs</u>: for a stabilizer $S \subseteq \mathcal{P}_n$, $U \in \mathcal{C}_n$, $\Sigma[U(T(S))] = S' =: USU^\dagger$

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 $U^\dagger$ 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 $U \in U(2^n)$:

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

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 $\mathcal{P}_n \to U\mathcal{P}_nU^\dagger$ 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 $QP = (-1)^{c(P,Q)} PQ$

then $UQU^\dagger UPU^\dagger = UQPU^\dagger = (-1)^{c(P,Q)} UPQU^\dagger$
$= (-1)^{c(P,Q)} UPU^\dagger UQU^\dagger$

Remarks:

- 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 pages 5-7)

* 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 $\forall n, \ P_n \subseteq C_n$.

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

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

When $V \in P_n$, $M_V(Q) \in \{Q, -Q\}$

$\forall U \in C_n$, M_U can be specified in 2 steps:

for each generator G_i for $\hat{P}_n$:

① Pick $M_W(G_i) \in \hat{P}_n$ for some $W \in \check{C}_n$

② Pick signs of each $M_W(G_i)$, which can be effected by conjugation by some $V \in \hat{P}_n$.

and $U = VW$ (See page ---)

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

Then $\left.\begin{array}{l} HXH = Z \\ HZH = X \end{array}\right\} (*)$ Note condition ③ is satisfied.

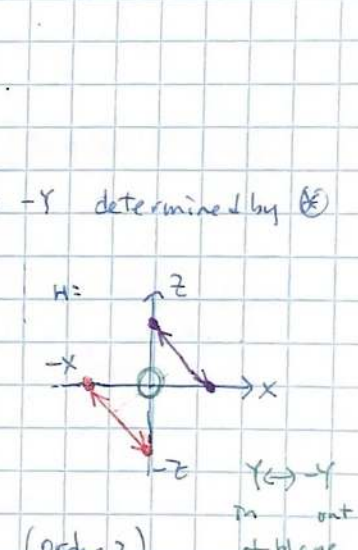
And $HYH = H(iXZ)H = i\, HXH\, HZH = iZX = -Y$ determined by $(*)$

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

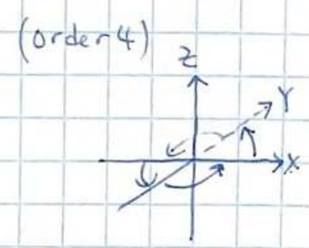
take $U = ZH$.

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

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



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

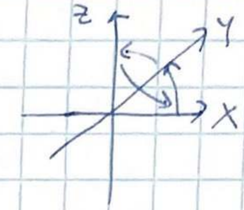


Then $UXU^\dagger = Y$
$UZU^\dagger = Z$

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

Ex: check that $U = ZH$ & $U' = e^{+i\frac{\pi}{4}Y}$ give $M_U = M_{U'}$.

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

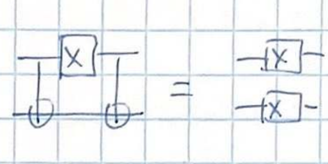


order 3.

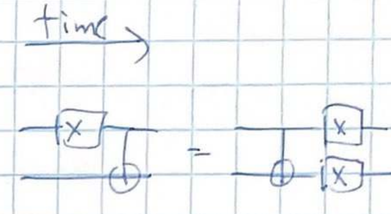
eg 6 $n=2$. $U = CNOT_{12} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Z$.

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

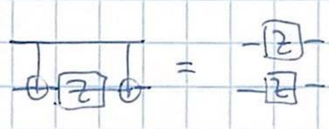
Useful later:



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 the first two commute with the last two

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

$$\therefore\ X1 \xrightarrow{IH} X1 \xrightarrow{CNOT_{12}} XX \xrightarrow{IH} XZ$$
$$Z1 \longrightarrow Z1 \longrightarrow Z1 \longrightarrow Z1$$
(In fact, C-Z diagonal, com with Z1)
$$1X \longrightarrow 1Z \longrightarrow ZZ \longrightarrow ZX$$
$$1Z \longrightarrow 1X \longrightarrow 1X \longrightarrow 1Z$$
(again, C-Z com with 1Z).

Note C-Z symmetric between the 2 qubits

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

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

$\bar{X}_i = f(X_i)$, $\bar{Z}_i = f(Z_i)$ (note diff usage of the "bar" from lec 3)

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 $\exists U \in \mathcal{U}(2^n)$ 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, $\underbrace{2n \text{ images}}_{\bar{X}_i, \bar{Z}_i}$ with correct com/anticom relations specify a unitary U whose conjugation map M_U realizes the gp homo.

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

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

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

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

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

$\therefore$ Uniqueness in Thm is proved.

NB Lemma holds whether we take $\forall P \in \mathcal{P}_n$ or $\forall P \in \hat{\mathcal{P}}_n$.

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 $\widetilde{X}(b) = \prod_{i=1}^{n} (\bar{X}_i)^{b_i}$.

③ Let $|\psi_b\rangle = \widetilde{X}(b)|\psi_0\rangle$.

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, $\overline{X}(b)$ unitary $\therefore \| |\psi_b\rangle \| = \| |\psi_0\rangle \| = 1$ $\forall b$.

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

(b) Verify $UX_iU^\dagger = \overline{X}_i$, $UZ_iU^\dagger = \overline{Z}_i$.

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

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

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

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

Obs: For any $2n$ bits $a_1a_2\ldots a_n\, b_1b_2\ldots b_n$
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 $M_W : P \mapsto WPW^\dagger$ 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 $(2^n \times 2^n)$.

Only 2 indep conditions

eg. for M_u: $\boxed{X \to Y}$ $\quad \bar{X} = Y$

$Y \to Z$

$\boxed{Z \to X}$ $\quad \bar{Z} = X$

$\Rightarrow U Y U^\dagger = U(iXZ)U^\dagger = iYX = Z$

anticommute

$|\psi_0\rangle \propto \left(\frac{I+\bar{Z}}{2}\right)|\alpha\rangle = \left(\frac{I+X}{2}\right)|0\rangle$ (take $|\alpha\rangle = |0\rangle$)

$|\psi_0\rangle = |+\rangle$

$|\psi_1\rangle = \bar{X}|\psi_0\rangle = Y|\psi_0\rangle = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \frac{\begin{bmatrix} 1 \\ 1 \end{bmatrix}}{\sqrt{2}} = \frac{\begin{bmatrix} -i \\ i \end{bmatrix}}{\sqrt{2}}$

$U = |\psi_1\rangle\langle 1| + |\psi_0\rangle\langle 0| = \begin{bmatrix} |\psi_0\rangle & |\psi_1\rangle \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & -i \\ 1 & i \end{bmatrix}$

relative phase between columns
is important!!

ie cannot change the phase of $\bar{X}$.

Ex: Check that indeed $UXU^\dagger = Y$
$UZU^\dagger = X$

NB: Without the recipe, one will need symmetry,
namely, $X+Y+Z$ is preserved to deduce the rotation axis,
and the order 3 to deduce the rotation angle
to obtain a matrix rep of this unitary.

eg If instead, we want $\bar{X} = -Y$, $\bar{Z} = X$, we choose $U = X \cdot \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & -i \\ 1 & i \end{bmatrix}$

Ex: Find what unitary gives $\bar{X} = Y$, $\bar{Z} = -X$ and $\bar{X} = -Y$, $\bar{Z} = -X$.

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's that do not fix some state $|\psi\rangle \in T(S)$

in $\check{C}_n$

in $\hat{P}_n$

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 (then Thm on page 5 implies correctness of logical operation)

eg 7-qubit code

$Q_1 = I\ I\ I\ X\ X\ X\ X$ $\qquad$ $Q_4 = I\ I\ I\ Z\ Z\ Z\ Z$
$Q_2 = I\ X\ X\ I\ I\ X\ X$ $\qquad$ $Q_5 = 1\ Z\ Z\ 1\ 1\ Z\ Z$
$Q_3 = X\ I\ X\ I\ X\ I\ X$ $\qquad$ $Q_6 = Z\ 1\ Z\ 1\ Z\ 1\ Z$

$\overline{X} = X\,X\,X\,X\,X\,X\,X$ $\qquad$ $\overline{Z} = Z\,Z\,Z\,Z\,Z\,Z\,Z$

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

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

$\therefore$ U is an encoded operation.

Also $U\overline{X}U^\dagger = \overline{Z}$, $U\overline{Z}U^\dagger = \overline{X}$.

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

- Consider $U = R_{\frac{\pi}{4}}^{\otimes 7}$, $\quad UXU^\dagger = Y$, $UZU^\dagger = Z$ $\quad (Y = iXZ)$ $\quad$ (see $R_{\frac{\pi}{4}}$ from ③)

Then $UQ_1U^\dagger = 1\,1\,1\,Y\,Y\,Y\,Y$

$= 1\,1\,1\,(iXZ)\,(iXZ)\,(iXZ)\,(iXZ)$ $\qquad$ (nice $i^4 = 1$)

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

Similarly $UQ_2U^\dagger = 1YY11YY = Q_2Q_5$
$UQ_3U^\dagger = Y1Y1Y1Y = Q_3Q_6$

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

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

$U\overline{X}U^\dagger = Y^{\otimes 7} = (iXZ)^{\otimes 7} = i^7\,\overline{X}\,\overline{Z} = -i\overline{X}\,\overline{Z} = \ominus\overline{Y}$
$U\overline{Z}U^\dagger = Z^{\otimes 7} = \overline{Z}$.

$\therefore U = \overline{R_{\frac{\pi}{4}}}^{\,\dagger} = \overline{R}(-\tfrac{\pi}{4})$. $\qquad$ (NB $\overline{R_{\frac{\pi}{4}}}$ can be implemented as $R(-\tfrac{\pi}{4})^{\otimes 7}$.)

- 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 $\overline{X}_i, \overline{Z}_i$ 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 $\overline{X}_j', \overline{Z}_j'$ 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:

$$
\begin{array}{ll}
\overline{X}_1 \otimes I^{\otimes n'}, & I^{\otimes n} \otimes \overline{X}_1' \\
\vdots & \vdots \\
\overline{X}_K \otimes I^{\otimes n'}, & I^{\otimes n} \otimes \overline{X}_{K'}' \\
 & \\
\overline{Z}_1 \otimes I^{\otimes n'}, & I^{\otimes n} \otimes \overline{Z}_1' \\
\vdots & \vdots \\
\overline{Z}_K \otimes I^{\otimes n'}, & I^{\otimes n} \otimes \overline{Z}_{K'}'
\end{array}
$$

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

$Q_1 \otimes I^{\otimes 7} = III\,XXXX\ \ III\,IIII = J_1$

$Q_2 \otimes I^{\otimes 7} = IXX\,IIXX\ \ III\,IIII = J_2$

$Q_3 \otimes I^{\otimes 7} = XIX\,IXIX\ \ III\,IIII = J_3$

$Q_4 \otimes I^{\otimes 7} = III\,ZZZZ\ \ III\,IIII = J_4$

$Q_5 \otimes I^{\otimes 7} = IZZ\,IIZZ\ \ III\,IIII = J_5$

$Q_6 \otimes I^{\otimes 7} = ZIZ\,IZIZ\ \ III\,IIII = J_6$

$\bar{X}_1 = X^{\otimes 7} \otimes I^{\otimes 7}$

$\bar{X}_2 = I^{\otimes 7} \otimes X^{\otimes 7}$

$\bar{Z}_1 = Z^{\otimes 7} \otimes I^{\otimes 7}$

$\bar{Z}_2 = I^{\otimes 7} \otimes Z^{\otimes 7}$

$I^{\otimes 7} \otimes Q_1 = IIIIIII\ \ III\,XXXX = J_7$

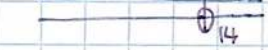
$I^{\otimes 7} \otimes Q_2 = IIIIIII\ \ IXX\,IIXX = J_8$

$I^{\otimes 7} \otimes Q_3 = IIIIIII\ \ XIX\,IXIX = J_9$

$I^{\otimes 7} \otimes Q_4 = IIIIIII\ \ III\,ZZZZ = J_{10}$

$I^{\otimes 7} \otimes Q_5 = IIIIIII\ \ IZZ\,IIZZ = J_{11}$

$I^{\otimes 7} \otimes Q_6 = IIIIIII\ \ ZIZ\,IZIZ = J_{12}$



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

Then $U J_1 U^\dagger = III\,XXXX\ \ III\,XXXX = J_1 J_7$

recall $CNOT\ XI\ CNOT = XX$

$U J_2 U^\dagger = J_2 J_8$

$U J_3 U^\dagger = J_3 J_9$

$U J_i U^\dagger = J_i$ for $i = 4, 5, 6, 7, 8, 9$.

$U J_{10} U^\dagger = III\,ZZZZ\ \ III\,ZZZZ = J_4 J_{10}$

$CNOT\ IZ\ CNOT = ZZ$

$U J_{11} U^\dagger = J_5 J_{11}$

$U J_{12} U^\dagger = J_6 J_{12}$ $\quad\therefore U$ is an encoded operation.

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

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

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

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

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

NB. Transversal operations do not spread errors within a code block - crucial for fault-tolerant QC.

Obs:

① $R_{\frac{\pi}{4}}$, H, CNOT generate the Clifford group!

② Logical Clifford ops for the 7-qubit code are not just transversal, but "bitwise" - being tensor power of a physical op symmetric over the qubits in the code block.

This may give advantages in implementation / cryptography.

eg 5-qubit code

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

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

$$\bar{H} \overset{?}{=} U = H\,H\,H\,H\,H$$

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.

Solution: gate teleportation, code switching, etc (measurement induced evolution).

<u>Thm</u>: $C_n = \langle e^{i\theta} I,\ H_i,\ R_{\frac{\pi}{4},i},\ CNOT_{ij}\ (i<j) \rangle$

ie H, $R_{\frac{\pi}{4}}$, CNOT generate $\hat{C}_n$ multiplicatively.

Pf: lin alg in symplectic rep, with all homomorphisms & symplectic inner product constraints, amounts to row/col operations with constraints.

Will return to this if there is time in lec 6.

See 2018 recording, lec 4 (around 1:00 into the video).

Important:

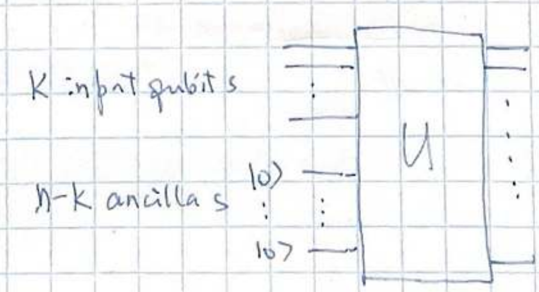
① Constructive proof gives U as product of H, $R_{\frac{\pi}{4}}$, CNOT, with $\Omega(n^2)$ such gates.

② Corollary: encoding circuit for any stabilizer code has size $\Omega(n^2)$:

Idea: $Q_1, \ldots, Q_{n-k}$ generators,
$\bar{X}_i, \bar{Z}_i$ encoded Paulis for $i = 1, \ldots, k$.

Take U s.t. for $i = 1, \ldots, k$, $X_i \to \bar{X}_i$
$Z_i \to \bar{Z}_i$
for $j = k+1, \ldots, n$, $Z_j \to Q_{j-k}$
$X_j \to$ Pauli's chosen to satisfy com/anti rel'ns.

Get $\mathcal{C}(U)$, then circuit in H, CNOT, $R_{\frac{\pi}{4}}$.



Observation: C_n is not universal (it's a finite, discrete, group)

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

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

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

The C^k hierarchy:

Let $C^1 = \bigcup_n P_n$

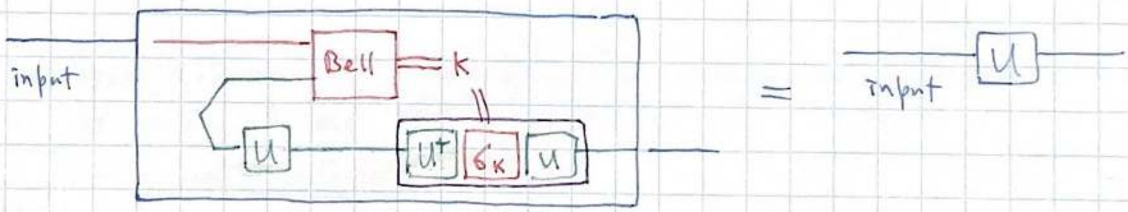
Let $C^2 = \bigcup_n \{U \in \mathcal{U}(2^n) : U P_n U^\dagger \subseteq P_n\} = \bigcup_n \{U \in \mathcal{U}(2^n) : U P_n U^\dagger \subseteq C^1\}$

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

$\vdots$

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

Teleporting a C^3 gate:



① This box teleports, then apply U

② This box can be implemented with

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

✓ (ii) Bell measurement (XX, ZZ)

✓ (iii) $U \sigma_K U^\dagger$ which is Clifford!

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