Quantum caupulation: lecture 14

Reminder: Steane code

Ingredient: Hamming code $(7, 4, 3)$

parity-check matrix $H = \begin{pmatrix} 0&0&0&1&1&1&1 \\ 0&1&1&0&0&1&1 \\ 1&0&1&0&1&0&1 \end{pmatrix}$

generator matrix $G = \begin{pmatrix} 0&0&0&1&1&1&1 \\ 0&1&1&0&0&1&1 \\ 1&0&1&0&1&0&1 \\ 1&1&1&1&1&1&1 \end{pmatrix}$

$\begin{pmatrix} \dim 4 \\ d = 3 \end{pmatrix}$ $\mathcal{C}_H = \{ c = u \cdot G, u \in \mathbb{F}_2^4 \} = \{ c \in \mathbb{F}_2^7 : H c^T = 0 \}$

$\mathcal{C}_H^\perp = \{ c = u \cdot H, u \in \mathbb{F}_2^3 \}$

Steane code $(7, 1, 3)$

$$|0\rangle_S = \frac{1}{\sqrt{8}} \sum_{c \in C_H^\perp} |c\rangle \left\{ = \frac{1}{\sqrt{8}} \left(|0000000\rangle + |0001111\rangle + \dots \right) \right\}$$

$$|1\rangle_S = \frac{1}{\sqrt{8}} \sum_{c \in C_H^\perp} |c \oplus 1111111\rangle = \dots$$

encoding: $\alpha|0\rangle + \beta|1\rangle \to |\psi\rangle := \alpha|0\rangle_S + \beta|1\rangle_S$

claim: this code can correct any single error

(either $\{X_i, Y_i, Z_i\}_{i=1}^{7}$) [NB: $Y_i = \underbrace{i}_{\sqrt{-1}} X_i Z_i$]

decoding:

stabilizers: $g_1 = X_4 X_5 X_6 X_7 \quad Z_4 Z_5 Z_6 Z_7 = g_4$

$g_2 = X_2 X_3 X_6 X_7 \quad Z_2 Z_3 Z_6 Z_7 = g_5$

$g_3 = X_1 X_3 X_5 X_7 \quad Z_1 Z_3 Z_5 Z_7 = g_6$

(these correspond to the 1's in the matrix H)

stabilizer group = group generated by these stabilizers (S)

claim: $|\psi\rangle$ = codeword of the Steane code

iff $\forall g \in S,\ g|\psi\rangle = |\psi\rangle$

proof: (on an example)

- $X_4X_5X_6X_7\,|0\rangle_S$: this flips the last 4 bits of every state

$$= \frac{1}{\sqrt{8}} \sum_{c \in \underbrace{C_H^\perp}_{=\text{group!}}} |c \oplus \underbrace{00001111}_{\in C_H^\perp}\rangle = \frac{1}{\sqrt{8}} \sum_{c \in C_H^\perp} |c\rangle = |0\rangle_S$$

- Same for $|1\rangle_S$
- and by a dimensionality argument, these are alone #

Next, all stabilizers commute!

(note $X_i Z_i = -Z_i X_i$, but there is always an even number of common X's and Z's between two stabilizers)

Assume now the received state is

$$|\psi'\rangle = X_7(\alpha|0\rangle_S + \beta|1\rangle_S) \quad \text{(bit-flip in } 7^{\text{th}} \text{ position)}$$

$g_1 |\psi'\rangle = (+1)|\psi'\rangle$ $\quad$ $g_4 |\psi'\rangle = (-1)|\psi'\rangle$

$g_2 |\psi'\rangle = (+1)|\psi'\rangle$ $\quad$ $g_5 |\psi'\rangle = (-1)|\psi'\rangle$

$g_3 |\psi'\rangle = (+1)|\psi'\rangle$ $\quad$ $g_6 |\psi'\rangle = (-1)|\psi'\rangle$

Syndrome $= (+1, +1, +1, \underline{-1, -1, -1})$ $\quad$ X

$\underline{\quad\quad\quad} \rightarrow 111 \rightarrow$ error in pos. 7

Other examples:

X_3 error $\rightarrow$ syndrome $= (1,1,1,\underline{1,-1,-1}) \rightarrow 011 \rightarrow \overset{X}{\text{error}}$ in pos. 3

Z_4 error $\rightarrow$ syndrome $= (\underline{-1,1,1}, 1, 1, 1) \rightarrow 100 \rightarrow \overset{Z}{\text{error}}$ in pos. 4

$Y_6 = iX_6 Z_6$ error $\rightarrow$ syndrome $= (\underbrace{-1,-1,1}_{110 \rightarrow 6}, \underbrace{-1,-1,1}_{110 \rightarrow 6})$

Building reliable quantum gates

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = iXZ \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \qquad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

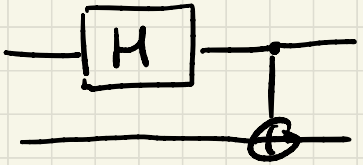
$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Steane code:

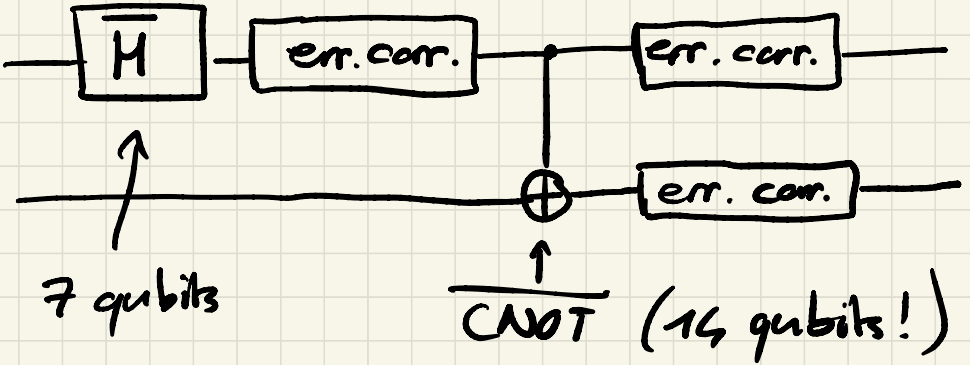
$\alpha|0\rangle + \beta|1\rangle \longrightarrow \alpha|0\rangle_S + \beta|1\rangle_S$ (= 7 qubit state)

Aim: to find 7-qubits gates $\overline{X}, \overline{Y}, \overline{Z}$ ...

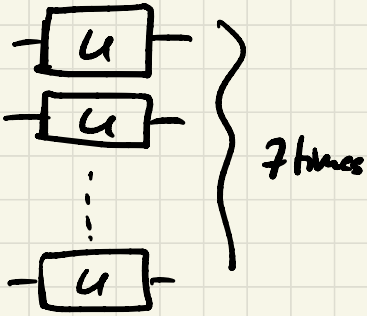
So a circuit like



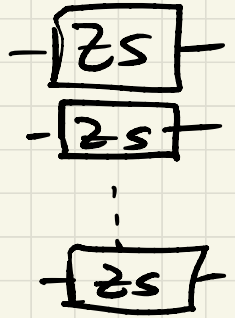
becomes



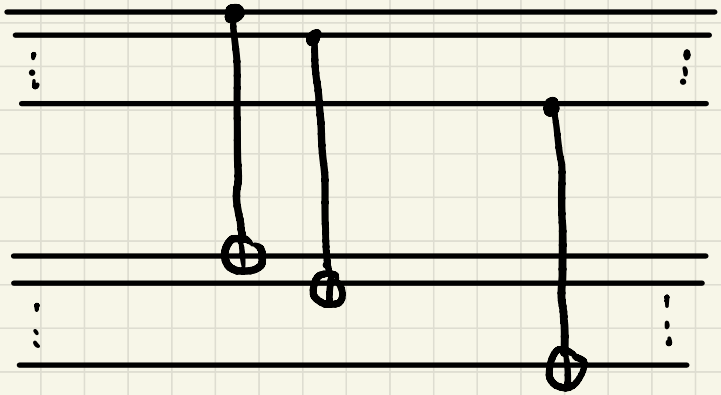
Claim: for $U = X, Y, Z, H$, $\overline{U}$ is given by



Now: • $S \longrightarrow \overline{S}$ is given by



• CNOT $\longrightarrow$ $\overline{\text{CNOT}}$ becomes:



• and the gate $\overline{T}$ needs more attention (undone)

To check: assume an error occurs somewhere

$$|\psi'\rangle = X_3 |\psi\rangle \quad \text{e.g.}$$

- $\overline{H}\, X_3 |\psi\rangle = Z_3 \overline{H} |\psi\rangle$ $\Rightarrow$ error correction is doable afterwards (in the 7-qubit block)

  transversality (because $HX = ZH$)

- In a $\overline{CNOT}$ gate, an error might propagate, but it will propagate to two separate 7-qubit blocks $\rightarrow$ fine also

Let us check:

- $X(\alpha|0\rangle + \beta|1\rangle) = \alpha|1\rangle + \beta|0\rangle$

$\xrightarrow{\text{Stream}}$ $\alpha|1\rangle_s + \beta|0\rangle_s$ ← match!

and $\overline{X}(\alpha|0\rangle_s + \beta|1\rangle_s) = \alpha|1\rangle_s + \beta|0\rangle_s$

all the states are complement of each other in these states

- $Z(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle - \beta|1\rangle$

  $\xrightarrow[\text{steam}]{}$ $\alpha|0\rangle_s - \beta|1\rangle_s$ ← match!

and $\overline{Z}(\alpha|0\rangle_s + \beta|1\rangle_s) = \alpha|0\rangle_s - \beta|1\rangle_s$

↑ even # of 1's ↑ odd # of 1's

- $Y = iXZ$ ⟶ fine also

- $H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$, $H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$

→ Steane: $\frac{|0\rangle_S + |1\rangle_S}{\sqrt{2}}$, $\frac{|0\rangle_S - |1\rangle_S}{\sqrt{2}}$

and $\overline{H}|0\rangle_S = \frac{|0\rangle_S + |1\rangle_S}{\sqrt{2}}$, $\overline{H}|1\rangle_S = \frac{|0\rangle_S - |1\rangle_S}{\sqrt{2}}$:

1°) $\overline{H}$ maps codewords into codewords

2°) $HX = ZH \rightarrow HXH = Z$
$HZ = XH \rightarrow HZH = X$
} same for $\overline{H}$!

(conjugation)

2°) $\overline{H}\,\overline{X}\,\overline{H} = H_1 \cdots H_7 X_1 \cdots X_7 H_1 \cdots H_7$

$= H_1 X_1 H_1 \cdots H_7 X_7 H_7 = Z_1 \cdots Z_7 = \overline{Z}$

and also $\overline{H}\,\overline{Z}\,\overline{H} = \overline{X}$ ✓

1°) $\overline{H}(\alpha|0\rangle_s + \beta|1\rangle_s)$ = code word ?

to check : $\forall g_i \in S \quad g_i \overline{H}(\alpha|0\rangle_s + \beta|1\rangle_s) = \overline{H}(\alpha|0\rangle_s + \beta|1\rangle_s)$

ie. $\overline{H}\, g_i\, \overline{H} \in S$? yes, because (eg):

$g_1 = X_4 X_5 X_6 X_7 \longrightarrow \overline{H}\, g_1\, \overline{H} = Z_4 Z_5 Z_6 Z_7 \in S$ ✓