

Quantum computation: lecture 18

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

$$\begin{pmatrix} \dim 4 \\ d=3 \end{pmatrix}$$

$$C_H = \{c = u \cdot G, u \in \mathbb{F}_2^4\} = \{c \in \mathbb{F}_2^7 : H c^T = 0\}$$

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

Steane code (7, 1, 3)

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

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

encoding: $\alpha|0\rangle + \beta|1\rangle \rightarrow |\psi\rangle = \alpha|0\rangle_s + \beta|1\rangle_s$

claim: This code can correct any single error

$$\left(\text{either } \{X_i, Y_i, Z_i\}_{i=1}^7 \right) \quad \left[\text{NB: } Y_i = \frac{1}{\sqrt{-1}} X_i Z_i \right]$$

decoding:

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

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

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

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

stabilizer group = group generated by these
stabilizers (S)

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

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

proof: (on an example)

- $X_4 X_5 X_6 X_7 |0\rangle_S$: This flips the last 4 bits of every _{State}

$$= \frac{1}{\sqrt{8}} \sum_{\substack{C \in C_H^\perp \\ \text{= group!}}} |C \oplus \underbrace{0001111}_{\in C_H^\perp}\rangle = \frac{1}{\sqrt{8}} \sum_{C \in C_H^\perp} |C\rangle = |0\rangle_S$$

- 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

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

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

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

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

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

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

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

$$\text{Syndrome} = (+1, +1, +1, \underbrace{-1, -1, -1}_X \rightarrow 111 \rightarrow \text{error in pos. 7})$$

Other examples:

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

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

$$Y_6 = i X_6 Z_6 \text{ error} \rightarrow \text{syndrome} = (\underline{-1, -1, 1}, \underline{-1, -1, 1}) \rightarrow 110 \rightarrow 6 \quad 110 \rightarrow 6$$

Building reliable quantum gates

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

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

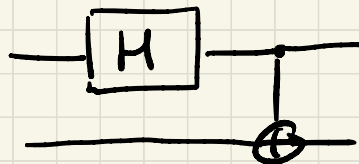
Steane code:

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

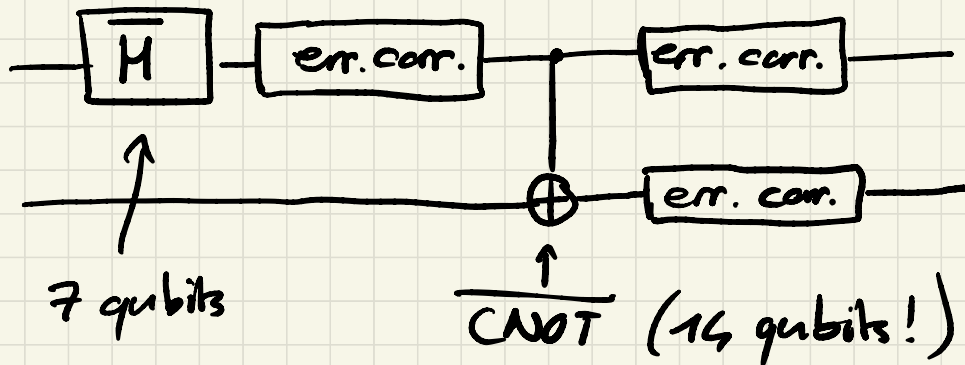
$$\alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|0\rangle_S + \beta|1\rangle_S \quad (= 7 \text{ qubit state})$$

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

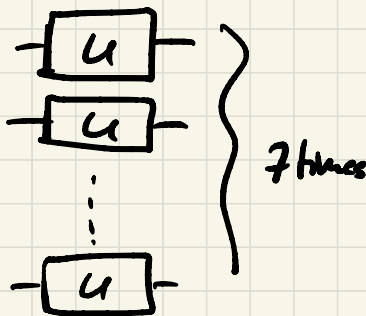
So a circuit like



becomes



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



Now: $S \rightarrow \bar{S}$ is given by

ZS

ZS

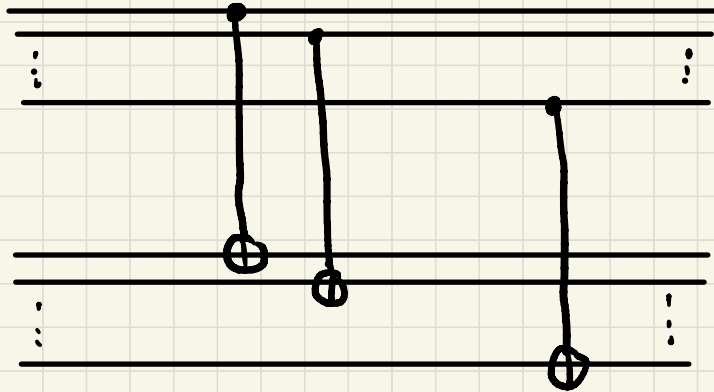
...

ZS

}

7 times

• $CNOT \rightarrow \overline{CNOT}$ becomes:



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

To check: assume an error occurs somewhere
 $|\psi'\rangle = X_3 |\psi\rangle$ e.g.

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

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

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

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

$\nearrow$
all the states are
complement of each other
in these states

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

$$\xrightarrow{\text{Steane}} \alpha|0\rangle_S - \beta|1\rangle_S$$

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

$\uparrow$ even # of 1's $\downarrow$ match! $\uparrow$ odd # of 1's

$$\cdot Y = iXZ \rightarrow \text{fine also}$$

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

$$\rightarrow \text{Stean: } \frac{|0\rangle_S + |1\rangle_S}{\sqrt{2}}, \quad \frac{|0\rangle_S - |1\rangle_S}{\sqrt{2}}$$

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

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

$$\begin{array}{lcl} 2^\circ) & HX = ZH & \rightarrow HXH = Z \\ & HZ = XH & \rightarrow HZH = X \end{array} \left. \vphantom{\begin{array}{lcl} 2^\circ) & HX = ZH & \rightarrow HXH = Z \\ & HZ = XH & \rightarrow HZH = X \end{array}} \right\} \text{same for } \overline{H} !$$

(conjugation)

$$\begin{aligned}
 2^\circ) \quad \overline{H} \overline{X} \overline{H} &= H_1 \dots H_7 X_1 \dots X_7 H_1 \dots H_7 \\
 &= H_1 X_1 H_1 \dots H_7 X_7 H_7 = Z_1 \dots Z_7 = \overline{Z} \\
 \text{and also} \quad \overline{H} \overline{Z} \overline{H} &= \overline{X} \quad \checkmark
 \end{aligned}$$

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

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

$$\text{i.e. } \overline{H} q_i \overline{H} \in S? \quad \text{yes, because (eq):}$$

$$q_1 = X_4 X_5 X_6 X_7 \rightarrow \overline{H} q_1 \overline{H} = Z_4 Z_5 Z_6 Z_7 \in S \quad \checkmark$$