Def: n-qubit **Clifford group** W_n

group of unitary operators U which map all elements of the Pauli group to elements of the Pauli group

(221) $$U G_n U^\dagger \in G_n^* \qquad (^* \text{ w/o } \pm \mathbb{1})$$

The n-qubit Clifford group is generated by the Hadamard gate, the phase gate and the CNOT gate

(222) $$W_n = \langle \{H, S, CNOT\} \rangle$$

rem: • Pauli X, Y, Z are elements of W_n

• the $\pi/8$ gate T is not element of the Clifford group

$$TXT^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

(223) $$= \begin{bmatrix} 0 & e^{-i\pi/4} \\ e^{i\pi/4} & 0 \end{bmatrix} = \underbrace{\frac{1}{\sqrt{2}} X + \frac{1}{\sqrt{2}} Y} \notin G_1$$

number of Pauli's increases by factor 2 in each step

The action of a quantum algorithm that only contains operators from the Clifford group on a suitable inital n-qubit state can efficiently be described classically (e.g. by keeping track of the action of the Clifford gates on the stabilizers of the state.

$\Rightarrow$ Gottesmann-Knill theorem

rem:
- also measurements in the computational basis can easily be described in the stabilizer formalism

(C) Constructing a stabilizer code, error detection, and correction

- $[n, k]$ stabilizer code: constructed of the 2^k orthonormal vectors $|\psi\rangle \in V_S$ of n qubits ($n > k$) stabilized by subgroup $S \subset G_n$

$$S = \langle g_1, g_2, \dots, g_{n-k} \rangle$$

and g_j independent and mutually commuting

$$g_j |\psi\rangle = |\psi\rangle \qquad j = 1, 2, \ldots, n-k$$

- **error detection**

Any error happening on a state $|\psi\rangle$ is an element (or superposition of elements) of G_n

(224) $$E \in G_n$$

So E either commutes or anticommutes with the generators g_j.

I If $\{E, g_e\} = 0$ i.e. it anticommutes with some g_e

(225) $$g_e E |\psi\rangle = -E g_e |\psi\rangle = -E |\psi\rangle$$

while $$g_e |\psi\rangle = |\psi\rangle$$

$\Rightarrow$ action of error easily detectable!

II E commutes with all g_j and $E \in S$

$\Rightarrow$ does not corrupt the code

III E commutes with all g_j but $E \notin S$ not detectable

Def: The set of all operators $E \in G_n$ which commute with all generators of stabilizer S

(225) i.e. $$E g_j = g_j E$$

is called centralizer $Z_1(S)$.

Def: The set of all operators $E \in G_n$ for which holds

(226) $$E g_j E^+ \in S$$

for all generators of stabilizer S are called normalizer $N(S)$

If S does not contain $-\mathbb{1}$ then $N(S) = Z_1(S)$.

Error correction condition for stabilizer codes

Let S be the stabilizer of a stabilizer code $C(S)$. Suppose $\{E_j\}$ is a set of operators in G_n. If

(227) $$E_j^+ E_k \notin N(S) - S \qquad \forall j,k$$

then $\{E_j\}$ is a correctable set of errors for the code $C(S)$

Can we define something analogous to the Hamming distance ?

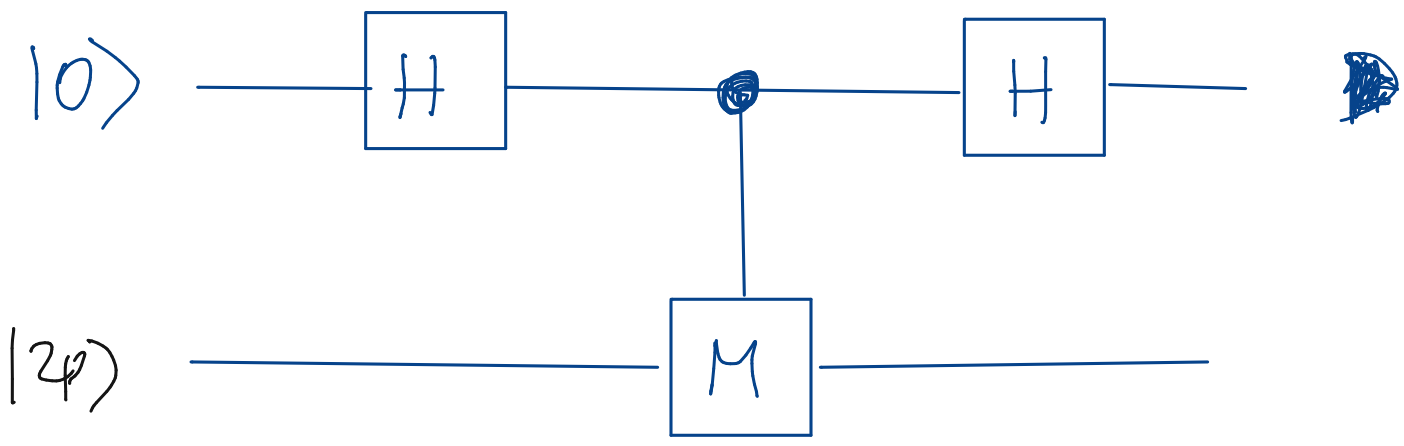
Def: The distance d of a stabilizer code $C(S)$ is the minimum number of single qubit operators different from the identity in $N(S) - S$.

> An $[n, k, d = 2t+1]$ stabilizer code can correct arbitrary qubit errors on any t qubits.

e.g. $E = I_1 I_2 X_3 I_4 Z_5 I_6 I_7 Y_8$ has 3 operators

- Quantum circuit for error detection

quantum circuit for measuring single-qubit operator M with eigenvalues ± 1



$$|\psi\rangle = \alpha |M=+1\rangle + \beta |M=-1\rangle = \alpha|+\rangle + \beta|-\rangle$$

$$|0\rangle|\psi\rangle \xrightarrow{H} \frac{(|0\rangle + |1\rangle)}{\sqrt{2}}|\psi\rangle \xrightarrow{M} \frac{|0\rangle|\psi\rangle + |1\rangle M|\psi\rangle}{\sqrt{2}}$$

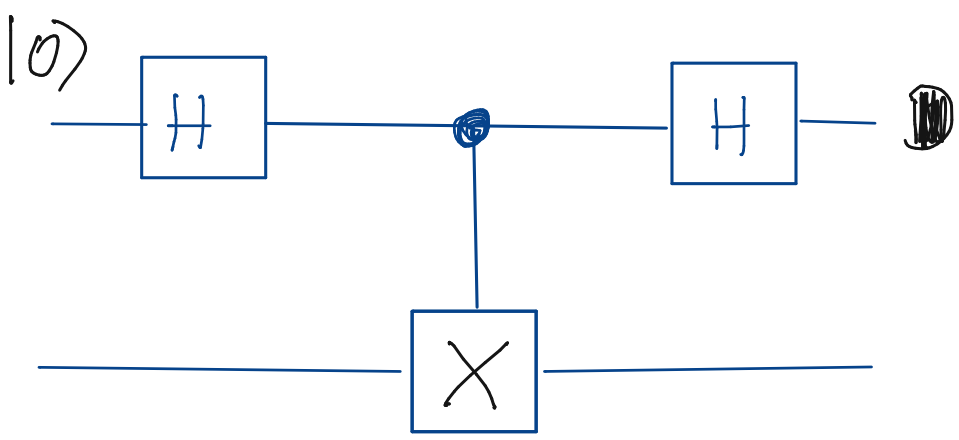
$$= \frac{|0\rangle(\alpha|+\rangle + \beta|-\rangle) + |1\rangle(\alpha|+\rangle - \beta|-\rangle)}{\sqrt{2}}$$

$$= \alpha \frac{|0\rangle + |1\rangle}{\sqrt{2}}|+\rangle + \beta \frac{|0\rangle - |1\rangle}{\sqrt{2}}|-\rangle$$

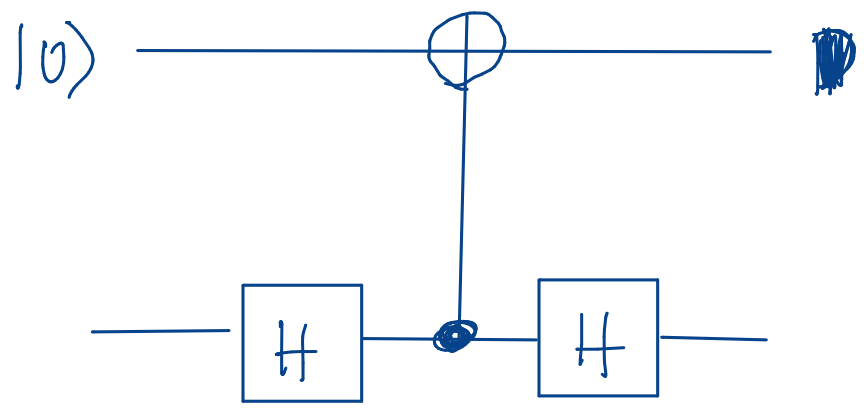
$$\xrightarrow{H} \alpha|1\rangle|+\rangle + \beta|0\rangle|-\rangle$$

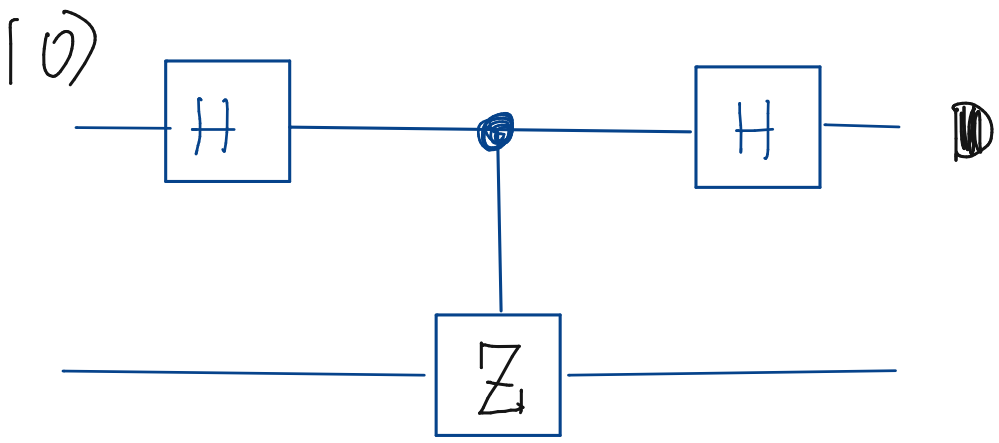
$$p(1) = |\alpha|^2 \qquad p(0) = |\beta|^2$$

equivalent circuit

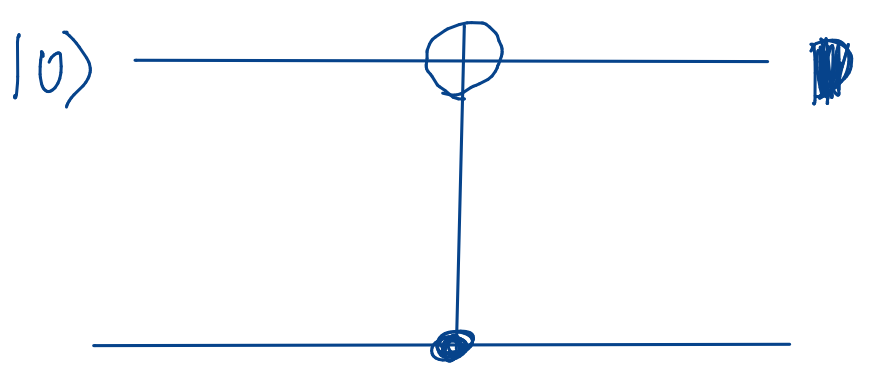


≙





≙



How to construct circuit for detecting error syndroms?
Starting point is the check matrix eq. (213).

(228) $$G = [\underbrace{G_X}_{2n} | \underbrace{G_Z}_{2n}] \Big\}_{n-k}$$

First we bring this matrix into a standard form by

- swapping rows (re-label generators)
- swapping colums simultaneously on the left and right submatrix (relabel qubits)
- adding two rows (multiplying generators)

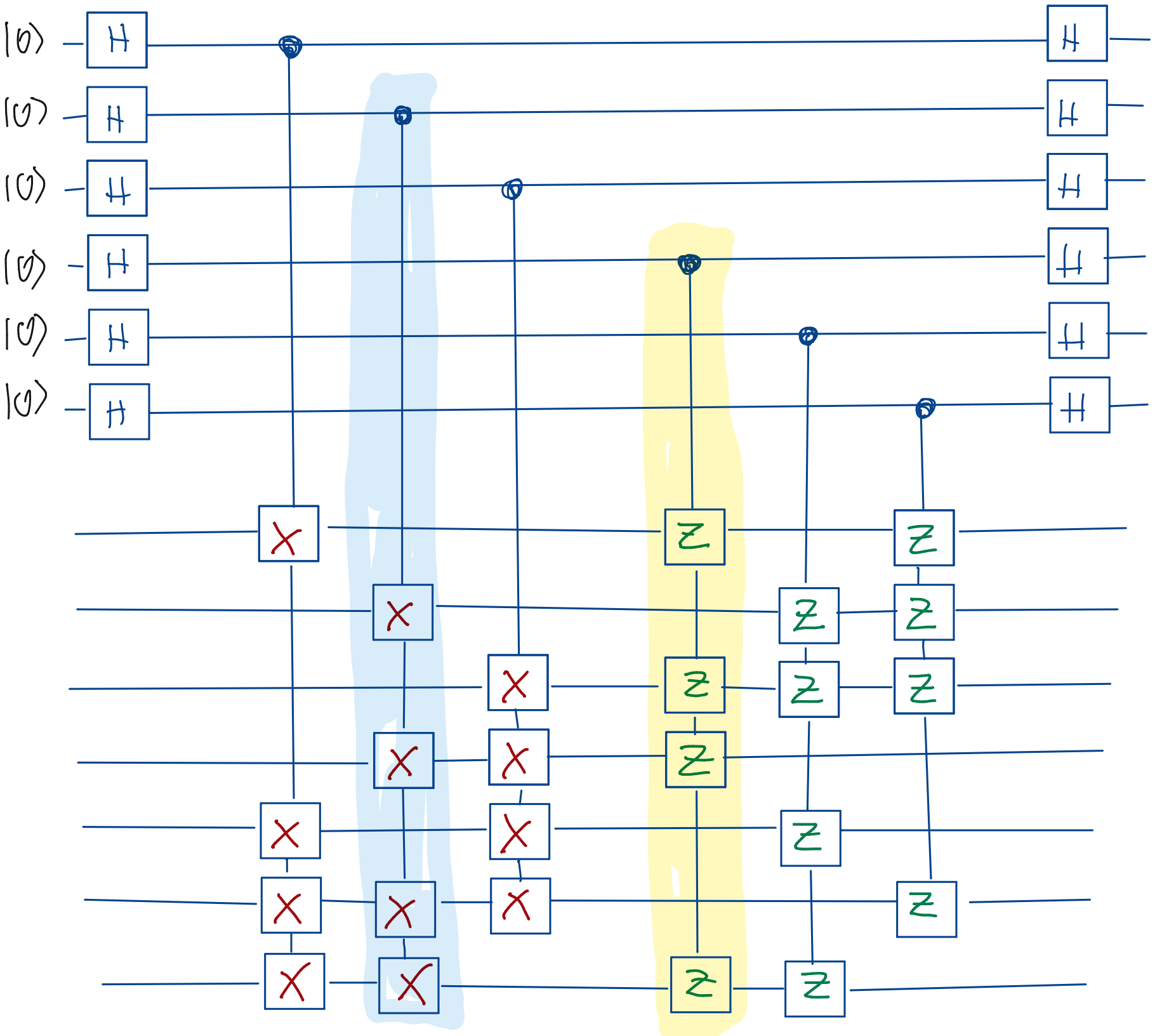
If r is the rank of G_1 than we can bring G to a standard form (not completely unique)

$$\begin{array}{c} \\ r\{ \\ n-k-r\{ \end{array} \overset{\begin{array}{ccc} r & n-k-r & k \end{array}}{\left[\begin{array}{ccc|ccc} \underline{1} & A_1 & A_2 & B & 0 & C \\ 0 & 0 & 0 & D & \underline{1} & E \end{array}\right]}$$

(229)

e.g. standard form of check matrix of 7-qubit Steane code

$$\left[\begin{array}{ccccccc|ccccccc}
1&0&0&0&1&1&1&0&0&0&0&0&0&0\\
0&1&0&1&0&1&1&0&0&0&0&0&0&0\\
0&0&1&1&1&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&1&1&0&0&1\\
0&0&0&0&0&0&0&0&1&1&0&1&0&1\\
0&0&0&0&0&0&0&1&1&1&0&0&1&0
\end{array}\right]$$



$\supset G_X^T$ $\supset G_Z^T$