

Examples

Trivial code  $S = \langle z_{k+1}, z_{k+2}, \dots, z_n \rangle$   $k$  qubits  
 $N(S) = \langle x_1, z_1, \dots, x_k, z_k, S \rangle$   $C = \{ |+\rangle \oplus |0\rangle \}^{\otimes k}$

Repetition code  $S = \langle z_1 z_2, z_2 z_3 \rangle$   
 $N(S) = \langle \bar{x} = x_1 x_2 x_3, \bar{z} = z_1, S \rangle$

Star code  $S = \langle z_1 z_2, z_2 z_3, z_4 z_5, z_5 z_6, z_7 z_8, z_8 z_9 \rangle$   
 $N(S) = \langle \bar{x} = x_1 x_2 x_3, \bar{z} = z_1 z_4 z_7, S \rangle$

When do Paulis commute?  $\Rightarrow$  symplectic  $\mathbb{F}_2$  inner product

$p \in P_n$        $p = (-1)^c x^a z^b$        $q = (-1)^{c'} x^{a'} z^{b'}$

$pq = (-1)^{c+c'} x^a z^b x^{a'} z^{b'}$   
 $= z^{b_1} x^{a_1} \otimes \dots \otimes z^{b_n} x^{a_n}$   
 $= (-1)^{c_1 b_1} x^{a_1} z^{b_1} \otimes \dots$   
 $= (-1)^{a_1 \cdot b} x^{a+c'} z^{b+b'}$

$qp = (-1)^{c+c'+a \cdot b'} x^{a+c'} z^{b+b'}$

$pq = (-1)^{a \cdot b + b \cdot a'} qp$

$a \cdot b + b \cdot a' = \begin{pmatrix} a \\ b \end{pmatrix}^T \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} \begin{pmatrix} a' \\ b' \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}^T \Omega \begin{pmatrix} a' \\ b' \end{pmatrix} = \langle \begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} a' \\ b' \end{pmatrix} \rangle_{\text{symplectic}}$

$S \subset P_n$        $L(S) \subset \mathbb{F}_2^{2n}$        $L(N(S)) = L(S)^\perp$   
subspace of dim  $n$

Clifford sp:  $U x^a z^b U^\dagger = \pm x^{a'} z^{b'}$        $\begin{pmatrix} a' \\ b' \end{pmatrix} = M \begin{pmatrix} a \\ b \end{pmatrix}$

$U^\dagger \Omega U = \Omega$       "symplectic matrix"

corollary Any stabilizer code is equivalent (via Clifford) to the trivial code

$$S = \langle S_1, \dots, S_{n-k} \rangle \quad Z(S) = \langle S, \bar{X}_1, \dots, \bar{X}_k, \bar{Z}_1, \dots, \bar{Z}_k \rangle$$

$$\exists U \text{ (Clifford)} \text{ st. } \begin{aligned} U S_i U^\dagger &= Z_i \\ U \bar{Z}_i U^\dagger &= Z_{n-k+i} \\ U \bar{X}_i U^\dagger &= X_{n-k+i} \end{aligned}$$

CSS codes  $S = \{ Z^a X^b : a \in C_1^\perp, b \in C_2 \}$

$$C(S) = \{ |x + C_2\rangle : x \in C_1 \} \quad C_2 \subset C_1$$

logical operations  $X^a : a \in C_1 / C_2$   
 $Z^b : b \in C_2^\perp / C_1^\perp$

example  $[[7, 1, 3]]$  Steane code

$$S = \langle X_1 X_2 X_3 X_4, X_4 X_5 X_6 X_7, X_1 X_2 X_3 X_4 X_5 X_6 X_7, Z_1 Z_2 Z_3 Z_4, Z_4 Z_5 Z_6 Z_7, Z_1 Z_2 Z_3 Z_4 Z_5 Z_6 Z_7 \rangle$$

$$C(S) = \langle S, \bar{X} = X^{\otimes 7}, \bar{Z} = Z^{\otimes 7} \rangle$$

$$N(S) \text{ includes } H^{\otimes 7} = \bar{H}$$

For 2 copies  $\overline{C_{NOT}} = C_{NOT}^{\otimes 7}$



# Kraus-Lafamme conditions

given a QECC  $C = \text{Im } E \in \mathbb{C}^{2^n}$

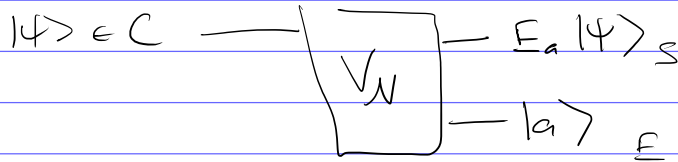
Kraus ops  $E_1, \dots, E_m$  can be corrected iff

$$P E_a^\dagger E_b P = \alpha_{ab} P \quad \text{where } P = \text{proj } C$$

for simplicity, assume  $\alpha_{ab} = \alpha_a \delta_{ab}$

so  $E_i C \perp E_j C$  for  $i \neq j$

correctable means  $\exists$  channel  $R$  s.t.  $R \circ N \circ E = \text{id}$

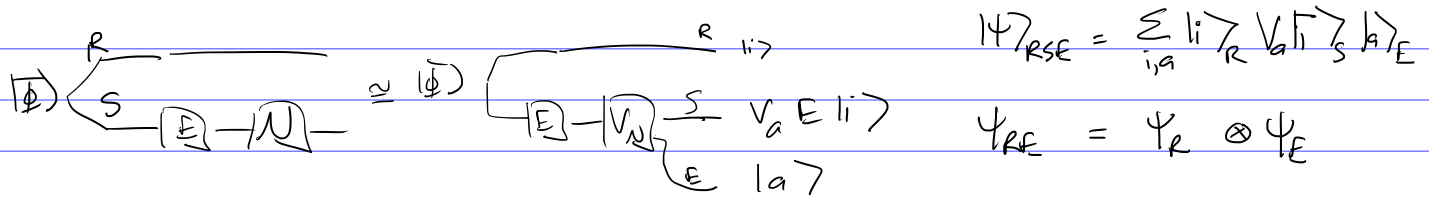


$$\begin{aligned} \text{tr}_S \rightarrow \rho_E &= \sum_{a,b} \langle \psi | E_a^\dagger E_b | \psi \rangle |a\rangle\langle b| = \sum_a \alpha_a |a\rangle\langle a| \\ &= \langle \psi | P E_a^\dagger E_b P | \psi \rangle \\ &= \alpha_{ab} \text{ indep of } |\psi\rangle \end{aligned}$$

to prove  $\exists R$  use two facts

- ① channel action on  $C^\dagger$  determined by action on half of  $|\Phi\rangle = \frac{1}{\sqrt{d}} \sum_{i,j} |i\rangle \otimes |j\rangle$  ( $\text{id} \otimes N(|\Phi\rangle) = \frac{1}{d} \sum_{i,j} |i\rangle\langle j| \otimes N(|i\rangle\langle j|)$ )
- ②  $|\psi\rangle_{AB} = |\phi\rangle_{AB} \iff \psi_A = \phi_A \iff \exists U_B$  s.t.  $|\psi\rangle = (U \otimes I)|\phi\rangle$

- ①  $\Rightarrow$  suffices to consider action on  $|\Phi\rangle$
- ②  $\Rightarrow$  suffices to **decouple**



trace out  $S$

$$\frac{1}{d} \sum_{i,j} |i\rangle\langle j| \otimes \sum_{a,b} |a\rangle\langle b| \langle j | E^\dagger V_b^\dagger V_a E | i \rangle = \frac{I}{d} \otimes \rho_E$$

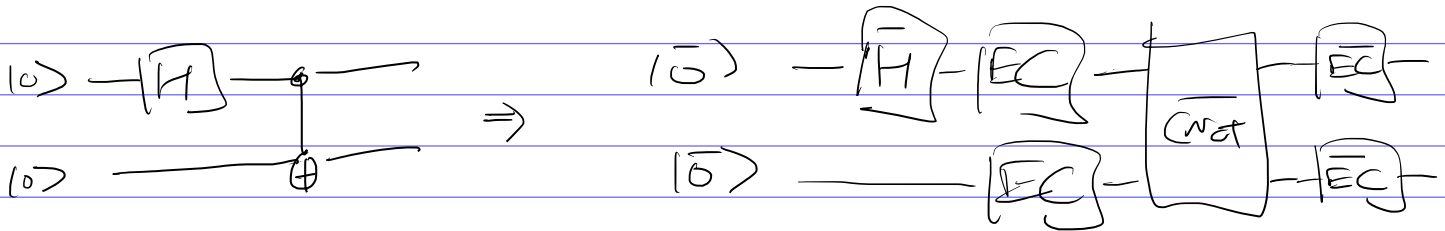
$\underbrace{\quad}_{P \alpha_{ba}} \quad \underbrace{\quad}_{\alpha_{ba} \delta_{ij}}$

$\psi_R \otimes \psi_E$  and  $\psi_{RE}$  purified by  $|\psi\rangle_{RSE}$

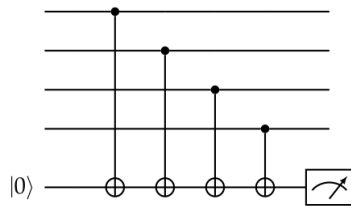
$\exists U_{S_1 S_2}$  s.t.  $(I_{RE} \otimes U) |\psi\rangle = |\Phi\rangle \otimes |\psi\rangle$

# FTQC

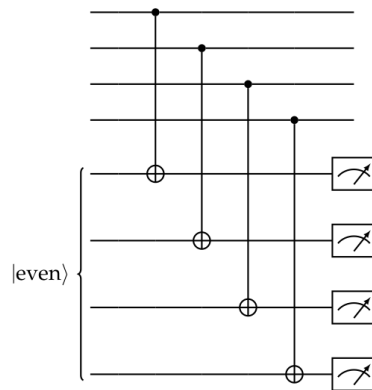
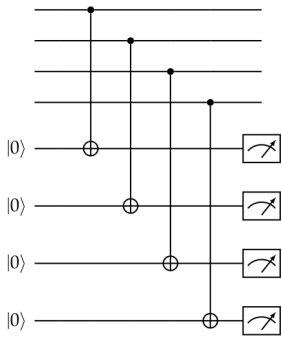
- 1 discrete gate set : Clifford + T
- 2 never decode
- 3 don't propagate errors within code blocks
- 4 FT error correction



FT measurement:  
 $Z_1 Z_2 Z_3 Z_4$



not FT

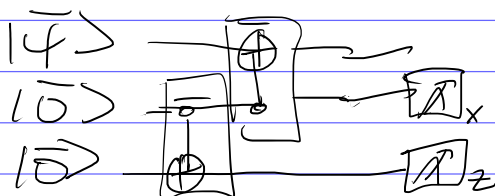


Shor

Also no good

$$|even\rangle = \frac{1}{\sqrt{8}} \sum_{|x| \text{ even}} |x\rangle$$

Another choice is Steane



# Transversal gates

Steane  $\bar{X} = X^{\otimes 7}$   $\bar{Z} = Z^{\otimes 7}$   $\bar{H} = H^{\otimes 7}$   
 $\bar{Cnot} = Cnot^{\otimes 7}$

These generate Clifford group. Not universal  
need a non-Clifford gate, like  $T = \exp(i\frac{\pi}{8}Z)$   
given  $\bar{T}|+\rangle$  can perform  $T$  by teleportation

