Stabilizer codes and logical gates

$$\sigma^{00} = I, \quad \sigma^{01} = \sigma^z, \quad \sigma^{10} = \sigma^x, \quad \sigma^{11} = \sigma^y$$

$$\sigma(\alpha_1, \ldots, \alpha_n | \beta_1, \ldots, \beta_n) = \sigma^{\alpha_1\beta_1} \otimes \cdots \otimes \sigma^{\alpha_n\beta_n}$$

$$\sigma(f)\,\sigma(g) = (-1)^{\omega(f,g)}\,\sigma(g)\,\sigma(f)$$

$$\omega(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n; \alpha'_1, \ldots, \alpha'_n, \beta'_1, \ldots, \beta'_n) = \sum_{j=1}^{n} (\alpha_j\beta'_j - \beta_j\alpha'_j) \mod 2$$

Definition of a stabilizer code

Stabilizer operators: $S_1, \ldots S_l$

$S_j = \pm\sigma(f_j)$, $\quad f_j \in G_n = \mathbb{F}_2^{2n}$

$S_j S_k = S_k S_j \quad \Longleftrightarrow \omega(f_j, f_k) = 0$

$S_1, \ldots, S_l$ are independent $\Longleftrightarrow f_1, \ldots, f_l$ are linearly independent

Stabilizer subgroup:

-- reduced: $D \subseteq G_n$, $\quad D =$ lin. span $\{f_1, \ldots, f_l\}$ over $\mathbb{F}_2$

-- extended: $\tilde{D} \subseteq \tilde{G}_n$, $\quad \tilde{D} = \{ S_1^{\gamma_1} \cdots S_l^{\gamma_l} : \quad \gamma_j = 0, 1 \}$

The code: $\boxed{\mathcal{M} = \{ |\xi\rangle \in \mathcal{B}^{\otimes n} : \ \forall S \in \tilde{D} \quad S|\xi\rangle = |\xi\rangle \}}$

$S^2 = I \Rightarrow S = \pm\sigma(g), \ g \in D$

Example: the 5-qubit code

$$\begin{aligned}
S_1 &= X\ Z\ Z\ X\ I, & f_1 &= (1\,0\,0\,1\,0\,|\,0\,1\,1\,0\,0) \\
S_2 &= I\ X\ Z\ Z\ X, & f_2 &= (0\,1\,0\,0\,1\,|\,0\,0\,1\,1\,0) \\
S_3 &= X\ I\ X\ Z\ Z, & f_3 &= (1\,0\,1\,0\,0\,|\,0\,0\,0\,1\,1) \\
S_4 &= Z\ X\ I\ X\ Z, & f_4 &= (\underbrace{0\,1\,0\,1\,0}_{X\text{ part}}\,|\,\underbrace{1\,0\,0\,0\,1}_{Z\text{ part}})
\end{aligned}$$

$S_1 S_2 = XYIYX \in \tilde{D}$

(In general, elements of $\tilde{D}$ may have a minus sign, e.g. if $S_1 = XXXXII$, $S_2 = IIZZZZ$, then $S_1S_2 = -XXYYZZ$)

Lemma. Any stabilizer code can be transformed to a *trivial code* by some Clifford operator U

$$S_j = \pm\sigma(f_j) \;\longmapsto\; U S_j U^{-1} = \sigma_j^z \quad \text{for } j=1,..,l$$

$$\mathcal{M} \;\longmapsto\; U\mathcal{M} = \boxed{|0^l\rangle \otimes \mathcal{B}^{\otimes(n-l)}}$$

Proof: Suppose we have already turned S_j to σ_j^z for $j=1,..,k-1$. Let's transform S_k to σ_k^z by a Clifford operator that commutes with $\sigma_1^z,..,\sigma_{k-1}^z$.

We have $S_k = \pm P_1 \otimes \cdots \otimes P_n$ (The sign can be changed at step 2 below)

$$P_j = \begin{cases} I, Z & \text{for } j=1,..k-1 \\ I, X, Y, Z & \text{for } j=k,..,n \end{cases}$$

(because $S_jS_k = S_kS_j$ and $S_j = \sigma_j^z$)

$P_r \neq I$ for some $r \in \{k,..,n\}$ (because S_k is independent of $S_1,..,S_{k-1}$)

Step 1: Swap r with k so that $P_k^{(1)} := SWAP \cdot P_k \cdot SWAP^{-1} = P_j \neq I$

Step 2: $P_j^{(1)} \mapsto P_j^{(2)} := U_2\, P_j^{(1)}\, U_2^{-1} \in \{I, Z\}$ (where U_2 is a product of single-qubit Clifford gates)

Step 3: For each $j \neq k$ such that $P_j^{(2)} = Z$, apply $CNOT[j,k]$:

$U_3 = \prod_{j\in A} CNOT[j,k]$, $\quad U_3\sigma_j^z U_3^{-1} = \sigma_j^z$, $\quad U_3\sigma_k^z U_3^{-1} = \sigma_k^z \prod_{j\in A}\sigma_j^z$

Example: $n=5$, $k=3$

$S_3 = Z\ I\ I\ X\ Y$

$SWAP[3,4]$

$S_3^{(1)} = Z\ I\ X\ I\ Y$

$S_3^{(2)} = Z\ I\ Z\ I\ Z$

$CNOT[1,3] \cdot CNOT[5,3]$

$S_3^{(3)} = I\ I\ Z\ I\ I$

Corollary. A code $\mathcal{M}$ given by ℓ stabilizer operators has $\dim \mathcal{M} = 2^{n-\ell}$. (Code of type *[[n,n-l]]*)

Theorem. *Let $\mathcal{M} \subseteq \mathcal{B}^{\otimes n}$ be a code with the reduced stabilizer group D, and let $\mathcal{E} \subseteq \mathbf{L}(\mathcal{B}^{\otimes n})$ have a Pauli basis. Then $\mathcal{M}$ detects errors from $\mathcal{E}$ if and only if*

$$\forall E = \sigma(g) \in \mathcal{E}, \quad g \in D \quad or \quad g \notin D^{+} := \{h \in G_n : \ \forall f \in D \ \ \omega(f,h)=0\}.$$

This space does not have a Pauli basis: $\mathcal{E} = \text{lin. span}\{I, H[j],\ j=1,..,n\}$

Proof

Case 1: $g \in D \Rightarrow E|\xi\rangle = |\xi\rangle$ for all $|\xi\rangle \in \mathcal{M} \Rightarrow \boxed{\langle \xi_1 | E | \xi_2 \rangle = \langle \xi_1 | \xi_2 \rangle}$

$C(E)=1$ (trivial error)

Case 2: $g \notin D^{+} \Rightarrow \omega(f,g)=1$ for some $f \in D \Rightarrow SE = -ES$ for some $S \in \tilde{D}$

$$\Rightarrow S \underbrace{E|\xi\rangle}_{\text{eigenvector}} = -ES|\xi\rangle = -\underbrace{E|\xi\rangle}_{} \Rightarrow E|\xi\rangle \perp \mathcal{M} \qquad \boxed{\langle \xi_1 | E | \xi_2 \rangle = 0}$$

eigenvalue $=-1$

$C(E)=0$ (detectable error)

Case 3: $g \in D^{+} \setminus D$: $\left.\begin{array}{l} g \in D^{+} \Rightarrow E\mathcal{M} = \mathcal{M} \\ g \notin D \Rightarrow E \text{ acts nontrivially on } \mathcal{M} \end{array}\right\} \Rightarrow \boxed{\langle \xi_1 | E | \xi_2 \rangle \not\propto \langle \xi_1 | \xi_2 \rangle}$

(bad error)

W.l.o.g. $\mathcal{M}$ is the trivial code given by $S_j = \sigma_j^z \ (j=1,..,\ell) \Rightarrow E = A \otimes B$

product of *I,Z* on the first *l* qubits — a nontrivial Pauli on the last *n-l* qubits

Stabilizer codes (summary)

$\mathcal{M} \subseteq \mathcal{B}^{\otimes n}$ is defined by the extended stabilizer group $\tilde{D} = \{\text{products of } S_1, \dots, S_\ell\} \subseteq \tilde{G}_n$

(reduced stabilizer group: $D \subseteq G_n = \mathbb{F}_2^{2n}$)

$$\boxed{d(\mathcal{M}) = \min \{ |g| : g \in D^{\perp} \setminus D \}}$$

$|g|$ is the Hamming weight of g

= # of qubits on which $\sigma(g)$ acts nontrivially

$g = (\alpha_1, \dots, \alpha_n | \beta_1, \dots, \beta_n)$, $\sigma(g) = \sigma^{\alpha_1\beta_1} \otimes \cdots \sigma^{\alpha_n\beta_n}$

$|g| = \# \{ j : (\alpha_j, \beta_j) \neq 0 \}$

A stabilizer code is *degenerate* if there is some error $E = \sigma(g) \in \mathcal{E}$ (i.e. $|g| < d(\mathcal{M})$) such that

$g \in D$ but $g \neq 0$

Shor's code is degenerate

$$S_1 = ZZI\ III\ III, \quad S_3 = III\ ZZI\ III, \quad S_5 = III\ III\ ZZI,$$
$$S_2 = IZZ\ III\ III, \quad S_4 = III\ IZZ\ III, \quad S_6 = III\ III\ IZZ,$$
$$S_7 = XXX\ XXX\ III, \qquad S_8 = III\ XXX\ XXX.$$

Type *[[9,1,3]]* $\leftarrow d(\mathcal{M})$

$\sigma(g) = S_1$ is a trivial error of weight < 3

Steane's code and the 5-qubit codes are not degenerate

$$\begin{array}{ll} S_1 = Z\ I\ Z\ I\ Z\ I\ Z & S_4 = X\ I\ X\ I\ X\ I\ X \\ S_2 = I\ Z\ Z\ I\ I\ Z\ Z & S_5 = I\ X\ X\ I\ I\ X\ X \\ S_3 = I\ I\ I\ Z\ Z\ Z\ Z & S_6 = I\ I\ I\ X\ X\ X\ X \end{array}$$

Type *[[7,1,3]]*

(all stabilizer operators an their products have weight ≥ 4)

$$\begin{aligned} S_1 &= X\ Z\ Z\ X\ I, \\ S_2 &= I\ X\ Z\ Z\ X, \\ S_3 &= X\ I\ X\ Z\ Z, \\ S_4 &= Z\ X\ I\ X\ Z. \end{aligned}$$

Type *[[5,1,3]]*

Logical operators

"Bad errors" (ones that preserve the code subspace but act on it nontrivially) are not always bad. When applied in a controlled fashion, such operators can be very useful. In particular, unitary logical operators act on the logical qubits without decoding them.

Let $V:\mathcal{L}\to\mathcal{N}$ $\left(V^{+}V=I_{\mathcal{L}},\ \mathrm{Image}\,V=\mathcal{M}\right)$ be an encoding for the quantum code $\mathcal{M}\subseteq\mathcal{N}$.

Definition. An operator $\tilde{A}$ acting in $\mathcal{N}$ is called *logical* if it preserves the code. It is called *logical* A for some A acting in $\mathcal{L}$ if $\underbrace{\forall\,|\psi\rangle\in\mathcal{L}\quad \tilde{A}V|\psi\rangle=VA|\psi\rangle}$,

equivalently, $\tilde{A}V=VA$, or the diagram

$$\begin{tikzcd} \mathcal{L} \arrow[r, "A"] \arrow[d, "V"'] & \mathcal{L} \arrow[d, "V"] \\ \mathcal{N} \arrow[r, "\tilde{A}"] & \mathcal{N} \end{tikzcd}$$

commutes

Examples

-- For any stabilizer code, $\sigma(g):\ g\in D^{+}$ is a logical operator

-- Shor's code $V:\ \mathcal{B}\to\mathcal{B}^{\otimes 9}$, $\quad V|x\rangle=\frac{1}{2}\sum\limits_{x_1\oplus x_2\oplus x_3=x}|x_1,x_1,x_1,\ x_2,x_2,x_2,\ x_3,x_3,x_3\rangle$

$X^{\otimes 9}$ is a logical X: $\quad X^{\otimes 9}V|x\rangle=\frac{1}{2}\sum\limits_{x_1\oplus x_2\oplus x_3=x}|\bar{x}_1\bar{x}_1\bar{x}_1,\ \bar{x}_2\bar{x}_2\bar{x}_2,\ \bar{x}_3\bar{x}_3\bar{x}_3\rangle=V|\bar{x}\rangle=VX|x\rangle$

$\bar{x}:=x\oplus 1$

$Z^{\otimes 9}$ is a logical Z: $\quad Z^{\otimes 9}V|x\rangle=\frac{1}{2}\sum\limits_{x_1\oplus x_2\oplus x_3=x}(-1)^{3(x_1+x_2+x_3)}|x_1x_1x_1,x_2x_2x_2,x_3x_3x_3\rangle=(-1)^{x}V|x\rangle=VZ|x\rangle$

These operators are *transversal*, i.e. products of single-qubit operators

Definition. A CSS code is called *self-dual* if it is defined by $S_j = \sigma^z(f_j)$, $S_{\ell+j} = \sigma^x(f_j)$ $(j=1,\dots,\ell)$

same indicator vectors $f_j \in \mathbb{F}_2^n$

Equivalently, $D_x = D_z$

Example: Steane's code

$$
\begin{aligned}
S_1 &= Z\ I\ Z\ I\ Z\ I\ Z & \qquad S_4 &= X\ I\ X\ I\ X\ I\ X\\
S_2 &= I\ Z\ Z\ I\ I\ Z\ Z & \qquad S_5 &= I\ X\ X\ I\ I\ X\ X\\
S_3 &= I\ I\ I\ Z\ Z\ Z\ Z & \qquad S_6 &= I\ I\ I\ X\ X\ X\ X
\end{aligned}
$$

Theorem. For a self-dual CSS code of type *[[2l+1,1]]*, any Clifford operator acting on one or several qubits can be realized as a transversal logical operator acting on the corresponding code blocks.

Logical *X* and *Z* are realized as $X_L = X^{\otimes n}$ and $Z_L = Z^{\otimes n}$, respectively $(n = 2\ell+1)$

All $f \in D_x = D_z$ have even weight because $D_x \perp D_z$, and hence, $0 = (f,f) = |f| \bmod 2$

Thus, $X^{\otimes n} S_j = S_j X^{\otimes n}$, $Z^{\otimes n} S_{\ell+j} = S_{\ell+j} Z^{\otimes n} \Rightarrow X^{\otimes n}, Z^{\otimes n}$ preserve the code

$$
\left.
\begin{aligned}
|0_L\rangle &:= V|0\rangle = 2^{-\ell/2} \sum_{w \in D_x} |w\rangle\\
|1_L\rangle &:= V|1\rangle = 2^{-\ell/2} \sum_{w \in D_x} |w \oplus 1^n\rangle
\end{aligned}
\right\} \Rightarrow \underline{X^{\otimes n}|x_L\rangle = |(x\oplus 1)_L\rangle, \quad Z^{\otimes n}|x_L\rangle = (-1)^x |x_L\rangle}
$$

Since the Clifford group is generated by *H*, *K*, and *CNOT*, proving the theorem amounts to constructing logical versions of these gates.

Logical Hadamard gate

$$H^{\otimes n} S_j (H^{\otimes n})^{-1} = S_{\ell+j}, \quad H^{\otimes} S_{\ell+j} (H^{\otimes n})^{-1} = S_j$$

$\Rightarrow$ $H^{\otimes n}$ preserves the code

$\Rightarrow$ $H^{\otimes n}$ is a logical *A* for some *A*

$$H^{\otimes n} X_L (H^{\otimes n})^{-1} = Z, \quad H^{\otimes n} Z_L (H^{\otimes n})^{-1} = X$$

$\Rightarrow$ $AXA^{-1} = Z, \quad AZA^{-1} = X$

$\Rightarrow$ $A = cH$ for some $c = e^{i\varphi}$

To show that $c=1$, we need to demonstrate that $H^{\otimes n}|0_L\rangle = \frac{1}{\sqrt{2}}\left(|0_L\rangle + |1_L\rangle\right)$ (homework problem)

Logical *K*

For simplicity, we assume that our CSS code is *doubly even*, i.e that $|f_j| \equiv 0 \pmod 4$

$$K = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

$$K \sigma^z K^{-1} = \sigma^z$$

$$K \sigma^x K^{-1} = \sigma^y$$

$$K \sigma^y K^{-1} = -\sigma^x$$

$$K^{\otimes n} S_j \left(K^{\otimes n}\right)^{-1} = S_j$$ (obvious because $S_j = \sigma^z(f_j)$)

$$K^{\otimes n} \underbrace{S_{\ell+j}}_{\sigma^x(f_j)} \left(K^{\otimes n}\right)^{-1} = \sigma^y(f_j) = i^{|f_j|} \sigma^x(f_j)\, \sigma^z(f_j) = S_{\ell+j} S_j$$

because $\sigma^y = i\,\sigma^x \sigma^z$

$\Rightarrow$ $K^{\otimes n}$ preserves the code

$$K^{\otimes n} X_L \left(K^{\otimes n}\right)^{-1} = i^n X_L Z_L = (-1)^\ell Y_L$$

$$K^{\otimes n} Z_L \left(K^{\otimes n}\right)^{-1} = Z_L$$

$\Rightarrow$ $K^{\otimes n}$ is a logical $\begin{cases} K & \text{if } l \text{ is even} \\ K^{-1} & \text{if } l \text{ is odd} \end{cases}$

up to an overall phase

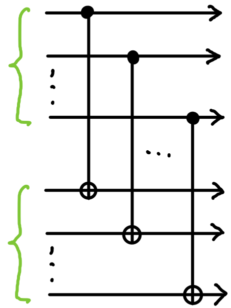
(Fixing the phase and dispensing with the "doubly even" assumption is a homework problem)

Logical *CNOT*

$CNOT_L =$

encoded qubit 1
(stabilizers $S_j^{(1)}, S_{\ell+j}^{(1)}$)

encoded qubit 2
(stabilizers $S_j^{(2)}, S_{\ell+j}^{(2)}$)



$$S_j^{(1)} \mapsto S_j^{(1)}, \qquad S_{\ell+j}^{(1)} \mapsto S_{\ell+j}^{(1)} S_{\ell+j}^{(2)}$$

$$\underbrace{S_j^{(2)} \mapsto S_j^{(1)} S_j^{(2)},}_{\text{products of } Z} \qquad \underbrace{S_{\ell+j}^{(2)} \mapsto S_{\ell+j}^{(2)}}_{\text{products of } X}$$

$$|x_L\rangle = 2^{-\ell/2} \sum_{u \in D_x} |u \oplus x^n\rangle, \qquad |y_L\rangle = 2^{-\ell/2} \sum_{v \in D_x} |v \oplus y^n\rangle$$

$$CNOT_L\big(|x_L\rangle \otimes |y_L\rangle\big) = |x_L\rangle \otimes |(y \oplus x)_L\rangle$$

The transversal CNOT works for any CSS code with $\mathbb{F}_2$-linear encoding $\tau : \{0,1\}^k \to D_z^\perp / D_x$

$$|x_L\rangle = V|x\rangle = |\psi_{\tau(x)}\rangle = \frac{1}{\sqrt{|D_x|}} \sum_{w \in \tau(x)} |w\rangle$$

This completes the proof that for a self-dual CSS code, logical Clifford gates can be realized transversally.

Related results. (We will derive them later)

-- Some stabilizer codes have some non-Clifford transversal logical gates

-- No code admits a universal set of transversal logical gates