Quantum stabilizer codes

Shor's 9-qubit code (recap)

$$\mathcal{M}_{\text{Shor}} = \text{Image}(V_{\text{Shor}}), \qquad V_{\text{Shor}} : \mathcal{B} \to \mathcal{B}^{\otimes 9}, \qquad V_{\text{Shor}}^\dagger V_{\text{Shor}} = I_{\mathcal{B}}.$$

$$V_{\text{Shor}}|x\rangle = \frac{1}{2} \sum_{x_1 \oplus x_2 \oplus x_3 = x} |x_1, x_1, x_1,\ x_2, x_2, x_2,\ x_3, x_3, x_3\rangle$$

code of type *[[9,1]]*:
encodes $\mathcal{B} = \mathbb{C}^2$ (1 qubit)
into $\mathcal{B}^{\otimes 9}$ (9 qubits)

Description in terms of stabilizer operators

$$\boxed{\mathcal{M} = \{ |\xi\rangle \in \mathcal{N} : \ S_j |\xi\rangle = |\xi\rangle \text{ for all } j \}}$$

$\mathcal{N} = \mathcal{B}^{\otimes 9}$, $\quad j = 1, .., 8$

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

$X = \sigma^x$, $Y = \sigma^y$, $Z = \sigma^z$

$ZZI = \sigma^z \otimes \sigma^z \otimes I$

Let $|\xi\rangle = V_{\text{Shor}} |x\rangle$

$S_1 |\xi\rangle = |\xi\rangle \iff$ all basis vectors $|a_1, a_2, .., a_9\rangle$ that enter $|\xi\rangle$ have $a_1 = a_2$ $(= x_1)$

$S_7 |\xi\rangle = |\xi\rangle \iff$ $|\xi\rangle$ does not change if we flip the first 6 bits $x_1 \mapsto x_1 \oplus 1$, $x_2 \mapsto x_2 \oplus 1$

Stabilizer codes

Defined by independent stabilizer operators $S_j = \pm P_1 \otimes \cdots \otimes P_n$,

such that $S_j S_\ell = S_\ell S_j$

$P_1, \dots, P_n \in \{I, X, Y, Z\}$

Examples

Steane' s code

$$S_1 = Z\ I\ Z\ I\ Z\ I\ Z \qquad S_4 = X\ I\ X\ I\ X\ I\ X = \sigma^x(1010101)$$
$$S_2 = I\ Z\ Z\ I\ I\ Z\ Z \qquad S_5 = I\ X\ X\ I\ I\ X\ X$$
$$S_3 = I\ I\ I\ Z\ Z\ Z\ Z \qquad S_6 = I\ I\ I\ X\ X\ X\ X$$

Type *[[7,1]]*,
based on the Hamming code
with the check matrix

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

This code belongs to the family of *Calderbank-Shor-Steane (CSS) codes*:
the stabilizer operators have the form

$$\sigma^z(f) = (\sigma^z)^{f_1} \otimes \cdots \otimes (\sigma^z)^{f_n} \quad \text{or} \quad \sigma^x(f) = (\sigma^x)^{f_1} \otimes \cdots \otimes (\sigma^x)^{f_n}, \qquad f = (f_1, \dots, f_n) \in \mathbb{F}_2^n.$$

The 5-qubit code

$$S_1 = X\ Z\ Z\ X\ I,$$
$$S_2 = I\ X\ Z\ Z\ X,$$
$$S_3 = X\ I\ X\ Z\ Z,$$
$$S_4 = Z\ X\ I\ X\ Z.$$

Type *[[5,1]]*

CSS codes

$\mathcal{M} = CSS(D_z, D_x)$ is defined by stabilizer operators $\sigma^z(f_j^{(z)})$, $\sigma^x(f_k^{(x)})$ such that $f_1^{(z)}, \dots, f_p^{(z)}$ form a basis of D_z and $f_1^{(x)}, \dots, f_q^{(x)}$ form a basis of D_x.
($D_z, D_x \subseteq \mathbb{F}_2^n$; $D_z \perp D_x$ so that all stabilizer operator commute.)

$f_j^{(z)}$, $f_k^{(x)}$ are the check vectors of classical codes $C_z = D_z^\perp$, $C_x = D_x^\perp$

$$\sigma^z(u)\,\sigma^x(v) = (-1)^{(u,v)}\,\sigma^x(v)\,\sigma^z(u)$$

For Shor's code,

$D_z^\perp = \{(x_1, x_1, x_1, x_2, x_2, x_2, x_3, x_3, x_3)\}$

$D_x = \{(x_1, x_1, x_1, x_2, x_2, x_2, x_3, x_3, x_3) : x_1 + x_2 + x_3 = 0\}$

e.g. $S_7 = \sigma^x(111\ 111\ 000)$, $S_8 = \sigma^x(000\ 111\ 111)$

Explicit form of the stabilizer conditions

Let $|\xi\rangle = \sum_{w \in \mathbb{F}_2^n} c_w |w\rangle \in \mathcal{M}$

$u \in D_z$: $\underbrace{\sigma^z(u)|\xi\rangle}_{\sum_w c_w (-1)^{(u,w)} |w\rangle} = |\xi\rangle \iff c_w = 0$ unless $(u,w) = 0$

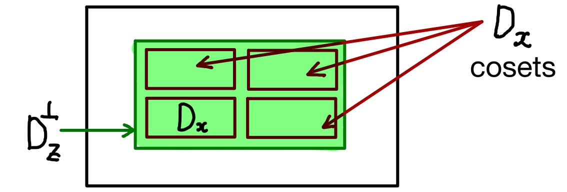
$v \in D_x$: $\underbrace{\sigma^x(v)|\xi\rangle}_{\sum_w c_w |w+v\rangle} = |\xi\rangle \iff c_w = c_{w+v}$

$c_w \neq 0$ only if $w \in D_z^\perp$

$c_w = c_{w'}$ if $w' - w \in D_x$

Some CSS codevectors

$$|\Psi_0\rangle = \frac{1}{\sqrt{|D_x|}} \sum_{w\in D_x} |w\rangle, \quad \text{e.g. } \frac{1}{2}\sum_{x_1+x_2+x_3=0} |x_1,x_1,x_1,x_2,x_2,x_2,x_3,x_3,x_3\rangle$$



$D_x \subseteq D_z^\perp$ because $D_x \perp D_z$

$$\boxed{|\Psi_K\rangle = \frac{1}{\sqrt{|D_x|}} \sum_{w\in K} |w\rangle \quad \text{-- basis vectors of } \mathcal{M}}$$

$K \in D_z^\perp / D_x$ -- quotient space (the set of D_x cosets)

$K = \tilde{K} + D_x = \{\tilde{K} + v : \; v \in D_x\}$ -- a coset $\qquad \tilde{K} \in D_z^\perp$ -- a representative of K

General form of CSS codevectors:
$$\boxed{|\xi\rangle = \sum_{K\in D_z^\perp/D_x} c_K |\Psi_K\rangle}$$

Logical operators (preserve the code but not individual codevectors)

$$\boxed{\begin{array}{ll} \sigma^x(g), & g\in D_z^\perp \\ \sigma^z(h), & h\in D_x^\perp \end{array}}$$

$$\sigma^x(g)|\Psi_K\rangle = \frac{1}{\sqrt{D_x}} \sum_{w\in K} |w+g\rangle = |\Psi_{K+g}\rangle$$ $\in \mathcal{M}$ because $g\in D_z^\perp$

constant if w changes by an element of D_x

$$\sigma^z(h)|\Psi_K\rangle = \frac{1}{\sqrt{D_x}} \sum_{w\in K} (-1)^{(h,w)} |w\rangle = (-1)^{(h,\tilde{K})} |\Psi_K\rangle$$

Error correction and detection (for general codes)

$\mathcal{E} \subseteq \mathbb{L}(\mathcal{N}, \mathcal{N})$ -- error space

Quantum error correction condition:

$$\forall |\xi_1\rangle, |\xi_2\rangle \in \mathcal{M}, \quad \forall E_1, E_2 \in \mathcal{E} \quad \langle \xi_1 | \underbrace{E_1^\dagger E_2}_{E} | \xi_2 \rangle = c(E_1^\dagger E_2) \langle \xi_1 | \xi_2 \rangle$$

$$\underline{E \in \mathcal{E}^\dagger \mathcal{E} = \text{lin. span}\{E_1^\dagger E_2 : \ E_1, E_2 \in \mathcal{E}\}}, \qquad \text{e.g. } \mathcal{E}(n,r)^\dagger \mathcal{E}(n,r) = \mathcal{E}(n, 2r)$$

Definition. A code $\mathcal{M}$ *detects errors from* $\widetilde{\mathcal{E}}$ if there is a linear map $c : \widetilde{\mathcal{E}} \to \mathbb{C}$ such that

$$\forall |\xi_1\rangle, |\xi_2\rangle \in \mathcal{M} \quad \forall E \in \widetilde{\mathcal{E}}, \qquad \langle \xi_1 | E | \xi_2 \rangle = c(E) \langle \xi_1 | \xi_2 \rangle.$$

Caveat: Since quantum codes can be degenerate, the error operator may have no effect on codevectors at all. The code only allows for the detection of the reduced error, i.e. the resulting change of the quantum state. It guarantees that if no error is detected, then quantum information has remained intact.

Code distance

$$d(\mathcal{M}) = \min\{p : \ \mathcal{M} \text{ does not detect errors from } \mathcal{E}(n,p)\} \qquad (\text{where } \mathcal{M} \subseteq \mathcal{B}^{\otimes n})$$

A code of distance d protects from errors in $\mathcal{E}(n,r)$, $r = \left\lfloor \frac{d-1}{2} \right\rfloor$ and detects errors in $\mathcal{E}(n, d-1)$

Error detection for CSS codes

Since $\tilde{\mathcal{E}} = \mathcal{E}(n,p)$ has a Pauli basis, it is sufficient to consider Pauli errors, $E = \underbrace{\sigma^x(f_x)}_{\text{bit flip}}\underbrace{\sigma^z(f_z)}_{\text{phase error}}$

For CSS codes, bit flips and phase errors can be detected or corrected separately.

Let us consider <u>bit flips</u>. (Properties of phase errors follow from the $\sigma^x \leftrightarrow \sigma^z$ duality.)

$$E = \sigma^x(g), \qquad |\xi_1\rangle, |\xi_2\rangle \in \mathcal{M}, \qquad \langle \xi_1 | E | \xi_2 \rangle \overset{?}{=} C(E)\langle \xi_1 | \xi_2 \rangle$$

fixed   vary

$$|\xi_2\rangle = \sum_{k \in D_z^\perp / D_x} c_k |\psi_k\rangle \quad \Rightarrow \quad \boxed{E|\xi_2\rangle = \sum_{k \in D_z^\perp / D_x} c_k |\psi_{k+g}\rangle}$$

Case 1: $g \notin D_z^\perp \Rightarrow E|\xi_2\rangle \perp \mathcal{M} \Rightarrow \langle \xi_1 | E | \xi_2 \rangle = 0 \Rightarrow C(E) = 0$ (detectable error)

Case 2: $g \in D_x \Rightarrow E|\xi_2\rangle = |\xi_2\rangle \Rightarrow \langle \xi_1 | E | \xi_2 \rangle = \langle \xi_1 | \xi_2 \rangle \Rightarrow C(E) = 1$ (trivial error)

Case 3: $\underbrace{g \in D_z^\perp \setminus D_x}_{\text{bad error (= nontrivial logical operator)}} \Rightarrow E|\xi_2\rangle \in \mathcal{M}$, but $E|\xi_2\rangle \neq \text{const} \cdot |\xi_2\rangle \Rightarrow C(E)$ cannot be defined

Error detection for CSS codes: conclusions

A bit flip $\sigma^x(g)$ is bad if $g \in D_z^\perp \setminus D_x$

(backslash means set difference)

$g \in D_z^\perp \iff \sigma^x(g)$ commutes with $S_j = \sigma^z(f_j^{(z)})$

$g \notin D_x \iff \sigma^x(g)$ is not a product of $S_k = \sigma^x(f_k^{(x)})$

A phase error $\sigma^z(h)$ is bad if $h \in D_x^\perp \setminus D_z$ (by the $\sigma^x \leftrightarrow \sigma^z$ duality)

$$\boxed{d(\mathcal{M}) = \min\{d_x, d_z\} \qquad \begin{aligned} d_x &= \min\{|g| : g \in D_z^\perp \setminus D_x\} \\ d_z &= \min\{|h| : h \in D_x^\perp \setminus D_z\} \end{aligned}} \quad \begin{aligned} &\geq d(D_z^\perp) \\ &\geq d(D_x^\perp) \end{aligned}$$

for nondegenerate codes, these are equalities

Example: Steane's 7-qubit code

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

$D_z^\perp = D_x^\perp = \mathrm{Ham}(3) \Rightarrow d_x = d_z \geq 3$

Actually, $d = d_x = d_z = 3$

$E = X\ X\ X\ I\ I\ I\ I = \sigma^x(1110000)$ is a bad error of weight 3, i.e. it commutes with Z-stabilizers but is not a product of X-stabilizers

$E' = X\ X\ X\ X\ X\ X\ X = E \cdot \underbrace{S_6}_{\text{acts trivially on codevectors}}$

E and *E*' are equivalent logical operators.
E is more likely to occur spontaneously;
E' is more convenient when applied intentionally

Symplectic formalism (preparation for the study of general stabilizer codes)

1 qubit

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

$$\sigma^{\alpha\beta}\sigma^{\alpha'\beta'} = C\,\sigma^{\alpha+\alpha',\,\beta+\beta'} = (-1)^{\omega(\alpha,\beta;\alpha',\beta)}\sigma^{\alpha'\beta'}\sigma^{\alpha\beta}$$

$C \in \{1, i, -1, -i\}$

***n* qubits**

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

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

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

This formalism has origin in Hamiltonian mechanics.

Consider linear combinations of canonical coordinates and momenta:

$$\hat{Q}(\alpha_1,..,\alpha_n;\beta_1,..,\beta_n) = \sum_{j=1}^{n}(\alpha_j\hat{x}_j + \beta_j\hat{p}_j)$$

real variables

$$\omega(f,g) = -\omega(g,f)$$

$$[\hat{Q}(f),\hat{Q}(g)] = i\,\underbrace{\omega(f,g)}_{\text{real symplectic form}}$$

Non-degeneracy:

$$\forall f \neq 0 \quad \exists g \quad \omega(f,g) \neq 0$$

Pauli group

-- reduced: $G_n = \mathbb{F}_2^{2n}$

-- extended: $\tilde{G}_n = \{ c\,\sigma(f) : \; f \in G_n, \quad c \in \{1, i, -1, -i\} \}$

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

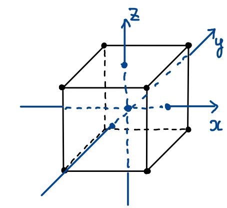
For example, $i \cdot X I Y \in \tilde{G}_n$

Clifford operators: unitary operators U that preserve $\tilde{G}_n$ when acting by conjugation $\boxed{P \mapsto U P U^{-1}}$

Pauli operators: $U = \sigma(g), \qquad U \sigma(f) U^{-1} = (-1)^{\omega(g,f)} \sigma(f)$

The Hadamard gate: $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

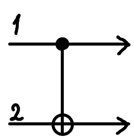
$$\sigma^x \mapsto H \sigma^x H^{-1} = \sigma^z$$
$$\sigma^y \mapsto -\sigma^y$$
$$\sigma^z \mapsto \sigma^x$$



$\frac{\pi}{2}$ -rotation: $K = \sqrt{i}\, e^{-i \frac{\pi}{4} \sigma^z} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$

$$\sigma^x \mapsto \sigma^y, \quad \sigma^y \mapsto -\sigma^x, \quad \sigma^z \mapsto \sigma^z$$

CNOT: $CNOT[1,2] =$



$$\sigma_1^x \mapsto \sigma_1^x \sigma_2^x \qquad \sigma_1^z \mapsto \sigma_1^z$$
$$\sigma_2^x \mapsto \sigma_2^x \qquad \sigma_2^z \mapsto \sigma_1^z \sigma_2^z$$

Clifford group

-- reduced: all Clifford operators considered up to an overall phase,

i.e. automorphisms of the extended Pauli group preserving *1, i, -1, -i*

Automorphism defined by a unitary operator *U*: $P \longmapsto f_U(P) = U P U^{-1}$

(This is an automorphism because $f_U(P_1 P_2) = f_U(P_1) f_U(P_2)$)

For example, Cl_1 is the group of rotational symmetries of the cube; $|Cl_1| = 24$

-- extended: actual Clifford operators with certain phases;

includes the constants $\underbrace{e^{i\frac{\pi}{4}s}, \quad s = 0, .., 7}$

$e^{i\frac{\pi}{4}} = \frac{1+i}{\sqrt{2}} = (H K)^3$

$|\widetilde{Cl}_1| = 24 \cdot 8 = 192$

$\widetilde{Cl}_1$ is generated by H, K

$\widetilde{Cl}_n$ is generated by $H[j], K[j], CNOT[j,k]$