5. Stabilizer codes

Have seen, e.g. for 3-qubit / 9-qubit code:

code space = joint +1 eigenspace of Paulis

error & correction $\longleftrightarrow$ anti-comm. pattern

$\longrightarrow$ General framework?

a) Definition

Definition: The Pauli group $\mathcal{G} \equiv \mathcal{G}_n$ on n qubits is

$$\mathcal{G} := \{ i^\ell P_1 \otimes \ldots \otimes P_n \mid P_i = I, X, Y, Z \, ; \ell = 0, \ldots, 3 \}$$

Note: Any two $S_1, S_2 \in \mathcal{G}$ either commute or anti-commute.

Definition (Stabilizer group, stabilizer code)

A subgroup $\mathcal{S} \subset \mathcal{G}$ with $-I \notin \mathcal{S}$ is called a stabilizer group $\mathcal{S}$. Since $-I \notin \mathcal{S} \Rightarrow S_1, S_2 \in \mathcal{S}$ commute (else $S_1 S_2 S_1^{-1} S_2^{-1} = -I$); this also implies $S = \pm \otimes P_i \;\; \forall S \in \mathcal{S}$.

The elements $S \in \mathcal{S}$ are called stabilizers.

$\mathcal{S}$ defines a subspace $\mathcal{C} \subset (\mathbb{C}^2)^{\otimes n}$,

$$\mathcal{C} := \{ |\psi\rangle \,|\, |\psi\rangle = S|\psi\rangle \ \forall S \in \mathcal{S} \},$$

the code space of a stabilizer code.

$\mathcal{S}$ can also be characterized by a minimal set of generators $S_1, \dots, S_r \in \mathcal{S}$.

Lemma: $\dim \mathcal{C} = 2^{n-r}$.

Proof: (sketch!)

i) S_1 has same # of ± 1 eigenvalues (as $\operatorname{tr} S_1 = 0$)

$\Rightarrow$ split space in half.

$\Pi_1 = \frac{1}{2}(I + S_1)$: proj. on $+1$ eigenspace of S_1.

ii) $\Pi_1 S_2 = S_2 \Pi_1$ (as $S_1 S_2 = S_2 S_1$),

and $\Pi_1 S_2 \Pi_1 = \frac{1}{2}(I + S_1) S_2$

$\mathbb{1}$ - eigensp. of S_2 on +1 - eigenspace of S_1
(0 on -1 - eigensp. of S_1)

$$\mathrm{tr}\left(\tfrac{1}{2}(\mathbb{1}+S_1)S_2\right) = \tfrac{1}{2}\Big(\underbrace{\mathrm{tr}(S_1)}_{=0} + \underbrace{\mathrm{tr}(S_1S_2)}_{=0\text{: ind. set of gen.-s}}\Big)$$

$$= 0$$

$\Rightarrow$ S_2 has eq. # of +1/-1 eigenvals

on +1 - eigenspace of S_1

$\Rightarrow$ split again in half.

iii) continue inductively! ☒

b) Error correction conditions for stabilizer codes

What about error corr. conditions?

E_α Pauli errors.

$E_\alpha^\dagger E_\beta$ have three possibilities:

i) $E_\alpha^\dagger E_\beta$ anti-comm. with some $S \in \mathcal{S}$:

$$\langle \hat{i} | E_\alpha^\dagger E_\beta | \hat{j} \rangle = \langle \hat{i} | E_\alpha^\dagger E_\beta \underbrace{S | \hat{j} \rangle}_{S|\hat{j}\rangle = |\hat{j}\rangle}$$

$$= -\langle \hat{i} | S E_\alpha^+ E_\beta | \hat{j} \rangle = -\langle \hat{i} | E_\alpha^+ E_\beta | \hat{j} \rangle$$

$$\Rightarrow \langle \hat{i} | E_\alpha^+ E_\beta | \hat{j} \rangle = 0$$

$\Rightarrow$ QECC satisfied $\Rightarrow$ error correctable!

ii) $E_\alpha^+ E_\beta \in \mathcal{S}$:

$$\langle \hat{i} | \underbrace{E_\alpha^+ E_\beta}_{\in \mathcal{S}} | \hat{j} \rangle = \langle \hat{i} | \hat{j} \rangle = \delta_{ij}$$

$\Rightarrow$ QECC satisfied $\Rightarrow$ error correctable!

iii) $E_\alpha^+ E_\beta$ comm. with all $S \in \mathcal{S}$,

but $E_\alpha^+ E_\beta \notin \mathcal{S}$:

$\Rightarrow$ $E_\alpha^+ E_\beta$ acts non-trivially on code space:

it is a logical operator

In particular: $E_\alpha^+ E_\beta \, \mathcal{C} \subset \mathcal{C}$, but

$\exists |\hat{j}\rangle$ s.th. $E_\alpha^+ E_\beta |\hat{j}\rangle \neq c \cdot |\hat{j}\rangle$

(else $E_\alpha^+ E_\beta \in \mathcal{S}$)

$\Rightarrow \langle \hat{i} | E_\alpha^\dagger E_\beta | \hat{j} \rangle \neq 0$ for some $i \neq j$

$\Rightarrow$ <u>not correctable</u>! ⚡ (as QEC cond. violated)

(<u>Diff. intuition</u>: Cannot tell w/ certainty if after error state is $E_\alpha |\hat{i}\rangle$ or $E_\beta |\hat{j}\rangle$, and – unlike (ii) – it does matter which of them occurred $\Rightarrow$ not correctable!)

How does the error correction work?

Correctable error model w/ errors $\{E_\alpha\}$,

E_α = product of Paulis.

Assume some error E_β (unknown!) occurred.

$$|\hat{\psi}\rangle \xmapsto{\text{error}} E_\beta |\hat{\psi}\rangle$$

Let $\sigma_i = \pm 1$ denote the commutator of S_i and E_β,

$$S_i E_\beta = E_\beta S_i \sigma_i \qquad (\text{as } S_i |\hat{\psi}\rangle = |\hat{\psi}\rangle).$$

<u>Step 1</u>: Measure all S_i, $i = 1, \dots, r$. Using the (anti)commutation, we find that the result is deterministically σ_i: $S_i E_\beta |\hat{\psi}\rangle = \sigma_i E_\beta S_i |\hat{\psi}\rangle = \sigma_i E_\beta |\hat{\psi}\rangle$

(measurement can be done using CNOTs & single-qubit rotations.)

__Step 2:__ Pick some E_γ from $\{E_\alpha\}$ with ~~same~~ commutation properties, $S_i E_\gamma = \sigma_i E_\gamma S_i$.

__Step 3:__ Apply $E_\gamma^\dagger$ as a correction:

$$E_\beta|\hat{\psi}\rangle \xmapsto{\text{corr.}} E_\gamma^\dagger E_\beta |\hat{\psi}\rangle.$$

Since $S_i E_\gamma^\dagger E_\beta = E_\gamma^\dagger E_\beta S_i$, we have (from (ii)) that

$E_\gamma^\dagger E_\beta |\hat{\psi}\rangle = |\hat{\psi}\rangle \Longrightarrow$ error corrected.

__Note:__ If case (iii) exists, the correction could induce a logical error!

__Key question:__ Given a stabilizer code, what is the shortest $E_\alpha^\dagger E_\beta$ (= Pauli product) of that type (here, "short" refers to # of non-trivial Paulis) ($\rightarrow$ distance of code!)

c) Example: 3-qubit code

$$\mathcal{C} = \text{span}\{|000\rangle, |111\rangle\}$$

$$\left.\begin{array}{l} S_1 = ZZI \\ S_2 = ZIZ \end{array}\right\} \Longrightarrow \mathcal{S} = \{III, ZZI, ZIZ, \underset{\overset{\shortparallel}{S_1 S_2}}{IZZ}\}$$

$$k = \underset{n}{\underset{\shortparallel}{3}} - \underset{r}{\underset{\shortparallel}{2}} = 1 \Rightarrow 1 \text{ encoded qubit}$$

Single-qubit X errors:

$E_\alpha = III, IIX, IXI, XII$ (up to prefactor $\sqrt{p_\alpha}$)

$E_\alpha^\dagger E_\beta = III, IIX, IXI, XII,$
XXI, XIX, IXX

$\Rightarrow$ anti-commu. w/ S_1, S_2, both S_1 & S_2,

or an element of S (for III).

$\Rightarrow$ correctable!

Single-qubit Z errors:

$E_\alpha = III, IIZ, IZI, ZII$

$E_\alpha^\dagger E_\beta = ZII$ is one possibility

But: ZII commu. w/ S_1, S_2, but $\underline{ZII \notin S}$!

$\Rightarrow$ Z errors not correctable!

Logical operators:

(at the same time: uncorrectable $E_\alpha^\dagger E_\beta$!)

$\hat{\cdot}$ ≡ logical Z operator

- $\hat{Z} = \underbrace{ZII}_{\text{distance 1 } \lightning}$

  – or any $\hat{Z}' = \hat{Z} \cdot S$, $S \in \mathcal{S}$, e.g. IZI, ZZZ, ...

- $\hat{X} = XXX$

  – or e.g. $\hat{X}' = XXX \cdot ZZI = -YYX$, etc ...

Note: $\hat{X}\hat{Z} = -\hat{Z}\hat{X}$ — and this is all we have to require from the logical Pauli operators!

Error detection and correction:

X error E_α can be detected by anti-commut. pattern.

e.g.: • XII anti-comm. w/ ZIZ, $ZZI \in \mathcal{S}$.

• can be measured: $ZZI|\psi\rangle \overset{?}{=} \pm|\psi\rangle$ etc.

$\Rightarrow$ allows to detect error (up to a T s.th. $TS = ST$ $\forall S \in \mathcal{S}$, and thus $T \in \mathcal{S}$ for correctable errors).

d) More examples:

3-qubit phase flip code:

$$S_1 = XXI$$
$$S_2 = IXX$$
$$\hat{X} = XII$$
$$\hat{Z} = ZZZ$$

9-qubit Shor code:

$$\left.\begin{aligned}
S_1 &= ZZI\ III\ III \\
S_2 &= IZZ\ III\ III \\
S_3 &= III\ ZZI\ III \\
S_4 &= III\ IZZ\ III \\
S_5 &= III\ III\ ZZI \\
S_6 &= III\ III\ IZZ \\
S_7 &= XXX\ XXX\ III \\
S_8 &= III\ \underline{XXX}\ \underline{XXX}
\end{aligned}\right\}$$

8 indep. stabilizers
||
1 encoded qubit

logical X of 3-qubit code!

Logical operators:

e.g.:

$\hat{Z} = ZZZ\,ZZZ\,ZZZ$

$\hat{X} = XXX\,XXX\,XXX$

— these commu. w/ S_i, as those have even # of X/Z,

but are $\notin S$, since they have odd # of X/Z.

simpler ("shorter") logical ops:

e.g. $\hat{Z} = ZII\,ZII\,ZII$

$\hat{X} = XXX\,III\,III$

($\Rightarrow$ distance 3!)

Also means that $\hat{X}$ and $\hat{Z}$ can be measured by measuring only 3 qubits!
(But: meas. a general function of $\hat{X}$ & $\hat{Z}$ requires at least 5 qubits because of no-cloning argument!)

Note: 9-qubit code is degenerate:

$E_1 = Z\,I\,I\,I\,I\,I\,I\,I\,I$ and

$E_2 = I\,Z\,I\,I\,I\,I\,I\,I\,I$

have same syndrome, since

$E_1 E_2 = Z\,Z\,I\,I\,I\,I\,I\,I\,I \in \mathcal{S}$.

e) The 5-qubit code

Consider the stabilizer code on 5 qubits w/ generators

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

encodes $5-4 = 1$ qubit

cyclic code: $S_1, \dots, S_5$ are cyclic permutations.

$\Rightarrow$ cyclic codewords!

$(S_5 = Z\,Z\,X\,I\,X = S_1 S_2 S_3 S_4)$

Corrects any 1-qubit error:

$E_\alpha^\dagger E_\beta$ = product of ≤ 2 Paulis

$\Rightarrow$ anti-comm. w/ <u>at least</u> one S_i, $i=1,\dots,5$

(Why? Fix pos. of 1st Pauli, pick S_k which has I there. Then, 2nd Pauli must agree with that on S_k; and conversely. But: can check that those choices won't commute w/ some other S_i.)

$\Rightarrow$ correctable $\Rightarrow$ $d \geq 3$.

(And $d \leq 3$ from no-cloning: $[[5,1,3]]$-QECC!)

<u>Error syndromes</u> ($1 \equiv$ anti-comm. = eigenval. -1)

	X error on qubit					Z error on					Y error on				
	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
S_1	0	1	1	0	0	1	0	0	1	0	1	1	1	1	0
S_2	0	0	1	1	0	0	1	0	0	1	0	1	1	1	1
S_3	0	0	0	1	1	1	0	1	0	0	1	0	1	1	1
S_4	1	0	0	0	1	0	1	0	1	0	1	1	0	1	1
S_5	1	1	0	0	0	0	0	1	0	1	1	1	1	0	1

15 errors, 15 syndromes $\Rightarrow$ non-degenerate.

All possible $2^4 - 1 = 15$ syndromes appear.

Logical operators:

$$\left.\begin{aligned}\hat{Z} &= ZZZZZ \\ \hat{X} &= XXXXX\end{aligned}\right\}$$ comm. w/ all S_i (even # of X & Z in S_i), but for same reason $\notin \mathcal{S}$!

simpler choices:

e.g. $\hat{Z}' = \hat{Z} \cdot S_3 = -YZYII$

$\hat{X}' = \hat{X} \cdot S_2 = -XIYYI$

$\Rightarrow$ distance $d = 3$

& logical info in $\hat{Z}$ or $\hat{X}$ basis can be obtained by meas. only 3 qubits!

(Note: General feature of distance-d code!)

Syndrome meas. + correction can be done using only CNOT, H, X (for corr.), and ancillas.

(Again: gen. feature of stabilizer code: need to compute parity of X & Z eigenvalues.)