V.4 Stabilizer codes

Consider the Pauli group on n qubits

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

Two elements $S_1, S_2 \in \mathcal{G}$ either <u>commute</u> or <u>anticommute</u>.

Let $S_1, \ldots, S_r \in \mathcal{G}$ be a lin. indep. set of <u>commuting S_i</u> (i.e., no S_i is a product of others).

Then, $S_1, \ldots, S_r$ generate a subgroup

$\mathcal{S} := \langle S_1, \ldots, S_r \rangle$, the <u>stabilizer group $\mathcal{S}$</u>.

<u>$\mathcal{S}$ defines subspace C</u>:

$$\boxed{\begin{array}{l} |\psi\rangle \in C :\Leftrightarrow |\psi\rangle = S|\psi\rangle \quad \forall S \in \mathcal{S}. \\ \\ C \text{ forms the } \underline{\text{code space}} \text{ of a } \underline{\text{stabilizer code}}. \\ S \in \mathcal{S} \text{ are called } \underline{\text{stabilizers}}. \end{array}}$$

(Techn. pt: This req. $-I \notin \mathcal{S}$, or $S_i = \pm \otimes P_i$).

We have $\dim C = 2^{n-r}$ – each lin. indep. stabilizer removes half the space!

What about err. corr. conditions?

Pauli errors $\Rightarrow$ $E_\alpha^\dagger E_\beta$ Pauli product.

3 possibilities:

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

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

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

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

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

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

Cases (i) & (ii): error correctable!

(iii) $E_\alpha^\dagger E_\beta$ comm. w/ all $S \in \mathcal{S}$, but $E_\alpha^\dagger E_\beta \notin \mathcal{S}$:

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

it is a logical operator.

$\Rightarrow$ not correctable.

Q: What is shortest $E_\alpha^\dagger E_\beta$ of that type?

Example: 3-qubit code.

$C = \mathrm{span}\{|000\rangle, |111\rangle\}$.

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

qubits must be pairwise equal $\rightarrow \alpha|000\rangle + \beta|111\rangle$

$k = 3 - 2 = 1$

$\Rightarrow$ 1 encoded qubit

Single-qubit X errors:

$E_\alpha = III, IIX, IXI, XII$

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

$\Rightarrow$ anti-comm. w/ S_1, S_2, $S_1 \& S_2$, or $\in \mathcal{S}$.

$\Rightarrow$ correctable!

Single-qubit Z errors:

$E_\alpha^\dagger E_\beta = ZII$ possible.

ZII comm. w/ S_1, S_2, but $ZII \notin \mathcal{S}$!

$\Rightarrow$ Z errors not correctable!

Logical operators (or uncorrectable errors...)

- $\hat{Z} = \underbrace{ZII}_{\text{distance } 1}$ (or any $\hat{Z}' = \hat{Z} \cdot S$, $S \in \mathcal{S}$, e.g. $\hat{Z}' = IZI, ZZZ, \ldots$)

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

Error detection / correction:

X error E_α can be identified by anti-com. pattern:

e.g.: XII anticom. w/ $ZZI, ZIZ \in \mathcal{S}$.

$\Rightarrow$ allows to (i) correct error

(ii) even: uniquely identify error ("non-degenerate" code).

More examples:

3-qubit phase flip code:

$S_1 = XXI$

$S_2 = IXX$

$\hat{X} = XII$

$\hat{Z} = ZZZ$

9-qubit Shor code

$$\left.\begin{array}{l l}
\text{3-qubit 1} \left\{ \begin{array}{l} S_1 = ZZI\ III\ III \\ S_2 = IZZ\ III\ III \end{array}\right. \\
\text{3-qubit 2} \left\{ \begin{array}{l} S_3 = III\ ZZI\ III \\ S_4 = III\ IZZ\ III \end{array}\right. \\
\text{3-qubit 3} \left\{ \begin{array}{l} S_5 = III\ III\ ZZI \\ S_6 = III\ III\ IZZ \end{array}\right. \\
\hline
\qquad\quad S_7 = XXX\ XXX\ III \\
\qquad\quad S_8 = III\ \underbrace{XXX}\ \underbrace{XXX}
\end{array}\right\}$$

8 stabilizers = 1 encoded qubit!

Logical X on 3-qubit code.

Logical operators: e.g.

$$\left.\begin{array}{l} \hat{Z} = ZZZ\ ZZZ\ ZZZ \\ \hat{X} = XXX\ XXX\ XXX \end{array}\right\}$$

odd # of Z/X: cannot be in S!

Shorter: e.g. $\hat{Z} = ZII\ ZII\ ZII$

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

$\hat{X}$ and $\hat{Z}$ can be measured by meas. only 3 qubits.

(Note: meas. a general function of $\hat{X}$ & $\hat{Y}$ must require at least 5 qubits: no cloning argument!)

$\Rightarrow \hat{X}, \hat{Z}$ shortest possible $\Rightarrow d = 3$ code!

(Note: Degenerate code: $\overbrace{ZII\ III\ III}^{=:S_1}$ and $\overbrace{IZI\ III\ III}^{=:S_2}$

have same syndrome, since $S_1 S_2 = ZZI\ III\ III \in \mathcal{S}$.)

The 5-qubit-code:

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

Encodes $5-4=1$ qubit

Cyclic code: $S_1, \dots, S_5$ are cyclic permutation: cyclic codewords!

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

Corrects any 1-qubit error:

$E_\alpha^\dagger E_\beta$ = prod. of 2 Pauli's:

$\Rightarrow$ anti-commun. w/ at least one S_i!

(E.g.: each col. has one $I \Rightarrow$ that S_i fixed other Pauli error $\Rightarrow$ both Pauli's fixed by 2 $S_i \Rightarrow$ ↯)

$\Rightarrow$ Distance $d \geq 3$ (and $d \leq 3$ from no-cloning)

$\Rightarrow$ $[\![5,1,3]\!]$ QECC!

Syndromes: ($1 \equiv$ anti-com.)

	X error on					Y error on					Z 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	1	1	1	0	1	0	0	1	0
S_2	0	0	1	1	0	0	1	1	1	1	0	1	0	0	1
S_3	0	0	0	1	1	1	0	1	1	1	1	0	1	0	0
S_4	1	0	0	0	1	1	1	0	1	1	0	1	0	1	0
(S_5)	1	1	0	0	0	1	1	1	0	1	0	0	1	0	1

$\Rightarrow$ each error has different syndrome $\Rightarrow$ non-degen.

and all 2^4-1 syndromes appear!

Logical operators:

$$\left.\begin{aligned} \hat{Z} &= ZZZZZ \\ \hat{X} &= XXXXX \end{aligned}\right\} \in \mathcal{N}, \text{ and } \notin \mathcal{S}, \text{ since all } S_i \text{ have even \# of } X \,\&\, Z.$$

or, simpler:
$$\hat{Z}' = \hat{Z} \cdot S_3 = -YZYII$$
$$\hat{X}' = \hat{X} \cdot S_2 = -XIYYI$$

$\Rightarrow$ distance $d=3$.

and: we can read out logical info in $\hat{Z}/\hat{X}$ basis by meas. 3 qubits only.

Syndrome measurement + correction can be done only w/ (Controlled-NOT, H, and ancillas

Clifford gates:

The Clifford group $\mathcal{C}$ consists of all gates which map Paulis to Paulis:

$$\mathcal{C} = \{ C \mid C(P_1 \otimes \ldots \otimes P_n)C^\dagger = P_1' \otimes \ldots \otimes P_n' \}$$

Theorem:

$$\mathcal{C} \equiv \{\text{all circuits built from CNOT, } S = \begin{pmatrix} 1 & \\ & i \end{pmatrix}, \text{ and } H. \}$$

(In part.: Any C which maps Paulis to Paulis is of this form!)

Note: Only $T = \begin{pmatrix} 1 & \\ & e^{i\pi/4} \end{pmatrix}$ missing for a universal gate set!

How to apply gates on encoded qubits?

→ Decode / Apply / Encode: Bad idea – info not protected!

→ Try to apply gates to encoded qubits!

<u>Stabilizer codes</u>: Clifford gates can be applied to encoded qubits:

Clifford gates on logical qubits

$\Downarrow$

maps Paulis to Paulis (logical)

$\Downarrow$ logical Paulis are prods. of Physical Paulis!

maps Paulis to Paulis (physical)

$\Downarrow$

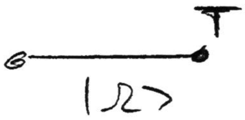
Clifford gates on <u>physical qubits</u>.

<u>E.g.</u>: 5-qubit code $\hat{H}$ gate:

$$\left.\begin{aligned} \hat{X} &= XXXXX \\ \hat{Z} &= ZZZZZ \\ \hat{H}\hat{X}\hat{H} &= \hat{Z} \end{aligned}\right\}$$ find Clifford s.th. $XXXXX \leftrightarrow ZZZZZ$ & stabilizers are preserved!

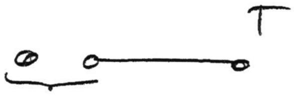
Can we also realize non-Clifford gates (e.g. $T = \begin{pmatrix} 1 & \\ & e^{i\pi/4} \end{pmatrix}$) in a robust way?

One idea: Gate teleportation:

Prepare $|\chi\rangle =$ 

↑ ME state $|\Omega\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

+ "teleport" through $|\chi\rangle$



Bell meas.

→ Outcome $|\Omega\rangle$: result is $T|\chi\rangle$

→ otherwise: different outcome, but can be transformed to T w/ Clifford gates (→ HW!)

& $|\chi\rangle$ can be prepared (+ tested) beforehand in an encoded state

& telep. circuit consists of Cliffords + meas. in 2 bases.