Lecture 7: Stabilizer Formalism - 2

• Recap of Stabilizer formalism - 1 from Lecture 6. [Ref. Gottesman's PhD thesis, 1998]

Defn: A $[n, k, d]$ stabilizer code is defined as the common eigenspace of a commuting set of Pauli operators: $g_1, g_2, g_3, \ldots, g_{n-k}$ with eigenvalue $+1$:

$$\mathcal{C} = \left\{ |\psi\rangle \in \mathbb{C}_2^n : g_i |\psi\rangle = |\psi\rangle \ \forall \ 1 \leq i \leq n-k \right\}$$

Remarks:

(a) $g_1, \ldots, g_{n-k}$: independent Pauli operators that generate a group:

$\mathcal{S} = \langle g_1, \ldots, g_{n-k} \rangle :=$ Stabilizer group (subgroup of $\mathcal{P}_n$). g_i : stabilizer generators.

(b) Projector on to the code space: $\Pi_0 = \dfrac{1}{2^{n-k}} \prod_{j=1}^{n-k} \dfrac{(\mathbb{1} + g_j)}{2} = \dfrac{1}{|\mathcal{S}|} \sum_{s \in \mathcal{S}} s$

② Quantum Error Correction: Assuming noise is $\mathcal{E}(\rho) = p_I \rho + p_X X\rho X + p_Y Y\rho Y + p_Z Z\rho Z$, and i.i.d.

$$|\bar{\psi}\rangle \rightsquigarrow E|\bar{\psi}\rangle \left\{ \begin{array}{lll} m_1 = \text{eigenvalue of } g_1 & \longmapsto & s_1 : (-1)^{s_1} = m_1 \\ m_2 = \text{eigenvalue of } g_2 & \longmapsto & s_2 : (-1)^{s_2} = m_2 \\ & \vdots & \\ m_{n-k} = \text{eigenvalue of } g_{n-k} & \longmapsto & s_{n-k} : (-1)^{s_{n-k}} = m_{n-k} \end{array} \right\}$$

Decoding

Best guess for an error that occurred conditioned on $\vec{s}$.

$\vec{s}$: Error syndrome

Error syndrome for a Stabilizer code:

Note: $g_i |\bar{\psi}\rangle = |\bar{\psi}\rangle$ for $|\bar{\psi}\rangle \in \mathcal{C}$, g_i: stabilizer generators.

• Let us say that measuring $|\bar{\psi}\rangle \longmapsto E|\bar{\psi}\rangle$ under some error.

• measuring g_i on $E|\bar{\psi}\rangle$ gives m_i :

$$g_i (E|\bar{\psi}\rangle) = m_i (E|\bar{\psi}\rangle)$$

In other words:

$$g_i E|\bar{\psi}\rangle = m_i E (g_i|\bar{\psi}\rangle) \quad \text{since } g_i|\bar{\psi}\rangle = |\bar{\psi}\rangle \text{ by definition.}$$

So:

$$g_i E = m_i E g_i$$

$$g_i E = (-1)^{s_i} E g_i$$

which implies that $s_i = \begin{cases} 0 & \text{if } [g_i, E] = 0 \\ 1 & \text{if } \{g_i, E\} = 0 \end{cases}$ Convenient definition of the error syndrome.

• The syndrome $s \equiv s(E)$ completely specifies the commutation relations between the (unknown) Error and the stabilizer generators of the code.

Eg. Shor code: $|\bar{0}\rangle = \frac{(|000\rangle + |111\rangle)^{\otimes 3}}{\sqrt{2}}$, $|\bar{1}\rangle = \left(\frac{|000\rangle - |111\rangle}{\sqrt{2}}\right)^{\otimes 3}$

Henceforth, we will never provide the encoded states. Only stabilizer-gens:

$$S = \langle Z_1Z_2,\ Z_2Z_3,\ Z_4Z_5,\ Z_5Z_6,\ Z_7Z_8,\ Z_8Z_9,\ X_1X_2X_3X_4X_5X_6,\ X_4X_5X_6X_7X_8X_9 \rangle$$

Say an error Y_4 occurs, then we had computed the syndrome by looking $Y_4|\bar{0}\rangle$ $(|\bar{1}\rangle)$. We can instead read off $s = (s_1, s_2, \dots, s_8)$ by observing commutation of X_1 with g_i.

$$s(Y_2) = (1\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 1)$$

Correspondance between Stabilizer Codes and Binary Linear Codes (Lecture 5):

Consider a matrix: $M_G = \begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_{n-k} \end{bmatrix}$

Recall the error syndrome: $s = H\vec{e}$ ← (error vector); H: parity check matrix

In this case, the error syndrome is:

$$s_i(E) = \begin{cases} 0 & \text{if } [\underbrace{(M_G)_i}_{i^{th} \text{ row of } M_G}, E] = 0 \\ 1 & \text{if } \{\underbrace{(M_G)_i}_{i^{th} \text{ row of } M_G}, E\} = 0 \end{cases}$$

defn: Symplectic representation of an n-qubit Pauli operator

$$P = c \prod_{i=1}^{n} X_i^{a_i} \prod_{i=1}^{n} Z_i^{b_i}$$

(Note: $Z^0 = X^0 = \mathbb{1}$)

is given by $\lambda(P) = (a|b)$.

Eg. $P = i\, X\, \mathbb{1}\, \mathbb{1}\, Y\, Z$, $\lambda(P) = (\underset{X}{1}\, 0\, 0\, \overset{Y}{1}\, 0 | 0\, 0\, 0\, \overset{Y}{1}\, \underset{Z}{1})$

defn: Symplectic dot product between two symplectic vectors $\lambda_1(P_1) = (a_1|b_1)$ and $\lambda_2(P_2) = (a_2|b_2)$ is given by:

$$\lambda(P_1) \odot \lambda(P_2) = (a_1 \cdot b_1 + a_2 \cdot b_1) \bmod 2$$

Note:

$$\lambda(P_1) \odot \lambda(P_2) = \begin{cases} 0 & \text{if } [P_1, P_2] = 0 \\ 1 & \text{if } \{P_1, P_2\} = 0 \end{cases}$$

Suppose: $P_1 = c_1 X^{a_1} Z^{b_1}$ and $P_2 = c_2 X^{a_2} Z^{b_2}$, then

$[P_1, P_2] = 0$ implies that $[X^{a_1}, Z^{b_2}] = 0$ and $[Z^{b_1}, X^{a_2}] = 0$

OR $\underbrace{\{X^{a_1}, Z^{b_2}\} = 0 \text{ and } \{Z^{b_1}, X^{a_2}\} = 0}$

$a_1 b_2 = b_1 a_2$

$a_1 b_2 + b_1 a_2 = 0 \mod 2$

$\{P_1, P_2\} = 0$ implies that $a_1 b_2 + a_2 b_1 = 1 \pmod 2$.

We can now write the matrix of Stabilizer generators as:

$$M = \begin{bmatrix} \lambda(g_1) \\ \lambda(g_2) \\ \vdots \\ \lambda(g_{n-k}) \end{bmatrix}$$

The error syndrome of E can now be described as how we wanted:

$$M \odot \lambda(E) = s$$

Note how this resembles $H \cdot e = s$ for Classical Binary linear codes.

Tutorial: What is the M matrix for the Shor's code?

$$\begin{array}{ll} \lambda(Z_1 Z_2) \longmapsto & 0\,0\,0\,0\,0\,0\,0\,0\,0 \mid 1\,1\,0\,0\,0\,0\,0\,0\,0 \\ \lambda(Z_2 Z_3) \longmapsto & 0 \cdots\cdots 0 \mid 0\,1\,1\,0 \cdots\cdots 0 \\ \vdots & \vdots \\ \lambda(Z_8 Z_9) \longmapsto & 0 \cdots\cdots 0 \mid 0 \cdots\cdots 1\,1 \\ \lambda(X_1 \dots X_6) \longmapsto & 1\,1\,1\,1\,1\,1\,0\,0\,0 \mid 0 \cdots\cdots 0 \\ \lambda(X_4 \dots X_9) \longmapsto & 0\,0\,0\,1\,1\,1\,1\,1\,1 \mid 0 \cdots\cdots 0 \end{array}$$

$\lambda(M_Z) := H_Z$

$\lambda(M_X) := H_X$

$$= \begin{pmatrix} H_X & 0 \\ 0 & H_Z \end{pmatrix}$$

Bits specifying commutation with Z-gens.

Note: The syndrome for any Error $E = s(E) = (s_Z(E) \; s_X(E))$, we have:

$\lambda(E) = (a|b)$

Bits specifying commutation with X-gens.

$s_Z(E) = H_X \cdot b$ and $s_Z(E) = H_Z \cdot a$. This looks like two Classical Error Correction codes.

Structure of the Pauli Group induced by the Stabilizer group:

- Pauli group $\mathcal{P}_n$: set of all n-qubit Pauli Errors.

  Basis for $\mathcal{P}_n$: attributing the elements to specific action on the encoded states of $\mathcal{C}$.

(a) Of these are errors which leave $\mathcal{C}$ invariant.

$$E|\bar{\varphi}\rangle = |\bar{\phi}\rangle \quad \text{So:} \quad E\, g_i |\bar{\varphi}\rangle = g_j |\bar{\phi}\rangle$$

$$E\, g_i E^{+} \underbrace{E|\bar{\varphi}\rangle}= g_j|\bar{\phi}\rangle$$

$$E\, g_i E^{+}\, |\bar{\phi}\rangle = g_j |\bar{\phi}\rangle$$

$\Rightarrow E \in \mathcal{N}(\mathcal{S})$: Normalizer of the Stabilizer subgroup

- Note that $s(N) = 0$ for all $N \in \mathcal{N}(\mathcal{S})$.
- Note that $s(E) = s(E\cdot N)$ for all $N \in \mathcal{N}(\mathcal{S})$ and $E \in \mathcal{P}_n$.

(b) Consider $\underbrace{\mathcal{N}(\mathcal{S})}_{\text{normalizer}}$ and $\mathcal{P}_n / \mathcal{N}(\mathcal{S})$.

$$\mathcal{P}_n / \mathcal{N}(\mathcal{S}) = \mathcal{T}$$

$$\mathcal{P}_n = \bigcup_{T \in \mathcal{T}} \text{cosets of } \mathcal{N}(\mathcal{S}), \text{ each identified by } T \equiv \text{error syndrome.}$$

- elements in the same coset have the same error syndrome.
- elements in different cosets have distinct syndromes.

Hence, any Pauli Error $E = N \cdot T$ where T is completely specified by the error syndrome $s(E)$.

Note: $|\mathcal{T}| = \#$ error syndromes $= 2^{n-k}$.

Since $|\mathcal{P}_n| = 4^n$, we must have $|\mathcal{N}(\mathcal{S})| = 2^{n+k}$

(b) We can further partition $\mathcal{N}(\mathcal{S})$ into cosets of $\mathcal{S}$:

$$\mathcal{N}(\mathcal{S}) / \mathcal{S} := \mathcal{L}$$

- Note:
  - elements of $\mathcal{N}(\mathcal{S})$ leave $\mathcal{C}$ invariant, so for any $N \in \mathcal{N}(\mathcal{S})$, $N|\bar{\varphi}\rangle = |\bar{\phi}\rangle$ for $|\bar{\varphi}\rangle, |\bar{\phi}\rangle \in \mathcal{C}$.
  - elements of $\mathcal{S}$ act as identity on every encoded state: $S|\bar{\varphi}\rangle = |\bar{\varphi}\rangle \ \forall\, S \in \mathcal{S}$, $|\bar{\varphi}\rangle \in \mathcal{C}$.
  - Hence elements of $\mathcal{L}$ should map $|\bar{\varphi}\rangle \mapsto |\bar{\phi}\rangle$ where $|\bar{\varphi}\rangle, |\bar{\phi}\rangle \in \mathcal{C}$ but $|\bar{\varphi}\rangle \neq |\bar{\phi}\rangle$.

• In other words $\mathcal{L}$ has elements that commute with $\mathcal{S}$ but are not in $\mathcal{S}$.

Recall: Errors in $\mathcal{N}(\mathcal{S})$ cannot be detected and those within $\mathcal{N}(\mathcal{S})$ but not in $\mathcal{S}$ also act non-trivially on the encoded states. These are logical errors.

defn: The distance of a stabilizer code $\mathcal{C}$ is the smallest weight of an element in $\mathcal{N}(\mathcal{S}) \setminus \mathcal{S}$.

Hence $\mathcal{N}(\mathcal{S}) / \mathcal{S} = \bigcup$ cosets of $\mathcal{S}$, indexed by $L \in \mathcal{L}$.

Since $|\mathcal{N}(\mathcal{S})| = 2^{n+k}$, $|\mathcal{S}| = 2^{n-k}$, we find $|\mathcal{L}| = 2^{2k}$.

Any element of the normalizer: $N = L \cdot S$ where $L \in \mathcal{L}$ and $S \in \mathcal{S}$.

Hence, in summary, we can write any Pauli Error E in the form:

$$E = c\, T \cdot L \cdot S$$

where

$T \in \mathcal{T}$: • takes an encoded state to a state outside the codespace : $s \neq 0$
• T anticommutes with stabilizer generators and determines the syndrome : $s(E) = s(T)$.

$L \in \mathcal{L}$: • maps encoded states to distinct encoded states (non-trivial transformation)
• logical operations on the encoded states.

$S \in \mathcal{S}$ • identity on every encoded state.

Tutorial topic : discuss how to compute T, L and S for any Error : using a Canonical generating set for $\mathcal{P}_n$.

Provide an example : The 5-qubit code. [Ref: Laflamme et. al. PRL 77 (198), 1996]

A $[[5,1,3]]$ code whose stabilizer generators are:

$$\mathcal{S}\begin{cases} g_1 = Z\,X\,I\,X\,Z \\ g_2 = Z\,Z\,X\,I\,X \\ g_3 = X\,Z\,Z\,X\,I \\ g_4 = I\,X\,Z\,Z\,X \end{cases}$$

$$\mathcal{L}\begin{cases} \bar{X} = X\,X\,X\,X\,X \\ \bar{Z} = Z\,Z\,Z\,Z\,Z \end{cases}$$

$$T_1 = X\,I\,I\,I\,I$$

Interesting facts

① Encoded states are complicated
$|\bar{0}\rangle, |\bar{1}\rangle \mapsto$ 8 basis vectors combined

② Invented before stabilizer formalism

③ Can correct only one error. Every syndrome $\xrightarrow{\text{unique}}$ single qubit error

④ Choice of Basis is not unique. Hence there is a different canonical choice of a basis.

$$\mathcal{T}\begin{cases} T_2 = \mathbb{1}\ X\ \mathbb{1}\ \mathbb{1}\ \mathbb{1} \\ T_3 = \mathbb{1}\ \mathbb{1}\ X\ \mathbb{1}\ \mathbb{1} \\ T_4 = \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ X\ \mathbb{1} \end{cases}$$

Decoding a Stabilizer Code

$$|\bar\Psi\rangle \xrightarrow[\text{(unknown Pauli)}]{E} E|\bar\Psi\rangle = c\,T \cdot L \cdot S\,|\bar\Psi\rangle \rightsquigarrow$$

- measure syndrome : $s(E) \equiv s(T)$
- Compute the most likely Error E?

- Let us assume $\mathcal{E}(P) = (1-p)P + \frac{p}{3} XPX + \frac{p}{3} YPY + \frac{p}{3} ZPZ$ and i.i.d version.
- Note that the probability of an error E: $\mathbb{P}(E)$ is:

$$\mathbb{P}(E) = \left(\frac{p}{3}\right)^{wt(E)} (1-p)^{n-wt(E)}.$$

(Most likely $\equiv$ least weight)

Goal: Given the error syndrome $\vec{s}$ for $E \in \mathcal{P}_n$, compute the most likely Error E.

Note:
- If some error E_1 has $s(E_1) = \vec{s}$, then all errors in the coset $E_1 \cdot N(\mathcal{S})$ have the syndrome $\vec{s}$.
- All errors in $E_1 \cdot N(\mathcal{S})$ are of the form: $c\,T_s \cdot L \cdot S$ where T_s is fixed by $\vec{s}$.
- Search for the most probable Element (least weight) in this coset.
- Each element of the coset $T_s . N(\mathcal{S})$ is of the form: $T_s \cdot L \cdot S$ for $L \in \mathcal{L}, S \in \mathcal{S}$.
- Once we find an element $N^* = L^* S^*$, we invert the error by applying $T_s \cdot L^* S^*$ on the noisy state $E|\bar\Psi\rangle = c\,T_s \cdot L \cdot S$:

$$E|\bar\Psi\rangle \xrightarrow{\text{Recovery}} c\,(T_s \cdot L^* \cdot S^*)(T_s \cdot L \cdot S)|\bar\Psi\rangle$$
$$= c\,(L^* \cdot L)(S^* \cdot S)|\bar\Psi\rangle$$

- If L^* and S^* are chosen to maximize $\mathbb{P}(T_s . L^* S^*)$, then $L^* S^* = LS$ for the most likely errors with syndrome $\vec{s}$.
- What if we find the wrong $S' \neq S^*$. Makes No Diff: $S' S^* |\bar\Psi\rangle = |\bar\Psi\rangle \ \forall\, |\bar\Psi\rangle \in \mathcal{C}$.

Decoding problem: Given an error syndrome $\vec{s}$, compute $L^* \in \mathcal{L}$ where

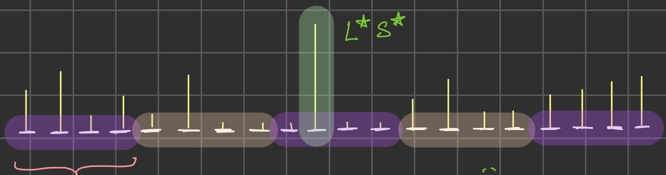
$$L^*_s = \underset{L \in \mathcal{L},\, S \in \mathcal{S}}{\operatorname{argmax}}\ \mathbb{P}(T_s \cdot L \cdot S)$$

Provide a graphical representation:

- Different cosets each corresponding to $L \in \mathcal{L}$. Each coset contains errors that have the same action on every $|\bar{\psi}\rangle \in \mathcal{C}$. But different cosets contain errors that have different logical effects on $|\bar{\psi}\rangle$.

- Hence we should choose the right coset: but need not care to choose the right error.

A subtle issue exclusive to the quantum case:



Errors in this set: $T_s \cdot L_1 \cdot S_1 \; |\bar{\psi}\rangle = |\bar{\varphi}\rangle$

$T_s \cdot L_1 \cdot S_2 \; |\bar{\psi}\rangle = |\bar{\varphi}\rangle$

$T_s \cdot L_1 \cdot S_3 \; |\bar{\psi}\rangle = |\bar{\varphi}\rangle$

$\vdots$

$T_s \cdot L_1 \cdot S_{2^{n-k}} \; |\bar{\psi}\rangle = |\bar{\varphi}\rangle$

All of these states are indistinguishable. $= |\phi(s)\rangle$

Hence $$\mathbb{P}(|\bar{\psi}\rangle \mapsto |\phi(s)\rangle) = \underbrace{\mathbb{P}(T_s \cdot L \cdot S_1) + \mathbb{P}(T_s \cdot L \cdot S_2) + \ldots + \mathbb{P}(T_s \cdot L_1 \cdot S_{2^{n-k}})}$$

this degeneracy feature is exclusive to Quantum Codes.

$$= \sum_{E \in L \cdot \mathcal{S}} \mathbb{P}(E \cdot T_s)$$

Definition (Optimal decoding): Given an error syndrome s, compute $L^* \in \mathcal{L}$ such that

$$\mathbb{P}(L^* \mid s) = \sum_{S \in \mathcal{S}} \mathbb{P}(T_s \cdot L^* \cdot S)$$

is the maximum over all $L \in \mathcal{L}$, i.e.,

$$\mathbb{P}(L^* \mid s) = \max_{L \in \mathcal{L}} \mathbb{P}(L \mid s).$$

In other words, $$L^* = \arg\max_{L \in \mathcal{L}} \mathbb{P}(L \mid s) = \sum_{S \in \mathcal{S}} \mathbb{P}(T_s \cdot L \cdot S)$$