Today we're going to see how to describe Pauli stabilizer codes using a linear algebra formalism much like for classical parity-check codes.

Pauli stabilizer codes define codespace

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

$\mathcal{S}$: stabilizer group generated by commuting Paulis.

$\mathcal{S} \leq P_n$; $-I \notin \mathcal{S}$

The key thing for error correction was understanding what (Pauli) error led to what syndrome? i.e. commutation relations....
Amazingly we can simplify P_n and still capture this data:

Def: Consider $\varphi : P_1 \to \mathbb{F}_2^2$ ← two bits

w/ $\varphi(I) = \begin{pmatrix}0\\0\end{pmatrix}$, $\varphi(X) = \begin{pmatrix}1\\0\end{pmatrix}$, $\varphi(Y) = \begin{pmatrix}1\\1\end{pmatrix}$, $\varphi(Z) = \begin{pmatrix}0\\1\end{pmatrix}$ } φ ignores phases

$= \varphi(-I) = \varphi(iI) = \varphi(-iI)$

Generalize φ to $n=2$ qubits: $\varphi(X_1) = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}$, $\varphi(Y_1 Z_2) = \begin{pmatrix}1\\0\\1\\1\end{pmatrix}$ etc.

and can straightforwardly generalize to $n>2$.

Prop: $\varphi(Q_1 Q_2) = \varphi(Q_1) + \varphi(Q_2)$ [φ is group homomorphism, $\mathbb{F}_2$ is a group under addition]

Easy to check cases explicitly so we won't do in class.

Prop: Define $\mathbb{F}_2$-matrix $J = \left(\begin{array}{c|c} 0_{n\times n} & I_{n\times n} \\ \hline I_{n\times n} & 0_{n\times n} \end{array}\right)$

$$[Q_1, Q_2] = 0 \iff \varphi(Q_1)^T J \varphi(Q_2) = 0$$

$$\{Q_1, Q_2\} = 0 \iff \varphi(Q_1)^T J \varphi(Q_2) = 1$$

Proof: If $\varphi(Q_{1,2}) = \begin{pmatrix} q^{(x)}_{1,2} \\ q^{(z)}_{1,2} \end{pmatrix}$, $\varphi(Q_1)^T J \varphi(Q_2) = q_1^{(x)} \cdot q_2^{(z)} + q_1^{(z)} \cdot q_2^{(x)}$

$(X_1 \cdots Z_1 Z_2 \cdots)(X_2 \cdots Z_1 \cdots) \to \pm Q_2 Q_1$?

Q_1 Q_2

So $\varphi(Q_1)^T J \varphi(Q_2)$ counts # of times Paulis would anticommute... if odd # of times, $\{Q_1, Q_2\} = 0$. If even, $[Q_1, Q_2] = 0$.

This vastly simplifies how to talk about Pauli stab. codes:

Def: stabilizer group $\mathcal{S} \Rightarrow$ parity-check matrix H.

$$H = \begin{pmatrix} \varphi(S_1)^T \\ \vdots \\ \varphi(S_m)^T \end{pmatrix}$$

each entry verifies each stabilizer pair commutes

The fact that all stabilizers commute $\Rightarrow$ $H J H^T = 0$

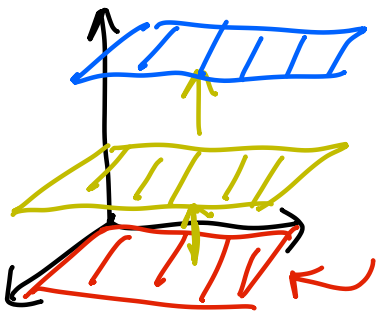
Paulis that commute w/ $\mathcal{S}$:

$$\varphi(N(\mathcal{S})) \to \ker(HJ) = \{ v \in \mathbb{F}_2^{2n} : HJv = 0 \}$$

Logical operators $\in \ker(HJ) \setminus \text{im}(H^T)$

$\{ H^T v \ \forall \ v \in \mathbb{F}_2^m \}$: all combos of stabilizers

Recall that we only care about logical/error up to stab. equiv. This is super natural in the $\mathbb{F}_2$ formalism!



any representative is fine for QEC!

measure syndrome: $\vec{s} = HJ\vec{e}$

$\Rightarrow$ think of error space as $\mathbb{F}_2^{2n} / \text{im}(H^T)$

$\mathbb{F}_2^{2n}$: all possible errors; $\text{im}(H^T)$: up to stabilizer redundancy

Def: reduced error weight: $|\vec{w}|_{red} := \min_{\vec{v} \in \text{im}(H^T)} |\vec{w} + \vec{v}|_H$

where Hamming weight $|\vec{w}|_H = \sum_{j=1}^{n} \begin{cases} 1 & w_j^{(x)} \text{ or } w_j^{(z)} = 1 \\ 0 & \text{else} \end{cases}$

Def: code distance $d = \min_{w \in \ker(H) \setminus \text{im}(H^T)} |w|_{red}$

We'll basically be studying quantum codes of a special form...

Def: CSS code has $H = \left(\begin{array}{c|c} H_X & 0 \\ \hline 0 & H_Z \end{array}\right)$

All stabilizer generators have only Pauli X or Pauli Z.

Example: Shor code: $X_1X_2X_3X_4X_5X_6$ Z_1Z_2

$$H_X = \begin{pmatrix} 1&1&1&1&1&1&0&0&0 \\ 0&0&0&1&1&1&1&1&1 \end{pmatrix} \qquad H_Z = \begin{pmatrix} 1&1&0&0&0&0&0&0&0 \\ 0&1&1&0&0&0&0&0&0 \\ 0&0&0&1&1&0&0&0&0 \\ 0&0&0&0&1&1&0&0&0 \\ 0&0&0&0&0&0&1&1&0 \\ 0&0&0&0&0&0&0&1&1 \end{pmatrix}$$

Prop: If stabilizer code, $H_X H_Z^T = 0$.

Proof:

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

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

$\blacksquare$

Note that $(H_Z H_X^T)^T = H_X H_Z^T$ so we only need to think about one!

Logical operators $\in \ker\left(\begin{pmatrix} H_X & 0 \\ 0 & H_Z \end{pmatrix}\begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}\right) = \ker\left(\begin{pmatrix} 0 & H_X \\ H_Z & 0 \end{pmatrix}\right)$

$\Rightarrow \begin{pmatrix} \ker(H_Z) \\ \ker(H_X) \end{pmatrix}$? $\begin{matrix} \text{(X-logicals)} \\ \text{(Z-logicals)} \end{matrix}$

But we have to mod out by stabilizers!

X-logicals $\in \dfrac{\ker(H_Z) \to \text{define: } C_Z}{\text{im}(H_X^T) \to C_X^\perp}$ Z-logicals $\in \dfrac{\ker(H_X) \to \text{define: } C_X}{\text{im}(H_Z^T) \to C_Z^\perp}$

Write $\text{im}(\tilde{G}_X^T) = C_Z$ & $\text{im}(\tilde{G}_Z^T) = C_X$

e.g. Shor code $\hookrightarrow \tilde{G}_X^T = \begin{pmatrix} 1&1&1&0&0&0&0&0&0 \\ 0&0&0&1&1&1&0&0&0 \\ 0&0&0&0&0&0&1&1&1 \end{pmatrix}$

Just a notation for collecting the independent null vectors of H_Z...

generator matrix $\hookrightarrow$ one independent logical:

$\hookrightarrow G_X = (1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0)$ $X_1X_2X_3$

$\text{im}(\tilde{G}_X^T) = \ker(H_Z) = \text{im}(G_X^T) \oplus \text{im}(H_X^T)$

$\oplus$: sum over independent generators

since $(000111000) = (111000000) + (111111000)$

$\in \text{im}(\tilde{G}_X^T)$ $\in \text{im}(G_X^T)$ $\in \text{im}(H_X^T)$

Similar calculation for Shor code: $G_Z = (100100100)$.

Prop: codespace has dimension 2^k, where

$$k := \dim[\ker(H_X)] - \dim[\text{im}(H_Z^T)] = \dim[\ker(H_Z)] - \dim[\text{im}(H_X^T)]$$

Proof: check two expressions equal? rank-nullity $\Rightarrow$

$$2^n = |\ker(H_X)| \cdot |\text{im}(H_X^T)| = |\ker(H_Z)|\,|\text{im}(H_Z^T)|.$$

So: $$\frac{|\ker(H_X)|}{|\mathrm{im}(H_Z^T)|} = \frac{|\ker(H_Z)|}{|\mathrm{im}(H_X^T)|} = \frac{2^n}{|\mathrm{im}(H_X^T)|\,|\mathrm{im}(H_Z^T)|} = 2^{n-m-m} = 2^k$$

count w/ Z-log — count w/ X-logicals — # of ind. stab.

Prop: can choose $G_X, G_Z \in \mathbb{F}_2^{k\times n}$ such that $G_X G_Z^T = I_{k\times k} \Rightarrow$ non-commuting X & Z-logicals for logical qubits.

Proof: Notice that $\ker(H_X) = \mathrm{im}(H_X^T)^\perp = \{v : v\cdot H_X^T s = 0 \ \forall s\}$ (Ditto for Z).

Let $v_Z \in \mathrm{im}(H_X^T)^\perp$ be a Z-logical; $v_X \in \mathrm{im}(H_Z^T)^\perp$ an X-log.

Then $v_Z \cdot v_X = (v_Z + H_Z^T s_Z)\cdot(v_X + H_X^T s_X)$ independent of stab. repres.

$= v_Z^T v_X + s_Z^T H_Z v_X + v_Z^T H_X^T s_X + s_Z^T H_Z H_X^T s_X$

If $\exists\, v_Z$ s.t. $v_Z \cdot v_X = 0 \ \forall\, v_X$, then $v_Z \in \ker(H_Z)^\perp = \mathrm{im}(H_Z^T)$ is not a non-trivial logical.

So we can choose a basis by Gaussian elimination of the desired form. Important that we found non-commuting logical X & Z operators, so we can actually manipulate the logical qubit!

e.g. for Shor code: $X_L = X_1X_2X_3$, $Z_L = Z_1Z_4Z_7$

any stab-equivalent representatives always anticommute

Def: X/Z distances: $$d_X = \min_{v\in \ker(H_Z)\setminus \mathrm{im}(H_X^T)} |v|, \quad d_Z = \min_{v\in\ker(H_X)\setminus\mathrm{im}(H_Z^T)} |v|$$

Finding these is NOT easy numerically. In contrast it is fairly easy to find G_X & G_Z. Challenge is finding smallest weight generators! Note that $d = \min(d_X, d_Z)$

We've now developed a sufficient formalism to start learning about practical quantum codes for future experiments. Key is to use this $\mathbb{F}_2$ formalism rather than work w/ Paulis directly → we'll see why in the next lecture.

Sometimes it's still useful to think about what codewords look like....

Let $\vec{z} \in \mathbb{F}_2^n$ and choose Hilbert space basis where

$$Z_j|\vec{z}\rangle = (1-2z_j)|\vec{z}\rangle$$

Logical codewords take the form:

$$|[\vec{z}]\rangle := \frac{1}{\sqrt{|\mathrm{im}(H_X^T)|}} \sum_{\vec{w}\in \mathrm{im}(H_X^T)} |\vec{z}+\vec{w}\rangle$$

an equivalence class in $C_Z/C_X^\perp = \ker(H_Z)/\mathrm{im}(H_X^T)$