Recall: n-qubit Pauli group

$$\Pi^n := \{ \underbrace{\alpha}_{\text{coeff}} (\overbrace{\sigma_1 \otimes \cdots \otimes \sigma_n}^{\text{principal part}}) : \sigma_j \text{ are Pauli operators}, \alpha \in \{1, -1, i, -i\} \}$$

Subgroup $G \leq \Pi^n$ is stabilizing if $-\mathbb{1} \notin G$

($\mathbb{1} := I \otimes \cdots \otimes I$)

Prop: If $G \leq \Pi^n$ is stabilizing, then $\forall g, h \in G$,

g has coeff ± 1

$gh = hg$

$g^2 = \mathbb{1}$

Def: $\mathcal{H} := (\mathbb{C}^2)^{\otimes n}$. G stab subgroup of Π^n.

$E_G \leq \mathcal{H}$ subspace

$E_G := \{ v \in \mathcal{H} : gv = v \quad \forall g \in G \}$

"g stabilizes v"

Fact: G is stabilizing iff $\dim(E_G) > 0$.

Def: $G \leq \Pi^n$ stabilizing. $\{g_1, \ldots, g_k\} \subseteq G$ is a minimal generating set for G if

$$G = \underbrace{\langle g_1, \ldots, g_k \rangle}_{\substack{\text{group generated} \\ \text{by } \{g_1, \ldots, g_k\}}}$$

and no proper subset of $\{g_1, \ldots, g_k\}$ generates G.

Fact: All min generating set for G have the same cardinality (dimension of G).

Prop: Let G (stab $\leq \Pi^n$) have dim k. Then

$$\dim(E_G) = 2^{n-k}.$$

Ex: $n = 3$.

$|000\rangle$ is fixed by $Z_1 = Z \otimes I \otimes I$

$Z_2 = I \otimes Z \otimes I$

$Z_3 = I \otimes I \otimes Z$

$\langle Z_1, Z_2, Z_3 \rangle$ is a min generating set for the space spanned by $|000\rangle$

$|010\rangle$ fixed by $Z_1, -Z_2, Z_3$

$|110\rangle$ " " $-Z_1, -Z_2, Z_3$

etc.

Can rep all comp. basis vectors by $\langle \pm Z_1, \pm Z_2, \ldots, \pm Z_n \rangle$

Fact:

$$P_G := \frac{1}{2^k} \sum_{g \in G} g \qquad (k = \dim G)$$

projects onto E_G

Connection with linear algebra over $\mathbb{Z}_2 = \{0, 1\}$:

Let $g = \alpha(\sigma_1 \otimes \cdots \otimes \sigma_n)$

$\varphi_x(g) = [b_1 \; b_2 \; \cdots \; b_n]$

$\varphi_z(g) = [c_1 \; c_2 \; \cdots \; c_n]$

where $\forall 1 \leq j \leq n$

$$b_j = \begin{cases} 1 & \text{if } \sigma_j \in \{X, Y\} \\ 0 & \text{if } \sigma_j \in \{I, Z\} \end{cases}$$

$$c_j = \begin{cases} 1 & \text{if } \sigma_j \in \{Z, Y\} \\ 0 & \text{if } \sigma_j \in \{I, X\} \end{cases}$$

b_j, c_j determine σ_j [$Y \propto XZ$]

$$\varphi(g) : \overbrace{[\, \varphi_x(g) \mid \varphi_z(g) \,]}^{2n \text{ dim}}$$

$\varphi(g)$ determines the principal part of g. ignores the coefficient

Fact: $\varphi(gh) = \varphi(g) + \varphi(h)$

[Easy Fact: No two distinct elements of a stabilizing G can have the same principal part.]

$\therefore \varphi$ is 1-1 on G (stab)

Ex: $X \otimes Y \otimes I = g$

$\varphi_x(g) = [1 \; 1 \; 0]$

$\varphi_z(g) = [0 \; 1 \; 0]$

$\varphi(g) = [1 \; 1 \; 0 \mid 0 \; 1 \; 0]$

$h = Z \otimes X \otimes Z$

$\varphi(h) = [0 \; 1 \; 0 \mid 1 \; 0 \; 1]$

Symplectic inner product.

Def: Let $u = [u_x \mid u_z]$
$v = [v_x \mid v_z]$

where $u_x, u_z, v_x, v_z \in \mathbb{Z}_2^n$ row vectors.

Define
$$u \diamond v = u_x \cdot v_z + u_z \cdot v_x$$
$$= u_x v_z^T + u_z v_x^T$$
$$= u \Omega v^T$$
where $\Omega = \left[\begin{array}{c|c} 0 & I_n \\ \hline I_n & 0 \end{array}\right] \in \mathbb{Z}_2^{2n \times 2n}$

Fact: $\forall g, h \in \Pi^n$
$$\varphi(g) \diamond \varphi(h) = \begin{cases} 1 & \text{if } gh = -hg \\ 0 & \text{if } gh = hg \end{cases}$$

Prop: $\{g_1, \ldots, g_k\}$ is a min generating set of a stab subgroup of Π^n iff $\forall g, h \in \{g_1, \ldots, g_k\}$
1. g has coeff ± 1
2. g, h commute $(\varphi(g) \diamond \varphi(h) = 0)$
3. $\varphi(g_1), \ldots, \varphi(g_k)$ are linearly independent over $\mathbb{Z}_2$.

Ex: $|+\rangle$ stab by X
$|-\rangle$ " " $-X$

Def: Given $\{g_1, \ldots, g_k\} \subseteq \Pi^n$ form a $k \times 2n$ matrix
$$M = \begin{bmatrix} \text{---}\ \varphi(g_1)\ \text{---} \\ \text{---}\ \varphi(g_2)\ \text{---} \\ \vdots \\ \text{---}\ \varphi(g_k)\ \text{---} \end{bmatrix}$$

Cond 3 above $\iff$ M has rank k
Cond 2 " $\iff$ $M \Omega M^T = 0$

Clifford gates:

The n-qubit Clifford group
$$\mathcal{C}_n = \{U \in \mathcal{L}(\mathcal{H}) \text{ unitary such that } UgU^* \in \Pi^n \text{ for every } g \in \Pi^n\}$$

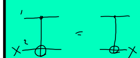
Ex: H, S are 1-qubit Clifford gates.

$HXH = Z$ $\quad SXS^* = Y$
$HZH = X$ $\quad SYS^* = -X$
$HYH = -Y$ $\quad SZS^* = Z$

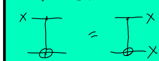
$\mathcal{C}_1$ is exactly those gates that map axes $(x-, y-, z-)$ to axes, possibly reversed.

Fact: $\{H, S\}$ generates $\mathcal{C}_1$

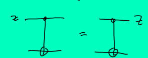
C-NOT $\in \mathcal{C}_2$



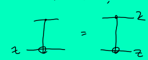
$$((C\text{-}X_{1,2}) X_2 (C\text{-}X_{1,2}) = X_2$$



$$(C\text{-}X_{1,2}) X_1 (C\text{-}X_{1,2}) = X_1 X_2 = X \otimes X$$



$$(C\text{-}X_{1,2}) Z_1 (C\text{-}X_{1,2}) = Z_1$$



$$(C\text{-}X_{1,2}) Z_2 (C\text{-}X_{1,2}) = Z_1 Z_2$$

Prop: $\mathcal{C}_n$ is generated by
$$\{H_j : 1 \leq j \leq n\} \cup$$
$$\{S_j : 1 \leq j \leq n\} \cup$$
$$\{C\text{-}X_{j,k} : 1 \leq j, k \leq n,\ j \neq k\}$$

Theorem (Gottesman - Knill)
Quantum circuits that have
1. qubits initially in the $|0\rangle$ state
2. only clifford gates
3. 1-qubit measurements in the comp basis

are efficiently simulatable classically.

Some ideas of the proof:

$\langle Z_1, \ldots, Z_n \rangle$ stabilizes the initial state $|00\cdots0\rangle$

Given any state stabilized by $\langle g_1, \ldots, g_n \rangle$ (min generating set)

Given any state ρ stabilized by $\langle g_1, \dots, g_n \rangle$ (min generating set)

and Clifford gate U,

$U \rho U^*$ is stabilized by the group with min generating set

$$\langle U g_1 U^*, \dots, U g_n U^* \rangle$$