Given errors \( \{ \mathbf{e} \} \in \mathcal{E} \) if \( \exists \mathbf{g} \in \mathcal{S} \) s.t.
\[
\mathbf{e}_g = -g \mathbf{e}, \quad \forall \mathbf{e} \in \mathcal{E},
\]
then \( \{ \mathbf{g} \} \) can be corrected by code \( \mathcal{C}(S) \).

**Proof:** \( \forall \mathbf{y} \in \mathcal{C}(S) \)
\[
\langle \mathbf{y}, \mathbf{e} \rangle = \langle \mathbf{y}, g \mathbf{e} \rangle = \langle g^{-1} \mathbf{y}, \mathbf{e} \rangle = \langle \mathbf{y}, \mathbf{g}^{-1} \mathbf{e} \rangle = \langle \mathbf{y}, \mathbf{e} - \mathbf{e}_g \rangle = 0
\]
\[
\langle \mathbf{y}, \mathbf{e} \rangle = 0
\]

**Lecture #5: Stabilizers II**

1. Stabilizer Codes (cont.)
2. The Normalizer
3. The Clifford Group
4. Computing on codes
5. Measurements

**Pauli group:**

\[
\begin{align*}
\mathcal{S} & \in \mathcal{E} \\
\mathbf{X}, \mathbf{Y}, \mathbf{Z}, \pm 1, \pm i
\end{align*}
\]

What is the stabilizer for \( |0\rangle \)? \( \mathcal{S} = \langle \mathbf{Z} \rangle \)
for \( |1\rangle \): \( \mathcal{S} = \langle -\mathbf{Z} \rangle \)

**Today's Question:**

- Quantum description of codes?
- Quantum computation on encoded data?

**I/ Stabilizer Codes**

Then given errors \( \{ \mathbf{e}_g \} \in \mathcal{E} \) if \( \exists \mathbf{g} \in \mathcal{S} \) s.t. \( \mathbf{e}_g = -g \mathbf{e} \), for all
\[
\mathbf{e} = \mathbf{e}_1 + \mathbf{e}_2,
\]
then \( \{ \mathbf{e}_g \} \) can be corrected by the code \( \mathcal{C}(S) \).
Def. For $S = \langle s_1, \ldots, s_k \rangle$, and error $E$, the error syndrome is

$$E = \begin{cases} 0, & \text{if } [s_i, E] = 0, \quad i = 1, \ldots, k^2 \\ 1, & \text{otherwise} \end{cases}$$

Ex. a) $S = \langle IZI, ZIZ \rangle$ \hspace{1cm} $CS(S) = \text{span } \{000, 111\}$

$$E = \begin{pmatrix} IZI \end{pmatrix}$$

error syndrome $= \{01\}$

uncorrectable $E = \begin{pmatrix} IZI \end{pmatrix}$

by Thm $\Rightarrow E = \begin{pmatrix} IZI, IZI \end{pmatrix}$

b) $S = \langle XX \rangle$ \hspace{1cm} $CS(S) = \left\{ \frac{00+11}{\sqrt{2}}, \frac{01+10}{\sqrt{2}} \right\}$

$$E = \begin{pmatrix} ZI \end{pmatrix}$$

if we form $\{ZI, ZI\}$

$Z^2 Z = Z^2$ \hspace{1cm} commute with $g = XX$ \hspace{1cm} uncorrectable by Thm

$\text{same syndrome}$

c) $XZIZ = g_1$ \hspace{1cm} $CS(S) = ?$

$ZXXZ = g_2$

$ZIZXX = g_3$

$d) \begin{pmatrix} IZI \end{pmatrix} = g_1$

$$E = \begin{pmatrix} IZI \end{pmatrix}$$

$E = \begin{pmatrix} IZI \end{pmatrix}$

How many possible single qubit errors?

$3 + 1 = 2^2$ \hspace{1cm} $t = 3$ (Hamming code $\rightarrow$ CSS)

Including no error "3 qubit stabilizer code"
e) $XZ^2X_1 = g_1$
   $IXZ^2X = g_2$
   $XIXZ^2 = g_3$
   $ZIXZ^2 = g_4$

   $n=5$
   $k=1$

   **Error Syndrome**: 16 possibilities
   **Errors**: $(5) \cdot 3 + 1 = 16$ ("perfect code")

3) $|100> = \frac{|001> + |110>}{\sqrt{2}}$, $|110> = |111>

   $S = \sigma_x$
   $XX|111> = 100>$
   $ZZ|010> = -|010>$

II/ The Normalizer

- Unitary ops: $|14> \rightarrow U |14>
- Stabilizer $S \rightarrow U S U^†$
- $g \in S \rightarrow U_g S U_g^†$

Def: The Normalizer of $S$ is $N(S) = \{ g \in G | ghg^† = g, \forall h \in S \}$

Up: group

Lemma: $N(S) = \{ g \in G | [g, h] = 0, \forall h \in S \}$

Proof: Recall: either $gh = hg$ or $gh = -hg$, $\forall g, h \in G$
Thus $ghg^† = \pm g^†hg = \pm h$
Recall $-I \notin S$, therefore $ghg^+ = h$.

$\Rightarrow ghg^+ = h \leq hgg^+$

$\Rightarrow \chi_hg^+ = 0$

a) $S = \langle 2I, 3I \rangle$

$N(S) = \{ 2I, 3I, 12, 21 \}$

b) $S = \langle x^2 \rangle$

$N(S) = \{ x^k, x^k, x^k, x^k, \ldots \}$

c) $S = \langle x^2, 3x^2 \rangle$

$N(S) = \{ x^2, zI, zI, \ldots, x^2, zI, zI, \ldots \}$

$G_f$

$\langle zI, 2zI \rangle = S$

$N(S) = XXX,$

Def. $wt(g) = \#$ of mm I's

Def. A code $C(S)$ has distance $d$ if $N(S) - S$ has no elements of $wt < d$

Def. If $S$ has elements of $wt < d$ (except 1)

then $C(S)$ is degenerate

otherwise $C(S)$ is mm-degenerate
III / The Clifford Group

What is the Normalizer of the Pauli group \( G \) ?

"generalized"

\[
\begin{array}{ccc}
2x & N(G) & \text{II} \\
\uparrow & \begin{array}{cccc}
I & X & Y & Z \\
X & -X & -X & Z \\
Y & Y & Y & -Y & -X \\
Z & -Z & -Z & Z & X \\
\end{array} \\
\end{array}
\]

\[
S = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \sqrt{Z}
\]

\[
\langle H, S \rangle \quad S^2 = Z \\
H^2 = H = X \\
X^2 = -X
\]

Define \( \langle H, S \rangle = \text{Clifford group on 1 qubit} \)

\[
N(G) = \quad \begin{array}{c}
\begin{array}{c}
XX \\
XY
\end{array}
\end{array} = \begin{array}{c}
\begin{array}{c}
X \\
I
\end{array}
\end{array}
\]

\[
\begin{array}{c|c}
\text{II} & \text{CNOT} \\
\hline
XY & XX \\
IX & IX \\
XX & XI \\
IZ & EZ \\
EZ & ZI \\
\end{array}
\]

Recall

\[
\begin{array}{c}
\begin{array}{c}
H \\
H
\end{array}
\end{array}
\]

Def. \( C_2 = \text{Clifford group} \)

\( = \langle H, S, \text{CNOT} \rangle \)

Is the \( N(G) \)
Thm. (Gottesman-Knill)

1) Suppose $U \in G_n$, $v, z \in G_n$
then $U$ can be constructed from $O(n^3)$ $H$, $S$, CNOT gates
(up to $e^{\Omega(n)}$)

2) Any quantum circuit
composed of $H$, $S$, CNOT, acting on an input $|0>^\otimes n$
and with meas. in the computational basis
$|00...0> + \text{classical control}$, can be efficiently simulated
on a classical computer!