Thm Given errors $\{E_a\} \in G$ if $\exists g \in S$ s.t

$E g = -g E$, $\forall E = E_a^\dagger E_b$, then $\{E_a\}$ can be

corrected by code $C(S)$

proof: $\forall |\psi\rangle \in C(S)$

$$\underset{0 = \langle\psi| E_a^\dagger E_b |\psi\rangle}{\langle\psi| E |\psi\rangle} = \langle\psi| E g |\psi\rangle = -\underbrace{\langle\psi| g}_{\langle\psi|} E |\psi\rangle = -\langle\psi| E |\psi\rangle$$

$\Rightarrow \langle\psi| E |\psi\rangle = 0$

Lecture #5: Stabilizers II

1. Stabilizer Codes (con't)
2. The Normalizer
3. The Clifford Group
4. Computing on codes
5. Measurements

Note: PS #2 due 04-MAR

stabilizer $S \subset G$ Pauli group

$X, Y, Z, \pm 1, \pm i$

What is the stabilizer for $|0\rangle$? $S = \langle Z \rangle$

for $|1\rangle$? $S = \langle -Z \rangle$

Today's Question:

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

I/ Stabilizer Codes

Thm Given errors $\{E_a\}$ (Pauli errors) $\in G$ if $(\exists g \in S$ s.t. $E g = -g E)$, for all $E = E_a^\dagger E_b$ $(a \neq b)$, then $\{E_a\}$ can be corrected by the code $C(S)$.

Def. For $S = \langle g_1, \cdots, g_k \rangle$, and error E,
the error syndrome is

k-bit string $\left\{ \begin{cases} 0, & \text{if } [g_i, E] = 0 \\ 1, & \text{otherwise} \end{cases} \;\middle|\; i = 1, \ldots, k \right\}$

Ex a) $S = \langle \overset{g_1}{IZZ}, \overset{g_2}{ZZI} \rangle$ $\qquad C(S) = \text{span}\{000, 111\}$

$E = XII$ $\qquad$ error syndrome $= \{01\}$

$E = IXI$ $\qquad \{11\}$

uncorrectable by Thm $\rightarrow$ $E = XXX$ $\qquad \{00\}$

$E = III$ $\qquad \{00\}$

b) $S = \langle XX \rangle$ $\qquad C(S) = \left\{ \frac{00+11}{\sqrt{2}}, \frac{01+10}{\sqrt{2}} \right\}$

$E = ZI$

IZ

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

$\underbrace{Z_a^{\dagger} E_b = ZZ}$ "commute" with $g = XX$ $\rightarrow$ uncorrectable by Thm
same syndrome

c) $XZIZ = g_1$ $\qquad C(S) = ?$

$ZXZI = g_2$ $\qquad E = XIII$

$IZXZ = g_3$

$ZIZX = g_4$ $\qquad n=4, \ k=0$

d)
$$\begin{pmatrix} I\,I\,I\,X\,X\,X\,X = g_1 \\ I\,X\,X\,I\,I\,X\,X = g_2 \\ X\,I\,X\,I\,X\,I\,X = g_3 \\ I\,I\,I\,Z\,Z\,Z\,Z = g_4 \\ I\,Z\,Z\,I\,I\,Z\,Z = g_5 \\ Z\,I\,Z\,I\,Z\,I\,Z = g_6 \end{pmatrix}$$

$E = XI^6$

$E = IXI^5$

$E = XI^6$

there are some g's that anticommutes with E.

Syndromes: 6 bits ~64 possibilities

How many possible single qubit errors?

$\binom{7}{1} \cdot \underset{X,Y,Z}{\overset{\uparrow}{3}} + \underset{\text{including no error}}{\overset{\uparrow}{1}} = 22$

($r=3$ Hamming code $\rightarrow$ CSS)
"7 qubit Steane code"

e) $XZZXI = g_1$
$IXZZX = g_2$
$XIXZZ = g_3$
$ZXIXZ = g_4$

$n=5$
$k=1$

single qubit error

	X_1	Z_3	Y_5	Y_4	...
g_1	0	0	0	1	
g_2	0	0	1	1	...
g_3	0	1	1	1	
g_4	1	0	1	1	

unique

error syndrome : 16 possibilities
errors : $\binom{5}{1} \cdot 3 + 1 = 16$
"perfect code"

f) $|0_L\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$, $|1_L\rangle = |11\rangle$

$S = ?$

$XX|11\rangle = |00\rangle$ ×

$ZZ|0_L\rangle = -|0_L\rangle$ ×

II/ The Normalizer

Unitary ops $\quad |\psi\rangle \xrightarrow{U} U|\psi\rangle$

Stabilizer $S \xrightarrow{U} USU^\dagger$

$g \in S \xrightarrow{U} UgU^\dagger$

because $U|\psi\rangle = Ug|\psi\rangle$
$= UgU^\dagger U|\psi\rangle$
$= (UgU^\dagger)(U|\psi\rangle)$

Def The Normalizer of S
is $N(S) = \{g \in G \mid ghg^\dagger \in S, \forall h \in S\}$
$\uparrow$ Pauli group

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

Proof Recall : either $gh = hg$ or $gh = -hg$, $\forall g,h \in G$
Thus $ghg^\dagger = \pm g g^\dagger h = \pm h$

Recall $-I \notin S$, therefore $ghg^\dagger \neq -h$

$\Rightarrow ghg^\dagger = h = hgg^\dagger$

$\Rightarrow [h, g] = 0$

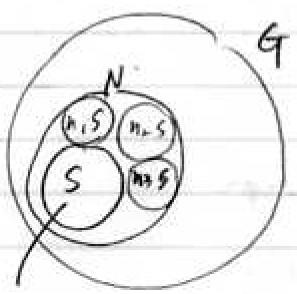
Ex a) $S = \langle IZ, ZI \rangle$

$N(S) = \{ZZ, II, IZ, ZI\}$

b) $S = \langle XX \rangle$

$N(S) = \{IX, XI, ZZ, YY, YZ, \ldots\}$

c) $S = \langle IXX, IZZ \rangle$ $N(S) = \{ZZZ, ZII = \bar{Z}, XXX, XII = \bar{X}$



$\left\langle \begin{matrix} IZZ \\ ZZI \end{matrix} \right\rangle = S$

$N(S) = XXX, \ldots$

Def. $wt(g) = \#$ of non I's, $g \in S$

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 I) then $C(S)$ is <u>degenerate</u>

otherwise $C(S)$ is <u>non-degenerate</u>

III / The Clifford Group

What is the Normalizer of the Pauli group G ?
"generalized"

Ex $N(G_1)$
$\uparrow$
$\{X, Y, Z\}$

I	X	Y	Z	H	S
X	X	-X	-X	Z	Y
Y	-Y	Y	-Y	-Y	-X
Z	-Z	-Z	Z	X	Z

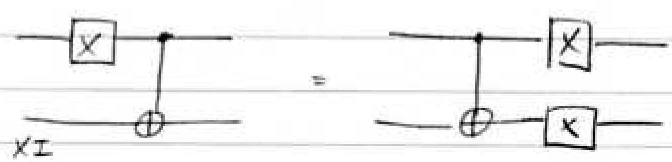
$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} = \sqrt{Z}$

$\langle H, S \rangle$ $\quad S^2 = Z$
$HZH = \underline{X}$
$XZ = -i\cancel{Y}$

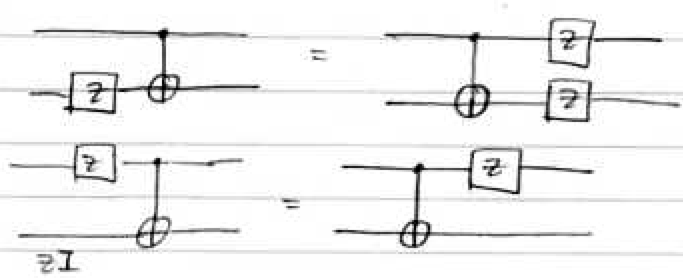
<u>Define</u> $\langle H, S \rangle$ = clifford group on 1 qubit

$N(G_2) = ?$

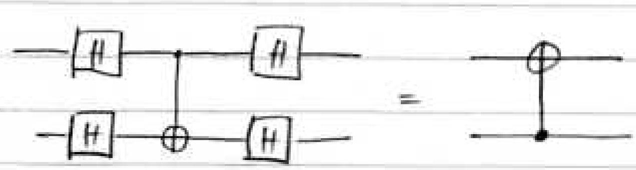
$XX \rightarrow YZ$
$\quad IY$
$\quad \vdots$



II	CNOT
XI	XX
IX	IX
XX	XI
IZ	ZZ
ZI	ZI
ZZ	IZ



Recall



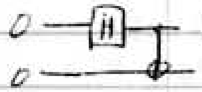
<u>Def.</u> $C_2 \equiv$ Clifford group
$= \langle H, S, CNOT \rangle$
Is the $N(G_2)$

Thm (Gottesman – Knill)

1) Suppose $U g U^\dagger \in G_n$, $\forall g \in G_n$

then U can be constructed from $O(n^2)$ H, S, CNOT gates (up to $e^{i\theta}$)

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



$|00\rangle + |11\rangle$