

Title: Quantum Error Correction 2A

Date: Jan 16, 2007 03:30 PM

URL: <http://pirsa.org/07010020>

Abstract: Stabilizer codes (definition of stabilizer, basic properties of stabilizer, binary vector representation of stabilizer)

TENSOR Product

\Rightarrow w/ overall phase $\pm 1, \pm i$

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad Y = iXZ$$

$$XY = -YX, XZ = -ZX, YZ = -ZY, X^2 = Y^2 = Z^2 = I$$

$$\forall P, Q \in P_n, \quad PQ = QP (\text{if } P, Q \neq 0) \quad \text{or} \quad PZQ = QP \quad (\Leftrightarrow \{P, Q\} = 0)$$
$$P^2 = \pm I$$

wt P = # of non-identity tensor factors

Pauli group qubits:

Tensor products of I, X, Y, Z w/ overall phase $\pm 1, \pm i$

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad Y = iXZ$$

$$XY = -YX, \quad XZ = -ZX, \quad YZ = -ZY, \quad X^2 = Y^2 = Z^2 = I$$

$$\forall P, Q \in \mathcal{P}_n, \quad PQ = QP \Leftrightarrow \{P, Q\} = 0 \quad \text{or} \quad PQ = -QP \Leftrightarrow \{P, Q\} = 0$$

$$P^2 = \pm I$$

w/ $P = \#$ of non-identity tensor factors

$$|0\rangle = (|000\rangle + |111\rangle)^{\otimes 3} \quad |1\rangle = (|000\rangle - |111\rangle)^{\otimes 3}$$

$$|0\rangle = (|000\rangle + |111\rangle)^{\otimes 3} \quad |1\rangle = (|000\rangle - |111\rangle)^{\otimes 3}$$

ପ୍ରକଟିତ
ପରିପାଳନ

$$|1\rangle = (|000\rangle + |111\rangle)^{\frac{1}{\sqrt{2}}}$$

દોડાંડા
ટ્રાન્સફોર્મ

દોડાંડા
ટ્રાન્સફોર્મ

દોડાંડા
ટ્રાન્સફોર્મ

$$|0\rangle = (|000\rangle - |111\rangle)^{\frac{1}{\sqrt{2}}}$$



$$|0\rangle = (|000\rangle + |111\rangle)^{\frac{1}{\sqrt{2}}} \quad |1\rangle = (|000\rangle - |111\rangle)^{\frac{1}{\sqrt{2}}}$$

$\begin{matrix} 0 & 0 & 0 \\ 1 & 0 & 0 \end{matrix}$

$\begin{matrix} 0 & 0 & 1 \\ 1 & 0 & 0 \end{matrix}$

$\begin{matrix} 0 & 1 & 0 \\ 1 & 0 & 0 \end{matrix}$

$\begin{matrix} 0 & 0 & 0 \\ 1 & 1 & 1 \end{matrix}$



$$|0\rangle = (|000\rangle + |111\rangle)^{\frac{1}{\sqrt{2}}} \quad |1\rangle = (|000\rangle - |111\rangle)^{\frac{1}{\sqrt{2}}}$$

000111
111000

000111
111000

000111
111000

X0X0X0X0X0X0X
X0X0X0X0X0X0X

$$|0\rangle = (|000\rangle + |111\rangle)^{\frac{1}{\sqrt{2}}}$$

$$|1\rangle = (|000\rangle - |111\rangle)^{\frac{1}{\sqrt{2}}}$$

$\begin{matrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{matrix}$

$\begin{matrix} 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \end{matrix}$

$\begin{matrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{matrix}$

$\begin{matrix} X & 0 & X & 0 \\ X & 0 & X & 0 \end{matrix}$

$\begin{matrix} X & 0 & X & 0 \\ X & 0 & X & 0 \end{matrix}$

8 operators
eigenvalues determine
error syndrome

$$|0\rangle = (|000\rangle + |111\rangle)^{\otimes 3}$$

$\begin{matrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{matrix}$

$\begin{matrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{matrix}$

$\begin{matrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{matrix}$

$\begin{matrix} X & 0 & X & 0 & X & 0 & X & 0 & X \\ X & 0 & X & 0 & X & 0 & X & 0 & X \end{matrix}$

$\begin{matrix} X & 0 & X & 0 & X & 0 & X & 0 & X \\ X & 0 & X & 0 & X & 0 & X & 0 & X \end{matrix}$

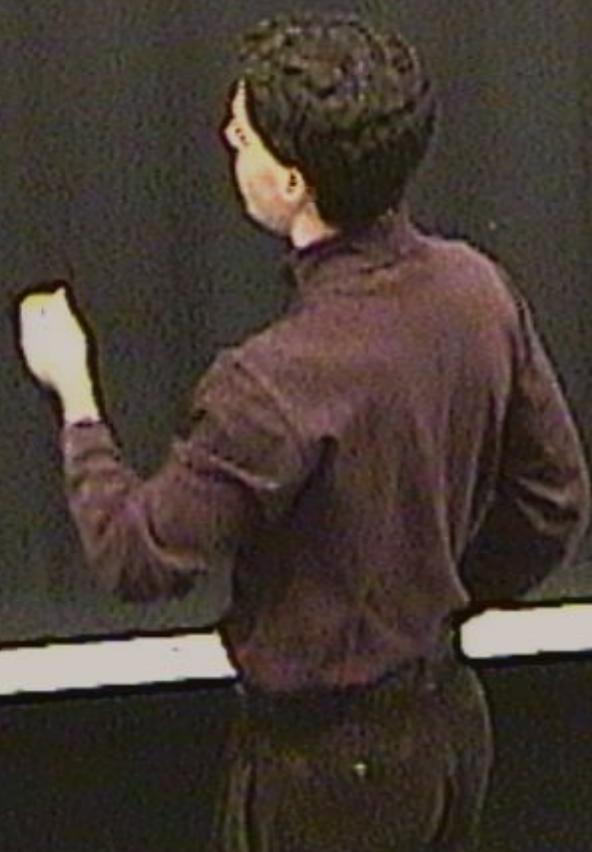
$$|1\rangle = (|000\rangle - |111\rangle)^{\otimes 3}$$

8 operators
eigenvalues determine
error syndrome

Def.:



Def.: Let T be a subspace of an n -qubit Hilbert space. Define



Def.: Let \bar{T} be a subspace of an n -qubit Hilbert space. Define

$$S(\bar{T}) = \{P \in P_0 \mid P \mid \bar{V}\}$$



Def.: Let \bar{T} be a subspace of an n -qubit Hilbert space. Define

$$S(\bar{T}) = \{P \in P_n | P|\psi\rangle = |\psi\rangle \forall |\psi\rangle \in \bar{T}\}$$

$S(\bar{T})$ is called the stabilizer of \bar{T} .

Def: Let \bar{T} be a subspace of an n -qubit Hilbert space. Define

$$S(\bar{T}) = \{P \in \mathcal{P} \mid P|\psi\rangle = |\psi\rangle \forall |\psi\rangle \in \bar{T}\}$$

$S(\bar{T})$ is called the stabilizer of \bar{T} .

Properties of the stabilizer:

$$\textcircled{1} \quad S(\bar{T}) \text{ is a group: } P, Q \in S(\bar{T}) \Rightarrow PQ|\psi\rangle = P|Q|\psi\rangle = |\psi\rangle$$

Def: Let \bar{T} be a subspace of an n -qubit Hilbert space. Define

$$S(\bar{T}) = \{P \in \mathcal{P} \mid P|\psi\rangle = |\psi\rangle \forall |\psi\rangle \in \bar{T}\}$$

$S(\bar{T})$ is called the stabilizer of \bar{T} .

Properties of the stabilizer:

① $S(\bar{T})$ is a group: $P, Q \in S(\bar{T}) \Rightarrow PQ|\psi\rangle = P|Q|\psi\rangle = |\psi\rangle \forall |\psi\rangle \in \bar{T}$

② $S(\bar{T})$ is Abelian:

Def: Let \bar{T} be a subspace of an n -qubit Hilbert space. Define

$$S(\bar{T}) = \{P \in \mathcal{P}_n \mid P|\psi\rangle = |\psi\rangle \forall |\psi\rangle \in \bar{T}\}$$

$S(\bar{T})$ is called the stabilizer of \bar{T} .

Properties of the stabilizer:

$$\text{Properties of the stabilizer: } P, Q \in S(\bar{T}) \Rightarrow PQ|\psi\rangle = P|Q|\psi\rangle = |\psi\rangle \quad \forall |\psi\rangle \in \bar{T}$$

① $S(\bar{T})$ is a group: $P, Q \in S(\bar{T}) \Rightarrow PQ|\psi\rangle = P|Q|\psi\rangle = Q|P|\psi\rangle \Rightarrow [P, Q]|\psi\rangle = 0$

② $S(\bar{T})$ is Abelian: $P, Q \in S(\bar{T}) \Rightarrow PQ|\psi\rangle = P|Q|\psi\rangle = Q|P|\psi\rangle$

Def.: Let \bar{T} be a subspace of an n -qubit Hilbert space. Define

$$S(\bar{T}) = \{P \in \mathcal{P}_n \mid P|\psi\rangle = |\psi\rangle \forall |\psi\rangle \in \bar{T}\}$$

$S(\bar{T})$ is called the stabilizer of \bar{T} .

Properties of the stabilizer:

$$\textcircled{1} \quad S(\bar{T}) \text{ is a group: } P, Q \in S(\bar{T}) \Rightarrow PQ|\psi\rangle = P|Q|\psi\rangle = P|\psi\rangle = |\psi\rangle \quad \forall |\psi\rangle \in \bar{T}$$

$$\textcircled{2} \quad S(\bar{T}) \text{ is Abelian: } P, Q \in S(\bar{T}) \Rightarrow PQ|\psi\rangle = QP|\psi\rangle = QP|\psi\rangle = [P, Q]|\psi\rangle = 0$$

$$\text{for Paulis } \Rightarrow [P, Q] = 0$$

Def: Let \bar{T} be a subspace of an n -qubit Hilbert space. Define

$$S(\bar{T}) = \{P \in \mathcal{P} \mid P|\psi\rangle = |\psi\rangle \forall |\psi\rangle \in \bar{T}\}$$

$S(\bar{T})$ is called the stabilizer of \bar{T} .

Properties of the stabilizer:

① $S(\bar{T})$ is a group: $P, Q \in S(\bar{T}) \Rightarrow PQ|\psi\rangle = P|Q|\psi\rangle = |\psi\rangle \quad \forall |\psi\rangle \in \bar{T}$

② $S(\bar{T})$ is Abelian: $P, Q \in S(\bar{T}) \Rightarrow PQ|\psi\rangle = QP|\psi\rangle = [P, Q]|\psi\rangle = 0 \quad \forall |\psi\rangle \in \bar{T}$

for Paulis $\Rightarrow [P, Q] = 0$

③ $-I \notin S(\bar{T})$

Def.: Let \bar{T} be a subspace of an n -qubit Hilbert space. Define

$$S(\bar{T}) = \{P \in \mathcal{P} \mid P|\psi\rangle = |\psi\rangle \forall |\psi\rangle \in \bar{T}\}$$

$S(\bar{T})$ is called the stabilizer of \bar{T} .

Properties of the stabilizer:

$$\textcircled{1} \quad S(\bar{T}) \text{ is a group: } P, Q \in S(\bar{T}) \Rightarrow PQ|\psi\rangle = P|Q|\psi\rangle = |\psi\rangle \quad \forall |\psi\rangle \in \bar{T}$$

$$\textcircled{2} \quad S(\bar{T}) \text{ is Abelian: } P, Q \in S(\bar{T}) \Rightarrow PQ|\psi\rangle = QP|\psi\rangle = [P, Q]|\psi\rangle = 0 \quad \forall |\psi\rangle \in \bar{T}$$

$$\text{for Paulis } \Rightarrow [P, Q] = 0$$

$$\textcircled{3} \quad -I \notin S(\bar{T})$$

$$\textcircled{4} \quad \text{①, ②, ③} \Rightarrow |S(\bar{T})| = 2^r$$

Def: Let \mathcal{T} be a subspace of an n -qubit Hilbert space. Define

$$S(\mathcal{T}) = \{P \in \mathcal{P} \mid P|\psi\rangle = |\psi\rangle \forall |\psi\rangle \in \mathcal{T}\}$$

$S(\mathcal{T})$ is called the stabilizer of \mathcal{T} .

Properties of the stabilizer:

① $S(\mathcal{T})$ is a group: $P, Q \in S(\mathcal{T}) \Rightarrow PQ|\psi\rangle = P|Q|\psi\rangle = |\psi\rangle \quad \forall |\psi\rangle \in \mathcal{T}$

② $S(\mathcal{T})$ is Abelian: $P, Q \in S(\mathcal{T}) \Rightarrow PQ|\psi\rangle = QP|\psi\rangle = [P, Q]|\psi\rangle = 0 \quad \forall |\psi\rangle \in \mathcal{T}$

③ For Paulis $\Rightarrow [P, Q] = 0$

④ $-I \in S(\mathcal{T})$

⑤ $①, ②, ③ \Rightarrow |S(\mathcal{T})| = 2^r$ r generators M_1, \dots, M_r
 $M_1, M_1^{\alpha_1}, \dots, M_r^{\alpha_r}$ ($\alpha_i \in \{0, 1\}$)

$$|0\rangle = (|000\rangle + |111\rangle)^{\frac{1}{\sqrt{2}}}$$

$$|1\rangle = (|000\rangle - |111\rangle)^{\frac{1}{\sqrt{2}}}$$

0000111
1111000

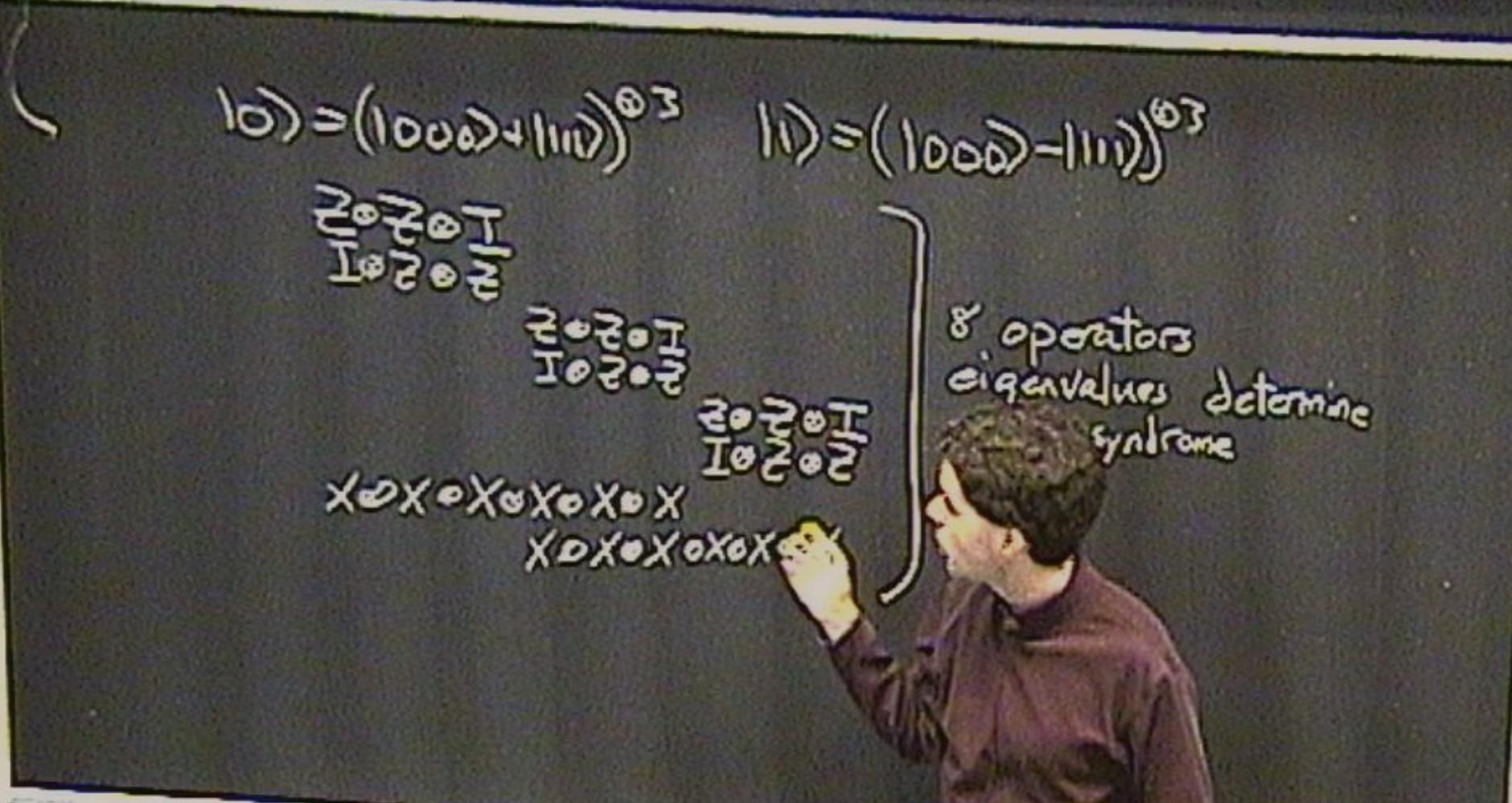
0000111
1111000

0000111
1111000

XOXOXOXOXOX

XOXOXOXOX

8 operators
eigenvalues determine
syndrome



Def: Let \bar{T} be a subspace of an n -qubit Hilbert space. Define

$$S(\bar{T}) = \{P \in P_0 \mid P|\psi\rangle = |\psi\rangle \forall |\psi\rangle \in \bar{T}\}$$

$S(\bar{T})$ is called the stabilizer of \bar{T} .

Properties of the stabilizer:

$$\textcircled{1} S(\bar{T}) \text{ is a group: } P, Q \in S(\bar{T}) \Rightarrow PQ|\psi\rangle = P|Q\psi\rangle = P|\psi\rangle = |\psi\rangle \quad \forall |\psi\rangle \in \bar{T}$$

$$\textcircled{2} S(\bar{T}) \text{ is Abelian: } P, Q \in S(\bar{T}) \Rightarrow PQ|\psi\rangle = QP|\psi\rangle = [P, Q]|\psi\rangle = 0 \quad \forall |\psi\rangle \in \bar{T}$$

for Paulis $\Rightarrow [P, Q] = 0$

$$\textcircled{3} -I \notin S(\bar{T})$$

$$\textcircled{4} \quad \textcircled{1}, \textcircled{2}, \textcircled{3} \Rightarrow |S(\bar{T})| = 2^r \quad r \text{ generators } M_1, \dots, M_r \\ M_1^{a_1}, M_2^{a_2}, \dots, M_r^{a_r} \quad (a_i \in \{0, 1\})$$

Def.: Let S be an Abelian subgroup of P_n -Ics.
The code space of S

θ $\theta, \theta, \dots, \theta, \theta$ $\in \mathbb{C}^n$

$M_1 M_2 \dots M_r (k, n)$

Def: Let S be an Abelian subgroup of $P_n - I \otimes S$.

The code space of S is

$$T(S) = \{ |\psi\rangle \}$$



θ $\theta, \theta, \theta = \lambda M_1 \theta$
 $r \leq n$ $M_1 M_2 \dots M_r (\lambda, 0) \theta$

Def: Let S be an Abelian subgroup of P_n , $I \in S$.

The code space of S is

$$T(S) = \{ |\psi\rangle \mid P|\psi\rangle = |\psi\rangle \quad \forall P \in S \}$$

Def.: Let S be an Abelian subgroup of P_n . Then

The code space of S is

$$T(S) = \{ |\psi\rangle \mid P|\psi\rangle = |\psi\rangle \quad \forall P \in S \}$$

S or $T(S)$ is a stabilizer code

Def.: Let S be an Abelian subgroup of P_n , $I \in S$.

The code space of S is

$$T(S) = \{ | \psi \rangle \mid P | \psi \rangle = | \psi \rangle \quad \forall P \in S \}$$

S or $T(S)$ is a stabilizer code

$S = S(T(S))$ but not always true that $T = T(S(T))$

Def.: Let S be an Abelian subgroup of P_0 , $I \in S$.

The code space of S is

$$T(S) = \{ |v\rangle \mid P|v\rangle = |v\rangle \quad \forall P \in S \}$$

S or $T(S)$ is a stabilizer code

$S = S(T(S))$ but not always true that $T = T(S(T))$
(but $T \subseteq T(S(T))$)

Def.: Let S be an Abelian subgroup of P_n , $I \in S$.

The code space of S is

$$T(S) = \{ |v\rangle \mid P|v\rangle = |v\rangle \quad \forall P \in S \}$$

S or $T(S)$ is a stabilizer code

$S = S(T(S))$ but not always true that $T = T(S(T))$
(but $T \subseteq T(S(T))$)
(Sometimes symplectic code or additive
additive GF(H))

Def.: Let S be an Abelian subgroup of P_n , $I \in S$.

The code space of S is

$$T(S) = \{ | \psi \rangle \mid P(| \psi \rangle) = | \psi \rangle \quad \forall P \in S \}$$

S or $T(S)$ is a stabilizer code

$S = S(T(S))$ but not always true that $T = T(S(T))$

(Sometimes symplectic code or additive
additive GF(2))

(but $T \subseteq T(S(T))$)

$$|0\rangle = (|000\rangle + |111\rangle)^{\otimes 3}$$

$$|1\rangle = (|000\rangle - |111\rangle)^{\otimes 3}$$

$\begin{smallmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{smallmatrix}$

$\begin{smallmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{smallmatrix}$

$\begin{smallmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{smallmatrix}$

$\begin{smallmatrix} X & 0 & X & 0 & X & 0 & X \\ X & 0 & X & 0 & X & 0 & X \end{smallmatrix}$

$\begin{smallmatrix} X & 0 & X & 0 & X & 0 & X \\ X & 0 & X & 0 & X & 0 & X \end{smallmatrix}$

8 operators
eigenvalues determine
error syndrome



Ihn.: Let S be a stabilizer with

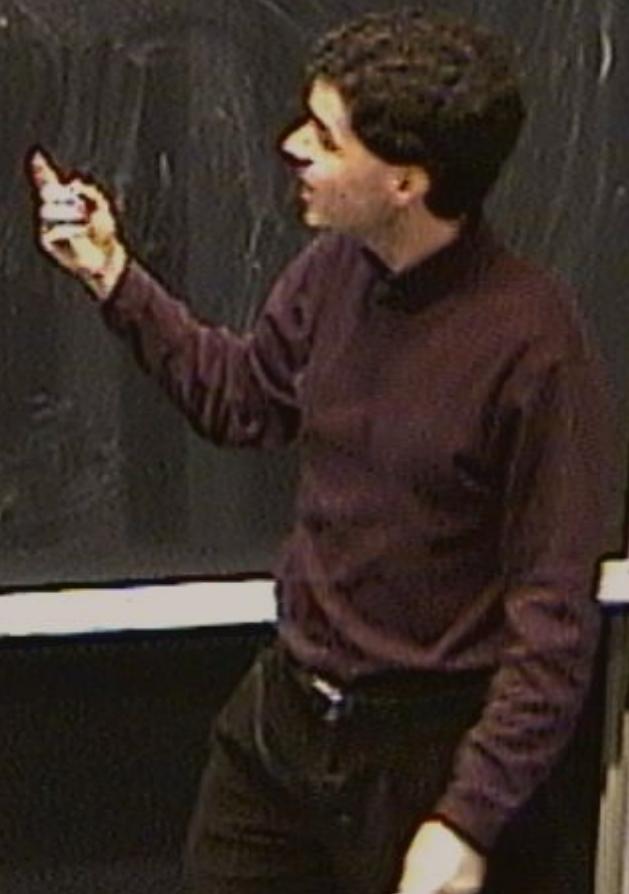


Ihm.: Let S be a stabilizer with r generators on n qubits. Then



Thm.: Let S be a stabilizer with r generators on n qubits. Then

a) $\dim T(S) = 2^{n-r}$ ($k=n-r$ encoded qubits)



Thm.: Let S be a stabilizer with r generators on n qubits. Then

a) $\dim T(S) = 2^{n-r}$ ($k = n-r$ encoded qubits)

b) Let $N(S) = S^\perp = \{P \in \mathcal{P}_n \mid PM = MP \ \forall M \in S\}$

$$|0\rangle = (|000\rangle + |111\rangle)^{0.5}$$

टैटॉड
टैटॉड

टैटॉड
टैटॉड

XOXOXOXOXOX
XOXOXOXOXOX

टैटॉड
टैटॉड

$$|1\rangle = (|000\rangle - |111\rangle)^{0.5}$$

8. operations
signature
determine

Signature
determine

Signature
determine

Def. L

The co

S or

S =
(Someti..)

Thm.: Let S be a stabilizer with r generators on n qubits. Then

a) $\dim T(S) = 2^{n-r}$ ($k=n-r$ encoded qubits)

b) Let $N(S) = S^\perp = \{P \in \mathcal{P}_n \mid PM = MP \ \forall M \in S\}.$

Then S can detect errors outside $N(S) \setminus S$

Thm.: Let S be a stabilizer with r generators on n qubits. Then

a) $\dim T(S) = 2^{n-r}$ ($k=n-r$ encoded qubits)

b) Let $N(S) = S^\perp = \{P \in \mathcal{P}_n \mid PM = MP \ \forall M \in S\}.$

Then S can detect errors outside $N(S) \setminus S$.

The distance of S is min. wt. P , $P \in N(S) \setminus S$

Thm.: Let S be a stabilizer with r generators on n qubits. Then

a) $\dim T(S) = 2^{n-r}$ ($k=n-r$ encoded qubits)

b) Let $N(S) = S^\perp = \{P \in \mathcal{P}_n \mid PM = MP \forall M \in S\}$.

Then S can detect errors outside $N(S) \setminus S$.
The distance of S is $\min_{P \in N(S) \setminus S} \text{wt}(P)$

Notation: A QECC encoding a k -dim. subspace in n qubits with distance d , is $((n, k, d))$. A \mathbb{Z}_2 -linear code

Thm. Let S be

an n qubits. Then

a) $\dim T(S) = 2^{n-r}$ ($k=n-r$ encoded qubits)

b) Let $N(S) = S^\perp = \{P \in \mathcal{P} \mid PM = MP \forall M \in S\}$.

Then S can detect errors outside $N(S) \setminus S$.

The distance of S is $\min_{P \in \mathcal{P}} |P \cap N(S) \setminus S|$.

Notation: A QCCC encoding a K -dim subspace in n qubits, with distance d , is $((n, k, d))$. A stabilizer code with $K=2$ is (n, k, d) .

Ihn.: Let S be a stabilizer with r generators on n qubits. Then

a) $\dim T(S) = 2^{n-r}$ ($k=n-r$ encoded qubits)

b) Let $N(S) = S^\perp = \{P \in \mathcal{P}_n \mid PM = MP \ \forall M \in S\}$.

Then S can detect errors outside $N(S) \setminus S$.

The distance of S is $\min_{P \in N(S) \setminus S} d(P)$

Notation: A QECC encoding a K -dim. subspace in n qubits, with rate d , is $((n, k, d))$. A stabilizer code with $K=2^k$ is $[[n, k, d]]$.

Proof of b:

Proof of b:

Suppose $M \in S$, $P \in P_n$, $\{P, M\} = 0$
 $P \models \psi$



Proof of b:

Suppose $M \in S$, $P \in P_n$, $\{P, M\} = 0$

$$M(P|\psi\rangle) = -PM|\psi\rangle - (P|M\rangle)$$

$P|\psi\rangle$ is $-I$ eigenstate of M

Proof of b:

Suppose $M \in S$, $P \in P_0$, $\{P, M\} = 0$

$$M(P|\psi) = -PM|\psi\rangle - (P|M|\psi\rangle)$$

$P|\psi\rangle$ is $-I$ eigenstate of M ($P \in N(S)$):

Suppose $P \in P_0$, $[P, M] = 0 \quad \forall M \in S$ ($P \in T(S)$):

$$\forall M \in S, M(P|\psi\rangle) = PM|\psi\rangle = P|\psi\rangle$$

$$P|\psi\rangle \in T(S)$$

Proof of b:

Suppose $M \in S$, $P \in P_n$, $\{P, M\} = 0$

$$M(P|\psi) = -PM|\psi\rangle - (P|M)\langle\psi|$$

$P|\psi\rangle$ is $-I$ eigenstate of M ($P \in N(S)$):

Suppose $P \in P_n$, $[P, M] = 0 \quad \forall M \in S$

$$\forall M \in S, M(P|\psi\rangle) = PM|\psi\rangle = P|M\rangle$$

$$P|M\rangle \in T(S)$$

P is undetectable except if $P|\psi\rangle = |\psi\rangle$ $\forall M \in S$

Then S can detect errors outside $\text{N}(S)$

The distance of S is $\min_{P \in \mathcal{P}} \text{wt}(P)$

Notation: A QECC encoding a K -dim. subspace in n qubits, with distance d , is $((n, K, d))$. A stabilizer code with $K=2^k$ is $[[n, k, d]]$.

$T|\psi\rangle$ is -1 eigenstate of T^\dagger

Suppose $P \in \mathcal{P}_n$, $[P, T] = 0 \quad \forall M \in S \quad (P \in N(S))$:

$$\forall M \in S, M(P|\psi\rangle) = P M |\psi\rangle = P |\psi\rangle$$

$$P|\psi\rangle \in T(S)$$

$P|\psi\rangle = |\psi\rangle$ $\forall M \in S$

P is undetectable except if $P|\psi\rangle = |\psi\rangle$

b) Let $N(S) = S^\perp = \{P \in \mathcal{P}_n \mid PM = MP \ \forall M \in S\}$.

Then S can detect errors outside $N(S) \setminus S$.

The distance of S is $\min_{P \in N(S) \setminus S} \|P\|$

Notation: A QECC encoding a K -dim. subspace in n qubits, with distance d , is $((n, K, d))$. A stabilizer code with $K=2^k$ is $[[n, k, d]]$.

Def.:

$$\text{times, } M(P|\psi) = PM|\psi\rangle = P|\psi\rangle$$

$$P|\psi\rangle \in T(S)$$

P is undetectable except if

$$V|\psi\rangle \in T(S)$$

b) Let $N(S) = S^\perp = \{P \in \mathcal{P}_n \mid PM = MP \ \forall M \in S\}$.

Then S can detect errors outside $N(S) \setminus S$.

The distance of S is $\min_{M \in S} \text{wt}(PM)$, $P \in N(S) \setminus S$.

Notation: A QECC encoding a K -dim. subspace in n qubits, with distance d , is $((n, K, d))$. A stabilizer code with $K=2^k$ is $[[n, k, d]]$.

Def.: A QECC is degenerate for a set of linearly independent set of errors C if $C_{ab} \subset T(S)$

$$\text{Since } M(P|Y) = PM(Y) = P(Y)$$

$$P(Y) \in T(S)$$

P is undetectable except if

$$P(Y) = 0 \Rightarrow P \in T(S)$$

b) Let $N(S) = S^\perp = \{P \in \mathcal{P}_n \mid PM = MP \ \forall M \in S\}$.

Then S can detect errors outside $N(S) \setminus S$.

The distance of S is min. wt. $P, P \in N(S) \setminus S$

Notation: A QECC encoding a K -dim. subspace in n qubits, with distance d , is $((n, K, d))$. A stabilizer code with $K=2^k$ is $[[n, k, d]]$.

Def.: A QECC is degenerate for a set of linearly independent set of errors C if C_{ab} does not have maximum rank. It is degenerate

$$\text{unless } P(PY) = PY(P) = PY \quad PY \in T(S)$$

P is undetectable except if $P(Y) = Y(P) \quad \forall Y \in T(S)$

b) Let $N(S) = S^\perp = \{P \in \mathcal{P}_n \mid PM = MP \ \forall M \in S\}$.

Then S can detect errors outside $N(S) \setminus S$.

The distance of S is $\min_{M \in S} \text{wt}(P, P \in N(S) \setminus S)$

Notation: A QECC encoding a K -dim. subspace in n qubits, with distance d , is $((n, K, d))$. A stabilizer code with $K=2^k$ is $[[n, k, d]]$.

Def.: A QECC is degenerate for a set of linearly independent set of errors C if C_{ab} does not have maximum rank. It is degenerate if it's degenerate for $C = \{P \in \mathcal{P}_n \mid \text{wt}(P) \leq t, d=2t+1\}$

$$\text{Since, } M(P|Y) = PM|Y = P|Y$$

$$P|Y \in T(S)$$

P is undetectable except if $P|Y = P$,
 $\Rightarrow P \in S$

b) Let $N(S) = S^\perp = \{P \in \mathcal{P}_n \mid PM = MP \ \forall M \in S\}$.

Then S can detect errors outside $N(S) \setminus S$.

The distance of S is min. wt. $P, P \in N(S) \setminus S$

Notation: A QECC encoding a K -dim. subspace in n qubits, with distance d , is $((n, K, d))$. A stabilizer code with $K=2^k$ is $[[n, k, d]]$.

Def.: A QECC is degenerate for a set of linearly independent set of errors C if C_{ab} does not have maximum rank. It is degenerate if it's degenerate for $C = \{P \in \mathcal{P}_n\}$ at $P \in S, d=2t+1$

Hence, $\text{Im}(P|_S) = PM|_S = P|M$
 $P|M \in T(S)$

P is undetectable except if $P|M = 0$ $\forall M \in S$

$$|1\rangle = (|000\rangle + |111\rangle)^{0.5}$$

0001
1110

$$|0\rangle = (|000\rangle - |111\rangle)^{0.5}$$

0000
1111

X0X0X0X0X
X0X0X0X0X

} 8 operations
eigenvalues determine
error syntax



of errors \mathcal{E} if C_{ab} does not have maximum rank. It is orthogonal if its degenerate for $\mathcal{E} = \{P \in \mathcal{P}_n \mid \text{wt } P < t, d=2t+1\}$

Proof of b:

Suppose $M \in S$, $P \in \mathcal{P}_n$, $\{P, M\} = 0 \quad P \in N(S)$

$$M(P|\psi\rangle) = -PM|\psi\rangle - (P|M\rangle)$$

$P|\psi\rangle$ is -1 eigenstate of M

Suppose $P \in \mathcal{P}_n$, $[P, M] = 0 \quad \forall M \in S \quad (P \in N(S))$:

$$\forall M \in S, M(P|\psi\rangle) = PM|\psi\rangle = P|M\rangle$$

$P|\psi\rangle \in T(S)$

P is undetectable except if $P|\psi\rangle = |\psi\rangle \quad \forall |\psi\rangle \in P \in S$

(A stabilizer code is degenerate if $E_a^{\perp} E_b$)

of errors \mathcal{E} if C_{ab} does not have maximum rank. It is degenerate if its degenerate for $\mathcal{E} = \{P \in \mathcal{P}_n \mid \text{wt } P < t, d=2t+1\}$

Proof of b:

Suppose $M \in S$, $P \in \mathcal{P}_n$, $\{P, M\} = 0 \quad P \in N(S)$

$$M(P|\psi) = -PM|\psi\rangle = \langle P|\psi\rangle$$

$P|\psi\rangle$ is -1 eigenstate of M

Suppose $P \in \mathcal{P}_n$, $[P, M] = 0 \quad \forall M \in S \quad (P \in N(S))$:

$$\forall M \in S, M(P|\psi) = PM|\psi\rangle = P|\psi\rangle$$

$P|\psi\rangle \in T(S)$

P is undetectable except if $P|\psi\rangle = |\psi\rangle \quad \forall |\psi\rangle \in T(S)$

(A stabilizer code is degenerate if $e_i, e_j \in S$ for e_i, e_j distinct correctable ones)

of errors \mathcal{E} if C_{ab} does not have maximum rank. It is degenerate if its degenerate for $\mathcal{E} = \{P \in \mathcal{P}_n\}$ at $P < t, d = 2t+1\}$

$$M(P|\Psi) = -PM|\Psi\rangle = -(P|\Psi\rangle)$$

$P|\Psi\rangle$ is -1 eigenstate of M

Suppose $P \in \mathcal{P}_n, [P, M] = 0 \forall M \in S \quad (P \in N(S))$:

$$\forall M \in S, M(P|\Psi\rangle) = PM|\Psi\rangle = P|\Psi\rangle$$

$$P|\Psi\rangle \in T(S)$$

$P|\Psi\rangle$ is undetectable except if $P|\Psi\rangle = |\Psi\rangle \quad \forall |\Psi\rangle \in T(S)$

P is undetectable $\Leftrightarrow P \in S$
(A stabilizer code is degenerate if $E_a, E_b \in S$ for E_a, E_b distinct correctable errors.)
In a non-degenerate stabilizer code, $\text{dist} = \min_{S \in S} N(S)$

of errors \mathcal{E} if C_{ab} does not have maximum rank. It is degenerate if its degenerate for $\mathcal{E} = \{P \in \mathcal{P}_n\}$ at $P < t, d = 2t+1\}$

Proof of b:

Suppose $M \in S, P \in \mathcal{P}_n, \{P, M\} = 0 \quad P \in N(S)$

$$M(P|\psi) = -PM|\psi\rangle = -(P|\psi\rangle)$$

$P|\psi\rangle$ is -1 eigenstate of M

Suppose $P \in \mathcal{P}_n, [P, M] = 0 \quad \forall M \in S \quad (P \in N(S))$:

$$\forall M \in S, M(P|\psi\rangle) = PM|\psi\rangle = P|\psi\rangle$$

$P|\psi\rangle \in T(S)$

$P|\psi\rangle = |\psi\rangle \quad \forall |\psi\rangle \in T(S)$

P is undetectable except if $P|\psi\rangle = |\psi\rangle \quad \forall |\psi\rangle \in S$

(A stabilizer code is degenerate if $e_1, e_2 \in S$ for e_1, e_2 distinct correctable errs.)

In a non-degenerate stabilizer code, $\text{fd} = \min_{e \in S} N(e)$

$$|0\rangle = (|000\rangle + |111\rangle)^{\otimes 3}$$

$\begin{matrix} 0 & 0 & 0 \\ 1 & 1 & 1 \end{matrix}$

$\begin{matrix} 0 & 0 & 0 \\ 1 & 0 & 0 \end{matrix}$

$\begin{matrix} 0 & 0 & 0 \\ 1 & 0 & 1 \end{matrix}$

$\begin{matrix} X & 0 & X \\ X & 0 & X \end{matrix}$

$\begin{matrix} X & 0 & X \\ X & 0 & X \end{matrix}$

$$|1\rangle = (|000\rangle - |111\rangle)^{\otimes 3}$$

8 operators
eigenvalues determine
error syndrome

of errors $\subset \mathcal{E}$
if it's degenerate for $\mathcal{E} = \{P_i P_j\}$ at $P < t, d > 2N$

Proof of b:

Suppose $M \in S$, $P \in P_n$, $\{P, M\} = 0 \quad P \in N(S)$

$$M(P|\Psi) = -PM|\Psi\rangle - \langle P|\Psi\rangle$$

$P|\Psi\rangle$ is -1 eigenstate of M

$P \in P_n$, $[P, M] = 0 \quad \forall M \in S \quad (P \in N(S))$:

Suppose $P \in P_n$, $P|\Psi\rangle = PM|\Psi\rangle = P|\Psi\rangle$

$$P|\Psi\rangle \in T(S)$$

\Rightarrow undetectable except if $P|\Psi\rangle = |\Psi\rangle$ $|H\rangle \in T(S)$

\Rightarrow degenerate if $C \in S$ for early initial conditions.

Increase stabilizer code, but error at MS



In general, for a stabilizer code,
error syndrome of P

In general, for a stabilizer code,

error syndrome of P given

by $\vec{e} \in \mathbb{Z}_2^r$, r-bit binary vector

$$e_i = \begin{cases} 0 & [P, M_i] = 0 \\ 1 & [P, M_i] \neq 0 \end{cases}$$

(M_1, \dots, M_r are g)

In general, for a stabilizer code,
error syndrome of P given
by $\vec{e} \in \mathbb{F}_2^r$, r -bit binary vector
 $e_i = \begin{cases} 0 & [P, M_i] = 0 \\ 1 & [P, M_i] \neq 0 \end{cases}$
(M_1, \dots, M_k are generators of S)



In general, for a stabilizer code,

error syndrome of P given

by $\vec{s} \in \mathbb{Z}_2^n$, n-bit binary vector

$$s_i = \begin{cases} 0 & [P, M_i] = 0 \\ 1 & [P, M_i] \neq 0 \end{cases}$$

(M_1, \dots, M_k are generators of S)

$$\text{Syndrome}(PQ) = \text{syndrome}(P) + \text{syndrome}(Q)$$

In general, for a stabilizer code,

error syndrome of P given

by $\vec{s} > r$ -bit binary vector

$$s_i = \begin{cases} 0 & [P, M_i] = 0 \\ 1 & [P, M_i] \neq 0 \end{cases}$$

(M_1, \dots, M_k are generators of S)

$$\text{Syndrome}(PQ) = \text{syndrome}(P) + \text{syndrome}(Q) \quad (\text{binary})$$

In general, for a stabilizer code,

error syndrome of P given

by $\vec{s} \in \mathbb{F}_2^r$, r-bit binary vector

$$s_i = \begin{cases} 0 & [P, M_i] = 0 \\ 1 & [P, M_i] \neq 0 \end{cases}$$

(M_1, \dots, M_k are generators of S)

Syndrome (PQ) = Syndrome (P) + syndrome (Q) (binary)

syndrome $P =$ syndrome $Q \Leftrightarrow$ syndrome (PQ) = 0 $\Leftrightarrow PQ \in N(S)$

The code space of S is

$$T(S) = \{ |\psi\rangle \mid P|\psi\rangle = |\psi\rangle \forall P \in S \}$$

S or $T(S)$ is a stabilizer code

$S = S(T(S))$ but not always true that $T = T(S(T))$
(but $T \subseteq T(S(T))$)
(Sometimes symplectic code or additive
additive (EFH))

Projector onto $T(s)$:



Projector onto $T(S)^\perp \Pi_S$:

Projector onto +1 eigenspace of $M \in \mathcal{P}_n$:

Projector onto $T(s)^\perp \Pi_S$:

Projector onto +1 eigenspace of $M \in \mathcal{P}_n$: $I - M$

Projector onto $T(s)^\perp \Pi_S$:
Projector onto +1 eigenspace of $M \in \mathcal{P}_n$: $\frac{1}{2}(I + M)$

Projector onto $T(s)$: Π_S :
Projector onto +1 eigenspace of $M \in \mathcal{P}_0$: $\frac{1}{2}(I+N)$

$$\Pi_S =$$

Projector onto $T(s)^\perp$ Π_s :

Projector onto +1 eigenspace of $M \circ T_0 : \frac{1}{2}(I+M)$

$$\Pi_s = \frac{1}{2}M^{-1}(I+M)$$

$\{M_i\}$ generators of s



Projector onto $T(S)$: Π_S :

Projector onto +1 eigenspace of $M \circ T_0$: $\frac{1}{2}(I+M)$

$$\Pi_S = \frac{1}{2} \sum_{m_i \in S} (I + M_i) = \frac{1}{2} \sum_{m_i \in S} M_i$$

$\{m_i\}_{i \in S}$ generators of S

Projector onto $T(S)$: Π_S :

Projector onto +1 eigenspace of $M \in \mathcal{P}_n$: $\frac{1}{2}(I+M)$

$$\Pi_S = \frac{1}{2} \sum_{M_i \in S} (I + M_i) = \frac{1}{2} I + \sum_{M_i \in S} M_i$$

$\{M_i\}$ generators of S

$M \in \mathcal{P}_n / \exists i, j \in S$ can be represented as $(M_x | M_z)$

Projector onto $T(S)$: Π_S :

Projector onto +1 eigenspace of $M \in \mathcal{P}_n$: $\frac{1}{2}(I+M)$

$$\Pi_S = \frac{1}{2} \sum_{M_i \in S} (I + M_i) = \frac{1}{2^n} \sum_{M \in S} M$$

from 3 generators of S

$M \in \mathcal{P}_n / \{I\}$, if can be represented as $(M_1 | M_2)$, M_1, M_2 n-bit binary vectors

Projector onto $T(S)$: Π_S :

Projector onto +1 eigenspace of MCP_0 : $\frac{1}{2}(I+M)$

$$\Pi_S = \frac{1}{2} \sum_{M_i \in S} (I + M_i) = \frac{1}{2^{n-k}} \sum_{M \in S} M$$

{m, s generators of S}

~~$MCP_0 / \{I\}_{S^{\perp}}$~~ can be represented as $(M_x | M_y)$ 1.8 Mb n-bit
array vectors
ith bit of M_x = ith bit of M_y

Projector onto $T(S)$: Π_S :

Projector onto +1 eigenspace of $M \in \mathcal{P}_n$: $\frac{1}{2}(I+M)$

$$\Pi_S = \frac{1}{2} \sum_{M_i \in S} (I + M_i) = \frac{1}{2^{n-h}} \sum_{M \in S} M$$

$\{M_i\}$ generators of S

$M \in \mathcal{P}_n / \{\pm 1, \pm i\}$ can be represented as $(M_x | M_z)$,

i-th bit of M_x & i-th bit of M_z to determine
i-th Pauli tensor product decompr. of M

n-bit
vectors

Projector onto $T(S)$: Π_S :

Projector onto +1 eigenspace of $M \in \mathcal{P}_n$: $\frac{1}{2}(I+M)$

$$\Pi_S = \frac{1}{2} \sum_{M_i \in S} (I + M_i) = \frac{1}{2^{n-k}} \sum_{M \in S} M$$

$\{M_i\}$ generators of S

$M \in \mathcal{P}_n / \{ \pm I, \pm i \}$ can be represented as $(M_x | M_z)$, M_x & M_z n-bit binary vectors
ith bit of M_x & ith bit of M_z to determine $\begin{cases} (M_x)_i = 1 \\ (M_z)_i = 0 \end{cases} \Rightarrow X$ in ith position
ith Pauli = tensor product decompr. of M

Projector onto $\overline{T(S)}$: Π_S :

Projector onto +1 eigenspace of $M \in \mathcal{P}_n$: $\frac{1}{2}(I+M)$

$$\Pi_S = \frac{1}{2} \sum_{M_i \in S} (I + M_i) = \frac{1}{2^{n-k}} \sum_{M \in S} M$$

$\{M_i\}$ generators of S

$M \in \mathcal{P}_n / \{\pm 1, \pm i\}$ can be represented as $(M_x | M_z)$, $M_x \otimes M_z$ $n \times n$.
ith bit of M_x & ith bit of M_z to determine $\begin{cases} (M_x)_i = 1 \\ (M_z)_i = 0 \end{cases} \Rightarrow X$ in i th position
ith Pauli is tensor product decompr. of M

Product in $\mathcal{P}_n \Leftrightarrow$ sum in binary vector notation

Projector onto $T(S)$: Π_S :

Projector onto +1 eigenspace of $M \in \mathcal{P}_n$: $\frac{1}{2}(I+M)$

$$\Pi_S = \frac{1}{2} \overline{\Pi} \cdot (I+M_i) = \frac{1}{2^{n-k}} \sum_{M \in S} M$$

$\{M_i\}$ generators of S

$M \in \mathcal{P}_n / \{I, -I\}$ can be represented as (P_1, P_2) , $M_1 \otimes M_2$ n-bit binary vectors
ith bit of $M_1 \otimes$ ith bit of M_2 to determine
ith Pauli in tensor product decomps. of M

Product in $\mathcal{P}_n \Leftrightarrow$ sum in binary vector notation

Def: Symplectic inner product $P \cdot Q =$

Projector onto $T(S)$: Π_S :

Projector onto +1 eigenspace of $M \in \mathcal{P}_n$: $\frac{1}{2}(I+M)$

$$\Pi_S = \frac{1}{2} \sum_{M_i \in S} (I + M_i) = \frac{1}{2^{n-k}} \sum_{M \in S} M$$

{M_i: i generators of S}

$M \in \mathcal{P}_n / \{ \pm 1, \pm i \}$ can be represented as $(M_x | M_z)$,

i-th bit of M_x & i-th bit of M_z to determine $\begin{cases} S(M)_i = 1 \\ S(M)_i = 0 \end{cases} \Rightarrow x_i$
i-th Pauli \rightarrow tensor product decompr. of M

Product in $\mathcal{P}_n \Leftrightarrow$ sum in binary vector notation

Def.: Symplectic inner product $P \cdot Q = P_x \cdot Q_z$

Projector onto $T(S)$: Π_S :

Projector onto +1 eigenspace of $M \in \mathcal{P}_n$: $\frac{1}{2}(I+M)$

$$\Pi_S = \frac{1}{2} \sum_{M_i \in S} (I + M_i) = \frac{1}{2^{n-k}} \sum_{M \in S} M$$

$\{M_i\}$ generators of S

$M \in \mathcal{P}_n / \{ \pm I, \pm i \}$ can be represented as $(M_x | M_z)$, M_x & M_z n-bit binary vectors
ith bit of M_x & ith bit of M_z to determine $\begin{cases} (M_j)_i = 1 \\ (M_{j'})_i = 0 \end{cases} \Rightarrow X$ in i th position
ith Pauli \rightarrow tensor product decompr. of M

Product in $\mathcal{P}_n \Leftrightarrow$ sum in binary vector notation

Def: Symplectic inner product $P \cdot Q = P_x \cdot Q_z + Q_x \cdot P_z$

Projector onto $T(S)$: Π_S :

Projector onto +1 eigenspace of $M \in \mathcal{P}_n$: $\frac{1}{2}(I+M)$

$$\Pi_S = \frac{1}{2} \sum_{M_i \in S} (I + M_i) = \frac{1}{2^{n-k}} \sum_{M \in S} M$$

$\sum_{M_i \in S}$ generators of S

$M \in \mathcal{P}_n / \{ \pm I, \pm iS \}$ can be represented as $(M_x | M_z)$, M_x & M_z n-bit binary vectors
ith bit of M_x & ith bit of M_z to determine $\begin{cases} (M_j)_i = 1 \\ (M_j)_i = 0 \end{cases} \Rightarrow X$ in ith position
ith Pauli : tensor product decomp. of M

Product in $\mathcal{P}_n \Leftrightarrow$ sum in binary vector notation

Def: Synaptic inner product $P \cdot Q = P_x \cdot Q_x + Q_x \cdot P_z$

$$(P_x | P_z)$$

$$(Q_x | Q_z)$$



Projector onto $\overline{T(S)}$: Π_S :

Projector onto +1 eigenspace of $M \in \mathcal{P}_n$: $\frac{1}{2}(I+M)$

$$\Pi_S = \frac{1}{2^n} \prod_{i=1}^n (I + M_i) = \frac{1}{2^{n-k}} \sum_{M \in S} M$$

$\{M_i\}$ generators of S

$M \in \mathcal{P}_n / \{z=1, z=i\}$ can be represented as $(M_x | M_z)$, M_x & M_z n-bit binary vectors
ith bit of M_x & ith bit of M_z to determine $\begin{cases} (M_x)_i = 1 \\ (M_z)_i = 0 \end{cases} \Rightarrow X$ in i th position
ith Pauli \rightarrow tensor product decompr. of M

Product in $\mathcal{P}_n \Leftrightarrow$ sum in binary vector notation
 $P \cdot Q = P_x \cdot Q_x + Q_x \cdot P_z \quad (\text{mod 2 addition})$

Def.: Symplectic inner product



Projector onto $\overline{T(S)}$: Π_S :

Projector onto +1 eigenspace of $M \in \mathcal{P}_n$: $\frac{1}{2}(I+M)$

$$\Pi_S = \frac{1}{2} \sum M_i (I + M_i) = \frac{1}{2^{n-k}} \sum_{M \in S} M$$

$\{M_i\}$ generators of S

$M \in \mathcal{P}_n / \{I, -I\}$ can be represented as $(M_x | M_z)$, M_x & M_z n-bit binary vectors
ith bit of M_x & ith bit of M_z to determine $\begin{cases} (M_x)_i = 1 \\ (M_z)_i = 0 \end{cases} \Rightarrow X$ in ith position
ith Pauli tensor product decompr. of M

Product in $\mathcal{P}_n \Leftrightarrow$ sum in binary vector notation

$$P \cdot Q = P_x \cdot Q_z + Q_x \cdot P_z \quad (\text{mod 2 addition}) \quad \begin{pmatrix} P_x | P_z \\ Q_x | Q_z \end{pmatrix}$$

Def.: Symplectic inner product $P \cdot Q = [P, Q] = 0$

Example: $X \oplus Y \oplus I = P$
 $Z \oplus Z \oplus Z = Q$



Example: $X \oplus Y \oplus I = P$ (110)
 $Z \oplus Z \oplus Z = Q$



Example: $X \oplus Y \oplus I = P$ $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}$
 $Z \oplus Z \oplus Z = Q$ $\begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}$

Example: $X \oplus Y \oplus I = P$ $\begin{pmatrix} 110 \\ 010 \end{pmatrix}$
 $Z \oplus Z \oplus Z = Q$ $\begin{pmatrix} 000 \\ 111 \end{pmatrix}$
 $P|Q = \text{complement}$



Example: $X \otimes Y \otimes I = P$ $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}$
 $Z \otimes Z \otimes Z = Q$ $\begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}$
 $X, Y, Z \Rightarrow \text{commute}$
 $P \cdot Q = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}$



Example: $X \oplus Y \oplus I = P$ $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}$
 $Z \oplus T \oplus Z = Q$ $\begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}$
 $\{I, X, Y\} \Rightarrow \text{commute}$
 $P \cdot Q = (1 \cdot 1 + 1 \cdot 1 - 0 \cdot 1) + (0 \cdot 0 - 1 \cdot 0 + 0 \cdot 0)$



Example: $X \oplus Y \oplus I = P$ $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}$

$Z \oplus Z \oplus Z = Q$ $\begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}$

$\hat{X}\hat{I}\hat{Y}(\hat{Z})\hat{Y}(\hat{Z}) \Rightarrow$ commute

$$P \cdot Q = (1 \cdot 1 \cdot 1 \cdot 1 \cdot 0 \cdot 1) - (0 \cdot 0 \cdot 1 \cdot 0 \cdot 0 \cdot 0) = 0$$



Example: $X \oplus Y \oplus I = P$ $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}$
 $Z \oplus Z \oplus Z = Q$ $\begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}$
 $\forall I \ (\neg I) \ (\neg 0) \Rightarrow \text{commute}$
 $P \cdot Q = (1 \cdot 1 + 1 \cdot 1 + 0 \cdot 1) - (0 \cdot 0 + 1 \cdot 0 + 0 \cdot 0) = 0$

Proof of b:

Lemma:

Example: $X \otimes Y \otimes I = P$ $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}$

$Z \otimes Z \otimes Z = Q$ $\begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}$

$\langle 1 | (-1) | 1 \rangle \Rightarrow$ commute

$$P \cdot Q = (1 \cdot 1 + 1 \cdot -1 + 0 \cdot 1) - (0 \cdot 0 + 1 \cdot 0 + 0 \cdot 0) = 0$$

Proof of q_1 :

Lemma: Given n independent Pauli operators

Example: $X \otimes Y \otimes I = P$ $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}$

$Z \otimes Z \otimes Z = Q$ $\begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}$

$\{I, (-I), (\tau_0)\} \Rightarrow$ commute

$$P \cdot Q = (1 \cdot 1 + 1 \cdot 1 + 0 \cdot 1) + (0 \cdot 0 + 1 \cdot 0 + 0 \cdot 0) = 0$$

Proof of α_1 : Given $s \in n$ independent Pauli operators, binary vector $a \in$
Lemma: Given $s \in n$ independent Pauli operators, binary vector $a \in$
(n. dim.)

Example: $X \otimes Y \otimes I = P$ $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}$

$Z \otimes Z \otimes Z = Q$ $\begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}$

$\langle \vec{I} | \vec{I} \rangle \langle \vec{I} | \vec{I} \rangle = \text{constant}$

$$P \cdot Q = (1 \cdot 1 + 1 \cdot 1 + 0 \cdot 1) - (0 \cdot 0 + 1 \cdot 0 + 0 \cdot 0) = 0$$

Proof of a_3 :

Lemma: Given $s \in n$ independent Pauli operators (i.e. binary vector are lin. indep.), vector \vec{s} (s bits)



Example: $X \otimes Y \otimes I = P$ $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes I = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$

$Z \otimes Z \otimes Z = Q$ $\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix}$

$\langle 1 | (-1) | 0 \rangle = \text{commute}$

$$P \cdot Q = (1 \cdot 1 \cdot 1 \cdot 1 \cdot 0 \cdot 1) + (0 \cdot 0 \cdot 1 \cdot 0 \cdot 0 \cdot 0) = 0$$

Proof of α_3 :

Lemma: Given $s \in \mathbb{N}$ independent Pauli operators (i.e. binary vector are lin. indep.), vector \vec{z} ($\leq s$ bits). Then \exists $n-s$ independent

Example: $X \otimes Y \otimes I = P$ $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes I = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$

$Z \otimes Z \otimes Z = Q$ $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \otimes \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \otimes \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$

$\{I, (-1), (-i)\} \Rightarrow$ commute

$$P \cdot Q = (\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}) \cdot (\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}) = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = 0$$

Proof of g_1 :

Lemma: Given $s \leq n$ independent Pauli operators P_i ($i = 1, \dots, s$), vector \vec{c} (s bits). Then \exists $n-s$ independent Pauli operators Q_j ($j = 1, \dots, n-s$) such that $P_i \cdot Q_j = c_i$.

Example: $X \otimes Y \otimes I = P$ $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}$

$Z \otimes Z \otimes Z = Q$ $\begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}$

$\{I, (-I), (\tau_0)\} \Rightarrow$ commute

$$P \cdot Q = (1 \cdot 1 - 1 \cdot 1 + 0 \cdot 1) + (0 \cdot 0 - 1 \cdot 0 + 0 \cdot 0) = 0$$

Proof of a_1 :

Lemma: Given $s \leq n$ independent Pauli operators P_i (i.e. binary lin. indep.), vector \vec{z} (s bits). Then $\exists 2^{n-s}$ independent Q_j 's

$$P_i \cdot Q_j = c_i$$

Proof:



Example: $X \otimes Y \otimes I = P$ $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes I = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$

$Z \otimes Z \otimes Z = Q$ $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix}$

$\{I, X, Y, Z\}$ commute

$$P \cdot Q = (\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}) \cdot (\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix}) = 0$$

Proof of a_1 :

Lemma: Given $s \in \mathbb{N}_0$ independent Pauli operators P_i (i.e. binary vector are lin. indep.), vector \vec{c} (s bits). Then $\exists s$ independent $Q_j \in \mathcal{P}_n$ st.

$$P_i \cdot Q_j = c_i$$

Proof: Linear algebra: linear equations in 2^n -dim. binary vector space

$$\text{Example: } X \otimes Y \otimes I = P \quad (110|010)$$

$$Z \otimes Z \otimes Z = Q \quad (000|111)$$

$\{I, (-I), (\tau)\} \Rightarrow$ commute

$$P \cdot Q = (1 \cdot 1 + 1 \cdot 1 + 0 \cdot 1) - (0 \cdot 0 + 1 \cdot 0 + 0 \cdot 0) = 0$$

Proof of q:

Lemma: Given $s \leq n$ independent Pauli operators P_i (i.e. binary vector w.r.t. lin. indep.), vector \vec{z} (\leq bits). Then $\exists 2^n-s$ independent $Q_j \in P_n$ st.

$$P_i \cdot Q_j = c_i$$

Proof: Linear algebra: 3 equations in 2^n -dim. binary vector space

r generators for S are P_1, \dots, P_r

$$\alpha_i \in \{0, 1\} \quad [P, M_i] = 0$$

$$[P, M_i] = 0$$

(M_1, \dots, M_k are generators of S)

$$\text{Syndrome } (PQ) = \text{syndrome } (P) + \text{syndrome } (Q) \quad (\text{binary})$$

$$\text{syndrome } P = \text{syndrome } Q \Leftrightarrow \text{syndrome } (PQ) = 0 \Leftrightarrow PQ \in N(S)$$

r generators for S are P_1, \dots, P_r

By lemma, for any \vec{e} , $\exists Q_{\vec{e}}$ s.t. $P_i \cdot Q_{\vec{e}} = e_i$

r generators for S are P_1, \dots, P_r

By lemma, for any \vec{e} , $\exists Q_{\vec{e}}$ st. $P_i \cdot Q_{\vec{e}} = e_i$
Define $S_{\vec{e}}$ to be generated by $\{(-1)^{e_i} P_i\}$

r generators for S are P_1, \dots, P_r

By lemma, for any \vec{e} , $\exists Q_{\vec{e}}$ s.t. $P_i \cdot Q_{\vec{e}} = e_i$

Define $S_{\vec{e}}$ to be generated by $\{(-1)^{e_i} P_i\}$

$Q_{\vec{e}}(\nu) \in T(S_{\vec{e}})$ when $(\nu) \in T(S)$

r generators for S are P_1, \dots, P_r

By lemma, for any \vec{e} , $\exists Q_{\vec{e}}$ st. $P_i \cdot Q_{\vec{e}} = e_i$

Define $S_{\vec{e}}$ to be generated by $\{(-1)^{e_i} P_i | Q_{\vec{e}}(v) \in T(S_{\vec{e}}) \text{ when } v \in T(S)\}$

$$\dim T(S_{\vec{e}}) = \dim T(S)$$

$$\prod S_{\vec{e}} = \frac{1}{2^r} \prod (I - (-1)^{e_i} M_i)$$

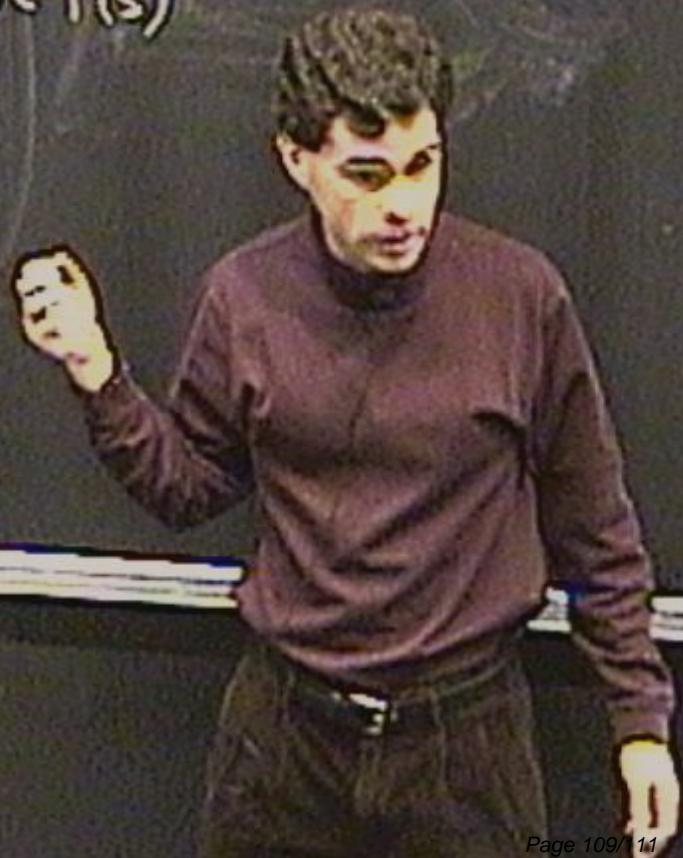
r generators for S are P_1, \dots, P_r

By lemma, for any \vec{e} , $\exists Q_{\vec{e}}$ st. $R_i Q_{\vec{e}} = e_i$

Define $S_{\vec{e}}$ to be generated by $\{(-1)^{e_i} P_i | Q_{\vec{e}}(\nu) \in T(S_{\vec{e}}) \text{ when } (\nu) \in T(S)\}$

$$\dim T(S_{\vec{e}}) = \dim T(S)$$

$$\prod S_{\vec{e}} = \prod \prod (I - (-1)^{e_i} R_i)$$



r generators for S are P_1, \dots, P_r

By lemma, for any \vec{e} , $\exists Q_{\vec{e}}$ s.t. $P_i \cdot Q_{\vec{e}} = e_i$

Define $S_{\vec{e}}$ to be generated by $\{(-1)^{e_i} P_i | Q_{\vec{e}}|\psi\rangle \in T(S_{\vec{e}}) \text{ when } |\psi\rangle \in T(S)\}$

$$\dim T(S_{\vec{e}}) = \dim T(S)$$

$$\Pi_{S_{\vec{e}}} = \bigcap_{i=1}^r \Pi(I - (-1)^{e_i} P_i)$$

$$\sum \Pi_{S_{\vec{e}}} = I \rightarrow \bigoplus_{\vec{e}} T(S_{\vec{e}}) = \text{whole Hilbert space}$$

r generators for S are P_1, \dots, P_r

By lemma, for any \vec{e} , $\exists Q_{\vec{e}}$ s.t. $P_i \cdot Q_{\vec{e}} = e_i$.

Define $S_{\vec{e}}$ to be generated by $\{(-1)^{e_i} P_i\}$
 $Q_{\vec{e}}|v\rangle \in T(S_{\vec{e}})$ when $|v\rangle \in T(S)$

$$\dim T(S_{\vec{e}}) = \dim T(S)$$

$$\Pi_{S_{\vec{e}}} = \frac{1}{2^{r-k}} \prod_i (I - (-1)^{e_i} P_i)$$

$$\sum \Pi_{S_{\vec{e}}} = I \rightarrow \bigoplus_{\vec{e}} T(S_{\vec{e}}) = \text{whole Hilbert space}$$

$$\dim T(S_{\vec{e}}) = 2^n / 2^r = 2^{n-r}$$