Quantum Stabilizer Codes

Chung-Chin Lu

Department of Electrical Engineering

National Tsing Hua University

June 10, 2010

A Primer of Group Theory

Groups

A group is a set $\mathcal{G}$ together with a binary operation $*$ on it such that

- Associativity : $(f * g) * h = f * (g * h)\ \forall\ f, g, h \in \mathcal{G}$;
- Identity element : there is an element $e \in \mathcal{G}$ such that

$$g * e = e * g = g;$$

- Inverse : for each $g \in \mathcal{G}$, there exists an $h \in \mathcal{G}$ such that

$$g * h = h * g = e.$$

If in addition,

- Commutativity : $f * g = g * f\ \forall\ f, g \in \mathcal{G}$,

then $\mathcal{G}$ is called an abelian group.

Elementary Properties

- The identity element e of a group $\mathcal{G}$ is unique.
- The inverse g^{-1} of an element $g \in \mathcal{G}$ is unique.

Examples of Groups

- $(C, +)$: the set C of all complex numbers together with addition operation $+$, where 0 is the identity element, is an abelian group.
- $(C^*, \ \ )$: the set C^* of all non-zero complex numbers together with multiplication operation $\ \ $, where 1 is the identity element, is an abelian group.
- $(M_{n\times n}, +)$: the set $M_{n\times n}$ of all $n \times n$ complex matrices together with matrix addition $+$, where the zero matrix $0_{n\times n}$ is the identity element, is an abelian group.
- $(M^*_{n\times n}, \ \ )$: the set $M^*_{n\times n}$ of all invertible $n \times n$ complex matrices together with matrix multiplication $\ \ $, where the identity matrix $I_{n\times n}$ is the identity element, is a non-abelian group.

The Pauli Group $\mathcal{G}_1$ on the State Space of a Qubit

$$\mathcal{G}_1 = \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}.$$

- $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$
- Hermitian : $X^\dagger = X, Y^\dagger = Y, Z^\dagger = Z.$
- Unitary : $X^2 = Y^2 = Z^2 = I.$
- Anti-commutative : $XY = -YX, YZ = -ZY, ZX = -XZ.$
- $XY = iZ, YZ = iX, ZX = iY.$
- $\mathcal{G}_1$ is non-abelian.

Subgroups of a Group $(\mathcal{G}, *)$

A subset $\mathcal{H}$ of $\mathcal{G}$ is called a subgroup of $\mathcal{G}$, denoted as $\mathcal{H} < \mathcal{G}$, if

- $\mathcal{H}$ is closed under the binary operation $*$, i.e.,

$$f * h \in \mathcal{H}, \ \forall \ f, h \in \mathcal{H};$$

- $\mathcal{H}$ is a group itself under the binary operation $*$.

Examples of Subgroups

- $(R, +) < (C, +)$.
- $(R^*, \ \ ) < (C^*, \ \ )$.
- $(H_{n\times n}, +) < (M_{n\times n}, +)$, where $H_{n\times n}$ is the set of all Hermitian $n \times n$ complex matrices.
- $(U_{n\times n}, \ \ ) < (M^*_{n\times n}, \ \ )$, where $U_{n\times n}$ is the set of all unitary $n \times n$ complex matrices.
- $\mathcal{H} = \{I, X\}$ is a subgroup of the Pauli group $\mathcal{G}_1$ on a qubit.

The Subgroup Generated by a Set

- $(\mathcal{G}, *)$: a group.
- $\mathcal{W}$: a subset of $\mathcal{G}$.
- $\{\mathcal{H}_i, i \in I\}$: the collection of all subgroups of $\mathcal{G}$ which contain $\mathcal{W}$.
- $\langle \mathcal{W} \rangle \stackrel{\triangle}{=} \cap_{i \in I} \mathcal{H}_i$: the subgroup of $\mathcal{G}$ generated by the set $\mathcal{W}$.
- $\langle \mathcal{W} \rangle = \{g_1^{n_1} * g_2^{n_2} * \cdots * g_k^{n_k}, g_i \in \mathcal{W}, n_i \in Z, 1 \leq i \leq k, k \geq 1\}$.
- Elements of $\mathcal{W}$ are called the generators of the subgroup $\langle \mathcal{W} \rangle$.

Examples

- $\langle 1 \rangle = \{\cdots, -2, -1, 0, 1, 2, \cdots\} < (C, +)$.
- $\langle 1 \rangle = \{1\} < (C^*, \ \ )$.
- $\langle X \rangle = \{I, X\} < \mathcal{G}_1$.
- $\langle X, Y \rangle = \{\pm I, \pm X, \pm Y, \pm iZ\} < \mathcal{G}_1$.

$$
\begin{aligned}
& X^{n_1} Y^{n_2} X^{n_3} Y^{n_4} \cdots, n_i \in Z \\
= \ & (XY)^n X, (YX)^n Y, (XY)^n, (YX)^n, n \geq 0, \\
= \ & \pm X, \pm Y, (\pm iZ)^n, n \geq 0, \text{since } XY = iZ,\ YX = -XY, \\
& (XY)^2 = (YX)^2 = -I, XYX = -Y, YXY = -X, \\
= \ & \pm I, \pm X, \pm Y, \pm iZ.
\end{aligned}
$$

- $\langle X, Y, Z \rangle = \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\} = \mathcal{G}_1$.
  - X, Y, Z are generators of the Pauli group $\mathcal{G}_1$.

Independent Generators of a Group

- $\mathcal{H} = \langle g_1, g_2, \ldots, g_k \rangle$.
- $\langle g_1, \ldots, g_{i-1}, g_{i+1}, \ldots, g_k \rangle \neq \mathcal{H}$ for all i, $1 \leq i \leq k$.
- $\{g_1, g_2, \ldots, g_k\}$ is a set of independent generators of $\mathcal{H}$.

The Action of the Pauli Group $\mathcal{G}_n$ on the State Space V of an n-Qubit System

The State Space V of an n-Qubit System

$$V = V_1 \otimes V_2 \otimes \cdots \otimes V_n.$$

- V_i : the state space of the ith qubit, a two-dimensional complex inner product space with a standard basis $\{|0\rangle, |1\rangle\}$.
- V is a 2^n-dimensional complex inner product space with a standard basis $\{|m\rangle, 0 \leq m \leq 2^n - 1\}$.
  - An example : for $n = 4$,

    $$|13\rangle = |1101\rangle = |1\rangle \otimes |1\rangle \otimes |0\rangle \otimes |1\rangle$$

    is a state vector in the standard basis.

The Pauli Group $\mathcal{G}_n$ on the State Space V of n Qubits

- $X_i \stackrel{\triangle}{=} \underbrace{I \otimes \cdots \otimes I}_{i-1} \otimes X \otimes \underbrace{I \otimes \cdots \otimes I}_{n-i}$.
- $Y_i \stackrel{\triangle}{=} \underbrace{I \otimes \cdots \otimes I}_{i-1} \otimes Y \otimes \underbrace{I \otimes \cdots \otimes I}_{n-i}$.
- $Z_i \stackrel{\triangle}{=} \underbrace{I \otimes \cdots \otimes I}_{i-1} \otimes Z \otimes \underbrace{I \otimes \cdots \otimes I}_{n-i}$.
- $\mathcal{G}_n \stackrel{\triangle}{=} \langle X_1, Y_1, Z_1, \ldots, X_n, Y_n, Z_n \rangle$.
- $i^{k_0}(\sigma_{k_1} \otimes \sigma_{k_2} \otimes \cdots \otimes \sigma_{k_n})$: elements in $\mathcal{G}_n$, where $k_0, k_1, \ldots, k_n \in \{0, 1, 2, 3\}$ and $\sigma_0 = I, \sigma_1 = X, \sigma_2 = Y, \sigma_3 = Z$.
- $|\mathcal{G}_n| = 4^{n+1}$.

Properties of $\mathcal{G}_n$

- Two elements g, h in $\mathcal{G}_n$ is either commutative or anti-commutative, i.e., $gh = \pm hg$.
- Each element g in $\mathcal{G}_n$ is unitary, i.e., $gg^\dagger = g^\dagger g = I$.
- Each element g in $\mathcal{G}_n$ has either $g^2 = I$ or $g^2 = -I$ and then either $g^\dagger = g$ or $g^\dagger = -g$.
- The set of eigenvalues of a $g \neq \pm I, \pm iI$ in $\mathcal{G}_n$ is either $\{1, -1\}$ or $\{i, -i\}$.

Proof

Consider two elements g, h in $\mathcal{G}_n$ such that

$$g = i^{k_0}(\sigma_{k_1} \otimes \sigma_{k_2} \otimes \cdots \otimes \sigma_{k_n}), \quad h = i^{m_0}(\sigma_{m_1} \otimes \sigma_{m_2} \otimes \cdots \otimes \sigma_{m_n}).$$

Then we have

$$\begin{aligned} gh &= i^{k_0+m_0}(\sigma_{k_1}\sigma_{m_1} \otimes \sigma_{k_2}\sigma_{m_2} \otimes \cdots \otimes \sigma_{k_n}\sigma_{m_n}) \\ &= (-1)^l i^{k_0+m_0}(\sigma_{m_1}\sigma_{k_1} \otimes \sigma_{m_2}\sigma_{k_2} \otimes \cdots \otimes \sigma_{m_n}\sigma_{k_n}) = \pm hg, \end{aligned}$$

where l is the number of indices i such that $(\sigma_{k_i}, \sigma_{m_i})$ is one of the pairs (X,Y), (Y,X), (Y,Z), (Z,Y), (Z,X), (X,Z). Now $g^\dagger = (-i)^{k_0}(\sigma_{k_1} \otimes \sigma_{k_2} \otimes \cdots \otimes \sigma_{k_n})$ and then $gg^\dagger = g^\dagger g = I$, i.e., g is unitary. Also $g^2 = (-1)^{k_0} I = I$ if $k_0 = 0, 2$ and $-I$ if $k_0 = 1, 3$ and then $g^\dagger = g$ if $k_0 = 0, 2$ and $-g$ if $k_0 = 1, 3$. Thus the minimal polynomial of g is a divisor of $x^2 - 1$ or $x^2 + 1$ and if $g \neq \pm I, \pm iI$, the set of eigenvalues of g is either $\{1, -1\}$ or $\{i, -i\}$. $\square$

Lemma

If $\mathcal{H}$ is a non-abelian subgroup of $\mathcal{G}_n$, then $-I \in \mathcal{H}$.

Proof. Assume that $-I \notin \mathcal{H}$. Then $g^2 = I$ for all $g \in \mathcal{H}$. Suppose there exists h, u in $\mathcal{H}$,

$$h = (-1)^{k_0}(\sigma_{k_1} \otimes \sigma_{k_2} \otimes \cdots \otimes \sigma_{k_n}), \quad u = (-1)^{m_0}(\sigma_{m_1} \otimes \sigma_{m_2} \otimes \cdots \otimes \sigma_{m_n}),$$

such that $hu = -uh$. Then we have

$$\begin{aligned} hu &= (-1)^{k_0+m_0}(\sigma_{k_1}\sigma_{m_1} \otimes \sigma_{k_2}\sigma_{m_2} \otimes \cdots \otimes \sigma_{k_n}\sigma_{m_n}) \\ &= (-1)^{l}(-1)^{m_0+k_0}(\sigma_{m_1}\sigma_{k_1} \otimes \sigma_{m_2}\sigma_{k_2} \otimes \cdots \otimes \sigma_{m_n}\sigma_{k_n}) \\ &= (-1)^{l} uh, \end{aligned}$$

where l is the number of indices i such that $(\sigma_{k_i}, \sigma_{m_i})$ is one of the pairs (X, Y), (Y, X), (Y, Z), (Z, Y), (Z, X), (X, Z). It is clear that l is an odd number. Note that for each i in the l indices in above,

we have $\sigma_{k_i}\sigma_{m_i}$ to be one of $iZ, -iZ, iX, -iX, iY, -iY$, and for other i, we have $\sigma_{k_i}\sigma_{m_i}$ to be one of I, X, Y, Z. Thus we have

$$\begin{aligned}(hu)^2 &= (-1)^{2(k_0+m_0)}((\sigma_{k_1}\sigma_{m_1})^2 \otimes (\sigma_{k_2}\sigma_{m_2})^2 \otimes \cdots \otimes (\sigma_{k_n}\sigma_{m_n})^2) \\ &= (-1)^l(I \otimes I \otimes \cdots \otimes I) = -I \in \mathcal{H},\end{aligned}$$

a contradiction. □

Stabilizers under the Action of $\mathcal{G}_n$ on V

- $\boldsymbol{v}$: a vector in the state space V of n qubits.
- $\mathcal{G}_n(\boldsymbol{v}) = \{g \in \mathcal{G}_n \mid g(\boldsymbol{v}) = \boldsymbol{v}\}$: the stabilizer of $\boldsymbol{v}$ in $\mathcal{G}_n$. Note that $\mathcal{G}_n(\boldsymbol{v}) < \mathcal{G}_n$.
- W' : a set of vectors in V
- $\mathcal{G}_n(W') = \{g \in \mathcal{G}_n \mid g(\boldsymbol{v}) = \boldsymbol{v} \ \forall \ \boldsymbol{v} \in W'\} = \cap_{\boldsymbol{v} \in W'} \mathcal{G}_n(\boldsymbol{v})$: the stabilizer of W' in $\mathcal{G}_n$.
- W : the subspace of V spanned by W'.
- $\mathcal{G}_n(W) = \mathcal{G}_n(W')$: for $g \in \mathcal{G}_n(W')$, we have

$$g(\sum_i \alpha_i \boldsymbol{u}_i) = \sum_i \alpha_i g(\boldsymbol{u}_i) = \sum_i \alpha_i \boldsymbol{u}_i,$$

where $\alpha_i \in C$ and $\boldsymbol{u}_i \in W'$ for all i. Then $g \in \mathcal{G}_n(W)$.

Examples of Stabilizers

- $\mathcal{G}_n(\mathbf{0}) = \mathcal{G}_n$.
- For $n = 2$ and $|\psi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, we have

$$\mathcal{G}_2(|\psi\rangle) = \langle X_1X_2, Z_1Z_2\rangle < \mathcal{G}_2.$$

- For $n = 2$ and $|\psi\rangle = (|01\rangle + |10\rangle)/\sqrt{2}$, we have

$$\mathcal{G}_2(|\psi\rangle) = \langle X_1X_2, -Z_1Z_2\rangle < \mathcal{G}_2.$$

- For $n = 2$ and $|\psi\rangle = (|00\rangle - |11\rangle)/\sqrt{2}$, we have

$$\mathcal{G}_2(|\psi\rangle) = \langle -X_1X_2, Z_1Z_2\rangle < \mathcal{G}_2.$$

- For $n = 2$ and $|\psi\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$, we have

$$\mathcal{G}_2(|\psi\rangle) = \langle -X_1X_2, -Z_1Z_2\rangle < \mathcal{G}_2.$$

Lemma

- W : a subspace of V.
- $\mathcal{S}'$: a subset of $\mathcal{G}_n$.
- $\langle \mathcal{S}' \rangle$: the subgroup of $\mathcal{G}_n$ generated by $\mathcal{S}'$.

$$\mathcal{S}' \subseteq \mathcal{G}_n(W) \Leftrightarrow \langle \mathcal{S}' \rangle < \mathcal{G}_n(W).$$

Proof. For all $\boldsymbol{v} \in W$, we have

$$(g_1^{n_1} g_2^{n_2} \cdots g_k^{n_k})(\boldsymbol{v}) = \boldsymbol{v}$$

for any $g_i \in \mathcal{S}'$, $n_i \in Z$, $1 \leq i \leq k$, and $k \geq 1$. $\square$

Theorem

If W is a non-trivial subspace of V, then the stabilizer $\mathcal{G}_n(W)$ of W in $\mathcal{G}_n$ does not contain $-I$. Thus, $\mathcal{G}_n(W)$ does not contain $\pm iI$ neither and is abelian.

Proof. Since W is non-trivial, there is a non-zero vector $\boldsymbol{v}$ in W. If $-I \in \mathcal{G}_n(W)$, then $(-I)(\boldsymbol{v}) = \boldsymbol{v}$. But $(-I)(\boldsymbol{v}) = -\boldsymbol{v}$ so that $\boldsymbol{v} = -\boldsymbol{v}$ and then $\boldsymbol{v} = \mathbf{0}$, a contradiction. □

Fixed Subspace

- g : an element in $\mathcal{G}_n$.
- $V(g) \stackrel{\triangle}{=} \{\boldsymbol{v} \in V \mid g\boldsymbol{v} = \boldsymbol{v}\}$: the fixed subspace of g in V.
  - If 1 is not an eigenvalue of g, i.e., $g = -I$ or $g^2 = -I$, then $V(g)$ is trivial.
  - If 1 is an eigenvalue of g, i.e., $g \neq -I$ and $g^2 = I$, then $V(g)$ is the eigenspace $E_1(g)$ of g corresponding to eigenvalue 1.
- $\mathcal{S}'$: a subset of $\mathcal{G}_n$.
- $V(\mathcal{S}') \stackrel{\triangle}{=} \{\boldsymbol{v} \in V \mid g\boldsymbol{v} = \boldsymbol{v} \ \forall \ g \in \mathcal{S}'\}$: the fixed subspace of $\mathcal{S}'$ in V.
  - $V(\mathcal{S}') = \cap_{g \in \mathcal{S}'} V(g)$.
  - If 1 is not an eigenvalue of a g in $\mathcal{S}'$, then $V(g)$ is trivial.

- $\mathcal{S} = \langle \mathcal{S}' \rangle$: the subgroup of $\mathcal{G}_n$ generated by $\mathcal{S}'$.
- $V(\mathcal{S}) = V(\mathcal{S}')$: for each $\boldsymbol{v} \in V(\mathcal{S}')$, we have

$$(g_1^{n_1} g_2^{n_2} \cdots g_k^{n_k})(\boldsymbol{v}) = \boldsymbol{v}$$

  for any $g_i \in \mathcal{S}'$, $n_i \in Z$, $1 \leq i \leq k$, and $k \geq 1$. Thus $\boldsymbol{v} \in V(\mathcal{S})$.
- If $-I \in \mathcal{S}$, then $V(\mathcal{S}) = \{\mathbf{0}\}$.
- If $V(\mathcal{S})$ is non-trivial, then $\mathcal{S}$ is an abelian subgroup of $\mathcal{G}_n$ with $-I \notin \mathcal{S}$.

Theorem

If $\mathcal{S} < \mathcal{G}_n$ and $-I \notin \mathcal{S}$, then

- $\mathcal{S}$ is abelian;
- $g^2 = I$ for all $g \in \mathcal{S}$;
- $g^\dagger = g$ for all $g \in \mathcal{S}$;
- the eigenvalues of each $g \neq I$ in $\mathcal{S}$ are 1, -1.

Proof

- If $g^2 = -I$ for some $g \in \mathcal{S}$, then $-I \in \mathcal{S}$, a contradiction. Thus $g^2 = I$ for all $g \in \mathcal{S}$ and since each element in $\mathcal{G}_n$ is unitary, we have $g^\dagger = g$.
- Since $g^2 = I$, the minimal polynomial of g divides $x^2 - 1$. If $g \neq I$, the eigenvalues if g is 1 and -1. $\square$

The Canonical Representation Theorem

If $\mathcal{S} = \langle g_1, g_2, \ldots, g_k \rangle < \mathcal{G}_n$ and $-I \notin \mathcal{S}$, then each g in $\mathcal{S}$ can be represented as

$$g = g_1^{m_1} g_2^{m_2} \cdots g_k^{m_k},$$

where $m_i \in \{0, 1\}$ for all i, and the representation is unique for all $g \in \mathcal{S}$ if and only if g_i's are independent generators of $\mathcal{S}$.

Proof

Since $-I \notin \mathcal{S} = \langle g_1, g_2, \ldots, g_k \rangle$, $\mathcal{S}$ is abelian and $g_i^2 = I$ such that every $g \in \mathcal{S}$ can be represented as

$$g = g_1^{m_1} g_2^{m_2} \cdots g_k^{m_k},$$

where $m_i \in \{0, 1\}$ for all i. Assume that the generators $g_1, g_2, \ldots, g_k$ of $\mathcal{S}$ are not independent. Then there exists an i, $1 \leq i \leq k$, such that $g_i \in \langle g_1, \ldots, g_{i-1}, g_{i+1}, \ldots, g_k \rangle$ and then we have

$$g_i = g_1^{m_1} \cdots g_{i-1}^{m_{i-1}} g_{i+1}^{m_{i+1}} \cdots g_k^{m_k},$$

for $m_i \in \{0, 1\}$, But $g_i = g_i$ and thus g_i has two different representations. Next assume that we have two different representations for an element in $\mathcal{S}$

$$g_1^{l_1} g_2^{l_2} \cdots g_k^{l_k} = g_1^{m_1} g_2^{m_2} \cdots g_k^{m_k}.$$

Let i be the largest index such that $l_i \neq m_i$. Without loss of generality, we assume $l_1 = 1$ and $m_i = 0$. Thus

$$g_i = g_{i-1}^{l_{i-1}} \cdots g_2^{l_2} g_1^{l_1} g_1^{m_1} g_2^{m_2} \cdots g_{i-1}^{m_{i-1}} \in \langle g_1, \ldots, g_{i-1}, g_{i+1}, \ldots, g_k \rangle,$$

which says that the generators $g_1, g_2, \ldots, g_k$ of $\mathcal{S}$ are not independent. $\square$

The Binary Representation Vector $\varphi(g)$ of $g \in \mathcal{G}_n$

- $g = i^{k_0}(\sigma_{k_1} \otimes \sigma_{k_2} \otimes \cdots \otimes \sigma_{k_n})$: an element in the Pauli group $\mathcal{G}_n$, where $k_i \in \{0, 1, 2, 3\}$, $1 \leq i \leq n$.
- $\varphi(g) = (u_1 u_2 \cdots u_n | v_1 v_2 \cdots v_n)$: a binary $2n$-tuple corresponding to g such that (note that $Y = iXZ$)

σ_{k_i}	$\sigma_0 = I$	$\sigma_1 = X$	$\sigma_2 = Y$	$\sigma_3 = Z$
u_i	0	1	1	0
v_i	0	0	1	1

- An example : $g = (-i)I \otimes I \otimes X \otimes X \otimes Y \otimes Y \otimes Z \otimes Z$,

$$\varphi(g) = (00111100|00001111).$$

The Binary Vector Mapping $g \mapsto \varphi(g)$ Is a Group Homomorphism from $\mathcal{G}_n$ into $(F_2^{2n}, +)$

$$\varphi(gh) = \varphi(g) + \varphi(h).$$

	I	X	Y	Z
I	I	X	Y	Z
X	X	I	iZ	$-iY$
Y	Y	$-iZ$	I	iX
Z	Z	iY	$-iX$	I

$\leftrightarrow$

$+$	(00)	(10)	(11)	(01)
(00)	(00)	(10)	(11)	(01)
(10)	(10)	(00)	(01)	(11)
(11)	(11)	(01)	(00)	(10)
(01)	(01)	(11)	(10)	(00)

The Binary Vector Mapping $g \mapsto \varphi(g)$ Is a Group Homomorphism from $\mathcal{G}_n$ into F_2^{2n}

- The mapping $g \mapsto \varphi(g)$ is a group epimorphism from $\mathcal{G}_n$ onto F_2^{2n} with kernel

$$\mathcal{K} = \{I, -I, iI, -iI\}.$$

- $\mathcal{G}_n/\mathcal{K} \cong F_2^{2n}$: a group isomorphism.
- The quotient group $\mathcal{G}_n/\mathcal{K}$ is abelian.
- The coset $\bar{g}$ of g in the quotient group $\mathcal{G}_n/\mathcal{K}$ is

$$\bar{g} = g\mathcal{K} = \{g, -g, ig, -ig\}.$$

The Binary Vector Mapping $g \mapsto \varphi(g)$ Is a Group Homomorphism from $\mathcal{G}_n$ into F_2^{2n}

- If $\mathcal{S} < \mathcal{G}_n$ such that $-I \notin \mathcal{S}$, then $\bar{g}, \bar{h}$ are different cosets in $\mathcal{G}_n/\mathcal{K}$ for any two different elements g, h in $\mathcal{S}$.
- If $\mathcal{S} < \mathcal{G}_n$ such that $-I \notin \mathcal{S}$ and $\mathcal{S}$ has k independent generators $\mathcal{S} = \langle g_1, g_2, \ldots, g_k \rangle$, then there are exactly 2^k subgroups $\mathcal{S}' < \mathcal{G}_n$ with $-I \notin \mathcal{S}'$ such that $\varphi(\mathcal{S}') = \varphi(\mathcal{S})$. In particular, we have $\mathcal{S}' = \langle (-1)^{m_1} g_1, (-1)^{m_2} g_2, \ldots, (-1)^{m_k} g_k \rangle$ with $m_i \in \{0, 1\}\ \forall\ i$.

Proof

- Suppose that $\bar{g} = \bar{h}$ for two different elements g, h in $\mathcal{S}$. Then we must have $h = -g$ since the eigenvalues of g and h are possibly ± 1 and then $hg = -g^2 = -I \in \mathcal{S}$, a contradiction. Let $\overline{\mathcal{S}} = \{\bar{h} | h \in \mathcal{S}\}$. Then we have $|\overline{\mathcal{S}}| = |\mathcal{S}|$, $\overline{\mathcal{S}} < \mathcal{G}_n/\mathcal{K}$ and that $\overline{\mathcal{S}}$ corresponds to $\varphi(\mathcal{S})$ under the binary vector mapping r.
- Let $\mathcal{S}' < \mathcal{G}_n$ with $-I \notin \mathcal{S}'$ such that $\varphi(\mathcal{S}') = \varphi(\mathcal{S})$. Then we have $\overline{\mathcal{S}'} = \overline{\mathcal{S}}$ and there are $m_i \in \{0, 1\}, \forall\ i$, such that $\langle (-1)^{m_1} g_1, (-1)^{m_2} g_2, \ldots, (-1)^{m_k} g_k \rangle < \mathcal{S}'$. If there is an i such that $(-1)^{m_i} g_i \in$ $\langle (-1)^{m_1} g_1, \ldots, (-1)^{m_{i-1}} g_{i-1}, (-1)^{m_{i+1}} g_{i+1}, \ldots, (-1)^{m_k} g_k \rangle$, then either g_i or $-g_i$ is in $\langle g_1, \ldots, g_{i-1}, g_{i+1}, \ldots, g_k \rangle$. The former case contradicts to the independence of the k generators $g_1, g_2, \ldots, g_k$. For the latter case, $(-g_i)g_i = -I \in \mathcal{S}$, a contradiction, too. Thus $(-1)^{m_1} g_1, (-1)^{m_2} g_2, \ldots, (-1)^{m_k} g_k$ are

independent. Since $|\mathcal{S}'| = |\overline{\mathcal{S}'}| = |\overline{\mathcal{S}}| = |\mathcal{S}|$, $\mathcal{S}'$ and $\mathcal{S}$ has the same number, says k, of independent generators. We conclude that $\mathcal{S}' = \langle (-1)^{m_1} g_1, (-1)^{m_2} g_2, \ldots, (-1)^{m_k} g_k \rangle$ and there are exactly 2^k such $\mathcal{S}'$'s. $\square$

Test of Commutativity

- g, h : two elements in $\mathcal{G}_n$.
- $\Lambda = \begin{bmatrix} 0_{n\times n} & I_{n\times n} \\ I_{n\times n} & 0_{n\times n} \end{bmatrix}$: a binary $2n \times 2n$ matrix.
- $gh = hg \Leftrightarrow \varphi(g)\Lambda\varphi(h)^t = 0$.
  - $g = i^{k_0}(\sigma_{k_1} \otimes \sigma_{k_2} \otimes \cdots \otimes \sigma_{k_n}) \leftrightarrow$
    $\varphi(g) = (u_1 u_2 \cdots u_n | v_1 v_2 \cdots v_n)$
  - $h = i^{m_0}(\sigma_{m_1} \otimes \sigma_{m_2} \otimes \cdots \otimes \sigma_{m_n}) \leftrightarrow$
    $\varphi(h) = (u'_1 u'_2 \cdots u'_n | v'_1 v'_2 \cdots v'_n)$
  - $gh = (-1)^l hg$, where l is the number of indices i such that

$$\sigma_{k_i}\sigma_{m_i} \in \{XY, YX, YZ, ZY, ZX, XZ\} \leftrightarrow u_i v'_i + v_i u'_i = 1$$

Test of Independent Generators

- $\mathcal{S} = \langle g_1, g_2, \ldots, g_k \rangle < \mathcal{G}_n$.
- $-I \notin \mathcal{S}$.

$g_1, g_2, \ldots, g_k$ are independent generators of $\mathcal{S} \Longleftrightarrow$

$\varphi(g_1), \varphi(g_2), \ldots, \varphi(g_k)$ are linearly independent vectors in F_2^{2n}.

Proof

"$\Leftarrow$" Suppose there exists an i, $1 \leq i \leq k$, such that $g_i \in \langle g_1, \ldots, g_{i-1}, g_{i+1}, \ldots, g_k \rangle$. Then we have $g_i = g_1^{m_1} \cdots g_{i-1}^{m_{i-1}} g_{i+1}^{m_{i+1}} \cdots g_k^{m_k}$, $m_j \in \{0, 1\}$, by the canonical representation theorem. Thus $\varphi(g_i) = \varphi(g_1^{m_1} \cdots g_{i-1}^{m_{i-1}} g_{i+1}^{m_{i+1}} \cdots g_k^{m_k})$ and $\sum_{i=1}^{k} m_i \varphi(g_i) = 0$ with $m_i = 1$, which implies that $\varphi(g_1), \varphi(g_2), \ldots, \varphi(g_k)$ are linearly dependent binary vectors.

"$\Rightarrow$" Suppose that $\varphi(g_1), \varphi(g_2), \ldots, \varphi(g_k)$ are linearly dependent in F_2^{2n}, i.e., $\sum_{i=1}^{k} m_i \varphi(g_i) = 0$, where $m_i \in \{0, 1\}$ for all i and at least one $m_i \neq 0$, which implies that $\varphi(\Pi_{i=1}^{k} g_i^{m_i}) = \varphi(I)$ and then $\Pi_{i=1}^{k} g_i^{m_i} = i^{m_0} I$. Since $-I \notin \mathcal{S}$, we must have $m_0 = 0$, i.e., $\Pi_{i=1}^{k} g_i^{m_i} = I = \Pi_{i=1}^{k} g_i^0$. By the canonical representations theorem, $g_1, g_2, \ldots, g_k$ are dependent generators of $\mathcal{S}$. $\square$

Remarks

- $-I$ is independent in $\mathcal{G}_n$ but $\varphi(-I) = 0$ is dependent in F_2^{2n}.
- X_1, Y_1, Z_1 are independent in $\mathcal{G}_n$ but $\varphi(X_1) + \varphi(Y_1) + \varphi(Z_1) = 0$.
- If $g_1, g_2, \cdots, g_n \in \mathcal{G}_n$ have $\varphi(g_1), \varphi(g_2), \cdots, \varphi(g_n)$ linearly independent in F_2^{2n}, then they are independent in $\mathcal{G}_n$.

The Check Matrix of a Set of Generators

- $\mathcal{S} = \langle g_1, g_2, \ldots, g_k \rangle < \mathcal{G}_n$.
- The check matrix of a set of generators $g_1, g_2, \ldots, g_k$ of $\mathcal{S}$ is a $k \times 2n$ binary matrix

$$H \stackrel{\triangle}{=} \begin{bmatrix} \varphi(g_1) \\ \varphi(g_2) \\ \vdots \\ \varphi(g_k) \end{bmatrix}.$$

An Example

$$g_1 = IIIXXX, \quad g_2 = IXIXIX, \quad g_3 = ZIZIZI,$$
$$g_4 = YYYIII, \quad g_5 = XYXYXY, \quad g_6 = YZYZYZ.$$

$$\left[\begin{array}{cccccc|cccccc} 0&0&0&1&1&1&0&0&0&0&0&0 \\ 0&1&0&1&0&1&0&0&0&0&0&0 \\ 0&0&0&0&0&0&1&0&1&0&1&0 \\ 1&1&1&0&0&0&1&1&1&0&0&0 \\ 1&1&1&1&1&1&0&1&0&1&0&1 \\ 1&0&1&0&1&0&1&1&1&1&1&1 \end{array}\right].$$

Maximum Rank of Check Matrices of Abelian Pauli Subgroups

- $\mathcal{S} = \langle g_1, g_2, \ldots, g_k \rangle < \mathcal{G}_n$.
- H: the $k \times 2n$ check matrix of $\mathcal{S}$.

If $\mathcal{S}$ is abelian, then $\mathrm{Rank}(H) \leq n$.

Proof. Let $\mathrm{Row}(A)$ be the row space of a matrix A. Since $\mathcal{S}$ is abelian,

$$
\begin{aligned}
& H\Lambda H^T = H(H\Lambda)^T = 0 \\
\Rightarrow\ & \mathrm{Row}(H\Lambda) \subseteq (\mathrm{Row}(H))^{\perp} \\
\Rightarrow\ & \dim(\mathrm{Row}(H\Lambda)) \leq \dim(\mathrm{Row}(H)^{\perp}) \\
\Rightarrow\ & \mathrm{Rank}(H) \leq 2n - \mathrm{Rank}(H), \quad \text{since } \Lambda \text{ is non-singular,} \\
\Rightarrow\ & \mathrm{Rank}(H) \leq n,
\end{aligned}
$$

which completes the proof. □

A Technical Lemma

- $\mathcal{S} = \langle g_1, g_2, \ldots, g_k \rangle < \mathcal{G}_n$: $g_1, g_2, \ldots, g_k$ are independent generators.
- $-I \notin \mathcal{S}$.

For each generator g_i, $1 \leq i \leq k$, there exists an $h_i \in \mathcal{G}_n$ such that

$$h_i g_i h_i^\dagger = -g_i \quad \text{and} \quad h_i g_j h_i^\dagger = g_j, \ \forall\ j \neq i,$$

$$(h_i g_i = -g_i h_i \quad \text{and} \quad h_i g_j = g_j h_i, \ \forall\ j \neq i.)$$

Proof

Let A be the $k \times 2n$ check matrix of the independent generators $g_1, g_2, \ldots, g_k$ of $\mathcal{S}$. Since A has k linearly independent rows, the binary matrix $A\Lambda$ has a right inverse, says a $2n \times k$ binary matrix $B = [\boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_k]$, such that $A\Lambda B = I_{k\times k}$. For each i, $1 \leq i \leq k$, select an h_i in $\mathcal{G}_n$ such that $\varphi(h_i) = \boldsymbol{y}_i^t$. It is clear that $\varphi(g_i)\Lambda\varphi(h_j)^t = \delta_{ij}$, $1 \leq i, j \leq k$, which implies that $h_j g_i = (-1)^{\delta_{ij}} g_i h_j$. □

Remark

The above technical lemma is also true if $g_1, g_2, \ldots, g_k$ in $\mathcal{G}_n$ have linearly independent $\varphi(g_1), \varphi(g_2), \ldots, \varphi(g_k)$ in F_2^{2n} even g_i's may not commute with each other.

Lemma

Let P_1 and P_2 be two projectors from a complex inner product space W onto the subspaces W_1 and W_2 of W, respectively. Then P_1 and P_2 commute if and only if P_1P_2 is a projector. In this case, P_1P_2 is the projector onto $W_1 \cap W_2$.

Proof. If P_1 and P_2 commute, then we have

$$\begin{aligned} (P_1P_2)^2 &= P_1P_2P_1P_2 = P_1^2P_2^2 = P_1P_2, \\ (P_1P_2)^\dagger &= P_2^\dagger P_1^\dagger = P_2P_1 = P_1P_2. \end{aligned}$$

Thus P_1P_2 is a projector from W onto $(P_1P_2)(W)$. Conversely, if P_1P_2 is a projector, then $P_1P_2 = (P_1P_2)^\dagger = P_2^\dagger P_1^\dagger = P_2P_1$. Note that $(W_1 \cap W_2) \subseteq (P_1P_2)(W)$ since $(P_1P_2)(W_1 \cap W_2) = W_1 \cap W_2$. Also $(P_1P_2)(W) = (P_2P_1)(W)$ implies $(P_1P_2)(W) \subseteq (W_1 \cap W_2)$. We conclude that $(P_1P_2)(W) = W_1 \cap W_2$. □

Remark

Since projectors are normal operators, two projectors P_1 and P_2 on a complex inner product space W commutes if and only if they can be unitarily diagonalized simultaneously, i.e., there exists a common orthonormal eigenbasis for P_1 and P_2.

Dimension Theorem

Let $\mathcal{S} < \mathcal{G}_n$ with $-I \notin \mathcal{S}$. If $\mathcal{S}$ is generated by $n-k$ independent generators, then $V(\mathcal{S})$ is a 2^k-dimensional complex vector space.

Proof

Let $\mathcal{S}$ be generated by $n-k$ independent generators $g_1, g_2, \ldots, g_{n-k}$ such that $V(\mathcal{S}) = \cap_{j=1}^{n-k} V(g_j)$. Since $-I \notin \mathcal{S}$, the eigenvalues of each g_i are 1 and -1 with corresponding eigenspaces $E_1(g_j) = V(g_j)$ and $E_{-1}(g_j)$, respectively. For $x_j \in \{0,1\}$, $(I + (-1)^{x_j} g_j)/2$ is the projector from V onto $E_{(-1)^{x_j}}(g_j)$. Now for each binary $(n-k)$-tuple $\boldsymbol{x} = (x_1, x_2, \ldots, x_{n-k})$, we let

$$P_{\boldsymbol{x}} = \frac{\Pi_{j=1}^{n-k}(I + (-1)^{x_j} g_j)}{2^{n-k}}.$$

Since $\mathcal{S}$ is abelian, $P_{\boldsymbol{x}}$ is the projector form V onto $\cap_{j=1}^{n-k} E_{(-1)^{x_j}}(g_j)$ by the previous lemma. In particular, $P_{\mathbf{0}}(V) = \cap_{j=1}^{n-k} E_1(g_j) = V(\mathcal{S})$. It is apparently that $P_{\boldsymbol{x}}(V)$'s are orthogonal. Let h_i in $\mathcal{G}_n$, $1 \le i \le n-k$, be in the technical lemma such that $h_i g_j = (-1)^{\delta_{ij}} g_j h_i$. And for each binary $(n-k)$-tuple $\boldsymbol{x}$,

let $h_{\boldsymbol{x}} = \Pi_{i=1}^{n-k} h_i^{x_i}$. We have

$$h_{\boldsymbol{x}} g_j = (\Pi_{i=1}^{n-k} h_i^{x_i}) g_j = (-1)^{x_j} g_j (\Pi_{i=1}^{n-k} h_i^{x_i}) = (-1)^{x_j} g_j h_{\boldsymbol{x}}.$$

Since $h_{\boldsymbol{x}}$ is unitary, we have $h_{\boldsymbol{x}} g_j h_{\boldsymbol{x}}^\dagger = (-1)^{x_j} g_j$, which implies $(I + (-1)^{x_j} g_j)/2 = h_{\boldsymbol{x}}(I + g_j)/2 h_{\boldsymbol{x}}^\dagger$ and

$$P_{\boldsymbol{x}} = h_{\boldsymbol{x}} P_{\boldsymbol{0}} h_{\boldsymbol{x}}^\dagger.$$

Thus $P_{\boldsymbol{x}}(V)$ and $P_{\boldsymbol{0}}(V)$ have the same dimension. Finally,

$$\sum_{\boldsymbol{x}} P_{\boldsymbol{x}} = \Pi_{j=1}^{n-k} \frac{(I + g_j) + (I - g_j)}{2} = I,$$

which implies that $V = \sum_{\boldsymbol{x}} P_{\boldsymbol{x}}(V)$ is a sum of 2^{n-k} orthogonal subspaces of the same dimension. Thus the dimension of $V(\mathcal{S}) = P_{\boldsymbol{0}}(V)$ is 2^k. □

Corollaries

- If W is a subspace of V, then

$$W \subseteq V(\mathcal{G}_n(W)).$$

Proof. Assume $W = \mathrm{Span}(W')$, where W' is a basis of W. Then $\mathcal{G}_n(W) = \mathcal{G}_n(W')$ and $V(\mathcal{G}_n(W)) = V(\mathcal{G}_n(W')) = V(\cap_{\boldsymbol{v}' \in W'} \mathcal{G}_n(\boldsymbol{v}'))$, i.e., $V(\mathcal{G}_n(W)) = \{\boldsymbol{v} \in V \mid g\boldsymbol{v} = \boldsymbol{v} \ \forall\ g \in \cap_{\boldsymbol{v}' \in W'} \mathcal{G}_n(\boldsymbol{v}')\}$, which contains all vectors w' in W'. Thus $W \subseteq V(\mathcal{G}_n(W))$. □

- If $\mathcal{S} < \mathcal{G}_n$ with $-I \notin \mathcal{S}$, then

$$\mathcal{S} = \mathcal{G}_n(V(\mathcal{S})).$$

Proof. Assume $\mathcal{S}$ is generated by $\mathcal{S}'$, a set of $n-k$ independent generators. Then $\dim V(\mathcal{S}) = \dim V(\mathcal{S}') = 2^k$ by the dimension

theorem. And $\mathcal{G}_n(V(\mathcal{S})) = \mathcal{G}_n(V(\mathcal{S}')) = \mathcal{G}_n(\cap_{g' \in \mathcal{S}'} V(g'))$, i.e.,

$$\mathcal{G}_n(V(\mathcal{S})) = \{g \in \mathcal{G}_n \mid g\boldsymbol{v} = \boldsymbol{v} \ \forall \ v \in \cap_{g' \in \mathcal{S}'} V(g')\},$$

which contains all elements g' in $\mathcal{S}'$. Thus $\mathcal{S} \subseteq \mathcal{G}_n(V(\mathcal{S}))$. Now suppose $\mathcal{S} \subsetneqq \mathcal{G}_n(V(\mathcal{S}))$ so that $\mathcal{G}_n(V(\mathcal{S}))$ has $n - k + m$ independent generators, $m \geq 1$. Since

$$V(\mathcal{S}) \subseteq V(\mathcal{G}_n(V(\mathcal{S}))),$$

we have

$$\dim(V(\mathcal{S})) = 2^k \leq \dim(V(\mathcal{G}_n(V(\mathcal{S}))) = 2^{k-m},$$

a contradiction. We conclude that $\mathcal{S} = \mathcal{G}_n(V(\mathcal{S}))$. $\square$

Remark

- Let $W \subseteq V$ be a non-trivial subspace of V. Then $W = V(\mathcal{G}_n(W))$ if and only if W is the fixed subspace of a certain $\mathcal{S} < \mathcal{G}_n$ with $-I \notin \mathcal{S}$.

  Proof. ($\Rightarrow$) Notice that $\mathcal{G}_n(W) < \mathcal{G}_n$ and $-I \notin \mathcal{G}_n(W)$. By letting $\mathcal{S} = \mathcal{G}_n(W)$, we have $V(\mathcal{S}) = V(\mathcal{G}_n(W)) = W$.
  ($\Leftarrow$) We have $W = V(\mathcal{S})$. Since $\mathcal{S} = \mathcal{G}_n(V(\mathcal{S}))$, $\mathcal{G}_n(W) = \mathcal{S}$. So $V(\mathcal{G}_n(W)) = V(\mathcal{S}) = W$. □

- $\mathcal{S} < \mathcal{G}_n$ is a stabilizer group if and only if $-I \notin \mathcal{S}$.

  Proof. $\mathcal{S}$ is a stabilizer group if and only if $V(\mathcal{S})$ is nontrivial if and only if $\mathcal{G}_n(V(\mathcal{S})) = \mathcal{S}$ does not contain $-I$. □

Unitary Operators

- u : a unitary operator on the state space V of n qubits.
- g : an element in $\mathcal{G}_n$.
- $V(g)$: the fixed subspace of g in V.
- $u(V(g)) = V(ugu^\dagger)$: the fixed subspace of $ugu^\dagger$ in V.
  - $\boldsymbol{v} \in V(ugu^\dagger) \Leftrightarrow (ugu^\dagger)(\boldsymbol{v}) = \boldsymbol{v} \Leftrightarrow g(u^\dagger(\boldsymbol{v})) = u^\dagger(\boldsymbol{v}) \Leftrightarrow u^\dagger(\boldsymbol{v}) \in V(g) \Leftrightarrow \boldsymbol{v} \in u(V(g))$.
- $\mathcal{S} < \mathcal{G}_n$: a subgroup of $\mathcal{G}_n$.
- $V(\mathcal{S})$: the fixed subspace of $\mathcal{S}$ in V.
- $u(V(\mathcal{S})) = V(u\mathcal{S}u^\dagger)$: the fixed subspace of $u\mathcal{S}u^\dagger$ in V.

Stabilizer Codes

- $\mathcal{S} = \langle g_1, g_2, \ldots, g_{n-k} \rangle < \mathcal{G}_n$: an abelian subgroup of $\mathcal{G}_n$ with $-I \notin \mathcal{S}$ which is generated by $n-k$ independent generators.
- $\mathcal{C}(\mathcal{S})$: an $[n, k]$ stabilizer code which is just the fixed subspace of $\mathcal{S}$ in the state space V of n qubits.

Centralizer and Normalizer

- $\mathcal{S} < \mathcal{G}_n$.
- $C_{\mathcal{G}_n}(\mathcal{S}) \stackrel{\triangle}{=} \{g \in \mathcal{G}_n \mid ghg^\dagger = h \ \forall \ h \in \mathcal{S}\}$: the centralizer of $\mathcal{S}$ in $\mathcal{G}_n$.
  - If $\mathcal{S} = \langle g_1, g_2, \ldots, g_{n-k} \rangle$, then $g \in C_{\mathcal{G}_n}(\mathcal{S}) \Leftrightarrow gg_i = g_i g$ for all i.
- $N_{\mathcal{G}_n}(\mathcal{S}) \stackrel{\triangle}{=} \{g \in \mathcal{G}_n \mid ghg^\dagger \in \mathcal{S} \ \forall \ h \in \mathcal{S}\}$: the normalizer of $\mathcal{S}$ in $\mathcal{G}_n$.
  - If $\mathcal{S} = \langle g_1, g_2, \ldots, g_{n-k} \rangle$, then $g \in N_{\mathcal{G}_n}(\mathcal{S}) \Leftrightarrow gg_i g^\dagger \in \mathcal{S}$ for all i.
- $\mathcal{S} \lhd N_{\mathcal{G}_n}(\mathcal{S})$ and $N_{\mathcal{G}_n}(\mathcal{S})$ is the largest subgroup of $\mathcal{G}_n$ which contains $\mathcal{S}$ as a normal group.
- $\mathcal{S} \lhd \mathcal{G}_n$ if and only if $N_{\mathcal{G}_n}(\mathcal{S}) = \mathcal{G}_n$.

- $C_{\mathcal{G}_n}(\mathcal{S}) < N_{\mathcal{G}_n}(\mathcal{S})$.
  - If $-I \notin \mathcal{S}$, then $C_{\mathcal{G}_n}(\mathcal{S}) = N_{\mathcal{G}_n}(\mathcal{S})$.

    Proof.

    Let $g \in N_{\mathcal{G}_n}(\mathcal{S})$. Suppose that

    $$gg_i = -g_i g$$

    for some i, where $\mathcal{S} = \langle g_1, g_2, \ldots, g_{n-k} \rangle$. Then

    $$gg_i g^\dagger = -g_i g g^\dagger = -g_i \in \mathcal{S}$$

    so that $g_i(-g_i) = -I \in \mathcal{S}$, a contradiction. $\square$

Error-Correction Conditions for Stabilizer Codes

If

- $\mathcal{S}$: an abelian subgroup of $\mathcal{G}_n$ with $-I \notin \mathcal{S}$,
- $\mathcal{C}(\mathcal{S})$: the stabilizer code fixed by $\mathcal{S}$,
- $\{E_i\}$: a set of operation elements (error patterns) in $\mathcal{G}_n$ such that $E_i^\dagger E_j \notin N_{\mathcal{G}_n}(\mathcal{S}) \backslash \mathcal{S}$ for all i, j,

then $\{E_i\}$ are correctable error patterns by the code $\mathcal{C}(\mathcal{S})$.

Proof

- $\mathcal{S} = \langle g_1, g_2, \ldots, g_{n-k} \rangle$: $g_1, g_2, \ldots, g_{n-k}$ are generators of $\mathcal{S}$.
- $P = \Pi_{i=1}^{n-k}(I + g_i)/2^{n-k}$: the projector from V onto the code space $\mathcal{C}(\mathcal{S})$.
- Two possibilities : either $E_i^\dagger E_j \in \mathcal{S}$ or $E_i^\dagger E_j \in \mathcal{G}_n \backslash N_{\mathcal{G}_n}(\mathcal{S})$.
- Case I : $E_i^\dagger E_j \in \mathcal{S}$.
  - $\mathcal{C}(\mathcal{S}) \subseteq V(E_i^\dagger E_j)$: $V(E_i^\dagger E_j)$ is the fixed subspace of $E_i^\dagger E_j$ in V.
  - $\mathcal{C}(\mathcal{S})^\perp$: the orthogonal complement of $\mathcal{C}(\mathcal{S})$ in V.
  - $\boldsymbol{v} = \boldsymbol{u} + \boldsymbol{u}^\perp$ in V : orthogonal decomposition of $\boldsymbol{v}$ with $\boldsymbol{u} \in \mathcal{C}(\mathcal{S})$ and $\boldsymbol{u}^\perp \in \mathcal{C}(\mathcal{S})^\perp$.
  - $E_i^\dagger E_j P(\boldsymbol{v}) = (E_i^\dagger E_j)(\boldsymbol{u}) = \boldsymbol{u} = P(\boldsymbol{v})$ for all $\boldsymbol{v}$ in V, which implies $E_i^\dagger E_j P = P$.

- $PE_i^\dagger E_j P = P^2 = P$ and then $PE_j^\dagger E_i P = P$.

- Case II : $E_i^\dagger E_j \in \mathcal{G}_n \backslash N_{\mathcal{G}_n}(\mathcal{S})$.
  - $E_i^\dagger E_j$ must anti-commute with some generator of $\mathcal{S}$, says g_1 without loss of generality.
  - $E_i^\dagger E_j P = E_i^\dagger E_j \Pi_{i=1}^{n-k}(I + g_i)/2^{n-k} =$ $(I - g_i)E_i^\dagger E_j \Pi_{i=2}^{n-k}(I + g_i)/2^{n-k}$.
  - $P(I - g_1) = 0$ since $(I + g_1)(I - g_1) = 0$.
  - $PE_i^\dagger E_j P = 0$ and then $PE_j^\dagger E_i P = 0$.

- $PE_i^\dagger E_j P = \alpha_{ij} P$ with $\alpha = [\alpha_{ij}]$ a Hermitian matrix.

- Conclusion : $\{E_i\}$ is a set of correctable error patterns by the stabilizer code $\mathcal{C}(\mathcal{S})$. $\square$

Syndrome Measurements and Syndromes

- $\mathcal{S} = \langle g_1, g_2, \ldots, g_{n-k} \rangle$: an abelian subgroup of $\mathcal{G}_n$ with $-I \notin \mathcal{S}$.
- $\mathcal{C}(\mathcal{S})$: the stabilizer code fixed by $\mathcal{S}$.
- $\{E_i\}$: a set of correctable error patterns in $\mathcal{G}_n$ by $\mathcal{C}(\mathcal{S})$ such that $E_i^\dagger E_j \notin N_{\mathcal{G}_n}(\mathcal{S}) \backslash \mathcal{S}$ for all i, j.
- $g_j^\dagger = g_j$ and $g_j = (I + g_j)/2 - (I - g_j)/2$: g_j can be regarded as a projective measurement $\{(I + g_j)/2, (I - g_j)/2\}$.
- Two possibilities : $E_i g_j = g_j E_i$, i.e., $E_i g_j E_i^\dagger = g_j$ or $E_i g_j = -g_j E_i$, i.e., $E_i g_j E_i^\dagger = -g_j$.
  - Case I : $E_i g_j = g_j E_i$. For each $|\psi\rangle \in \mathcal{C}(\mathcal{S})$,

$$(I + g_j)/2 E_i(|\psi\rangle) = E_i (I + g_j)/2 (|\psi\rangle) = E_i(|\psi\rangle).$$

The measurement of g_j on the (un-normalized) possibly

corrupted state $E_i(|\psi\rangle)$ is +1 with probability one. And the post-measurement state remains unchanged.

– Case I : $E_i g_j = -g_j E_i$. For each $|\psi\rangle \in \mathcal{C}(\mathcal{S})$,

$$(I - g_j)/2 E_i(|\psi\rangle) = E_i(I + g_j)/2(|\psi\rangle) = E_i(|\psi\rangle).$$

The measurement of g_j on the (un-normalized) possibly corrupted state $E_i(|\psi\rangle)$ is -1 with probability one. And the post-measurement state remains unchanged.

- $g_1, g_2, \ldots, g_{n-k}$: $n-k$ syndrome measurements
- $\boldsymbol{\beta}_i = (\beta_{i1}, \beta_{i2}, \ldots, \beta_{i(n-k)})$: syndrome vector of the error pattern E_i, where

$$E_i g_j E_i^\dagger = \beta_{ij} g_j.$$

Error Detection

If the syndrome vector $\boldsymbol{\beta}$ is not equal to $(1, 1, \ldots, 1)$, then the channel output is a corrupted state and error is detected.

Error Correction

- If there is only one error pattern E_i associated with the syndrome vector $\boldsymbol{\beta}$, then apply $E_i^\dagger$ to any of the syndrome measurement output to recover the channel input state.
- If there are two error patterns E_i and $E_{i'}$ associated with the syndrome vector $\boldsymbol{\beta}$, then $E_i g_j E_i^\dagger = E_{i'} g_j E_{i'}^\dagger$ for all j and then $(E_{i'}^\dagger E_i) g_j = g_j (E_{i'}^\dagger E_i)$ for all j. Thus $E_{i'}^\dagger E_i$ is in $C_{\mathcal{G}_n}(\mathcal{S}) = N_{\mathcal{G}_n}(\mathcal{S})$. But $E_{i'}^\dagger E_i \notin N_{\mathcal{G}_n}(\mathcal{S}) \backslash \mathcal{S}$, we have $E_{i'}^\dagger E_i \in \mathcal{S}$. Thus we can apply $E_i^\dagger$ or $E_{i'}^\dagger$ to any of the syndrome measurement output to recover the channel input state.

Minimum Distance of a Stabilizer Code

- $E = i^{k_0}(\sigma_{k_1} \otimes \sigma_{k_2} \otimes \cdots \otimes \sigma_{k_n})$: an error pattern in $\mathcal{G}_n$.
- $w(E)$: the number of non-identity terms σ_{k_i} in the tensor product representation of E.
- $\mathcal{S}$: an abelian subgroup of $\mathcal{G}_n$ with $-I \notin \mathcal{S}$.
- $\mathcal{C}(\mathcal{S})$: the stabilizer code fixed by $\mathcal{S}$.
- $d = \min\{w(E) \mid E \in N_{\mathcal{G}_n}(\mathcal{S}) \backslash \mathcal{S}\}$: the minimum distance of the stabilizer code $\mathcal{C}(\mathcal{S})$.
- Let $d \geq 2t + 1$. Then all E in $\mathcal{G}_n$ with $w(E) \leq t$ are correctable error patterns since

$$w(E_i^\dagger E_j) \leq w(E_i) + w(E_j) \leq 2t$$

for any E_i, E_j in $\mathcal{G}_n$ with $w(E_i) \leq t$ and $w(E_j) \leq t$ and then $E_i^\dagger E_j \notin N_{\mathcal{G}_n}(\mathcal{S}) \backslash \mathcal{S}$.