# IQC Note for April 16

Yuantian Ding

April, 2024

## 1 Pauli Group $G_1$

To reduce Pauli stabilizer codes to classical representation, we are interested in the commutation of Pauli operators. Here we use $[g,h] = ghg^{-1}h^{-1}$ to denote the commutator in group-theoretic sense. So, the commutator of Pauli operators are,

$$\begin{gathered}[X,Y] = XYX^{-1}Y^{-1} = XYXY = -I \\ [X,Z] = [Y,Z] = -I\end{gathered}$$

Using this notion of commutator, Pauli group $G_1$ of one qubit $G_1 = \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}$ can be decomposed into two subgroups:

- The *center* (i.e. the subset of elements that commute with every other element) of $G_1$, $C(G_1) = \{\pm I, \pm iI\}$. This subgroup is isomorphic to $\mathbb{Z}/4\mathbb{Z}$.
- The quotient group $G_1/\{\pm 1, \pm i\}$. This subgroup is isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

In the following sections, we use $\mathbb{F}_2$ to denote $\mathbb{Z}/2\mathbb{Z}$ for convenience.

## 2 Reduce Pauli Group $G_n$ to Symplectic Vector Space

We already have a good idea about $G_1$. Now we will use *symplectic vector space* to investigate $G_n$. First, let's define a notation that encode a sequence of Pauli operators as a vector of $\mathbb{F}_2$,

$$\begin{aligned} X(\vec{x}) &= \prod_{i=1}^{n} X_i^{\vec{x}(i)} \quad \text{for any } \vec{x} \in \mathbb{F}_2^n \\ Z(\vec{z}) &= \prod_{i=1}^{n} Z_i^{\vec{z}(i)} \quad \text{for any } \vec{z} \in \mathbb{F}_2^n \end{aligned}$$

For example, $X(1,0,1) = X \otimes I \otimes X$. Using this notation, $G_n$ can be written as,

$$G_n = \left\{ \eta X(\vec{x}) Z(\vec{z}) \,\middle|\, \vec{x}, \vec{z} \in \mathbb{F}_2^n, \eta \in \{\pm 1, \pm i\} \right\}$$

Here are some simple observations of $X(\vec{x})$ and $Z(\vec{z})$.

$$\begin{matrix} X(\vec{x})^{-1} = X(\vec{x}) & Z(\vec{x})^{-1} = Z(\vec{x}) \\ X(\vec{x}_1)X(\vec{x}_2) = X(\vec{x}_1 + \vec{x}_2) & Z(\vec{x}_1)Z(\vec{x}_2) = Z(\vec{x}_1 + \vec{x}_2) \end{matrix}$$

$$\begin{aligned} Z(\vec{z})X(\vec{x}) &= \Big(\prod_{i=1}^{n} Z_i^{\vec{z}(i)}\Big)\Big(\prod_{i=1}^{n} X_i^{\vec{x}(i)}\Big) \\ &= Z^{\vec{z}(1)}X^{\vec{x}(1)} \otimes \cdots \otimes Z^{\vec{z}(n)}X^{\vec{x}(n)} \\ &= (-1)^{\vec{z}(1)\vec{x}(1)} X^{\vec{x}(1)}Z^{\vec{z}(1)} \otimes \cdots \otimes (-1)^{\vec{z}(n)\vec{x}(n)} X^{\vec{x}(n)}Z^{\vec{z}(n)} \\ &= (-1)^{\vec{z}\cdot\vec{x}} (X^{\vec{x}(1)}Z^{\vec{z}(1)} \otimes \cdots \otimes X^{\vec{x}(n)}Z^{\vec{z}(n)}) \\ &= (-1)^{\vec{z}\cdot\vec{x}} X(\vec{x})Z(\vec{z}) \end{aligned} \tag{1}$$

Then we define symplectic product as a operator on symplectic vector space $\mathbb{F}_2^n \oplus \mathbb{F}_2^n$.

**Definition 1** (Symplectic Product on $\mathbb{F}_2^n \oplus \mathbb{F}_2^n$)**.** *Symplectic product* is an operator $\omega$ takes two $\mathbb{F}_2^n \oplus \mathbb{F}_2^n$ and returns a single $F_2$, which

$$\begin{aligned} \omega : \quad (\mathbb{F}_2^n \oplus \mathbb{F}_2^n) \times \mathbb{F}_2^n \oplus \mathbb{F}_2^n &\mapsto \mathbb{F}_2 \\ \big((\vec{x}_1, \vec{z}_1), (\vec{x}_2, \vec{z}_2)\big) &\mapsto \vec{x}_1 \cdot \vec{z}_2 + \vec{x}_2 \cdot \vec{z}_1 \end{aligned}$$

Now we are ready to introduce a homomorphism from Pauli group $G_n$ to symplectic vector space $\mathbb{F}_2^n \oplus \mathbb{F}_2^n$.

**Lemma 1** (Homomorphism from Pauli Group to $\mathbb{F}_2^n \oplus \mathbb{F}_2^n$)**.** There exists a surjective group homomorphism $\pi$, that maps elements in Pauli group $G_n$ to $\mathbb{F}_2^n \oplus \mathbb{F}_2^n$

$$\begin{array}{rccc} \pi: & G_n & \mapsto & \mathbb{F}_2^n \oplus \mathbb{F}_2^n \\ & \eta X(\vec{x})Z(\vec{x}) & \mapsto & (\vec{x}, \vec{z}) \end{array}$$

*Proof.* Once we multiply two elements in $G_n$, we have,

$$\begin{aligned} & \eta_1 X(\vec{x}_1)Z(\vec{z}_1)\eta_2 X(\vec{x}_2)Z(\vec{z}_2) \\ = & \eta_1\eta_2 X(\vec{x}_1)Z(\vec{z}_1)X(\vec{x}_2)Z(\vec{z}_2) \\ = & \eta_1\eta_2(-1)^{\vec{z}_1\cdot\vec{x}_2} X(\vec{x}_1)X(\vec{x}_2)Z(\vec{z}_1)Z(\vec{z}_2) \\ = & \eta_1\eta_2(-1)^{\vec{z}_1\cdot\vec{x}_2} X(\vec{x}_1+\vec{x}_2)Z(\vec{z}_1+\vec{z}_2) \end{aligned}$$

Thus, $\pi(\eta_1 X(\vec{x}_1)Z(\vec{z}_1)\ \eta_2 X(\vec{x}_2)Z(\vec{z}_2)) = \pi(\eta_1 X(\vec{x}_1)Z(\vec{z}_1)) + \pi(\eta_2 X(\vec{x}_2)Z(\vec{z}_2))$. □

**Lemma 2.** $\eta_1 X(\vec{x}_1)Z(\vec{z}_1)$ and $\eta_2 X(\vec{x}_2)Z(\vec{z}_2)$ commute iff $\omega\big((\vec{x}_1,\vec{z}_1),(\vec{x}_2,\vec{z}_2)\big) = 0$.

*Proof.* Using (1) to exchange $X$ and $Z$,

$$\begin{aligned} & \eta_1 X(\vec{x}_1)Z(\vec{z}_1)\eta_2 X(\vec{x}_2)Z(\vec{z}_2) \\ = & \eta_1\eta_2 X(\vec{x}_1)Z(\vec{z}_1)X(\vec{x}_2)Z(\vec{z}_2) \\ = & \eta_1\eta_2(-1)^{\vec{z}_1\cdot\vec{x}_2} X(\vec{x}_1)X(\vec{x}_2)Z(\vec{z}_1)Z(\vec{z}_2) \\ = & \eta_1\eta_2(-1)^{\vec{z}_1\cdot\vec{x}_2} X(\vec{x}_2)X(\vec{x}_1)Z(\vec{z}_2)Z(\vec{z}_1) \\ = & \eta_1\eta_2(-1)^{\vec{z}_1\cdot\vec{x}_2}(-1)^{\vec{x}_1\cdot\vec{z}_2} X(\vec{x}_2)Z(\vec{z}_2)X(\vec{x}_1)Z(\vec{z}_1) \\ = & (-1)^{\omega((\vec{x}_1,\vec{z}_1),(\vec{x}_2,\vec{z}_2))}\eta_2 X(\vec{x}_2)Z(\vec{z}_2)\eta_1 X(\vec{x}_1)Z(\vec{z}_1) \end{aligned}$$

Thus

$$\big[\eta_1 X(\vec{x}_1)Z(\vec{z}_1), \eta_2 X(\vec{x}_2)Z(\vec{z}_2)\big] = (-1)^{\omega((\vec{x}_1,\vec{z}_1),(\vec{x}_2,\vec{z}_2))} I$$

Then $\eta_1 X(\vec{x}_1)Z(\vec{z}_1)$ and $\eta_2 X(\vec{x}_2)Z(\vec{z}_2)$ commute if and only if $\omega\big((\vec{x}_1,\vec{z}_1),(\vec{x}_2,\vec{z}_2)\big) = 0$. □

# 3 Subspaces generated by Pauli Stabilizer

Now we discuss subspaces generated by a set of Pauli stabilizer: $S \subseteq G_n$.

**Lemma 3.** If $\langle S\rangle$ generates a nonabelian group, then $-I \in \langle S\rangle$.

*Proof.* On one hand, if $\langle S\rangle$ is nonabelian, exists $g, h \in \langle S\rangle$ such that, $[g,h] \neq I$. On the other hand, as we know from Lemma 2, $[g,h] = \pm I$. Thus we get $[g,h] = -I$. And because $[g,h] \in \langle S\rangle$, we know $-I \in \langle S\rangle$. □

**Lemma 4.** If $\langle S\rangle$ generates an abelian group and $-I \notin \langle S\rangle$, then for any $g \in \langle S\rangle$, $g^2 = I$, and in particular, $\eta(g) = \pm 1$ where $g = \eta(g)X(\vec{x}_g)Z(\vec{z}_g)$.

*Proof.* If $\langle S\rangle$ is abelian, then, $g^2 = \eta(g)^2 X(2\vec{x}_g)Z(2\vec{z}_g) = \eta(g)^2$. And because $-I \notin \langle S\rangle$, $g^2 \neq -I$, which means $\eta(g) \neq \pm i$. Then $\eta(g) = \pm 1$. □

Before discussing $C_S$, the vector space stabilized by $S$, we have to define notation of *sympletic complement* for sympletic vector space.

**Definition 2** (Sympletic Complement)**.** Let $W \subseteq \mathbb{F}_2^n \oplus \mathbb{F}_2^n$, the *sympletic complement* of $W$ is defined by,

$$W^\perp = \Big\{(\vec{x},\vec{z}) \in \mathbb{F}_2^n \oplus \mathbb{F}_2^n \;\Big|\; \omega\big((\vec{x},\vec{z}),(\vec{w}_1,\vec{w}_2)\big) = 0, \text{for any } (\vec{w}_1,\vec{w}_2) \in W\Big\}$$

We also say $W$ is isotropic iff $W \subseteq W^\perp$.

**Example 1.** Let $W = \{(\vec{x},0) | \vec{x} \in \mathbb{F}_2\} \subseteq \mathbb{F}_2^n \oplus \mathbb{F}_2^n$. It's easy to show that $W = W^\perp$.

- $W \subseteq W^\perp$: Obviously, $\omega((\vec{x}_1,0),(\vec{x}_2,0)) = 0$.
- $W^\perp \subseteq W$: If for any $w \in \mathbb{F}_2$, $\omega((\vec{w},0),(\vec{x},\vec{z})) = 0$, then $\vec{z} = 0$.

**Lemma 5.** If $\langle S\rangle$ is abelian, then $\pi(\langle S\rangle)$ is an isotropic subspace. And $\pi : \langle S\rangle \mapsto \mathbb{F}_2^n \oplus \mathbb{F}_2^n$ is injective iff $-I \notin \langle S\rangle$.

Lemma 5 means we can always map any abelian subspace of $G_n$ that not containing $-I$ to an isotropic subspace of $\mathbb{F}_2^n \oplus \mathbb{F}_2^n$. This map is also bijection but it will be hard to prove that.

**Definition 3** (Symplectomorphism)**.** An isomorphism $\alpha : \mathbb{F}_2^n \oplus \mathbb{F}_2^n \mapsto \mathbb{F}_2^n \oplus \mathbb{F}_2^n$ is a *symplectomorphism*, if for any $(\vec{x}_1,\vec{z}_1), (\vec{x}_2,\vec{z}_2) \in \mathbb{F}_2^n \oplus \mathbb{F}_2^n$,

$$\omega(\alpha(\vec{x}_1,\vec{z}_1), \alpha(\vec{x}_2,\vec{z}_2)) = \omega((\vec{x}_1,\vec{z}_1),(\vec{x}_2,\vec{z}_2))$$

**Definition 4** (Clifford Unitary)**.** Any unitary $U : (\mathbb{C}^2)^{\otimes n} \mapsto (\mathbb{C}^2)^{\otimes n}$ is called *Clifford*, if for any $g \in G_n$,

$$UgU^* \in G_n$$

Here we list some key facts about isotropic subspace and symplectomorphism.

1. Isotropic subspace of $\mathbb{F}_2^n \oplus \mathbb{F}_2^n$ have dimension at most $n$.
2. Any two isotropic subspace of the same dimension are equal up to symplectomorphism.
3. Any symplectomorphism can be implemented by a Clifford operator $U$, i.e. $\pi(UgU^*) = \alpha(\pi(g))$.

**Proposition 1.** $C_S = \{\vec{0}\} \Leftrightarrow -I \in \langle S \rangle$.

*Proof.* ($\Leftarrow$) This direction we have proved last time.

($\Rightarrow$) For any clifford $U$ we have $U(-I)U^* = -I$ and $UC_S = C_{USU^*}$. So in particular, it suffice to find a clifford $U$ for which we can show $-I \notin \langle USU^* \rangle$.

By Fact 3, it suffices to find a symplectomorphism $\alpha$, such that $\alpha\Big(\pi\big(\langle S \rangle\big)\Big) = \pi\big(\langle S' \rangle\big)$ where $-I \notin \langle S' \rangle$.

By Fact 1 and 2, we know that $\dim \pi\big(\langle S \rangle\big) = k \leq n$.

And by Fact 2, we can use symplectomorphism $\alpha$ that maps $\pi\big(\langle S \rangle\big)$ to the following isotropic subspaces.

$$\big\{(x_1, x_2, \dots, x_k, \underbrace{0, \dots, 0,}_{n-k} \underbrace{0, \dots, 0}_{n}) \bigm| x_1, x_2, \dots, x_k \in \mathbb{F}_2\big\} \subseteq \mathbb{F}_2^n \oplus \mathbb{F}_2^n$$

This is exactly $\pi\big(\langle S' \rangle\big)$ where,

$$S' = \big\{X(x_1, x_2, \dots, x_k, 0, \dots, 0) \bigm| x_1, x_2, \dots, x_k \in \mathbb{F}_2\big\} \subseteq G_n$$

which means $-I \notin \langle S' \rangle$. □

With a little more work we can prove,

**Proposition 2.** There exists a bijection: $\big\{$subgroups $\langle S \rangle \in G_n$ that are abelian and don't contain $-1\big\} \longleftrightarrow \big\{$isotropic subgroup of $\mathbb{F}_2^n \oplus \mathbb{F}_2^n\big\}$

**Theorem 1.** There exists a bijection: $\big\{$Pauli stabilizer codes $\big\} \longleftrightarrow \big\{$ isotropic subgroup of $\mathbb{F}_2^n \oplus \mathbb{F}_2^n\big\}$