Symplectic Isometries of Quantum Stabilizer Codes

Tefjol Pllaha

Department of Mathematics
University of Kentucky
http://www.ms.uky.edu/∼tpl222

30$^{\text{th}}$ Cumberland Conference on Combinatorics, Graph Theory, and Computing

Disclaimer(s)

Disclaimer(s)

- Results hold in a more general setting.

Disclaimer(s)

- Results hold in a more general setting.
- Motivation and connection with quantum computation will be bypassed.

Disclaimer(s)

- Results hold in a more general setting.
- Motivation and connection with quantum computation will be bypassed.
- The main theorem has connections with the LU-LC conjecture.

Set up

- Fix a finite field with $q = p^\ell$ elements, $\mathbb{F}_q$, and $n \in \mathbb{N}$.

Set up

- Fix a finite field with $q = p^\ell$ elements, $\mathbb{F}_q$, and $n \in \mathbb{N}$.
- The map $\langle \cdot \mid \cdot \rangle_{\mathsf{s}} : \mathbb{F}_q^{2n} \times \mathbb{F}_q^{2n} \to \mathbb{F}_q$ defined as

$$\langle (a, b) \mid (a', b') \rangle_{\mathsf{s}} := b \cdot a' - b' \cdot a,$$

Set up

- Fix a finite field with $q = p^{\ell}$ elements, $\mathbb{F}_q$, and $n \in \mathbb{N}$.
- The map $\langle \cdot \mid \cdot \rangle_s : \mathbb{F}_q^{2n} \times \mathbb{F}_q^{2n} \to \mathbb{F}_q$ defined as

$$\langle (a, b) \mid (a', b') \rangle_s := b \cdot a' - b' \cdot a,$$

  is a non-degenerate, symplectic, bilinear form.

Set up

- Fix a finite field with $q = p^\ell$ elements, $\mathbb{F}_q$, and $n \in \mathbb{N}$.
- The map $\langle \cdot \mid \cdot \rangle_s : \mathbb{F}_q^{2n} \times \mathbb{F}_q^{2n} \to \mathbb{F}_q$ defined as

$$\langle (a, b) \mid (a', b') \rangle_s := b \cdot a' - b' \cdot a,$$

is a non-degenerate, symplectic, bilinear form. For $A \subseteq \mathbb{F}_q^{2n}$, $A^\perp := \{x \in R^{2n} \mid \langle x \mid A \rangle_s = 0\}$.

Set up

- Fix a finite field with $q = p^\ell$ elements, $\mathbb{F}_q$, and $n \in \mathbb{N}$.
- The map $\langle \cdot \mid \cdot \rangle_s : \mathbb{F}_q^{2n} \times \mathbb{F}_q^{2n} \to \mathbb{F}_q$ defined as

$$\langle (a, b) \mid (a', b') \rangle_s := b \cdot a' - b' \cdot a,$$

  is a non-degenerate, symplectic, bilinear form. For $A \subseteq \mathbb{F}_q^{2n}$, $A^\perp := \{x \in R^{2n} \mid \langle x \mid A \rangle_s = 0\}$.
- $\mathrm{tr} : \mathbb{F}_q \to \mathbb{F}_p$ will denote the **trace** over the prime field, and $\omega = e^{2\pi i/p}$ will be a fixed p^{th} primitive root of unity.

A (very short) word on quantum errors

A (very short) word on quantum errors

- Let $\mathcal{B} = \{v_x \mid x \in \mathbb{F}_q\}$ be an orthonormal basis of $\mathbb{C}^q$.

A (very short) word on quantum errors

- Let $\mathcal{B} = \{v_x \mid x \in \mathbb{F}_q\}$ be an orthonormal basis of $\mathbb{C}^q$. For all $a \in \mathbb{F}_q$ we define two unitary transformations of $\mathbb{C}^q$:

A (very short) word on quantum errors

- Let $\mathcal{B} = \{v_x \mid x \in \mathbb{F}_q\}$ be an orthonormal basis of $\mathbb{C}^q$. For all $a \in \mathbb{F}_q$ we define two unitary transformations of $\mathbb{C}^q$:
- $$X(a) : \mathbb{C}^q \longrightarrow \mathbb{C}^q : v_x \longmapsto v_{x+a}.$$

A (very short) word on quantum errors

- Let $\mathcal{B} = \{v_x \mid x \in \mathbb{F}_q\}$ be an orthonormal basis of $\mathbb{C}^q$. For all $a \in \mathbb{F}_q$ we define two unitary transformations of $\mathbb{C}^q$:
- $$X(a) : \mathbb{C}^q \longrightarrow \mathbb{C}^q : v_x \longmapsto v_{x+a}.$$

  X(a) is called a **flip error**.

A (very short) word on quantum errors

- Let $\mathcal{B} = \{v_x \mid x \in \mathbb{F}_q\}$ be an orthonormal basis of $\mathbb{C}^q$. For all $a \in \mathbb{F}_q$ we define two unitary transformations of $\mathbb{C}^q$:
- $$X(a) : \mathbb{C}^q \longrightarrow \mathbb{C}^q : v_x \longmapsto v_{x+a}.$$

  X(a) is called a **flip error**.
- $$Z(a) : \mathbb{C}^q \longrightarrow \mathbb{C}^q : v_x \longmapsto \omega^{\mathrm{tr}(ax)} v_x,$$

A (very short) word on quantum errors

- Let $\mathcal{B} = \{v_x \mid x \in \mathbb{F}_q\}$ be an orthonormal basis of $\mathbb{C}^q$. For all $a \in \mathbb{F}_q$ we define two unitary transformations of $\mathbb{C}^q$:
- $$X(a) : \mathbb{C}^q \longrightarrow \mathbb{C}^q : v_x \longmapsto v_{x+a}.$$

  X(a) is called a **flip error**.
- $$Z(a) : \mathbb{C}^q \longrightarrow \mathbb{C}^q : v_x \longmapsto \omega^{\mathrm{tr}(ax)} v_x,$$

  Z(a) is called a **phase error**.

(Quantum) Stabilizer Codes

Definition

A $\mathbb{F}_q$-subspace $C \subseteq \mathbb{F}_q^{2n}$ such that $C \subseteq C^{\perp}$ is called a **stabilizer code**.

(Quantum) Stabilizer Codes

Definition

A $\mathbb{F}_q$-subspace $C \subseteq \mathbb{F}_q^{2n}$ such that $C \subseteq C^{\perp}$ is called a **stabilizer code**.

- The **symplectic weight** of a vector $(a, b) \in \mathbb{F}_q^{2n}$ is

$$\mathrm{wt_s}(a, b) := \#\{i \mid (a_i, b_i) \neq (0, 0)\}.$$

(Quantum) Stabilizer Codes

Definition

A $\mathbb{F}_q$-subspace $C \subseteq \mathbb{F}_q^{2n}$ such that $C \subseteq C^\perp$ is called a **stabilizer code**.

- The **symplectic weight** of a vector $(a, b) \in \mathbb{F}_q^{2n}$ is

$$\mathrm{wt_s}(a, b) := \#\{i \mid (a_i, b_i) \neq (0, 0)\}.$$

- The **minimum distance** of a stabilizer code is

$$\mathrm{dist}(C) := \begin{cases} \min\{\mathrm{wt_s}(a, b) \mid (a, b) \in C^\perp - C\} & \text{if } C \subsetneq C^\perp \\ \min\{\mathrm{wt_s}(a, b) \mid (a, b) \in C^\perp - \{0\}\} & \text{if } C = C^\perp \end{cases}.$$

Symplectic Isometries

Symplectic Isometries

Let $A \subseteq \mathbb{F}_q^{2n}$ be a subspace. A linear map $f : A \to \mathbb{F}_q^{2n}$ is called a **symplectic isometry** if for all $x, y \in \mathbb{F}_q^{2n}$

$$\mathrm{wt}_{\mathrm{s}}(x) = \mathrm{wt}_{\mathrm{s}}(f(x)) \text{ and } \langle x \mid y \rangle_{\mathrm{s}} = \langle f(x) \mid f(y) \rangle_{\mathrm{s}}.$$

Symplectic Isometries

Let $A \subseteq \mathbb{F}_q^{2n}$ be a subspace. A linear map $f : A \to \mathbb{F}_q^{2n}$ is called a **symplectic isometry** if for all $x, y \in \mathbb{F}_q^{2n}$

$$\mathrm{wt_s}(x) = \mathrm{wt_s}(f(x)) \text{ and } \langle x \mid y \rangle_{\mathrm{s}} = \langle f(x) \mid f(y) \rangle_{\mathrm{s}}.$$

Example

1. For a permutation $\sigma \in S_n$, $(a, b) \mapsto (\sigma(a), \sigma(b))$.

Symplectic Isometries

Let $A \subseteq \mathbb{F}_q^{2n}$ be a subspace. A linear map $f : A \to \mathbb{F}_q^{2n}$ is called a **symplectic isometry** if for all $x, y \in \mathbb{F}_q^{2n}$

$$\mathrm{wt_s}(x) = \mathrm{wt_s}(f(x)) \text{ and } \langle x \mid y \rangle_{\mathrm{s}} = \langle f(x) \mid f(y) \rangle_{\mathrm{s}}.$$

Example

1. For a permutation $\sigma \in S_n$, $(a, b) \mapsto (\sigma(a), \sigma(b))$.
2. $(a, b) \mapsto (\cdots, a_{i-1}, b_i, a_{i+1}, \cdots, \cdots, b_{i-1}, -a_i, b_{i+1}, \cdots)$.

Symplectic Isometries of $\mathbb{F}_q^{2n}$

Symplectic Isometries of $\mathbb{F}_q^{2n}$

Question

What is the structure of symplectic isometries of $\mathbb{F}_q^{2n}$?

Symplectic Isometries of $\mathbb{F}_q^{2n}$

Question

What is the structure of symplectic isometries of $\mathbb{F}_q^{2n}$?

- To answer this question we transfer the problem on $(\mathbb{F}_q^2)^n$ via the change of coordinates

$$\gamma : \mathbb{F}_q^{2n} \to (\mathbb{F}_q^2)^n, (a, b) \mapsto (a_1, b_1 \mid \cdots \mid a_n, b_n).$$

Symplectic Isometries of $\mathbb{F}_q^{2n}$

Question

What is the structure of symplectic isometries of $\mathbb{F}_q^{2n}$?

- To answer this question we transfer the problem on $(\mathbb{F}_q^2)^n$ via the change of coordinates

$$\gamma : \mathbb{F}_q^{2n} \to (\mathbb{F}_q^2)^n, (a, b) \mapsto (a_1, b_1 \mid \cdots \mid a_n, b_n).$$

- The symplectic weight now becomes the **Hamming weight** on $\mathbb{F}_q^2$, that is, $\mathrm{wt}_{\mathrm{H}}(x) = \mathrm{wt}_{\mathrm{s}}(\gamma^{-1}(x))$ for all $x \in (\mathbb{F}_q^2)^n$.

Symplectic Isometries of $\mathbb{F}_q^{2n}$

Question

What is the structure of symplectic isometries of $\mathbb{F}_q^{2n}$?

- To answer this question we transfer the problem on $(\mathbb{F}_q^2)^n$ via the change of coordinates

$$\gamma : \mathbb{F}_q^{2n} \to (\mathbb{F}_q^2)^n, (a, b) \mapsto (a_1, b_1 \mid \cdots \mid a_n, b_n).$$

- The symplectic weight now becomes the **Hamming weight** on $\mathbb{F}_q^2$, that is, $\mathrm{wt}_\mathrm{H}(x) = \mathrm{wt}_\mathrm{s}(\gamma^{-1}(x))$ for all $x \in (\mathbb{F}_q^2)^n$.
- Define $\langle x \mid y \rangle := \langle \gamma^{-1}(x) \mid \gamma^{-1}(y) \rangle_\mathrm{s}$ for all $x, y \in (\mathbb{F}_q^2)^n$.

Symplectic Isometries of $\mathbb{F}_q^{2n}$

Question

What is the structure of symplectic isometries of $\mathbb{F}_q^{2n}$?

- To answer this question we transfer the problem on $(\mathbb{F}_q^2)^n$ via the change of coordinates

$$\gamma : \mathbb{F}_q^{2n} \to (\mathbb{F}_q^2)^n, (a, b) \mapsto (a_1, b_1 \mid \cdots \mid a_n, b_n).$$

- The symplectic weight now becomes the **Hamming weight** on $\mathbb{F}_q^2$, that is, $\mathrm{wt}_{\mathrm{H}}(x) = \mathrm{wt}_{\mathrm{s}}(\gamma^{-1}(x))$ for all $x \in (\mathbb{F}_q^2)^n$.
- Define $\langle x \mid y \rangle := \langle \gamma^{-1}(x) \mid \gamma^{-1}(y) \rangle_{\mathrm{s}}$ for all $x, y \in (\mathbb{F}_q^2)^n$.
- For a linear map $f : \mathbb{F}_q^{2n} \to \mathbb{F}_q^{2n}$, denote $\widetilde{f} := \gamma \circ f \circ \gamma^{-1}$.

Symplectic Isometries of $\mathbb{F}_q^{2n}$

Theorem (Gluesing-Luerssen/P, 2017)

A linear map $f : \mathbb{F}_q^{2n} \to \mathbb{F}_q^{2n}$ *is a symplectic isometry iff the map* $\widetilde{f} : (\mathbb{F}_q^2)^n \to (\mathbb{F}_q^2)^n$ *is given by*

Symplectic Isometries of $\mathbb{F}_q^{2n}$

Theorem (Gluesing-Luerssen/P, 2017)

A linear map $f : \mathbb{F}_q^{2n} \to \mathbb{F}_q^{2n}$ is a symplectic isometry iff the map $\widetilde{f} : (\mathbb{F}_q^2)^n \to (\mathbb{F}_q^2)^n$ is given by

$$\widetilde{f} = diag(A_1, \cdots, A_n)$$

for $A_i \in SL_2(\mathbb{F}_q)$.

Symplectic Isometries of $\mathbb{F}_q^{2n}$

Theorem (Gluesing-Luerssen/P, 2017)

A linear map $f : \mathbb{F}_q^{2n} \to \mathbb{F}_q^{2n}$ is a symplectic isometry iff the map $\widetilde{f} : (\mathbb{F}_q^2)^n \to (\mathbb{F}_q^2)^n$ is given by

$$\widetilde{f} = diag(A_1, \cdots, A_n)(P \otimes I_2),$$

for $A_i \in SL_2(\mathbb{F}_q)$.

Symplectic Isometries of $\mathbb{F}_q^{2n}$

Theorem (Gluesing-Luerssen/P, 2017)

A linear map $f : \mathbb{F}_q^{2n} \to \mathbb{F}_q^{2n}$ is a symplectic isometry iff the map $\widetilde{f} : (\mathbb{F}_q^2)^n \to (\mathbb{F}_q^2)^n$ is given by

$$\widetilde{f} = diag(A_1, \cdots, A_n)(P \otimes I_2),$$

for $A_i \in SL_2(\mathbb{F}_q)$.

- We call such symplectic isometries **monomial** isometries.

Symplectic Isometries of $\mathbb{F}_q^{2n}$

Theorem (Gluesing-Luerssen/P, 2017)

A linear map $f : \mathbb{F}_q^{2n} \to \mathbb{F}_q^{2n}$ is a symplectic isometry iff the map $\widetilde{f} : (\mathbb{F}_q^2)^n \to (\mathbb{F}_q^2)^n$ is given by

$$\widetilde{f} = diag(A_1, \cdots, A_n)(P \otimes I_2),$$

for $A_i \in SL_2(\mathbb{F}_q)$.

- We call such symplectic isometries **monomial** isometries.

Question

What is the structure of symplectic isometries $f : A \subsetneq \mathbb{F}_q^{2n} \to \mathbb{F}_q^{2n}$?

Symplectic Isometries of $\mathbb{F}_q^{2n}$

Theorem (Gluesing-Luerssen/P, 2017)

A linear map $f : \mathbb{F}_q^{2n} \to \mathbb{F}_q^{2n}$ is a symplectic isometry iff the map $\widetilde{f} : (\mathbb{F}_q^2)^n \to (\mathbb{F}_q^2)^n$ is given by

$$\widetilde{f} = diag(A_1, \cdots, A_n)(P \otimes I_2),$$

for $A_i \in SL_2(\mathbb{F}_q)$.

- We call such symplectic isometries **monomial** isometries.

Question

What is the structure of symplectic isometries $f : A \subsetneq \mathbb{F}_q^{2n} \to \mathbb{F}_q^{2n}$?

- We are interested on stabilizer codes.

Symplectic Isometries of Stabilizer Codes

Let $C \subseteq \mathbb{F}_q^{2n}$ be a stabilizer code. We define two groups:

Symplectic Isometries of Stabilizer Codes

Let $C \subseteq \mathbb{F}_q^{2n}$ be a stabilizer code. We define two groups:

$$\mathrm{Mon}_{\mathrm{SL}}(C) := \{f \in \mathrm{Aut}(C) \mid f \text{ is monomial isometry}\}$$

Symplectic Isometries of Stabilizer Codes

Let $C \subseteq \mathbb{F}_q^{2n}$ be a stabilizer code. We define two groups:

$$\begin{aligned} \mathrm{Mon}_{\mathrm{SL}}(C) &:= \{f \in \mathrm{Aut}(C) \mid f \text{ is monomial isometry}\} \\ \mathrm{Symp}(C) &:= \{f \in \mathrm{Aut}(C) \mid f \text{ is symplectic isometry}\} \end{aligned}$$

Symplectic Isometries of Stabilizer Codes

Let $C \subseteq \mathbb{F}_q^{2n}$ be a stabilizer code. We define two groups:

$$\mathrm{Mon}_{\mathrm{SL}}(C) := \{f \in \mathrm{Aut}(C) \mid f \text{ is monomial isometry}\}$$
$$\mathrm{Symp}(C) := \{f \in \mathrm{Aut}(C) \mid f \text{ is symplectic isometry}\}$$

- $\mathrm{Mon}_{\mathrm{SL}}(C) \subseteq \mathrm{Symp}(C)$.

Symplectic Isometries of Stabilizer Codes

Let $C \subseteq \mathbb{F}_q^{2n}$ be a stabilizer code. We define two groups:

$$\mathrm{Mon}_{\mathrm{SL}}(C) := \{f \in \mathrm{Aut}(C) \mid f \text{ is monomial isometry}\}$$
$$\mathrm{Symp}(C) := \{f \in \mathrm{Aut}(C) \mid f \text{ is symplectic isometry}\}$$

- $\mathrm{Mon}_{\mathrm{SL}}(C) \subseteq \mathrm{Symp}(C)$.
  - **Fact:** $\mathrm{Mon}_{\mathrm{SL}}(C) \subsetneq \mathrm{Symp}(C)$.

Symplectic Isometries of Stabilizer Codes

Let $C \subseteq \mathbb{F}_q^{2n}$ be a stabilizer code. We define two groups:

$$\begin{aligned} \mathrm{Mon}_{\mathrm{SL}}(C) &:= \{f \in \mathrm{Aut}(C) \mid f \text{ is monomial isometry}\} \\ \mathrm{Symp}(C) &:= \{f \in \mathrm{Aut}(C) \mid f \text{ is symplectic isometry}\} \end{aligned}$$

- $\mathrm{Mon}_{\mathrm{SL}}(C) \subseteq \mathrm{Symp}(C)$.
  - **Fact:** $\mathrm{Mon}_{\mathrm{SL}}(C) \subsetneq \mathrm{Symp}(C)$.
  - **Reason:** Explicit construction of a stabilizer code that does not admit a monomial symplectic isometry.

Symplectic Isometries of Stabilizer Codes

Let $C \subseteq \mathbb{F}_q^{2n}$ be a stabilizer code. We define two groups:

$$\mathrm{Mon}_{\mathrm{SL}}(C) := \{f \in \mathrm{Aut}(C) \mid f \text{ is monomial isometry}\}$$
$$\mathrm{Symp}(C) := \{f \in \mathrm{Aut}(C) \mid f \text{ is symplectic isometry}\}$$

- $\mathrm{Mon}_{\mathrm{SL}}(C) \subseteq \mathrm{Symp}(C)$.
  - **Fact:** $\mathrm{Mon}_{\mathrm{SL}}(C) \subsetneq \mathrm{Symp}(C)$.
  - **Reason:** Explicit construction of a stabilizer code that does not admit a monomial symplectic isometry.
- Computing these groups is difficult in general. An easier question is the following.

Symplectic Isometries of Stabilizer Codes

Let $C \subseteq \mathbb{F}_q^{2n}$ be a stabilizer code. We define two groups:

$$\begin{aligned} \mathrm{Mon}_{\mathrm{SL}}(C) &:= \{f \in \mathrm{Aut}(C) \mid f \text{ is monomial isometry}\} \\ \mathrm{Symp}(C) &:= \{f \in \mathrm{Aut}(C) \mid f \text{ is symplectic isometry}\} \end{aligned}$$

- $\mathrm{Mon}_{\mathrm{SL}}(C) \subseteq \mathrm{Symp}(C)$.
  - **Fact:** $\mathrm{Mon}_{\mathrm{SL}}(C) \subsetneq \mathrm{Symp}(C)$.
  - **Reason:** Explicit construction of a stabilizer code that does not admit a monomial symplectic isometry.
- Computing these groups is difficult in general. An easier question is the following.

Open Problem

How different can the groups $\mathrm{Mon}_{\mathrm{SL}}(C)$ and $\mathrm{Symp}(C)$ be?

Theorem (P, 2018)

Let $H \leq G$ be two subgroups **that satisfy some necessary conditions**. *Then there exists a stabilizer code C such that $H = \mathrm{Mon}_{\mathrm{SL}}(C)$ and $G = \mathrm{Symp}(C)$.*

Thank You!