On Quantum Stabilizer Codes over Local Frobenius Rings

Tefjol Pllaha

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

AMS Sectional Meetings - Columbus, OH
The Ohio State University
March 18, 2018

*Joint with Heide Gluesing-Luerssen

Outline

Outline

Outline

Outline

Outline

Outline

Frobenius Rings

Frobenius Rings

- R will denote a finite commutative ring with identity.

Frobenius Rings

- R will denote a finite commutative ring with identity.
- $\widehat{R} := \mathrm{Hom}((R,+),\mathbb{C}^*)$ will denote the **character group**.

Frobenius Rings

- R will denote a finite commutative ring with identity.
- $\widehat{R} := \mathrm{Hom}((R,+),\mathbb{C}^*)$ will denote the **character group**.
  - $\widehat{R} \cong R$ as groups.

Frobenius Rings

- R will denote a finite commutative ring with identity.
- $\widehat{R} := \mathrm{Hom}((R,+),\mathbb{C}^*)$ will denote the **character group**.
    - $\widehat{R} \cong R$ as groups.
    - $\widehat{R}$ is a R-module structure via

$$(r\cdot\chi)(x) := \chi(rx), \text{ for all } r,x \in R \text{ and } \chi \in \widehat{R}.$$

Frobenius Rings

- R will denote a finite commutative ring with identity.
- $\widehat{R} := \mathrm{Hom}((R,+),\mathbb{C}^*)$ will denote the **character group**.
  - $\widehat{R} \cong R$ as groups.
  - $\widehat{R}$ is a R-module structure via

$$(r \cdot \chi)(x) := \chi(rx), \text{ for all } r, x \in R \text{ and } \chi \in \widehat{R}.$$

- R is called **Frobenius** if ${}_R\widehat{R} \cong {}_RR$ as R-modules.

Frobenius Rings

- R will denote a finite commutative ring with identity.
- $\widehat{R} := \mathrm{Hom}((R,+),\mathbb{C}^*)$ will denote the **character group**.
  - $\widehat{R} \cong R$ as groups.
  - $\widehat{R}$ is a R-module structure via

$$(r\cdot\chi)(x) := \chi(rx), \text{ for all } r, x \in R \text{ and } \chi \in \widehat{R}.$$

- R is called **Frobenius** if ${}_R\widehat{R} \cong {}_RR$ as R-modules.
  - There exists $\chi \in \widehat{R}$ such that $\widehat{R} = \{r\cdot\chi \mid r \in R\}$.

Frobenius Rings

- R will denote a finite commutative ring with identity.
- $\widehat{R} := \mathrm{Hom}((R,+),\mathbb{C}^*)$ will denote the **character group**.
  - $\widehat{R} \cong R$ as groups.
  - $\widehat{R}$ is a R-module structure via

$$(r\cdot\chi)(x) := \chi(rx), \text{ for all } r,x \in R \text{ and } \chi \in \widehat{R}.$$

- R is called **Frobenius** if ${}_R\widehat{R} \cong {}_RR$ as R-modules.
  - There exists $\chi \in \widehat{R}$ such that $\widehat{R} = \{r\cdot\chi \mid r \in R\}$.
  - Such χ is called **generating character**.

Outline

Basic Notions

- Fix $|R| = q$ and a generating character $\chi \in \widehat{R}$.

Basic Notions

- Fix $|R| = q$ and a generating character $\chi \in \widehat{R}$.
- Fix a ON-bais of $\mathbb{C}^q$: $\mathcal{B} = \{v_x \mid x \in R\}$.

Basic Notions

- Fix $|R| = q$ and a generating character $\chi \in \widehat{R}$.
- Fix a ON-bais of $\mathbb{C}^q$: $\mathcal{B} = \{v_x \mid x \in R\}$.
- For $a \in R$, define two unitary transformations of $\mathbb{C}^q$:

Basic Notions

- Fix $|R| = q$ and a generating character $\chi \in \widehat{R}$.
- Fix a ON-bais of $\mathbb{C}^q$: $\mathcal{B} = \{v_x \mid x \in R\}$.
- For $a \in R$, define two unitary transformations of $\mathbb{C}^q$:

$$X(a) : v_x \quad \longrightarrow \quad v_{x+a}$$

Basic Notions

- Fix $|R| = q$ and a generating character $\chi \in \widehat{R}$.
- Fix a ON-bais of $\mathbb{C}^q$: $\mathcal{B} = \{v_x \mid x \in R\}$.
- For $a \in R$, define two unitary transformations of $\mathbb{C}^q$:

$$\begin{aligned} X(a) : v_x &\longrightarrow v_{x+a} \\ Z(a) : v_x &\longrightarrow \chi(ax) v_x \end{aligned}$$

Basic Notions

- Fix $|R| = q$ and a generating character $\chi \in \widehat{R}$.
- Fix a ON-bais of $\mathbb{C}^q$: $\mathcal{B} = \{v_x \mid x \in R\}$.
- For $a \in R$, define two unitary transformations of $\mathbb{C}^q$:

$$\begin{array}{rcl} X(a) : v_x & \longrightarrow & v_{x+a} \\ Z(a) : v_x & \longrightarrow & \chi(ax)v_x \end{array}$$

- For all $n \in \mathbb{N}$, $(\mathbb{C}^q)^{\otimes n} \cong \mathbb{C}^{q^n}$.

Basic Notions

- Fix $|R| = q$ and a generating character $\chi \in \widehat{R}$.
- Fix a ON-bais of $\mathbb{C}^q$: $\mathcal{B} = \{v_x \mid x \in R\}$.
- For $a \in R$, define two unitary transformations of $\mathbb{C}^q$:

$$\begin{array}{rcl} X(a) : v_x & \longrightarrow & v_{x+a} \\ Z(a) : v_x & \longrightarrow & \chi(ax)v_x \end{array}$$

- For all $n \in \mathbb{N}$, $(\mathbb{C}^q)^{\otimes n} \cong \mathbb{C}^{q^n}$. We use the ON-basis

$$\mathcal{B}^{\otimes n} := \{v_{x_1} \otimes \cdots \otimes v_{x_n} \mid (x_1, \ldots, x_n) \in R^n\}$$

Basic Notions

- Fix $|R| = q$ and a generating character $\chi \in \widehat{R}$.
- Fix a ON-bais of $\mathbb{C}^q$: $\mathcal{B} = \{v_x \mid x \in R\}$.
- For $a \in R$, define two unitary transformations of $\mathbb{C}^q$:

$$\begin{array}{rcl} X(a) : v_x & \longrightarrow & v_{x+a} \\ Z(a) : v_x & \longrightarrow & \chi(ax)v_x \end{array}$$

- For all $n \in \mathbb{N}$, $(\mathbb{C}^q)^{\otimes n} \cong \mathbb{C}^{q^n}$. We use the ON-basis

$$\mathcal{B}^{\otimes n} := \{v_{x_1} \otimes \cdots \otimes v_{x_n} \mid (x_1, \ldots, x_n) \in R^n\}$$

For $a = (a_1, \ldots, a_n) \in R^n$ define

$$\left.\begin{array}{l} X(a) := X(a_1) \otimes \cdots \otimes X(a_n) \\ Z(a) := Z(a_1) \otimes \cdots \otimes Z(a_n) \end{array}\right\} \in \mathcal{U}(q^n)$$

Basic Notions

- The n **qubit quantum error basis** is

$$\begin{aligned}\mathcal{E}_n &= \{X(a) \cdot Z(b) \mid a, b \in R^n\} \\ &= \{X(a_1)Z(a_1) \otimes \cdots \otimes X(a_n)Z(a_n) \mid (a, b) \in R^{2n}\}\end{aligned}$$

Basic Notions

- The n **qubit quantum error basis** is

$$\begin{aligned}\mathcal{E}_n &= \{X(a)\cdot Z(b) \mid a, b \in R^n\} \\ &= \{X(a_1)Z(a_1)\otimes\cdots\otimes X(a_n)Z(a_n) \mid (a,b)\in R^{2n}\}\end{aligned}$$

- Let $e = X(a)Z(b)$, $e' = X(a')Z(b') \in \mathcal{E}_n$. Then

$$\begin{aligned}ee' &= \chi(b\cdot a')X(a+a')Z(b+b') \\ e'e &= \chi(b'\cdot a)X(a+a')Z(b+b')\end{aligned}$$

Basic Notions

- The n **qubit quantum error basis** is

$$\begin{aligned}\mathcal{E}_n &= \{X(a)\cdot Z(b) \mid a, b \in R^n\} \\ &= \{X(a_1)Z(a_1)\otimes\cdots\otimes X(a_n)Z(a_n) \mid (a,b)\in R^{2n}\}\end{aligned}$$

- Let $e = X(a)Z(b)$, $e' = X(a')Z(b') \in \mathcal{E}_n$. Then

$$\begin{aligned}ee' &= \chi(b\cdot a')X(a+a')Z(b+b') \\ e'e &= \chi(b'\cdot a)X(a+a')Z(b+b')\end{aligned}$$

- $ee' = e'e$

Basic Notions

- The n **qubit quantum error basis** is

$$\begin{aligned}\mathcal{E}_n &= \{X(a)\cdot Z(b) \mid a, b \in R^n\}\\ &= \{X(a_1)Z(a_1)\otimes\cdots\otimes X(a_n)Z(a_n) \mid (a,b)\in R^{2n}\}\end{aligned}$$

- Let $e = X(a)Z(b)$, $e' = X(a')Z(b') \in \mathcal{E}_n$. Then

$$\begin{aligned}ee' &= \chi(b\cdot a')X(a+a')Z(b+b')\\ e'e &= \chi(b'\cdot a)X(a+a')Z(b+b')\end{aligned}$$

- $ee' = e'e \iff \chi(b\cdot a' - b'\cdot a) = 1.$

Basic Notions

- The n **qubit quantum error basis** is

$$\begin{aligned}\mathcal{E}_n &= \{X(a)\cdot Z(b) \mid a, b \in R^n\} \\ &= \{X(a_1)Z(a_1)\otimes\cdots\otimes X(a_n)Z(a_n) \mid (a,b)\in R^{2n}\}\end{aligned}$$

- Let $e = X(a)Z(b)$, $e' = X(a')Z(b') \in \mathcal{E}_n$. Then

$$\begin{aligned}ee' &= \chi(b\cdot a')X(a+a')Z(b+b') \\ e'e &= \chi(b'\cdot a)X(a+a')Z(b+b')\end{aligned}$$

- $ee' = e'e \iff \chi(b\cdot a' - b'\cdot a) = 1.$
- For any $n\in\mathbb{N}$, the map $\langle\cdot\mid\cdot\rangle_s : R^{2n}\times R^{2n}\to R$ defined as

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

Basic Notions

- The n **qubit quantum error basis** is

$$\begin{aligned}\mathcal{E}_n &= \{X(a)\cdot Z(b) \mid a, b \in R^n\}\\ &= \{X(a_1)Z(a_1)\otimes\cdots\otimes X(a_n)Z(a_n) \mid (a,b)\in R^{2n}\}\end{aligned}$$

- Let $e = X(a)Z(b)$, $e' = X(a')Z(b') \in \mathcal{E}_n$. Then

$$\begin{aligned}ee' &= \chi(b\cdot a')X(a+a')Z(b+b')\\ e'e &= \chi(b'\cdot a)X(a+a')Z(b+b')\end{aligned}$$

- $ee' = e'e \iff \chi(b\cdot a' - b'\cdot a) = 1.$
- For any $n\in\mathbb{N}$, the map $\langle\cdot\mid\cdot\rangle_s : R^{2n}\times R^{2n}\to R$ defined as

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

  is a non-degenerate, symplectic, bilinear form.

Basic Notions

- The n **qubit quantum error basis** is

$$\begin{aligned}\mathcal{E}_n &= \{X(a)\cdot Z(b) \mid a, b \in R^n\} \\ &= \{X(a_1)Z(a_1)\otimes\cdots\otimes X(a_n)Z(a_n) \mid (a,b)\in R^{2n}\}\end{aligned}$$

- Let $e = X(a)Z(b)$, $e' = X(a')Z(b') \in \mathcal{E}_n$. Then

$$\begin{aligned} ee' &= \chi(b\cdot a')X(a+a')Z(b+b') \\ e'e &= \chi(b'\cdot a)X(a+a')Z(b+b')\end{aligned}$$

- $ee' = e'e \iff \chi(b\cdot a' - b'\cdot a) = 1$.
- For any $n \in \mathbb{N}$, the map $\langle\cdot \mid \cdot\rangle_s : R^{2n}\times R^{2n} \to R$ defined as

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

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

The Pauli Group

- Let $\mathrm{char}(R) = c$.

The Pauli Group

- Let $\mathrm{char}(R) = c$. Fix a N^{th}-PRU ω, where
$$N = \begin{cases} c & \text{if } c \text{ is odd} \\ 2c & \text{if } c \text{ is even} \end{cases}$$

The Pauli Group

- Let $\text{char}(R) = c$. Fix a N^{th}-PRU ω, where

$$N = \begin{cases} c & \text{if } c \text{ is odd} \\ 2c & \text{if } c \text{ is even} \end{cases}$$

Definition

The n-th qubit **Pauli Group** associated to the error basis $\mathcal{E}_n$ is defined as

$$\mathcal{P}_n := \{\omega^l X(a)Z(b) \mid (a, b) \in R^{2n}, l \in \mathbb{Z}\}.$$

The Pauli Group

- Let $\mathrm{char}(R) = c$. Fix a N^{th}-PRU ω, where

$$N = \begin{cases} c & \text{if } c \text{ is odd} \\ 2c & \text{if } c \text{ is even} \end{cases}$$

Definition

The n-th qubit **Pauli Group** associated to the error basis $\mathcal{E}_n$ is defined as

$$\mathcal{P}_n := \{\omega^l X(a)Z(b) \mid (a,b) \in R^{2n}, l \in \mathbb{Z}\}.$$

- We have a group homomorphism

$$\Psi : \mathcal{P}_n \longrightarrow R^{2n}, \ \omega^l X(a)Z(b) \mapsto (a,b)$$

Quantum Stabilizer Codes

Definition

- A subgroup $S \leq \mathcal{P}_n$ is called a **stabilizer group** if it is abelian and $S \cap \ker \Psi = \{I\}$.

Quantum Stabilizer Codes

Definition

- A subgroup $S \leq \mathcal{P}_n$ is called a **stabilizer group** if it is abelian and $S \cap \ker \Psi = \{I\}$.
- A **quantum stabilizer code** (of length n over R) is

$$\mathcal{Q}(S) := \{v \in \mathbb{C}^{q^n} \mid ev = v, \text{ for all } e \in S\}$$

Quantum Stabilizer Codes

Definition

- A subgroup $S \leq \mathcal{P}_n$ is called a **stabilizer group** if it is abelian and $S \cap \ker \Psi = \{I\}$.
- A **quantum stabilizer code** (of length n over R) is

$$\mathcal{Q}(S) := \{v \in \mathbb{C}^{q^n} \mid ev = v, \text{ for all } e \in S\} = \bigcap_{e \in S} \operatorname{eig}(e, 1)$$

Quantum Stabilizer Codes

Definition

- A subgroup $S \leq \mathcal{P}_n$ is called a **stabilizer group** if it is abelian and $S \cap \ker \Psi = \{I\}$.
- A **quantum stabilizer code** (of length n over R) is

$$\mathcal{Q}(S) := \{v \in \mathbb{C}^{q^n} \mid ev = v, \text{ for all } e \in S\} = \bigcap_{e \in S} \mathrm{eig}(e, 1)$$

- NOTE: $S \subseteq \mathcal{C}(\mathcal{P}_n)$.

Quantum Stabilizer Codes

Definition

- A subgroup $S \leq \mathcal{P}_n$ is called a **stabilizer group** if it is abelian and $S \cap \ker \Psi = \{I\}$.
- A **quantum stabilizer code** (of length n over R) is

$$\mathcal{Q}(S) := \{v \in \mathbb{C}^{q^n} \mid ev = v, \text{ for all } e \in S\} = \bigcap_{e \in S} \operatorname{eig}(e, 1)$$

- NOTE: $S \subseteq \mathcal{C}(\mathcal{P}_n)$.

Theorem

$\mathcal{Q}(S)$ can detect all the errors outside $\mathcal{C}(\mathcal{P}_n) - S$.

Quantum Stabilizer Codes

Definition

- The **symplectic weight** of an error $e = \omega^l X(a)Z(b)$ is

$$\mathrm{wt}_s(e) := |\{i \mid (a_i, b_i) \neq (0,0)\}|.$$

Quantum Stabilizer Codes

Definition

- The **symplectic weight** of an error $e = \omega^l X(a)Z(b)$ is

$$\mathrm{wt_s}(e) := |\{i \mid (a_i, b_i) \neq (0,0)\}|.$$

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

$$\mathrm{dist}(\mathcal{Q}(S)) := \min\{\mathrm{wt_s}(e) \mid e \in \mathcal{C}(\mathcal{P}_n) - S\}.$$

Outline

Stabilizer Codes

Stabilizer Codes

Definition

A submodule $C \leq R^{2n}$ is called a **stabilizer code** if there exists a stabilizer group S such that $C = \Psi(S)$.

Stabilizer Codes

Definition

A submodule $C \leq R^{2n}$ is called a **stabilizer code** if there exists a stabilizer group S such that $C = \Psi(S)$.

Theorem (Gluesing-Luerssen/P, 2017)

A submodule $C \leq R^{2n}$ is a stabilizer code iff $C \subseteq C^{\perp}$.

Stabilizer Codes

Definition

A submodule $C \leq R^{2n}$ is called a **stabilizer code** if there exists a stabilizer group S such that $C = \Psi(S)$.

Theorem (Gluesing-Luerssen/P, 2017)

A submodule $C \leq R^{2n}$ is a stabilizer code iff $C \subseteq C^{\perp}$.

Definition

The **symplectic weight** of a codeword is
$\mathrm{wt_s}(a, b) := |\{i \mid (a_i, b_i) \neq (0, 0)\}|$.

Stabilizer Codes

Definition

A submodule $C \leq R^{2n}$ is called a **stabilizer code** if there exists a stabilizer group S such that $C = \Psi(S)$.

Theorem (Gluesing-Luerssen/P, 2017)

A submodule $C \leq R^{2n}$ is a stabilizer code iff $C \subseteq C^{\perp}$.

Definition

The **symplectic weight** of a codeword is
$\mathrm{wt_s}(a, b) := |\{i \mid (a_i, b_i) \neq (0, 0)\}|$.
The minimum distance of a stabilizer code is

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

Outline

Symplectic Isometries

Symplectic Isometries

Let $A \leq R^{2n}$ be a submodule. A linear map $f : A \to R^{2n}$ is called a **symplectic isometry** if for all $x, y \in R^{2n}$

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

Symplectic Isometries

Let $A \leq R^{2n}$ be a submodule. A linear map $f : A \to R^{2n}$ is called a **symplectic isometry** if for all $x, y \in R^{2n}$

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

Example

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

Symplectic Isometries

Let $A \leq R^{2n}$ be a submodule. A linear map $f : A \to R^{2n}$ is called a **symplectic isometry** if for all $x, y \in R^{2n}$

$$\mathrm{wt}_s(x) = \mathrm{wt}_s(f(x)) \text{ and } \langle x \mid y \rangle_s = \langle f(x) \mid f(y) \rangle_s.$$

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 R^{2n}

Symplectic Isometries of R^{2n}

Question

What is the structure of symplectic isometries of R^{2n}?

Symplectic Isometries of R^{2n}

Question

What is the structure of symplectic isometries of R^{2n}?

- To answer this question we transfer the problem on $(R^2)^n$ via the change of coordinates

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

Symplectic Isometries of R^{2n}

Question

What is the structure of symplectic isometries of R^{2n}?

- To answer this question we transfer the problem on $(R^2)^n$ via the change of coordinates

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

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

Symplectic Isometries of R^{2n}

Question

What is the structure of symplectic isometries of R^{2n}?

- To answer this question we transfer the problem on $(R^2)^n$ via the change of coordinates

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

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

Symplectic Isometries of R^{2n}

Question

What is the structure of symplectic isometries of R^{2n}?

- To answer this question we transfer the problem on $(R^2)^n$ via the change of coordinates

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

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

Symplectic Isometries of R^{2n}

Theorem (Gluesing-Luerssen/P, 2017)

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

Symplectic Isometries of R^{2n}

Theorem (Gluesing-Luerssen/P, 2017)

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

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

for $A_i \in SL_2(R)$.

Symplectic Isometries of R^{2n}

Theorem (Gluesing-Luerssen/P, 2017)

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

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

for $A_i \in SL_2(R)$.

Symplectic Isometries of R^{2n}

Theorem (Gluesing-Luerssen/P, 2017)

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

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

for $A_i \in SL_2(R)$.

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

Symplectic Isometries of R^{2n}

Theorem (Gluesing-Luerssen/P, 2017)

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

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

for $A_i \in SL_2(R)$.

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

Question

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

Symplectic Isometries of R^{2n}

Theorem (Gluesing-Luerssen/P, 2017)

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

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

for $A_i \in SL_2(R)$.

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

Question

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

- Although this question is interesting for submodule $A \leq R^{2n}$, we are interested on stabilizer codes.

Symplectic Isometries of Stabilizer Codes

Let $C \leq R^{2n}$ be a stabilizer code. We define two groups:

Symplectic Isometries of Stabilizer Codes

Let $C \leq R^{2n}$ be a stabilizer code. We define two groups:

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

Symplectic Isometries of Stabilizer Codes

Let $C \leq R^{2n}$ be a stabilizer code. We define two groups:

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

Symplectic Isometries of Stabilizer Codes

Let $C \leq R^{2n}$ be a stabilizer code. We define two groups:

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

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

Symplectic Isometries of Stabilizer Codes

Let $C \leq R^{2n}$ be a stabilizer code. We define two groups:

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

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

Symplectic Isometries of Stabilizer Codes

Let $C \leq R^{2n}$ be a stabilizer code. We define two groups:

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

- $\mathrm{Mon}_{\mathrm{SL}}(C) \subseteq \mathrm{Symp}(C)$.
  - **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 $C \leq R^{2n}$ be a stabilizer code. We define two groups:

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

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

Symplectic Isometries of Stabilizer Codes

Let $C \leq R^{2n}$ be a stabilizer code. We define two groups:

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

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

Open Problem

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

Theorem (P, 2018)

For any groups $H \leq K$ **that satisfy some necessary conditions** *there exists a stabilizer code such that* $H = \mathrm{Mon}_{\mathrm{S}L}(C)$ *and* $G = \mathrm{Symp}(C)$.

Outline

Minimum distance of a Stabilizer Code

Minimum distance of a Stabilizer Code

- Let R be a local Frobenius ring with maximal ideal $\mathfrak{m}$, and $k := R/\mathfrak{m}$ the residue field.

Minimum distance of a Stabilizer Code

- Let R be a local Frobenius ring with maximal ideal $\mathfrak{m}$, and $k := R/\mathfrak{m}$ the residue field.
- Let $C \leq R^{2n}$ be a *free* stabilizer code. Denote $\overline{C} \leq k^{2n}$ coordinate-wise projection of C onto k.

Minimum distance of a Stabilizer Code

- Let R be a local Frobenius ring with maximal ideal $\mathfrak{m}$, and $k := R/\mathfrak{m}$ the residue field.
- Let $C \leq R^{2n}$ be a *free* stabilizer code. Denote $\overline{C} \leq k^{2n}$ coordinate-wise projection of C onto k.
  - $\overline{C}$ is a stabilizer code over k.

Minimum distance of a Stabilizer Code

- Let R be a local Frobenius ring with maximal ideal $\mathfrak{m}$, and $k := R/\mathfrak{m}$ the residue field.
- Let $C \leq R^{2n}$ be a *free* stabilizer code. Denote $\overline{C} \leq k^{2n}$ coordinate-wise projection of C onto k.
  - $\overline{C}$ is a stabilizer code over k.

Theorem (Gluesing-Luerssen/P, 2017)

$\text{dist}(C) \leq \text{dist}(\overline{C})$

Minimum distance of a Stabilizer Code

- Let R be a local Frobenius ring with maximal ideal $\mathfrak{m}$, and $k := R/\mathfrak{m}$ the residue field.
- Let $C \leq R^{2n}$ be a *free* stabilizer code. Denote $\overline{C} \leq k^{2n}$ coordinate-wise projection of C onto k.
  - $\overline{C}$ is a stabilizer code over k.

Theorem (Gluesing-Luerssen/P, 2017)

$\mathrm{dist}(C) \leq \mathrm{dist}(\overline{C})$

- The theorem says that stabilizer codes over local Frobenius rings cannot over-perform stabilizer codes over fields.

Minimum distance of a Stabilizer Code

- Let R be a local Frobenius ring with maximal ideal $\mathfrak{m}$, and $k := R/\mathfrak{m}$ the residue field.
- Let $C \leq R^{2n}$ be a *free* stabilizer code. Denote $\overline{C} \leq k^{2n}$ coordinate-wise projection of C onto k.
  - $\overline{C}$ is a stabilizer code over k.

Theorem (Gluesing-Luerssen/P, 2017)

$\mathrm{dist}(C) \leq \mathrm{dist}(\overline{C})$

- The theorem says that stabilizer codes over local Frobenius rings cannot over-perform stabilizer codes over fields.
- When $C = C^{\perp}$ we have equality.

Minimum distance of a Stabilizer Code

- Let R be a local Frobenius ring with maximal ideal $\mathfrak{m}$, and $k := R/\mathfrak{m}$ the residue field.
- Let $C \leq R^{2n}$ be a *free* stabilizer code. Denote $\overline{C} \leq k^{2n}$ coordinate-wise projection of C onto k.
  - $\overline{C}$ is a stabilizer code over k.

Theorem (Gluesing-Luerssen/P, 2017)

$\mathrm{dist}(C) \leq \mathrm{dist}(\overline{C})$

- The theorem says that stabilizer codes over local Frobenius rings cannot over-perform stabilizer codes over fields.
- When $C = C^{\perp}$ we have equality.
- When $C \subsetneq C^{\perp}$, we don't know.

Minimum distance of a Stabilizer Code

- Let R be a local Frobenius ring with maximal ideal $\mathfrak{m}$, and $k := R/\mathfrak{m}$ the residue field.
- Let $C \leq R^{2n}$ be a *free* stabilizer code. Denote $\overline{C} \leq k^{2n}$ coordinate-wise projection of C onto k.
  - $\overline{C}$ is a stabilizer code over k.

Theorem (Gluesing-Luerssen/P, 2017)

$\mathrm{dist}(C) \leq \mathrm{dist}(\overline{C})$

- The theorem says that stabilizer codes over local Frobenius rings cannot over-perform stabilizer codes over fields.
- When $C = C^{\perp}$ we have equality.
- When $C \subsetneq C^{\perp}$, we don't know. However, computational and theoretical data suggest that equality still holds.

Minimum distance of a Stabilizer Code

Conjecture

Let C be a free stabilizer code. Then $\mathrm{dist}(C) = \mathrm{dist}(\overline{C})$.

Thank You!