(On Quantum) Stabilizer Codes over Local Frobenius Rings

Tefjol Pllaha

Department of Mathematics
University of Kentucky

Joint Mathematics Meetings 2018
San Diego, CA
January 12, 2018

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

Stabilizer Codes

- For any $n \in \mathbb{N}$, the map $\langle \cdot \mid \cdot \rangle_{\mathrm{s}} : R^{2n} \times R^{2n} \to R$ defined as
$$\langle (a, b) \mid (a', b') \rangle_{\mathrm{s}} := b \cdot a' - b' \cdot a$$
is a non-degenerate, symplectic, bilinear form.

Stabilizer Codes

- 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 $A \subseteq R^{2n}$, $A^{\perp} := \{x \in R^{2n} \mid \langle x \mid A \rangle_s = 0\}$.

Stabilizer Codes

- 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 $A \subseteq R^{2n}$, $A^\perp := \{x \in R^{2n} \mid \langle x \mid A \rangle_s = 0\}$.

Definition

A submodule $C \leq R^{2n}$ is called a **stabilizer code** (of length n) if $C \subseteq C^\perp$.

Stabilizer Codes

- 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 $A \subseteq R^{2n}$, $A^\perp := \{x \in R^{2n} \mid \langle x \mid A \rangle_s = 0\}$.

Definition

A submodule $C \leq R^{2n}$ is called a **stabilizer code** (of length n) if $C \subseteq C^\perp$.

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

Stabilizer Codes

- 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 $A \subseteq R^{2n}$, $A^{\perp} := \{x \in R^{2n} \mid \langle x \mid A \rangle_s = 0\}$.

Definition

A submodule $C \leq R^{2n}$ is called a **stabilizer code** (of length n) if $C \subseteq C^{\perp}$.
The **symplectic weight** 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 $x, y \in R^{2n}$

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

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 $x, y \in R^{2n}$

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

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 $x, y \in R^{2n}$

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

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 R^{2n}

Symplectic Isometries of R^{2n}

Question

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

Symplectic Isometries of R^{2n}

Question

What is the structure of 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 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 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, $\mathrm{wt_H}(x) = \mathrm{wt_s}(\gamma^{-1}(x))$ 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 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)

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)

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)

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)

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)

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)

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:

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

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:

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

- $\mathrm{Mon}_{\mathrm{SL}}(C) \subseteq \mathrm{Symp}(C)$.
  - **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.
- Computing $\mathrm{Symp}(C)$ is unrealistic in general. An easier question is the following.

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.
- Computing $\mathrm{Symp}(C)$ is unrealistic 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?

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)

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

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)

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

- 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)

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

- 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)

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

- 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)

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

- 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

Stabilizer codes over local Frobenius rings perform as good as stabilizer codes over fields.

Thank You!