Self-Dual Codes over Commutative and Non-Commutative Frobenius Rings

Steven T. Dougherty

June 16, 2014

Introduction

A code is a subset of A^n where A is any alphabet.

Introduction

A code is a subset of A^n where A is any alphabet.

Initially, A was a field, but now in general A can be a variety of algebraic structures.

Introduction

A code is a subset of A^n where A is any alphabet.

Initially, A was a field, but now in general A can be a variety of algebraic structures.

If A is a ring then we say that the code C is linear if C is s submodule of R^n.

Introduction

A code is a subset of A^n where A is any alphabet.

Initially, A was a field, but now in general A can be a variety of algebraic structures.

If A is a ring then we say that the code C is linear if C is s submodule of R^n.

For non-commutative rings we say it is either left linear or right linear depending on whether it is a left or right module.

Inner-product

The ambient space is attached with the inner-product:

$$[\mathbf{v}, \mathbf{w}] = \sum v_i w_i$$

Inner-product

The ambient space is attached with the inner-product:

$$[\mathbf{v}, \mathbf{w}] = \sum v_i w_i$$

For commutative rings there is a unique orthogonal:

$$C^{\perp} = \{\mathbf{v} \mid [\mathbf{v}, \mathbf{w}] = 0,\ \forall \mathbf{w} \in C\}.$$

Non-commutative orthogonals

For non-commutative rings we have two orthogonals:

$$\mathcal{L}(C) = \{\mathbf{v} \in R^n \mid [\mathbf{v}, \mathbf{c}] = 0, \forall \mathbf{c} \in C\}$$

Non-commutative orthogonals

For non-commutative rings we have two orthogonals:

$$\mathcal{L}(C) = \{\mathbf{v} \in R^n \mid [\mathbf{v}, \mathbf{c}] = 0, \forall \mathbf{c} \in C\}$$

$$\mathcal{R}(C) = \{\mathbf{v} \in R^n \mid [\mathbf{c}, \mathbf{v}] = 0, \forall \mathbf{c} \in C\}.$$

Non-commutative orthogonals

For non-commutative rings we have two orthogonals:

$$\mathcal{L}(C) = \{\mathbf{v} \in R^n \mid [\mathbf{v}, \mathbf{c}] = 0, \forall \mathbf{c} \in C\}$$

$$\mathcal{R}(C) = \{\mathbf{v} \in R^n \mid [\mathbf{c}, \mathbf{v}] = 0, \forall \mathbf{c} \in C\}.$$

Lemma

Let C be a code, then $\mathcal{L}(C)$ is a left linear code and $\mathcal{R}(C)$ is a right linear code.

Weight Enumerator

For a code over an alphabet $A = \{a_0, a_1, \ldots, a_{s-1}\}$, the complete weight enumerator is defined as:

$$cwe_C(x_{a_0}, x_{a_1}, \ldots, x_{a_{s-1}}) = \sum_{\mathbf{c} \in C} \prod_{i=0}^{s-1} x_{a_i}^{n_i(\mathbf{c})} \tag{1}$$

where there are $n_i(\mathbf{c})$ occurrences of a_i in the vector $\mathbf{c}$.

Weight Enumerator

For a code over an alphabet $A = \{a_0, a_1, \ldots, a_{s-1}\}$, the complete weight enumerator is defined as:

$$cwe_C(x_{a_0}, x_{a_1}, \ldots, x_{a_{s-1}}) = \sum_{\mathbf{c} \in C} \prod_{i=0}^{s-1} x_{a_i}^{n_i(\mathbf{c})} \tag{1}$$

where there are $n_i(\mathbf{c})$ occurrences of a_i in the vector $\mathbf{c}$.
The Hamming weight enumerator of a code C of length n is defined to be

$$W_C(x, y) = \sum_{\mathbf{c} \in C} x^{n - wt(\mathbf{c})} y^{wt(\mathbf{c})},$$

where $wt(\mathbf{c}) = |\{i \mid c_i \neq 0\}|$.

MacWilliams Relations

If R is a Frobenius ring then it has a generating character χ. Then let T be the square matrix indexed by the elements of R.

$$T_{a,b} = \chi(ab).$$

MacWilliams Relations

Theorem

(Generalized MacWilliams Relations) Let R be a Frobenius ring. If C is a left submodule of R^n, then

$$cwe_C(x_0, x_1, \ldots, x_k) = \frac{1}{|\mathcal{R}(C)|} cwe_{\mathcal{R}(C)}(T^t \cdot (x_0, x_1, \ldots, x_k)).$$

If C is a right submodule of R^n, then

$$cwe_C(x_0, x_1, \ldots, x_k) = \frac{1}{|\mathcal{L}(C)|} cwe_{\mathcal{L}(C)}(T \cdot (x_0, x_1, \ldots, x_k)).$$

MacWilliams Relations

Theorem

(Generalized MacWilliams Relations) Let R be a Frobenius ring. For the Hamming weight enumerator we have the following. If C is a left submodule of R^n, then

$$W_C(x,y) = \frac{1}{|\mathcal{R}(C)|} W_{\mathcal{R}(C)}(x + (|R| - 1)y, x - y)).$$

If C is a right submodule of R^n, then

$$W_C(x,y) = \frac{1}{|\mathcal{L}(C)|} W_{\mathcal{L}(C)}(x + (|R| - 1)y, x - y)).$$

Orthogonals

Lemma

If C is a left linear code then $|\mathcal{R}(C)||C| = |R|^n$. If C is a right linear code then $|\mathcal{L}(C)||C| = |R|^n$. For commutative rings $|C||C^{\perp}| = |R|^n$.

Self-Dual

A code over a commutative ring is self-dual if $C = C^{\perp}$.

Self-Dual

A code over a commutative ring is self-dual if $C = C^{\perp}$.

A code over a non-commutative ring is self-dual if $C = \mathcal{L}(C)$.

Self-dual codes

Self-dual codes have connections to:

- Finite Designs
- Unimodular Lattices
- Invariant Theory

Direct Product

Lemma

Let R be a finite Frobenius ring. Let C be a self-dual code of length n over R and D be a self-dual code of length m over R. Then the direct product $C \times D$ is a self-dual code of length $n + m$ over R.

Commutative Case

Theorem

Let R be a finite Frobenius ring and n be a positive integer. Then

$$R^n = CRT(R_1^n, R_2^n, \ldots, R_k^n),$$

where each R_i is a local Frobenius ring.

Commutative Case

Theorem

Let R be a finite Frobenius ring and n be a positive integer. Then

$$R^n = CRT(R_1^n, R_2^n, \ldots, R_k^n),$$

where each R_i is a local Frobenius ring.

Let R be a finite ring with the local rings R_i for $1 \leq i \leq k$. Let C_i be a code of length n over R_i for $1 \leq i \leq k$, and let $C = CRT(C_1, C_2, \ldots, C_k)$.

Commutative Case

Theorem

Let R be a finite Frobenius ring with a local Frobenius ring R_i for $1 \leq i \leq k$. If C_i is a self-dual code over R_i, then $C = CRT(C_1, C_2, \ldots, C_k)$ is a self-dual code over R.

Existence of self-dual codes over Commutative Rings

Theorem

Let R be a finite Frobenius local ring with maximal ideal $\mathfrak{m}$ and nilpotency index e with the property that $(\mathfrak{m}^i)^\perp = \mathfrak{m}^{e-i}$ for $i = 1, \ldots, e$. If e is even, then there are self-dual codes over R of all lengths.

Existence of self-dual codes over Commutative Rings

Theorem

Let R be a finite Frobenius local ring with maximal ideal $\mathfrak{m}$ such that char$(|R/\mathfrak{m}) \equiv 1 \pmod 4$. Then there exist free self-dual codes over R of all even lengths.

Existence of self-dual codes over Commutative Rings

Theorem

Let R be a finite Frobenius local ring with maximal ideal $\mathfrak{m}$ such that $char(R/\mathfrak{m}) \equiv 3 \pmod 4$. Then there exist self-dual codes over R of all lengths a multiple of 4.

Self-duality over non-commutative rings

Lemma

If C is a left linear code then $\mathcal{L}(\mathcal{R}(C)) = C$. If C is a right linear code then $\mathcal{R}(\mathcal{L}(C)) = C$.

Self-duality over non-commutative rings

Theorem

If $C \subseteq \mathcal{L}(C)$ *then* $C \subseteq \mathcal{R}(C)$ *and if* $C \subseteq \mathcal{R}(C)$ *then* $C \subseteq \mathcal{L}(C)$.

Self-duality over non-commutative rings

Theorem

If $C = \mathcal{L}(C)$ *then* $C = \mathcal{R}(C)$. *If* $C = \mathcal{R}(C)$ *then* $C = \mathcal{L}(C)$.

Self-duality over non-commutative rings

It follows immediately that if C is a self-dual code then C is both left linear and right linear. That is, it is a bimodule.

Self-dual codes of length 1

Let R be a ring, the Jacobson radical $J(R)$ consists of all annihilators of simple left R-modules. The Jacobson radical can be characterized as the intersection of all maximal right ideals.

Self-dual codes of length 1

Let R be a ring, the Jacobson radical $J(R)$ consists of all annihilators of simple left R-modules. The Jacobson radical can be characterized as the intersection of all maximal right ideals.

For any ring R, we define the center of the ring $Z(R)$ to be $\{\alpha \mid \alpha \in R, \alpha\beta = \beta\alpha, \forall \beta \in R\}$.

Self-dual codes of length 1

Let R be a ring, the Jacobson radical $J(R)$ consists of all annihilators of simple left R-modules. The Jacobson radical can be characterized as the intersection of all maximal right ideals.

For any ring R, we define the center of the ring $Z(R)$ to be $\{\alpha \mid \alpha \in R, \alpha\beta = \beta\alpha, \forall \beta \in R\}$.

The socle of a ring R, $Soc(R)$, is defined as the sum of all the minimal one sided ideals of the ring. For Frobenius rings, the sum of all the minimal left ideals is equal to the sum of all the minimal right ideals. In this case, the socle is equal the left annihilator of the Jacobson radical.

Self-dual codes of length 1

Theorem

Let R be a finite Frobenius ring with Jacobson radical $J(R)$. All self-dual codes of length 1 are two sided ideals contained in the Jacobson radical of the ring. Then $J(R)$ is a self-dual code if and only if $J(R) = Soc(R)$ and in this case there are no other self-dual codes of length 1.

Existence of self-dual codes over non-commutative rings

Theorem

Let R be a finite ring such that there exists x and y in $Z(R)$ with $x^2 + y^2 = 0$ and $ann_R(x, y) = \{0\}$. Then there exists free self-dual codes of all even lengths over R.

Existence of self-dual codes over non-commutative rings

Theorem

Let R be a finite ring such that there exists x, y and z in $Z(R)$ with $x^2 + y^2 + z^2 = 0$ and $ann_R(x, y, z) = \{0\}$. Then there exists free self-dual codes of all lengths congruent to $0 \mod 4$ *over R.*

Existence of self-dual codes over non-commutative rings

Theorem

Let R and $A \subseteq Z(R)$ be finite Frobenius rings where R is a free module over A. If C is a self-dual code over A then $\langle C \rangle_L$ is a self-dual code.

Existence of self-dual codes over non-commutative rings

Theorem

Let R be a finite Frobenius ring of characteristic k. If there exists a free self-dual code of length n over $\mathbb{Z}_k$ then there exists a free self-dual code of length n over R.