Formally Self-Dual Codes and Gray Maps

Steven T. Dougherty

May 24, 2012

Introduction

- Linear code of length n – submodule of R^n

Introduction

- Linear code of length n – submodule of R^n
- $[\mathbf{v}, \mathbf{w}] = \sum \mathbf{v}_i \overline{\mathbf{w}_i}$

Introduction

- Linear code of length n – submodule of R^n
- $[\mathbf{v}, \mathbf{w}] = \sum \mathbf{v}_i \overline{\mathbf{w}_i}$
- $C^\perp = \{\mathbf{v} \mid [\mathbf{v}, \mathbf{w}] = 0, \ \forall \mathbf{w} \in C\}$

Introduction

- R Frobenius $\Rightarrow |C||C^{\perp}| = |R|^n$.

Introduction

- R Frobenius $\Rightarrow |C||C^\perp| = |R|^n$.
- $C = C^\perp$ the code is self-dual.

Introduction

- R Frobenius $\Rightarrow |C||C^\perp| = |R|^n$.
- $C = C^\perp$ the code is self-dual.
- $W_C(y) = \sum_{\mathbf{c}\in C} y^{wt(\mathbf{c})}$.

Introduction

- R Frobenius $\Rightarrow |C||C^{\perp}| = |R|^n$.
- $C = C^{\perp}$ the code is self-dual.
- $W_C(y) = \sum_{\mathbf{c} \in C} y^{wt(\mathbf{c})}$.
- $W_C(y) = W_{C^{\perp}}(y)$ the code is formally self-dual.

Rings

- $\mathbb{Z}_4 = \{0, 1, 2, 3\}$

Rings

- $\mathbb{Z}_4 = \{0, 1, 2, 3\}$
- $R_k = \mathbb{F}_2[u_1, u_2, \ldots, u_k]/\langle u_i^2 = 0, u_i u_j = u_j u_i \rangle$

Rings

- $\mathbb{Z}_4 = \{0, 1, 2, 3\}$
- $R_k = \mathbb{F}_2[u_1, u_2, \ldots, u_k]/\langle u_i^2 = 0, u_i u_j = u_j u_i \rangle$
- $A_k = \mathbb{F}_2[v_1, v_2, \ldots, v_k]/\langle v_i^2 = v_i, v_i v_j = v_j v_i \rangle$

Gray Maps

$$\phi_{\mathbb{Z}_4} : \mathbb{Z}_4 \to \mathbb{F}_2^2$$

$$\begin{aligned}
\phi_{\mathbb{Z}_4}(0) &= (00) \\
\phi_{\mathbb{Z}_4}(1) &= (01) \\
\phi_{\mathbb{Z}_4}(2) &= (11) \\
\phi_{\mathbb{Z}_4}(3) &= (10)
\end{aligned}$$

Gray Maps

$$\phi_{R_1}(a + bu_1) = (b, a + b)$$

$$\phi_{R_k}(a + bu_k) = (\phi_{R_{k-1}}(b), \phi_{R_{k-1}}(a) + \phi_{R_{k-1}}(b))$$

Gray Maps

$$\phi_{A_1}(a + bv_1) = (a, a + b)$$

$$\phi_{A_k}(a + bu_k) = (\phi_{A_{k-1}}(a), \phi_{A_{k-1}}(a) + \phi_{A_{k-1}}(b))$$

Gray Maps

$$\phi_{A_1}(a + bv_1) = (a, a + b)$$

$$\phi_{A_k}(a + bu_k) = (\phi_{A_{k-1}}(a), \phi_{A_{k-1}}(a) + \phi_{A_{k-1}}(b))$$

The maps ϕ_{R_k} and ϕ_{A_k} are linear but the map $\phi_{\mathbb{Z}_4}$ is not.

Gray Maps

$$\phi_{A_1}(a + bv_1) = (a, a + b)$$

$$\phi_{A_k}(a + bu_k) = (\phi_{A_{k-1}}(a), \phi_{A_{k-1}}(a) + \phi_{A_{k-1}}(b))$$

The maps ϕ_{R_k} and ϕ_{A_k} are linear but the map $\phi_{\mathbb{Z}_4}$ is not.
The Lee weight is the Hamming weight of its binary image.

Inner Products

Over A_k, the Euclidean inner product is:

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

and the Hermitian is

$$[\mathbf{v}, \mathbf{w}]_H = \sum \mathbf{v}_i \overline{\mathbf{w}_i}$$

where $\overline{v_i} = 1 + v_i$.

Theorem

If C is a formally self-dual code over $\mathbb{Z}_4, R_k$ or A_k then the image under the corresponding Gray map is a binary formally self-dual code.

Major Result

Theorem

Let C be an odd formally self-dual binary code of even length n. Let C_0 be the subcode of even vectors. The code $\overline{C} = \langle \{(0,0,\mathbf{c}) \mid \mathbf{c} \in C_0\} \cup \{(1,0,\mathbf{c}) \mid \mathbf{c} \in C - C_0\}, (1,1,\mathbf{1})\rangle$ is an even formally self-dual code of length $n+2$ with weight enumerator $W_{\overline{C}} = x^2 W_{C_{0,0}}(x,y) + xyW_{C_{1,0}}(x,y) + y^2 W_{C_{0,0}}(y,x) + xyW_{C_{1,0}}(y,x)$. The code $\overline{C} = \langle \{(0,0,\mathbf{c}) \mid \mathbf{c} \in C_0\} \cup \{(1,1,\mathbf{c}) \mid \mathbf{c} \in C - C_0\}, (1,0,\mathbf{1})\rangle$ is an odd formally self-dual code of length $n+2$ with weight enumerator: $W_{\overline{C}} = x^2 W_{C_{0,0}}(x,y) + y^2 W_{C_{1,0}}(x,y) + xyW_{C_{0,0}}(y,x) + xyW_{C_{1,0}}(y,x)$. Moreover, any code with these weight enumerators is a formally self-dual code.

Outline of Proof

- Let C be an odd formally self-dual code.
- There exists a vector $\mathbf{t}$ such that $C = \langle C_0, \mathbf{t} \rangle$, where C_0 is the subcode of even vectors.

Outline of Proof

- Let C be an odd formally self-dual code.
- There exists a vector $\mathbf{t}$ such that $C = \langle C_0, \mathbf{t} \rangle$, where C_0 is the subcode of even vectors.
- $C_{\alpha,\beta} = C_0 + \alpha\mathbf{t} + \beta\mathbf{1}$.

Outline of Proof

- Let C be an odd formally self-dual code.
- There exists a vector $\mathbf{t}$ such that $C = \langle C_0, \mathbf{t} \rangle$, where C_0 is the subcode of even vectors.
- $C_{\alpha,\beta} = C_0 + \alpha\mathbf{t} + \beta\mathbf{1}$.
- $C^{\perp} = D$ and let D_0 be the subcode of D of even vectors.

Outline of Proof

- Let C be an odd formally self-dual code.
- There exists a vector $\mathbf{t}$ such that $C = \langle C_0, \mathbf{t} \rangle$, where C_0 is the subcode of even vectors.
- $C_{\alpha,\beta} = C_0 + \alpha\mathbf{t} + \beta\mathbf{1}$.
- $C^\perp = D$ and let D_0 be the subcode of D of even vectors.
- There exists a vector $\mathbf{t}'$ such that $D = \langle D_0, \mathbf{t}' \rangle$.

Outline of Proof

- Let C be an odd formally self-dual code.
- There exists a vector $\mathbf{t}$ such that $C = \langle C_0, \mathbf{t} \rangle$, where C_0 is the subcode of even vectors.
- $C_{\alpha,\beta} = C_0 + \alpha\mathbf{t} + \beta\mathbf{1}$.
- $C^{\perp} = D$ and let D_0 be the subcode of D of even vectors.
- There exists a vector $\mathbf{t}'$ such that $D = \langle D_0, \mathbf{t}' \rangle$.
- $D_{\alpha,\beta} = D_0 + \alpha\mathbf{t}' + \beta\mathbf{1}$.

Outline of Proof

- $\overline{C} = \bigcup (v_{\alpha,\beta}, C_{\alpha,\beta})$

Outline of Proof

- $\overline{C} = \bigcup (v_{\alpha,\beta}, C_{\alpha,\beta})$
- $\overline{D} = \bigcup (w_{\alpha,\beta}, D_{\alpha,\beta})$

Outline of Proof

- $\overline{C} = \bigcup (v_{\alpha,\beta}, C_{\alpha,\beta})$
- $\overline{D} = \bigcup (w_{\alpha,\beta}, D_{\alpha,\beta})$
- We need $[v_{\alpha,\beta}, w_{\alpha',\beta'}] = [C_{\alpha,\beta}, D_{\alpha,\beta}]$.

Outline of Proof

- $\overline{C} = \bigcup(v_{\alpha,\beta}, C_{\alpha,\beta})$
- $\overline{D} = \bigcup(w_{\alpha,\beta}, D_{\alpha,\beta})$
- We need $[v_{\alpha,\beta}, w_{\alpha',\beta'}] = [C_{\alpha,\beta}, D_{\alpha,\beta}]$.
- To insure linearity we need $v_{\alpha,\beta} = \alpha v_{1,0} + \beta v_{0,1}$ and $w_{\alpha,\beta} = \alpha w_{1,0} + \beta w_{0,1}$.

Outline of Proof

- $\overline{C} = \bigcup(v_{\alpha,\beta}, C_{\alpha,\beta})$
- $\overline{D} = \bigcup(w_{\alpha,\beta}, D_{\alpha,\beta})$
- We need $[v_{\alpha,\beta}, w_{\alpha',\beta'}] = [C_{\alpha,\beta}, D_{\alpha,\beta}]$.
- To insure linearity we need $v_{\alpha,\beta} = \alpha v_{1,0} + \beta v_{0,1}$ and $w_{\alpha,\beta} = \alpha w_{1,0} + \beta w_{0,1}$.
- $v_{1,0} = (1,0)$, $v_{0,1} = (1,1)$ and $w_{1,0} = (0,1)$, $v_{0,1} = (1,1)$

Outline of Proof

- $\overline{C} = \bigcup(v_{\alpha,\beta}, C_{\alpha,\beta})$
- $\overline{D} = \bigcup(w_{\alpha,\beta}, D_{\alpha,\beta})$
- We need $[v_{\alpha,\beta}, w_{\alpha',\beta'}] = [C_{\alpha,\beta}, D_{\alpha,\beta}]$.
- To insure linearity we need $v_{\alpha,\beta} = \alpha v_{1,0} + \beta v_{0,1}$ and $w_{\alpha,\beta} = \alpha w_{1,0} + \beta w_{0,1}$.
- $v_{1,0} = (1,0)$, $v_{0,1} = (1,1)$ and $w_{1,0} = (0,1)$, $v_{0,1} = (1,1)$
- $W_{\overline{C}} = W_{\overline{D}} = x^2 W_{C_{0,0}}(x,y) + xyW_{C_{1,0}}(x,y) + y^2 W_{C_{0,0}}(y,x) + xyW_{C_{1,0}}(y,x)$.

Outline of Proof

- $\overline{C} = \bigcup(v_{\alpha,\beta}, C_{\alpha,\beta})$
- $\overline{D} = \bigcup(w_{\alpha,\beta}, D_{\alpha,\beta})$
- We need $[v_{\alpha,\beta}, w_{\alpha',\beta'}] = [C_{\alpha,\beta}, D_{\alpha,\beta}]$.
- To insure linearity we need $v_{\alpha,\beta} = \alpha v_{1,0} + \beta v_{0,1}$ and $w_{\alpha,\beta} = \alpha w_{1,0} + \beta w_{0,1}$.
- $v_{1,0} = (1, 0)$, $v_{0,1} = (1, 1)$ and $w_{1,0} = (0, 1)$, $v_{0,1} = (1, 1)$
- $W_{\overline{C}} = W_{\overline{D}} = x^2 W_{C_{0,0}}(x, y) + xyW_{C_{1,0}}(x, y) + y^2 W_{C_{0,0}}(y, x) + xyW_{C_{1,0}}(y, x)$.
- $\overline{C}$ and $\overline{D}$ are formally self-dual

Odd formally self-dual codes

- There exist odd formally self-dual codes of all lengths over A_k for all k.

Odd formally self-dual codes

- There exist odd formally self-dual codes of all lengths over A_k for all k.
- Linear odd formally self-dual codes exist over $\mathbb{Z}_4$ and R_k for all lengths greater than 1.

Formally self-dual codes

Let $\mathbf{2}$ be the all 2 vector in $\mathbb{Z}_4^n$, $\mathbf{u_1 u_2 \ldots u_k}$ be the all $u_1 u_2 \ldots u_k$ vector in R_k^n and $\mathbf{1}$ be the all one-vector (over any ring). Note that the Gray image of these vectors is the binary all-one vector.

Formally self-dual codes

Let $\mathbf{2}$ be the all 2 vector in $\mathbb{Z}_4^n$, $\mathbf{u_1 u_2 \ldots u_k}$ be the all $u_1 u_2 \ldots u_k$ vector in R_k^n and $\mathbf{1}$ be the all one-vector (over any ring). Note that the Gray image of these vectors is the binary all-one vector.

Theorem

Let C be a formally self-dual code. The code C is even over $\mathbb{Z}_4$ if and only if $\mathbf{2} \in C$. The code C is even over R_k if and only if $\mathbf{u_1 u_2 \ldots u_k} \in C$. The code C is even over A_k if and only if $\mathbf{1} \in C$.

Formally self-dual codes

Theorem

Let C be an odd formally self-dual code over A_k or $\mathbb{Z}_4$ of length n. Then C is a neighbor of an even formally self-dual code.

Importance of these codes

- Formally self-dual codes over R_k produce binary formally self-dual codes that have k distinct automorphisms

Importance of these codes

- Formally self-dual codes over R_k produce binary formally self-dual codes that have k distinct automorphisms
- Formally self-dual codes over $\mathbb{Z}_4$ produce non-linear formally self-dual codes which may have higher minimum distance than any linear formally self-dual codes.

Importance of these codes

- Formally self-dual codes over R_k produce binary formally self-dual codes that have k distinct automorphisms
- Formally self-dual codes over $\mathbb{Z}_4$ produce non-linear formally self-dual codes which may have higher minimum distance than any linear formally self-dual codes.
- A formally self-dual code over A_k can be constructed using any 2^{k-1} binary codes.