Self-Dual Codes over Chain Rings

Simon Eisenbarth, Gabriele Nebe

RWTH Aachen University

20th of June, 2018

PhD-student of Prof. Nebe, RWTH Aachen University (since Oct. 2016)

Projects:

- $\mathbb{F}_p$-linear self-dual codes with an automorphism of order p (this talk)
- Extremal p-modular lattices with an automorphism of order p (current)
- (Relative) projective group ring codes over chain rings

Definitions and notation

A code C of length n over some finite field $\mathbb{F}$ is a subspace of $\mathbb{F}^n$.

Let $\overline{}$ be a field automorphism of order 1 or 2 and define

$$(v, w) := \sum_{i=1}^{n} v_i \overline{w_i}.$$

The dual code $C^\perp$ of C is the orthogonal space w.r.t. this inner product.

If $C = C^\perp$, then C is called (hermitian) self-dual.

Automorphism group of a code

Full Monomial group of a field: $\mathbb{F}^* \wr S_n$, acting on coordinates of $\mathbb{F}^n$ (permutation matrices with non-zero entries in $\mathbb{F}^*$ instead of 1)

Automorphism group of a code

Full Monomial group of a field: $\mathbb{F}^* \wr S_n$, acting on coordinates of $\mathbb{F}^n$ (permutation matrices with non-zero entries in $\mathbb{F}^*$ instead of 1)

Problem: this group doesn't preserve the inner product, especially self-duality.

Automorphism group of a code

Full Monomial group of a field: $\mathbb{F}^* \wr S_n$, acting on coordinates of $\mathbb{F}^n$ (permutation matrices with non-zero entries in $\mathbb{F}^*$ instead of 1)

Problem: this group doesn't preserve the inner product, especially self-duality.

Define

$$U := \{\alpha \in \mathbb{F} \mid \alpha\overline{\alpha} = 1\} \leq \mathbb{F}^* .$$

Then

$$|U| = \left\{ \begin{array}{cl} 1 & \text{if } \operatorname{char}(\mathbb{F}) = 2 \text{ and } ^- = id \\ 2 & \text{if } \operatorname{char}(\mathbb{F}) \neq 2 \text{ and } ^- = id \\ \sqrt{|\mathbb{F}|}+1 & \text{if } ^- \neq id \end{array} \right\}.$$

Let

$$\mathrm{Mon}_n(\mathbb{F}) := U \wr S_n,$$

then the automorphism group of a code C is

$$\mathrm{Aut}(C) := \{g \in \mathrm{Mon}_n(\mathbb{F}) \mid C \cdot g = C\}.$$

Let

$$\mathrm{Mon}_n(\mathbb{F}) := U \wr S_n,$$

then the automorphism group of a code C is

$$\mathrm{Aut}(C) := \{g \in \mathrm{Mon}_n(\mathbb{F}) \mid C \cdot g = C\}.$$

Every $g \in \mathrm{Mon}_n(\mathbb{F})$ has unique decomposition

$$g = \mathrm{diag}(\alpha_1, \ldots, \alpha_n)\pi(g),\ \pi(g) \in S_n,\ \alpha_i \in U$$

and the fixcode of g is

$$C(g) := \{c \in C \mid c \cdot g = c\}.$$

Remark

Let $g \in \mathrm{Mon}_n(\mathbb{F})$ be an element of order r such that $\gcd(r, |U|) = 1$. Then g is conjugate in $\mathrm{Mon}_n(\mathbb{F})$ to some element of S_n.

Theorem (MacWilliams, Mallos, Sloane, Ward, Rains)

Let C be a self-dual code in $\mathbb{F}_q^n$ with minimum distance d.

If $q = 2$ and C is even, then

$$d \leq \left\{ \begin{array}{ll} 4 \cdot \lfloor n/24 \rfloor + 4 & \text{if } n \neq 22 \pmod{24} \\ 4 \cdot \lfloor n/24 \rfloor + 6 & \text{if } n = 22 \pmod{24} \end{array} \right\}.$$

If $q = 2$ and C is doubly-even, then $d \leq 4 \cdot \lfloor n/24 \rfloor + 4$.

If $q = 3$, then $d \leq 3 \cdot \lfloor n/12 \rfloor + 3$.

If $q = 4$ and C is Hermitian self-dual, then $d \leq 2 \cdot \lfloor n/6 \rfloor + 2$.

Definition

Self-dual codes, which achieve those bounds are called extremal.

If a full classification of self-dual (resp. extremal) codes is not possible, one tries to classify those codes with given automorphisms.

If a full classification of self-dual (resp. extremal) codes is not possible, one tries to classify those codes with given automorphisms.

Theorem (Huffmann, 1992)

Let $C \leq \mathbb{F}_3^{36}$ be a ternary, extremal ($d = 12$) code of length 36 such that $|\mathrm{Aut}(C)|$ is divided by some prime $p \geq 5$. Then C is isomorphic to the Pless-Code P_{36}.

Theorem (Nebe, 2011)

Let $C \leq \mathbb{F}_3^{48}$ be a ternary, extremal ($d = 15$) code of length 48 such that $|\mathrm{Aut}(C)|$ is divided by some prime $p \geq 5$. Then C is isomorphic to the Pless-Code P_{48} or to the extended quadratic residue code Q_{48}.

Basic idea of the proofs:

Let C be an $\mathbb{F}$-linear code with an automorphism g of prime order $p \neq \mathrm{char}(\mathbb{F})$.

Decomposition theory of Huffman (1988)

Basic idea of the proofs:

Let C be an $\mathbb{F}$-linear code with an automorphism g of prime order $p \neq \mathrm{char}(\mathbb{F})$.

C is an $\mathbb{F}[g]$-module, this ring is isomorphic to $\mathbb{F}[x]/(x^p - 1)$ and is the direct sum of field extensions of $\mathbb{F}_q$

$\rightarrow$ C is the direct sum of linear codes over those field extension of smaller lengths.

Decomposition theory of Huffman (1988)

Basic idea of the proofs:

Let C be an $\mathbb{F}$-linear code with an automorphism g of prime order $p \neq \mathrm{char}(\mathbb{F})$.

C is an $\mathbb{F}[g]$-module, this ring is isomorphic to $\mathbb{F}[x]/(x^p - 1)$ and is the direct sum of field extensions of $\mathbb{F}_q$

$\rightarrow$ C is the direct sum of linear codes over those field extension of smaller lengths.

If C is self-dual: those subcodes are self-dual or pairs are dual to each other.

Decomposition theory of Huffman (1988)

Basic idea of the proofs:

Let C be an $\mathbb{F}$-linear code with an automorphism g of prime order $p \neq \mathrm{char}(\mathbb{F})$.

C is an $\mathbb{F}[g]$-module, this ring is isomorphic to $\mathbb{F}[x]/(x^p - 1)$ and is the direct sum of field extensions of $\mathbb{F}_q$

$\rightarrow$ C is the direct sum of linear codes over those field extension of smaller lengths.

If C is self-dual: those subcodes are self-dual or pairs are dual to each other.

What happens if $p = \mathrm{char}(\mathbb{F})$? (motivation: prove the Theorems for $p = 3$)

Let $C \leq \mathbb{F}^n$ be a self-dual code with an automorphism g of order $p = \mathrm{char}(\mathbb{F})$.

Let $C \leq \mathbb{F}^n$ be a self-dual code with an automorphism g of order $p = \mathrm{char}(\mathbb{F})$.

The group ring $\mathbb{F}[g] \cong \mathbb{F}[x]/(x^p)$ via $x \mapsto (1-g)$ is an Artinian chain ring with chain of ideals

$$\mathbb{F}[g] \supset \langle (1-g) \rangle \supset \langle (1-g)^2 \rangle \supset \cdots \supset \langle (1-g)^q \rangle = \{0\}.$$

Let $C \leq \mathbb{F}^n$ be a self-dual code with an automorphism g of order $p = \mathrm{char}(\mathbb{F})$.

The group ring $\mathbb{F}[g] \cong \mathbb{F}[x]/(x^p)$ via $x \mapsto (1-g)$ is an Artinian chain ring with chain of ideals

$$\mathbb{F}[g] \supset \langle (1-g) \rangle \supset \langle (1-g)^2 \rangle \supset \cdots \supset \langle (1-g)^q \rangle = \{0\}.$$

This chain gives raise to a chain of subcodes:

$$C \supset C \cdot (1-g) \supset C \cdot (1-g)^2 \supset \cdots \supset C \cdot (1-g)^q = \{0\}.$$

Theorem (E.)

Let $C \leq \mathbb{F}_3^n$ be a ternary, extremal code of length 36 resp. 48 and let $g \in \mathrm{Aut}(C)$ be of order 3. We can assume that

$$g = (1, 2, 3) \dots (3t - 2, 3t - 1, 3t)(3t + 1) \dots (n).$$

Then g has no fixpoints (i.e. $3t = n$) and C is a free a $\mathbb{F}_3[g]$-module, i.e. isomorphic to $\mathbb{F}_3[g]^6$ resp. to $\mathbb{F}_3[g]^8$.

If g acts without fixpoints on the coordinates, then the map

$$\mathbb{F}^n \to \mathbb{F}[g]^t, (c_1, \ldots, c_{pt}) \mapsto \left(\sum_{i=1}^{p} c_i g^{i-1}, \ldots, \sum_{i=1}^{p} c_{(t-1)p+i} g^{i-1} \right)$$

is a bijection between the self-dual codes in $\mathbb{F}^n$ and the self-dual codes in $\mathbb{F}[g]^t$ with respect to an inner product defined later.

(Example: $(0, 1, 2, 1, 1, 0) \mapsto (g + 2 \cdot g^2, 1 + g) \in \mathbb{F}_3[g]$).

If g acts without fixpoints on the coordinates, then the map

$$\mathbb{F}^n \to \mathbb{F}[g]^t, (c_1, \ldots, c_{pt}) \mapsto \left(\sum_{i=1}^{p} c_i g^{i-1}, \ldots, \sum_{i=1}^{p} c_{(t-1)p+i} g^{i-1} \right)$$

is a bijection between the self-dual codes in $\mathbb{F}^n$ and the self-dual codes in $\mathbb{F}[g]^t$ with respect to an inner product defined later.

(Example: $(0,1,2,1,1,0) \mapsto (g + 2 \cdot g^2, 1 + g) \in \mathbb{F}_3[g]$).

What is the structure of self-dual codes over chain rings?

Self-dual codes over chain rings

Let R be a commutative Artinian chain ring with 1 and let $^{-}: R \to R$ be an involution (i.e. automorphism of order 1 or 2).

Self-dual codes over chain rings

Let R be a commutative Artinian chain ring with 1 and let $^- : R \to R$ be an involution (i.e. automorphism of order 1 or 2).

Let $\mathfrak{m} \leq R$ denote the maximal ideal of R, then $^-$ induces an involution of the residue field $\mathbb{F} := R/\mathfrak{m}$.
(if the order on $\mathbb{F}$ is 2 we call it Hermitian case)

Self-dual codes over chain rings

Let R be a commutative Artinian chain ring with 1 and let $^{-} : R \to R$ be an involution (i.e. automorphism of order 1 or 2).

Let $\mathfrak{m} \leq R$ denote the maximal ideal of R, then $^{-}$ induces an involution of the residue field $\mathbb{F} := R/\mathfrak{m}$.
(if the order on $\mathbb{F}$ is 2 we call it Hermitian case)

Fix generator x of $\mathfrak{m}$ such that

$$\overline{x} \equiv \epsilon x \pmod{Rx^2},\ \epsilon \in \{1, -1\}.$$

Let $a \in \mathbb{N}_0$, such that

$$R \supset Rx \supset Rx^2 \supset \cdots \supset Rx^{a+1} = \{0\}$$

is the complete chain of ideals in R.

Example

The group ring $\mathbb{F}_3[g]$ carries the involution $\left\{ \begin{array}{l} 1 \mapsto 1 \\ g \mapsto g^{-1} \end{array} \right\}$.

Example

The group ring $\mathbb{F}_3[g]$ carries the involution $\left\{ \begin{array}{l} 1 \mapsto 1 \\ g \mapsto g^{-1} \end{array} \right\}$.

We have

$$\begin{aligned} \overline{(1-g)} &= -(1-g) + (1-g)\cdot(1-g^{-1}) \\ &= -(1-g) - (1-g)^2 \\ &\equiv -(1-g) \pmod{\langle (1-g)^2 \rangle} \end{aligned}$$

$\rightarrow$ choose $x := (1-g)$ as generator with $\epsilon = -1$.

All indecomposable R-modules:

$$S_b := Rx^b \text{ for some } 0 \leq b \leq a,$$

where $S_0 = R$ is the free module of rank 1 and S_a is the unique simple R-module.

All indecomposable R-modules:

$$S_b := Rx^b \text{ for some } 0 \leq b \leq a,$$

where $S_0 = R$ is the free module of rank 1 and S_a is the unique simple R-module.

$V := R^t = \{(v_1, \ldots, v_t) \mid v_i \in R\}$ denotes the free R-module of rank t.

An R-submodule C of V is called code of length t.

Theorem of Krull, Remak, Schmidt:

$$C = S_0^{t_0} \oplus S_1^{t_1} \oplus \cdots \oplus S_a^{t_a}.$$

Define (Hermitian) inner product

$$\langle \cdot , \cdot \rangle : V \times V \to R, \langle v, w \rangle := \sum_{j=1}^{t} v_j \overline{w_j}.$$

Define (Hermitian) inner product

$$\langle \cdot, \cdot \rangle : V \times V \to R, \langle v, w \rangle := \sum_{j=1}^{t} v_j \overline{w_j}.$$

Now let $C = C^{\perp}$ be a self-dual code which is a free R-module, i.e. $C \cong R^{t/2}$. Then the subcodes

$$C^{(i)} := Cx^i \cong S_i^{t/2}$$

form the following chain:

$$V$$

$$C^{(a)\perp}$$

$$C^{(1)\perp}$$

$$C = C^{\perp}$$

$$C^{(1)}$$

$$C^{(2)}$$

$$C^{(a)}$$

$$C^{(a+1)} = \{0\}$$

V

${C^{(a)}}^\perp$

${C^{(1)}}^\perp$

$C = C^\perp$

$C^{(1)}$

$C^{(2)}$

$C^{(a)}$

$C^{(a+1)} = \{0\}$

What be said about the socle $\operatorname{soc}(C) = C^{(a)}$ of C?

$$\begin{array}{l}
\bullet\ V \\
\bullet\ C^{(a)^{\perp}} \\
\vdots \\
\bullet\ C^{(1)^{\perp}} \\
\bullet\ C = C^{\perp} \\
\bullet\ C^{(1)} \\
\bullet\ C^{(2)} \\
\vdots \\
\bullet\ C^{(a)} \\
\bullet\ C^{(a+1)} = \{0\}
\end{array}$$

What be said about the socle $\mathrm{soc}(C) = C^{(a)}$ of C?

Assume we know $C^{(i+1)}$, how can we construct all possible $C^{(i)}$?

The socle of C

Multiplication by x^a defines an isomorphism between the residue field $\mathbb{F}$ and the socle of R:

$$\varphi : \mathbb{F} = R/Rx \xrightarrow{\sim} Rx^a = S_a, r + Rx \mapsto rx^a.$$

The socle of C

Multiplication by x^a defines an isomorphism between the residue field $\mathbb{F}$ and the socle of R:

$$\varphi : \mathbb{F} = R/Rx \xrightarrow{\sim} Rx^a = S_a, r + Rx \mapsto rx^a.$$

This defines an $\mathbb{F}$-linear isomorphism:

$$\pi : \mathrm{soc}(V) = Vx^a \to \mathbb{F}^t, (v_1, \dots, v_t) \mapsto (\varphi^{-1}(v_1), \dots, \varphi^{-1}(v_t))$$

The socle of C

Multiplication by x^a defines an isomorphism between the residue field $\mathbb{F}$ and the socle of R:

$$\varphi : \mathbb{F} = R/Rx \xrightarrow{\sim} Rx^a = S_a, r + Rx \mapsto rx^a.$$

This defines an $\mathbb{F}$-linear isomorphism:

$$\pi : \mathrm{soc}(V) = Vx^a \to \mathbb{F}^t, (v_1, \ldots, v_t) \mapsto (\varphi^{-1}(v_1), \ldots, \varphi^{-1}(v_t))$$

What does that mean?

The socle of C

Multiplication by x^a defines an isomorphism between the residue field $\mathbb{F}$ and the socle of R:

$$\varphi : \mathbb{F} = R/Rx \xrightarrow{\sim} Rx^a = S_a, r + Rx \mapsto rx^a.$$

This defines an $\mathbb{F}$-linear isomorphism:

$$\pi : \mathrm{soc}(V) = Vx^a \to \mathbb{F}^t, (v_1, \ldots, v_t) \mapsto (\varphi^{-1}(v_1), \ldots, \varphi^{-1}(v_t))$$

What does that mean?

The socle $C^{(a)}$ is generated by some matrix Mx^a, where $M \in \mathbb{F}^{\frac{t}{2} \times t}$ generates a self-dual code in $\mathbb{F}^t$ (only true if C is a free module, in general it's the dual of a self-orthogonal code)

$\to$ those are classified (for moderat length t)

Example

Let C be an extremal, ternary code of length 36 (resp. 48) with an automorphism g of order 3 (which is then fixpoint-free).

We choose $1 - g$ as a generator of the maximal ideal in $\mathbb{F}_3[g]$.

Example

Let C be an extremal, ternary code of length 36 (resp. 48) with an automorphism g of order 3 (which is then fixpoint-free).

We choose $1 - g$ as a generator of the maximal ideal in $\mathbb{F}_3[g]$.

The socle $C \cdot (1-g)^2$ is the fixcode $C(g)$ and is generated by some matrix

$$M \otimes \begin{pmatrix} 1 & 1 & 1 \end{pmatrix},$$

where M generates a self-dual code in $\mathbb{F}_3^{12}$ (resp. $\mathbb{F}_3^{16}$).

Example

Let C be an extremal, ternary code of length 36 (resp. 48) with an automorphism g of order 3 (which is then fixpoint-free).

We choose $1 - g$ as a generator of the maximal ideal in $\mathbb{F}_3[g]$.

The socle $C \cdot (1 - g)^2$ is the fixcode $C(g)$ and is generated by some matrix

$$M \otimes \begin{pmatrix} 1 & 1 & 1 \end{pmatrix},$$

where M generates a self-dual code in $\mathbb{F}_3^{12}$ (resp. $\mathbb{F}_3^{16}$).

We must have $d(\langle M \rangle) \geq \frac{12}{3} = 4$ (resp. $\geq \frac{15}{3} = 5$)

$\rightarrow \langle M \rangle$ is an extremal, ternary code, hence unique.

The lifting process

Let $0 \leq i \leq a$ and fix some $C^{(i+1)}$.

We want to find all lifts, i.e. all codes D which are self-orthogonal and $Dx = C^{(i+1)}$.

The lifting process

Let $0 \leq i \leq a$ and fix some $C^{(i+1)}$.

We want to find all lifts, i.e. all codes D which are self-orthogonal and $Dx = C^{(i+1)}$.

Define

$$W_i := {C^{(i+1)}}^{\perp} x^i / C^{(i+1)} \cong \mathbb{F}^t$$

The lifting process

Let $0 \leq i \leq a$ and fix some $C^{(i+1)}$.

We want to find all lifts, i.e. all codes D which are self-orthogonal and $Dx = C^{(i+1)}$.

Define

$$W_i := C^{(i+1)^{\perp}} x^i / C^{(i+1)} \cong \mathbb{F}^t$$

with the inner product

$$(\cdot,\cdot)_i : W_i \times W_i \to \mathbb{F}, (Ax^i + C^{(i+1)}, Bx^i + C^{(i+1)})_i := \varphi^{-1}(\langle A, B\rangle x^i).$$

which is well-defined, non-degenerate and Hermitian in the Hermitian case and $\epsilon^{(i+a)}$-symmetric otherwise.

$X_i := (\mathrm{soc}(V) + C^{(i+1)})/C^{(i+1)}$ is a self-dual code in W_i.

$X_i := (\mathrm{soc}(V) + C^{(i+1)})/C^{(i+1)}$ is a self-dual code in W_i.

$C^{(i)}/C^{(i+1)}$ is self-dual as well and it complements X_i, i.e.

$$W_i = C^{(i)}/C^{(i+1)} \oplus X_i.$$

$X_i := (\mathrm{soc}(V) + C^{(i+1)})/C^{(i+1)}$ is a self-dual code in W_i.

$C^{(i)}/C^{(i+1)}$ is self-dual as well and it complements X_i, i.e.

$$W_i = C^{(i)}/C^{(i+1)} \oplus X_i.$$

$\rightarrow$ the lifts are given by the complements of X_i.

$X_i := (\mathrm{soc}(V) + C^{(i+1)})/C^{(i+1)}$ is a self-dual code in W_i.

$C^{(i)}/C^{(i+1)}$ is self-dual as well and it complements X_i, i.e.

$$W_i = C^{(i)}/C^{(i+1)} \oplus X_i.$$

$\rightarrow$ the lifts are given by the complements of X_i.

How does one construct those complements?

Choose some isotropic complement Y_i of X_i in W_i.

There are bases B_1 and B_2 of X_i resp. Y_i such that the Gram matrix of $(\cdot, \cdot)_i$ w.r.t (B_1, B_2) is

$$\begin{pmatrix} 0 & I \\ \epsilon^{a+i} I & 0 \end{pmatrix}.$$

Choose some isotropic complement Y_i of X_i in W_i.

There are bases B_1 and B_2 of X_i resp. Y_i such that the Gram matrix of $(\cdot,\cdot)_i$ w.r.t (B_1, B_2) is

$$\begin{pmatrix} 0 & I \\ \epsilon^{a+i} I & 0 \end{pmatrix}.$$

$\to$ all self-dual complements of X_i are given by $\langle B_2 + B_1 \cdot A \rangle$, where

$$A \in \mathbb{F}^{t/2 \times t/2} \text{ such that } \overline{A}^{\mathrm{tr}} + \epsilon^{a+i} A = 0.$$

(the set of all thoses matrices form a vector space over $\mathbb{F}$)

Example

We determined the socle $C^{(2)}$ of an extremal, ternary code of length 36 with an automorphism g of order 3.

Example

We determined the socle $C^{(2)}$ of an extremal, ternary code of length 36 with an automorphism g of order 3.

Vectorspace of all $A \in \mathbb{F}_3^{6\times 6}$ such that

$$\begin{aligned} \overline{A}^{\text{tr}} + \epsilon^{a+i} A &= 0 \\ \Leftrightarrow A^{\text{tr}} - A &= 0 \end{aligned}$$

has dimension 21 over $\mathbb{F}_3$, the centralizer of g in $\mathrm{Aut}(C^{(2)})$ has 16 orbits on this set, so we have 16 possibilities for $C^{(1)}$.

Example

We determined the socle $C^{(2)}$ of an extremal, ternary code of length 36 with an automorphism g of order 3.

Vectorspace of all $A \in \mathbb{F}_3^{6\times 6}$ such that

$$\begin{aligned} \overline{A}^{\mathrm{tr}} + \epsilon^{a+i} A &= 0 \\ \Leftrightarrow A^{\mathrm{tr}} - A &= 0 \end{aligned}$$

has dimension 21 over $\mathbb{F}_3$, the centralizer of g in $\mathrm{Aut}(C^{(2)})$ has 16 orbits on this set, so we have 16 possibilities for $C^{(1)}$.

For these 16 codes we constructed all 3^{15} codes $C^{(0)}$ and have shown:

Theorem (Nebe, E.)

Let C be an extremal, ternary code of length 36 with an automorphism of order 3. Then C is isomorphic to the Pless Code P_{36}.

Theorem (Nebe, E.)

Let C be an extremal, ternary code of length 36 with an automorphism of order 3. Then C is isomorphic to the Pless Code P_{36}.

Remark

The search spaces for $n = 48$ has size 3^{36} resp. 3^{28} - I can wait a few days for a result, but not 10000 years.

If C is a $[72, 36, 16]$-code with an automorphism g of order 2, then g has no fixpoints and C is a free $\mathbb{F}_2[g]$-module $\rightarrow$ there are 41 possibilities for $C^{(1)}$, the search space for $C^{(0)}$ has dimension 171 over $\mathbb{F}_2$.