On the search of extremal self-dual codes of length 72

Martino Borello

BunnyTN3, Trento, 12.03.2012

Extremal self-dual codes

A (binary) **self-dual doubly-even code** $\mathcal{C}$ of parameters $[n,k,d]$ is a linear code s.t.

- $\mathcal{C} = \mathcal{C}^{\perp}$ (so $k = \frac{n}{2}$)
- $\{\mathrm{wt}(c) \mid c \in \mathcal{C}\} \subseteq 4\mathbb{Z}$

Some results

- $n = 8m$ with $m \in \mathbb{N}$ (Gleason '71);
- if $n = 24m$ then all codewords of a given weight support 5-designs (Assmus and Mattson '69);
- $d \leq 4\left[\frac{n}{24}\right] + 4$ (Mallows and Sloane '73).

If $d = 4\left[\frac{n}{24}\right] + 4$ then $\mathcal{C}$ is called **extremal** self-dual code.

Doubly-even self-dual codes

$\mathcal{C}$ extremal self-dual code of length a multiple of 24. Then $n \in \{24, 48, 72, \dots, 3672\}$ (Zhang '99).

Examples

Only two extremal self-dual codes are known:

- $\mathcal{G}_{24}$ (**Golay code**), unique (up to equivalence) with parameters $[24, 12, 8]$;
- QR_{48} (**extended quadratic residue code**), unique (up to equivalence) with parameters $[48, 24, 12]$.

A longstanding open problem

Is there a $[72, 36, 16]$ self-dual doubly-even code? (Sloane '73)

Automorphism Group

There is (right) action of $\mathcal{S}_n$ on $\mathbb{F}_2^n$ (**action on the coordinates**): if $v = (v_1, v_2, \ldots, v_n) \in \mathbb{F}_2^n$ and $g \in \mathcal{S}_n$ then define

$$v^g := (v_{g^{-1}(1)}, v_{g^{-1}(2)}, \ldots, v_{g^{-1}(n)}).$$

Definition

$\mathrm{Aut}(\mathcal{C}) := \{g \in \mathcal{S}_n \mid \mathcal{C}^g = \mathcal{C}\} \leq \mathcal{S}_n$ (**Automorphism Group**)

- $\mathrm{Aut}(\mathcal{G}_{24}) = M_{24}$;
- $\mathrm{Aut}(QR_{48}) = \mathsf{PSL}(2, 47)$;
- what do we know when the length is 72?

Automorphism Group

Theorem (...Bouyuklieva, O'Brien, Willems, Nebe, Feulner)

If $\mathcal{C}$ is a binary self-dual doubly-even $[72, 36, 16]$ code then $\mathrm{Aut}(\mathcal{C})$ is trivial or is isomorphic to one of the following:

- Order 2: $\mathbb{Z}_2$;
- Order 3: $\mathbb{Z}_3$;
- Order 4: $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$;
- Order 5: $\mathbb{Z}_5$;
- Order 6: $\mathcal{S}_3$ or $\mathbb{Z}_6$;
- Order 8: $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ or $\mathcal{D}_8$;
- Order 12: $\mathcal{A}_4$, $\mathbb{Z}_{12}$, $\mathbb{Z}_6 \times \mathbb{Z}_2$, $\mathcal{D}_{12}$ or $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$;
- Order 24: $\mathcal{S}_4$, $\mathcal{D}_{24}$, $(\mathbb{Z}_6 \times \mathbb{Z}_2) : \mathbb{Z}_2$, $\mathcal{D}_8 \times \mathbb{Z}_3$, $\mathcal{A}_4 \times \mathbb{Z}_2$, $\mathcal{D}_{12} \times \mathbb{Z}_2$ or $\mathbb{Z}_6 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Automorphism Group

Conjecture

If $\mathcal{C}$ is a binary self-dual doubly-even $[72, 36, 16]$ code then $\mathrm{Aut}(\mathcal{C})$ is trivial or is isomorphic to one of the following:

- Order 2: $\mathbb{Z}_2$;
- Order 3: $\mathbb{Z}_3$;
- Order 4: $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$;
- Order 5: $\mathbb{Z}_5$;
- Order 6: $\mathcal{S}_3$;
- Order 8: $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ or $\mathcal{D}_8$;
- Order 12: $\mathcal{A}_4$;
- Order 24: $\mathcal{S}_4$.

A classical decomposition

Definition

Let $h \in \mathrm{Aut}(\mathcal{C})$. $\mathcal{C}(h) := \{c \in \mathcal{C} \mid c^h = c\}$ is the **fixed code** (by h).

Theorem (Huffman '82)

If h has odd order

$$\mathcal{C} = \mathcal{C}(h) \oplus \mathcal{E}(h)$$

where

$$\mathcal{E}(h) := \{c \in \mathcal{C} \mid \mathrm{wt}(c_{|\Omega_i}) \equiv 0 \pmod 2, \text{ for all } i\}$$

Decomposition of codes as $\mathbb{F}_2G$-modules

Theorem

Let $\mathcal{C}$ be a binary linear code, $G \leq \mathrm{Aut}(\mathcal{C})$ and

$$1 = f_1 + \ldots + f_t$$

be a decomposition of $1 \in \mathbb{F}_2G$ into *central orthogonal idempotents* $f_i \in \mathbb{F}_2G$.
Set $\mathcal{V}_i = \mathcal{V}f_i$ and $\mathcal{C}_i = \mathcal{C}f_i \subseteq \mathcal{V}_i$ for $i \in \{1, \ldots, t\}$. Then

$$\mathcal{V} = \mathcal{V}_1 \oplus \ldots \oplus \mathcal{V}_t \qquad \text{and} \qquad \mathcal{C} = \mathcal{C}_1 \oplus \ldots \oplus \mathcal{C}_t$$

as $\mathbb{F}_2G$-modules.

Decomposition of $\mathcal{C}$

$\mathcal{V} = \mathbb{F}_2^{72}$, $\mathcal{C}$ binary self-dual doubly-even $[72, 36, 16]$ code. Suppose that there exist $g \in \mathrm{Aut}(\mathcal{C})$ of order 6.

g^2 ha order 3, so $\mathcal{C} = \mathcal{C}(g^2) \oplus \mathcal{E}(g^2)$.

Set $G = \langle g \rangle$. Then $f_1 = 1 + g^2 + g^4$ and $f_2 = g^2 + g^4$ are (central) idempotents in $\mathbb{F}_2\langle g \rangle$ such that $\hat{f}_1 = f_1$ and $\hat{f}_2 = f_2$.

1. $\mathcal{C}_1 = \mathcal{C}f_1 = \mathcal{C}(g^2)$ and $\mathcal{C}_2 = \mathcal{C}f_2 = \mathcal{E}(g^2)$;
2. $\mathcal{V}_1 = \mathcal{V}f_1 = \mathcal{V}(g^2)$, the subspace of all the vectors fixed by g^2;
3. $\mathcal{V}_2 = \mathcal{V}f_2$ is the set of vectors of even weight on the orbits of g^2.

Decomposition of $\mathcal{C}$

There are only two types of cyclic $\mathbb{F}_2\langle g\rangle$-submodules of $\mathcal{V}_2$:

I. irreducible of dimension 2.

II. indecomposable of dimension 4 with a socle of dimension 2.

Theorem (B.)

Let $\mathcal{M}$ be a $\mathbb{F}_2\langle g\rangle$-submodule of $\mathcal{V}_2$ such that $\dim(\mathcal{M}) = 2\dim(\mathrm{soc}(\mathcal{M})) = 4m$. Then for every decomposition

$$\mathrm{soc}(\mathcal{M}) = \mathfrak{p}_1 \oplus \ldots \oplus \mathfrak{p}_m$$

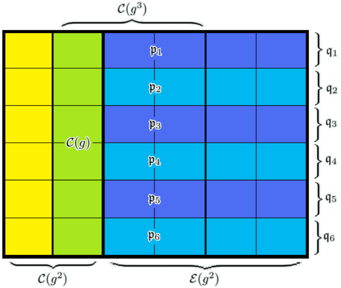
of the socle in irreducible $\mathbb{F}_2\langle g\rangle$-submodules, there exist $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$, cyclic $\mathbb{F}_2\langle g\rangle$-submodules of type II of $\mathcal{M}$ with $\mathrm{soc}(\mathfrak{q}_i) = \mathfrak{p}_i$ such that

$$\mathcal{M} = \mathfrak{q}_1 \oplus \ldots \oplus \mathfrak{q}_m.$$

Our method

Lemma

$$\mathrm{soc}(\mathcal{E}(g^2)) = (\mathcal{E}(g^2))(g^3) = (\mathcal{C}(g^2) + \mathcal{C}(g^3)) \cap \mathcal{V}_2.$$



Problems

Determine the fixed codes, classify the possible socles and do an exhaustive search.

Fixed codes

Proposition (Nebe '11)

$\mathcal{C}(g^2)$ is equivalent to $\mathcal{G}_{24} \otimes \langle(1,1,1)\rangle$.

Proposition (Nebe '11)

$\mathcal{C}(g^3)$ is equivalent to $\mathcal{K} \otimes \langle(1,1)\rangle$, with $\mathcal{K}$ one of the 41 self-dual $[36,18,8]$ codes classified by Mechor and Gaborit.

Proposition (B.)

$\mathcal{C}(g)$ is equivalent to $\mathcal{F} \otimes \langle(1,1,1,1,1,1)\rangle$, where $\mathcal{F}$ is binary self-dual $[12,6,4]$ code with generator matrix

$$M = \begin{bmatrix} 1&1&1&1&0&0&0&0&0&0&0&0 \\ 0&0&1&1&1&1&0&0&0&0&0&0 \\ 0&0&0&0&1&1&1&1&0&0&0&0 \\ 0&0&0&0&0&0&1&1&1&1&0&0 \\ 0&0&0&0&0&0&0&0&1&1&1&1 \\ 0&1&0&1&0&1&0&1&0&1&0&1 \end{bmatrix}.$$

Thank you very much for the attention!