A class of singly even self-dual codes

Stefka Bouyuklieva, Zlatko Varbanov, Katina Toncheva

Veliko Tarnovo University

BULGARIA

Outline

- Binary self-dual codes
- Codes and designs
- Secret-sharing scheme based on SD codes
- Singly-even SD binary codes and their shadows
- Applications: A secret-sharing scheme based on SD codes

C - binary linear [n,k,d] code

- C - self-orthogonal code if $C \subseteq C^{\perp}$
- C - self-dual code if $C = C^{\perp}$
- Any self-dual code has dimension $k = n/2$
- All codewords in a binary self-orthogonal code have even weights
- Doubly-even code - all its weights are divisible by 4
- Singly-even self-dual code - if it contains a codeword of weight $w \equiv 2 \pmod 4$

Extremal self-dual codes

If C is a binary self-dual $[n, n/2, d]$ code then

$$d \leq 4[n/24] + 4$$

except when $n \equiv 22 \pmod{24}$ when

$$d \leq 4[n/24] + 6$$

When n is a multiple of 24, any code meeting the bound must be doubly-even.

Optimal self-dual codes

A self-dual code is called optimal if it has the largest minimum weight among all self-dual codes of that length.

- Any extremal self-dual code is optimal.
- For some lengths, no extremal self-dual codes exist!
- There are no extremal self-dual codes of lengths 2, 4, 6, 10, 26, 28, 30, 34, 50, 52, 54, 58, ...

Conjecture: The optimal self-dual codes of lengths $24m+r$ for $r=2$, 4, 6, and 10 are not extremal.

The shadow of a singly even code

C - singly even self-dual $[n, k = n/2, d]$ code
C_0 - its doubly even subcode:

$$C_0 = \{v \in C \mid wt(v) \equiv 0 \pmod 4\}$$

$$dim C_0 = k - 1$$

$$C_2 = \{v \in C \mid wt(v) \equiv 2 \pmod 4\}$$

$$C = C_0 \cup C_2$$

$$\Rightarrow C_0^{\perp} = C_0 \cup C_1 \cup C_2 \cup C_3$$

$S = C_0^{\perp} \setminus C = C_1 \cup C_3$ - the shadow of C

Properties of the shadow

- $u, v \in C_i \Rightarrow u + v \in C_0, i = 0, 1, 2, 3;$
- $u \in C_1, v \in C_3 \Rightarrow u + v \in C_2;$
- if $n \equiv 2 \pmod 4$ then $C_2 = \mathbf{1} + C_0;$
- if $n \equiv 0 \pmod 4$ then $\mathbf{1} \in C_0.$

Singly-even self-dual codes

If

$$W(x,y)=\sum_{j=0}^{[n/8]} a_j(x^2+y^2)^{n/2-4j}(xy(x^2-y^2))^{2j}$$

then

$$S(x,y)=\sum_{j=0}^{[n/8]} (-1)^j a_j 2^{n/2-6j}(xy)^{n/2-4j}(x^4-y^4)^{2j}$$

Weight enumerators

$$S(x,y) = \sum B_i x^{n-i} y^i$$

- $B_i = B_{n-i}$;
- $B_0 = 0$;
- $B_r = 0$ for all $r \not\equiv n/2 \pmod 4$;
- $B_r \leq 1$ for $r < d/2$;
- $B_{d/2} \leq 2n/d$, $B_{d/2} \neq 2n/d - 1$;
- if $n \equiv 2 \pmod 4$ then $B_{d/2} \leq 2$.

Example - [50,25,10] codes

$$S(y) = \frac{1}{2048}a_6 y + (-\frac{1}{32}a_5 - \frac{3}{512}a_6)y^5 + \cdots$$

$$\Rightarrow a_6 = 2048 \text{ or } 0$$

$$S(y) = y + 196y^9 + \cdots \quad W(y) = 1 + 196y^{10} + \cdots$$

$$a_6 = 0,\ a_5 = -32\beta$$

$$S(y) = \beta y^5 + (250 - 10\beta)y^9 + (42800 + 45\beta)y^{13} + \cdots$$

$$W(y) = 1 + (580 - 32\beta)y^{10} + (7400 + 160\beta)y^{12} + \cdots$$

$$\Rightarrow 0 \leq \beta \leq 2$$

Example - [50,25,10] codes

Let C be a [50,25,10] SD code with

$$S(y) = y + 196y^9 + \cdots \quad W(y) = 1 + 196y^{10} + \cdots$$

Then all the codewords of weight 10 in C share a common nonzero coordinate and the deletion of that coordinate gives a $[49, 25, 9]$ code whose minimum weight codewords support a quasi-symmetric 2-$(49, 9, 6)$ design.

$t-(v,k,\lambda)$ **designs**

A $t-(v,k,\lambda)$ **design** is:

- a set of v points $\mathcal{P}$;
- a family of blocks $\mathcal{B} = \{B \subset \mathcal{P}, |B| = k\}$;
- an incidence relation between them such that $v = |\mathcal{P}|$, every block is incident with precisely k points, and every t distinct points are incident with λ blocks.

Any t-design is also a $s-(v,k,\lambda_s)$ design for $s \le t$:

$$\lambda_s = \frac{(v-s)}{(k-s)}\lambda_{s+1}(s = 1,\dots,t-1),\ \lambda_t = \lambda$$

Assmus-Mattson Theorem

Binary case:

C - $[n,k,d]$ binary linear code;

$C^{\perp}$ - its orthogonal $[n,n-k,d^{\perp}]$ code;

t - an integer, $0 < t < d$, such that $C^{\perp}$ has not more than $d-t$ nonzero weights $w \leq n-t$.

Then:

- the supports of all codewords in C of weight u form a t-design;
- the supports of all codewords in $C^{\perp}$ of weight w, $d^{\perp} \leq w \leq n-t$, form a t-design.

Secret-sharing ($n-1$ parties)

- $s \in \mathbb{F}_q$ - the secret;
- $G = (G_0 G_1 \dots G_{n-1})$ - a generator matrix of a code C of length n;
- $v \in \mathbb{F}_q^k$ - the information vector, $vG_0 = s$;
- $u = vG$;
- to each party we assign $u_i, i = 1, \dots, n-1$;

Computing the secret

s is determined by the set of shares $\{u_{i_1}, u_{i_2}, \ldots, u_{i_m}\}$

$$\iff G_0 = \sum_{j=1}^{m} x_j G_{i_j},\ 1 \leq i_1 < \cdots < i_m \leq n-1$$

$$\iff \exists (1, 0, ..., 0, c_{i_1}, 0, ..., 0, c_{i_m}, 0.., 0) \in C^{\perp},\ (c_{i_1}, \ldots, c_{i_m}) \neq$$

So by solving this linear equation, we find x_j and from then on the secret by $s = vG_0 = \sum_{j=1}^{m} x_j v G_{i_j} = \sum_{j=1}^{m} x_j u_{i_j}$.

Γ - access structure

If $\mathcal{P}$ is the set of parties involved in the secret-sharing, then

$$\Gamma = \{A \subset \mathcal{P} : \ A \text{ can uncover the secret}\}$$

$A \in \Gamma$ - **minimum access group** if

$$B \in \Gamma \text{ and } B \subseteq A \text{ implies } B = A$$

$$\overline{\Gamma} = \{A \mid A \text{ is a minimum access group}\}$$

$\overline{\Gamma}$ - the minimum access structure.

Secret-sharing based on an SD code

C - an SD code with $\mathrm{wt}(S) = 1$

$$\Gamma = \{A \mid A \text{ is the support of a vector } v \in C_2\}.$$

- Any group of size less than $d-1$ cannot recover the secret.
- There are A_i groups of size $i-1$ that can recover the secret.
- It is perfect, which means that a group of shares either determines the secret or gives no information about the secret.
- When the parties come together $\lfloor \frac{d-1}{2} \rfloor$ cheaters can be found.

Secret-sharing based on an SD code

D_i - the 1-design formed from the vectors of weight i

$\Gamma = \{A \mid A$ is the support of a vector $v \in C$ with $v_0 = 1\}$.

- Any group of size less than $d-1$ cannot recover the secret.
- There are $\lambda_1(D_i)$ groups of size $i-1$ that can recover the secret.
- It is perfect, which means that a group of shares either determines the secret or gives no information about the secret.
- When the parties come together $\lfloor \frac{d-1}{2} \rfloor$ cheaters can be found.

$n = 24m + 8l + 2$, $l = 0, 1, 2$, $\mathrm{wt}(S) = 1$

$$W(y) = \sum_{j=0}^{12m+4l+1} a_j y^{2j} = \sum_{i=0}^{3m+l} c_i (1+y^2)^{4(3m+l-i)+1} (y-y^3)^{2i}$$

$$S(y) = \sum_{j=0}^{6m+2l} b_j y^{4j+1} = \sum_{i=0}^{3m+l} (-1)^i c_i \frac{(2y)^{4(3m+l-i)+1} (1-y^4)^{2}}{4^i}$$

$$c_i = \sum_{j=0}^{i} \alpha_{ij} a_j = \sum_{j=0}^{3m+l-i} \beta_{ij} b_j$$

$n = 24m + 8l + 2$, $l = 0, 1, 2$, $\mathrm{wt}(S) = 1$

Theorem 1 *Extremal self-dual codes of lengths* $24m+2$ *and* $24m+10$ *with* $\mathrm{wt}(S) = 1$ *do not exist.*

$$c_{2m+1} = \alpha_{2m+1,0} = \beta_{2m+1,0}$$

$$l = 0 \Rightarrow -\frac{(12m+1)(56m+4)}{(2m+1)(m-1)}\binom{5m-1}{m-2} = -\frac{96m}{2m+1}\binom{5m}{m-$$

$$l = 1 \Rightarrow -\frac{12m+5}{2m+1}\binom{5m+1}{m} = -2\frac{3m+1}{2m+1}\binom{5m+1}{m}$$

$n = 24m + 8l + 2$, $l = 0, 1, 2$, $\mathrm{wt}(S) = 1$

Theorem 2 *C - optimal $[24m+2, 12m+1, 4m+2]$ SD code with $\mathrm{wt}(S) = 1$:*

- *The set of codewords of weight u in C_0 without the common zero coordinate holds a 2-design.*
- *The set of codewords of weight w in C_2 without the common 1-coordinate holds a 2-design.*

C - extremal self-dual $[24m+18, 12m+9, 4m+4]$ code with $\mathrm{wt}(S) = 1$:

- *The set of codewords of weight u in C_0 without the common zero coordinate holds a 1-design.*
- *The set of codewords of weight w in C_2 without the common 1-coordinate holds a 1-design.*

One-part secret sharing

Let C be a binary self-dual
$[24m+18, 12m+9, 4m+4]$ or
$[24m+10, 12m+5, 4m+2]$ or
$[24m+2, 12m+1, 4m+2]$ code with $\mathrm{wt}(S) = 1$

$$\Gamma = \{A \mid A \text{ is the support of a vector } v \in C_2\}.$$

Two-part secret sharing

Let C be a binary self-dual $[24m+2, 12m+1, 4m+2]$ code with $\mathrm{wt}(S) = 1$

$$\Gamma_1 = \{A \mid A \text{ is the support of a vector } v \in C_2\}.$$

$\Gamma_2 = \{A \mid A \text{ is the support of a vector } v \in C_2 \text{ with } v_1 = v_2 = 1$

Two-part secret sharing

Let C be a binary self-dual $[50, 25, 10]$ code with $\mathrm{wt}(S) = 1$

- For the first part of the secret, the access structure contains 196 groups of size 9.
- For the second part we take these 36 blocks of D that have 1 in the first position. Without the first point, the blocks of D hold $1 - (48, 8, 6)$ design D_1.
- We take these 6 blocks of D_1 that have 1 in the first position. Then, for the second part of the secret, the access structure consists of 6 groups of size 7.

Two-part secret sharing

- To recover the two-part secret should first be used the groups of size 7. They recover the second part of the secret.
- After that to recover the other part of the secret we use these groups (they are of size 8 already) and the other 30 groups of size 8. We add a new participant that has ones in these 36 groups (the other entries are 0).
- At last, we use the obtained 36 groups of size 9, and the other 160 groups of size 9 to recover the first part of the secret.