Connections between different types of binary self-dual codes

Stefka Bouyuklieva, Wolfgang Willems

Outline

- Binary self-dual codes
- Extremal and optimal codes
- Shadow codes
- *s*-extremal codes and codes with minimal shadow
- Self-dual codes and their children
- Weight enumerators

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

Rains (1998):

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

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

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

Conway, Sloane (1990):

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

s-extremal self-dual codes

Bachoc, Gaborit (2004):

If s is the minimum weight of the shadow of a singly-even self-dual $[n,n/2,d]$ code then

$$2d+s \leq \frac{n}{2}+4$$

except if $n \equiv 22 \pmod{24}$ when $2d+s \leq \frac{n}{2}+8$

Codes, meeting the bound are called ***s-extremal***.

Self-dual codes with minimal shadow

Bouyuklieva, Willems (2012):

A self-dual code C of length n is a ***code with minimal shadow*** if:

(i) $\mathrm{wt}(S) = r$ if $n \equiv 2r \pmod 8$, $r = 1, 2, 3$, and

(ii) $\mathrm{wt}(S) = 4$ if $n \equiv 0 \pmod 8$.

Bouyuklieva, Varbanov (2011) - $\mathrm{wt}(S) = 1$
Bouyuklieva, Malevich, Willems (2011) - $\mathrm{wt}(S) = 4$

Singly-even vs doubly-even codes

C - singly-even self-dual $[n, n/2, d]$ code, $n \equiv 0 \pmod 8$

$\Rightarrow C_0 \cup C_1$ and $C_0 \cup C_3$ - doubly-even codes

If C is an extremal self-dual code with minimal shadow then
$C_0 \cup C_1$ - doubly-even $[8m, 4m, 4]$ code
$C_0 \cup C_3$ - extremal doubly-even $[8m, 4m]$ code

Self-dual codes and their children

$$G = \left(\begin{array}{cc|c} 1 & 0 & b \\ \hline 1 & 1 & a \\ \hline 0 & 0 & \\ \vdots & \vdots & D \\ 0 & 0 & \end{array}\right) \Rightarrow \overline{C} = \mathcal{D} \cup (a + \mathcal{D}) - \text{self-dual code}$$

$$d - 2 \leq d(\overline{C}) \leq d$$

$s = 1 \Rightarrow n \equiv 2 \pmod 8$

$(100\ldots0) \in S$

$$G = \left(\begin{array}{cc|c} 1 & 0 & b \\ \hline 1 & 1 & a \\ \hline 0 & 0 & \\ \vdots & \vdots & D \\ 0 & 0 & \end{array}\right) \Rightarrow\ C_0 = (00, \mathcal{D}) \cup (01, a+b+\mathcal{D})$$

$\Rightarrow \overline{C} = \mathcal{D} \cup (a + \mathcal{D})$ - doubly-even code

If C is extremal then $\overline{C}$ is also extremal.

$s = 2 \Rightarrow n \equiv 4 \pmod 8$

$(1100\ldots0) \in S$

$$G = \left(\begin{array}{cc|c} 1 & 0 & b \\ \hline 1 & 1 & a \\ \hline 0 & 0 & \\ \vdots & \vdots & D \\ 0 & 0 & \end{array}\right) \Rightarrow C_0 = (00, \mathcal{D}) \cup (11, a + \mathcal{D})$$

If C is extremal then $\overline{d} = d(\overline{C}) = d$ or $d-2$, $\overline{s} \geq d+1$

$s = 2 \Rightarrow n \equiv 4 \pmod 8$

$(1100\ldots0) \in S$, $d = 4m+4$, $n = 24m+8l+4$, $l = 0,1,2$

- $n = 24m+4 \;\Rightarrow \overline{d} = 4m+4$ or $4m+2$, $\overline{s} \geq 4m+5$ $\Rightarrow 2(4m+2)+4m+5 \leq 2\overline{d}+\overline{s} \leq 12m+5$ - impossible
- $n = 24m+12 \;\Rightarrow \overline{d} = 4m+4$ or $4m+2$, $\overline{s} \geq 4m+5$ $\Rightarrow 2(4m+2)+4m+5 \leq 2\overline{d}+\overline{s} \leq 12m+9$ $\Rightarrow \overline{C}$ is an s-extremal $[24m+10, 12m+5, 4m+2]$ code
- $n = 24m+4, d = 4m+2 \;\Rightarrow \overline{d} = 4m+4$ or $4m+2$, $\overline{s} = 4m+1$ $\Rightarrow \overline{C}$ is an s-extremal $[24m+2, 12m+1, 4m+2]$ code

$s = 2 \Rightarrow n \equiv 4 \pmod 8$

(1) There exists a self-dual $[24m+4, 12m+2, 4m+2]$ code with minimal shadow if and only if there is an s-extremal $[24m+2, 12m+1, 4m+2]$ code ($\bar{s} = 4m+1$).
(2) There exists a self-dual $[24m+12, 12m+6, 4m+4]$ code with minimal shadow if and only if there is an s-extremal $[24m+10, 12m+5, 4m+2]$ code ($\bar{s} = 4m+5$).
(3) There exists an extremal self-dual $[24m+20, 12m+10, 4m+4]$ code with minimal shadow if and only if there is a $[24m+18, 12m+9, \geq 4m+2]$ code with $\bar{s} \geq 4m+5$.

Singly-even self-dual codes

$n = 24m + 8l + 2r$, $l = 0, 1, 2$, $r = 0, 1, 2, 3$

$$W(y) = \sum_{j=0}^{12m+4l+r} a_j y^{2j}$$

$$= \sum_{i=0}^{3m+l} c_i (1+y^2)^{12m+4l+r-4i} (y^2(1-y^2)^2)^i, \text{ and}$$

$$S(y) = \sum_{j=0}^{6m+2l} b_j y^{4j+r}$$

$$= \sum_{i=0}^{3m+l} (-1)^i c_i 2^{12m+4l+r-6i} y^{12m+4l+r-4i} (1-y^4)^{2i}.$$

Weight enumerators

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

$$d = 4m+4 \Rightarrow a_0 = 1, a_1 = a_2 = \cdots = a_{2m+1} = 0$$

$$\Rightarrow c_i = \alpha_{i0} = \alpha_i(n), i = 0, 1, \ldots, 2m+1$$

$$s = 4m+4l+r-4 \Rightarrow b_0 = b_1 = b_2 = \cdots = b_{m+l-2} = 0$$

$$\Rightarrow c_i = 0, i = 2m+2, \ldots, 3m+l$$

$$c_{2m+1} = \alpha_{2m+1}(n) = \beta_{2m+1,m+l-1} b_{m+l-1} = -2^{6-t} b_{m+l-1}$$

Weight enumerators, $t = 4l + r$

$$c_{2m+1} = \alpha_{2m+1}(n) = \beta_{2m+1,m+l-1} b_{m+l-1} = -2^{6-t} b_{m+l-1}$$

$$\Rightarrow b_{m+l-1} = -2^{t-6} \alpha_{2m+1}(n)$$

$$\begin{aligned} c_{2m} = \alpha_{2m}(n) &= \beta_{2m,m+l-1} b_{m+l-1} + \beta_{2m,m+l} b_{m+l} \\ &= 2^{1-t}(2m+1) b_{m+l-1} + 2^{-t} b_{m+l}. \end{aligned}$$

$$\begin{aligned} \Rightarrow b_{m+l} &= 2^t \alpha_{2m}(n) - 2(2m+1) b_{m+l-1} \\ &= 2^t \alpha_{2m}(n) + 2^{t-5}(2m+1)\alpha_{2m+1}(n). \end{aligned}$$

$n = 24m + 2$

$$b_m = \frac{(12m+1)(39-14m)}{20m}\binom{5m}{m-1} \geq 0$$

$$\Rightarrow m \leq 2$$

But self-dual $[2,1,4]$, $[26,13,8]$ and $[50,25,12]$ do not exist

Hence self-dual $[24m+2, 12m+1, 4m+4]$ s-extremal codes do not exist

Weight enumerators, $t = 4l + r$

No s-extremal singly-even self-dual $[24m+2t, 12m+t, 4m+4]$ codes exist if
(1) $t = 1$; (2) $t = 2$ and $m \neq 7$;
(3) $t = 3$ and $m \neq 7, 13, 14, 15$;
(4) $t = 4$ and $m \geq 43$;
(5) $t = 5$ and $m \geq 78$;
(6) $t = 6$ and $m \geq 113$;
(7) $t = 7$ and $m \geq 136$;
(8) $t = 8$ and $m \geq 148$;
(9) $t = 9$ and $m \geq 152$;
(10) $t = 10$ and $m \geq 153$.