*Thirteenth International Workshop on Algebraic and Combinatorial Coding Theory*
*June 15-21, 2012, Pomorie, Bulgaria* *pp. 111–116*

# Connections between different types of binary self-dual codes

Stefka Bouyuklieva[1] stefka@uni-vt.bg
Faculty of Mathematics and Informatics, Veliko Tarnovo University,
5000 Veliko Tarnovo, Bulgaria
Wolfgang Willems willems@ovgu.de
Institut für Algebra und Geometrie, Fakultät für Mathematik,
Otto-von-Guericke Universität, 39016 Magdeburg, Germany

**Abstract.** In this note we consider the connection between singly-even self-dual codes with minimal shadow, s-extremal self-dual codes and doubly-even self-dual codes. Moreover, we give a bound on the length $n$ of s-extremal self-dual codes with minimum distance $4\lfloor n/24\rfloor + 4$.

## 1 Introduction

Throughout this paper all codes are assumed to be binary. Let $C$ be a singly-even self-dual code of length $n$ and let $C_0$ be its doubly-even subcode. There are three cosets $C_1, C_2, C_3$ of $C_0$ such that $C_0^{\perp} = C_0 \cup C_1 \cup C_2 \cup C_3$, where $C = C_0 \cup C_2$. The set $S = C_1 \cup C_3 = C_0^{\perp} \setminus C$ is called the shadow of $C$. Shadows for self-dual codes were introduced by Conway and Sloane [3] in order to derive upper bounds for the minimum weight of singly-even self-dual codes and to provide restrictions on their weight enumerators. According to [6] the minimum weight $d$ of a self-dual code of length $n$ is bounded by $4[n/24] + 4$ if $n \not\equiv 22 \pmod{24}$ and by $4[n/24] + 6$ if $n \equiv 22 \pmod{24}$. A self-dual code meeting this bound is called extremal. Moreover, all extremal self-dual codes of length $24m$, $m \geq 1$, are doubly-even.

Elkies studied in [4] the minimum weight $s$ of the shadow of self-dual codes, especially in the cases where it attains a high value. Bachoc and Gaborit proposed to study the parameters $d$ and $s$ simultaneously [1]. They proved that

$$2d + s \leq \frac{n}{2} + 4, \qquad (1)$$

except in the case $n \equiv 22 \pmod{24}$ where $2d + s \leq \frac{n}{2} + 8$. They called codes attaining this bound *s-extremal.* In our work [2] we introduced self-dual codes with minimal shadow as singly-even self-dual codes for which the minimum

[1]The research of this author is partially supported by VTU Science Fund under Contract RD-642-01/26.07.2010

weight of the shadow has the smallest possible value. More precisely, a self-dual code $C$ of length $n = 24m + 8l + 2r$, $l = 0, 1, 2$, $r = 0, 1, 2, 3$, is a code with minimal shadow if: (i) $\mathrm{wt}(S) = r$ if $r > 0$, and (ii) $\mathrm{wt}(S) = 4$ if $r = 0$.

If $W_S(y) = \sum_{i=0}^{n} B_i y^i$ is the weight enumerator of the shadow $S$ then, by [3], $B_0 = 0$ and $B_i = 0$ unless $i \equiv n/2 \pmod 4$.

## 2 Self-dual codes and their children

Let $C$ be a binary $[n, n/2, d > 2]$ self-dual code and let $\mathcal{D}$ be the subcode which consists of all codewords with 0's in the first two coordinate positions. So

$$\mathcal{D} = \{v \in \mathbb{F}_2^{n-2} \mid (00, v) \in C\}.$$

If $(11, a) \in C$ and $(10, b) \in C$ then

$$C = (00, \mathcal{D}) \cup (11, a + \mathcal{D}) \cup (10, b + \mathcal{D}) \cup (01, a + b + \mathcal{D}).$$

**Lemma 1.** *The code* $\overline{C} = \mathcal{D} \cup (a + \mathcal{D})$ *is a self-dual* $[n - 2, n/2 - 1]$ *code with minimum distance at least* $d - 2$*, called a child of* $C$*.*

We can consider a generator matrix of $C$ in the form

$$G = \left(\begin{array}{cc|c} 1 & 0 & b \\ \hline 1 & 1 & a \\ \hline 0 & 0 & \\ \vdots & \vdots & D \\ 0 & 0 & \end{array}\right), \tag{2}$$

where $D$ generates the code $\mathcal{D}$.

We investigate two cases according to the minimum weight $s$ of the shadow of the codes.

Case 1: $s = 1$

Let $C$ be a singly-even self-dual code of length $n$ and $(100\ldots0) \in S$. Since $B_1 = 1$ we have $n \equiv 2 \pmod 8$ and therefore $n = 24m + 8l + 2$, $l = 0, 1, 2$. In this case the doubly-even subcode of $C$ is $C_0 = (00, \mathcal{D}) \cup (01, a + b + \mathcal{D})$ since $(100\ldots0) \in S$. We proved in [2] that extremal self-dual codes with minimal shadow of lengths $24m+2$ and $24m+10$ do not exist. So consider a self-dual code $C$ with parameters $[24m+18, 12m+9, 4m+4]$. Then the code $\overline{C} = \mathcal{D} \cup (a+\mathcal{D})$ is an extremal doubly-even $[24m + 16, 12m + 8, 4m + 4]$ code.

**Theorem 1.** *If no extremal doubly-even code of length* $24m + 16$ *exists, then there are no extremal singly-even codes of length* $24m+18$ *with minimal shadow.*

Case 2: $s = 2$

Let $C$ be a singly-even self-dual code and let its doubly-even subcode be $C_0 = (00, \mathcal{D}) \cup (11, a + \mathcal{D})$. This means that $(1100\ldots0) \in S$ and $n \equiv 4 \pmod 8$. Let now $C$ be an extremal singly-even $[n = 24m + 8l + 4, n/2, 4m + 4]$ self-dual code, $l = 1, 2$, or an $[n = 24m + 4, n/2, 4m + 2]$ self-dual code. It follows that $\overline{C} = \mathcal{D} \cup (a + \mathcal{D})$ is a singly-even $[n = 24m + 8l + 2, n/2 - 1, 4m + 4$ or $4m + 2]$ code with shadow $\overline{S} = b + \overline{C} = (b + \mathcal{D}) \cup (a + b + \mathcal{D})$. Since $C_2 = (10, b + \mathcal{D}) \cup (01, a + b + \mathcal{D})$ has minimum weight at least $4m + 6$ if $d = 4m + 4$ and $4m + 2$ if $d = 4m + 2$ then the minimum weight $\overline{s}$ of $\overline{S}$ satisfies $\overline{s} \geq 4m + 5$ if $l = 1, 2$, and $\overline{s} = 4m + 1$ if $l = 0$. Using (1), we obtain that:

- if $l = 0$ and $d = 4m + 2$ then $\overline{C}$ is an s-extremal $[24m + 2, 12m + 1, 4m + 2]$ code ($\overline{s} = 4m + 1$),
- if $l = 1$ and $d = 4m + 4$ then $\overline{C}$ is an s-extremal $[24m + 10, 12m + 1, 4m + 2]$ code ($\overline{s} = 4m + 5$),
- if $l = 2$ and $d = 4m + 4$ then $\overline{C}$ is an s-extremal $[24m + 18, 12m + 9, 4m + 4]$ code ($\overline{s} = 4m + 5$) or an $[24m + 18, 12m + 9, 4m + 2]$ code with $\overline{s} = 4m + 5$ or $\overline{s} = 4m + 9$ since all vectors in the shadow $\overline{S}$ have weights $\equiv 1 \pmod 4$.

Conversely, if $\overline{C}$ is a self-dual code of length $24m + 8l + 2$ then the code

$$C = (00, \overline{C}_0) \cup (11\overline{C}_2) \cup (10, \overline{C}_1) \cup (01, \overline{C}_3)$$

is a self-dual code of length $24m + 8l + 4$ with minimal shadow and minimum distance $d = \min\{d(\overline{C}_0), \mathrm{wt}(\overline{C}_2) + 2, \mathrm{wt}(\overline{S}) + 1\}$. It follows that

- if $\overline{C}$ is an s-extremal $[24m + 2, 12m + 1, 4m + 2]$ code ($\overline{s} = 4m + 1$) then $C$ is a $[24m + 4, 12m + 2, 4m + 2]$ code with minimal shadow ($\mathrm{wt}(S) = 2$),
- if $\overline{C}$ is an s-extremal $[24m + 10, 12m + 5, 4m + 2]$ code ($\overline{s} = 4m + 5$) then $C$ is an extremal $[24m + 12, 12m + 6, 4m + 4]$ code with minimal shadow,
- if $\overline{C}$ is a $[24m + 18, 12m + 9, 4m + 2$ or $4m + 4]$ code with $\overline{s} \geq 4m + 5$ then $C$ is an extremal $[24m + 20, 12m + 10, 4m + 4]$ code with minimal shadow.

**Theorem 2.** (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 (*$\overline{s} = 4m + 1$*).*

(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 (*$\overline{s} = 4m + 5$*).*

(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* $\overline{s} \geq 4m + 5$.

# 3 Bounds for $s$-extremal self-dual codes

In [2] we proved that extremal self-dual codes of lengths $n = 24m+2$, $24m+4$, $24m+6$, $24m+10$ and $24m+22$ with minimal shadow do not exist. For the other lengths, we obtained the following proposition

**Proposition 1.** [2, Corollary 4, Corollary 6] *There are no extremal singly-even self-dual codes of length $n$ with minimal shadow if*

*(i)* $n = 24m+8$ *and* $m \geq 53$,

*(ii)* $n = 24m+12$ *and* $m \geq 142$,

*(iii)* $n = 24m+14$ *and* $m \geq 146$,

*(iv)* $n = 24m+16$ *and* $m \geq 164$,

*(v)* $n = 24m+18$ *and* $m \geq 157$.

We apply the same technique here to obtain similar bounds for the extremal singly-even self-dual codes of length $24m+2t$ for $1 \leq t \leq 10$, which attain the bound (1). The weight enumerators of $C$ and its shadow are given by [3]:

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

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

where $t = 4l+r$, $r = 0,1,2,3$, $l = 0,1,2$. Moreover by [6]

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

The values of $\alpha_{2m+1,0} = \alpha_{2m+1}(n)$ and $\alpha_{2m,0} = \alpha_{2m}(n)$ for $n = 24m+2t$, $t = 1,2,\ldots,10$, are calculated in [2].

**Theorem 3.** *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* $m \geq 153$.

*Proof.* Since $d = 4m+4$, it follows that $s = 12m+t+4-8m-8 = 4m+t-4 = 4m + 4l + r - 4$. According to [5] extremal self-dual codes of length $24m + 2r$ do not exist for $r = 1, 2, 3$ and $m = 1, 2, \dots, 6, 8, \dots, 12, 16, \dots, 22$. Hence we can consider only codes with $m > 23$. As $s = 4(m + l - 1) + r$, for these codes

$$a_0 = 1, \quad a_1 = a_2 = \cdots = a_{2m+1} = 0, \quad b_0 = b_1 = \cdots = b_{m+l-2} = 0.$$

Using the formula (3) and the values $\beta_{2m+1,m+l-1} = -2^{6-t}$, $\beta_{2m,m+l-1} = 2^{1-t}(2m + 1)$ and $\beta_{2m,m+l} = 2^{-t}$ [2], we obtain

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

and hence $b_{m+l-1} = -2^{t-6}\alpha_{2m+1}(n)$. Similarly,

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

Hence $b_{m+l} = 2^t\alpha_{2m}(n)-2(2m+1)b_{m+l-1} = 2^t\alpha_{2m}(n)+2^{t-5}(2m+1)\alpha_{2m+1}(n)$.

The values of $b_{m+l}$ are given in Table1.

For the given values of $n$ above the parameter $b_{m+l}$ is negative, which is impossible. □

## References


[1] C. Bachoc and P. Gaborit, Designs and self-dual codes with long shadows, *J. Combin. Theory Ser. A*, **105** (2004), 15–34.

[2] S. Bouyuklieva and W. Willems, Singly-even self-dual codes with minimal shadow, *IEEE Transactions on Information Theory* (to appear), [arXiv:1106.5936v1].

[3] J.H.Conway and N.J.A.Sloane, A new upper bound on the minimal distance of self-dual codes, *IEEE Trans. Inform. Theory*, **36** (1990), 1319–1333.

[4] N. Elkies, Lattices and codes with long shadows, *Math. Res. Lett.* (5) (1995), 643–651.

[5] S. Han and J.B. Lee, Nonexistence of some extremal self-dual codes, J. Korean Math. Soc. **43** (2006), 1357-1369.

[6] E.M. Rains, Shadow bounds for self-dual codes, *IEEE Trans. Inform. Theory* **44** (1998), 134–139.

Table 1: The coefficient $b_{m+l}$ for an $s$-extremal self-dual code of length $n$ and minimum distance $4m+4$

| $n$ | $b_{m+l}(n)$ |
|---|---|
| $24m+2$ | $\frac{(12m+1)(39-14m)}{20m}\binom{5m}{m-1}$ |
| $24m+4$ | $\frac{(15-2m)(8m+1)(6m+1)}{2m(4m+2)}\binom{5m}{m-1}$ |
| $24m+6$ | $\frac{3(4m+1)(6m+1)(-8m^2+150m+29)}{2m(4m+2)(4m+3)}\binom{5m}{m-1}$ |
| $24m+8$ | $\frac{4(3m+1)(-8m^3+334m^2+171m+21)}{m(m+1)(4m+3)}\binom{5m+1}{m-1}$ |
| $24m+10$ | $\frac{2(12m+5)(4m+1)(-8m^3+614m^2+447m+81)}{m(m+1)(4m+3)(4m+5)}\binom{5m+1}{m-1}$ |
| $24m+12$ | $\frac{24(2m+1)(-32m^4+3568m^3+4146m^2+1573m+195)}{m(m+1)(4m+5)(4m+6)}\binom{5m+2}{m-1}$ |
| $24m+14$ | $\frac{24(2m+1)(12m+7)(-32m^4+4304m^3+5850m^2+2593m+375)}{m(m+1)(4m+5)(4m+6)(4m+7)}\binom{5m+2}{m-1}$ |
| $24m+16$ | $\frac{256(3m+2)(2m+1)(-32m^4+4656m^3+7322m^2+3759m+630)}{m(m+2)(4m+5)(4m+6)(4m+7)}\binom{5m+3}{m-1}$ |
| $24m+18^*$ | $\frac{384a_m(-224m^5+33360m^4+83870m^3+77955m^2+31869m+4830)}{m(m+2)(4m+5)(4m+6)(4m+7)(4m+9)}\binom{5m+3}{m-1}$ |
| $24m+20^*$ | $\frac{64a_m(6m+5)(20m+11)(-8m^3+1210m^2+1743m+630)}{m(m+2)(2m+3)(4m+7)(4m+9)(2m+5)}\binom{5m+4}{m-1}$ |

$^*a_m = (2m+1)(4m+3)$