A class of singly even self-dual codes[1]

Stefka Bouyuklieva, Zlatko Varbanov, Katina Toncheva
Veliko Tarnovo University, BULGARIA

Abstract. Some properties of the singly even self-dual codes whose shadow contains a vector of weight 1 are considered. A new upper bound for the minimum weight of these codes is proved. Two types of secret sharing schemes based on such codes are proposed.

1 Introduction

In the present work we study a class of singly even self-dual codes with the special property that the minimum weight of their shadow is 1. Using them, we describe two types of schemes based on codes - with one-part secret and with two-part secret. A **secret sharing scheme** is a way of sharing a secret among a finite set of people or entities such that only some distinguished subsets of these have access to the secret. The collection of all such distinguished subsets is called the **access structure** of the scheme.

Our motivations are the following: First, the known codes of lengths $24m+2$ and $24m+10$ with the mentioned property are not extremal. Second, these codes enjoy some design properties. Third, their structure could be used in characterizing the access groups in a secret sharing scheme based on codes.

The article is organized as follows. Section 2 collects the necessary definitions. Section 3 is devoted to the properties of the codes. In Section 4 we describe the proposed one-part and two-part secret sharing schemes and their access structures.

2 Preliminaries

Let C be a singly even self-dual $[n, n/2, d]$ code and 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 [1] in order to derive new upper bounds for the minimum weight of singly even self-dual codes, and to provide restrictions on their weight enumerators.

[1] Partially supported by the VTU Science Fund under Contract RD-491-08/27.06.2008.

If B_r is the number of the vectors of weight r in the shadow S, $0 \le r \le n$, then $B_r = 0$ for $r \not\equiv \frac{n}{2} \pmod 4$. Moreover, $B_r \le 1$ for $r < d/2$, $B_0 = 0$, and $B_i = B_{n-i}$ for $i = 0, 1, \dots, n$ [1, Theorem 5]. It follows that $B_1 > 0$ only for lengths $n \equiv 2 \pmod 8$, and in such a case $B_1 = 1$ when $d \ge 4$.

It was shown in [4] that the minimum weight d of a self-dual code of length n is bounded by $4[n/24] + 4$ for $n \not\equiv 22 \pmod{24}$. We call a self-dual code meeting this bound extremal. Note that for some lengths, for example, length 34, no extremal self-dual code exists. A self-dual code is called optimal if it has the largest minimum weight among all self-dual codes of that length. An extremal self-dual code is automatically optimal if it exists.

Let C be a self-dual code of length $n = 24m + 8l + 2$ with $\mathrm{wt}(S) = 1$, $l = 0, 1, 2$. The weight enumerators of C and its shadow are [1]:

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

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

Using these expressions, we can write c_i as a linear combination of the a_j and as a linear combination of the b_j in the following ways [4]:

$$c_i = \sum_{j=0}^{i} \alpha_{ij} a_j = \sum_{j=0}^{3m+l-i} \beta_{ij} b_j. \qquad (1)$$

Theorem 1 (Assmus and Mattson Theorem, p.303 of [3]): *Let $A_0, A_1, \dots, A_n$ be the weight distribution of the codewords in a binary linear $[n, k, d]$ code C, and let $A_0^\perp, A_1^\perp, \dots, A_n^\perp$ be the weight distribution of the codewords in its dual $[n, n-k, d^\perp]$ code $C^\perp$. Fix a t, $0 < t < d$, and let $s = |\{i \mid A_i^\perp \ne 0, 0 < i \le n-t\}|$. Assume $s \le d - t$.*

- *If $A_i \ne 0$ and $i > 0$, then $C_i = \{c \in C \mid wt(c) = i\}$ holds a t-design.*
- *If $A_i^\perp \ne 0$ and $0 < i \le n - t$ then $C_i^\perp = \{c \in C^\perp \mid wt(c) = i\}$ holds a t-design.*

3 Optimal self-dual codes with $\mathrm{wt}(S) = 1$

Let C be an extremal $[24m + 8l + 2, 12m + 4l + 1, 4m + 4]$ code, $l = 0, 1, 2$, $m \ge 0$, $\mathrm{wt}(S) = 1$, and $(100\dots0) \in C_1$. Then $C_1 = (100\dots0) + C_0, C_2 =$

$(111\ldots1)+C_0, C_3=(011\ldots1)+C_0$, and therefore

$$W_C(y)=1+a_{2m+2}y^{4m+4}+a_{2m+3}y^{4m+6}+\cdots+a_{2m+2}y^{20m+8l-2}+y^n,$$

$$S(y)=y+(a_{2m+2}+a_{2m+3})y^{4m+5}+\cdots+(a_{2m+2}+a_{2m+3})y^{20m+8l-3}+y^{n-1}.$$

In our case $a_1=a_2=\cdots=a_{2m+1}=0$, $b_1=b_2=\cdots=b_m=0$, $a_0=1$, $b_0=1$. It follows that $c_i=\alpha_{i0}$ for $i=0,1,\ldots,2m+1$, and $c_i=\beta_{i0}$ for $i=2m+l,\ldots,3m$. Hence for $l\le 1$ we have

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

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

Proof. We know (see [1]) that extremal self-dual codes of lengths 2, 10, 26, 34, 50 and 58 do not exist. According [4], $\beta_{ij}=(-1)^i2^{-n/2+6i}\frac{k-j}{i}\binom{k+i-j-1}{k-i-j}$, where $k=\lfloor n/8\rfloor=3m+l$. Therefore

$$\beta_{2m+1,0}=-2^{5-4l}\frac{3m+l}{2m+1}\binom{5m+l}{m+l-1}.$$

In another hand, $\alpha_{i0}=-\frac{n}{2i}[\text{coeff. of } y^{i-1} \text{ in } (1+y)^{-n/2-1+4i}(1-y)^{-2i}]$

$$\Rightarrow \alpha_{2m+1,0}=-\frac{12m+4l+1}{2m+1}[\text{coeff. of } y^{2m} \text{ in } (1+y)^{4-4l}(1-y^2)^{-4m-2}].$$

As $(1-y^2)^{-4m-2}=\sum_{j=0}^{\infty}\binom{-4m-2}{j}(-1)^jy^{2j}=\sum_{j=0}^{\infty}\binom{4m+1+j}{j}y^{2j}$, then

$$\alpha_{2m+1,0}=-\frac{12m+4l+1}{2m+1}[\text{coeff. of } y^{2m} \text{ in } (1+y)^{4-4l}(\sum_{j=0}^{\infty}\binom{4m+1+j}{j}y^{2j})].$$

If $l=0$ then $\alpha_{2m+1,0}=-\frac{(12m+1)(56m+4)}{(2m+1)(m-1)}\binom{5m-1}{m-2}$.

$$\Rightarrow c_{2m+1}=-\frac{(12m+1)(56m+4)}{(2m+1)(m-1)}\binom{5m-1}{m-2}=-2^5\frac{3m}{2m+1}\binom{5m}{m-1}$$

$$\Rightarrow \frac{(12m+1)(56m+4)}{(2m+1)(m-1)}=32\frac{15m^2}{(2m+1)(m-1)} \quad \Rightarrow 48m^2+26m+1=0.$$

As this is impossible for $m \geq 0$, self-dual $[24m+2, 12m+1, 4m+4]$ codes with $\mathrm{wt}(S) = 1$ do not exist.

In the case $l = 1$ we have $\alpha_{2m+1,0} = -\dfrac{12m+5}{2m+1}\dbinom{5m+1}{m}$. Hence $c_{2m+1} = -\dfrac{12m+5}{2m+1}\dbinom{5m+1}{m} = -2\dfrac{3m+1}{2m+1}\dbinom{5m+1}{m}$ and so $6m+3 = 0$, which is impossible. Therefore self-dual $[24m+10, 12m+5, 4m+4]$ codes with $\mathrm{wt}(S) = 1$ do not exist. □

When $n = 24m+18$, we have $c_i = \alpha_{i0}$ for $i = 0, 1, \ldots, 2m+1$, and $c_i = \beta_{i0}$ for $i = 2m+2, \ldots, 3m$. Hence the values of c_i can be calculated and they do not depend on any parameters, so if self-dual $[24m+18, 12m+9, 4m+4]$ codes with $\mathrm{wt}(S) = 1$ exist, they have the same fixed weight enumerator. Moreover, their subcode C_0 has at most $4m+3$ different nonzero weights, that is why according Theorem 1, the set of codewords of weight i in C_0 for $i > 0, A_i > 0$, holds 1-designs.

Suppose that C is an optimal $[24m+8l+2, 12m+4l+1, 4m+2]$ code, $l = 0, 1$, $m \geq 0$, $\mathrm{wt}(S) = 1$ and

$$W_C(y) = 1 + a_{2m+1}y^{4m+2} + a_{2m+2}y^{4m+4} + \cdots + a_{2m+2}y^{20m-2} + a_{2m+1}y^{20m+8l} + y^n.$$

$$\Rightarrow S(y) = y + a_{2m+1}y^{4m+1} + (a_{2m+2} + a_{2m+3})y^{4m+5} + \cdots + a_{2m+1}y^{20m+8l+1} + y^{n-1}.$$

Then $a_1 = a_2 = \cdots = a_{2m} = 0$, $a_0 = 1$, $b_1 = \cdots = b_{m-1} = 0$, $b_0 = 1$. It follows that $c_i = \alpha_{i0}$ for $i = 0, 1, \ldots, 2m$, and $c_i = \beta_{i0}$ for $i = 2m+l+1, \ldots, 3m$. When $l = 0$, the values of the parameters c_i can be calculated and so the self-dual $[24m+2, 12m+1, 4m+2]$ codes with $wt(S) = 1$ have the same fixed weight enumerator. Moreover, the code C_0 has at most $4m$ different nonzero weights, that's why according Theorem 1, the set of codewords of weight i in C_0 for $i > 0, A_i > 0$, holds a 2-design.

Theorem 3 *The set of codewords of weight i in C_0 without the common zero coordinate and the set of codewords of weight i in C_2 without the common 1-coordinate for $i > 0, A_i > 0$, in an optimal self-dual $[24m+2, 12m+1, 4m+2]$ code with $\mathrm{wt}(S) = 1$ holds a 2-design. The set of codewords of weight i in C_0 without the common zero coordinate and the set of codewords of weight i in C_2 without the common 1-coordinate for $i > 0, A_i > 0$, in an extremal self-dual $[24m+18, 12m+9, 4m+4]$ code with $\mathrm{wt}(S) = 1$ holds a 1-design.*

4 Two-part secret sharing

Dougherty, Mesnager, and Sole [2] proposed the following secret sharing scheme. A secret consisting of elements of $\mathbb{F}_q$ is split into its components. Let $s \in \mathbb{F}_q$ be the secret we wish to share, and let G be a generator matrix for a code C of length n with columns $G_0, G_1, \dots, G_{n-1}$. Let v be the information vector such that $vG_0 = s$, and $u = vG$. To each party corresponding to all coordinates except the first u_i is assigned. Assume that G_0 is a linear combination of the $n-1$ columns $G_1, \dots, G_{n-1}$. The secret s is then determined by the set of shares $\{u_{i_1}, u_{i_2}, \dots, u_{i_m}\}$, if and only if G_0 is a linear combination $G_0 = \sum_{j=1}^{m} x_j G_{i_j}$, where $1 \le i_1 < \cdots < i_m \le n-1$ and $m \le n-1$. So by solving this linear equation, we find x_j and from then on the secret by $s = vG_0 = \sum_{j=1}^{m} x_j v G_{i_j} = \sum_{j=1}^{m} x_j u_{i_j}$. The set of m shares $\{u_{i_1}, u_{i_2}, \dots, u_{i_m}\}$ determines the secret if and only if there is a codeword $(1, 0, ..., 0, c_{i_1}, 0, ..., 0, c_{i_m}, 0.., 0) \in C^{\perp}$, where $c_{i_j} \neq 0$ for at least one j [2]. Let $\mathcal{P}$ be the set of parties involved in the secret sharing. In this case $\mathcal{P}$ is the set of coordinates except for the first one. The set Γ, called the **access structure** of the secret sharing scheme, consists of subsets of $\mathcal{P}$ such that any element of Γ can uncover the secret.

Here we explain a similar scheme that is the following: Let C be a singly even binary self-dual code of length n and $x = (1, 0, 0, \dots, 0) \in S$. Then the vectors in the doubly even subcode C_0 are orthogonal to x, hence their first coordinate is 0. Since all codewords of weight $\equiv 2 \pmod 4$ are in the coset $C_2 = x + C_0$, their first coordinate is 1. Also, let the codewords of C_2 of given weight i hold 1-design (excluding the first coordinate). By Theorem 3 this is true for $[24m+2, 12m+1, 4m+2]$ and $[24m+18, 12m+9, 4m+4]$ codes with $\mathrm{wt}(S) = 1$. For the secret s, the access structure contains A_i groups of size $i-1$. For that $1-$design we have $v = n-1$, $k = i-1$, and $b = A_i$. The number of ones in any column is $r = \frac{bk}{v} = \frac{A_i(i-1)}{n-1}$.

This scheme can be extended in the following way. Let the codewords of weight i (without the common coordinate $= 1$) hold $2-(v, k, \lambda_2)$ design D (that is $1-(v, k, \frac{v-1}{k-1}\lambda_2)$ design, too). We describe our technique for the codewords of given weight i, where $i \equiv 2 \pmod 4$. For the first part of the secret s, the access structure contains A_i groups of size $i-1$. We take the blocks that have 1 in the first position. There are $\frac{v-1}{k-1}\lambda_2$ such blocks. These blocks without the first point hold $1-(v-1, k-1, \lambda_1)$ design D_1, where $\lambda_1 = \lambda_2$. For the second part we take the λ_1 blocks of D_1 that have 1 in the first position. Then, for the second part of the secret, the access structure consists of λ_1 groups of size $i-3$. To recover the two-part secret we should use the groups of size $i-3$ at first. 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 $i-2$ already) and the other $\frac{v-1}{k-1}\lambda_2 - \lambda_1$ groups of size $i-2$. We add a new participant that has ones in these groups of size $i-2$ (the other values are 0). At last, we use the obtained $\frac{v-1}{k-1}\lambda_2$ groups of size $i-1$, and the other groups of the same size to recover the first part of the secret.

Example (two-part secret): Let C be a binary self-dual $[50, 25, 10]$ code with weight enumerator $1+196y^{10}+\cdots+y^{50}$. The shadow of this code contains a vector of weight 1. By Theorem 3, the set of codewords of weight i in C_0 for $i > 0, A_i > 0$, holds a 2-design. We take the set A_{10} of the vectors of weight 10. Up to equivalence, the first position in any vector $x \in A_{10}$ must be 1. Without the first column, the codewords hold $2-(49, 9, 6)$ design D (that is $1-(49, 9, 36)$ design, too). 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. 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.

In general, in the secret sharing scheme produced from the $[50, 25, 10]$ code C for the first part of the secret the access structure contains 196 groups of size 9, 31752 groups of size 13, 773073 groups of size 17, etc. It is easy to calculate that for the second part of the secret the access structure consists of 6 groups of size 7, 8424 groups of size 11, 268209 groups of size 15, etc.

References

[1] J. H. Conway, N. J. A. Sloane, A new upper bound on the minimal distance of self-dual codes, *IEEE Trans. Inform. Theory* 36, 1991, 1319-1333.

[2] S. Dougherty, S. Mesnager, P. Sole, Secret-sharing schemes based on self-dual codes, Inform. Theory Workshop, Porto, 5-9 May 2008, 338-342.

[3] W. C. Huffman, V. Pless, *Fundamentals of error-correcting codes*, Cambridge Univ. Press, 2003.

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