Korean J. Math. **26** (2018), No. 4, pp. 729–740 https://doi.org/10.11568/kjm.2018.26.4.729

EXTREMAL TYPE I ADDITIVE SELF-DUAL CODES OVER GF(4) WITH NEAR-MINIMAL SHADOW

SUNGHYU HAN

ABSTRACT. In this paper, we define near-minimal shadow and study the existence problem of extremal Type I additive self-dual codes over GF(4) with near-minimal shadow. We prove that there is no such codes if the code length $n = 6m+1 (m \ge 0), n = 6m+5 (m \ge 1)$.

1. Introduction

The additive code C over GF(4) of length n is an additive subgroup of $GF(4)^n$. The weight of a codeword $u = (u_1, u_2, \ldots, u_n)$ in $GF(4)^n$ is the number of non-zero u_j and is denoted by wt(u). The minimum distance of C is the smallest non-zero weight of any codeword in C. Here, C is a k-dimensional GF(2)-subspace of $GF(4)^n$, and, therefore, it has 2^k codewords. It is denoted as an $(n, 2^k)$ code, and, if its minimum distance is d, the code is an $(n, 2^k, d)$ code.

The trace map, $\text{Tr} : GF(4) \to GF(2)$, is defined by $\text{Tr}(x) = x + x^2$. The Hermitian trace inner product of two vectors over GF(4) of length $n, u = (u_1, u_2, ..., u_n)$ and $v = (v_1, v_2, ..., v_n)$ is given by

(1)
$$u * v = \sum_{i=1}^{n} \operatorname{Tr}(u_i v_i^2) = \sum_{i=1}^{n} (u_i v_i^2 + u_i^2 v_i) \pmod{2}.$$

Received August 31, 2018. Revised December 11, 2018. Accepted December 12, 2018.

2010 Mathematics Subject Classification: 94B05.

Key words and phrases: additive codes over GF(4), extremal codes, minimal shadow, near-minimal shadow, self-dual codes.

© The Kangwon-Kyungki Mathematical Society, 2018.

This is an Open Access article distributed under the terms of the Creative commons Attribution Non-Commercial License (http://creativecommons.org/licenses/by -nc/3.0/) which permits unrestricted non-commercial use, distribution and reproduction in any medium, provided the original work is properly cited.

We define the dual of the code C with respect to the Hermitian trace inner product as follows:

(2)
$$C^{\perp} = \{ u \in GF(4)^n : u * c = 0 \text{ for all } c \in C \}.$$

If $C \subseteq C^{\perp}$, we say C is self-orthogonal, and if $C = C^{\perp}$, we say C is self-dual. If C is self-dual, then it must be an $(n, 2^n)$ code.

We distinguish between two types of additive self-dual codes over GF(4). A code is Type II if all codewords have even weights, otherwise it is Type I. Bounds on the minimum distance of additive self-dual codes over GF(4) were provided in [9].

THEOREM 1.1. [9] Let C be an $(n, 2^n, d)$ additive self-dual code over GF(4). If C is Type I, then

(3)
$$d \leq \begin{cases} 2[n/6] + 1, & \text{if } n \equiv 0 \pmod{6}; \\ 2[n/6] + 3, & \text{if } n \equiv 5 \pmod{6}; \\ 2[n/6] + 2, & \text{otherwise.} \end{cases}$$

If C is Type II, then

(4)
$$d \le 2[n/6] + 2$$

A code that meets the appropriate bound is called extremal. The proof of Theorem 1.1 for Type I codes is formulated using a shadow code, which is defined as follows: Let C be an additive self-dual code over GF(4) and C_0 be the subset of C consisting of all codewords whose weights are multiples of two. Then, C_0 is a subgroup of C. The shadow code of an additive code C over GF(4) is defined by:

(5)
$$S = C_0^{\perp} \backslash C.$$

Alternately, it can be defined as:

(6)

$$S = \{ u \in GF(4)^n \mid u * v = 0 \text{ for all } v \in C_0, \ u * v = 1 \text{ for all } v \in C \setminus C_0 \}.$$

Bautista, et al. [1] studied the minimum weight d of C and the minimum weight s of S simultaneously, and they showed that $2d+s \le n+2$, unless n = 6m + 5 and d = 2m + 3, in which 2d + s = n + 4. If equality holds, i.e., 2d + s = n + 2 (or 2d + s = n + 4), then the codes are called *s*-extremal. They also classified *s*-extremal codes with $1 \le d \le 4$.

On the other hand, the author made a research for the smallest value s of S [4]. The following is the definition of minimal shadow.

DEFINITION 1.2. [4] Let C be a Type I additive self-dual code over GF(4) of length $n = 6m + r(0 \le r \le 5)$. Then, C is a code with minimal shadow if:

- 1. d(S) = 1 if r = 1, 3, 5; and
- 2. d(S) = 2 if r = 0, 2, 4,

where d(S) is the minimum weight of S.

The author proved nonexistence of extremal self-dual codes with minimal shadow [4]. More specific, the author proved that extremal Type I additive self-dual codes over GF(4) of lengths n = 6m + 1, 6m + 5with minimal shadow do not exist. The author also proved that there are no extremal Type I additive self-dual codes over GF(4) of length nwith minimal shadow if $n = 6m(m \ge 40)$, $n = 6m + 2(m \ge 6)$, and $n = 6m + 3(m \ge 22)$.

The author studied near-extremal additive self-dual codes over GF(4) with minimal shadow [5]. The following is the definition of near-extremal codes.

DEFINITION 1.3. Let C be an $(n, 2^n, d)$ Type I additive self-dual code over GF(4). Then, C is near-extremal if: d = 2[n/6] if $n \equiv 0 \pmod{6}$, d = 2[n/6] + 2 if $n \equiv 5 \pmod{6}$, and d = 2[n/6] + 1 otherwise.

The author proved that there are no near-extremal Type I additive self-dual codes over GF(4) of length n with minimal shadow if $n = 6m + 1 (m \ge 22)$ [5].

In this paper, we study near-minimal shadow. In the following, we give the definition of a code with near-minimal shadow.

DEFINITION 1.4. Let C be a Type I additive self-dual code over GF(4) of length $n = 6m + r(0 \le r \le 5)$. Then, C is a code with near-minimal shadow if:

1. d(S) = 3 if r = 1, 3, 5; and

2. d(S) = 4 if r = 0, 2, 4,

where d(S) is the minimum weight of S.

The main result of this paper is the following theorem.

1.

THEOREM 1.5. There are no extremal Type I additive self-dual codes over GF(4) of length n with near-minimal shadow if

1.
$$n = 6m + 1;$$

2. $n = 6m + 5$ and $m >$

$(d,s)\backslash p$	0	1	2	3	4	5
(ext, min)	≥ 40	х	≥ 6	≥ 22		х
(n-ext, min)		≥ 22				
(ext, n-min)		х				≥ 1

TABLE 1. Non-existence of extremal(or near-extremal) Type I additive self-dual codes over GF(4) with minimal(or near-minimal) shadow of length n = 6m + p

We summarize the results so far in Table 1. In the table, we give the results of non-existence of extremal(or near-extremal) Type I additive self-dual codes over GF(4) with minimal(or near-minimal) shadow of length n = 6m + p, $(0 \le p \le 5)$. The first row of the table represent the value p, and the first column of the table represents extremal(or near-extremal) w.r.t. the minimum weight d of C and minimal(or near-minimal) w.r.t. the minimum weight s of S. More specific, (ext, min) corresponds to the case d is extremal and s is minimal, (n-ext, min) corresponds to the case d is near-extremal and s is minimal. In the table, 'x' represents the non-existence of the corresponding codes. ' \geq number' represents the non-existence of the corresponding codes if $m \ge$ number.

This paper is organized by the following. In section 2, we give the proof of Theorem 1.5. In section 3, we give example codes. In section 4, we give the summary of this paper. All the computation of this paper were done with Maple software and Magma [2].

REMARK 1.6. In [6], the author made a research for near-minimal shadow of binary self-dual codes. In the paper, the author defined nearminimal shadow and studied the existence problem of extremal Type I binary self-dual codes with near-minimal shadow. The author proved that there is no such codes if the code length $n = 24m + 2(m \ge 0)$, $n = 24m + 4(m \ge 9)$, $n = 24m + 6(m \ge 21)$, and $n = 24m + 10(m \ge 87)$. The structure of this paper is similar to the one of the paper [6].

2. Proof of Theorem 1.5

In this section, we give the proof of Theorem 1.5. The weight enumerator of a code is given by

(7)
$$W_C(x,y) = \sum_{i=0}^{n} A_i x^{n-i} y^i,$$

where there are A_i codewords of weight *i* in *C*. The following lemma is needed in this paper.

LEMMA 2.1. [4] Let C be a Type I additive self-dual code over GF(4)and S be the shadow code of C. If $u, v \in S$, then $u + v \in C$.

LEMMA 2.2. [4] Let C be an additive self-dual code over GF(4) of length n and minimum weight d. Let $S(y) = \sum_{r=0}^{n} B_r y^r$ be the weight enumerator of S. Then:

1. $B_0 = 0;$ 2. $B_r \le 1$ for r < d/2.

Let C be a Type I additive self-dual code over GF(4). By [9], the weight enumerator of C, $W_C(x, y)$, and its shadow code weight enumerator, $W_S(x, y)$, are given by:

(8)
$$W_C(x,y) = \sum_{i=0}^{[n/2]} c_i (x+y)^{n-2i} \{y(x-y)\}^i,$$

(9)
$$W_S(x,y) = \sum_{i=0}^{[n/2]} (-1)^i 2^{n-3i} c_i y^{n-2i} (x^2 - y^2)^i,$$

for suitable constants c_i . We rewrite Eqn. (8) and Eqn. (9) to the following:

(10)
$$W_C(1,y) = \sum_{j=0}^n a_j y^j = \sum_{i=0}^{[n/2]} c_i (1+y)^{n-2i} \{y(1-y)\}^i$$

and

(11)
$$W_S(1,y) = \sum_{j=0}^{[n/2]} b_j y^{2j+t} = \sum_{i=0}^{[n/2]} (-1)^i 2^{n-3i} c_i y^{n-2i} (1-y^2)^i,$$

where t = 0 if n is even, and t = 1 if n is odd. Note that all a_j and b_j must be nonnegative integers. One can write c_i as a linear combination of the a_j for $0 \le j \le i$, and one can write c_i as a linear combination of b_j for $0 \le j \le [n/2] - i$ in the following form for suitable constants α_{ij} and β_{ij} :

(12)
$$c_i = \sum_{j=0}^{i} \alpha_{ij} a_j = \sum_{j=0}^{[n/2]-i} \beta_{ij} b_j.$$

In our computation, we need to calculate α_{i0} and β_{ij} . The following formulas can be found in [9] for i > 0:

(13)
$$\alpha_{i0} = -\frac{n}{i} \left[\text{coeff. of } y^{i-1} \text{ in } (1+y)^{-n-1+2i} (1-y)^{-i} \right]$$

and

(14)
$$\beta_{ij} = (-1)^{i} 2^{3i-n} \binom{k-j}{i},$$

where k = [n/2]. Note that $a_0 = c_0 = \alpha_{00} = 1$. In the following lemma, we give another formula for α_{i0} .

LEMMA 2.3. Let $0 \le i \le \lfloor n/2 \rfloor$. Then we have

$$\alpha_{i,0} = \begin{cases} -\frac{n}{i} \sum_{t=0,t+i \text{ is odd}}^{n+1-3i} (-1)^t \binom{n+1-3i}{t} \binom{\frac{2n-3i-t-1}{2}}{\frac{i-t-1}{2}}, & \text{if } n+1-3i \ge 0; \\ -\frac{n}{i} \sum_{0 \le t \le [\frac{i-1}{2}]} \binom{n-2i+t}{t} \binom{-n+4i-3-2t}{i-1-2t}, & \text{else.} \end{cases}$$

Proof. From Eqn. (13), we have

(15)
$$\alpha_{i0} = -\frac{n}{i} \left[\text{coeff. of } y^{i-1} \text{ in } (1+y)^{-n-1+2i} (1-y)^{-i} \right].$$

And

(16)
$$(1+y)^{-n-1+2i}(1-y)^{-i} = (1-y^2)^{-n-1+2i}(1-y)^{n+1-3i}.$$

Suppose that $n + 1 - 3i \ge 0$. Since

$$(1-y^2)^{-n-1+2i}(1-y)^{n+1-3i} = (1-y^2)^{-n-1+2i} \sum_{t=0}^{n+1-3i} (-1)^t \binom{n+1-3i}{t} y^t,$$

we have

$$\alpha_{i0} = -\frac{n}{i} \sum_{t=0}^{n+1-3i} (-1)^t \binom{n+1-3i}{t} \left[\text{coeff. of } y^{i-1} \text{ in } (1-y^2)^{-n-1+2i} y^t \right].$$

Note that

(17)
$$(1-y^2)^{-n-1+2i}y^t = \sum_{0 \le j} \binom{n+1-2i+j-1}{j} y^{2j+t}.$$

In Eqn. (17), we use the following formula.

(18)
$$(1-x)^{-a} = \sum_{0 \le j} {\binom{-a}{j}} (-1)^j x^j = \sum_{0 \le j} {\binom{a+j-1}{j}} x^j,$$

for a > 0. In Eqn. (17), let 2j + t = i - 1. Then $j = \frac{i-t-1}{2}$. Therefore,

$$\begin{aligned} \alpha_{i0} &= -\frac{n}{i} \sum_{t=0,t+i \text{ is odd}}^{n+1-3i} (-1)^t \binom{n+1-3i}{t} \binom{n+1-2i+\frac{i-t-1}{2}-1}{\frac{i-t-1}{2}}, \\ &= -\frac{n}{i} \sum_{t=0,t+i \text{ is odd}}^{n+1-3i} (-1)^t \binom{n+1-3i}{t} \binom{\frac{2n-3i-t-1}{2}}{\frac{i-t-1}{2}}. \end{aligned}$$

Suppose that n + 1 - 3i < 0. Since

(19)
$$(1-y^2)^{-n-1+2i}(1-y)^{n+1-3i} \\ = \left[\sum_{0 \le t} \binom{n+1-2i+t-1}{t} y^{2t}\right] \times \left[\sum_{0 \le j} \binom{-n-1+3i+j-1}{j} y^j\right] \\ = \sum_{0 \le t,j} \binom{n-2i+t}{t} \binom{-n-2+3i+j}{j} y^{2t+j},$$

we have

(20)
$$\alpha_{i0} = -\frac{n}{i} \sum_{0 \le t,j \text{ and } 2t+j=i-1} \binom{n-2i+t}{t} \binom{-n-2+3i+j}{j} y^{2t+j}.$$

Let j = i - 1 - 2t in Eqn. (20). Then we have the following result.

(21)
$$\alpha_{i0} = -\frac{n}{i} \sum_{0 \le t \le \left[\frac{i-1}{2}\right]} {n-2i+t \choose t} {-n-2+3i+i-1-2t \choose i-1-2t}$$

(22)
$$= -\frac{n}{i} \sum_{0 \le t \le \left[\frac{i-1}{2}\right]} \binom{n-2i+t}{t} \binom{-n+4i-3-2t}{i-1-2t}.$$

This completes the proof.

Throughout this section, we assume that C be an extremal Type I additive self-dual code over GF(4) with near-minimal shadow of length n = 6m + r. In the following subsection, we prove the first part of Theorem 1.5.

2.1. The case n = 6m + 1. Suppose that r = 1. Since C is extremal, we have $a_0 = 1, a_1 = a_2 = \cdots = a_{2m+1} = 0$. By Lemma 2.2, we have $b_0 = 0, b_1 = 1$ if $m \ge 3$. Also we have $b_2 = b_3 = \cdots = b_{m-2} = 0$. Otherwise, S would contain a vector v of weight less than or equal to 2m - 4 + 1, and if $u \in S$ is a vector of weight 3, then $u + v \in C$ with wt $(u + v) \le 2m$, a contradiction to the minimum distance of C.

Using Eqn. (12) and the above discussion, we have the following.

(23)
$$c_i = \sum_{j=0}^{i} \alpha_{ij} a_j = \alpha_{i0} \ (0 \le i \le 2m+1)$$

and

(24)
$$c_i = \sum_{j=0}^{3m-i} \beta_{ij} b_j = \beta_{i1} + \sum_{j=2}^{3m-i} \beta_{ij} b_j = \beta_{i1} \ (2m+2 \le i \le 3m-1).$$

Note that $c_{3m} = 0$.

From Eqn. (23) and Eqn. (24) we have

(25)
$$c_{2m+1} = \alpha_{2m+1,0} = \beta_{2m+1,1} + \beta_{2m+1,m-1}b_{m-1}.$$

Therefore, we get:

(26)
$$b_{m-1} = \frac{\alpha_{2m+1,0} - \beta_{2m+1,1}}{\beta_{2m+1,m-1}}.$$

From Eqn. (13) and Eqn. (14) we have

(27)
$$\alpha_{2m+1,0} = -\frac{6m+1}{2m+1} \binom{3m}{m}$$

and

(28)
$$\beta_{2m+1,1} = -4 \times \binom{3m-1}{2m+1}, \ \beta_{2m+1,m-1} = -4.$$

Therefore, we get:

(29)
$$b_{m-1} = \frac{6m+1}{4(2m+1)} \binom{3m}{m} - \binom{3m-1}{2m+1}.$$

736

From Eqn. (23) and Eqn. (24) we have

(30)
$$c_{2m} = \alpha_{2m,0} = \beta_{2m,1} + \beta_{2m,m-1}b_{m-1} + \beta_{2m,m}b_m$$

Therefore, we get:

(31)
$$b_m = \frac{\alpha_{2m,0} - \beta_{2m,1} - \beta_{2m,m-1} b_{m-1}}{\beta_{2m,m}}$$

From Eqn. (13) and Eqn. (14) we have

(32)
$$\alpha_{2m,0} = \frac{6m+1}{m} \binom{3m}{m-1}$$

and

(33)
$$\beta_{2m,1} = \frac{1}{2} \binom{3m-1}{2m}, \ \beta_{2m,m-1} = \frac{2m+1}{2}, \ \beta_{2m,m} = \frac{1}{2}.$$

Therefore, we get:

(34)
$$b_m = -\frac{(3m-1)!f(m)}{4(2m+1)!(m-1)!} ,$$

where

(35)
$$f(m) = 28m^2 - 108m - 13.$$

We can see that f(m) > 0 if $m \ge 4$. Therefore, if $m \ge 4$, then $b_m < 0$. This is a contradiction. We know that there is no extremal code if m = 0, 1, 2, 3 [8]. This completes the first part of Theorem 1.5.

2.2. The case n = 6m + 5. In this subsection, we prove the second part of Theorem 1.5. Suppose that r = 5. Since C is extremal, we have $a_0 = 1, a_1 = a_2 = \cdots = a_{2m+2} = 0$. By Lemma 2.2, we have $b_0 = 0$, $b_1 = 1$ if $m \ge 2$. Also we have $b_2 = b_3 = \cdots = b_{m-1} = 0$. Otherwise, S would contain a vector v of weight less than or equal to 2m - 2 + 1, and if $u \in S$ is a vector of weight 3, then $u + v \in C$ with wt $(u + v) \le 2m + 2$, a contradiction to the minimum distance C.

Using Eqn. (12) and the above discussion, we have the following.

(36)
$$c_i = \sum_{j=0}^{i} \alpha_{ij} a_j = \alpha_{i0} \ (0 \le i \le 2m+2)$$

and

(37)
$$c_i = \sum_{j=0}^{3m+2-i} \beta_{ij} b_j = \beta_{i1} + \sum_{j=2}^{3m+2-i} \beta_{ij} b_j = \beta_{i1} \ (2m+3 \le i \le 3m+1).$$

Note that $c_{3m+2} = 0$. From Eqn. (36) and Eqn. (37) we have

(38)
$$c_{2m+2} = \alpha_{2m+2,0} = \beta_{2m+2,1} + \beta_{2m+2,m} b_m.$$

Therefore, we get:

(39)
$$b_m = \frac{\alpha_{2m+2,0} - \beta_{2m+2,1}}{\beta_{2m+2,m}}$$

From Eqn. (13) and Eqn. (14) we have

(40)
$$\alpha_{2m+2,0} = 0$$

and

(41)
$$\beta_{2m+2,1} = 2 \times {\binom{3m+1}{m-1}}, \ \beta_{2m+2,m} = 2.$$

Therefore, we get:

(42)
$$b_m = -\binom{3m+1}{m-1}.$$

Note that b_m is negative. Therefore if $m \ge 2$, then the code does not exist. If m = 1, then C is a $(11, 2^{11}, 5)$ extremal code. For this case, we can easily check that the code is not near-extremal(see Example 3.2 in Section 3). This completes the second part of Theorem 1.5.

3. Exmaples

In this section, we give two example codes. One is an extremal Type I code with near-minimal shadow. The other is an extremal Type I code but not near-minimal.

EXAMPLE 3.1. There is unique $(5, 2^5, 3)$ extremal code [7]. We can easily find a generator matrix G for the code.

(43)
$$G = \begin{pmatrix} 0 & 0 & w & w^2 & w^2 \\ 1 & 0 & w & 1 & w \\ w & 0 & w^2 & w & w^2 \\ 0 & 1 & w & w & 1 \\ 0 & w & w^2 & w^2 & w \end{pmatrix}$$

The weight enumerator is

(44)
$$W(1,y) = 1 + 10y^3 + 15y^4 + 6y^5$$

and the shadow weight enumerator is

(45)
$$S(1,y) = 20y^3 + 12y^5.$$

Therefore the code is near-minimal.

EXAMPLE 3.2. There is unique $(11, 2^{11}, 5)$ extremal code [3]. The generator matrix is QC_{11} [3].

The weight enumerator is

(47)
$$W(1,y) = 1 + 198y^5 + 198y^6 + 990y^7 + 495y^8 + 1650y^9 + 330y^{10} + 234y^{11}$$

and the shadow weight enumerator is

(48)
$$S(1,y) = 132y^5 + 660y^7 + 1100y^9 + 156y^{11}.$$

Therefore QC_{11} is not near-minimal.

4. Summary

In this paper, we gave the definition of near-minimal shadow and proved that there is no extremal Type I additive self-dual codes over GF(4) with near-minimal shadow if the code length n = 6m + 1, $n = 6m + 5 (m \ge 1)$. We have also considered *near-extremal* Type I additive self-dual codes over GF(4) with *near-minimal* shadow. But we could not obtain the similar results. In the future work, it is worth while to improve Table 1.

References

- E.P. Bautista, P. Gaborit, J.-L. Kim, J.L. Walker, s-extremal additive codes, Adv. Math. Commun. 1 (2007), 111–130.
- [2] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system I: The user language, J. Symbolic Comput. 24 (1997), 235–265.
- [3] P. Gaborit, W.C. Huffman, J.-L. Kim, V. Pless, On additive GF(4) codes, in: A. Barg, S. Litsyn (Eds.), Codes and Association Schemes, DIMACS Series in Discrete Mathematics and Theoretical Computer Science 56, American Mathematical Society, Providence, RI, 2001, 135–149.
- [4] S. Han, Additive self-dual codes over GF(4) with minimal shadow, MDPI Information 9 81 (2018), 1–11.
- [5] S. Han, Near-Extremal Type I Self-Dual Codes with Minimal Shadow over GF(2) and GF(4), MDPI Information 9 172 (2018), 1–12.
- [6] S. Han, On the extremal Type I binary self-dual codes with near-minimal shadow, submitted.
- [7] G. Hhn, Self-dual codes over the Kleinian four group, Math. Ann. 327 (2003), 227-255.
- [8] W.C. Huffman, On the classification and enumeration of self-dual codes, Finite Fields Appl. 11 (2005), 451–490.
- [9] E.M. Rains, Shadow bounds for self-dual codes, IEEE Trans. Inform. Theory 44 (1998), 134–139.

Sunghyu Han School of Liberal Arts KoreaTech Cheonan 31253, Korea *E-mail*: sunghyu@koreatech.ac.kr