information

MDPI

Article

Additive Self-Dual Codes over $GF(4)$ with Minimal Shadow

Sunghyu Han

School of Liberal Arts, Korea University of Technology and Education, Cheonan 31253, Korea; sunghyu@koreatech.ac.kr; Tel.: +82-41-640-8611

Received: 19 March 2018; Accepted: 5 April 2018; Published: 7 April 2018

Abstract: We define additive self-dual codes over $GF(4)$ with minimal shadow, and we prove the nonexistence of extremal Type I additive self-dual codes over $GF(4)$ with minimal shadow for some parameters.

Keywords: additive codes over $GF(4)$; minimal shadow; self-dual codes

1. Introduction

There are many interesting classes of codes in coding theory such as cyclic codes, quadratic residue codes, algebraic geometry codes, and self-dual codes. This study focuses on self-dual codes, which are closely related to other mathematical structures such as block designs, lattices, modular forms, and sphere packings (see [1] for example).

For the error correction, the minimum weight of self-dual codes is very important. One research direction for self-dual codes is to find the highest minimum weight of the codes. In general, if the code length is small, the highest minimum weight of self-dual codes is easily found. However, if the code length is large, then determining the highest minimum weight of self-dual codes becomes difficult. In this case, we can use the upper bound of the highest minimum weight. The code meeting the upper bound is called an extremal.

Conway and Sloane gave an upper bound on the minimum weight of binary self-dual codes [2]. They used the concept of shadow codes. Using the same concept, Rains improved the bound on the minimum weight of binary self-dual codes and applied the same technique to additive self-dual codes over $GF(4)$ [3].

Many papers have been published on shadow codes. Among them, Bouyuklieva and Willems studied binary self-dual codes for which the minimum weight of the shadow codes had the smallest possible value. They proved that extremal binary self-dual codes with minimal shadow for particular parameters do not exist [4].

The purpose of this study is to apply the idea and technique of Bouyuklieva and Willems to additive self-dual codes over $GF(4)$. In particular, we define additive self-dual codes over $GF(4)$ with minimal shadow and prove the nonexistence of extremal additive self-dual codes over $GF(4)$ with minimal shadow for some parameters.

This paper is organized in the following manner: In Section 2, we state the basic definitions and facts for additive self-dual codes over $GF(4)$. In Section 3, we define additive self-dual codes over $GF(4)$ with minimal shadow and prove that extremal Type I additive self-dual codes over $GF(4)$ with minimal shadow of length $n = 6m + r$ for $r = 1, 5$ do not exist. For $r = 0, 2, 3$, we prove the nonexistence of such codes if $m \geq 40, m \geq 6, m \geq 22$, respectively. In Section 4, we summarize this paper and add some comments to our findings.

2. Preliminaries

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

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

Note that $u * v$ is also the number (modulo 2) of places where u and v have different non-zero values. We define the dual of the code C with respect to the Hermitian trace inner product as follows:

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

If $C \subseteq C^{\perp}$, we say C is self-orthogonal, and, if $C = C^{\perp}$, we say C is self-dual. It has been shown that additive self-orthogonal codes over $GF(4)$ can be used to represent quantum error-correcting codes [5]. If C is self-dual, then it must be an $(n, 2^n)$ code. Additive self-dual codes over $GF(4)$ correspond to zero-dimensional quantum codes, which represent single quantum states. If the code has a high minimum distance, then the corresponding quantum state is highly entangled.

We distinguished between two types of additive self-dual codes over $GF(4)$. If all codewords have an even weight, it is a Type II code; otherwise, it is a Type I code. It can be shown that a Type II code must have an even length value. Bounds on the minimum distance of self-dual codes were given by Rains and Sloane.

Theorem 1. *([1,3]) Let C be an $(n, 2^n, d)$ additive self-dual code over $GF(4)$. If C is Type I, then $d \leq 2[n/6] + 1$ if $n \equiv 0 \pmod 6$, $d \leq 2[n/6] + 3$ if $n \equiv 5 \pmod 6$, and $d \leq 2[n/6] + 2$. If C is Type II, then $d \leq 2[n/6] + 2$.*

A code that meets the appropriate bound is called extremal. It can be shown that extremal Type II codes must have a unique weight enumerator. The proof of Theorem 1 was given by using the shadow code, which is defined in the following text.

Let C be an additive self-dual code over $GF(4)$ and C_0 be the subset of C, consisting of all even weight codewords. Then, C_0 is a subgroup of C. The shadow code of an additive code C over $GF(4)$ is defined as follows:

$$S = C_0^{\perp} \backslash C, \tag{3}$$

or equivalently,

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

The weight enumerator of an additive code is given as follows:

$$W_C(x, y) = \sum_{i=0}^{n} A_i x^{n-i} y^i. \tag{5}$$

Here, we have A_i codewords of weight i in C. We are only interested in Type I codes. From now on, let us assume C as a Type I code. According to [3], the weight enumerator of C, $W_C(x,y)$, and its shadow code weight enumerator, $W_S(x,y)$, are given as follows:

$$W_C(x,y) = \sum_{i=0}^{[n/2]} c_i(x+y)^{n-2i}\{y(x-y)\}^i, \tag{6}$$

$$W_S(x,y) = \sum_{i=0}^{[n/2]} (-1)^i 2^{n-3i} c_i y^{n-2i}(x^2-y^2)^i. \tag{7}$$

We have these equations for suitable constants c_i. We rewrite Equations (6) and (7) as follows:

$$W_C(1,y) = \sum_{j=0}^{n} a_j y^j = \sum_{i=0}^{[n/2]} c_i(1+y)^{n-2i}\{y(1-y)\}^i, \tag{8}$$

$$W_S(1,y) = \sum_{j=0}^{[n/2]} b_j y^{2j+t} = \sum_{i=0}^{[n/2]} (-1)^i 2^{n-3i} c_i y^{n-2i}(1-y^2)^i. \tag{9}$$

Here, $t = 0$ if n is even, and $t = 1$ if n is odd. Note that $a_0 = 1$, and all a_j and b_j must be non-negative integers. c_i can be written as a linear combination of a_j for $0 \leq j \leq i$, and c_i as a linear combination of b_j for $0 \leq j \leq [n/2] - i$ as depicted in the following form:

$$c_i = \sum_{j=0}^{i} \alpha_{ij} a_j = \sum_{j=0}^{[n/2]-i} \beta_{ij} b_j. \tag{10}$$

We have these equations for suitable constants α_{ij} and β_{ij}.

In our computation, we calculate α_{i0} and β_{ij}. The following formulas can be found in [3]. For $i > 0$, we have the following equations:

$$\alpha_{i0} = -\frac{n}{i}\left[\text{coeff. of } y^{i-1} \text{ in } (1+y)^{-n-1+2i}(1-y)^{-i}\right], \tag{11}$$

$$\beta_{ij} = (-1)^i 2^{3i-n}\binom{k-j}{i}. \tag{12}$$

Here, $k = [n/2]$.

3. Extremal Type I Additive Self-Dual Codes over *GF*(4) with Minimal Shadow

In this section, we study Type I additive self-dual codes over $GF(4)$ for which the minimum weight of the shadow code has the smallest possible value. We especially define a code with minimal shadow and prove that no extremal Type I additive self-dual codes over $GF(4)$ with minimal shadow for some parameters exist. We start with the following definition:

Definition 1. *Let C be a Type I additive self-dual code over $GF(4)$ of length $n = 6m + r (0 \leq r \leq 5)$. Then, C is a code with minimal shadow if*

1. *$d(S) = 1$ if $r > 0$;*
2. *$d(S) = 2$ if $r = 0$.*

Here, $d(S)$ is the minimum weight of S.

Lemma 1. *Let C be a Type I additive self-dual code over $GF(4)$ and S the shadow code of C. If $u, v \in S$, then $u + v \in C$.*

Proof. Considering $u, v \in S$, and then using Equation (4), if $z \in C_0$ then $u * z = 0$ and $v * z = 0$. If $z \in C \backslash C_0$, then $u * z = 1$ and $v * z = 1$. Thus, $(u+v) * z = u * z + v * z = 0 + 0 = 0$ for all $z \in C_0$, and $(u+v) * z = u * z + v * z = 1 + 1 = 0$ for all $z \in C \backslash C_0$. Therefore, $u + v \in C^{\perp} = C$. □

Lemma 2. *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, we have the following values:*

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

Proof. Because $S = C_0^{\perp} \backslash C$, $B_0 = 0$. Hence, this completes the first statement. Considering $B_r > 1$ for $r < d/2$, let $u, v \in S$ with $\mathrm{wt}(u) = \mathrm{wt}(v) = r$ and $u \neq v$. Then, $u + v \in C$ and $0 < \mathrm{wt}(u+v) \leq 2r < d$. This is a contradiction. Hence, this completes the second statement. □

In the following text, we prove the uniqueness of weight enumerators for some codes. For this, we need to look at the observation mentioned below. Let C be an extremal Type I additive self-dual code over $GF(4)$ with a minimal shadow of length $n = 6m + r$. We have the following equations:

$$W_C(1, y) = \sum_{j=0}^{n} a_j y^j \tag{13}$$

and

$$W_S(1, y) = \sum_{j=0}^{[n/2]} b_j y^{2j+t}. \tag{14}$$

Here, $t = 0$ if n is even, and $t = 1$ if n is odd.

If $r = 0$, then C is a $(6m, 2^{6m}, 2m+1)$ code. The minimum weight of the shadow code is two, and $a_0 = 1$ and $a_1 = a_2 = \ldots = a_{2m} = 0$. $b_0 = 0$. By Lemma 2, $b_1 = 1$ if $m \geq 2$. In addition, we have $b_2 = b_3 = \ldots = b_{m-1} = 0$. Otherwise, S contains a vector v bearing weight that is less than or equal to $2m - 2$, and, if $u \in S$ is a vector of weight two, then $u + v \in C$, with $wt(u+v) \leq 2m - 2 + 2 = 2m$, which is a contradiction to the minimum distance of C.

If $r = 1, 3$, then C is a $(6m + r, 2^{6m+r}, 2m+2)$ code. The minimum weight of the shadow code is one, and $a_0 = 1$ and $a_1 = a_2 = \ldots = a_{2m+1} = 0$. By Lemma 2, $b_0 = 1$ if $m \geq 1$. In addition, we have $b_1 = b_2 = \ldots = b_{m-1} = 0$. Otherwise, S contains a vector v bearing weight that is less than or equal to $2m - 1$, and, if $u \in S$ is a vector of weight one, then $u + v \in C$, with $wt(u+v) \leq 2m - 1 + 1 = 2m$, which is a contradiction to the minimum distance of C.

If $r = 2, 4$, then C is a $(6m + r, 2^{6m+r}, 2m+2)$ code. The minimum weight of the shadow code is two, and $a_0 = 1$ and $a_1 = a_2 = \ldots = a_{2m+1} = 0$. $b_0 = 0$. By Lemma 2, $b_1 = 1$ if $m \geq 2$. In addition, we have $b_2 = b_3 = \ldots = b_{m-1} = 0$. Otherwise, S contains a vector v bearing weight that is less than or equal to $2m - 2$, and, if $u \in S$ is a vector of weight two, then $u + v \in C$, with $wt(u+v) \leq 2m - 2 + 2 = 2m$, which is a contradiction to the minimum distance of C.

If $r = 5$, then C is a $(6m + 5, 2^{6m+5}, 2m+3)$ code. The minimum weight of the shadow code is one, and $a_0 = 1$ and $a_1 = a_2 = \ldots = a_{2m+2} = 0$. By Lemma 2, $b_0 = 1$. In addition, we have $b_1 = b_2 = \ldots = b_{m-1} = b_m = 0$. Otherwise, S contains a vector v bearing weight that is less than or equal to $2m + 1$, and, if $u \in S$ is a vector of weight one, then $u + v \in C$, with $wt(u+v) \leq 2m + 1 + 1 = 2m + 2$, which is a contradiction to the minimum distance of C.

Now, we are ready to prove the following theorem.

Theorem 2. *Extremal Type I additive self-dual codes over $GF(4)$ with minimal shadow of lengths $n = 6m, 6m+1, 6m+2, 6m+3$, and $6m+5$ have uniquely determined weight enumerators.*

Proof. Let C be an extremal Type I additive self-dual code over $GF(4)$ with a minimal shadow of length n. We rewrite Equation (10) in the following manner:

$$c_i = \sum_{j=0}^{i} \alpha_{ij} a_j = \sum_{j=0}^{[n/2]-i} \beta_{ij} b_j. \tag{15}$$

Let $n = 6m$, and, considering $m \geq 2$, we have the following equations:

$$c_i = \sum_{j=0}^{i} \alpha_{ij} a_j = \alpha_{i0} \ \text{ for } \ i = 0, 1, 2, \ldots, 2m, \tag{16}$$

$$c_i = \sum_{j=0}^{3m-i} \beta_{ij} b_j = \beta_{i1} \ \text{ for } \ i = 2m+1, 2m+2, \ldots, 3m. \tag{17}$$

Hence, we prove that c_i is uniquely determined and the weight enumerator of C is unique as well. If $m = 1$, then we have a unique $(6, 2^6, 3)$ extremal code [6]. Hence, we prove that the weight enumerator is unique. See Example 1.

Let $n = 6m + 1$, and, considering $m \geq 1$, we have the following equations:

$$c_i = \sum_{j=0}^{i} \alpha_{ij} a_j = \alpha_{i0} \ \text{ for } \ i = 0, 1, 2, \ldots, 2m+1, \tag{18}$$

$$c_i = \sum_{j=0}^{3m-i} \beta_{ij} b_j = \beta_{i0} \ \text{ for } \ i = 2m+1, 2m+2, \ldots, 3m. \tag{19}$$

Hence, we prove that c_i is uniquely determined and the weight enumerator of C is unique as well. If $m = 0$, then we have no extremal code [6].

Let $n = 6m + 2$, and, considering $m \geq 2$, we have the following equations:

$$c_i = \sum_{j=0}^{i} \alpha_{ij} a_j = \alpha_{i0} \ \text{ for } \ i = 0, 1, 2, \ldots, 2m+1, \tag{20}$$

$$c_i = \sum_{j=0}^{3m+1-i} \beta_{ij} b_j = \beta_{i1} \ \text{ for } \ i = 2m+2, 2m+2, \ldots, 3m+1. \tag{21}$$

Hence, we prove that c_i is uniquely determined and the weight enumerator of C is unique as well. If $m = 0$, then we have no extremal code [6]. If $m = 1$, then we have two extremal codes [6], and they have the same weight enumerator. Hence, we prove that the weight enumerator is unique. See Example 1.

Let $n = 6m + 3$, and, considering $m \geq 1$, we have the following equations:

$$c_i = \sum_{j=0}^{i} \alpha_{ij} a_j = \alpha_{i0} \ \text{ for } \ i = 0, 1, 2, \ldots, 2m+1, \tag{22}$$

$$c_i = \sum_{j=0}^{3m+1-i} \beta_{ij} b_j = \beta_{i0} \ \text{ for } \ i = 2m+2, 2m+2, \ldots, 3m+1. \tag{23}$$

Hence, we prove that c_i is uniquely determined and the weight enumerator of C is unique as well. If $m = 0$, then we have a unique extremal code [6]. Hence, we prove that the weight enumerator is unique. See Example 1.

Let $n = 6m + 5$, then we have the following equations:

$$c_i = \sum_{j=0}^{i} \alpha_{ij} a_j = \alpha_{i0} \text{ for } i = 0, 1, 2, \ldots, 2m + 2, \tag{24}$$

$$c_i = \sum_{j=0}^{3m+2-i} \beta_{ij} b_j = \beta_{i0} \text{ for } i = 2m + 2, 2m + 3, \ldots, 3m + 2. \tag{25}$$

Hence, we prove that c_i is uniquely determined and the weight enumerator of C is unique as well. In conclusion, the weight enumerators are unique in all cases. □

Remark 1. *In Theorem 2, the missing case is $n = 6m + 4$. If $n = 6m + 4$, then we have the following equations:*

$$c_i = \sum_{j=0}^{i} \alpha_{ij} a_j = \alpha_{i0} \text{ for } i = 0, 1, 2, \ldots, 2m + 1, \tag{26}$$

$$c_i = \sum_{j=0}^{3m+2-i} \beta_{ij} b_j = \beta_{i1} \text{ for } i = 2m + 3, \ldots, 3m + 2. \tag{27}$$

Therefore, c_{2m+2} cannot be determined by the above equations, and we cannot prove that the weight enumerator is unique.

Using the above results, we prove the nonexistence of extremal Type I codes with minimal shadow for some parameters.

Theorem 3. *Extremal Type I additive self-dual codes over $GF(4)$ with minimal shadow of lengths $n = 6m + 1$ and $n = 6m + 5$ do not exist.*

Proof. Let $n = 6m + 1$, and, considering $m \geq 1$, from Equations (18) and (19), we have the following outcome:

$$c_{2m+1} = \alpha_{2m+1,0} = \beta_{2m+1,0}. \tag{28}$$

Using Equations (11) and (12), we have the following outcome:

$$\alpha_{2m+1,0} = -\frac{6m+1}{2m+1}, \beta_{2m+1,0} = -4\binom{3m}{2m+1}. \tag{29}$$

Thus,

$$-\frac{6m+1}{2m+1} = -4\binom{3m}{2m+1}. \tag{30}$$

Therefore, we have the conclusion as follows:

$$2m + 1 = 0. \tag{31}$$

This is a contradiction. If $m = 0$, then there is no extremal code [6].

Let $n = 6m + 5$. From Equations (24) and (25), we have the following outcome:

$$c_{2m+2} = \alpha_{2m+2,0} = \beta_{2m+2,0}. \tag{32}$$

Using Equations (11) and (12), we have the outcome:

$$\alpha_{2m+1,0} = 0, \beta_{2m+2,0} = 2\binom{3m+2}{2m+2}. \tag{33}$$

Thus,

$$0 = 2\binom{3m+2}{2m+2}. \tag{34}$$

This is a contradiction. □

Theorem 4. *There are no extremal Type I additive self-dual codes over $GF(4)$ with minimal shadow if*

1. $n = 6m$ *and* $m \geq 40$;
2. $n = 6m + 2$ *and* $m \geq 6$; *and*
3. $n = 6m + 3$ *and* $m \geq 22$.

Proof. Let $n = 6m$. From Equations (10) and (16), we have the following outcome:

$$c_{2m} = \alpha_{2m,0} = \beta_{2m,1} + \beta_{2m,m} b_m. \tag{35}$$

Hence,

$$b_m = \beta_{2m,m}^{-1}(\alpha_{2m,0} - \beta_{2m,1}). \tag{36}$$

Using Equations (11) and (12), we have the following outcome:

$$\beta_{2m,m} = 1, \alpha_{2m,0} = 3\binom{3m-1}{m-1}, \beta_{2m,1} = \binom{3m-1}{2m}. \tag{37}$$

Hence,

$$b_m = 3\binom{3m-1}{m-1} - \binom{3m-1}{2m} = 2\binom{3m-1}{m-1}. \tag{38}$$

From Equations (10) and (16), we have the following outcome:

$$c_{2m-1} = \alpha_{2m-1,0} = \beta_{2m-1,1} + \beta_{2m-1,m} b_m + \beta_{2m-1,m+1} b_{m+1}. \tag{39}$$

Hence,

$$b_{m+1} = \beta_{2m-1,m+1}^{-1}(\alpha_{2m-1,0} - \beta_{2m-1,1} - \beta_{2m-1,m} b_m). \tag{40}$$

Using Equations (11) and (12), we have the following outcomes:

$$\beta_{2m-1,m+1} = -\frac{1}{8}, \alpha_{2m-1,0} = -\frac{6m}{2m-1}\left[\binom{3m+1}{m-1} + 6\binom{3m}{m-2} + \binom{3m-1}{m-3}\right] \tag{41}$$

and

$$\beta_{2m-1,1} = -\frac{1}{8}\binom{3m-1}{2m-1}, \beta_{2m-1,m} = -\frac{m}{4}. \tag{42}$$

Hence,

$$b_{m+1} = 8 \cdot \frac{6m}{2m-1}\left[\binom{3m+1}{m-1} + 6\binom{3m}{m-2} + \binom{3m-1}{m-3}\right] - \binom{3m-1}{2m-1} - 4m\binom{3m-1}{m-1}. \tag{43}$$

Then,

$$b_{m+1} = \frac{4(3m-1)!}{(2m+2)!(m-1)!} h_0(m), \tag{44}$$

Here,

$$h_0(m) = -4m^3 + 160m^2 - 29m - 1. \tag{45}$$

Thus, $h_0(m) < 0$ if $m \geq 40$. Therefore, if $m \geq 40$, then $b_{m+1} < 0$. This is a contradiction. Let $n = 6m + 2$. From Equations (10) and (20), we have the following equation:

$$c_{2m+1} = \alpha_{2m+1,0} = \beta_{2m+1,1} + \beta_{2m+1,m} b_m. \tag{46}$$

Therefore,

$$b_m = \beta_{2m+1,m}^{-1}(\alpha_{2m+1,0} - \beta_{2m+1,1}). \tag{47}$$

Using Equations (11) and (12), we have the following equations:

$$\beta_{2m+1,m} = -2, \alpha_{2m+1,0} = -\frac{6m+2}{2m+1}\binom{3m}{m}, \beta_{2m+1,1} = -2\binom{3m}{2m+1}. \tag{48}$$

Therefore,

$$b_m = \frac{3m+1}{2m+1}\binom{3m}{m} - \binom{3m}{m-1}. \tag{49}$$

From Equations (10) and (20), we have the following equations:

$$c_{2m} = \alpha_{2m,0} = \beta_{2m,1} + \beta_{2m,m}b_m + \beta_{2m,m+1}b_{m+1}. \tag{50}$$

Therefore,

$$b_{m+1} = \beta_{2m,m+1}^{-1}(\alpha_{2m,0} - \beta_{2m,1} - \beta_{2m,m}b_m). \tag{51}$$

Using Equations (11) and (12), we have the following:

$$\beta_{2m,m+1} = \frac{1}{4}, \alpha_{2m,0} = \frac{3m+1}{m}\left[\binom{3m}{m-2} + 3\binom{3m+1}{m-1}\right] \tag{52}$$

and

$$\beta_{2m,1} = \frac{1}{4}\binom{3m}{m}, \beta_{2m,m} = \frac{2m+1}{4}. \tag{53}$$

Therefore,

$$b_{m+1} = 4 \cdot \frac{3m+1}{m}\left[\binom{3m}{m-2} + 3\binom{3m+1}{m-1}\right] - \binom{3m}{m} - (2m+1) \cdot \left[\frac{3m+1}{2m+1}\binom{3m}{m} - \binom{3m}{m-1}\right]. \tag{54}$$

Then,

$$b_{m+1} = \frac{(3m)!}{(2m+1)!(m+1)!}h_2(m). \tag{55}$$

Here,

$$h_2(m) = -8m^3 + 44m^2 + 22m + 2. \tag{56}$$

Thus, $h_2(m) < 0$ if $m \geq 6$. Therefore, if $m \geq 6$, then $b_{m+1} < 0$. This is a contradiction.
Let $n = 6m + 3$. From Equations (10) and (22), we have the following equation:

$$c_{2m+1} = \alpha_{2m+1,0} = \beta_{2m+1,0} + \beta_{2m+1,m}b_m. \tag{57}$$

Therefore,

$$b_m = \beta_{2m+1,m}^{-1}(\alpha_{2m+1,0} - \beta_{2m+1,0}). \tag{58}$$

Using Equations (11) and (12), we have the following outcome:

$$\beta_{2m+1,m} = -1, \alpha_{2m+1,0} = -3\binom{3m+1}{m}, \beta_{2m+1,0} = -\binom{3m+1}{m}. \tag{59}$$

Therefore,

$$b_m = 2\binom{3m+1}{m}. \tag{60}$$

From Equations (10) and (22), we have the following equation:

$$c_{2m} = \alpha_{2m,0} = \beta_{2m,0} + \beta_{2m,m}b_m + \beta_{2m,m+1}b_{m+1}. \tag{61}$$

Therefore,

$$b_{m+1} = \beta_{2m,m+1}^{-1}(\alpha_{2m,0} - \beta_{2m,0} - \beta_{2m,m}b_m). \tag{62}$$

Using Equations (11) and (12), we have the following equations:

$$\beta_{2m,m+1} = \frac{1}{8}, \alpha_{2m,0} = \frac{12m+6}{m}\left[\binom{3m+1}{m-2} + \binom{3m+2}{m-1}\right] \tag{63}$$

and

$$\beta_{2m,0} = \frac{1}{8}\binom{3m+1}{m+1}, \beta_{2m,m} = \frac{2m+1}{8}. \tag{64}$$

Therefore,

$$b_{m+1} = 8 \cdot \frac{12m+6}{m}\left[\binom{3m+1}{m-2} + \binom{3m+2}{m-1}\right] - \binom{3m+1}{m+1} - 2(2m+1) \cdot \binom{3m+1}{m}. \tag{65}$$

Then,

$$b_{m+1} = \frac{(3m+1)!(2m+1)}{(2m+3)!(m)!}h_3(m). \tag{66}$$

Here,

$$h_3(m) = -8m^2 + 168m + 30. \tag{67}$$

Thus, $h_3(m) < 0$ if $m \geq 22$. Therefore, if $m \geq 22$, then $b_{m+1} < 0$. This is a contradiction. □

In the following example, we give some extremal Type I additive self-dual codes over $GF(4)$ with minimal shadow.

Example 1. *Consider that there is a unique* $(3, 2^3, 2)$ *extremal Type I additive self-dual code over* $GF(4)$*, say* C_3*, with the following generator matrix:*

$$G_3 = \begin{pmatrix} w & 1 & 1 \\ 1 & w & 1 \\ 1 & 1 & w \end{pmatrix}. \tag{68}$$

The weight enumerator of the code C_3 *and the shadow code* S_3 *are given as follows:*

$$W_{C_3}(1,y) = 1 + 3y^2 + 4y^3, \tag{69}$$

$$W_{S_3}(1,y) = 3y + 5y^3. \tag{70}$$

Therefore, the code C_3 *is an extremal Type I additive self-dual code over* $GF(4)$ *with minimal shadow.*

Consider that there is a unique $(6, 2^6, 3)$ *extremal Type I additive self-dual code over* $GF(4)$*, say* C_6*, with the following generator matrix:*

$$G_6 = \begin{pmatrix} w & 0 & 0 & 0 & 1 & 1 \\ 0 & w & 0 & 1 & 0 & 1 \\ 0 & 0 & w & 1 & 1 & 0 \\ 0 & 1 & 1 & w & 0 & 0 \\ 1 & 0 & 1 & 0 & w & 0 \\ 1 & 1 & 0 & 0 & 0 & w \end{pmatrix}. \tag{71}$$

The weight enumerator of the code C_6 *and the shadow code* S_6 *are given as follows:*

$$W_{C_6}(1,y) = 1 + 8y^3 + 21y^4 + 24y^5 + 10y^6, \tag{72}$$

$$W_{S_6}(1,y) = 3y^2 + 42y^4 + 19y^6. \tag{73}$$

Therefore, the code C_6 is an extremal Type I additive self-dual code over $GF(4)$ with minimal shadow.

Consider that there are exactly two $(8, 2^8, 4)$ extremal Type I additive self-dual codes over $GF(4)$, say C_{8a} and C_{8b}, with the following generator matrices [7]:

$$G_{8a} = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & w & w & w & w \\ 0 & 1 & 0 & 0 & 1 & w & w^2 & 0 \\ 0 & 0 & 1 & 0 & w & w^2 & w^2 & w \\ w & w & 0 & 0 & 1 & 0 & w & w \\ w & 0 & w & 0 & 1 & w & w^2 & 1 \\ w & 0 & 0 & w & w^2 & w^2 & 0 & 1 \end{pmatrix}, G_{8b} = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & w & w & w & w \\ 0 & 1 & 0 & 0 & w & w & w^2 & w^2 \\ 0 & 0 & 1 & 0 & w & w^2 & w^2 & w \\ w & w & 0 & 0 & w^2 & w^2 & 0 & 1 \\ w & 0 & w & 0 & 1 & w & w^2 & 1 \\ w & 0 & 0 & w & w & 1 & w^2 & 1 \end{pmatrix}. \quad (74)$$

The weight enumerators of both codes are the same. The following are the weight enumerators of the codes and the corresponding shadow codes:

$$W_{C_{8a}}(1, y) = W_{C_{8b}}(1, y) = 1 + 26y^4 + 64y^5 + 72y^6 + 64y^7 + 29y^8 \quad (75)$$

and

$$W_{S_{8a}}(1, y) = W_{S_{8b}}(1, y) = 4y^2 + 36y^4 + 172y^6 + 44y^8. \quad (76)$$

Therefore, the codes C_{8a} and C_{8b} are extremal Type I additive self-dual codes over $GF(4)$ with minimal shadow.

4. Summary

In this study, we investigate Type I additive self-dual codes over $GF(4)$. We especially define a code C with minimal shadow. We prove that extremal Type I additive self-dual codes over $GF(4)$ with minimal shadow of lengths $n = 6m, 6m + 1, 6m + 2, 6m + 3$, and $6m + 5$ have uniquely determined weight enumerators. Using this fact, we prove that extremal Type I additive self-dual codes over $GF(4)$, with minimal shadow of lengths $n = 6m + 1$ and $6m + 5$, do not exist. For $n = 6m, 6m + 2, 6m + 3$, we prove that extremal Type I additive self-dual codes over $GF(4)$, with minimal shadow, do not exist if $m \geq 40, m \geq 6, m \geq 22$, respectively.

For future work, it is worth studying the problem of existence of such codes for the missing case $n = 6m + 4$, as well as for the incomplete cases $n = 6m, 6m + 2, 6m + 3$.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Rains, E.M.; Sloane, N.J.A. Self-dual codes. In *Handbook of Coding Theory*; Pless, V.S., Huffman, W.C., Eds.; Elsevier: Amsterdam, The Netherlands, 1998.
2. Conway, J.H.; Sloane, N.J.A. A new upper bound on the minimal distance of self-dual codes. *IEEE Trans. Inf. Theory* **1990**, *36*, 1319–1333.
3. Rains, E.M. Shadow bounds for self-dual codes. *IEEE Trans. Inf. Theory* **1998**, *44*, 134–139.
4. Bouyuklieva, S.; Willems, W. Singly even self-dual codes with minimal shadow. *IEEE Trans. Inf. Theory* **2012**, *58*, 3856–3860.
5. Calderbank, A.R.; Rains, E.M.; Shor, P.M.; Sloane, N.J.A. Quantum error correction via codes over GF(4). *IEEE Trans. Inf. Theory* **1998**, *44*, 1369–1387.

6. Huffman, W.C. On the classification and enumeration of self-dual codes. *Finite Fields Appl.* **2005**, *11*, 451–490.
7. Gaborit, P.; Huffman, W.C.; Kim, J.-L.; Pless, V. On the Classification of Extremal Additive Codes over *GF*(4). In Proceedings of the 37th Allerton Conference on Communication, Control and Computing, Urbana-Champaign, IL, USA, 22–24 September 1999; pp. 535–544.