information

Article

Near-Extremal Type I Self-Dual Codes with Minimal Shadow over $GF(2)$ and $GF(4)$

Sunghyu Han

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

Received: 23 June 2018; Accepted: 11 July 2018; Published: 13 July 2018

Abstract: Binary self-dual codes and additive self-dual codes over $GF(4)$ contain common points. Both have Type I codes and Type II codes, as well as shadow codes. In this paper, we provide a comprehensive description of extremal and near-extremal Type I codes over $GF(2)$ and $GF(4)$ with minimal shadow. In particular, we prove that there is no near-extremal Type I $[24m, 12m, 2m+2]$ binary self-dual code with minimal shadow if $m \geq 323$, and we prove that there is no near-extremal Type I $(6m+1, 2^{6m+1}, 2m+1)$ additive self-dual code over $GF(4)$ with minimal shadow if $m \geq 22$.

Keywords: additive codes over $GF(4)$; binary codes; extremal codes; minimal shadow; near-extremal codes; 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 paper focuses on self-dual codes, which, while of interest themselves, are closely related to other mathematical structures such as block designs, lattices, modular forms and sphere packings (for example, see [1]).

There are several types of self-dual codes. Among them, binary self-dual codes and additive self-dual codes over $GF(4)$ have common points. Firstly, there are Type I and Type II codes in both classes. Secondly, there are shadow codes in both classes. Using shadow theory, E. M.Rains provided an upper bound to the minimum distances of Type I codes in both classes [2]. If a code meets this bound, then it is called an extremal code.

For extremal Type II codes, there is a systematic nonexistence proof [3]. However, for extremal Type I codes, no such nonexistence proof exists. Research has also been conducted on extremal Type I codes with minimal shadow. S. Bouyuklieva and W. Willems studied the nonexistence of extremal Type I binary codes with minimal shadow [4]. Impressed by the results, S. Han studied the nonexistence of extremal Type I additive codes over $GF(4)$ with minimal shadow [5]. Recently, S. Bouyuklieva, M. Harada and A. Munemasa studied the nonexistence of near-extremal Type I binary self-dual codes with minimal shadow [6].

In this paper, we cover the missing case of the nonexistence of near-extremal Type I binary self-dual codes with minimal shadow, which was not covered in [6], and we apply the technique to near-extremal Type I additive codes over $GF(4)$ with minimal shadow. The main contribution of this paper is three-fold. Firstly, it provides a comprehensive presentation of the nonexistence of extremal and near-extremal Type I codes over $GF(2)$ and $GF(4)$. Secondly, we prove that there is no near-extremal Type I $[24m, 12m, 2m+2]$ binary self-dual code with minimal shadow if $m \geq 323$. Thirdly, we prove that there is no near-extremal Type I $(6m+1, 2^{6m+1}, 2m+1)$ additive self-dual code over $GF(4)$ with minimal shadow if $m \geq 22$.

The rest of the paper is organized as follows. In Section 2, we deal with binary self-dual codes with minimal shadow. We consider the nonexistence of extremal Type I binary self-dual codes with minimal shadow. In Section 3, we consider the nonexistence of near-extremal Type I binary self-dual codes with minimal shadow. In Section 4, we deal with additive self-dual codes over $GF(4)$ with minimal shadow. We consider the nonexistence of extremal Type I additive self-dual codes over $GF(4)$ with minimal shadow. In Section 5, we consider the nonexistence of near-extremal Type I additive self-dual codes over $GF(4)$ with minimal shadow. All computer calculations in this study were performed using the mathematical software Maple.

2. Extremal Type I Binary Self-Dual Codes with Minimal Shadow

In this section, we deal with binary self-dual codes with minimal shadow. First, we discuss basic facts about binary self-dual codes. Secondly, we consider the nonexistence of extremal Type I binary self-dual codes with minimal shadow.

A binary linear code C is a subspace of a vector space $GF(2)^n$, and the vectors in C are called codewords. The weight of a codeword $u = (u_1, u_2, \cdots, u_n)$ in $GF(2)^n$ is the number of nonzero u_j. The minimum distance of C is the smallest nonzero weight of any codeword in C. If the dimension of C is k and the minimum distance in C is d, we say C is an $[n, k, d]$ code.

The scalar product in $GF(2)^n$ is defined by:

$$(u, v) = \sum_{j=1}^{n} u_j v_j \,, \tag{1}$$

where the sum is evaluated in $GF(2)$. The dual code of a binary linear code C is defined by:

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

If $C \subseteq C^{\perp}$, we say C is self-orthogonal, and if $C = C^{\perp}$, we say C is self-dual.

A binary code is even if all its codewords have even weights. Clearly, self-dual binary codes are even. In addition, some of these codes have all codewords of weights divisible by four. A self-dual code with all codewords of weights divisible by four is called doubly-even or Type II; a self-dual code where some codewords have weights not divisible by four is called singly-even or Type I. Bounds on the minimum distance of binary self-dual codes were provided in [2].

Theorem 1. *([2]) Let C be an $[n, n/2, d]$ binary self-dual code. Then, $d \leq 4[n/24] + 4$ if $n \not\equiv 22 \pmod{24}$. If $n \equiv 22 \pmod{24}$, then $d \leq 4[n/24] + 6$, and if the equality holds, C can be obtained by shortening a Type II code of length $n + 2$. If $24|n$ and $d = 4[n/24] + 4$, then C is Type II.*

A code meeting the bounds of Theorem 1, i.e., for which equality holds within the bounds, is called extremal. From Theorem 1, note that there is no extremal Type I code of length $n = 24m$ ($m \geq 1$). There is a systematic proof for the nonexistence of extremal Type II codes if the code length is sufficiently large [3].

Theorem 2. *([3]) Let C be an extremal binary Type II code of length $n = 24m + 8\ell$. Then, the code C does not exist if $m \geq 154$ (for $\ell = 0$), $m \geq 159$ (for $\ell = 1$) and $m \geq 164$ (for $\ell = 2$).*

The proof of Theorem 1 for Type I codes is formulated using a shadow code. In [7], the concept of a shadow code was introduced. The shadow code of a self-dual code C is defined as follows: let $C^{(0)}$ be the subset of C consisting of all codewords whose weights are multiples of four, and let $C^{(2)} = C \backslash C^{(0)}$. The shadow code of C is defined by:

$$S = S(C) = \{u \in GF(2)^n : (u, v) = 0 \text{ for all } v \in C^{(0)}, (u, v) = 1 \text{ for all } v \in C^{(2)}\}. \tag{3}$$

The weight enumerator of a code is given by:

$$W_C(x,y) = \sum_{i=0}^{n} A_i x^{n-i} y^i, \tag{4}$$

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

Lemma 1. *[7] Let C be a Type I binary self-dual code of length n and minimum weight d. Let $S(y) = \sum_{i=0}^{n} b_i y^i$ be the weight enumerator of $S(C)$. Then:*

1. $b_0 = 0$
2. $b_i \le 1$ *for* $i < d/2$

Let C be a Type I binary self-dual code of length $n = 24m + 8\ell + 2r$ where $\ell = 0,1,2$ and $r = 0,1,2,3$. By Gleason's theorem [8–10], we can calculate the weight enumerator of C as follows for suitable constants c_i:

$$W_C(x,y) = \sum_{i=0}^{[n/8]} c_i (x^2+y^2)^{n/2-4i} \{x^2y^2(x^2-y^2)^2\}^i. \tag{5}$$

Using the shadow code theory [7], we can calculate the weight enumerator of shadow code $S(C)$:

$$W_S(x,y) = \sum_{i=0}^{[n/8]} (-1)^i 2^{n/2-6i} c_i (xy)^{n/2-4i} (x^4-y^4)^{2i}. \tag{6}$$

We rewrite Equations (5) and (6) to the following:

$$W_C(1,y) = \sum_{j=0}^{12m+4\ell+r} a_j y^{2j} = \sum_{i=0}^{3m+\ell} c_i (1+y^2)^{12m+4\ell+r-4i} \{y^2(1-y^2)^2\}^i, \tag{7}$$

$$W_S(1,y) = \sum_{j=0}^{6m+2\ell} b_j y^{4j+r} = \sum_{i=0}^{3m+\ell} (-1)^i c_i\, 2^{12m+4\ell+r-6i} y^{12m+4\ell+r-4i} (1-y^4)^{2i}. \tag{8}$$

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 $0 \le j \le 3m + \ell - i$, as follows for suitable constants α_{ij} and β_{ij}:

$$c_i = \sum_{j=0}^{i} \alpha_{ij} a_j = \sum_{j=0}^{3m+\ell-i} \beta_{ij} b_j. \tag{9}$$

In our computation, we need to calculate α_{i0} and β_{ij}. The following formula can be found in [2] for $i > 0$:

$$\alpha_{i0} = -\frac{n}{2i}\left[\text{coeff. of } y^{i-1} \text{ in } (1+y)^{-(n/2)-1+4i}(1-y)^{-2i}\right] \tag{10}$$

and:

$$\beta_{ij} = (-1)^i 2^{-\frac{n}{2}+6i} \frac{k-j}{i} \binom{k+i-j-1}{k-i-j}, \tag{11}$$

where $k = 3m + \ell$. Note that $a_0 = c_0 = \alpha_{00} = 1$. Now, we introduce the definition of a code with minimal shadow:

Definition 1. *Let C be a Type I binary self-dual code of length $n = 24m + 8\ell + 2r$ with $\ell = 0,1,2$ and $r = 0,1,2,3$. Then, C is a code with minimal shadow if:*

1. $d(S) = r$ *for* $r > 0$ *and*

2. *$d(S) = 4$ for $r = 0$*

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

Let C be an extremal Type I binary self-dual code with a minimal shadow of length n. Then, the following facts can be found in [4]: For a_i, we have $a_0 = 1, a_1 = a_2 = \cdots = a_{2m+1} = 0$. Moreover, if $n \equiv 22 \pmod{24}$, then $a_{2m+2} = 0$. For b_j, we have $b_0 = 1$ if (i) $r = 1$ and $m \geq 0$ and (ii) $r = 2,3$ and $m \geq 1$. Furthermore, we have $b_0 = 0, b_1 = 1$ if $r = 0$ and $m \geq 2$. If $r > 0$, then $b_1 = b_2 = \cdots = b_{m-1} = 0$. If $r = 0$, then $b_2 = b_3 = \cdots = b_{m-1} = 0$. Moreover, if $n = 24m + 8l + 2$, then $b_m = 0$. Using these facts, we have the following lemma:

Lemma 2. *Using the above notations, we have the following results:*

1. *If $n = 24m + 2$ $(m \geq 0)$, then $c_i = \alpha_{i0}$ for $0 \leq i \leq 2m + 1$, $c_i = \beta_{i0}$ for $2m \leq i \leq 3m$.*
2. *If $n = 24m + 4$ $(m \geq 1)$, then $c_i = \alpha_{i0}$ for $0 \leq i \leq 2m + 1$, $c_i = \beta_{i0}$ for $2m + 1 \leq i \leq 3m$.*
3. *If $n = 24m + 6$ $(m \geq 1)$, then $c_i = \alpha_{i0}$ for $0 \leq i \leq 2m + 1$, $c_i = \beta_{i0}$ for $2m + 1 \leq i \leq 3m$.*
4. *If $n = 24m + 8$ $(m \geq 2)$, then $c_i = \alpha_{i0}$ for $0 \leq i \leq 2m + 1$, $c_i = \beta_{i1}$ for $2m + 2 \leq i \leq 3m + 1$.*
5. *If $n = 24m + 10$ $(m \geq 0)$, then $c_i = \alpha_{i0}$ for $0 \leq i \leq 2m + 1$, $c_i = \beta_{i0}$ for $2m + 1 \leq i \leq 3m + 1$.*
6. *If $n = 24m + 12$ $(m \geq 1)$, then $c_i = \alpha_{i0}$ for $0 \leq i \leq 2m + 1$, $c_i = \beta_{i0}$ for $2m + 2 \leq i \leq 3m + 1$.*
7. *If $n = 24m + 14$ $(m \geq 1)$, then $c_i = \alpha_{i0}$ for $0 \leq i \leq 2m + 1$, $c_i = \beta_{i0}$ for $2m + 2 \leq i \leq 3m + 1$.*
8. *If $n = 24m + 16$ $(m \geq 2)$, then $c_i = \alpha_{i0}$ for $0 \leq i \leq 2m + 1$, $c_i = \beta_{i1}$ for $2m + 3 \leq i \leq 3m + 2$.*
9. *If $n = 24m + 18$ $(m \geq 0)$, then $c_i = \alpha_{i0}$ for $0 \leq i \leq 2m + 1$, $c_i = \beta_{i0}$ for $2m + 2 \leq i \leq 3m + 2$.*
10. *If $n = 24m + 20$ $(m \geq 1)$, then $c_i = \alpha_{i0}$ for $0 \leq i \leq 2m + 1$, $c_i = \beta_{i0}$ for $2m + 3 \leq i \leq 3m + 2$.*
11. *If $n = 24m + 22$ $(m \geq 1)$, then $c_i = \alpha_{i0}$ for $0 \leq i \leq 2m + 2$, $c_i = \beta_{i0}$ for $2m + 3 \leq i \leq 3m + 2$.*

Proof. Let C be an extremal Type I binary self-dual code with minimal shadow of length $n = 24m + 2$. We can rewrite Equation (9) as follows:

$$c_i = \sum_{j=0}^{i} \alpha_{ij} a_j = \sum_{j=0}^{3m-i} \beta_{ij} b_j. \tag{12}$$

Then, we have:

$$c_i = \sum_{j=0}^{i} \alpha_{ij} a_j = \alpha_{i0} \text{ for } i = 0, 1, 2, \ldots, 2m + 1 \tag{13}$$

and:

$$c_i = \sum_{j=0}^{3m-i} \beta_{ij} b_j = \beta_{i0} \text{ for } i = 2m, 2m + 1, \ldots, 3m. \tag{14}$$

Therefore, the first statement is proven. The other cases can be proven similarly. □

Using Lemma 2, we have the following theorem:

Theorem 3. *Let C be an extremal Type I binary self-dual code of length n with minimal shadow. Then, the weight enumerator of C is unique if $n \not\equiv 24m + 16, 24m + 20$.*

Proof. Suppose that $n \not\equiv 24m + 16, 24m + 20$. From Lemma 2, we can see that c_i can be calculated by Equations (10) and (11), and they depend only on the length n for all i, $(0 \leq i \leq [n/8])$, except the following cases. By [7], we know that:

1. $n = 24m + 4$: If $m = 0$, then $n = 4$. For this case, there is no extremal code.
2. $n = 24m + 6$: If $m = 0$, then $n = 6$. For this case, there is no extremal code.
3. $n = 24m + 8$: If $m = 0$, then $n = 8$. For this case, there is no extremal Type I code. If $m = 1$, then $n = 32$. For this case, there are three extremal Type I codes. They have the same weight enumerator: $W_C(1, y) = 1 + 364y^8 + 2048y^{10} + 6720y^{12} + 14336y^{14} + 18598y^{16} + \cdots$,

$W_S(1,y) = 8y^4 + 592y^8 + 13944y^{12} + 36448y^{16} + \cdots$. We can see that the codes have minimal shadow.
4. $n = 24m+12$: If $m = 0$, then $n = 12$. For this case, there is a unique extremal Type I code. The weight enumerator is the following: $W_C(1,y) = 1 + 15y^4 + 32y^6 + \cdots$, $W_S(1,y) = 6y^2 + 5y^6 + \cdots$. We can see that the code has minimal shadow.
5. $n = 24m+22$: If $m = 0$, then $n = 22$. For this case, there is a unique extremal Type I code. The weight enumerator is the following: $W_C(1,y) = 1 + 77y^6 + 330y^8 + 616y^{10} + \cdots$, $W_S(1,y) = 352y^7 + 1344y^{11} + \cdots$.

This completes the proof. □

The following nonexistence theorems are proven in [4].

Theorem 4. *[4] Extremal self-dual codes of lengths $n = 24m+2, 24m+4, 24m+6, 24m+10$ and $24m+22$ with minimal shadow do not exist.*

Theorem 5. *[4] There are no extremal Type I binary self-dual codes of length n with minimal shadow if:*

1. *$n = 24m+8$ and $m \geq 53$;*
2. *$n = 24m+12$ and $m \geq 142$;*
3. *$n = 24m+14$ and $m \geq 146$;*
4. *$n = 24m+16$ and $m \geq 164$;*
5. *$n = 24m+18$ and $m \geq 157$.*

Remark 1. *Currently, $n = 24m+20$ is the unique untouched code length for the nonexistence or an explicit bound for the length n of an extremal Type I binary self-dual code with minimal shadow.*

3. Near-Extremal Type I Binary Self-Dual Codes with Minimal Shadow

In this section, we consider the nonexistence of near-extremal Type I binary self-dual codes with minimal shadow. We start with the following definition:

Definition 2. *Let C be an $[n, n/2, d]$ Type I binary self-dual code. Then, C is a near-extremal code if:*

1. *$d = 4[n/24] + 2$ for $n \not\equiv 22 \pmod{24}$; and*
2. *$d = 4[n/24] + 4$ for $n \equiv 22 \pmod{24}$.*

Let C be a near-extremal Type I binary self-dual code with minimal shadow. Then, we have the following: $a_0 = 1, a_1 = a_2 = \cdots = a_{2m} = 0$. Moreover, if $n \equiv 22 \pmod{24}$, then $a_{2m+1} = 0$.

By Lemma 1, $b_0 = 1$ if (i) $r = 1,2$ and $m \geq 1$, (ii) $r = 3$, $n \not\equiv 22 \pmod{24}$ and $m \geq 2$ and (iii) $r = 3$, $n \equiv 22 \pmod{24}$ and $m \geq 1$. In addition, $b_0 = 0, b_1 = 1$ if $r = 0$ and $m \geq 2$.

If $r = 1,2$ or $r = 3$ and $n \equiv 22 \pmod{24}$, then $b_1 = b_2 = \cdots = b_{m-1} = 0$. Otherwise, S would contain a vector v of weight less than or equal to $4m - 4 + r$, and if $u \in S$ is a vector of weight r, then $u + v \in C$ with $\mathrm{wt}(u+v) \leq 4m - 4 + 2r$, a contradiction with a minimum distance of C. If $r = 3$ and $n \not\equiv 22 \pmod{24}$, then $b_1 = b_2 = \cdots = b_{m-2} = 0$. Furthermore, if $r = 0$, then $b_2 = b_3 = \cdots = b_{m-1} = 0$. The proofs are similar to the above case. Using this fact, we have the following lemma:

Lemma 3. *Using the above notations, we have the following results:*

1. *If $n = 24m$ $(m \geq 2)$, then $c_i = \alpha_{i0}$ for $0 \leq i \leq 2m$, $c_i = \beta_{i1}$ for $2m+1 \leq i \leq 3m$.*
2. *If $n = 24m+2$ $(m \geq 1)$, then $c_i = \alpha_{i0}$ for $0 \leq i \leq 2m$, $c_i = \beta_{i0}$ for $2m+1 \leq i \leq 3m$.*
3. *If $n = 24m+4$ $(m \geq 1)$, then $c_i = \alpha_{i0}$ for $0 \leq i \leq 2m$, $c_i = \beta_{i0}$ for $2m+1 \leq i \leq 3m$.*
4. *If $n = 24m+6$ $(m \geq 2)$, then $c_i = \alpha_{i0}$ for $0 \leq i \leq 2m$, $c_i = \beta_{i0}$ for $2m+2 \leq i \leq 3m$.*
5. *If $n = 24m+8$ $(m \geq 2)$, then $c_i = \alpha_{i0}$ for $0 \leq i \leq 2m$, $c_i = \beta_{i1}$ for $2m+2 \leq i \leq 3m+1$.*
6. *If $n = 24m+10$ $(m \geq 1)$, then $c_i = \alpha_{i0}$ for $0 \leq i \leq 2m$, $c_i = \beta_{i0}$ for $2m+2 \leq i \leq 3m+1$.*

7. *If* $n = 24m + 12$ *(*$m \geq 1$*), then* $c_i = \alpha_{i0}$ *for* $0 \leq i \leq 2m$*,* $c_i = \beta_{i0}$ *for* $2m + 2 \leq i \leq 3m + 1$*.*
8. *If* $n = 24m + 14$ *(*$m \geq 2$*), then* $c_i = \alpha_{i0}$ *for* $0 \leq i \leq 2m$*,* $c_i = \beta_{i0}$ *for* $2m + 3 \leq i \leq 3m + 1$*.*
9. *If* $n = 24m + 16$ *(*$m \geq 2$*), then* $c_i = \alpha_{i0}$ *for* $0 \leq i \leq 2m$*,* $c_i = \beta_{i1}$ *for* $2m + 3 \leq i \leq 3m + 2$*.*
10. *If* $n = 24m + 18$ *(*$m \geq 1$*), then* $c_i = \alpha_{i0}$ *for* $0 \leq i \leq 2m$*,* $c_i = \beta_{i0}$ *for* $2m + 3 \leq i \leq 3m + 2$*.*
11. *If* $n = 24m + 20$ *(*$m \geq 1$*), then* $c_i = \alpha_{i0}$ *for* $0 \leq i \leq 2m$*,* $c_i = \beta_{i0}$ *for* $2m + 3 \leq i \leq 3m + 2$*.*
12. *If* $n = 24m + 22$ *(*$m \geq 1$*), then* $c_i = \alpha_{i0}$ *for* $0 \leq i \leq 2m + 1$*,* $c_i = \beta_{i0}$ *for* $2m + 3 \leq i \leq 3m + 2$*.*

Proof. The proof is similar to the one for Lemma 2. □

Using Lemma 3, we have the following theorem [6]:

Theorem 6. *[6] Let C be a near-extremal Type I binary self-dual code with minimal shadow of length n. Then, we have the following:*

1. *The weight enumerator of C is uniquely determined if* $n = 24m + 2, 24m + 4, 24m + 10$*.*
2. *The code C does not exist if:*
   (a) $n = 24m + 2$ *and* $m \geq 155$
   (b) $n = 24m + 4$ *and* $m \geq 156$
   (c) $n = 24m + 10$ *and* $m \geq 160$

The missing case in Theorem 6 is the code length $n = 24m$. We can prove similar results for the missing case using the following theorem:

Theorem 7. *Let C be a* $[24m, 12m, 4m + 2]$ *near-extremal Type I binary self-dual code with minimal shadow. Then, we have the following:*

1. *The weight enumerator of C is uniquely determined.*
2. *The code C does not exist if* $m \geq 323$*.*

Proof. From Lemma 3, we can see that c_i can be calculated by Equations (10) and (11), and they depend only on the length n for all $i, (0 \leq i \leq [n/8])$ unless $m = 1$. If $m = 1$, then $n = 24$. For this case, there is a unique near-extremal Type I code [7]. The weight enumerator is the following: $W_C(1, y) = 1 + 64y^6 + 375y^8 + 960y^{10} + 1296y^{12} + \cdots$. $W_S(1, y) = 6y^4 + 744y^8 + 2596y^{12} + \cdots$. We can see that the code has minimal shadow. This proves the first statement.

For the second statement, from Equation (9) and the fact that $c_i = \alpha_{i,0}$ for $0 \leq i \leq 2m$, we have:

$$c_{2m} = \alpha_{2m,0} = \beta_{2m,1} + \beta_{2m,m} b_m. \tag{15}$$

Therefore, we get:

$$b_m = \beta_{2m,m}^{-1}(\alpha_{2m,0} - \beta_{2m,1}). \tag{16}$$

Using Equations (10) and (11), we have:

$$\beta_{2m,m} = 1, \alpha_{2m,0} = 6\binom{5m-1}{m-1}, \beta_{2m,1} = \frac{3m-1}{2m}\binom{5m-2}{m-1}. \tag{17}$$

From this, we get:

$$b_m = 6\binom{5m-1}{m-1} - \frac{3m-1}{2m}\binom{5m-2}{m-1}. \tag{18}$$

From Equation (9) and the fact that $c_i = \alpha_{i,0}$ for $0 \leq i \leq 2m$, we have:

$$c_{2m-1} = \alpha_{2m-1,0} = \beta_{2m-1,1} + \beta_{2m-1,m} b_m + \beta_{2m-1,m+1} b_{m+1}. \tag{19}$$

From this, we get:

$$b_{m+1} = \beta_{2m-1,m+1}^{-1}(\alpha_{2m-1,0} - \beta_{2m-1,1} - \beta_{2m-1,m} b_m). \tag{20}$$

Using Equations (10) and (11), we have:

$$\beta_{2m-1,m+1} = -2^{-6}, \tag{21}$$

$$\alpha_{2m-1,0} = -\frac{24m}{2(2m-1)}\left[\binom{5m+3}{m-1} + \binom{5m+2}{m-2}\binom{7}{2} + \binom{5m+1}{m-3}\binom{7}{4} + \binom{5m}{m-4}\binom{7}{6}\right] \tag{22}$$

and:

$$\beta_{2m-1,1} = -2^{-6} \times \frac{3m-1}{2m-1}\binom{5m-3}{m}, \quad \beta_{2m-1,m} = -\frac{m}{16}. \tag{23}$$

Therefore, we get:

$$b_{m+1} = \frac{64(6m-1)(5m-1)(5m-3)!}{(4m+4)!(m-1)!}h_0(m), \tag{24}$$

where:

$$h_0(m) = -64m^5 + 20640m^4 - 9388m^3 + 582m^2 - 49m - 3. \tag{25}$$

We can see that $h_0(m) < 0$ if $m \geq 323$. Therefore, if $m \geq 323$, then $b_{m+1} < 0$. This is a contradiction. □

Remark 2. *The definition of near-extremal Type II binary self-dual codes and the corresponding nonexistence proof can be found in [11].*

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

In this section, we deal with additive self-dual codes over $GF(4)$ with minimal shadow. First, we discuss basic facts about additive self-dual codes over $GF(4)$. Then, we consider the nonexistence of extremal Type I additive self-dual codes over $GF(4)$ with minimal shadow.

An additive code C over $GF(4)$ of length n is an additive subgroup of $GF(4)^n$. The weight of a vector $u = (u_1, u_2, \cdots, u_n)$ in $GF(4)^n$ and the minimum distance of C are defined the same way as for binary linear codes. C is a k-dimensional $GF(2)$-subspace of $GF(4)^n$ and thus 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, $u = (u_1, u_2, ..., u_n)$ and $v = (v_1, v_2, ..., v_n)$ is given by:

$$u * v = \sum_{i=1}^{n} \mathrm{Tr}(u_i {v_i}^2) = \sum_{i=1}^{n} (u_i {v_i}^2 + {u_i}^2 v_i) \pmod 2. \tag{26}$$

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

$$C^{\perp} = \{u \in GF(4)^n : u * c = 0 \text{ for all } c \in C\}. \tag{27}$$

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 [1,2].

Theorem 8. *[1,2] Let C be an $(n, 2^n, d)$ additive self-dual code over $GF(4)$. If C is Type I, then:*

$$d \leq \begin{cases} 2[n/6] + 1, & \text{if } n \equiv 0 \pmod 6; \\ 2[n/6] + 3, & \text{if } n \equiv 5 \pmod 6; \\ 2[n/6] + 2, & \text{otherwise.} \end{cases} \tag{28}$$

If C is Type II, then:

$$d \leq 2[n/6] + 2. \tag{29}$$

A code that meets the appropriate bound is called extremal. There is a systematic proof for the nonexistence of extremal Type II codes if the code length is sufficiently large.

Theorem 9. *Let C be an extremal Type II additive self-dual code over $GF(4)$ of length n. Then, the code C does not exist if $n = 6m$ $(m \geq 17)$, $n = 6m + 2$ $(m \geq 20)$ and $n = 6m + 4$ $(m \geq 22)$.*

Proof. The Gleason polynomials of Type II additive self-dual codes over $GF(4)$ are the same as the ones for Type IV Hermitian self-dual linear codes over $GF(4)$ (see [1], Section 7.7, for examples). Both have the same upper bounds on the minimum distance and the same definition of extremal codes w.r.t. minimum distance. There is a nonexistence theorem for Type IV Hermitian self-dual linear codes over $GF(4)$ that is the same as the above statements [3]. The proof is formulated with Gleason polynomials, so that the nonexistence statements are still valid for Type II additive self-dual codes over $GF(4)$. □

The proof of Theorem 8 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:

$$S = C_0^{\perp} \backslash C. \tag{30}$$

Alternately, it can be defined as:

$$S = \{u \in GF(4)^n \mid u * v = 0 \text{ for all } v \in C_0,\ u * v = 1 \text{ for all } v \in C \backslash C_0\}. \tag{31}$$

The following lemmas for shadow codes can be found in [5]:

Lemma 4. *[5] 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 5. *[5] 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. $B_r \leq 1$ *for* $r < d/2$

Let C be a Type I additive self-dual code over $GF(4)$. By [2], the weight enumerator of C, $W_C(x, y)$, and its shadow code weight enumerator, $W_S(x, y)$, are given by:

$$W_C(x, y) = \sum_{i=0}^{[n/2]} c_i (x + y)^{n-2i} \{y(x - y)\}^i, \tag{32}$$

$$W_S(x, y) = \sum_{i=0}^{[n/2]} (-1)^i 2^{n-3i} c_i y^{n-2i} (x^2 - y^2)^i, \tag{33}$$

for suitable constants c_i. We rewrite Equations (32) and (33) to the following:

$$W_C(1, y) = \sum_{j=0}^{n} a_j y^j = \sum_{i=0}^{[n/2]} c_i (1 + y)^{n-2i} \{y(1 - y)\}^i \tag{34}$$

and:

$$W_S(1, y) = \sum_{j=0}^{[n/2]} b_j y^{2j+t} = \sum_{i=0}^{[n/2]} (-1)^i 2^{n-3i} c_i y^{n-2i} (1 - y^2)^i, \tag{35}$$

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 $0 \leq j \leq i$, and one can write c_i as a linear combination of b_j for $0 \leq j \leq [n/2] - i$ in the following form for suitable constants α_{ij} and β_{ij}:

$$c_i = \sum_{j=0}^{i} \alpha_{ij} a_j = \sum_{j=0}^{[n/2]-i} \beta_{ij} b_j. \tag{36}$$

In our computation, we need to calculate α_{i0} and β_{ij}. The following formulas can be found in [2] for $i > 0$:

$$\alpha_{i0} = -\frac{n}{i}\left[\text{coeff. of } y^{i-1} \text{ in } (1+y)^{-n-1+2i}(1-y)^{-i}\right] \tag{37}$$

and:

$$\beta_{ij} = (-1)^i 2^{3i-n} \binom{k-j}{i}, \tag{38}$$

where $k = [n/2]$. Note that $a_0 = c_0 = \alpha_{00} = 1$. Now, we will introduce the definition of a code with minimal shadow:

Definition 3. *([5]) 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 $r = 1, 3, 5$; and*
2. *$d(S) = 2$ if $r = 0, 2, 4$,*

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

Let C be an extremal Type I additive self-dual code over $GF(4)$ with minimal shadow of length $n = 6m + r$. Then, the following facts can be found in [5]:

Suppose that $r = 0$. Then, $a_0 = 1$, $a_1 = a_2 = \cdots = a_{2m} = 0$, $b_0 = 0$, $b_1 = 1$ if $m \geq 2$, and $b_2 = b_3 = \cdots = b_{m-1} = 0$.

Suppose that $r = 1, 3$. Then, $a_0 = 1$, $a_1 = a_2 = \cdots = a_{2m+1} = 0$, $b_0 = 1$ if $m \geq 1$, and $b_1 = b_2 = \cdots = b_{m-1} = 0$.

Suppose that $r = 2, 4$. Then, $a_0 = 1$, $a_1 = a_2 = \cdots = a_{2m+1} = 0$, $b_0 = 0$, $b_1 = 1$ if $m \geq 2$, and $b_2 = b_3 = \cdots = b_{m-1} = 0$.

Suppose that $r = 5$. Then, $a_0 = 1$, $a_1 = a_2 = \cdots = a_{2m+2} = 0$, $b_0 = 1$, and $b_1 = b_2 = \cdots = b_{m-1} = b_m = 0$. Using this fact, we have the following lemma:

Lemma 6. *[5] Using the above notations, we have the following results:*

1. *If $n = 6m$ $(m \geq 2)$, then $c_i = \alpha_{i0}$ for $0 \leq i \leq 2m$, $c_i = \beta_{i1}$ for $2m + 1 \leq i \leq 3m$.*
2. *If $n = 6m + 1$ $(m \geq 1)$, then $c_i = \alpha_{i0}$ for $0 \leq i \leq 2m + 1$, $c_i = \beta_{i0}$ for $2m + 1 \leq i \leq 3m$.*
3. *If $n = 6m + 2$ $(m \geq 2)$, then $c_i = \alpha_{i0}$ for $0 \leq i \leq 2m + 1$, $c_i = \beta_{i1}$ for $2m + 2 \leq i \leq 3m + 1$.*
4. *If $n = 6m + 3$ $(m \geq 1)$, then $c_i = \alpha_{i0}$ for $0 \leq i \leq 2m + 1$, $c_i = \beta_{i0}$ for $2m + 2 \leq i \leq 3m + 1$.*
5. *If $n = 6m + 4$ $(m \geq 2)$, then $c_i = \alpha_{i0}$ for $0 \leq i \leq 2m + 1$, $c_i = \beta_{i1}$ for $2m + 3 \leq i \leq 3m + 2$.*
6. *If $n = 6m + 5$ $(m \geq 0)$, then $c_i = \alpha_{i0}$ for $0 \leq i \leq 2m + 2$, $c_i = \beta_{i0}$ for $2m + 2 \leq i \leq 3m + 2$.*

Using Lemma 6, we have the following theorems [5]:

Theorem 10. *[5] Extremal Type I additive self-dual codes over $GF(4)$ with minimal shadows of lengths $n = 6m, 6m + 1, 6m + 2, 6m + 3$ and $6m + 5$ have uniquely-determined weight enumerators.*

Theorem 11. *[5] Extremal Type I additive self-dual codes over $GF(4)$ with minimal shadows of lengths $n = 6m + 1$ and $n = 6m + 5$ do not exist.*

Theorem 12. *[5] 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* $m \geq 6$*;*
3. $n = 6m + 3$ *and* $m \geq 22$*.*

Remark 3. *Currently, $n = 6m + 4$ is the unique untouched code length for the nonexistence or an explicit bound for the length n of an extremal Type I additive self-dual code over $GF(4)$ with minimal shadow.*

5. Near-Extremal Type I Additive Self-Dual Codes over $GF(4)$ with Minimal Shadow

In this section, we consider the nonexistence of near-extremal Type I additive self-dual codes over $GF(4)$ with minimal shadow. We start with the following definition:

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

Let C be a near-extremal Type I additive self-dual code over $GF(4)$ with a minimal shadow of length $n = 6m + r$. Then, we have the following facts:

Suppose that $r = 0$. Then, $a_0 = 1$, $a_1 = a_2 = \cdots = a_{2m-1} = 0$ and $b_0 = 0$. By Lemma 5, $b_1 = 1$ if $m \geq 3$. 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 $2m - 4$, and if $u \in S$ is a vector of weight two, then $u + v \in C$ with $wt(u + v) \leq 2m - 4 + 2 = 2m - 2$, a contradiction with the minimum distance of C.

Suppose that $r = 1, 3$. Then, $a_0 = 1$ and $a_1 = a_2 = \cdots = a_{2m} = 0$. By Lemma 5, $b_0 = 1$ if $m \geq 1$. We have $b_1 = b_2 = \cdots = b_{m-1} = 0$. The proof is similar to the above case.

Suppose that $r = 2, 4$. Then, $a_0 = 1$, $a_1 = a_2 = \cdots = a_{2m} = 0$ and $b_0 = 0$. By Lemma 5, $b_1 = 1$ if $m \geq 2$. We have $b_2 = b_3 = \cdots = b_{m-1} = 0$. The proof is similar to the above case.

Suppose that $r = 5$. Then, $a_0 = 1$ and $a_1 = a_2 = \cdots = a_{2m+1} = 0$. By Lemma 5, $b_0 = 1$ if $m \geq 1$. We have $b_1 = b_2 = \cdots = b_{m-1} = 0$. The proof is similar to the above case. Using this fact, we have the following lemma:

Lemma 7. *Using the above notations, we have the following results:*

1. *If $n = 6m$ $(m \geq 3)$, then $c_i = \alpha_{i0}$ for $0 \leq i \leq 2m - 1$, $c_i = \beta_{i1}$ for $2m + 2 \leq i \leq 3m$.*
2. *If $n = 6m + 1$ $(m \geq 1)$, then $c_i = \alpha_{i0}$ for $0 \leq i \leq 2m$, $c_i = \beta_{i0}$ for $2m + 1 \leq i \leq 3m$.*
3. *If $n = 6m + 2$ $(m \geq 2)$, then $c_i = \alpha_{i0}$ for $0 \leq i \leq 2m$, $c_i = \beta_{i1}$ for $2m + 2 \leq i \leq 3m + 1$.*
4. *If $n = 6m + 3$ $(m \geq 1)$, then $c_i = \alpha_{i0}$ for $0 \leq i \leq 2m$, $c_i = \beta_{i0}$ for $2m + 2 \leq i \leq 3m + 1$.*
5. *If $n = 6m + 4$ $(m \geq 2)$, then $c_i = \alpha_{i0}$ for $0 \leq i \leq 2m$, $c_i = \beta_{i1}$ for $2m + 3 \leq i \leq 3m + 2$.*
6. *If $n = 6m + 5$ $(m \geq 1)$, then $c_i = \alpha_{i0}$ for $0 \leq i \leq 2m + 1$, $c_i = \beta_{i0}$ for $2m + 3 \leq i \leq 3m + 2$.*

Proof. Let C be an near-extremal Type I additive self-dual code over $GF(4)$ with a minimal shadow of length $n = 6m(m \geq 3)$. We rewrite Equation (36) as follows:

$$c_i = \sum_{j=0}^{i} \alpha_{ij} a_j = \sum_{j=0}^{3m-i} \beta_{ij} b_j. \tag{39}$$

Then, we have:

$$c_i = \sum_{j=0}^{i} \alpha_{ij} a_j = \alpha_{i0} \text{ for } i = 0, 1, 2, \ldots, 2m - 1 \tag{40}$$

and:

$$c_i = \sum_{j=0}^{3m-i} \beta_{ij} b_j = \beta_{i1} \text{ for } i = 2m + 2, 2m + 2, \ldots, 3m. \tag{41}$$

Therefore, the first statement is proven. The other cases can be proven similarly. □

Using Lemma 7, we have the following theorem:

Theorem 13. *Let C be a near-extremal Type I additive self-dual code over $GF(4)$ with a minimal shadow of length $n = 6m + 1$. Then, we have the following:*

1. *The weight enumerator of C is uniquely determined.*
2. *The code C does not exist if $m \geq 22$.*

Proof. From Lemma 7, we can see that c_i can be calculated by Equations (37) and (38), and the values depend only on the length n for all i, $(0 \leq i \leq [n/3])$ unless $m = 0$. If $m = 0$, then there is only one code for that code length [12]. This proves the first statement.

For the second statement, from Equation (36) and the fact that $c_i = \alpha_{i,0}$ for $0 \leq i \leq 2m$, we have:

$$c_{2m} = \alpha_{2m,0} = \beta_{2m,0} + \beta_{2m,m} b_m. \tag{42}$$

Therefore, we get:

$$b_m = \beta^{-1}_{2m,m}(\alpha_{2m,0} - \beta_{2m,0}). \tag{43}$$

Using Equations (37) and (38), we have:

$$\beta_{2m,m} = \frac{1}{2}, \alpha_{2m,0} = \frac{6m+1}{m}\binom{3m}{m-1}, \beta_{2m,0} = \frac{1}{2}\binom{3m}{2m}. \tag{44}$$

Therefore, we get:

$$b_m = \frac{12m+2}{m}\binom{3m}{m-1} - \binom{3m}{2m}. \tag{45}$$

From Equation (36) and the fact that $c_i = \alpha_{i0}$ for $0 \leq i \leq 2m$, we have:

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

Therefore, we get:

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

Using Equations (37) and (38), we have:

$$\beta_{2m-1,m+1} = -\frac{1}{16}, \alpha_{2m-1,0} = -\frac{6m+1}{2m-1}\left[\binom{3m+2}{m-1} + 10\binom{3m+1}{m-2} + 5\binom{3m}{m-3}\right] \tag{48}$$

and:

$$\beta_{2m-1,0} = -\frac{1}{16}\binom{3m}{2m-1}, \beta_{2m-1,m} = -\frac{m}{8}. \tag{49}$$

Therefore, we get:

$$\begin{aligned} b_{m+1} &= 16 \cdot \frac{6m+1}{2m-1}\left[\binom{3m+2}{m-1} + 10\binom{3m+1}{m-2} + 5\binom{3m}{m-3}\right] \\ &\quad -\binom{3m}{2m-1} - 2m\left[\frac{12m+2}{m}\binom{3m}{m-1} - \binom{3m}{2m}\right]. \end{aligned} \tag{50}$$

From this, we have:

$$b_{m+1} = \frac{(3m)!}{(2m+3)!(m-1)!} h_1(m), \tag{51}$$

where:

$$h_1(m) = -88m^3 + 1864m^2 - 34m - 62. \tag{52}$$

We can see that $h_1(m) < 0$ if $m \geq 22$. Therefore, if $m \geq 22$, then $b_{m+1} < 0$. This is a contradiction. □

Remark 4. *The definition of near-extremal Type II additive self-dual codes over $GF(4)$ and the corresponding nonexistence proof can be found in [11].*

6. Summary

In this paper, we provided a comprehensive presentation of extremal and near-extremal Type I self-dual codes over $GF(2)$ and $GF(4)$ with minimal shadow. We discussed recent research results for these codes. We also proved that there is no near-extremal Type I $[24m, 12m, 2m+2]$ binary self-dual code with minimal shadow if $m \geq 323$, and we proved that there is no near-extremal Type I $(6m+1, 2^{6m+1}, 2m+1)$ additive self-dual code over $GF(4)$ with minimal shadow if $m \geq 22$.

Funding: This research received no external funding.

Acknowledgments: The author wishes to thank the reviewers for valuable remarks, which helped to improve this article.

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. Rains, E.M. Shadow bounds for self-dual codes. *IEEE Trans. Inform. Theory* **1998**, *44*, 134–139. [CrossRef]
3. Zhang, S. On the nonexistence of extremal self-dual codes. *Discrete Appl. Math.* **1999**, *91*, 277–286.
4. Bouyuklieva, S.; Willems, W. Singly even self-dual codes with minimal shadow. *IEEE Trans. Inf. Theory* **2012**, *58*, 3856–3860. [CrossRef]
5. Han, S. Additive self-dual codes over $GF(4)$ with minimal shadow. *Information* **2018**, *9*, 81. [CrossRef]
6. Bouyuklieva, S.; Harada, M.; Munemasa, A. Nonexistence of certain singly even self-dual codes with minimal shadow. *Electron. J. Comb.* **2018**, *25*, 1–13.
7. 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. [CrossRef]
8. Berlekamp, E.R.; MacWilliams, F.J.; Sloane, N.J.A. Gleason's theorem on self-dual codes. *IEEE Trans. Inf. Theory* **1972**, *18*, 409–414. [CrossRef]
9. Conway, J.H.; Sloane, N.J.A. *Sphere Packings, Lattices and Groups*; Springer: New York, NY, USA, 1988.
10. MacWilliams, F.J.; Sloane, N.J.A. *The Theory of Error Correcting Codes*, 9th ed.; North-Holland: Amsterdam, The Netherlands, 1998.
11. Han, S.; Kim, J.L. The nonexistence of near-extremal formally self-dual codes. *Des. Codes Cryptogr.* **2009**, *51*, 69–77. [CrossRef]
12. Huffman, W.C. On the classification and enumeration of self-dual codes. *Finite Fields Appl.* **2005**, *11*, 451–490. [CrossRef]