Extremal and Near-extremal Type I self-dual codes with minimal shadow over $GF(2)$ and $GF(4)$

Sunghyu Han

School of Liberal Arts, KoreaTech

The 5th Sino-Korea Conference on Coding Theory and Its Related Topics
July 02 – July 06, 2018, Shanghai University, Shanghai, China

Self-Dual codes

- Binary self-dual codes & Additive self-dual codes over $GF(4)$
- Common points
  1. Type I, Type II
  2. Shadow codes

Upper bounds of minimum distance

Theorem

(Rains) Let C be an $[n, n/2, d]$ self-dual binary 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 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.

Theorem

(Rains) 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 $d \leq 2[n/6] + 2$ otherwise. If C is Type II, then $d \leq 2[n/6] + 2$.

A code meeting the bound, i.e., equality holds in the bound, is called *extremal*.

Extremal Type II

$\exists$ systematic nonexistence proof

Theorem

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

Theorem

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

Proof.

The proof is the same as the ones of Type IV Hermitian self-dual linear codes over $GF(4)$. The same Gleason polynomials. $\square$

Near-Extremal Type II

Definition

(Han, Kim) Near-extremal Type II code

- binary case: if $d = 4[n/24]$
- additive case: if $d = 2[n/6]$

Theorem

(Han, Kim) There is no near-extremal code with length n for

- *binary case:* $n = 24i(i \geq 315), 24i + 8(i \geq 320), 24i + 16(i \geq 325)$
- *additive case:* $n = 6i(i \geq 38), 6i + 2(i \geq 41), 6i + 4(i \geq 43)$

How about Type I ?

Extremal code : No such proof for the nonexistence proof.
Near-extremal code : No definition for the codes.

Type I codes with minimal shadow

Definition

(Bouyuklieva, Willems) 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.

Definition

(Han) 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 $r > 0$; and
2. $d(S) = 2$ if $r = 0$,

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

Extremal Type I codes with minimal shadow

- binary case: nonexistence proof for some codes
- additive case: nonexistence proof for some codes

Near-extremal Type I codes

Definition

Let C be a $[n, n/2, d]$ 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 $n \equiv 22 \pmod{24}$.

Definition

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.

Near-extremal Type I codes with minimal shadow

- binary case: nonexistence proof for some codes
- additive case: nonexistence proof for some codes

Contents

- Extremal Type I binary self-dual codes with minimal shadow
- Near-extremal Type I binary self-dual codes with minimal shadow
- Extremal Type I additive self-dual codes over $GF(4)$ with minimal shadow
- Near-extremal Type I additive self-dual codes over $GF(4)$ with minimal shadow

Extremal Type I binary self-dual codes with minimal shadow

- $GF(2)$: Finite Field of order 2
- A linear code : $GF(2)$-subspace $C \subseteq GF(2)^n$
- Inner Product : for $\mathbf{x}, \mathbf{y} \in GF(2)^n$, $\mathbf{x} \cdot \mathbf{y} = x_1 y_1 + \cdots + x_n y_n$.
- Dual code : $C^{\perp} = \{\mathbf{x} \in GF(2)^n \,\big|\, \mathbf{x} \cdot \mathbf{c} = 0, \forall\, \mathbf{c} \in C\}$
- Self-dual : $C = C^{\perp}$
- Type II : if the weights of all codewords are divisible by 4
- Type I : otherwise

Extremal Type I binary self-dual codes with minimal shadow

Theorem

(Rains) Let C *be an* $[n, n/2, d]$ *self-dual binary 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 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 bound, i.e., equality holds in the bound, is called *extremal*.

- $\exists$ systematic nonexistence proof

Theorem

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

- Shadow code

Extremal Type I binary self-dual codes with minimal shadow

Shadow code

- let $C^{(0)}$ be the subset of C consisting of all codewords whose weights are multiples of 4
- let $C^{(2)} = C \backslash C^{(0)}$
- $$S = S(C) = \{u \in GF(2)^n : (u,v) = 0 \text{ for all } v \in C^{(0)}, (u,v) = 1 \text{ for all } v \in C^{(2)}\}.$$

Lemma

(Conway, Sloane) 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. $b_i \leq 1$ *for* $i < d/2$

Extremal Type I binary self-dual codes with minimal shadow

Let C be a Type I binary self-dual code of length $n = 24m + 8\ell + 2r$ where $\ell = 0, 1, 2$ and $r = 0, 1, 2, 3$.

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

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

$\Rightarrow$

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

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

Extremal Type I binary self-dual codes with minimal shadow

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

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

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

where $k = 3m + \ell$.

Extremal Type I binary self-dual codes with minimal shadow

Definition

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.

Extremal Type I binary self-dual codes with minimal shadow

Let C be an extremal Type I binary self-dual code with a minimal shadow of length n.

- 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 $a_{2m+2} = 0$.
- $b_0 = 1$ if (i) $r = 1$ and $m \geq 0$ and (ii) $r = 2, 3$ and $m \geq 1$.
- $b_0 = 0, b_1 = 1$ 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 $b_m = 0$.

Extremal Type I binary self-dual codes with minimal shadow

Lemma

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* $2m + 3 \leq i \leq 3m + 2$.

Extremal Type I binary self-dual codes with minimal shadow

Theorem

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 $n \not\equiv 24m + 16, 24m + 20$.

Theorem

(Bouyuklieva, Willems) 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

(Bouyuklieva, Willems) 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* $m \geq 157$.

Extremal Type I binary self-dual codes with minimal shadow

Remark

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.

Near-extremal Type I binary self-dual codes with minimal shadow

Definition

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 $n \equiv 22 \pmod{24}$.

Near-extremal Type I binary self-dual codes with minimal shadow

Let C be a near-extremal Type I binary self-dual code with minimal shadow.

- $a_0 = 1, a_1 = a_2 = \cdots = a_{2m} = 0$.
- Moreover, if $n \equiv 22 \pmod{24}$, then $a_{2m+1} = 0$.
- $b_0 = 1$ if (i) $r = 1, 2$ and $m \geq 1$ (ii) $r = 3$, $n \not\equiv 22 \pmod{24}$, and $m \geq 2$ (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 $b_1 = b_2 = \cdots = b_{m-1} = 0$.
- 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 $b_2 = b_3 = \cdots = b_{m-1} = 0$.

Near-extremal Type I binary self-dual codes with minimal shadow

Lemma

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* $2m+3 \leq i \leq 3m+2$.

Near-extremal Type I binary self-dual codes with minimal shadow

Theorem

(Bouyuklieva, Harada, Munemasa) 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:*
   - **2.1** $n = 24m + 2$ *and* $m \geq 155$
   - **2.2** $n = 24m + 4$ *and* $m \geq 156$
   - **2.3** $n = 24m + 10$ *and* $m \geq 160$

Near-extremal Type I binary self-dual codes with minimal shadow

Theorem

(Han) 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.

If $n = 24m$ ($m \geq 2$), then $c_i = \alpha_{i0}$ for $0 \leq i \leq 2m$, $c_i = \beta_{i1}$ for $2m+1 \leq i \leq 3m$. If $m = 1$, then $n = 24$. For this case, there is a unique near-extremal Type I code. 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. □

Near-extremal Type I binary self-dual codes with minimal shadow

Proof.
For the second statement,

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

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

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

$$b_m = 6\binom{5m-1}{m-1} - \frac{3m-1}{2m}\binom{5m-2}{m-1}. \tag{4}$$

□

Near-extremal Type I binary self-dual codes with minimal shadow

Proof.

$$c_{2m-1} = \alpha_{2m-1,0} = \beta_{2m-1,1} + \beta_{2m-1,m} b_m + \beta_{2m-1,m+1} b_{m+1}. \tag{5}$$

$$b_{m+1} = \beta_{2m-1,m+1}^{-1} (\alpha_{2m-1,0} - \beta_{2m-1,1} - \beta_{2m-1,m} b_m). \tag{6}$$

$$\beta_{2m-1,m+1} = -2^{-6}, \tag{7}$$

$$\alpha_{2m-1,0} = -\frac{24m}{2(2m-1)} \left[\binom{5m+3}{m-1} + \binom{5m+2}{m-2}\binom{7}{2} + \binom{5m+1}{m-3}\binom{7}{4} + \binom{5m}{m-4}\binom{7}{6} \right] \tag{8}$$

$$\beta_{2m-1,1} = -2^{-6} \times \frac{3m-1}{2m-1}\binom{5m-3}{m}, \quad \beta_{2m-1,m} = -\frac{m}{16}. \tag{9}$$

$$b_{m+1} = \frac{64(6m-1)(5m-1)(5m-3)!}{(4m+4)!(m-1)!} h_0(m), \tag{10}$$

$$h_0(m) = -64m^5 + 20640m^4 - 9388m^3 + 582m^2 - 49m - 3. \tag{11}$$

We can see that $h_0(m) < 0$ if $m \geq 323$. □

Extremal Type I additive self-dual codes over $GF(4)$ with minimal shadow

- $GF(4)$: Finite Field of order 4
- An additive code : $GF(4)$-subgroup $C \subseteq GF(4)^n$
- Hermitian Trace Inner Product : for $\mathbf{x}, \mathbf{y} \in GF(4)^n$,
  $u * v = \sum_{i=1}^{n} \mathrm{Tr}(u_i {v_i}^2) = \sum_{i=1}^{n} (u_i {v_i}^2 + {u_i}^2 v_i) \pmod 2.$
- Dual code : $C^{\perp} = \{\mathbf{u} \in GF(4)^n \,\big|\, \mathbf{u} * \mathbf{c} = 0, \forall\, \mathbf{c} \in C\}$
- Self-dual : $C = C^{\perp}$
- Type II : if the weights of all codewords are divisible by 2
- Type I : otherwise

Extremal Type I additive self-dual codes over $GF(4)$ with minimal shadow

Theorem

(Rains) 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 $d \leq 2[n/6] + 2$ otherwise. If C is Type II, then $d \leq 2[n/6] + 2$.

$\Rightarrow$ A code that meets the appropriate bound is called extremal.

Theorem

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 proof is the same as the ones for Type IV Hermitian self-dual linear codes over $GF(4)$ □

$\Rightarrow$ Shadow code

Extremal Type I additive self-dual codes over $GF(4)$ with minimal shadow

Shadow code

- let $C^{(0)}$ be the subset of C consisting of all codewords whose weights are multiples of 2
- $$S = C_0^{\perp} \backslash C.$$
- Alternately, it can be defined as:

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

Lemma

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

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* $r < d/2$

Extremal Type I additive self-dual codes over $GF(4)$ with minimal shadow

Let C be a Type I additive self-dual code over $GF(4)$.

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

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

$\Rightarrow$

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

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

Extremal Type I additive self-dual codes over $GF(4)$ with minimal shadow

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

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

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

where $k = [n/2]$.

Extremal Type I additive self-dual codes over $GF(4)$ with minimal shadow

Definition

(Han) 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 $r > 0$; and
2. $d(S) = 2$ if $r = 0$,

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

Extremal Type I additive self-dual codes over $GF(4)$ with minimal shadow

Let C be an extremal Type I additive self-dual codes over $GF(4)$ with minimal shadow of length $n = 6m + r$.

- $r = 0$:
  $a_0 = 1$ and $a_1 = a_2 = \cdots = a_{2m} = 0$.
  $b_0 = 0$. $b_1 = 1$ if $m \geq 2$. $b_2 = b_3 = \cdots = b_{m-1} = 0$.
- $r = 1, 3$:
  $a_0 = 1$ and $a_1 = a_2 = \cdots = a_{2m+1} = 0$.
  $b_0 = 1$ if $m \geq 1$. $b_1 = b_2 = \cdots = b_{m-1} = 0$.
- $r = 2, 4$:
  $a_0 = 1$ and $a_1 = a_2 = \cdots = a_{2m+1} = 0$.
  $b_0 = 0$. $b_1 = 1$ if $m \geq 2$. $b_2 = b_3 = \cdots = b_{m-1} = 0$.
- $r = 5$:
  $a_0 = 1$ and $a_1 = a_2 = \cdots = a_{2m+2} = 0$.
  $b_0 = 1$. $b_1 = b_2 = \cdots = b_{m-1} = b_m = 0$.

Extremal Type I additive self-dual codes over $GF(4)$ with minimal shadow

Lemma

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* $2m + 2 \leq i \leq 3m + 2$.

Extremal Type I additive self-dual codes over $GF(4)$ with minimal shadow

Theorem

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

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

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* $m \geq 22$.

Extremal Type I additive self-dual codes over $GF(4)$ with minimal shadow

Remark

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.

Near-extremal Type I additive self-dual codes over $GF(4)$ with minimal shadow

Definition

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.

Near-extremal Type I additive self-dual codes over $GF(4)$ with minimal shadow

Let C be a near-extremal Type I additive self-dual code over $GF(4)$ with a minimal shadow of length $n = 6m + r$.

- $r = 0$:
  $a_0 = 1$ and $a_1 = a_2 = \cdots = a_{2m-1} = 0$.
  $b_0 = 0$. $b_1 = 1$ if $m \geq 3$. $b_2 = b_3 = \cdots = b_{m-2} = 0$.
- $r = 1, 3$:
  $a_0 = 1$ and $a_1 = a_2 = \cdots = a_{2m} = 0$. $b_0 = 1$ if $m \geq 1$.
  $b_1 = b_2 = \cdots = b_{m-1} = 0$.
- $r = 2, 4$:
  $a_0 = 1$ and $a_1 = a_2 = \cdots = a_{2m} = 0$.
  $b_0 = 0$. $b_1 = 1$ if $m \geq 2$. $b_2 = b_3 = \cdots = b_{m-1} = 0$.
- $r = 5$:
  $a_0 = 1$ and $a_1 = a_2 = \cdots = a_{2m+1} = 0$.
  $b_0 = 1$ if $m \geq 1$. $b_1 = b_2 = \cdots = b_{m-1} = 0$.

Near-extremal Type I additive self-dual codes over $GF(4)$ with minimal shadow

Lemma

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* $2m+3 \leq i \leq 3m+2$.

Near-extremal Type I additive self-dual codes over $GF(4)$ with minimal shadow

Theorem

Let C be an 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.

If $n = 6m + 1$ ($m \geq 1$), then $c_i = \alpha_{i0}$ for $0 \leq i \leq 2m$, $c_i = \beta_{i0}$ for $2m + 1 \leq i \leq 3m$. If $m = 0$, then there is only one code for that code length. This proves the first statement. □

Near-extremal Type I additive self-dual codes over $GF(4)$ with minimal shadow

For the second statement,

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

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

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

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

Near-extremal Type I additive self-dual codes over $GF(4)$ with minimal shadow

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

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

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

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

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

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

$$h_1(m) = -88m^3 + 1864m^2 - 34m - 62.$$

We can see that $h_1(m) < 0$ if $m \geq 22$.