J. Korean Math. Soc. **43** (2006), No. 6, pp. 1357–1369

NONEXISTENCE OF SOME EXTREMAL SELF-DUAL CODES

SUNGHYU HAN AND JUNE BOK LEE

ABSTRACT. It is known that if C is an $[24m + 2l, 12m + l, d]$ self-dual binary linear code with $0 \leq l < 11$, then $d \leq 4m + 4$. We present a sufficient condition for the nonexistence of extremal self-dual binary linear codes with $d = 4m + 4, l = 1, 2, 3, 5$. From the sufficient condition, we calculate m's which correspond to the nonexistence of some extremal self-dual binary linear codes. In particular, we prove that there are infinitely many such m's. We also give similar results for additive self-dual codes over $GF(4)$ of length $n = 6m + 1$.

1. Introduction

We are mainly interested in binary linear codes and additive codes over $GF(4)$. First, we introduce binary linear codes. 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 $u = (u_1, u_2, \ldots, u_n)$ 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

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

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

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

Received March 30, 2006.
2000 Mathematics Subject Classification: Primary 94B60, 94B65.
Key words and phrases: self-dual code, extremal code, shadow.

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 weight. Clearly self-dual binary codes are even. In addition, some of these codes have all codewords of weight divisible by 4. A self-dual code with all codewords of weight divisible by 4 is called doubly-even or Type II; a self-dual code with some codeword of weight not divisible by 4 is called singly-even or Type I. Type II codes exist only for lengths a multiple of 8 [7].

Bounds on the minimum distance of self-dual binary codes were given in [8, 9].

THEOREM 1. *Let C be an $[n, n/2, d]$ self-dual binary code. Then $d \leq 4[n/24] + 4$ if $n \not\equiv 22 (\mathrm{mod}\ 24)$. If $n \equiv 22 (\mathrm{mod}\ 24)$, 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 of Theorem 1, i.e., equality holds in the bound, is called extremal. Extremal Type II codes do not exist for lengths $n > 3928$ [10].

The proof of Theorem 1 when the code is Type I used the concept of the shadow. In [3], the shadow code of a 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 multiple of 4, and let $C^{(2)} = C \backslash C^{(0)}$. The shadow code of C is defined by

$$\begin{aligned} S &= S(C) \\ &= \{u \in GF(2)^n : (u, v) = 0 \text{ for all } v \in C^{(0)}, \\ &\qquad\qquad (u, v) = 1 \text{ for all } v \in C^{(2)}\}. \end{aligned}$$

For the general definition of shadow code and related information is presented in [3].

Next, we explain additive codes over $GF(4)$. An additive code, C, over $GF(4)$ of length n is an additive subgroup of $GF(4)^n$. The weight of a vector $u \in GF(4)^n$, the minimum distance of C, and codewords are defined by the same way in the binary linear codes. C is a k-dimensional $GF(2)$-subspace of $GF(4)^n$ and so has 2^k codewords. It is denoted an $(n, 2^k)$ code, and if its minimum distance is d, the code is an $(n, 2^k, d)$ code.

The trace map, $Tr : GF(4) \rightarrow GF(2)$, is defined by $Tr(x) = x + x^2$. 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 by

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

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,

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

Self-orthogonal and self-dual are defined by the same way in the binary linear codes. It has been shown that self-orthogonal additive codes over $GF(4)$ can be used to represent quantum error-correcting codes [2]. If C is self-dual, then it must be an $(n, 2^n)$ code. Self-dual additive codes over $GF(4)$ correspond to zero-dimensional quantum codes, which represent single quantum states. If the code has high minimum distance, the corresponding quantum state is highly entangled.

We distinguish between two types of self-dual additive codes over $GF(4)$. A code is of Type II if all codewords have even weight, otherwise it is of Type I. It can be shown that a Type II code must have even length.

Bounds on the minimum distance of self-dual codes were given by Rains and Sloane [8, 9].

THEOREM 2. *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 that meets the appropriate bound is called extremal. It can be shown that extremal Type II codes must have a unique weight enumerator.

As in the case of binary codes, the proof of Theorem 2 used the shadow codes. Let C_0 be the subset of C consisting of all codewords whose weights are multiple of 2. The shadow codes of an additive code C over $GF(4)$ is defined by

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

In this paper, we will prove that some extremal self-dual codes do not exist. First, in Section 2, we give a sufficient condition for the nonexistence of extremal self-dual binary codes $C[24m+2l, 12m+l, 4m+4]$ with $l = 1, 2, 3, 5$. The sufficient condition is used to calculate m's

which correspond to the nonexistence of some extremal self-dual binary codes. In particular, we prove that there are infinitely many such m's for each $l = 1, 2, 3, 5$. In section 3, we give similar results for additive self-dual codes over $GF(4)$ of length $n = 6m + 1$.

2. Binary self-dual codes

The weight enumerator of a binary code is given by

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

where there are A_i codewords of weight i in C. We are interested in only Type I code. From now on C is assumed as a Type I code. By Gleason's theorem [1, 4, 6], we can write the weight enumerator of C:

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

for suitable constants c_i. Using the shadow code theory [3], we can write the weight enumerator of shadow code $S(C)$,

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

We rewrite (1), (2) as the following form

$$\begin{aligned} W_C(1, y) &= \sum_{j=0}^{[n/2]} a_j y^{2j} \\ &= \sum_{i=0}^{[n/8]} c_i (1 + y^2)^{n/2-4i} \{y^2 (1 - y^2)^2\}^i, \end{aligned}$$

$$\begin{aligned} W_S(1, y) &= \sum_{j=0}^{2[n/8]} b_j y^{4j+t} \\ &= \sum_{i=0}^{[n/8]} (-1)^i 2^{n/2-6i} c_i y^{n/2-4i} (1 - y^4)^{2i}, \end{aligned}$$

where $t \equiv n/2 \pmod 4$. Note that $a_0 = 1$, and all a_j and b_j must be nonnegative integers. One can write c_i as a linear combination of

the a_j for $0 \le j \le i$. Also one can write $(-1)^i 2^{n/2-6i} c_i$ as a linear combination of b_j for $0 \le j \le [n/8] - i$. Note that the coefficients of these linear combinations are all integers. As a result, c_i and $2^{n/2-6i} c_i$ are all integers for $0 \le i \le [n/8]$.

Define $\alpha_i(n)$ to be the coefficient of a_0 in the expansion of c_i in terms of a_j for $0 \le j \le i$. For $i > 0$,

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

This comes from [8]. We are ready to prove the following theorem which states the sufficient condition for the nonexistence of extremal self-dual binary codes.

THEOREM 3. *Let C be a $[24m+2l, 12m+l, d]$ Type I binary self-dual code. Let*

$$e = \sum_{k=1}^{\infty}\left[\frac{5m-1}{2^k}\right] - \left(\sum_{k=1}^{\infty}\left[\frac{4m+1}{2^k}\right] + \sum_{k=1}^{\infty}\left[\frac{m-1}{2^k}\right]\right).$$

(i) *If $l = 1, 2, 3$ and $e < 3$, then $d < 4m + 4$.*
(ii) *If $l = 5$, $m =$ even, and $e < 1$, then $d < 4m + 4$.*

Proof. Let C be a $[24m + 2l, 12m + l, 4m + 4]$. Type I extremal self-dual code. Since $a_i = 0$ for $1 \le i \le 2m + 1$,

$$\begin{aligned} c_{2m+1} &= \alpha_{2m+1}(24m+2l) \\ &= -\frac{12m+l}{2m+1}\left[\text{coeff. of } y^{2m} \text{ in } (1+y)^{-4m-l+3}(1-y)^{-4m-2}\right] \\ &= -\frac{12m+l}{2m+1}\left[\text{coeff. of } y^{2m} \text{ in } (1+y)^{5-l}(1-y^2)^{-4m-2}\right]. \end{aligned}$$

Suppose that $l = 1$.

$$\begin{aligned} c_{2m+1} &= -\frac{12m+1}{2m+1}\left[\text{coeff. of } y^{2m} \text{ in } (1+y)^4(1-y^2)^{-4m-2}\right] \\ &= -\frac{12m+1}{2m+1} \\ &\quad \times \left[\text{coeff. of } y^{2m} \text{ in } \left(\sum_{i=0}^{4}\binom{4}{i}y^i\right)\left(\sum_{j=0}^{\infty}\binom{4m+1+j}{j}y^{2j}\right)\right] \\ &= -\frac{12m+1}{2m+1}\cdot\frac{4(14m+1)}{5m}\binom{5m}{m-1}. \end{aligned} \tag{3}$$

$$
\begin{aligned}
& -c_{2m+1} \cdot 2^{(24m+2)/2-6(2m+1)} \\
= \; & \frac{1}{8} \cdot \frac{12m+1}{2m+1} \cdot \frac{14m+1}{5m} \binom{5m}{m-1} \\
= \; & \frac{(12m+1)(14m+1)}{2m+1} \cdot \frac{(5m-1)!}{2^3(4m+1)!(m-1)!}. \qquad (4)
\end{aligned}
$$

Note that (4) is an integer. Let f be the exponent of 2 in (4).

$$f = \sum_{k=1}^{\infty} \left[\frac{5m-1}{2^k} \right] - \left(\sum_{k=1}^{\infty} \left[\frac{4m+1}{2^k} \right] + \sum_{k=1}^{\infty} \left[\frac{m-1}{2^k} \right] \right) - 3.$$

Since (4) is an integer, $f \geq 0$ and

$$e = \sum_{k=1}^{\infty} \left[\frac{5m-1}{2^k} \right] - \left(\sum_{k=1}^{\infty} \left[\frac{4m+1}{2^k} \right] + \sum_{k=1}^{\infty} \left[\frac{m-1}{2^k} \right] \right) \geq 3.$$

We can conclude that if $e < 3$, then the minimum distance $d \neq 4m+4$, i.e., $d < 4m+4$.

The cases of $l = 2$ and $l = 3$ can be proved similarly. Now assume that $l = 5$ and $m =$ even. By a similar calculation to (3),

$$
\begin{aligned}
& -c_{2m+1} \cdot 2^{(24m+10)/2-6(2m+1)} \\
= \; & \frac{5(12m+5)(5m+1)}{2m+1} \cdot \frac{(5m-1)!}{2(4m+1)!(m-1)!}. \qquad (5)
\end{aligned}
$$

Let g be the exponent of 2 in (5). Since m is assumed to be even,

$$g = \sum_{k=1}^{\infty} \left[\frac{5m-1}{2^k} \right] - \left(\sum_{k=1}^{\infty} \left[\frac{4m+1}{2^k} \right] + \sum_{k=1}^{\infty} \left[\frac{m-1}{2^k} \right] \right) - 1.$$

Since (5) is an integer, $g \geq 0$ and

$$e = \sum_{k=1}^{\infty} \left[\frac{5m-1}{2^k} \right] - \left(\sum_{k=1}^{\infty} \left[\frac{4m+1}{2^k} \right] + \sum_{k=1}^{\infty} \left[\frac{m-1}{2^k} \right] \right) \geq 1.$$

If $e < 1$, then the minimum distance $d \neq 4m+4$, i.e., $d < 4m+4$. □

In the above Theorem 3, the main point is the calculation of e. The following Lemma gives another method for the calculation of e.

LEMMA 4. *Let m be a positive integer. Suppose $m, m-1, 5m-1$ are described by binary representations,*

$$
\begin{aligned}
m &= a_{r-1} \cdot 2^{r-1} + a_{r-2} \cdot 2^{r-2} + \cdots + a_1 \cdot 2^1 + a_0 \cdot 2^0, \\
m-1 &= b_{r-1} \cdot 2^{r-1} + b_{r-2} \cdot 2^{r-2} + \cdots + b_1 \cdot 2^1 + b_0 \cdot 2^0, \\
5m-1 &= c_{r+2} \cdot 2^{r+2} + c_{r+1} \cdot 2^{r+1} + \cdots + c_1 \cdot 2^1 + c_0 \cdot 2^0,
\end{aligned}
$$

where $(a_i, b_i, c_i \in \{0,1\}, 0 \le i \le r+2)$. *If*

$$e = \sum_{k=1}^{\infty}\left[\frac{5m-1}{2^k}\right] - \left(\sum_{k=1}^{\infty}\left[\frac{4m+1}{2^k}\right] + \sum_{k=1}^{\infty}\left[\frac{m-1}{2^k}\right]\right)$$

and

$$A = \{i : c_{i+2} < a_i + b_{i+2}, 0 \le i \le r-1\},$$

then

$$e = |A|.$$

Proof. Note that

$$4m+1 = a_{r-1}\cdot 2^{r+1} + a_{r-2}\cdot 2^r + \cdots + a_0 \cdot 2^2 + 0\cdot 2^1 + 1\cdot 2^0.$$

Since $5m-1 = (m-1) + (4m+1) - 1$,

$$\begin{aligned} 5m-1 = {} & (a_{r-1}+b_{r+1})\cdot 2^{r+1} + (a_{r-2}+b_r)\cdot 2^r + \cdots + (a_0+b_2)\cdot 2^2 \\ & + b_1\cdot 2^1 + b_0\cdot 2^0, \end{aligned}$$

where $b_{r+1} = b_r = 0$. We use the following identities.

$$\sum_{k=1}^{\infty}\left[\frac{\sum_{i=0}^{r-1} d_i\cdot 2^i}{2^k}\right] = \sum_{i=0}^{r-1}\sum_{k=1}^{\infty}\left[\frac{d_i\cdot 2^i}{2^k}\right], \quad (d_i \in 0,1).$$

$$\sum_{k=1}^{\infty}\left[\frac{(1+1)\cdot 2^i}{2^k}\right] = \sum_{k=1}^{\infty}\left[\frac{2^i}{2^k}\right] + \sum_{k=1}^{\infty}\left[\frac{2^i}{2^k}\right] + 1.$$

If $c_{i+2} < a_i + b_{i+2}$, then there is a carry to 2^{i+3}th position. This fact and above two identities imply that e is equal to the sum of carries, i.e., $e = |A|$. □

We obtain the following Corollary from the above Lemma 4 and Theorem 3.

COROLLARY 5. (i) *For each* $l = 1,2,3,5$, *there are infinitely many* m*'s such that there is no* $[24m+2l, 12m+l, d]$ *extremal Type I self-dual code.*

(ii) *If* $l = 1,2,3$ *and* $1 \le m \le 100$, *then for at least* 61 *values of* m, *there is no* $[24m+2l, 12m+l, d]$ *extremal Type I self-dual code.*

(iii) *If* $l = 1,2,3$ *and* $1 \le m \le 1000$, *then for at least* 336 *values of* m, *there is no* $[24m+2l, 12m+l, d]$ *extremal Type I self-dual code.*

(iv) *If* $l = 5$, $m =$ *even, and* $1 \le m \le 100$, *then for at least* 23 *values of* m, *there is no* $[24m+2l, 12m+l, d]$ *extremal Type I self-dual code.*

(v) *If* $l = 5$, $m =$ *even, and* $1 \leq m \leq 1000$, *then for at least* 103 *values of* m, *there is no* $[24m + 2l, 12m + l, d]$ *extremal Type I self-dual code.*

Proof. For (i), if we take $m = 2^k + 2$ $(k \geq 4)$, then $|A| = e = 0$ in Lemma 4. The remaining assertions follow from Table 1. □

We include Table 1 which contains these m values of Corollary 5(ii), (iii), (iv), (v). We added $l = 5, m = 1$ in Table 1, since there is no $[34, 17, 8]$ extremal self-dual codes by the Table 1 in [5].

Until now, there is no known $[24m + 2l, 12m + l, 4m + 4]$ extremal binary self-dual code with $l = 1, 2, 3, 5$. We invite the reader to prove the following conjecture or find a counter-example.

CONJECTURE. *There is no* $[24m+2l, 12m+l, 4m+4]$ *extremal Type I binary self-dual code with* $l = 1, 2, 3, 5$.

3. Additive self-dual codes over $GF(4)$

The main idea of this section is similar to section 2. The weight enumerator of an additive self-dual code over $GF(4)$ is defined by the same way in the binary code. We are interested in only Type I code. From now on C is assumed as a Type I code. By [8], the weight enumerator of C, $W_C(x, y)$, and its shadow code weight enumerator, $W_S(x, y)$, are given by

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

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

for suitable constants c_i. We rewrite (6), (7) as the following form

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

TABLE 1. Values of m for which no $[24m + 2l, 12m + l, 4m + 4]$ extremal Type I binary self-dual code exists

$l = 1, 2, 3$ $1 \leq m \leq 100$	1 2 3 4 5 6 8 9 10 11 12 16 17 18 19 20 21 22 24 25 32 33 34 35 36 37 38 40 41 42 43 44 48 49 50 51 64 65 66 67 68 69 70 72 73 74 75 76 80 81 82 83 84 86 88 89 96 97 98 99 100
$l = 1, 2, 3$ $101 \leq m \leq 1000$	101 102 128 129 130 131 132 133 134 136 137 138 139 140 144 145 146 147 148 149 150 152 153 160 161 162 163 164 165 166 168 169 172 176 177 178 179 192 193 194 195 196 197 198 200 201 202 203 204 256 257 258 259 260 261 262 264 265 266 267 268 272 273 274 275 276 277 278 280 281 288 289 290 291 292 293 294 296 297 298 299 300 304 305 306 307 320 321 322 323 324 325 326 328 329 330 331 332 336 337 338 339 344 345 352 353 354 355 356 357 358 384 385 386 387 388 389 390 392 393 394 395 396 400 401 402 403 404 405 406 408 409 512 513 514 515 516 517 518 520 521 522 523 524 528 529 530 531 532 533 534 536 537 544 545 546 547 548 549 550 552 553 554 555 556 560 561 562 563 576 577 578 579 580 581 582 584 585 586 587 588 592 593 594 595 596 598 600 601 608 609 610 611 612 613 614 640 641 642 643 644 645 646 648 649 650 651 652 656 657 658 659 660 662 664 665 672 673 674 675 676 678 688 689 690 691 704 705 706 707 708 709 710 712 713 714 715 716 768 769 770 771 772 773 774 776 777 778 779 780 784 785 786 787 788 789 790 792 793 800 801 802 803 804 805 806 808 809 810 811 812 816 817 818 819
$l = 5$ $1 \leq m \leq 100$	1 2 4 6 8 12 16 18 24 32 34 36 38 48 50 64 66 68 70 72 76 96 98 100
$l = 5$ $101 \leq m \leq 1000$	102 128 130 132 134 136 140 144 146 152 192 194 196 198 200 204 256 258 260 262 264 268 272 274 280 288 290 292 294 304 306 384 386 388 390 392 396 400 402 408 512 514 516 518 520 524 528 530 536 544 546 548 550 560 562 576 578 580 582 584 588 608 610 612 614 768 770 772 774 776 780 784 786 792 800 802 804 806 816 818

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

where $t \equiv n \pmod 2$. As before, $a_0 = 1$, and all a_j and b_j must be nonnegative integers. One can write c_i as a linear combination of the a_j for $0 \le j \le i$. Also one can write $(-1)^i 2^{n-3i} c_i$ as a linear combination of b_j for $0 \le j \le [n/2] - i$. Note that the coefficients of these linear combinations are all integers. As a result, c_i and $2^{n-3i} c_i$ are all integers for $0 \le i \le [n/2]$.

Define $\alpha_i(n)$ to be the coefficient of a_0 in the expansion of c_i in terms of a_j for $0 \le j \le i$. For $i > 0$,

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

This follows from the Bürman-Lagrange theorem in [9]. We are ready to prove the following theorem which states the sufficient condition for the nonexistence of extremal self-dual additive codes over $GF(4)$.

THEOREM 6. *Let C be a $(6m+1, 2^{6m+1}, d)$ Type I additive self-dual code over $GF(4)$. Let*

$$e = \sum_{k=1}^{\infty}\left[\frac{3m}{2^k}\right] - \left(\sum_{k=1}^{\infty}\left[\frac{2m}{2^k}\right] + \sum_{k=1}^{\infty}\left[\frac{m}{2^k}\right]\right).$$

If $e < 2$, then $d < 2m+2$.

Proof. Let $(6m+1, 2^{6m+1}, 2m+2)$ be a Type I extremal self-dual code. Since $a_i = 0$ for $1 \le i \le 2m+1$,

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

$$2^{6m+1-3(2m+1)} \cdot c_{2m+1} = -\frac{1}{4} \cdot \frac{6m+1}{2m+1} \cdot \binom{3m}{m}. \tag{8}$$

Note that (8) is an integer. Let f be the exponent of 2 in (8).

$$f = \sum_{k=1}^{\infty}\left[\frac{3m}{2^k}\right] - \left(\sum_{k=1}^{\infty}\left[\frac{2m}{2^k}\right] + \sum_{k=1}^{\infty}\left[\frac{m}{2^k}\right]\right) - 2.$$

Since $f \geq 0$,

$$e = \sum_{k=1}^{\infty} \left[\frac{3m}{2^k} \right] - \left(\sum_{k=1}^{\infty} \left[\frac{2m}{2^k} \right] + \sum_{k=1}^{\infty} \left[\frac{m}{2^k} \right] \right) \geq 2.$$

We can conclude that if $e < 2$, then the minimum distance $d \neq 2m + 2$, i.e., $d < 2m + 2$. □

As before, the following Lemma gives another method for the calculation of e in Theorem 6.

LEMMA 7. *Let m be a positive integer. Suppose $m, 3m$ are described by binary representations,*

$$\begin{aligned} m &= a_{r-1} \cdot 2^{r-1} + a_{r-2} \cdot 2^{r-2} + \cdots + a_1 \cdot 2^1 + a_0 \cdot 2^0, \\ 3m &= c_{r+1} \cdot 2^{r+1} + c_r \cdot 2^r + \cdots + c_1 \cdot 2^1 + c_0 \cdot 2^0, \end{aligned}$$

where $(a_i, c_i \in \{0, 1\}, 0 \leq i \leq r + 1)$. If

$$e = \sum_{k=1}^{\infty} \left[\frac{3m}{2^k} \right] - \left(\sum_{k=1}^{\infty} \left[\frac{2m}{2^k} \right] + \sum_{k=1}^{\infty} \left[\frac{m}{2^k} \right] \right) \tag{9}$$

and

$$A = \{i : c_{i+1} < a_i + a_{i+1}, 0 \leq i \leq r - 1\},$$

then

$$e = |A|.$$

Proof. Similar to Lemma 4. □

We obtain the following Corollary from the above Lemma 7 and Theorem 6.

COROLLARY 8. (i) *There are infinitely many m's such that there is no $(6m + 1, 2^{6m+1}, d)$ extremal Type I additive self-dual code over $GF(4)$.*

(ii) *If $1 \leq m \leq 100$, then for at least 38 values of m, there is no $(6m + 1, 2^{6m+1}, d)$ extremal Type I additive self-dual code over $GF(4)$.*

(iii) *If $1 \leq m \leq 1000$, then for at least 164 values of m, there is no $(6m + 1, 2^{6m+1}, d)$ extremal Type I additive self-dual code over $GF(4)$.*

Proof. For (i), if we take $m = 2^k$ $(k \geq 0)$, then $|A| = e = 0$ in Lemma 7. (ii), (iii) follow from Table 2. □

We include Table 2 which contains these m values of Corollary 8 (ii), (iii). As in Section 2, we conjecture the following statement.

TABLE 2. Values of m for which no $(6m+1, 2^{6m+1}, 2m+2)$ extremal Type I additive self-dual code over $GF(4)$ exists

$1 \leq m \leq 100$	1 2 3 4 5 8 9 10 16 17 18 19 20 21 32 33 34 35 36 37 40 41 42 64 65 66 67 68 69 72 73 74 80 81 82 83 84 85
$101 \leq m \leq 1000$	128 129 130 131 132 133 136 137 138 144 145 146 147 148 149 160 161 162 163 164 165 168 169 170 256 257 258 259 260 261 264 265 266 272 273 274 275 276 277 288 289 290 291 292 293 296 297 298 320 321 322 323 324 325 328 329 330 336 337 338 339 340 341 512 513 514 515 516 517 520 521 522 528 529 530 531 532 533 544 545 546 547 548 549 552 553 554 576 577 578 579 580 581 584 585 586 592 593 594 595 596 597 640 641 642 643 644 645 648 649 650 656 657 658 659 660 661 672 673 674 675 676 677 680 681 682

CONJECTURE. *There is no* $(6m+1, 2^{6m+1}, 2m+2)$ *extremal Type I additive self-dual code over* $GF(4)$.

ACKNOWLEDGEMENT. The authors wish to thank the referee for valuable remarks which helped us to improve the exposition of this article.

References

[1] E. R. Berlekamp, F. J. MacWilliams, and N. J. A. Sloane, *Gleason's theorem on self-dual codes*, IEEE Trans. Inform. Theory, **IT-18** (1972), 409–414.

[2] A. R. Calderbank, E. M. Rains, P. M. Shor, and N. J. A. Sloane, *Quantum error correction via codes over* $GF(4)$, IEEE Trans. Inform. Theory **44** (1998), no. 4, 1369–1387.

[3] J. H. Conway and N. J. A. Sloane, *A new upper bound on the minimal distance of self -dual codes*, IEEE Trans. Inform. Theory **36** (1990), no. 6, 1319–1333.

[4] ———, *Sphere Packings, Lattices and Groups*, New York: Springer-Verlag, 1988.

[5] W. C. Huffman, *On the classification and enumeration of self-dual codes*, Finite Fields Appl. **11** (2005), no. 3, 451–490.

[6] F. J. MacWilliams and N. J. A. Sloane, *The theory of error correcting codes,* I., II., North-Holland, 1977.

[7] F. J. MacWilliams, N. J. A. Sloane, and J. G. Thompson, *Good self dual codes exist*, Discrete Math. **3** (1972), 153–162.

[8] E. M. Rains, *Shadow bounds for self-dual codes*, IEEE Trans. Inform. Theory **44** (1998), no. 1, 134–139.
[9] E. M. Rains and N. J. A. Sloane, *Self-dual codes*, in: V.S. Pless, W.C. Huffman (Eds.), Handbook of Coding Theory, Elsevier, Amsterdam, 1998.
[10] S. Zhang, *On the nonexistence of extremal self-dual codes*, Discrete Appl. Math. **91** (1999), no. 1-3, 277–286.

Mathematics Section
College of Science
Yonsei University
Seoul 120-749, Korea
E-mail: sunghyu@yonsei.ac.kr
leejb@yonsei.ac.kr