Math. J. Okayama Univ. 37(1995), 1–14

ON EXTREMAL SELF-DUAL CODES

Dedicated to Professor Takeshi Kondo on his 60th birthday

MASAAKI HARADA and HIROSHI KIMURA

1. Introduction. A binary $[n,k]$ linear code C is a k-dimensional vector subspace of $GF(2)^n$, where $GF(2)$ is the field of 2 elements. The elements of C are called codewords and the weight of a codeword is the number of non-zero coordinates. An $[n,k,d]$ code is an $[n,k]$ code with minimum (non-zero) weight d. Two codes are equivalent if one can be obtained from the other by a permutation of coordinates. The dual code $C^{\perp}$ of C is defined as $C^{\perp} = \{x \in GF(2)^n \mid x \cdot y = 0 \text{ for all } y \in C\}$. C is *self-dual* if $C = C^{\perp}$. A code is *doubly-even* if all codewords have weight divisible by four, and *singly-even* if all weights are even and there is at least one codeword of weight $\equiv 2 \pmod 4$. The minimum weight d of a doubly-even self-dual code of length n satisfies $d \leq 4[n/24]+4$. A self-dual code is *extremal* if it has the largest minimum weight for that length. For each length, the largest possible minimum weight is listed in Table I in [4].

Conway and Sloane [4] defined the shadows of self-dual codes. The shadows provide restrictions on the weight enumerators of binary extremal self-dual codes, and were used to determine new upper bounds for the minimum weight of binary self-dual codes. A list of possible weight enumerators for such codes was given in [4]. However, the existence of some extremal self-dual codes is still unknown. Recently several papers have provided constructions for some of these unknown codes (cf., e.g. [1], [2], [3], [5], [6], [8], [13], [14], [15] and the references given therein). In particular, Gulliver and the first author [5] have constructed extremal singly-even $[60,30,12]$ codes with a weight enumerator which was not listed in [4] and have determined the possible weight enumerators for extremal singly-even codes of length 60, correcting the results given in [4].

In this paper, we investigate the existence of new extremal self-dual codes. In order to construct such codes, we present general methods for constructing self-dual codes in Section 2. In Section 3, we construct extremal self-dual codes having weight enumerators for which extremal codes were not previously known to exist, using some matrices. These matrices are given in Section 6. Our methods can be applied to doubly-even codes as well. We give examples of extremal doubly-even self-dual codes in Section 4. In Section 5, we construct a new extremal doubly-even self-dual [88, 44, 16] code by the construction in [11]. Our notation and terminology for coding theory follows that in [12].

2. Constructions of self-dual codes. In this section, we give two constructions of self-dual codes, starting from a self-dual code.

First we give a new construction of self-dual codes. Let A and B be n by n (1, 0)-matrices with $A{\cdot}A^T = I_n$ over $GF(2)$, where I_n is the identity matrix of order n. It is easy to see that the matrix $G = [\,A\,, B\,]$ generates a self-dual code of length $2n$ if and only if $B{\cdot}B^T = I_n$. Let S_n be the symmetric group of degree n and let σ be an element of S_n. Let S_n act on the set of all rows of the matrix B. Let $B^\sigma = [{b_{\sigma^{-1}(1)}}^T, \cdots, {b_{\sigma^{-1}(n)}}^T]^T$ be a matrix obtained from B by a permutation σ where b_i is the i-th row of B.

Proposition 2.1. *Let the notations be as above and assume that* $A{\cdot}A^T = B{\cdot}B^T = I_n$. *Then the following matrix*

$$G^\sigma = [\,A\,,\,B^\sigma\,],$$

generates a self-dual code of length $2n$.

Proof. It is trivial.

Remark 2.2. Any self-dual code of length $2n$ is equivalent to a self-dual code with generator matrix of the form $[\,A\,, X{\cdot}B\,]$, where $X{\cdot}X^T = I_n$. B^σ is nothing but $P{\cdot}B$, where P is the permutation matrix obtained from σ. This construction can easily be applied to self-dual codes over a Galois field $GF(p)$ where p is prime (cf. [9]). For the case $p = 3$, we constructed new extremal ternary self-dual codes using weighing matrices in [9].

If A is the identity matrix I_n, then G and G^σ generate equivalent self-dual codes for any permutation σ. But if A is different from the identity matrix, starting from matrices satisfying the assumptions in Proposition 2.1 one can transform it into $n!$ different generator matrices which may generate inequivalent self-dual codes. Since any generator matrix is transformed into a standard form, we can easily get matrices A and B. Thus we can construct many new self-dual codes from old ones. By this method, we shall construct extremal singly-even codes and extremal doubly-even codes in Sections 3 and 4, respectively.

Now we describe another general method to construct self-dual codes from a self-dual code. Let $[I_n, M]$ be a generator matrix which generates a self-dual code of length $2n$ with n even. Let Γ be a set consisting of 2α columns of the matrix M where $0 < \alpha < n/2$. For every i-th column contained in Γ, we interchange 0 with 1 in the i-th column in M. Then we have a matrix M_Γ from M and Γ. We assume that a new matrix $M_\Gamma{}'$ is obtained from Γ and M_Γ as follows. Let $m_j = (m_{j1}, \cdots, m_{jn})$ be the j-th row of M_Γ. This method is divided into the following two cases. In the first case, for each row m_j $(1 \le j \le n)$, if the number of $k \in \Gamma$ with $m_{jk} = 1$ is odd then interchange 0 with 1 in this row m_j and if the number of $k \in \Gamma$ with $m_{jk} = 1$ is even, then put m_j as the j-th row of $M_\Gamma{}'$. Then we have a new matrix $M_\Gamma{}'$ from the matrix M. In the second case, if the number of $k \in \Gamma$ with $m_{jk} = 1$ is even then interchange 0 with 1 in this row and if the number of $k \in \Gamma$ with $m_{jk} = 1$ is odd, then put m_j as the j-th row of $M_\Gamma{}'$. Then we have a new matrix $M_\Gamma{}'$ from M and Γ.

Theorem 2.3. *We assume that n is an even number. Let M, Γ and $M_\Gamma{}'$ be as above in the both cases. For every set Γ, the following matrix*

$$[I_n, M_\Gamma{}'],$$

generates a self-dual code of length $2n$.

This method was established in [11] and [8] in order to construct extremal self-dual codes.

3. New extremal singly-even codes by Proposition 2.1. The aim of this section is to construct extremal singly-even codes whose weight enumerators were not previously known to exist.

3.1. $[34, 17, 6]$ codes. Any extremal self-dual [34,17,6] code has weight enumerator of the form

$$W = 1 + (34 - 4\beta)y^6 + (255 + 4\beta)y^8 + (1921 + 20\beta)y^{10} + \cdots \quad \text{or} \quad (1)$$
$$W = 1 + 6y^6 + 411y^8 + 1165y^{10} + \cdots, \quad (2)$$

where β is an undetermined parameter. Extremal codes corresponding to $\beta = 0, \ldots, 7$ in (1), and (2) exist (cf. [4]). Since the coefficients of the weight enumerators of any self-dual code and its shadow code must be nonnegative integers, it holds that $0 \le \beta \le 8$ for (1).

Let $M_{34,1}$ and $M_{34,2}$ be the right halves of the generator matrices of the [34, 17, 6] codes $D2$ and $R1$ in [4], respectively. By Proposition 2.1, we have found an extremal [34, 17, 6] code with generator matrix of the form $[\, M_{34,1}\, , M_{34,2}{}^{\sigma}\,]$ where

$$\sigma = (1,2,9,6)(3,4)(5,15,10,17,8,16,13,7)(11,14)(12).$$

Needless to say, $\sigma(1) = 2$, $\sigma(2) = 9$, $\sigma(9) = 6$, $\sigma(6) = 1$ and so on. This code has the weight enumerator (1) with $\beta = 8$. Thus we have the following proposition.

Proposition 3.1. *There exist extremal singly-even self-dual* [34, 17, 6] *codes for all possible extremal weight enumerators.*

3.2. [38, 19, 8] codes. A cyclic 2-(19, 9, 4) design D is listed in Hall [7]. Let M_{38} be the circulant incidence matrix with first row (1001111010100001100) of the design D. We have found an extremal singly-even [38, 19, 8] code C_{38} from M_{38} by Proposition 2.1. The generator matrix of C_{38} is $[\, M_{38}\, , M_{38}{}^{\sigma}\,]$ where

$$\sigma = (1,2,8,9,10,5,17,19,15,4,16,18)(3,12,13,14)(6)(7)(11).$$

Now we consider the weight enumerator of the code C_{38}. There are two possibilities for the weight enumerator of an extremal singly-even [38, 19, 8] code:

$$W = 1 + 171y^8 + 1862y^{10} + 10374y^{12} + 36765y^{14} + \cdots \text{ or} \quad (3)$$

$$W = 1 + 203y^8 + 1702y^{10} + 10598y^{12} + 36925y^{14} + \cdots. \quad (4)$$

The above code C_{38} has the weight enumerator (4). It is mentioned in [4] that the codes with the both weight enumerators (3) and (4) exist. But we checked that both codes $D4$ and $R3$ in [4] have the weight enumerator (3). Thus it seems that the code with the weight enumerator (4) is constructed for the first time.

3.3. [40, 20, 8] codes. Any extremal singly-even [40, 20, 8] code has weight enumerator of the form

$$W = 1 + (125 + 16\beta)y^8 + (1664 - 64\beta)y^{10} + (10720 + 32\beta)y^{12} + \cdots, \quad (5)$$

where β is an undetermined parameter. Extremal singly-even [40, 20, 8] codes corresponding to $\beta = 0$ and 10 were constructed in [4]. Some codes with $\beta = 1$, 2 and 5 were also found in [3] and [8]. By Proposition 2.1, we have constructed three extremal codes corresponding to $\beta = 3$, 4 and 7 from three matrices $M_{40,1}$, $M_{40,2}$ and $M_{40,3}$. These matrices are given in Section 6. For each code, we list in Table 1 the weight enumerator W, the chosen matrices A, B and the permutation σ.

Table 1: New extremal singly-even [40, 20, 8] codes

Codes	W	A	B	the permutation σ
$C_{40,1}$	$\beta = 3$	$M_{40,1}$	$M_{40,2}$	(1, 12, 3, 14, 5, 16, 17, 8, 19, 10) (2, 13, 4, 15, 6, 7, 18, 9, 20, 11)
$C_{40,2}$	$\beta = 4$	$M_{40,2}$	$M_{40,2}$	(1, 16, 11, 6)(2, 17, 12, 7)(3, 18, 13, 8)(4, 19, 14) (5, 20, 15, 10, 9)
$C_{40,3}$	$\beta = 7$	$M_{40,3}$	$M_{40,3}$	(1, 17, 11, 15, 9, 3, 18, 12, 6, 20, 14, 8, 2, 16, 10, 4, 19, 13, 7)(5)

Thus there exist extremal singly-even [40, 20, 8] codes corresponding to $\beta = 0, \dots, 5$, 7 and 10. It follows from Theorem 5 in [4] that $0 \le \beta \le 10$ for (5). Hence it is not known whether there exist extremal codes with $\beta = 6$, 8 and 9.

3.4. [42, 21, 8] codes. Weight enumerators for extremal self-dual [42, 21, 8] codes are given in [4] as

$$W = 1 + (84 + 8\beta)y^8 + (1449 - 24\beta)y^{10} + (10640 - 16\beta)y^{12} + \cdots \quad \text{or} \tag{6}$$

$$W = 1 + 164y^8 + 697y^{10} + 15088y^{12} + \cdots, \tag{7}$$

where β is an undetermined parameter. There are extremal codes corresponding to $\beta = 0, \dots, 7$ and 42 in (6) (cf. [4]). An extremal self-dual code with weight enumerator (7) was found in [13]. Recently the existence of extremal codes corresponding to $\beta = 12$ and 32 in (6) has been announced in [2].

The code $R4$ in [4] is an extremal self-dual [42, 21, 8] code corresponding to $\beta = 0$ in (6). Let M_{42} be the right half of the generator matrix of the code $R4$. Using the matrix M_{42}, we have found new extremal self-dual [42, 21, 8] codes with weight enumerator (6) for $\beta = 8$, 9, 10 and 11. The

Table 2: New extremal singly-even [42, 21, 8] codes

Codes	W	A	B	the permutation σ
$C_{42,1}$	$\beta = 8$	M_{42}	M_{42}	(1, 5, 2, 20, 17, 14, 11, 8, 6, 3, 21, 18, 15, 19, 16, 13, 10, 7, 4)(9)(12)
$C_{42,2}$	$\beta = 9$	M_{42}	M_{42}	(1, 2, 8, 17, 12, 3, 5, 21, 7, 16, 11, 10, 9, 18, 14, 20, 19)(4, 6, 15, 13)
$C_{42,3}$	$\beta = 10$	M_{42}	M_{42}	(1)(2, 20, 17, 14, 11, 8, 6, 3, 21, 18, 15, 12, 19, 16, 13, 10, 7, 4, 5)(9)
$C_{42,4}$	$\beta = 11$	M_{42}	M_{42}	(1, 13, 3, 10, 9, 4, 11, 5, 16, 19, 21, 8, 15, 14, 20, 12, 6, 17)(2, 7, 18)

results are given in Table 2. It was not known to exist codes with these weight enumerators.

3.5. [44, 22, 8] codes. Any extremal singly-even [44, 22, 8] code has weight enumerator of the form

$$W = 1 + (44 + 4\beta)y^8 + (976 - 8\beta)y^{10} + (12289 - 20\beta)y^{12} + \cdots \quad \text{or} \tag{8}$$

$$W = 1 + (44 + 4\beta)y^8 + (1232 - 8\beta)y^{10} + (10241 - 20\beta)y^{12} + \cdots, \tag{9}$$

where β is an undetermined parameter. By Proposition 2.1, we have constructed 27 extremal singly-even [44, 22, 8] codes with weight enumerators which were not previously known to be attainable, using matrices $M_{44,1}$, $M_{44,2}$ and $M_{44,3}$ given in Section 6. The results are listed in Table 3, where the weight enumerator W, the matrices A and B and the permutation σ are given.

For (8), it holds that $10 \le \beta \le 122$. We summarize the existence of extremal codes with these weight enumerators in Table 4. In the table, for each β the case that the code is found in this paper gives the code $C_{44,i}$, the case that the existence of the corresponding codes was known gives the reference and a blank expresses the case that existence of the corresponding codes is still unknown. Similarly we summarize the the existence of [44, 22, 8] codes with weight enumerator (9) in Table 5. We note that $0 \le \beta \le 154$ for (9).

3.6. [54, 27, 10] codes. There are two possibilities for the weight

Table 3: New extremal singly-even [44, 22, 8] codes

Codes	W	A	B	the permutation σ
$C_{44,1}$	$\beta = 21$ (8)	$M_{44,2}$	$M_{44,1}$	(1, 9, 12, 15, 3, 6, 13, 16, 19, 22, 4, 7, 10, 18, 21, 2, 5, 8, 11, 14, 17, 20)
$C_{44,2}$	$\beta = 23$ (8)	$M_{44,2}$	$M_{44,1}$	(1, 15, 6, 4, 19, 10)(2, 17, 8, 21, 12, 3, 16, 7, 20, 11)(5, 18, 9, 22, 13, 14)
$C_{44,3}$	$\beta = 24$ (8)	$M_{44,2}$	$M_{44,1}$	(1, 6, 13, 16, 4, 7, 10, 19, 22, 3, 9, 12, 15, 18, 21, 2, 5, 8, 11, 14, 17, 20)
$C_{44,4}$	$\beta = 25$ (8)	$M_{44,1}$	$M_{44,1}$	(1, 6, 10, 14, 18, 2, 8, 12, 16, 20, 5, 9, 13, 17, 21, 3, 7, 11, 15, 19)(4, 22)
$C_{44,5}$	$\beta = 26$ (8)	$M_{44,2}$	$M_{44,1}$	(1, 7, 11, 15, 19)(2, 6, 10, 14)(3, 18, 22, 5, 9, 13, 17, 21)(4, 8, 12, 16, 20)
$C_{44,6}$	$\beta = 28$ (8)	$M_{44,2}$	$M_{44,1}$	(1, 8, 10, 17, 19, 21)(2, 4, 6, 12, 14, 16, 18, 20, 3, 5, 7, 9, 11, 13, 15, 22)
$C_{44,7}$	$\beta = 29$ (8)	$M_{44,2}$	$M_{44,1}$	(1, 5, 7, 9, 11, 13, 15, 17, 19, 21)(2, 4, 6, 12, 14, 16, 3, 8, 10, 13, 20, 22)
$C_{44,8}$	$\beta = 30$ (8)	$M_{44,2}$	$M_{44,1}$	(1, 7, 11, 15, 19)(2, 6, 10, 14, 18, 22, 4, 8, 17, 21, 3, 12, 16, 5, 9, 13, 20)
$C_{44,9}$	$\beta = 31$ (8)	$M_{44,2}$	$M_{44,1}$	(1, 5, 9, 13, 17, 21, 6, 10, 14, 18, 22, 4, 8, 12)(2, 7, 11, 15, 19, 3, 16, 20)
$C_{44,10}$	$\beta = 33$ (8)	$M_{44,1}$	$M_{44,3}$	(1, 16, 22, 6, 12, 18, 2, 8, 14, 20, 7, 13, 19, 4, 10)(3, 9, 15, 21, 5, 11, 17)
$C_{44,11}$	$\beta = 34$ (8)	$M_{44,1}$	$M_{44,3}$	(1)(2, 21, 18, 15, 19, 16, 13, 12, 9, 6, 3, 22, 20, 17, 14, 11, 8, 5)(4, 10, 7)
$C_{44,12}$	$\beta = 35$ (8)	$M_{44,1}$	$M_{44,3}$	(1, 4, 17, 20)(2, 7, 10, 13, 16, 19)(3, 6, 9, 12, 15, 18, 21, 5, 8, 11, 14, 22)
$C_{44,13}$	$\beta = 36$ (8)	$M_{44,1}$	$M_{44,3}$	(1, 8, 13, 22, 5, 10, 15, 20, 3, 18)(2, 7, 12, 17)(4, 9, 14, 19, 6, 11, 16, 21)
$C_{44,14}$	$\beta = 39$ (8)	$M_{44,1}$	$M_{44,3}$	(1, 4, 16, 19, 2, 7, 10, 13, 22, 3, 6, 9, 12, 15, 18, 21, 5, 8, 11, 14, 17, 20)
$C_{44,15}$	$\beta = 2$ (9)	$M_{44,1}$	$M_{44,3}$	(1, 14, 4, 17, 7, 19, 9, 21, 11)(2, 16, 6, 18, 13, 3, 15, 5, 8, 20, 10, 22, 12)
$C_{44,16}$	$\beta = 16$ (9)	$M_{44,1}$	$M_{44,1}$	(1, 16, 8, 22, 14, 6, 20, 12, 4, 18, 10, 2, 17, 9)(3, 21, 15, 7, 13, 5, 19, 11)
$C_{44,17}$	$\beta = 17$ (9)	$M_{44,1}$	$M_{44,1}$	(1, 7, 12, 17, 22, 5, 10, 15, 20, 3, 21, 6, 11, 16, 4, 9, 14, 19, 2, 8, 13, 18)
$C_{44,18}$	$\beta = 18$ (9)	$M_{44,1}$	$M_{44,1}$	(1, 17, 10, 3, 20, 13, 6, 21, 16, 9, 2, 18, 11, 4, 19, 12, 5, 14, 7, 22, 15, 8)
$C_{44,19}$	$\beta = 21$ (9)	$M_{44,1}$	$M_{44,1}$	(1, 18, 12, 6, 2, 19, 13, 7)(3, 22, 16, 10, 4, 20, 14, 8, 17, 11, 5, 21, 15, 9)
$C_{44,20}$	$\beta = 23$ (9)	$M_{44,1}$	$M_{44,1}$	(1, 6, 10, 14, 18, 4, 22, 5, 9, 13, 17, 21, 3, 7, 11, 15, 9)(2, 8, 12, 16, 20)
$C_{44,21}$	$\beta = 26$ (9)	$M_{44,1}$	$M_{44,1}$	(1, 6, 10, 14, 18, 3, 7, 11, 15, 19)(2, 8, 12, 16, 20)(4, 22)(5, 9, 13, 17, 21)
$C_{44,22}$	$\beta = 27$ (9)	$M_{44,2}$	$M_{44,1}$	(1, 6, 10, 14, 18, 3, 7, 22, 4, 8, 12, 16, 20, 2, 11, 15, 19)(5, 9, 13, 17, 21)
$C_{44,23}$	$\beta = 28$ (9)	$M_{44,2}$	$M_{44,1}$	(1, 8, 13, 18, 3, 22, 5, 10, 15, 20, 6, 11, 16, 21, 4, 9, 14, 19, 2, 7, 12, 17)
$C_{44,24}$	$\beta = 31$ (9)	$M_{44,2}$	$M_{44,1}$	(1, 8, 11, 14, 17, 20, 2, 5, 13, 16, 19, 22, 3, 6, 9, 12, 15, 18, 21, 4, 7, 10)
$C_{44,25}$	$\beta = 32$ (9)	$M_{44,2}$	$M_{44,1}$	(1, 6, 10, 14, 18, 3, 7, 11, 15, 19)(2, 8, 12, 16, 20)(4, 22)(5, 9, 13, 17, 21)
$C_{44,26}$	$\beta = 35$ (9)	$M_{44,1}$	$M_{44,3}$	(1, 21, 17, 13, 9, 5)(2, 20, 16, 12, 19, 15, 11, 8, 4, 22, 18, 14, 10, 6, 7, 3)
$C_{44,27}$	$\beta = 38$ (9)	$M_{44,1}$	$M_{44,3}$	(1)(2, 21, 18, 15, 12, 11, 8, 5)(3, 22, 20, 17, 14, 19, 16, 13, 10, 7, 4, 9, 6)

Table 4: Existence of extremal [44, 22, 8] codes with (8)

β	code	β	code	β	code	β	code	β	code	β	code	β	code
10	[1]	20	[8]	30	$C_{44,8}$	40		50		60		70	
11	[8]	21	$C_{44,1}$	31	$C_{44,9}$	41		51		61		:	
12	[8]	22	[2]	32	[2]	42	[2]	52	[2]	62	[2]	:	
13	[8]	23	$C_{44,2}$	33	$C_{44,10}$	43		53		63		81	
14	[4]	24	$C_{44,3}$	34	$C_{44,11}$	44		54		64		82	[2]
15	[8]	25	$C_{44,4}$	35	$C_{44,12}$	45		55		65		83	
16	[8]	26	$C_{44,5}$	36	$C_{44,13}$	46		56		66		:	
17	[4]	27	[2]	37	[2]	47		57		67		:	
18	[8]	28	$C_{44,6}$	38	[6]	48		58		68		121	
19	[8]	29	$C_{44,7}$	39	$C_{44,14}$	49		59		69		122	[2]

Table 5: Existence of extremal [44, 22, 8] codes with (9)

β	code	β	code	β	code	β	code	β	code	β	code	β	code
0	[10]	10	[4]	20	[2]	30	[2]	40		50		91	
1		11	[4]	21	$C_{44,19}$	31	$C_{44,24}$	41		:		:	
2	$C_{44,15}$	12	[4]	22	[10]	32	$C_{44,25}$	42		:		:	
3	[8]	13	[4]	23	$C_{44,20}$	33		43		73		103	
4	[4]	14	[4]	24	[2]	34	[2]	44	[10]	74	[2]	104	[2]
5	[4]	15	[4]	25	[2]	35	$C_{44,26}$	45		75		105	
6	[4]	16	$C_{44,16}$	26	$C_{44,21}$	36		46		:		:	
7	[4]	17	$C_{44,17}$	27	$C_{44,22}$	37		47		:		:	
8	[4]	18	$C_{44,18}$	28	$C_{44,23}$	38	$C_{44,27}$	48		89		153	
9	[4]	19	[2]	29	[2]	39		49		90	[2]	154	[15]

enumerator of an extremal singly-even [54, 27, 10] code:

$$W = 1 + (351 - 8\beta)y^{10} + (5031 + 24\beta)y^{12} + (48492 + 32\beta)y^{14} + \cdots \quad \text{or} \tag{10}$$

$$W = 1 + (351 - 8\beta)y^{10} + (5543 + 24\beta)y^{12} + (43884 + 32\beta)y^{14} + \cdots, \tag{11}$$

where β is an undetermined parameter. An extremal singly-even [54, 27, 10] code corresponding to $\beta = 0$ in (10) was constructed in [4]. A singly-even code with weight enumerator (11) is known to exist for $\beta = 12$ (cf. [14]).

By Proposition 2.1, we have constructed extremal codes corresponding to $\beta = 1, 2, 3, 4$ and 5 in (10) from $M_{54,1}$, $M_{54,2}$, $M_{54,3}$, $M_{54,4}$, $M_{54,5}$, $M_{54,6}$, $M_{54,7}$ and $M_{54,8}$ given in Section 6. For each code, we list in Table 6 the weight enumerator W, the chosen matrices A, B and the permutation σ. It was not known to exist codes with weight enumerator (10) for $\beta = 1$, 2, 3, 4 and 5.

Table 6: New extremal singly-even [54, 27, 10] codes

Codes	W	A	B	the permutation σ
$C_{54,1}$	$\beta = 1$ (10)	$M_{54,1}$	$M_{54,2}$	$(1)(2)(3)\cdots\cdots(25)(26)(27)$
$C_{54,2}$	$\beta = 2$ (10)	$M_{54,3}$	$M_{54,4}$	$(1)(2)(3)\cdots\cdots(25)(26)(27)$
$C_{54,3}$	$\beta = 3$ (10)	$M_{54,5}$	$M_{54,5}$	$(1,12,23,7,18,2,21,5,16,27,11,22,6,17)$ $(3,14,25,9,20,4,15,26,10,13,24,8,19)$
$C_{54,4}$	$\beta = 4$ (10)	$M_{54,6}$	$M_{54,7}$	$(1)(2)(3)\cdots\cdots(25)(26)(27)$
$C_{54,5}$	$\beta = 5$ (10)	$M_{54,8}$	$M_{54,4}$	$(1,8,10,18,17,16,3,13,2,21,4,14,27,7,$ $12,11,25,19,22,5,24,9,15,26,6,20,23)$

3.7. [58, 29, 10] codes. Any extremal singly-even [58, 29, 10] code has weight enumerator of the form

$$W = 1 + (165 - 2\gamma)y^{10} + (5078 + 2\gamma)y^{12} + \cdots \quad \text{or} \qquad (12)$$

$$W = 1 + (319 - 24\beta - 2\gamma)y^{10} + (3132 + 152\beta + 2\gamma)y^{12} + \cdots, \qquad (13)$$

where β is an undetermined parameter. Two extremal singly-even [58, 29, 10] codes corresponding to $\beta = \gamma = 0$ and $\beta = 0$, $\gamma = 58$ in (13) were constructed in [4]. A singly-even code with $\gamma = 55$ in (12) was also found in [13].

New extremal self-dual codes with weight enumerator (13) and $\beta = 0$ are constructed using matrices $M_{58,1}$ and $M_{58,2}$ by Proposition 2.1. The results are listed in Table 7. Since the values of β in the weight enumerator (13) of all our codes in the table are 0, we list only the value of γ with A, B and σ in the table.

3.8. Other lengths. We have constructed extremal singly-even self-dual codes of lengths 36, 38, 46 and 48 by Proposition 2.1. For such lengths, however, the existence of extremal self-dual codes is known for all possible extremal weight enumerators. Therefore we do not present extremal codes for such lengths.

4. Extremal doubly-even codes by Proposition 2.1. In this section, we give examples of extremal doubly-even self-dual codes constructed by Proposition 2.1.

Table 7: New extremal singly-even [58, 29, 10] codes

Codes	W	A	B	the permutation σ
$C_{58,1}$	$\gamma = 52$	$M_{58,1}$	$M_{58,1}$	(1, 25, 18, 23, 16, 9, 11, 4, 2, 24, 17, 10, 3, 26, 19, 12, 5, 27, 20, 13, 6, 28, 21, 14, 7, 29, 22, 15, 8)
$C_{58,2}$	$\gamma = 60$	$M_{58,2}$	$M_{58,1}$	(1, 13, 24, 6, 21, 3, 17, 28, 10, 12, 23, 5, 16, 27, 9, 20, 2, 14, 25, 7, 18, 29, 11, 22, 4, 15, 26, 8, 19)
$C_{58,3}$	$\gamma = 62$	$M_{58,2}$	$M_{58,1}$	(1, 10, 18, 26, 5, 13, 21, 29, 8, 16, 24, 3, 17, 25, 4, 12, 20, 28, 7, 15, 23, 2, 11, 9, 19, 27, 6, 14, 22)
$C_{58,4}$	$\gamma = 64$	$M_{58,2}$	$M_{58,1}$	(1, 25, 19, 13, 7)(2, 26, 20, 14, 8)(3, 28, 22, 16, 10, 4, 27, 21, 15, 9)(5, 6, 29, 23, 17, 11)(12, 24, 18)
$C_{58,5}$	$\gamma = 66$	$M_{58,1}$	$M_{58,1}$	(1, 5, 8, 11, 14, 17, 20, 23, 26, 29, 3, 7, 10, 13, 4, 16, 19, 22, 25, 28, 2, 6, 9, 12, 15, 18, 21, 24, 27)
$C_{58,6}$	$\gamma = 68$	$M_{58,2}$	$M_{58,1}$	(1, 13, 24, 6, 17, 28, 10, 21, 3, 16, 27, 9, 20, 2, 14, 25, 7, 18, 29, 11, 12, 23, 5, 22, 4, 15, 26, 8, 19)
$C_{58,7}$	$\gamma = 70$	$M_{58,1}$	$M_{58,1}$	(1, 21, 11)(2, 26, 16, 6, 25, 15, 10, 29, 19, 9, 28, 18, 8, 27, 17, 7, 5, 24, 14, 4, 23, 13, 3, 22, 12)(20)
$C_{58,8}$	$\gamma = 72$	$M_{58,2}$	$M_{58,1}$	(1, 11, 25, 5, 14, 23, 3, 20, 29, 9, 18, 27, 7, 16, 10, 19, 28, 8, 17, 26, 6, 15, 24, 4, 13, 22, 2, 12, 21)
$C_{58,9}$	$\gamma = 74$	$M_{58,1}$	$M_{58,1}$	(1, 20, 9, 4, 22, 11, 29, 18, 7, 25, 14, 3, 21, 10, 28, 17, 6, 27, 16, 5, 23, 12)(2, 24, 13)(8, 26, 15, 19)
$C_{58,10}$	$\gamma = 76$	$M_{58,1}$	$M_{58,1}$	(1, 18, 5, 27, 14)(2, 20, 7, 23, 10, 26, 13, 29, 16, 3, 19, 6, 22, 9, 25, 12, 28, 15)(4, 21, 8, 24, 11, 17)
$C_{58,11}$	$\gamma = 78$	$M_{58,1}$	$M_{58,1}$	(1, 5, 8, 11, 4, 14, 17, 20, 23, 26, 29, 3, 7, 10, 13, 16, 19, 22, 25, 28, 2, 6, 9, 12, 15, 18, 21, 24, 27)
$C_{58,12}$	$\gamma = 80$	$M_{58,2}$	$M_{58,1}$	(1, 26, 21, 16, 11, 6)(2, 27, 22, 17, 12, 7)(3, 29, 24, 19, 14, 9, 4, 28, 23, 18, 13, 8)(5, 15, 10)(20, 25)
$C_{58,13}$	$\gamma = 82$	$M_{58,1}$	$M_{58,1}$	(1, 26, 20, 14, 8, 2, 25, 19, 13, 24, 18, 12, 6, 29, 23, 17, 11, 5, 4, 27, 21, 15, 9, 3, 28, 22, 16, 10, 7)
$C_{58,14}$	$\gamma = 84$	$M_{58,1}$	$M_{58,1}$	(1, 25, 19, 13, 7)(2, 28, 22, 16, 10, 4, 27, 21, 15, 24, 18, 12, 6, 29, 23, 17, 11, 5, 8)(3, 26, 20, 14, 9)

Let A_{40} and B_{40} be the right halves of the generator matrices of the codes $D5$ and $D6$ in [4], respectively. We have found an extremal doubly-even [40, 20, 8] code with generator matrix of the form $[\,A_{40}\,, {B_{40}}^{\sigma}\,]$ where

$$\sigma = (1, 3, 5, 2, 4, 6, 7, 8, \ldots, 18, 19, 20).$$

In [8] at least 1000 inequivalent extremal doubly-even codes of length 40 were constructed by Theorem 2.3. Thus we do not check the equivalence of our code and the codes in [8]. Similarly we have found an extremal doubly-even [64, 32, 12] code constructed by Proposition 2.1. Let A_{64} and B_{64} be the right halves of the generator matrices of the code No. 1 in [11] and the code $D15$ in [4], respectively. We put

$$\sigma = (1,10,18,26,2,11,19,27,3,12,20,28,4,16,24,32,8,9,17,25)$$
$$(5,13,21,29)(6,14,22,30)(7,15,23,31).$$

By Proposition 2.1, the matrix $[\,A_{64}\,, B_{64}{}^{\sigma}\,]$ generates an extremal doubly-even $[64,32,12]$ code. It was shown in [11] that there are at least 3270 inequivalent extremal doubly-even codes of length 64.

5. A new extremal doubly-even code by Theorem 2.3. In this section, we construct a new extremal doubly-even $[88,44,16]$ code by Theorem 2.3.

Let C_{88} be a code with generator matrix of the form

$$\left[\begin{array}{c|c} & \begin{array}{cccc} 0 & 1 & \cdots & 1 \end{array} \\ I & \begin{array}{c} 1 \\ \vdots \\ 1 \end{array} \quad R \end{array}\right],$$

where R is a circulant matrix with first row

$$(0110010100\ 1110111110\ 0010111000\ 0010001101\ 011).$$

This code C_{88} is given in Fig. 16.7 of [12] and an extremal doubly-even code of length 88. Only one extremal doubly-even code is known of length 88. Some codes in Fig. 16.7 of [12] are extremal double circulant self-dual codes. Recently all extremal double circulant self-dual codes of length up to 62 have been classified in [10].

Let $C_{88}{}'$ be a self-dual code of length 88 constructed from C_{88} by Theorem 2.3 with $\Gamma = \{2,3,9,19\}$. This code $C_{88}{}'$ is an extremal doubly-even self-dual code. In order to check the inequivalence of C_{88} and $C_{88}{}'$, we compared the maximal and minimal numbers $M(2)$ and $m(2)$ (see [9] or [10] for definition) in the set of the minimum weight codewords. For the codes C_{88} and $C_{88}{}'$, the values $(M(2), m(2))$ are $(1081, 301)$ and $(1126, 541)$, respectively. Thus the codes C_{88} and $C_{88}{}'$ are inequivalent.

6. Matrices. In this section, we display the matrices which were used in Section 3 to construct extremal singly-even codes. In order to save space, these matrices have been written in octal using $0 = (000)$, $1 = (001)$, $\ldots$, $6 = (110)$ and $7 = (111)$, together with $a = (0)$ and $b = (1)$.

$M_{40,1}$ 37777777774003740760746143570306675410376462347453255312564561 3
45554257446607623526465324656524744715147315171125635450746271 7
1132556a

$M_{40,2}$ 377777777740037407607461435652066745213366070735225437131263615
515540776426235435434553261527251552651534631662256326332456237
1075342b

$M_{40,3}$ 042162556306510734533401520173127074453536025660725040342421614
567106673434542171536702653341724560725707432703615351706211034
5040162a

$M_{44,1}$ 277322532105327131051255366556441624451454505212312052471526560
144226074653322061262241465675031524320432166404660550063224576
35526403275226074324641366517742000b

$M_{44,2}$ 263022505066451101651254756555357553252434502426465454531531111
633545403124241717252441464245032232057346671373054227712413201
72451375132552015724735471260176777a

$M_{44,3}$ 500755272111326646126555356555337553251434505211312052531531211
633551403124441717262441412132746252057345671373114227714413216
35326474532551702053136471267741000b

$M_{54,1}$ 541430656224127532222035237012061074247655770226173051573517254
473656564647030427536004627001043646605505711647203262116225133
046641204123663424135114004631225072174401003133216152044314260
05103502125332710254326666701240272402735643007133777 0

$M_{54,2}$ 072214012426114404537002343326523373751025071374375461623704017
524750115222120225476241311363465157774121203547616014701661630
111520450407541010331141020404426610427050571216244237316407603
23157250217747423642734727304642366502207533321410212 3

$M_{54,3}$ 207566122107633411407355244720656212710363141740535424072665221
071336114074553442122207566411107633244407355212720656141710363
424740535221072665114071336442074553566122207633411107355244407
65621272036314171053542474066522107233611407155344207 4

$M_{54,4}$ 142653611777740000750434644364216322642163226043664562421732270
230542743172127150217222714721071512514261361264621057323044275
646110571132330427075053464436405632210755134504346456055174213
42647610555140213746130570510751134661321704330552742 1

$M_{54,5}$ 4777700006061343236034525155266054251007777005320315523252360 51
3161530646052616466660515254277007700650323431564062334343465032
5455031430233413710155245745510546616306461625133062163613105 26
33454061335262034505425511706216644703143322704661 2672

$M_{54,6}$ 4260157262130467131450237453125016745416043726243025711611504 37
4344602572522301670467464460237232230157151153046746215023723 14
6015715421302374524501572612604671347234160457152430267461250 13
67132460437451230257264150145743243026725125013716 4160

$M_{54,7}$ 1710474524744236242362117121171247440653344234236251702117124 74
1047452364423625166211712467104745226530042373254221171526310 47
0474523620325762114152571056065074433032636215415117112606447 45
53030236325416117152605047577774000074423625036211 7124

$M_{54,8}$ 4777700002770077001007777006061343236034525155266054256605152 54
5455031435510546616306461626503234315640623345320315523252360 51
6052616465133062163161530643434650323613105263345406133526203 45
05425511706216644703143322704661267202334137101552 4574

$M_{58,1}$ 0164073606060350167603570301641407203574140720355016741407703 01
6407301640736070164073601674140720167414072167414072074140720 35
2035703015640736060301640736030164073600736060350603501674741 40
2035703015640736060301640736030164073600736060350603501674741 40
7203674140720364073606036407360603360603501736060350035016741 40
35016741403501674140736060 35a

$M_{58,2}$ 1551653317316332352731633235233163323531633235265266346647526 63
4664733163323507155165337155165331471551653332352663426634664 73
2663466473526634664352663466463466472556332352666533163322352 66
2663466473526634664352663466463466472556332352666533163322352 66
3466635266346623526634672352663465551653316466472554746647255 47
23526634632352663473235266 34b

References

[1] R. A. Brualdi and V. S. Pless: Weight enumerators of self-dual codes, IEEE Trans. Inform. Theory **37** (1991), 1222–1225.

[2] S. Buyuklieva: Existence of certain extremal self-dual codes of lengths 42 and 44, Proc. Optimal Codes and Related Topics, Bulgaria, 1995, 29–31.

[3] S. Buyuklieva and V. Yorgov: Singly-even self-dual codes of length 40, Preprint.

[4] 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), 1319–1333.
[5] T. A. GULLIVER and M. HARADA: Weight enumerators of extremal singly-even [60, 30, 12] codes, IEEE Trans. Inform. Theory **42** (1996), 658–659.
[6] T. A. GULLIVER and M. HARADA: Weight enumerators of double circulant codes and new extremal self-dual codes, Des. Codes and Cryptogr., to appear.
[7] M. HALL, Jr.: Combinatorial Theory, 2nd ed., Wiley, New York, 1986.
[8] M. HARADA: Existence of new extremal doubly-even codes and extremal singly-even codes, Des. Codes and Cryptogr., to appear.
[9] M. HARADA: Extremal ternary self-dual codes and weighing matrices, Submitted for publication.
[10] M. HARADA, T. A. GULLIVER and H. KANETA: Classification of extremal double circulant self-dual codes of length up to 62, Submitted for publication.
[11] M. HARADA and H. KIMURA: New extremal doubly-even [64, 32, 12] codes, Des. Codes and Cryptogr. **6** (1995), 91–96.
[12] F. J. MACWILLIAMS and N. J. A. SLOANE: The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1977.
[13] H.-P. TSAI: Existence of certain extremal self-dual codes, IEEE Trans. Inform. Theory **38** (1992), 501–504.
[14] H.-P. TSAI: Existence of some extremal self-dual codes, IEEE Trans. Inform. Theory **38** (1992), 1829–1833.
[15] V. YORGOV and R. RUSEVA: Two extremal codes of length 42 and 44, Probl. Pereda. Inform. **29** (1993), 99–103 (in Russian). English translation in: Problems Inform. Transmission **29** (1994), 385–388.

MASAAKI HARADA
DEPARTMENT OF MATHEMATICS, OKAYAMA UNIVERSITY
OKAYAMA 700, JAPAN

HIROSHI KIMURA
DEPARTMENT OF MATHEMATICS, EHIME UNIVERSITY
MATSUYAMA 790-77, JAPAN

(*Received September 19, 1995*)