of ϵ corresponding to $s = s_1$. It is straightforward to check, using (32), that $P_{\mathrm{u\,d}}(\mathcal{C}^4, \epsilon) \leq (2^4 - 1)/2^8$ for this ϵ. Therefore, $\mathcal{C}^4$ is good. Substituting $s = 0.6$ in (34) shows that $\mathcal{C}^4$ is improper. □

We complete the proof of Theorem 1. First, notice from Lemma 18 that for any $(n, M)_q$ code $\mathcal{C}$, $\mathcal{C}^4$ is bad if $n = M = q = 2$ is not true, and $\mathcal{C}^5$ is bad if $n = M = q = 2$. It is easy to check that if $\mathcal{C}$ is a $(2, 2)_2$ code of distance one, then $\mathcal{C}^2$ is bad, and therefore, by Proposition 1, $\mathcal{C}^m$ is bad and improper for $m \geq 2$. On the other hand, Lemma 19 shows that if $\mathcal{C}$ is a $(2, 2)_2$ code of distance two, then $\mathcal{C}^3$ is proper and $\mathcal{C}^4$ is good but improper. Such codes are the only codes that are good if used four times. This confirms the results of Theorem 1 in case $q = 2$.

Next, we assume that $q \geq 3$. If $M = q^k$, where k is an integer such that $1 \leq k \leq n - 1$, then Lemma 11 implies that for any $m > m'_g(q)$, as specified in Theorem 1, the tuple (n, M, q, m) is bad. In particular, for such m, $\mathcal{C}^m$ is bad, and therefore improper, for any $(n, M)_q$ code $\mathcal{C}$. On the other hand, Lemma 19 indicates that for the $(2, q)_q$ linear repetition code $\mathcal{C}$, the code $\mathcal{C}^m$ is proper if $3 \leq q \leq 5$ and $m = 2$, or if $q \geq 6$ and $m = 1$. From this, we conclude that indeed the values of $m'_g(q)$ and $m'_p(q)$ given in Theorem 1 are correct. More generally, if $2 \leq M \leq q^n - 1$, then Lemma 18 implies that for any $m > 2$, the tuple (n, M, q, m) is bad. In particular, for such m, $\mathcal{C}^m$ is bad, and therefore improper, for any $(n, M)_q$ code $\mathcal{C}$. However, Lemma 19 shows that, for $q \geq 3$, there is a q-ary code, $\mathcal{C}$, for which $\mathcal{C}^2$ is proper and good. We conclude that the values of $m_g(q)$ and $m_p(q)$ in Theorem 1 are correct.

REFERENCES

[1] K. A. S. Abdel-Ghaffar, "A lower bound on the undetected error probability and strictly optimal codes," *IEEE Trans. Inform. Theory*, vol. 43, pp. 1489–1502, Sept. 1997.

[2] A. Ashikhmin and A. Barg, "Binomial moments of the distance distribution: Bounds and applications," *IEEE Trans. Inform. Theory*, vol. 45, pp. 438–452, Mar. 1999.

[3] T. Kløve and V. I. Korzhik, *Error Detecting Codes*. Norwell, MA: Kluwer, 1995.

[4] W. W. Peterson and E. J. Weldon, Jr., *Error-Correcting Codes*. Cambridge, MA: MIT Press, 1972.

New Extremal Self-Dual Codes of Length 62 and Related Extremal Self-Dual Codes

Radinka Dontcheva and Masaaki Harada

***Abstract*—In this correspondence, new extremal self-dual codes of length 62 are constructed with weight enumerators of three different types. Two of these types were not represented by any known code up till now. All these codes possess an automorphism of order 15. Some of them are used to construct extremal self-dual codes of length 60 by the method of subtracting. By additional subtracting, an extremal self-dual [58, 29, 10] code was obtained having a weight enumerator which does not correspond to any code known so far.**

***Index Terms*—Automorphism, extremal self-dual code, weight enumerator.**

Manuscript received November 20, 2001; revised January 12, 2002. This work was supported in part by Shumen University under Grant N5/08.05.2001.

R. Dontcheva is with the Faculty of Information Technology and Systems, Delft University of Technology, 2628 CD Delft, The Netherlands, on leave from the University of Shumen, Bulgaria.

M. Harada is with the Department of Mathematical Sciences, Yamagata University, Yamagata 990-8560, Japan.

Communicated by P. Solé, Associate Editor for Coding Theory.

Publisher Item Identifier S 0018-9448(02)05334-8.

I. INTRODUCTION

A binary $[n, k]$ code C is a k-dimensional vector subspace of $\mathbb{F}_2^n$, where $\mathbb{F}_2$ is the field of two elements. The weight of a vector is the number of its nonzero coordinates. An $[n, k, d]$ code is an $[n, k]$ code with minimum weight d. A code C is *self-dual* if $C = C^{\perp}$, where $C^{\perp}$ is the dual code of C under the standard inner product. A self-dual code C is *doubly-even* if all codewords of C have a weight divisible by four, and *singly-even* if there is at least one codeword of weight $\equiv 2 \pmod 4$. Let C be a singly-even self-dual code and let C_0 be its doubly-even subcode. Then $C_0^{\perp} = C_0 \cup C_1 \cup C_2 \cup C_3$ where C_i are cosets of C_0 and $C = C_0 \cup C_2$. The code $S = C_1 \cup C_3$ is called the shadow code of C. Shadow codes were introduced by Conway and Sloane [3]. An *automorphism* of C is a permutation of the coordinates of the codewords of C which preserves C. The set consisting of all automorphisms of C is called the *automorphism group* of C.

A self-dual code is called *extremal* if it has the largest minimum weight for that length. For doubly-even self-dual codes of length n it is known that n is a multiple of 8 and the minimum weight d is bounded by $d \leq 4[n/24] + 4$ [10]. For singly-even self-dual codes, Conway and Sloane [3] provided new upper bounds for the minimum weight, and gave a list of the possible weight enumerators of singly-even self-dual codes meeting the bounds for lengths up to 64 and for length 72. For example, the largest minimum weights for length 58, 60, and 62 are 10, 12, and 12, respectively. An obvious problem is to determine if a self-dual code exists for a given possible weight enumerator. In this correspondence, extremal self-dual codes of lengths 58, 60, and 62 are constructed.

In Section II, we construct new extremal self-dual codes of length 62 with an automorphism of order 15, using the results derived in [8]. Some of them have a weight enumerator for which codes were not known to exist. In Section III, new extremal self-dual $[60, 30, 12]$ codes are constructed by applying subtracting to extremal self-dual codes of length 62. By one more subtraction we also construct an extremal self-dual $[58, 29, 10]$ code with a weight enumerator which was not known to be attainable before.

II. NEW EXTREMAL SELF-DUAL CODES OF LENGTH 62

The possible weight enumerators $W_{62,i}$ and $S_{62,i}$, $i = 1, 2$, of extremal self-dual codes of length 62 and their shadow codes are as follows:

$$W_{62,1} = 1 + (1860 + 32\beta)y^{12} + (28055 - 160\beta)y^{14} + (255533 + 96\beta)y^{16} + \cdots \quad (1)$$

$$S_{62,1} = \beta y^7 + (1116 - 12\beta)y^{11} + (171368 + 66\beta)y^{15} + \cdots \quad (2)$$

$$W_{62,2} = 1 + 2308y^{12} + 23767y^{14} + 279405y^{16} + \cdots \quad (3)$$

$$S_{62,2} = y^3 + 1039y^{11} + 171928y^{15} + \cdots \quad (4)$$

where β is an undetermined parameter with $0 \leq \beta \leq 93$. Only one extremal singly-even self-dual code with weight enumerator $W_{62,1}$ and $\beta = 10$ is known [6]. Unfortunately, the coefficient of y^{14} in $W_{62,1}$ of (1) was reported incorrectly in both [3, p. 1326] and [6, p. 1232]. Using the method from [3], we obtain the correct weight enumerator $W_{62,1}$.

0018-9448/02$17.00 © 2002 IEEE

TABLE I
EXTREMAL SELF-DUAL CODES OF LENGTH 62

Codes	β	$M_{12}(3)$	$m_{12}(3)$	$M_{12}(2)$	$m_{12}(2)$	$M_{12}(1)$	$m_{12}(1)$	$\lvert\mathrm{Aut}\rvert$
$C_{62,1}$	0	20	2	82	30	360	360	15
$C_{62,2}$	0	20	3	84	52	360	360	15
$C_{62,3}$	0	21	4	88	30	360	360	15
$C_{62,4}$	0	21	3	90	46	360	360	15
$C_{62,5}$	0	24	0	84	28	360	360	30
$C_{62,6}$	0	21	0	96	0	360	360	30
$C_{62,7}$	0	24	0	84	0	360	360	15
$C_{62,8}$	0	21	0	86	0	360	360	30
$C_{62,9}$	0	20	2	86	30	360	360	15
$C_{62,10}$	15	25	3	112	52	480	416	15
$C_{62,11}$	10	24	0	96	0	424	360	15
$C_{62,12}$	10	24	0	100	0	424	360	30
$C_{62,13}$	10	24	0	102	0	424	360	30
$C_{62,14}$	10	25	0	104	0	424	360	15
$C_{62,15}$	10	24	0	104	0	424	360	15
$C_{62,16}$	10	24	0	106	0	424	360	15
$C_{62,17}$	10	25	0	106	0	424	360	15
$C_{62,18}$	10	23	0	108	0	424	360	30
$C_{62,19}$	10	25	0	112	0	424	360	30
$C_{62,20}$	10	25	0	114	0	424	360	30

In this section, we construct extremal self-dual codes of length 62 by making use of the method developed in [8] under the assumption that they possess an automorphism of order 15. It will appear that such codes have weight enumerators $W_{62,1}$ with $\beta = 0, 10$, and 15, as defined in (1). From [14, Theorem 1] it follows that an extremal self-dual code of length 62 cannot have an automorphism of odd prime order greater than 5. Since the investigation of the existence of codes having automorphisms of order 3 and 5 appears to require a lot of calculations, we restrict ourselves in this correspondence to automorphisms of order 15.

Let C be an extremal self-dual code of length 62 with the following automorphism of order 15:

$$\sigma = (1, \ldots, 15)(16, \ldots, 30)(31, \ldots, 45)(46, \ldots, 60)(61)(62). \tag{5}$$

We denote the four cycles of length 15 by Ω_1, Ω_2, Ω_3, Ω_4 and the two fixed points by Ω_5 and Ω_6. Let

$$F_\sigma(C) = \{x \in C \mid \sigma(x) = x\}$$

and

$$E_\sigma(C) = \{x \in C \mid \mathrm{wt}(x|\Omega_i) \equiv 0 (\mathrm{mod} 2), \text{ for } i = 1, 2, 3, 4 \text{ and } x|\Omega_i = 0 \text{ for } i = 5, 6\}$$

where $x|\Omega_i$ is the restriction of x on Ω_i and $\mathrm{wt}(x)$ denotes the weight of x. Consider the map ϕ: $F_\sigma(C) \to \mathbb{F}_2^6$ defined by $\phi(x|\Omega_i) = x_j$ for some $j \in \Omega_i$, $i = 1, 2, 3, 4$. Note that $x|\Omega_i$ is either the all-one vector $\mathbf{1}$ or the zero vector $\mathbf{0}$ of length 15 for any $x \in F_\sigma(C)$. The next proposition follows from [8, Theorems 1–3].

Proposition 1: Let C be a self-dual code of length 62 with automorphism σ as defined in (5). Then

1) $C = F_\sigma(C) \oplus E_\sigma(C)$.
2) $F_\sigma(C)$ and $E_\sigma(C)$ are σ-invariant, that is, invariant under the action of σ.
3) The subcodes $F_\sigma(C)$ and $E_\sigma(C)$ have dimensions 3 and 28, respectively.
4) $\phi(F_\sigma(C))$ is a self-dual code of length 6.

It is well known that there is a unique self-dual code of length 6 up to equivalence. Thus, without loss of generality, we may assume that $F_\sigma(C)$ has a generator matrix of the form

$$X = \left(\begin{array}{cccc|cc} \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{0} & 0 & 0 \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} & 1 & 0 \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & 0 & 1 \end{array}\right) \tag{6}$$

since C has minimum weight 12.

Let $E_\sigma(C)^*$ be the code obtained from $E_\sigma(C)$ by deleting the last two coordinates. Denote by P the set of the even-weight polynomials in $\mathbb{F}_2[x]/(x^{15} - 1)$. So, it is clear that P is a cyclic code of length 15 generated by $x - 1$. Also P is a ring with identity element

$$e(x) = x + x^2 + x^3 + \cdots + x^{14}.$$

We have

$$x^{15} - 1 = (x - 1)h_1(x)h_2(x)h_3(x)h_4(x)$$

where

$$h_1(x) = 1 + x + x^2 + x^3 + x^4$$
$$h_2(x) = 1 + x^3 + x^4$$
$$h_3(x) = 1 + x + x^4$$

and

$$h_4(x) = 1 + x + x^2$$

are irreducible polynomials in P. Let I_j be the ideal of P generated by the polynomial $\frac{x^{15}-1}{h_j(x)}$. It is well known that I_j is a cyclic code, which is isomorphic to the field $\mathbb{F}_2^4$ for $j = 1, 2, 3$ and to the field $\mathbb{F}_2^2$ for $j = 4$, and that P is the direct sum $P = I_1 \oplus I_2 \oplus I_3 \oplus I_4$.

Since the code C has an automorphism σ containing four cycles of length 15, a generator matrix of $E_\sigma(C)^*$ consists of elements of I_1, I_2, I_3, and I_4. Hence, one possibility for a generator matrix of the subcode $E_\sigma(C)^*$ is

$$Y = \begin{pmatrix} r_1 & r_2 & r_3 & r_4 \\ r_5 & r_6 & r_7 & r_8 \\ s_1 & s_2 & s_3 & s_4 \\ s_5 & s_6 & s_7 & s_8 \\ u_1 & u_2 & u_3 & u_4 \\ u_5 & u_6 & u_7 & u_8 \\ v_1 & v_2 & v_3 & v_4 \\ v_5 & v_6 & v_7 & v_8 \end{pmatrix} \tag{7}$$

where all the r_i, s_j, u_t are 4×15 matrices and all the v_k are 2×15 matrices ($1 \le i, j, t, k \le 8$). The first rows of the circulant matrices r_i, s_j, u_t, and v_k are elements of I_1, I_2, I_3, and I_4, respectively. Therefore, we have the following characterization about the form of some generator matrices.

Proposition 2: Let X and Y be matrices of the form (6) and (7), respectively. Then the 31×62 matrix

$$G = \left(\begin{array}{c|c} X & \\ \hline Y & \begin{matrix} 00 \\ \vdots \\ 00 \end{matrix} \end{array}\right)$$

is a possible generator matrix of a self-dual code of length 62 with automorphism σ.

Using matrices of the form in Proposition 2 we found extremal self-dual codes of length 62. We present 20 examples $C_{62,1}$, $C_{62,2}$, $\ldots$, $C_{62,20}$ of such codes. The codes $C_{62,i}$, $i = 1, \ldots, 20$, have weight enumerators of type $W_{62,1}$ with $\beta = 0$, 10, or 15. This was established by calculating the number of codewords of minimum weight. We list the values β in Table I. The orders of the automorphism groups $|\mathrm{Aut}|$ were calculated by MAGMA, and are also listed in Table I.

Proposition 3: There are extremal self-dual $[62, 31, 12]$ codes with weight enumerator $W_{62,1}$ for $\beta = 0, 15$.

Remark: By this method we found more extremal self-dual codes with weight enumerator $W_{62,1}$ and $\beta = 0, 10$. However, an extensive computer search failed to discover an extremal self-dual code with $W_{62,2}$ or $W_{62,1}$ for other values of β.

We now present generator matrices of the codes $C_{62,i}$, $i = 1, \ldots, 20$. It is sufficient to give the submatrices Y of G (see Proposition 2). Denote the submatrices by Y_i for $C_{62,i}$. The 20 circulant matrices in Y_i are listed in Table II, where o is the zero matrix and the first rows of the circulant matrices e_i, α_j, β_s, γ_r, and δ_t are given in Table III.

To show that all presented codes are inequivalent, we use the following invariant. Let C be a self-dual code of length n. Let $M = (m_{ij})$ be the matrix of all A_t codewords of weight t in C, $1 \le i \le A_t$ and $1 \le j \le n$. For any integer k, $1 \le k \le n$ and for any set of columns $j_1, j_2, \ldots, j_k$ let $n_t(j_1, \ldots, j_k)$ be the number of rows r such that $m_{rj_1} \cdots m_{rj_k} \neq 0$. We consider the set

$$S_t(k) = \{n_t(j_1, \ldots, j_k) | 1 \le j_1 < \cdots < j_k \le n\}.$$

Let $M_t(k)$ and $m_t(k)$ denote the maximum and the minimum of $S_t(k)$, respectively. For the 20 codes $C_{62,i}$, $i = 1, \ldots, 20$, the values of $M_{12}(k)$ and $m_{12}(k)$, $k = 1, 2, 3$, were computed and listed in Table I. We verified that the code C_{62} as defined in [6] and $C_{62,19}$ have identical values for $M_{12}(k)$ and $m_{12}(k)$, $k = 1, 2, 3$. Moreover, using MAGMA, it was shown that the two codes are equivalent. Hence, the other codes are new. From the table it appears that the codewords of minimum weight in $C_{62,i}$, $i = 1, \ldots, 9$, form a 1-$(62, 12, 360)$ design which cannot be explained by the Assmus–Mattson theorem.

TABLE II
MATRICES Y_i

Matrices	$(r_1, r_2, r_3, r_4, r_5, r_6, r_7, r_8)$ $(u_1, u_2, u_3, u_4, u_5, u_6, u_7, u_8)$	$(s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8)$ $(v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8)$
Y_1	$(e_1, \alpha_2, o, \alpha_1, o, \alpha_{10}, e_1, \alpha_{14})$ $(o, o, \gamma_1, e_3, \gamma_1, e_3, \gamma_1, o)$	$(e_2, \beta_1, o, o, o, \beta_1, e_2, \beta_1)$ $(e_4, o, o, \delta_2, o, \delta_1, e_4, o)$
Y_2	$(e_1, \alpha_5, o, \alpha_1, o, \alpha_{13}, e_1, \alpha_{14})$ $(o, o, \gamma_1, e_3, \gamma_1, e_3, \gamma_3, o)$	$(e_2, \beta_1, o, o, o, \beta_3, e_2, \beta_1)$ $(e_4, o, o, \delta_1, o, \delta_2, e_4, o)$
Y_3	$(e_1, \alpha_5, o, \alpha_1, o, \alpha_{13}, e_1, \alpha_{14})$ $(o, o, \gamma_1, e_3, \gamma_1, e_3, \gamma_4, o)$	$(e_2, \beta_1, o, o, o, \beta_4, e_2, \beta_1)$ $(e_4, o, o, \delta_1, o, e_4, e_4, o)$
Y_4	$(e_1, o, \alpha_2, \alpha_4, o, e_1, \alpha_7, \alpha_{14})$ $(o, \gamma_1, e_3, o, \gamma_1, \gamma_1, o, e_3)$	$(e_2, o, o, \beta_1, o, e_2, \beta_1, \beta_1)$ $(e_4, o, \delta_2, o, o, e_4, o, \delta_1)$
Y_5	$(e_1, o, \alpha_1, \alpha_5, o, e_1, \alpha_5, \alpha_4)$ $(o, \gamma_1, e_3, o, \gamma_1, \gamma_2, o, e_3)$	$(e_2, o, o, \beta_1, o, e_2, \beta_1, \beta_2)$ $(e_4, o, o, \delta_2, o, e_4, e_4, o)$
Y_6	$(e_1, \alpha_{11}, o, \alpha_7, o, \alpha_{13}, e_1, \alpha_{14})$ $(\gamma_1, o, \gamma_3, e_3, \gamma_1, e_3, \gamma_{11}, o)$	$(e_2, \beta_1, o, \beta_1, o, \beta_{11}, e_2, \beta_3)$ $(e_4, o, o, \delta_2, o, \delta_2, e_4, o)$
Y_7	$(e_1, \alpha_8, o, \alpha_4, o, \alpha_{13}, e_1, \alpha_{14})$ $(\gamma_1, o, \gamma_4, e_3, \gamma_1, e_3, \gamma_{11}, o)$	$(e_2, \beta_1, o, \beta_1, o, \beta_{11}, e_2, \beta_4)$ $(e_4, o, o, \delta_2, o, \delta_1, e_4, o)$
Y_8	$(e_1, \alpha_8, o, \alpha_1, o, \alpha_1, e_1, \alpha_{14})$ $(\gamma_1, o, \gamma_5, e_3, \gamma_1, e_3, \gamma_{14}, o)$	$(e_2, \beta_1, o, \beta_1, o, \beta_{14}, e_2, \beta_5)$ $(e_4, o, o, \delta_1, o, \delta_1, e_4, o)$
Y_9	$(e_1, \alpha_{11}, o, \alpha_4, o, \alpha_1, e_1, \alpha_{14})$ $(\gamma_1, o, \gamma_6, e_3, \gamma_1, e_3, \gamma_5, o)$	$(e_2, \beta_1, o, \beta_1, o, \beta_5, e_2, \beta_6)$ $(e_4, o, o, \delta_1, o, \delta_1, e_4, o)$
Y_{10}	$(e_1, \alpha_8, o, \alpha_7, o, \alpha_{10}, e_1, \alpha_{14})$ $(\gamma_1, o, \gamma_3, e_3, \gamma_1, e_3, \gamma_9, o)$	$(e_2, \beta_1, o, \beta_1, o, \beta_9, e_2, \beta_3)$ $(e_4, o, o, \delta_1, o, \delta_1, e_4, o)$
Y_{11}	$(o, \alpha_3, e_1, o, \alpha_9, o, o, e_1)$ $(e_3, o, \gamma_2, \gamma_1, o, e_3, \gamma_1, \gamma_7)$	$(\beta_2, \beta_1, e_2, o, \beta_1, \beta_7, o, e_2)$ $(\delta_1, o, e_4, o, o, \delta_2, o, e_4)$
Y_{12}	$(o, \alpha_3, e_1, o, e_1, o, o, e_1)$ $(e_3, o, \gamma_2, \gamma_1, o, e_3, \gamma_1, \gamma_5)$	$(\beta_2, \beta_1, e_2, o, \beta_1, \beta_5, o, e_2)$ $(o, \delta_1, e_4, o, \delta_1, o, o, e_4)$
Y_{13}	$(o, \alpha_3, e_1, o, \alpha_{12}, o, o, e_1)$ $(e_3, o, \gamma_1, \gamma_{14}, o, e_3, \gamma_8, \gamma_6)$	$(\beta_1, \beta_8, e_2, o, \beta_{14}, \beta_6, o, e_2)$ $(o, \delta_2, e_4, o, \delta_2, o, o, e_4)$
Y_{14}	$(o, \alpha_3, e_1, o, \alpha_6, o, o, e_1)$ $(e_3, o, \gamma_1, \gamma_{14}, o, e_3, \gamma_8, \gamma_3)$	$(\beta_1, \beta_8, e_2, o, \beta_{14}, \beta_3, o, e_2)$ $(\delta_2, o, e_4, o, o, \delta_2, o, e_4)$
Y_{15}	$(o, \alpha_3, e_1, o, \alpha_3, o, o, e_1)$ $(e_3, o, \gamma_1, \gamma_{14}, o, e_3, \gamma_8, \gamma_9)$	$(\beta_1, \beta_8, e_2, o, \beta_{14}, \beta_9, o, e_2)$ $(\delta_1, o, e_4, o, o, \delta_2, o, e_4)$
Y_{16}	$(o, \alpha_3, e_1, o, \alpha_3, o, o, e_1)$ $(e_3, o, \gamma_2, \gamma_1, o, e_3, \gamma_1, \gamma_6)$	$(\beta_2, \beta_1, e_2, o, \beta_1, \beta_6, o, e_2)$ $(o, \delta_1, e_4, o, e_4, o, o, e_4)$
Y_{17}	$(o, \alpha_3, e_1, o, \alpha_9, o, o, e_1)$ $(e_3, o, \gamma_1, \gamma_{14}, o, e_3, \gamma_8, \gamma_7)$	$(\beta_1, \beta_8, e_2, o, \beta_{14}, \beta_7, o, e_2)$ $(o, \delta_1, e_4, o, \delta_2, o, o, e_4)$
Y_{18}	$(o, \alpha_3, e_1, o, \alpha_3, o, o, e_1)$ $(e_3, o, \gamma_1, e_3, o, e_3, \gamma_9, \gamma_8)$	$(\beta_1, \beta_9, e_2, o, e_2, \beta_8, o, e_2)$ $(o, \delta_1, e_4, o, \delta_1, o, o, e_4)$
Y_{19}	$(o, \alpha_3, e_1, o, \alpha_3, o, o, e_1)$ $(e_3, o, \gamma_2, \gamma_1, o, e_3, \gamma_1, \gamma_8)$	$(\beta_2, \beta_1, e_2, o, \beta_1, \beta_8, o, e_2)$ $(o, \delta_2, e_4, o, \delta_2, o, o, e_4)$
Y_{20}	$(o, \alpha_3, e_1, o, \alpha_{12}, o, o, e_1)$ $(e_3, o, \gamma_1, \gamma_{14}, o, e_3, \gamma_8, \gamma_1)$	$(\beta_1, \beta_8, e_2, o, \beta_{14}, \beta_1, o, e_2)$ $(o, \delta_1, e_4, o, \delta_1, o, o, e_4)$

III. Related Extremal Self-Dual Codes of Lengths 58 and 60

In this section, extremal self-dual codes of lengths 58 and 60 are constructed from some of the extremal self-dual codes of length 62 which were discussed in the previous section.

A. Extremal Self-Dual Codes of Length 60

New extremal self-dual codes of length 60 are constructed from some extremal self-dual codes of length 62 by the process of subtraction.

First we give the possible weight enumerators of extremal self-dual $[60, 30, 12]$ codes, which were derived in [3] and [5]

$$W_{60,1} = 1 + (2555 + 64\beta)y^{12} + (33600 - 384\beta)y^{14} + \cdots$$

$$W_{60,2} = 1 + 3451y^{12} + 24128y^{14} + \cdots$$

where β is an undetermined parameter with $0 \le \beta \le 10$. An extremal self-dual code with weight enumerator $W_{60,2}$ was constructed in [3].

TABLE III
FIRST ROWS OF THE CIRCULANT MATRICES e_i, α_j, β_s, γ_r, AND δ_t

	First rows		First rows		First rows
e_1	011110111101111	e_2	000100110101111	e_3	011110101100100
e_4	011011011011011	α_1	110001100011000	α_2	101001010010100
α_3	111101111011110	α_4	100011000110001	α_5	010010100101001
α_6	111011110111101	α_7	000110001100011	α_8	100101001010010
α_9	110111101111011	α_{10}	001100011000110	α_{11}	001010010100101
α_{12}	101111011110111	α_{13}	011000110001100	α_{14}	010100101001010
β_1	110001001101011	β_2	111100010011010	β_3	101111000100110
β_4	101011110001001	β_5	011010111100010	β_6	100110101111000
β_7	001001101011110	β_8	100010011010111	β_9	111000100110101
β_{10}	011110001001101	β_{11}	010111100010011	β_{12}	110101111000100
β_{13}	001101011110001	β_{14}	010011010111100	γ_1	111010110010001
γ_2	101011001000111	γ_3	101100100011110	γ_4	110010001111010
γ_5	001000111101011	γ_6	100011110101100	γ_7	001111010110010
γ_8	111101011001000	γ_9	110101100100011	γ_{10}	010110010001111
γ_{11}	011001000111101	γ_{12}	100100011110101	γ_{13}	010001111010110
γ_{14}	000111101011001	δ_1	110110110110110	δ_2	101101101101101

As for weight enumerators of type $W_{60,1}$, some extremal double circulant self-dual codes with $\beta = 10$ were constructed in [5]. These codes are equivalent to the code P_{60} defined in [7]. Furthermore, two codes with $\beta = 0$ and with $\beta = 10$, respectively, were constructed in [13], and a code with $\beta = 7$ in [4]. Let C be one of the codes $C_{62,l}$, $l = 6, 7, 8, 11, \ldots, 20$. Since C has the property that $m_{12}(2) = 0$, there are two coordinates i, j with $n_{12}(i, j) = 0$, that is, there is no codeword $(x_1, \ldots, x_{62})$ of weight 12 such that $(x_i, x_j) = (1, 1)$. More precisely, $\{61, 62\}$ is the unique pair of two coordinates $\{i, j\}$ with $n_{12}(i, j) = 0$ for every code $C_{62,l}$, $l = 6, 7, 8, 11, \ldots, 20$.

Let C' denote the code of length 60, obtained from C by subtracting the last two coordinates, that is,

$$C' = \{(x_1, \ldots, x_{60}) \mid (x_1, \ldots, x_{62}) \in C, x_{61} + x_{62} \equiv 0 \pmod 2\}.$$

Then C' is self-dual. In addition, C' has minimum weight 12. Note that C' is an extremal self-dual $[60, 30, 12]$ code with an automorphism σ' of order 15

$$\sigma' = (1, \ldots, 15)(16, \ldots, 30)(31, \ldots, 45)(46, \ldots, 60).$$

For the 13 codes $C'_{62,i}$, $i = 6, 7, 8, 11, \ldots, 20$, the value of β in the weight enumerator $W_{60,1}$, $M_{12}(k)$ and $m_{12}(k)$, $k = 1, 2, 3$ and the order $|\mathrm{Aut}|$ of the automorphism group are also listed in Table IV. For the three codes with $\beta = 0, 10$ in [5] and [13], which were mentioned before, the results are also listed. Note that the codewords of minimum weight in every code of Table IV form a 1-design. This property is not explained by the Assmus–Mattson theorem.

From Table IV, it appears that $C'_{62,14}$ and $C'_{62,15}$ have identical values $M_{12}(k)$ and $m_{12}(k)$, for $k = 1, 2, 3$. Moreover, using MAGMA, we verified that these two codes are equivalent. It was also verified by MAGMA that the extremal self-dual codes with $\beta = 0$ and $\beta = 10$ in [13] are equivalent to $C'_{62,6}$ and $C'_{62,19}$, respectively. Therefore, the codes $C'_{62,i}$ for $i = 7, 8, 11, 12, 13, 14, 16, 17, 18, 20$ are new extremal self-dual codes of length 60.

B. Extremal Self-Dual Codes of Length 58

Extremal self-dual $[58, 29, 10]$ codes have possible weight enumerators

$$W_{58,1} = 1 + (165 - 2\gamma)y^{10} + (5078 + 2\gamma)y^{12} + \cdots$$

$$W_{58,2} = 1 + (319 - 24\beta - 2\gamma)y^{10} + (3132 + 152\beta + 2\gamma)y^{12} + \cdots$$

where β and γ are undetermined parameters [3]. As for the weight enumerator $W_{58,1}$, an extremal self-dual code with $\gamma = 55$ is known [12]. As for the weight enumerator $W_{58,2}$, we refer to [1] and [9],

---

00111110111010000011101000011, 10110000111010011111011111101,
11110111111010010001000100010, 11010100011010110110001001101,
11000101101010000101101111010, 11001101010010111100011100001,
11001001001110000000100101100, 11001011000000111110111001010,
11001010000111100001110111001, 11111111100001100101011101000,
01001010110101111001100011100, 10111111111000001001010111010,
01011111111100000100101011101, 00101111111110100010010101110,
10001011101010101000011111111, 01000101110101110100001111111,
10010001011101111101000011111, 01111101101011010101101100111,
10100100010111111111010000111, 01100111001110010100100101011,
10011100000000010100111001001, 11100001100111010100110111000,
11101010010001011111111101000, 01000000001101100100110011100,
10111010100100000111111111010, 01011101010010000011111111101,
00101110101001100001111111110, 00100010010001111011110010111,
00110101000101101011001101000.

TABLE IV
EXTREMAL SELF-DUAL CODES OF LENGTH 60

Codes	β	$M_{12}(3)$	$m_{12}(3)$	$M_{12}(2)$	$m_{12}(2)$	$M_{12}(1)$	$m_{12}(1)$	$\lvert\mathrm{Aut}\rvert$
$C'_{62,6}$	0	28	5	135	71	511	511	60
$C'_{62,7}$	0	25	7	115	71	511	511	30
$C'_{62,8}$	0	24	7	111	71	511	511	60
$C'_{62,11}$	10	39	9	175	95	639	639	15
$C'_{62,12}$	10	35	9	183	95	639	639	60
$C'_{62,13}$	10	34	10	155	103	639	639	60
$C'_{62,14}$	10	36	10	171	95	639	639	15
$C'_{62,15}$	10	36	10	171	95	639	639	15
$C'_{62,16}$	10	35	9	167	99	639	639	30
$C'_{62,17}$	10	35	8	175	91	639	639	30
$C'_{62,18}$	10	38	9	191	95	639	639	60
$C'_{62,19}$	10	36	10	147	95	639	639	60
$C'_{62,20}$	10	33	10	163	95	639	639	60
P_{60} in [7]	10	36	9	175	95	639	639	60
[13]	0	28	5	135	71	511	511	60
[13]	10	36	10	147	95	639	639	60

where the existence is established of extremal self-dual codes for the following parameter values:

$$\beta = 0 \quad \text{and} \quad \gamma \in \{0,\ 32,\ 36\} \cup \{2m \mid 40 \le 2m \le 122\}$$

$$\beta = 1 \quad \text{and} \quad \gamma \in \{2m \mid 42 \le 2m \le 100\}$$

$$\beta = 2 \quad \text{and} \quad \gamma \in \{32,\ 36,\ 40,\ 44\} \cup \{2m \mid 48 \le 2m \le 88\} \cup \{92\}.$$

We remark that the code with $\beta = 0$ and $\gamma = 44$ does not occur in [1] and [9], but is mentioned in [2, Table VIII].

An extremal self-dual code of length 60 yields extremal self-dual $[58,\ 29,\ 10]$ codes by subtracting. In fact, in [13], extremal self-dual $[58,\ 29,\ 10]$ codes for various types of weight enumerators are constructed from known codes. Here, we investigate extremal self-dual codes constructed from the new extremal self-dual codes, discussed in Section III-A.

Let C_{58} be a $[58, 29]$ code with generator matrix $(I,\ M)$ where M is written as $m_1,\ \ldots,\ m_{29}$ with the ith row m_i as shown at the bottom of the previous page. The code C_{58} is an extremal self-dual code which is constructed from the new extremal self-dual $[60,\ 30,\ 12]$ code $C'_{62,7}$ by subtracting the first and 18th coordinates. This code has the weight enumerator

$$1 + 71y^{10} + 3380y^{12} + 38772y^{14} + 297309y^{16} + 1672840y^{18} + \cdots.$$

Thus, the code C_{58} has weight enumerator $W_{58,2}$ with $\beta = 0$ and $\gamma = 124$. It was also verified that C_{58} has an automorphism group of order 2.

Proposition 4: There is an extremal self-dual $[58,\ 29,\ 10]$ code with weight enumerator $W_{58,2}$, with $\beta = 0$ and $\gamma = 124$.

When applying the subtraction method to the other codes of length 60, they all yield extremal self-dual codes of length 58 with weight enumerators belonging to codes already known.

ACKNOWLEDGMENT

The authors wish to thank Ahikiro Munemasa for his useful conversations and comments and A. J. van Zanten for constructive remarks that led to an improvement of the manuscript. The first author would like to thank Delft University of Technology for the excellent working conditions provided.

REFERENCES

[1] S. Bouyuklieva, "A method for constructing self-dual codes with an automorphism of order 2," *IEEE Trans. Inform. Theory*, vol. 46, pp. 496–504, Mar. 2000.

[2] S. Boyuklieva and I. Boukliev, "Extremal self-dual codes with an automorphism of order 2," *IEEE Trans. Inform. Theory*, vol. 44, pp. 323–328, Jan. 1998.

[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*, vol. 36, pp. 1319–1333, Nov. 1990.

[4] R. Dontcheva and M. Harada, "Some extremal self-dual codes with an automorphism of order 7," manuscript, submitted for publication.

[5] T. A. Gulliver and M. Harada, "Weight enumerators of extremal singly-even [60, 30, 12] codes," *IEEE Trans. Inform. Theory*, vol. 42, pp. 658–659, Mar. 1996.

[6] M. Harada, "Construction of an extremal self-dual code of length 62," *IEEE Trans. Inform. Theory*, vol. 45, pp. 1232–1233, May 1999.

[7] M. Harada, T. A. Gulliver, and H. Kaneta, "Classification of extremal double circulant self-dual codes of length up to 62," *Discr. Math.*, vol. 188, pp. 127–136, 1998.

[8] W. C. Huffman, "Decomposing and shortening codes using automorphisms," *IEEE Trans. Inform. Theory*, vol. IT-32, pp. 833–836, Nov. 1986.

[9] J.-L. Kim, "New extremal self-dual codes of lengths 36, 38 and 58," *IEEE Trans. Inform. Theory*, vol. 47, pp. 386–393, Jan. 2001.

[10] C. L. Mallows and N. J. A. Sloane, "An upper bound for self-dual codes," *Inform. Contr.*, vol. 22, pp. 188–200, 1973.

[11] E. Rains and N. J. A. Sloane, "Self-dual codes," in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands: Elsevier, 1998, pp. 177–294.

[12] H.-P. Tsai, "Existence of certain extremal self-dual codes," *IEEE Trans. Inform. Theory*, vol. 38, pp. 501–504, Mar. 1992.

[13] H.-P. Tsai and Y. J. Jiang, "Some new extremal self-dual $[58,\ 29,\ 10]$ codes," *IEEE Trans. Inform. Theory*, vol. 44, pp. 813–814, Mar. 1998.

[14] V. Y. Yorgov, "Binary self-dual codes with automorphisms of odd order" (in Russian), *Probl. Pered. Inform.*, vol. 19, pp. 11–24, 1983. English translation: *Probl. Inform. Transm.*, vol. 19, pp. 260–270, 1983.