

## ON EXTREMAL BINARY DOUBLY-EVEN SELF-DUAL CODES OF LENGTH 88\*

Radinka Yorgova, Nuray At

**ABSTRACT.** In this paper we present 35 new extremal binary self-dual doubly-even codes of length 88. Their inequivalence is established by invariants. Moreover, a construction of a binary self-dual  $[88, 44, 16]$  code, having an automorphism of order 21, is given.

**1. Introduction.** Binary self-dual codes are an interesting class of codes for several reasons. These codes include the extended  $[8, 4, 4]$  Hamming code, the extended binary Golay code and the extended binary quadratic residue codes. Many of the self-dual codes are related to block designs, graphs, lattices and other combinatorial structures.

All binary self-dual codes of Type II of length up to 32 and all of Type I of length up to 34 are classified and given in [1], [2], [11], [12] and [15]. It is known that with increasing length the number of self-dual codes grows very fast. For example, there are 85 inequivalent self-dual codes of Type II of length 32 and

---

*ACM Computing Classification System* (1998): E.4, H.1.1.

*Key words:* Automorphisms, self-dual codes.

\*This work was partly supported by the Norwegian Government Scholarship.

at least 17000 of length 40. Therefore, the question of classifying all self-dual codes of a given length loses interest for increasing values of  $n$ .

In this work we study extremal binary doubly-even self-dual codes of length 88 having an automorphism of order 21. The greatest length of an extremal doubly-even self-dual code with minimum distance 16 is 88. The first example of such a code is given in [9, p. 633]. The next 33 codes are presented in [6]. A construction of a self-dual  $[88,44,16]$  code having an automorphism of order 5 is given in [5] and 36 new codes are listed. Here we construct 35 new binary  $[88,44,16]$  doubly-even self-dual codes. These codes and the previously known 70 codes are inequivalent.

A binary  $[n, k]$  code  $\mathcal{C}$  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  $\mathcal{C}$  is *self-dual* if  $\mathcal{C} = \mathcal{C}^\perp$  where  $\mathcal{C}^\perp$  is the dual code of  $\mathcal{C}$  under the standard inner product. A self-dual code  $\mathcal{C}$  is *doubly-even* if all codewords of  $\mathcal{C}$  have weight divisible by four, and *singly-even* if there is at least one codeword of weight  $\equiv 2 \pmod{4}$ . Self-dual doubly-even codes exist only when  $n$  is a multiple of eight. It is known [13] that for a self-dual  $[n, n/2, d]$  code:

$$(1) \quad d \leq 4 \left\lfloor \frac{n}{24} \right\rfloor + 4, \text{ if } n \not\equiv 22 \pmod{24},$$

and

$$(2) \quad d \leq 4 \left\lfloor \frac{n}{24} \right\rfloor + 6, \text{ if } n \equiv 22 \pmod{24}.$$

If  $n$  is a multiple of 24, then any code reaching limit (1) must be doubly-even.

Self-dual codes which reach these bounds are called *extremal*.

The weight enumerator of a  $[n, k]$  code is the polynomial  $\sum_{i=1}^n A_i y^i$ , where  $A_i$  is the number of the codewords of weight  $i$ . The weight enumerator of extremal doubly-even self-dual codes of a given length is uniquely determined [4]. Two binary codes are *equivalent* if one can be obtained from the other by a permutation of the coordinates. A permutation  $\sigma$  of  $n$  elements is an automorphism of a code  $\mathcal{C}$  if  $\mathcal{C}$  coincides with its image  $\sigma(\mathcal{C})$ . The set of all automorphisms of a code  $\mathcal{C}$  forms the automorphism group  $Aut(\mathcal{C})$  of  $\mathcal{C}$ .

In the next section we investigate the possible types of automorphisms of order 21 of a binary doubly-even  $[88,44,16]$  self-dual code. Further, we present a construction of a binary  $[88,44,16]$  self-dual code having an automorphism of order 21, and at last we list the new 35 codes.

**2. Automorphisms of order 21 of a binary doubly-even [88, 44, 16] self-dual code.** Let  $\mathcal{C}$  be a [88,44,16] self-dual code having an automorphism  $\sigma$  of order 21. Then,  $\sigma$  is a permutation and, without loss of generality we may write

$$(3) \quad \begin{aligned} \sigma = & \Omega_1 \Omega_2 \dots \Omega_{t_1} \Omega_{t_1+1} \Omega_{t_1+2} \dots \Omega_{t_1+t_2} \\ & \Omega_{t_1+t_2+1} \Omega_{t_1+t_2+2} \dots \Omega_{t_1+t_2+t_3} \\ & \Omega_{t_1+t_2+t_3+1} \Omega_{t_1+t_2+t_3+2} \dots \Omega_{t_1+t_2+t_3+f}, \end{aligned}$$

where  $\Omega_i$  is a cycle of length 3 for  $1 \leq i \leq t_1$ , a cycle of length 7 for  $t_1 + 1 \leq i \leq t_1 + t_2$ , and a cycle of length 21 for  $t_1 + t_2 + 1 \leq i \leq t_1 + t_2 + t_3$ . For  $t_1 + t_2 + t_3 + 1 \leq i \leq t_1 + t_2 + t_3 + f$  the symbol  $\Omega_i$  represents a fixed point. For short we say that  $\sigma$  is of type  $21-(t_1, t_2, t_3; f)$ . From [3, Proposition 3.1] it follows that  $\mathcal{C}$  has also automorphisms of type  $3 - (7t_3 + t_1; 7t_2 + f)$  and type  $7 - (3t_3 + t_2; 3t_1 + f)$ . The possible automorphisms of order 3 and order 7 of an extremal self-dual binary code of length 88 are of types  $3 - (28; 4)$ ,  $3 - (26; 10)$ ,  $3 - (24; 16)$ ,  $3 - (22; 22)$ ,  $3 - (16; 40)$ ,  $3 - (14; 46)$ ,  $7 - (12; 4)$  and  $7 - (11; 11)$  [14, Theorem 1]. Hence, the type of the automorphism  $\sigma$  can be  $21 - (0, 0, 4; 4)$ ,  $21 - (1, 3, 3; 1)$ ,  $21 - (0, 6, 2; 4)$ ,  $21 - (2, 5, 2; 5)$ ,  $21 - (0, 5, 2; 11)$ ,  $21 - (1, 2, 3; 8)$  and  $21 - (3, 2, 3; 2)$ .

Similar to [3] we define

$$(4) \quad F_\sigma(\mathcal{C}) = \{v \in \mathcal{C} \mid v\sigma = v\}$$

and

$$(5) \quad \begin{aligned} E_\sigma(\mathcal{C}) = \{v \in \mathcal{C} \mid & wt(v|\Omega_i) \equiv 0 \pmod{2}, \\ & i = 1, \dots, t_1 + t_2 + t_3 + f\}, \end{aligned}$$

where  $v|\Omega_i$  is the restriction of  $v$  to  $\Omega_i$ .

It is clear that  $v \in F_\sigma(\mathcal{C})$ , if and only if  $v \in \mathcal{C}$  and the coordinates of  $v$  are constant on each cycle  $\Omega_j$ ,  $j = 1, 2, \dots, t_1 + t_2 + t_3 + f$ . The map  $\pi$  is defined by

$$(6) \quad \pi : F_\sigma(\mathcal{C}) \rightarrow \mathbb{F}_2^{t_1+t_2+t_3+f}, \quad \pi(v|\Omega_i) = v_j,$$

for some  $j \in \Omega_i$ ,  $i = 1, 2, \dots, t_1 + t_2 + t_3 + f$ .

Let  $\sigma$  be of type  $21 - (0, 5, 2; 11)$ . Then,  $\pi(F_\sigma(\mathcal{C}))$  is a binary self-dual [18,9] code [3, Proposition 3.2].

**Theorem 1** [10, Theorem 11]. *Let  $\mathcal{C}$  be a self-dual code of length  $n = n_a + n_b$  over  $GF(q)$ . Partition the generator matrix of  $\mathcal{C}$  as follows:*

$$\begin{array}{c} n_a \quad n_b \\ k_a \\ k_b \\ k_d \end{array} \begin{pmatrix} A & O \\ O & B \\ D & E \end{pmatrix},$$

where  $k_a$  and  $k_b$  are to be chosen as large as possible. Then

- i)  $k_d = \text{rank } D = \text{rank } E$ ,
- ii)  $k_b = 1/2n - (n_a - k_a)$ ,
- iii) the code generated by the rows of  $A$  and  $D$  is the dual of the code generated by the rows of  $A$ .

Therefore, the generator matrix of any binary [18, 9] self-dual code can be presented in the form:

$$\begin{array}{c} 7 \quad 11 \\ k_a \\ k_b \\ k_d \end{array} \begin{pmatrix} A & O \\ O & B \\ D & E \end{pmatrix},$$

where  $k_b = 2 + k_a$ . Then,  $k_b \geq 2$ . If a binary self-dual [18, 9] code generates  $\pi(F_\sigma(\mathcal{C}))$ , then the matrix  $B$  generates [11,  $k_b$ ,  $d_b$ ] code where  $k_b \geq 2$ ,  $d_b \geq 16$ . So, the automorphism  $\sigma$  is not of type  $21 - (0, 5, 2; 11)$ .

In a similar way one can show that the automorphism  $\sigma$  is not of type  $21 - (1, 2, 3; 8)$  either.

Therefore if an extremal binary [88, 44, 16] self-dual doubly-even code has an automorphism of order 21, then its type is  $21 - (0, 0, 4; 4)$ ,  $21 - (1, 3, 3; 1)$ ,  $21 - (0, 6, 2; 4)$ ,  $21 - (2, 5, 2; 5)$  or  $21 - (3, 2, 3; 2)$ .

**3. Construction of a Self-Dual [88, 44, 16] code with an automorphism of type  $21 - (0, 0, 4; 4)$ .** Let now the permutation  $\sigma$  of type  $21 - (0, 0, 4; 4)$  be an automorphism of  $\mathcal{C}$ .  $F_\sigma(\mathcal{C})$  and  $E_\sigma(\mathcal{C})$  are defined as in (4) and (5).

The next proposition follows from [8, Theorems 1–3].

**Proposition 2.** *Let  $\mathcal{C}$  be a self-dual doubly-even code of length 88 with an automorphism  $\sigma$  of type  $21 - (0, 0, 4; 4)$ . Then,*

- (1)  $\mathcal{C} = F_\sigma(\mathcal{C}) \oplus E_\sigma(\mathcal{C})$ .

- (2)  $F_\sigma(\mathcal{C})$  and  $E_\sigma(\mathcal{C})$  are  $\sigma$ -invariant, that is, invariant under the action of  $\sigma$ .
- (3) The subcodes  $F_\sigma(\mathcal{C})$  and  $E_\sigma(\mathcal{C})$  have dimensions 4 and 44 respectively.
- (4)  $\pi(F_\sigma(\mathcal{C}))$  is a self-dual code of length 8.

The image  $\pi(F_\sigma(\mathcal{C}))$  is a binary self-dual  $[8, 4]$  code. The only such codes are  $C_2^4$  and  $A_8$ . Let  $\pi(F_\sigma(\mathcal{C})) = A_8$ . Then as a generator matrix of  $F_\sigma(\mathcal{C})$  we can consider the following matrix:

$$(7) \quad X = \left( \begin{array}{cccc|ccc} \mathbf{1} & & & & 1 & 1 & 1 \\ & \mathbf{1} & & & 1 & & 1 \\ & & \mathbf{1} & & 1 & 1 & \\ & & & \mathbf{1} & 1 & 1 & 1 \end{array} \right),$$

where  $\mathbf{1}$  is the all-one vector of length 21 and the blanks are zeroes.

Denote by  $\mathcal{P}$  the set of even-weight polynomials in the factor-ring  $\mathcal{R}_{21} = \mathbb{F}_2[x]/(x^{21} - 1)$ . The factorization of the polynomial  $x^{21} - 1$  over the binary field is given by  $x^{21} - 1 = h_0(x)h_1(x)h_2(x)h_3(x)h_4(x)h_5(x)$ , where  $h_0(x) = 1 + x$ ,  $h_1(x) = 1 + x + x^2$ ,  $h_2(x) = 1 + x + x^3$ ,  $h_3(x) = 1 + x^2 + x^3$ ,  $h_4(x) = 1 + x + x^2 + x^4 + x^6$  and  $h_5(x) = 1 + x^2 + x^3 + x^4 + x^5 + x^6$  are irreducible polynomials over  $\mathbb{F}_2$ .

Let  $I_j$  be the ideal of  $\mathcal{R}_{21}$  generated by the polynomial  $\frac{x^{21} - 1}{h_j(x)}$ . Then

$I_j$  is a cyclic code which is isomorphic to the field  $\mathbb{F}_2^{\deg h_j(x)}$  for  $j = 1, 2, 3, 4, 5$  and, moreover,  $\mathcal{P} = I_1 \oplus I_2 \oplus I_3 \oplus I_4 \oplus I_5$ . The orthogonal idempotent of  $I_j$ ,  $j = 1, \dots, 5$  is  $\epsilon_j(x) = e_0 + e_1x + e_2x^2 + \dots + e_{20}x^{20}$ , where  $\epsilon_j$  are:

$j$	$e_0e_1 \dots e_{20}$
1	011011011011011011011
2	111010011101001110100
3	100101110010111001011
4	011010011001001010000
5	000001010010011001011

As a primitive element of  $I_j$ ,  $j = 1, \dots, 5$ , we use  $\mu_j(x) = m_0 + m_1x + m_2x^2 + \dots + m_{20}x^{20}$ , where  $\mu_j$  are:

$j$	$m_0m_1 \dots m_{20}$
1	110110110110110110110
2	100111010011101001110
3	101110010111001011100
4	011011110000101110101
5	010101110100001111011

Using GAP [17], the minimum distance of the cyclic codes  $I_1, \dots, I_5$  is calculated. We obtain that  $I_1, I_2, I_3, I_4$  and  $I_5$  are respectively  $[21, 2, 14], [21, 3, 12], [21, 3, 12], [21, 6, 8]$  and  $[21, 6, 8]$  codes.

Let  $E_\sigma(\mathcal{C})^*$  be the subcode  $E_\sigma(\mathcal{C})$  with the last four coordinates deleted. We define the map  $\varphi : E_\sigma(\mathcal{C})^* \rightarrow \mathcal{P}^4$  by identifying the restricted vector  $v|\Omega_i = (v_0, v_1, \dots, v_{20})$  with the polynomial  $\varphi(v|\Omega_i)(x) = v_0 + v_1x + \dots + v_{20}x^{20}$  for  $i = 1, 2, 3, 4$ .

From [16, Lemma 6]  $\varphi(E_\sigma(\mathcal{C})^*)$  is a self-orthogonal code in  $\mathcal{P}^4$  under the inner product  $\langle u, v \rangle = \sum_{i=1}^4 u_i(x)v_i(x^{-1})$ . Therefore, we can take a generator matrix for  $\varphi(E_\sigma(\mathcal{C})^*)$  of the form

$$Y' = \begin{pmatrix} \epsilon_1(x) & 0 & \alpha_1(x) & \alpha_2(x) \\ 0 & \epsilon_1(x) & \alpha_3(x) & \alpha_4(x) \\ \epsilon_2(x) & 0 & \beta_1(x) & \beta_2(x) \\ 0 & \epsilon_2(x) & \beta_3(x) & \beta_4(x) \\ \beta_1(x^{-1}) & \beta_3(x^{-1}) & \epsilon_3(x) & 0 \\ \beta_2(x^{-1}) & \beta_4(x^{-1}) & 0 & \epsilon_3(x) \\ \epsilon_4(x) & 0 & \gamma_1(x) & \gamma_2(x) \\ 0 & \epsilon_4(x) & \gamma_3(x) & \gamma_4(x) \\ \gamma_1(x^{-1}) & \gamma_3(x^{-1}) & \epsilon_5(x) & 0 \\ \gamma_2(x^{-1}) & \gamma_4(x^{-1}) & 0 & \epsilon_5(x) \end{pmatrix},$$

where  $\alpha_i(x) \in I_1$ , for  $i = 1, 2, 3, 4$ ,  $\beta_i(x) \in I_2$  and  $\beta_i(x^{-1}) \in I_3$ ,  $i = 1, 2, 3, 4$ , and  $\gamma_i(x) \in I_4$ ,  $\gamma_i(x^{-1}) \in I_5$  for  $i = 1, 2, 3, 4$ , whereas  $\epsilon_i(x)$ ,  $i = 1, 2, 3, 4, 5$  are defined above.

The corresponding generator matrix of the subcode  $E_\sigma(\mathcal{C})^*$  is

$$(8) \quad Y = \begin{pmatrix} y_{1,1} & \dots & y_{1,4} \\ \vdots & \ddots & \vdots \\ y_{10,1} & \dots & y_{10,4} \end{pmatrix},$$

where  $y_{i,j}$ ,  $i = 1, 2$ ,  $j = 1, \dots, 4$  are right-circulant  $2 \times 21$  matrices,  $y_{i,j}$  for  $i = 3, \dots, 6$ ,  $j = 1, \dots, 4$  are right-circulant  $3 \times 21$  matrices,  $y_{i,j}$  for  $i = 7, \dots, 10$ ,  $j = 1, \dots, 4$ , are right-circulant  $6 \times 21$  matrices. The first rows of the circulants correspond to the polynomials of the matrix  $Y'$ . Thus, we constructed a possible generator matrix of  $\mathcal{C}$ .

**Proposition 3.** *Let a binary self-dual doubly-even code  $\mathcal{C}$  of length 88 have an automorphism  $\sigma$  of type  $21-(0, 0, 4; 4)$ . Then a possible generator matrix*

of  $\mathcal{C}$  can be written as

$$(9) \quad G = \left( \begin{array}{c|c} X & \\ \hline Y & \begin{array}{c} 0000 \\ \vdots \\ 0000 \end{array} \end{array} \right),$$

where  $X$  and  $Y$  are defined in (7) and (8).

A computer check shows that many self-dual doubly-even codes with a generator matrix of the type (9) are extremal. Here we present 35 examples  $\mathcal{C}_1, \mathcal{C}_2, \dots, \mathcal{C}_{35}$  of extremal codes. To define completely their generator matrices  $G_1, \dots, G_{35}$ , it is sufficient to give the submatrix  $Y$  of  $G$  in (9). The matrix  $Y$  is determined by the circulant matrices  $y_{i,j}, i = 1, \dots, 12, j = 1, \dots, 6$  whose first rows are vectors corresponding to polynomials of the matrix  $Y'$ . The values of the polynomials in  $Y'$  for the codes  $\mathcal{C}_1, \mathcal{C}_2, \dots, \mathcal{C}_{35}$  are as follows:  $\alpha_1(x) = \alpha_4(x) = 0, \alpha_2(x) = \alpha_3(x) = \mu_1(x); \beta_1(x) = 0, \beta_i(x)$  is 0 or  $\mu_2^{t_i}(x)$  for  $i = 2, 3, 4$  and  $t_i = 1, \dots, 7; \gamma_1(x) = \epsilon_4(x), \gamma_i(x)$  is 0 or  $\mu_4^{s_i}(x)$  for  $i = 2, 3, 4$  and  $s_i = 1, \dots, 63$ . The values of the degrees  $t_i$  and  $s_i$  for  $i = 2, 3, 4$  are listed in Table 1. We note that if the value of  $\gamma_i(x)$  or  $\beta_i(x)$  is 0, then the corresponding entry for  $t_i$  or  $s_i$  is empty.

The weight enumerator of an extremal doubly-even self-dual [88,44,16] code is uniquely determined [4]:

$$W_C = 1 + 32164y^{16} + 6992832y^{20} + 535731625y^{24} + 16623384448y^{28} + 225426781470y^{32} + \dots$$

To prove the inequivalence of the codes we use the same invariants as in [6] and [5]. Let  $M$  be the set of all 32164 codewords of weight 16 and  $A_{i,j}$  be the number of the codewords of  $M$  that have one at the coordinate positions  $i$  and  $j$ . It is clear that the set of numbers  $\{A_{i,j} | 1 \leq i < j \leq 88\}$  is an invariant for equivalent codes. So, the smallest and the largest element  $m(2)$  and  $M(2)$ , respectively, in the set are invariants as well.

The values of  $m(2)$  and  $M(2)$  for the codes  $\mathcal{C}_1, \mathcal{C}_2, \dots, \mathcal{C}_{35}$  are listed in Table 1.

Table 1 implies that the presented new 35 extremal self-dual codes of length 88 are inequivalent and, moreover, together with the data in [7] and [5] it follows that these codes and the codes given in [6] and [5] are inequivalent as well.

Table 1. Matrices  $Y'$  and invariants

<i>Code</i>	$t_2$	$t_3$	$t_4$	$s_2$	$s_3$	$s_4$	$M(2)$	$m(2)$
$\mathcal{C}_1$	1	1	1	63	1	21	1071	672
$\mathcal{C}_2$	1	1	1	3	2	30	1080	819
$\mathcal{C}_3$	1	1	1	3	1	27	1089	777
$\mathcal{C}_4$	5	3	1		1	28	1092	756
$\mathcal{C}_5$	7	1	1		2	42	1095	714
$\mathcal{C}_6$	1	1	1		1	54	1098	714
$\mathcal{C}_7$	1	1	1	3	2	39	1101	777
$\mathcal{C}_8$	1	1	1		2	26	1104	777
$\mathcal{C}_9$	1	1	1	3	1	3	1107	801
$\mathcal{C}_{10}$	7	1	1		2	19	1110	864
$\mathcal{C}_{11}$	7	1	1		2	11	1113	738
$\mathcal{C}_{12}$	7	7	1		1	26	1113	777
$\mathcal{C}_{13}$	1	1	1		1	6	1116	672
$\mathcal{C}_{14}$	7	7	1		1	25	1131	861
$\mathcal{C}_{15}$	1	1	1	3	1	20	1134	819
$\mathcal{C}_{16}$	1	1	1	3	1	45	1137	777
$\mathcal{C}_{17}$	1	1	1	1	1	5	1152	882
$\mathcal{C}_{18}$	1	1	1		1	8	1155	630
$\mathcal{C}_{19}$	1	1	1		1	21	1158	780
$\mathcal{C}_{20}$	7	1	1		2	62	1176	630
$\mathcal{C}_{21}$	1	1	1		1	52	1179	735
$\mathcal{C}_{22}$	1	1	1		2	23	1197	693
$\mathcal{C}_{23}$	7	1	1		2	61	1218	717
$\mathcal{C}_{24}$	7	7	1		1	12	1221	903
$\mathcal{C}_{25}$	1	1	1		2	30	1239	693
$\mathcal{C}_{26}$	7	1	1		3	1	1242	840
$\mathcal{C}_{27}$	7	1	1		2	59	1263	885
$\mathcal{C}_{28}$	7	1	1		2	21	1281	735
$\mathcal{C}_{29}$	5	3	1		1	12	1302	756
$\mathcal{C}_{30}$	1	1	1		1	55	1323	612
$\mathcal{C}_{31}$	7	1	1		2	57	1344	843
$\mathcal{C}_{32}$	1	1	1	63	1	37	1347	798
$\mathcal{C}_{33}$	1	1	1	3	1	21	1365	840
$\mathcal{C}_{34}$	7	1	1		3	8	1368	840
$\mathcal{C}_{35}$	1	1	1	3	1	6	1389	861



**Theorem 4.** *Up to equivalence there are at least 105 binary extremal self-dual doubly-even codes of length 88, where 35 are new.*

**Acknowledgment.** The authors would like to thank the anonymous referees for their useful comments.

#### REFERENCES

- [1] CONWAY J. H., V. PLESS. On the enumeration of self-dual codes. *J. Combin. Theory*, ser. A, **28** (1980), 26–53.
- [2] CONWAY J. H., V. PLESS, N. J. SLOANE. The binary self-dual codes of length up to 32: a revised enumeration. *J. Combin. Theory*, ser. A, **60** (1992), 183–195.
- [3] DONTCHEVA R., A. J. VAN ZANTEN, S. M. DODUNEKOV. Binary self-dual codes with automorphisms of composite order. *IEEE Trans. Inform. Theory*, **50** (2004), 311–318.
- [4] DOUGHERTY S. T., T. A. GULLIVER, M. HARADA. Extremal binary self-dual codes. *IEEE Trans. Inform. Theory*, **43** (1997), 2036–2047.
- [5] GOODWIN V., V. YORGOV. New extremal self-dual doubly-even binary codes of length 88. *Finite Fields and Applications*, **11** (2005), 1–5.
- [6] GULLIVER T. A., M. HARADA, J-L. KIM. Construction of new extremal self-dual codes. *Discrete Mathematics*, **263** (2003), 81–91.
- [7] HARADA M. Private correspondence.
- [8] HUFFMAN W. C. Decomposing and shortening codes using automorphisms. *IEEE Trans. Inform. Theory*, **32** (1986), 833–836.
- [9] MACWILLIAMS F. J., N. J. A. SLOANE. *The Theory of Error-Correcting Codes*. Amsterdam: North-Holland, 1977.
- [10] PLESS V., N. J. A. SLOANE, H. N. WARD. Ternary codes of minimum weight 6 and the classification of the self-dual codes of length 20. *IEEE Trans. Inform. Theory*, **IT-26** (1980), 305–316.
- [11] PLESS V. A classification of self-orthogonal codes over  $\text{GF}(2)$ . *Discrete Mathematics*, **3** (1972), 209–246.

- [12] PLESS V., N. J. A. SLOANE. On the Classification and Enumeration of Self-Dual Codes. *J. Combinatorial Theory*, **18** (1975), 313–335.
- [13] RAINS E. M. Shadow bounds for self-dual codes. *IEEE Trans. Inform. Theory*, **44** (1998), 134–139.
- [14] YORGOV V. Y. Binary self-dual codes with automorphisms of odd order (in Russian). *Problemi Peredachi Informatcii*, **19** (1983), 11–24, English translation in *Probl. Inform. Transm.* **19** (1983), 260–270.
- [15] YORGOV V. Y. On the extremal binary codes of length 32. In: Proceedings of the 4th Joint Swedish-Russian International Workshop on Information Theory, Gotland, Sweden, 1989, 275–279.
- [16] YORGOVA R. On binary self-dual codes with automorphisms. *IEEE Trans. Inform. Theory*, **54** (2008), 3345–3351.
- [17] [www.gap-system.org](http://www.gap-system.org).

Radinka Yorgova  
CIPR, University of Bergen, Norway  
e-mail: [radinka.yorgova@cipr.uib.no](mailto:radinka.yorgova@cipr.uib.no)

Nuray At  
Dept. of Electrical and Electronics Engineering  
Anadolu University, Turkey  
e-mail: [nat@anadolu.edu.tr](mailto:nat@anadolu.edu.tr)

Received April 2, 2009  
Final Accepted June 11, 2009