Serdica
Mathematical Journal
Сердика
Математическо списание

Serdica Math. J. **27** (2001), 287-302

Serdica
Mathematical Journal

Bulgarian Academy of Sciences
Institute of Mathematics and Informatics

NEW BINARY [70, 35, 12] SELF-DUAL AND BINARY [72, 36, 12] SELF-DUAL DOUBLY-EVEN CODES*

Radinka Dontcheva

Communicated by R. Hill

Abstract. In this paper we prove that up to equivalence there exist 158 binary [70, 35, 12] self-dual and 119 binary [72, 36, 12] self-dual doubly-even codes all of which have an automorphism of order 23 and we present their construction. All these codes are new.

1. Introduction. An $[n, k]$ *linear code* C over the binary field F_2 is a k-dimensional subspace of F_2^n. The *weight* $wt(v)$ of a vector $v \in F_2^n$ is the number of nonzero coordinates of v. If d is the minimum weight of the nonzero vectors of C, C is called an $[n, k, d]$ code. For every pair $u = (u_1, u_2, \ldots, u_n)$, $v = (v_1, v_2, \ldots, v_n) \in F_2^n$ the expression $u.v = u_1.v_1 + u_2.v_2 + \ldots + u_n.v_n \in F_2$ defines an inner product in F_2^n.

The *dual code* $C^\perp$ of code C is defined as $C^\perp = \{v \in F_2^n | \ u.v = 0 \text{ for all } u \in C\}$. If $C = C^\perp$, n must be even and C is called a *self-dual* code. It is obvious that all vectors of a self-dual code have an even weight. A *doubly-even* code is a binary code in which the weight of every vector is divisible by four. Self-dual doubly-even codes exist only when n is a multiple of eight. It is known that for a self-dual $[n, n/2, d]$ code one has (cf. [7])

2000 *Mathematics Subject Classification:* 94B05, 94B60.
Key words: Automorphisms, self-dual codes, weight enumerators.
*This work was supported in part by the Bulgarian NSF under Grant MM-901/99

$$d \leq 4 \left[\frac{n}{24}\right] + 6 \text{ if } n \equiv 22 \pmod{24}$$

and

$$d \leq 4 \left[\frac{n}{24}\right] + 4 \text{ otherwise.}$$

A self-dual code with a minimum weight equal to one of these upper bounds is called *extremal*. The vector $v\sigma$ is obtained from vector v after applying a permutation σ on the coordinates of vector v. The codes C and $C_\sigma = \{v\sigma \mid v \in C\}$ are called *equivalent* codes. If $C = C_\sigma$, then σ is called an *automorphism* of the code C. The set of all automorphisms of the code C forms the *automorphism group* of this code.

The polynomial $W(y) = A_0 + A_1 y + A_2 y^2 + \cdots + A_n y^n$ is called *the weight enumerator* of C, if A_i is the number of the vectors of C with weight i, for $0 \leq i \leq n$. All possible weight enumerators of extremal codes of length up to 72 were derived by Conway and Sloane in [1]. The largest minimum distance for known $[70, 35]$ self-dual codes and for known $[72, 36]$ doubly-even codes is 12. The first example of a $[70, 35, 12]$ code was found by Harada in [3]. Until now there are 35 codes known which are of type $[72, 36, 12]$ (cf. [2]).

For the construction of self-dual codes of lengths 70 and 72 by applying an automorphism of order 23, we use the method developed by Huffman and Yorgov in [4], [8] and [9]. For the sake of completeness we describe this method in *Section* 2. In *Section* 3 we show that there are exactly 158 inequivalent $[70, 35, 12]$ self-dual codes with an automorphism of order 23. In *Section* 4 we present all 119 inequivalent $[72, 36, 12]$ codes which have an automorphism of order 23. All codes presented in *Sections* 3 and 4 are new.

2. Description of the method.

Let C be a binary $[n, n/2, d]$ self-dual code which has an automorphism σ of odd prime order p with c cycles of length p and f fixed points in its decomposition. We shortly say that σ is of type p-(c, f).

Lemma 1 [8]. *Let the self-dual code C have an automorphism of type p-(c, f). Then one has*

(i) $pc \geq \displaystyle\sum_{i=0}^{\frac{(p-1)c}{2}-1} \left\lceil \frac{d}{2^i} \right\rceil$, *where the equality sign does not occur if* $d \leq 2^{\frac{(p-1)c}{2}-2} - 2$;

(ii) if $f > c$, *then* $f \geq \displaystyle\sum_{i=0}^{\frac{(f-c)}{2}-1} \left\lceil \frac{d}{2^i} \right\rceil$, *where the equality sign does not occur if* $d \leq 2^{\frac{(f-c)}{2}-2} - 2$.

Let $\Omega_1, \Omega_2, \ldots, \Omega_c$ be the cycles of length p and let $\Omega_{c+1}, \Omega_{c+2}, \ldots, \Omega_{c+f}$ be the fixed points of σ.

Furthermore we introduce the linear subspaces $F_\sigma(C)=\{v \in C| \ v\sigma = v\}$ and $E_\sigma(C)=\{v \in C| \ wt(v|\Omega_i) \equiv 0 \pmod 2), \ i = 1, \ldots, c+f\}$, where $v|\Omega_i$ is the restriction of v on Ω_i.

Lemma 2 [4]**.** *If the code C is self-dual, then one has $C = F_\sigma(C) \oplus E_\sigma(C)$ and $\dim_{F_2}(E_\sigma(C))=\frac{(p-1)c}{2}$, where $\oplus$ stands for the internal direct sum of two subspaces.*

From Lemma 2 we conclude that the generator matrix of the code C can be represented in the form

$$(1) \qquad G(C) = \begin{array}{c} \textit{cycles} \quad \textit{fixed points} \\ \left(\begin{array}{cc} A & \qquad 0 \\ X & \qquad Y \end{array} \right) \end{array} \quad \begin{array}{l} \} \ G(E_\sigma(C)) \\ \} \ G(F_\sigma(C)) \end{array}$$

We consider the map $\pi : F_\sigma(C) \to F^{c+f}$, defined by $\pi(v|\Omega_i) = v_j$ for some $j \in \Omega_i, \ i = 1, 2, \ldots, c+f$. It is known that $\pi(F_\sigma(C))$ is a binary $\left[c+f, \dfrac{c+f}{2}\right]$ self-dual code ([4]). Every vector of length p can be identified with a polynomial in the factor-ring $F_2[x]/(x^p - 1)$, i.e. $(v_0, v_1, \ldots, v_{p-1})$ corresponds to $v_0 + v_1 x + \cdots + v_{p-1}x^{p-1}$. Let P be the set of even-weight polynomials in $F_2[x]/(x^p - 1)$. It will be clear that P is a cyclic code of length p generated by $x - 1$.

We denote by $E_\sigma(C)^*$ the code $E_\sigma(C)$ with the last f coordinates deleted. For $v \in E_\sigma(C)^*$ we can consider each $v|\Omega_i = (v_0, v_1, \ldots, v_{p-1})$ as a polynomial $\varphi(v|\Omega_i)(x) = v_0 + v_1 x + \cdots + v_{p-1}x^{p-1}$ in P, $i = 1, 2, \ldots, c$. Here, we suppress the i-dependence of the coefficients of the polynomial for the sake of simplicity. In this way we define the map $\varphi : \ E_\sigma(C)^* \to P^c$. It is known ([4]) that $\varphi(E_\sigma(C)^*)$ is a submodule of the P-module P^c and, furthermore, that for each $u, v \in \varphi(E_\sigma(C)^*)$ the orthogonality relation

$$(2) \qquad u_1(x)v_1(x^{-1}) + u_2(x)v_2(x^{-1}) + \cdots + u_c(x)v_c(x^{-1}) = 0$$

holds (cf. [8]).

Let $x^p - 1 = (x-1)h_1(x)h_2(x)\cdots h_s(x)$ be the factorization of $x^p - 1$ into irreducible polynomials over the field F_2. Then $P = I_1 \oplus I_2 \oplus \cdots \oplus I_s$, where the ideal I_j, $j = 1, 2, \ldots, s$ is generated by the polynomial $\dfrac{x^p - 1}{h_j(x)}$. It is well known that, because of the irreducibility of $h_j(x)$, I_j is a field with $2^{(p-1)/s}$

elements, for all values of j (cf. [6]). Thus $M_j = \{u \in \varphi(E_\sigma(C)^*) \mid u_i \in I_j,\ i = 1,2,\dots,s\}$ is a code over the field I_j for $j = 1,2,\dots,s$. It is proved in [8] that $\varphi(E_\sigma(C)^*) = M_1 \oplus M_2 \oplus \cdots \oplus M_s$, where the dimension of $\varphi(E_\sigma(C)^*)$ is equal to $\frac{cs}{2}$ with respect to the ring P.

Lemma 3 [8]**.** *Let C have an automorphism of type p-(c,f). The following transformations lead to codes which are equivalent to C.*

(i) any permutation of the first c cycles of C;

(ii) any permutation of the last f coordinates of C;

(iii) any multiplication of the j-th coordinate of $\varphi(E_\sigma(C)^*)$ by x^{t_j}, where t_j is an integer, $1 \le t_j \le p-1$, for $j = 1,2,\dots,c$;

(iv) any substitution $x \to x^j$, for $j = 1,2,\dots,p-1$ in the polynomials of $\varphi(E_\sigma(C)^*)$.

For the classification of inequivalent codes we use the following invariants.

Let $H_d = (h_{i,j})$ be the $A_d \times n$ matrix the rows of which are all weight d vectors of C. Denote by $n(j_1, j_2)$ the number of integers r such that $h_{r\,j_1} h_{r\,j_2} \neq 0$ for $1 \le j_1 \le j_2 \le n$. Let $S = \{n(j_1, j_2) \mid 1 \le j_1 \le j_2 \le n\}$. We denote the maximum and the minimum of S by M and m, respectively, and the frequency of l, $0 \le l \le A_d$, in the set S by b_l. Each permutation of the columns of H_d, which is in $Aut(C)$, also permutes the rows of H_d and hence, leaves the numbers M, m and b_l invariant for all relevant values of l. Therefore, any two codes with different numbers M, m or b_l are inequivalent.

3. Binary [70, 35, 12] self-dual codes with an automorphism of order 23.

Theorem 1. *Up to equivalence there exist* 158 *binary* $[70, 35, 12]$ *self-dual codes with an automorphism of order* 23.

Proof. Any binary $[70, 35, 12]$ self-dual code has a weight enumerator equal to one of the following two forms (cf. [3]):

$$W(y)=1+2\beta y^{12}+(11730-2\beta-128\gamma)y^{14}+(150535-22\beta+896\gamma)y^{16}+\cdots \tag{3}$$

$$W(y) = 1 + 2\beta y^{12} + (9682 - 2\beta)y^{14} + (173063 - 22\beta)y^{16} + \cdots, \tag{4}$$

where β and γ are undetermined parameters. The only known example of such a code has weight enumerator (3) with $\beta = 416$ and $\gamma = 1$ (see [3]).

Let C be a binary $[70, 35, 12]$ self-dual code with an automorphism σ of order 23. By Lemma 1 it follows that σ is of type $23-(3,1)$. Hence, the code

$\pi(F_\sigma(C))$ is a binary $[4,2]$ self-dual code. The repetition code C_2^2, with generator matrix $\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$ is the only self-dual code with these parameters (see [5]). Therefore we can take as generator matrix of $F_\sigma(C)$ one of the matrices

$$(5)\qquad \left(\begin{array}{c|c} X_i & \begin{matrix} 1 \\ 0 \end{matrix} \end{array} \right),$$

where $X_1 = \begin{pmatrix} \mathbf{1} & \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} \end{pmatrix}$, $X_2 = \begin{pmatrix} \mathbf{1} & \mathbf{0} & \mathbf{1} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} \end{pmatrix}$, $X_3 = \begin{pmatrix} \mathbf{0} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{0} & \mathbf{0} \end{pmatrix}$, $\mathbf{1}$ is the all-one vector and $\mathbf{0}$ is the zero vector, both of length 23.

Let A_i, B_i and D_i be the coefficients in the weight enumerators of the codes C, $F_\sigma(C)$ and $E_\sigma(C)$ respectively. With respect to permutation σ of order 23 the vectors of the code C belong to orbits of length 1 or of length 23. By definition, the vectors which belong to an orbit of length 1, constitute the subcode $F_\sigma(C)$. All non-zero vectors of $E_\sigma(C)$ belong to orbits of length 23. Since all vectors in an orbit have the same weight, it follows that $D_i \equiv 0 \pmod{23}$ and $A_i \equiv B_i (\bmod 23)$.

From (5) we obtain that $B_{24} = 1$, $B_{46} = 1$, $B_{70} = 1$ whereas all other coefficients B_i are equal to zero.

Since $B_{12} = 0$ and $B_{14} = 0$, we have $A_{12} \equiv 0 \pmod{23}$ and $A_{14} \equiv 0 \pmod{23}$. If the weight enumerator is of type (4), this would give that $9682 \equiv 0 \pmod{23}$, which is false. Therefore, the weight enumerator is of type (3).

Since $x^{23} - 1 = (x-1)h_1(x)h_2(x)$, where $h_1(x) = x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1$, $h_2(x) = x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1$ are irreducible polynomials over F_2, it follows that $P = I_1 \oplus I_2$, $I_j = \left\langle \dfrac{x^{23}-1}{h_j(x)} \right\rangle$ for $j = 1, 2$. The idempotents of the fields I_1 and I_2 are $e_1(x) = x^{22} + x^{21} + x^{20} + x^{19} + x^{17} + x^{15} + x^{14} + x^{11} + x^{10} + x^7 + x^5 + 1$ and $e_2(x) = e(x) - e_1(x)$, where $e(x) = x^{22} + x^{21} + \cdots + x$ is the identity of P. So $\varphi(E_\sigma(C)^*) = M_1 \oplus M_2$ and $\dim \varphi(E_\sigma(C)^*) = 3$.

The substitution $x \to x^5$ interchanges $e_1(x)$ and $e_2(x)$ and therefore also M_1 and M_2. So we may assume that $\dim_{I_1}(M_1) \geq \dim_{I_2}(M_2)$. Hence, we may take $\dim_{I_1}(M_1) = 2$ and $\dim_{I_2}(M_2) = 1$. The orthogonality condition (2) implies that M_2 is uniquely determined by M_1. Consider the element $\alpha_1(x) = x^{20} + x^{17} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + +x^{10} + x^7 + x^3 + x + 1$ from I_1 of multiplicative order 89. Using this polynomial we can write $I_1 = \{0,\ \ x^k \alpha_1^t(x) \mid k = 0, 1, \ldots, 22,\ t = 0, 1, \ldots, 88\}$. By applying transformations i), iii) of Lemma 3 and by multiplying rows with nonzero elements of I_1, we always can write the generator matrix of

M_1 in reduced echelon form

(6) $$L_1 = \begin{pmatrix} e_1(x) & 0 & \alpha_1^{t_1}(x) \\ 0 & e_1(x) & \alpha_1^{t_2}(x) \end{pmatrix},$$

where $t_l \in \{0, 1, \ldots, 88\}$, for $l = 1, 2$.

Since the substitution $x \to x^2$ in the row vector $(e_1(x), 0, \alpha_1^{t_1}(x))$ gives rise to an equivalent code, we can restrict ourselves to t_1-values from the set $\{0, 1, 3, 5, 9, 11, 13, 19, 33\}$, the elements of which are the cyclotomic coset representatives mod 2. The set of relevant t_1-values can even be restricted further by multiplying the first row with $\alpha_i^{89-t_1}(x)$, interchanging the first and third coordinates in L_1, and again reducing the matrix to echelon form. All these arguments show that it is sufficient to consider the matrix L_1 of (6) only for $t_1 \in \{0, 1, 3, 5, 13\}$ and $t_2 \in \{0, 1, \ldots, 88\}$

From the orthogonality condition (2) it now follows that $\varphi(E_\sigma(C)^*)$ has a generator matrix

(7) $$L = \begin{pmatrix} e_1(x) & 0 & \alpha_1^{t_1}(x) \\ 0 & e_1(x) & \alpha_1^{t_2}(x) \\ \alpha_1^{t_1}(x^{-1}) & \alpha_1^{t_2}(x^{-1}) & e_2(x) \end{pmatrix},$$

where $t_1 \in \{0, 1, 3, 5, 13\}$, $t_2 \in \{0, 1, \ldots, 88\}$.

So, as a generator matrix of $E_\sigma(C)^*$ we can take a matrix of the form

(8) $$A = \begin{pmatrix} u & o & r_1 \\ o & u & r_2 \\ r_1' & r_2' & v \end{pmatrix},$$

where o is the all-zero 11×23 matrix and u, v, r_1 ,r_2, r_1' and r_2' are all 11×23 circulant matrices with as first rows the vectors which correspond to the polynomials $e_1(x)$, $e_2(x)$, $\alpha_1^{t_1}(x)$, $\alpha_1^{t_2}(x)$, $\alpha_1^{t_1}(x^{-1})$ and $\alpha_1^{t_2}(x^{-1})$, respectively. In this way we prove the following proposition.

Proposition 1. *Any binary* $[70, 35, 12]$ *self-dual code* C *with an automorphism of order* 23 *has a generator matrix of the form*

(9) $$G_i = \left(\begin{array}{c|c} & 0 \\ X_i & 1 \\ \hline & 0 \\ A & \vdots \\ & 0 \end{array}\right), \ i = 1, 2, 3.$$

A computer test showed that only 469 of all possible 3×445 matrices given by (9), generate a $[72,36,12]$ code C. By applying transformations $i)$, $ii)$ and $iii)$ from Lemma 3, we can further reduce this number to 158 inequivalent codes. For these codes we calculate the values of the parameters β and γ of the weight enumerator of C and of the invariants M, m and b_l for $l=0,1,\dots,A_{12}$. All 158 codes C have a weight enumerator (3) with parameters $\gamma=0$ and β=1012, 460 414, 368, 322, 276, 230, 184, and 138.

The values of t_1, t_2, the parameter β and the invariants M, m, b_{12} and b_{13} for the obtained codes are given in Table 1 and Table 2. It appeared that all codes generated by G_3 are equivalent to some of the codes generated by G_1 or G_2.

Table 1. Codes generated by G_1

Code	t_1	t_2	β	M	m	b_{12}	b_{13}
$C_{70,1}$	0	0	1012	506	0		
$C_{70,2}$	0	1	184	64	3	253	115
$C_{70,3}$	5	74	184	64	3	115	138
$C_{70,4}$	1	4	184	92	3	230	161
$C_{70,5}$	1	66	184	92	4	276	230
$C_{70,6}$	3	7	184	92	4	276	207
$C_{70,7}$	3	88	184	92	5	345	253
$C_{70,8}$	1	5	184	69	3	299	115
$C_{70,9}$	1	26	184	69	3	138	115
$C_{70,10}$	1	58	184	69	2	138	207
$C_{70,11}$	5	60	184	69	4	161	161
$C_{70,12}$	5	26	184	66	3	161	184
$C_{70,13}$	13	88	184	66	0	368	115
$C_{70,14}$	1	55	184	65	2	115	299
$C_{70,15}$	13	13	184	70	4	253	138
$C_{70,16}$	0	3	276	138	4	138	299
$C_{70,17}$	3	10	276	138	5	322	115
$C_{70,18}$	3	75	276	138	6	230	207
$C_{70,19}$	1	2	276	96	4	184	207
$C_{70,20}$	13	50	276	96	4	230	184
$C_{70,21}$	1	24	276	96	2	230	138
$C_{70,22}$	13	85	276	96	6	184	161
$C_{70,23}$	1	25	276	115	7	184	322
$C_{70,24}$	3	11	276	115	7	115	460
$C_{70,25}$	3	33	276	115	7	92	253
$C_{70,26}$	1	49	276	115	6	115	207
$C_{70,27}$	3	27	276	115	5	207	161
$C_{70,28}$	5	83	276	115	4	69	299

Code	t_1	t_2	β	M	m	b_{12}	b_{13}
$C_{70,29}$	1	31	276	98	6	115	276
$C_{70,30}$	1	42	276	98	6	230	184
$C_{70,31}$	3	34	276	98	6	253	230
$C_{70,32}$	3	31	276	98	5	184	414
$C_{70,33}$	3	85	276	98	2	230	207
$C_{70,34}$	3	87	276	98	7	230	184
$C_{70,35}$	5	31	276	98	7	322	230
$C_{70,36}$	5	59	276	98	8	138	299
$C_{70,37}$	1	47	276	100	8	69	138
$C_{70,38}$	13	57	276	100	8	115	253
$C_{70,39}$	1	71	276	100	6	92	184
$C_{70,40}$	5	44	276	100	6	115	253
$C_{70,41}$	5	70	276	100	6	276	138
$C_{70,42}$	13	42	276	100	7	161	230
$C_{70,43}$	3	41	276	102	4	276	138
$C_{70,44}$	13	55	276	97	6	138	230
$C_{70,45}$	13	72	276	99	8	161	207
$C_{70,46}$	0	5	138	69	2	115	0
$C_{70,47}$	0	9	138	69	1	69	23
$C_{70,48}$	5	5	138	69	3	46	69
$C_{70,49}$	3	73	138	51	3	92	46
$C_{70,50}$	0	11	230	82	6	322	184
$C_{70,51}$	5	9	230	82	6	276	345
$C_{70,52}$	13	36	230	82	6	299	276
$C_{70,53}$	1	57	230	82	3	276	161
$C_{70,54}$	3	35	230	82	3	138	276
$C_{70,55}$	13	18	230	82	3	299	161
$C_{70,56}$	3	17	230	82	5	253	322
$C_{70,57}$	3	71	230	82	5	230	207
$C_{70,58}$	1	8	230	115	3	299	207
$C_{70,59}$	1	28	230	115	4	345	207
$C_{70,60}$	3	25	230	115	4	299	207
$C_{70,61}$	1	68	230	115	6	207	230
$C_{70,62}$	3	20	230	115	6	207	276
$C_{70,63}$	1	85	230	115	6	276	276
$C_{70,64}$	3	77	230	115	6	299	276
$C_{70,65}$	3	26	230	115	5	299	161
$C_{70,66}$	5	41	230	115	5	276	322
$C_{70,67}$	13	86	230	115	5	207	161
$C_{70,68}$	1	10	230	92	6	299	345
$C_{70,69}$	5	55	230	92	6	391	184
$C_{70,70}$	5	57	230	92	6	230	207

Code	t_1	t_2	β	M	m	b_{12}	b_{13}
$C_{70,71}$	1	27	230	92	3	207	230
$C_{70,72}$	3	18	230	92	5	230	161
$C_{70,73}$	13	31	230	92	5	230	276
$C_{70,74}$	5	66	230	92	5	276	345
$C_{70,75}$	13	21	230	92	5	253	414
$C_{70,76}$	13	33	230	92	5	161	138
$C_{70,77}$	13	44	230	92	4	230	345
$C_{70,78}$	1	44	230	86	4	253	115
$C_{70,79}$	3	15	230	86	3	230	184
$C_{70,80}$	3	43	230	86	3	207	391
$C_{70,81}$	1	56	230	81	2	391	230
$C_{70,82}$	5	22	230	81	6	322	391
$C_{70,83}$	5	27	230	81	5	207	184
$C_{70,84}$	1	62	230	80	4	345	322
$C_{70,85}$	3	81	230	80	3	184	115
$C_{70,86}$	5	65	230	80	7	414	161
$C_{70,87}$	13	22	230	80	5	253	299
$C_{70,88}$	13	73	230	80	6	299	276
$C_{70,89}$	1	63	230	83	6	322	276
$C_{70,90}$	13	75	230	83	6	345	253
$C_{70,91}$	5	36	230	83	4	391	253
$C_{70,92}$	1	70	230	84	5	161	230
$C_{70,93}$	1	77	230	84	5	184	276
$C_{70,94}$	3	9	230	84	4	276	276
$C_{70,95}$	3	79	230	84	6	230	575
$C_{70,96}$	1	86	230	90	2	345	115
$C_{70,97}$	1	12	322	114	6	115	138
$C_{70,98}$	3	60	322	114	9	69	184
$C_{70,99}$	13	38	322	114	9	115	92
$C_{70,100}$	13	11	322	114	5	92	184
$C_{70,101}$	1	15	322	115	8	0	115
$C_{70,102}$	13	54	322	115	9	161	46
$C_{70,103}$	1	73	322	112	7	138	230
$C_{70,104}$	1	82	322	112	7	161	69
$C_{70,105}$	13	69	322	112	7	184	138
$C_{70,106}$	1	76	322	112	9	115	69
$C_{70,107}$	1	83	322	118	4	138	23
$C_{70,108}$	5	29	322	118	10	115	184
$C_{70,109}$	1	84	322	138	7	92	230
$C_{70,110}$	3	22	322	116	8	69	207
$C_{70,111}$	3	61	322	116	9	92	207
$C_{70,112}$	5	81	322	116	6	138	207

Code	t_1	t_2	β	M	m	b_{12}	b_{13}
$C_{70,113}$	3	54	322	120	9	92	161
$C_{70,114}$	5	84	322	113	8	115	115
$C_{70,115}$	13	79	322	117	8	115	138
$C_{70,116}$	1	17	414	152	8	92	92
$C_{70,117}$	1	18	414	161	11	92	0
$C_{70,118}$	5	73	414	161	11	69	46
$C_{70,119}$	3	83	414	144	11	0	69
$C_{70,120}$	1	81	368	138	11	23	115
$C_{70,121}$	5	72	368	138	11	23	23
$C_{70,122}$	5	85	368	138	10	23	69
$C_{70,123}$	3	6	368	128	9	69	138
$C_{70,124}$	5	79	368	128	9	46	46
$C_{70,125}$	5	53	368	128	10	92	46
$C_{70,126}$	3	86	368	130	7	115	46
$C_{70,127}$	1	59	460	162	12	23	23

Table 2. Codes generated by G_2

Code	t_1	t_2	β	M	m	b_{12}	b_{13}
$C_{72,128}$	1	4	184	92	3	230	184
$C_{72,129}$	3	7	184	92	5	161	207
$C_{72,130}$	1	5	184	69	4	322	115
$C_{72,131}$	13	53	184	69	3	184	276
$C_{72,132}$	0	3	276	138	4	414	92
$C_{72,133}$	3	10	276	138	6	184	414
$C_{72,134}$	1	7	276	98	6	161	345
$C_{72,135}$	3	5	276	98	4	184	230
$C_{72,136}$	5	8	276	98	7	299	230
$C_{72,137}$	5	12	276	98	5	138	207
$C_{72,138}$	1	32	276	100	6	184	299
$C_{72,139}$	0	5	138	69	3	138	69
$C_{72,140}$	1	8	230	115	2	322	299
$C_{72,141}$	1	68	230	115	6	299	299
$C_{72,142}$	3	16	230	115	5	207	276
$C_{72,143}$	3	20	230	115	5	299	184
$C_{72,144}$	3	26	230	115	5	184	207
$C_{72,145}$	1	13	230	115	8	92	92
$C_{72,146}$	1	15	230	115	8	92	138
$C_{72,147}$	3	17	230	86	5	276	230
$C_{72,148}$	5	51	230	86	6	437	253
$C_{72,149}$	3	23	230	92	6	529	115
$C_{72,150}$	13	60	230	92	5	299	368

Code	t_1	t_2	β	M	m	b_{12}	b_{13}
$C_{72,151}$	1	40	230	116	7	115	138
$C_{72,152}$	3	51	230	116	9	184	138
$C_{72,153}$	3	35	230	82	2	322	207
$C_{72,154}$	3	71	230	83	5	253	299
$C_{72,155}$	1	16	230	114	7	46	161
$C_{72,156}$	5	6	230	138	7	138	92
$C_{72,157}$	5	53	368	129	11	46	69
$C_{72,158}$	13	52	460	164	12	23	46

These tables imply that all 158 codes are inequivalent, and so Theorem 1 has been proved. □

4. Binary [72, 36, 12] self-dual doubly-even codes with an automorphism of order 23.

Theorem 2. *Up to equivalence there exist* 119 *binary* $[72, 36, 12]$ *self-dual doubly-even codes with an automorphism of order* 23.

Proof. Let D be a $[72, 36, 12]$ self-dual doubly-even code. The weight enumerator for a such code is given in [1], and can be written as

$$W(y)=1+(4398+\alpha)y^{12}+(197073-12\alpha)y^{16}+(18396972+66\alpha)y^{20}+\cdots \tag{10}$$

Suppose that the code D has an automorphism σ of order 23. From Lemma 1 it follows that σ is of type $23-(3,3)$. Hence $\pi(F_\sigma(D))$ is a binary $[6,3]$ self-dual code. According to [5] the only code satisfying these conditions is C_2^3 which has a generator matrix $\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$.

Therefore a generator matrix of $F_\sigma(D)$ can be chosen in the form

$$X = \left(\begin{array}{ccc|ccc} \mathbf{1} & \mathbf{0} & \mathbf{0} & 1 & 0 & 0 \\ \mathbf{0} & \mathbf{1} & \mathbf{0} & 0 & 1 & 0 \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & 0 & 0 & 1 \end{array}\right), \tag{11}$$

where $\mathbf{1}$ is the all-one vector and $\mathbf{0}$ is the zero vector, both of length 23. □

By arguments similar to those in Section 3 we may conclude that the generator matrix of $E_\sigma(D)^*$ is a matrix as defined in (8). Therefore we have the following proposition.

Proposition 2. *Any binary* $[72, 36, 12]$ *self-dual doubly-even code* D *with an automorphism of order* 23 *has a generator matrix of the form*

$$G = \begin{pmatrix} & X & \\ A & & O \end{pmatrix}, \tag{12}$$

where O *is the all zero* 33×3 *matrix.*

A computer check shows that 309 of all the 445 matrices, given by (12) generate a $[72, 36, 12]$ code. Applying transformations *i*), *ii*) and *iii*) of Lemma 3 we obtain that precisely 190 of these codes are equivalent to some of the other 119 codes.

The values for the parameter α in the weight enumerator (10) of the obtained codes are: -3984, -3846, -3708, -3570, -3432, -3294, -3156, -3018 and -1362.

By computing the invariants M, m and b_l, we prove that all remaining 119 codes D are inequivalent.

Two previously known $[72, 36, 12]$ codes (cf. [2]) also have parameter values -3846 and -3708 for α. However, the values of the invariants M, m and b_l for these codes show they are not equivalent to the codes we found.

For the sake of completeness we present all these parameter values in Table 3 and in Table 4 respectively.

Table 3. List of [72,36,12] self-dual double-even codes and their invariants

Code	t_1	t_2	α	M	m	b_{19}	b_{20}	b_{21}
$D_{72,1}$	0	0	-1362					
$D_{72,2}$	0	1	-3846	46	0	92	92	46
$D_{72,3}$	5	26	-3846	46	0	92	69	92
$D_{72,4}$	1	14	-3846	46	0	161	69	69
$D_{72,5}$	1	55	-3846	46	0	69	23	138
$D_{72,6}$	1	26	-3846	26	0	92	92	115
$D_{72,7}$	1	66	-3846	26	0	69	92	46
$D_{72,8}$	0	19	-3846	23	0	184	184	92
$D_{72,9}$	1	4	-3846	22	0	92	46	0
$D_{72,10}$	1	5	-3846	24	0	230	69	0
$D_{72,11}$	5	54	-3846	30	0	115	92	46
$D_{72,12}$	13	26	-3846	46	7	184	23	46
$D_{72,13}$	0	3	-3570	35	0	184	184	138
$D_{72,14}$	1	25	-3570	35	0	253	230	115
$D_{72,15}$	1	38	-3570	35	13	253	207	207
$D_{72,16}$	0	13	-3570	34	8	92	161	92
$D_{72,17}$	1	49	-3570	34	0	138	92	230

Code	t_1	t_2	α	M	m	b_{19}	b_{20}	b_{21}
$D_{72,18}$	3	58	-3570	34	0	115	184	207
$D_{72,19}$	1	2	-3570	46	0	184	253	345
$D_{72,20}$	1	24	-3570	46	0	184	322	138
$D_{72,21}$	1	43	-3570	46	0	184	253	276
$D_{72,22}$	3	36	-3570	46	0	184	299	184
$D_{72,23}$	1	32	-3570	46	0	230	253	115
$D_{72,24}$	1	42	-3570	46	0	230	230	184
$D_{72,25}$	5	31	-3570	46	0	230	253	253
$D_{72,26}$	1	47	-3570	46	0	161	138	115
$D_{72,27}$	1	71	-3570	46	0	161	207	299
$D_{72,28}$	1	7	-3570	46	0	276	322	115
$D_{72,29}$	3	31	-3570	46	0	299	230	184
$D_{72,30}$	3	34	-3570	46	0	207	230	299
$D_{72,31}$	5	20	-3570	46	0	69	322	299
$D_{72,32}$	5	35	-3570	46	0	253	184	253
$D_{72,33}$	3	38	-3570	46	11	207	276	161
$D_{72,34}$	1	9	-3570	69	0	230	230	345
$D_{72,35}$	1	48	-3570	69	12	184	161	322
$D_{72,36}$	5	34	-3570	69	7	161	184	253
$D_{72,37}$	1	34	-3570	33	0	161	322	184

Code	t_1	t_2	α	M	m	b_{19}	b_{20}
$D_{72,38}$	3	10	-3570	33	0	184	92
$D_{72,39}$	3	27	-3570	32	0	161	230
$D_{72,40}$	1	31	-3570	92	0	69	207
$D_{72,41}$	5	59	-3570	31	0	276	115
$D_{72,42}$	0	11	-3708	69	0	184	230
$D_{72,43}$	3	9	-3708	69	0	207	276
$D_{72,44}$	0	33	-3708	69	8	230	138
$D_{72,45}$	1	46	-3708	69	9	299	207
$D_{72,46}$	1	61	-3708	69	6	115	345
$D_{72,47}$	1	3	-3708	46	0	161	184
$D_{72,48}$	3	17	-3708	46	0	161	345
$D_{72,49}$	1	21	-3708	46	0	276	322
$D_{72,50}$	1	77	-3708	46	0	276	207
$D_{72,51}$	3	79	-3708	46	0	276	184
$D_{72,52}$	1	23	-3708	46	0	184	138
$D_{72,53}$	1	56	-3708	46	0	184	230
$D_{72,54}$	1	57	-3708	46	0	184	161
$D_{72,55}$	1	62	-3708	46	0	207	253
$D_{72,56}$	1	70	-3708	46	0	207	138
$D_{72,57}$	3	71	-3708	46	0	207	276

Code	t_1	t_2	α	M	m	b_{19}	b_{20}
$D_{72,58}$	1	63	-3708	46	0	138	322
$D_{72,59}$	3	15	-3708	46	0	391	92
$D_{72,60}$	3	37	-3708	46	0	230	115
$D_{72,61}$	5	36	-3708	46	0	299	92
$D_{72,62}$	3	21	-3708	46	7	276	138
$D_{72,63}$	1	60	-3708	46	9	322	322
$D_{72,64}$	1	8	-3708	28	0	207	115
$D_{72,65}$	1	28	-3708	28	0	184	138
$D_{72,66}$	1	53	-3708	28	0	299	207
$D_{72,67}$	3	63	-3708	28	0	161	230
$D_{72,68}$	1	10	-3708	27	0	207	138
$D_{72,69}$	1	19	-3708	31	8	322	161
$D_{72,70}$	3	18	-3708	31	0	230	253
$D_{72,71}$	3	20	-3708	31	0	184	161
$D_{72,72}$	3	26	-3708	32	0	207	207
$D_{72,73}$	1	27	-3708	33	0	161	184
$D_{72,74}$	1	54	-3708	30	0	368	276
$D_{72,75}$	3	12	-3708	30	0	322	322
$D_{72,76}$	1	68	-3708	29	0	230	207
$D_{72,77}$	5	63	-3708	29	0	184	253
$D_{72,78}$	1	75	-3708	92	0	115	253
$D_{72,79}$	3	6	-3294	92	0	46	46
$D_{72,80}$	1	6	-3294	92	15	0	207
$D_{72,81}$	3	29	-3294	92	15	46	46
$D_{72,82}$	5	18	-3294	92	12	23	69
$D_{72,83}$	1	72	-3294	69	17	46	115
$D_{72,84}$	3	72	-3294	69	0	92	23
$D_{72,85}$	5	52	-3294	69	0	0	115
$D_{72,86}$	1	69	-3294	46	0	0	46
$D_{72,87}$	1	79	-3294	48	0	115	92
$D_{72,88}$	3	62	-3294	115	12	46	23
$D_{72,89}$	1	12	-3432	69	0	138	46
$D_{72,90}$	1	76	-3432	69	0	138	115
$D_{72,91}$	1	16	-3432	69	0	161	92
$D_{72,92}$	1	40	-3432	69	0	184	207
$D_{72,93}$	1	83	-3432	69	0	230	46
$D_{72,94}$	3	51	-3432	69	0	92	69
$D_{72,95}$	3	24	-3432	69	13	115	161
$D_{72,96}$	3	59	-3432	69	9	46	207
$D_{72,97}$	3	69	-3432	69	14	184	161
$D_{72,98}$	1	13	-3432	46	0	138	138

Code	t_1	t_2	α	M	m	b_{19}	b_{20}
$D_{72,99}$	1	15	-3432	46	0	184	207
$D_{72,100}$	1	30	-3432	46	0	46	138
$D_{72,101}$	1	35	-3432	46	0	69	46
$D_{72,102}$	3	40	-3432	46	0	69	92
$D_{72,103}$	3	54	-3432	46	0	161	46
$D_{72,104}$	3	55	-3432	46	0	92	92
$D_{72,105}$	5	10	-3432	46	0	92	138
$D_{72,106}$	1	52	-3432	46	13	138	161
$D_{72,107}$	5	15	-3432	46	11	115	138
$D_{72,108}$	1	84	-3432	41	0	69	161
$D_{72,109}$	3	30	-3432	38	0	46	92
$D_{72,110}$	3	74	-3432	49	0	69	92
$D_{72,111}$	1	17	-3156	54	0	0	69
$D_{72,112}$	1	18	-3156	48	0	46	92
$D_{72,113}$	1	41	-3156	92	18	46	69
$D_{72,114}$	3	49	-3156	69	0	92	23
$D_{72,115}$	3	52	-3156	138	14	46	69
$D_{72,116}$	1	59	-3018	92	0	46	46
$D_{72,117}$	0	5	-3984	18	0	46	
$D_{72,118}$	0	9	-3984	18	0	115	
$D_{72,119}$	1	29	-3984	23	0	46	

Table 4. Other known [72,36,12] self-dual doubly-even codes

Code	α	M	m	*Code*	α
$C_{72,13}$	-3708	35	5	$C_{72,16}$	-3810
$C_{72,21}$	-3846	29	3	$C_{72,17}$	-3798
$C_{72,1}$	-3744			$C_{72,18}$	-3828
$C_{72,2}$	-3774			$C_{72,19}$	-3678
$C_{72,3}$	-3768			$C_{72,20}$	-3816
$C_{72,4}$	-3714			$C_{72,22}$	-3654
$C_{72,5}$	-3762			$C_{72,23}$	-3648
$C_{72,6}$	-3792			$C_{72,24}$	-3690
$C_{72,7}$	-3732			$C_{72,25}$	-3822
$C_{72,8}$	-3702			$C_{72,26}$	-3696
$C_{72,9}$	-3756			$C_{72,27}$	-3660
$C_{72,10}$	-3750			$C_{72,28}$	-3684
$C_{72,11}$	-3738			$C_{72,29}$	-3642
$C_{72,12}$	-3726			$C_{72,30}$	-3672
$C_{72,14}$	-3720			Q_{72}	-1416
$C_{72,15}$	-3786			D_{72}	-3936

Acknowledgment. The author would like to thank the referees for their suggestions, Professor A.J. van Zanten for useful remarks and Professor M. Harada for helpful correspondence.

REFERENCES

[1] J. H. Conway, N. J. A. Sloane. A new upper bound on the minimal distance of self-dual codes. *IEEE Trans. Inform. Theory* **36** (1990), 1319–1333.

[2] S. T. Dougherty, T. A. Gulliver, M. Harada. Extremal binary self-dual codes. *IEEE Trans. Inform. Theory* **43** (1997), 2036–2047.

[3] M. Harada. The existence of a self-dual [70,35,12] code and formally self-dual codes. *Finite Fields Appl.* **3** (1997), 131–139.

[4] W. C. Huffman. Automorphisms of codes with application to extremal doubly-even codes of length 48. *IEEE Trans. Inform. Theory* **28** (1982), 511–521.

[5] V. Pless. A classification of self-orthogonal codes over GF(2). *Discrete Math.* **3** (1972), 209–246.

[6] H. Weyl. Algebraic Theory of Numbers. Princeton University Press, 1945.

[7] E. Rains, N. J. A. Sloane. Self-dual codes. In: Handbook of Coding Theory (Eds V. S. Pless and W. C. Huffman), Elsevier, Amsterdam, 1998, 177–294.

[8] V. Y. Yorgov. Binary self-dual codes with automorphisms of odd order. *Probl. Pered. Inform.* **19** (1983), 11–24 (in Russian).

[9] V. Y. Yorgov. A method for constructing inequivalent self-dual codes with applications to length 56. *IEEE Trans. Inform. Theory* **33** (1987), 77–82.

Faculty of Information Technology and Systems
Delft University of Technology
2628 CD Delft, The Netherlands
On leave from University of Shumen, Bulgaria

Received February 9, 2001
Revised October 3, 2001