МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2001
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2001
Proceedings of Thirtieth Spring Conference of
the Union of Bulgarian Mathematicians
Borovets, April 8–11, 2001

ON THE BINARY SELF-DUAL CODES OF LENGTH 70*

Radinka Alexandrova Dontcheva

In this paper we construct 156 new nonequivalent binary [70,35,12] self-dual codes. They are all possible such codes which have an automorphism of order 23.

1. Introduction. For a binary $[70,35,12]$ self-dual code two possible weight enumerators exist and they are given in [2]:

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

and

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

where β and γ are undetermined parameters.

In 1997 M.Harada [2] found the first example for a binary [70,35,12] self-dual code. This code has weight enumerator (1.1) for $\beta = 416$ and $\gamma = 1$.

Let C be a $[70,35,12]$ code via an automorphism σ of order 23. By *Theorem*1 of [5] it follows that σ can have only 3 cycles - Ω_1, Ω_2, Ω_3 and 1 fixed point - Ω_4. Denote $F_\sigma(C)$=$\{v \in C| \ \ v\sigma = v\}$ and $E_\sigma(C) = \{v \in C| \ \ wt(v|\Omega_i) \equiv 0 \ (mod\ 2), \ i = 1,2,3,4\}$, where $v|\Omega_i$ is the restriction of v on Ω_i. It is known [3] that $C = F_\sigma(C) \oplus E_\sigma(C)$ ($\oplus$ denotes the internal direct sum).

By A_i, B_i and D_i are denoted the coefficients in the weight enumerators of the codes C, $F_\sigma(C)$ and $E_\sigma(C)$ respectively. The permutation σ of order 23 splits the vectors of the code C in orbits of length 1 or 23. Any vector of $F_\sigma(C)$ is in an orbit of length 1. A vector of $E_\sigma(C)$ is in an orbit of length 1 if and only if it is the all zero vector. Hence 23 divides D_i and $A_i \equiv B_i \ (mod\ 23)$ for $i = 12, 14, 16, \ldots, 58$.

The code $F_\sigma(C)$ has the coefficients $B_{24} = 1$, $B_{46} = 1$, $B_{70} = 1$ and any other is equal to zero.

Suppose C has the weight enumerator (1.1). From $A_{12} \equiv 0 \ (mod\ 23)$ and $A_{14} \equiv 0 \ (mod\ 23)$ it follows that $\beta \equiv 0 \ (mod\ 23)$ and $\gamma \equiv 0 \ (mod\ 23)$.

Consider the weight enumerator (1.2). Since $A_{12} \equiv 0 \ (mod\ 23)$ we obtain that $\beta \equiv 0 \ (mod\ 23)$ and then $A_{14} \equiv 22 \ (mod\ 23)$, which contradicts to $A_{14} \equiv 0 \ (mod\ 23)$. Therefore the code C can have only the weight enumerator (1.1).

The map $\pi : F_\sigma(C) \to F^3$ is defined by $\pi(v|\Omega_i) = v_j$ for some $j \in \Omega_i, \ i = 1,2,3$. Hence $\pi(F_\sigma(C))$ is a binary $[4,2]$ self-dual code [3]. Let P be the set of even-weight polynomials in $F_2[x]/(x^{23}-1)$. It is known that P is a cyclic code of length 23 generated by $x+1$. Let $E_\sigma(C)^*$ be the code $E_\sigma(C)$ with the last coordinate deleted. For $v \in E_\sigma(C)^*$

*Author has been supported by UVO-POSTE 875.695.0

we can consider each $v|\Omega_i = (v_0, v_1, \ldots, v_{22})$ as a polynomial $\varphi(v|\Omega_i)(x) = v_0 + v_1x + \cdots + v_{22}x^{22}$ in P, $i = 1,2,3$. Then $\varphi(E_\sigma(C)^*)$ is a submodule of the P- module P^3 [3] and for each $u, v \in \varphi(E_\sigma(C)^*)$ it holds (see [5]):

$$u_1(x)v_1(x^{-1}) + u_2(x)v_2(x^{-1}) + u_3(x)v_3(x^{-1}) = 0. \tag{1.3}$$

2. Results. Suppose C possesses an automorphism σ of order 23 with 3 cycles and 1 fixed point in its decomposition. Then the image $\pi(F_\sigma(C))$ is a binary [4,2] self-dual code. There is only one such code: C_2^2 with generator matrix $gen(C_2^2) = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$ (see [4]). Hence we can choose a generator matrix of $F_\sigma(C)$ in the form:

$$\text{(2.1)}\quad X_1 = \begin{pmatrix} a & a & & 0 \\ & & a & 1 \end{pmatrix},\ X_2 = \begin{pmatrix} a & & a & 0 \\ & a & & 1 \end{pmatrix}\ \ or\ \ X_3 = \begin{pmatrix} & a & a & 0 \\ a & & & 1 \end{pmatrix},$$

where a is the all-one vector of length 23 and non-indicated entries are equal to zero.

Note, that over F_2 $x^{23} - 1 = (x-1)h_1(x)h_2(x)$, 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. Hence $P = I_1 \oplus I_2$, where $I_j =< \dfrac{x^{23}-1}{h_j(x)} >$ for $j = 1,2$ is irreducible cyclic code and $\varphi(E_\sigma(C)^*)$=$M_1 \oplus M_2$. The set $M_j = \{u \in \varphi(E_\sigma(C)^*) \mid u_i \in I_j,\ i = 1,2,3\}$ is a code over the field I_j for $j = 1,2$. The orthogonal idempotents of 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. Denote $\delta_j(x) = \dfrac{x^{23}-1}{h_j(x)}$ for $j = 1,2$. Then $I_j = \{0,\ \delta_j^k(x) \mid k = 0,1,\ldots,2^{11}-2\}$ for $j = 1,2$. The multiplicative order of $\delta_j(x)$ is equal to 23×89 and we can express $\delta_1(x)$ as $x\alpha_1(x)$, where the order of $\alpha_1(x)$ is 89 and then $I_j = \{0,\ x^k\alpha_j^t(x) \mid k = 0,1,\ldots,22,\ t = 0,1,...,88\}$ for $j = 1,2$. The following transformations lead to an equivalent code [5]:

(i) permutation of the first 3 cycles of C;

(ii) multiplication of the j-th coordinate of $\varphi(E_\sigma(C)^*)$ by x^{t_j}, where t_j is an integer, $1 \le t_j \le 22$ for $j = 1,2,3$;

(iii) substitution $x \to x^j$ for $j = 1,2,\ldots 22$ in $\varphi(E_\sigma(C)^*)$.

Since $dim_{I_1}M_1 + dim_{I_2}M_2 = 3$ we may assume that $dim_{I_1}M_1 = 2$. Applying transformations i), ii) and a multiplication with a nonzero element of I_1 we obtain the generator matrix of M_1 in the

$$L = \begin{pmatrix} e_1(x) & 0 & \alpha_1^{t_1}(x) \\ 0 & e_1(x) & \alpha_1^{t_2}(x) \end{pmatrix}, \tag{2.2}$$

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

Using transformations i) and iii) we reduce the pairs $(\alpha_1^0(x),\ \alpha_1^{t_1}(x))$ to 5 nonequivalent cases: $(e_1(x),\ e_1(x))$, $(e_1(x),\ \alpha_1(x))$, $(e_1(x),\ \alpha_1^3(x))$, $(e_1(x),\ \alpha_1^5(x))$ and $(e_1(x),\ \alpha_1^{13}(x))$. Therefore it is sufficient to consider the generator matrix L for M_1 only for $t_1 = 0,1,3,5,13$, $t_2 = 0,1,\ldots,88$. By the orthogonal condition (1.3) from (2.2) we calculate the elements of the corresponding generator matrix of M_2. Hence $\varphi(E_\sigma(C)^*)$ has

Table 1. Codes generated by G_1

$Code$	β	t_1	t_2	$Code$	β	t_1	t_2	$Code$	β	t_1	t_2
$C_{70,1}$	1 012	0	0	$C_{70,21}$	276	1	42	$C_{70,41}$	276	13	55
$C_{70,2}$	184	0	1	$C_{70,22}$	276	1	47	$C_{70,42}$	276	13	57
$C_{70,3}$	184	1	4	$C_{70,23}$	276	1	49	$C_{70,43}$	276	13	72
$C_{70,4}$	184	1	5	$C_{70,24}$	276	1	71	$C_{70,44}$	276	13	85
$C_{70,5}$	184	1	26	$C_{70,25}$	276	3	10	$C_{70,45}$	138	0	5
$C_{70,6}$	184	1	55	$C_{70,26}$	276	3	27	$C_{70,46}$	138	0	9
$C_{70,7}$	184	1	58	$C_{70,27}$	276	3	31	$C_{70,47}$	138	3	73
$C_{70,8}$	184	1	66	$C_{70,28}$	276	3	33	$C_{70,48}$	138	5	5
$C_{70,9}$	184	3	7	$C_{70,29}$	276	3	34	$C_{70,49}$	230	0	11
$C_{70,10}$	184	3	88	$C_{70,30}$	276	3	41	$C_{70,50}$	230	1	8
$C_{70,11}$	184	5	26	$C_{70,31}$	276	3	75	$C_{70,51}$	230	1	10
$C_{70,12}$	184	5	60	$C_{70,32}$	276	3	85	$C_{70,52}$	230	1	27
$C_{70,13}$	184	5	74	$C_{70,33}$	276	3	87	$C_{70,53}$	230	1	28
$C_{70,14}$	184	13	13	$C_{70,34}$	276	5	31	$C_{70,54}$	230	1	44
$C_{70,15}$	184	13	88	$C_{70,35}$	276	5	34	$C_{70,55}$	230	1	56
$C_{70,16}$	276	0	3	$C_{70,36}$	276	5	59	$C_{70,56}$	230	1	57
$C_{70,17}$	276	1	2	$C_{70,37}$	276	5	70	$C_{70,57}$	230	1	62
$C_{70,18}$	276	1	24	$C_{70,38}$	276	5	83	$C_{70,58}$	230	1	63
$C_{70,19}$	276	1	25	$C_{70,39}$	276	13	42	$C_{70,59}$	230	1	68
$C_{70,20}$	276	1	31	$C_{70,40}$	276	13	50	$C_{70,60}$	230	1	70
$C_{70,61}$	230	1	77	$C_{70,83}$	230	5	57	$C_{70,105}$	322	3	61
$C_{70,62}$	230	1	85	$C_{70,84}$	230	5	65	$C_{70,106}$	322	5	29
$C_{70,63}$	230	1	86	$C_{70,85}$	230	5	66	$C_{70,107}$	322	5	81
$C_{70,64}$	230	3	9	$C_{70,86}$	230	13	18	$C_{70,108}$	322	5	84
$C_{70,65}$	230	3	15	$C_{70,87}$	230	13	21	$C_{70,109}$	322	13	11
$C_{70,66}$	230	3	17	$C_{70,87}$	230	13	22	$C_{70,110}$	322	13	38
$C_{70,67}$	230	3	18	$C_{70,89}$	230	13	31	$C_{70,111}$	322	13	54
$C_{70,68}$	230	3	20	$C_{70,90}$	230	13	33	$C_{70,112}$	322	13	69
$C_{70,69}$	230	3	25	$C_{70,91}$	230	13	36	$C_{70,113}$	322	13	79
$C_{70,70}$	230	3	26	$C_{70,92}$	230	13	44	$C_{70,114}$	424	1	17
$C_{70,71}$	230	3	35	$C_{70,93}$	230	13	73	$C_{70,115}$	424	1	18
$C_{70,72}$	230	3	43	$C_{70,94}$	230	13	75	$C_{70,116}$	424	3	83
$C_{70,73}$	230	3	71	$C_{70,95}$	322	1	12	$C_{70,117}$	424	5	73
$C_{70,74}$	230	3	77	$C_{70,96}$	322	1	15	$C_{70,118}$	460	1	59
$C_{70,75}$	230	3	79	$C_{70,97}$	322	1	73	$C_{70,119}$	368	1	81
$C_{70,76}$	230	3	81	$C_{70,98}$	322	1	76	$C_{70,120}$	368	3	6
$C_{70,77}$	230	5	9	$C_{70,99}$	322	1	82	$C_{70,121}$	368	3	86
$C_{70,78}$	230	5	22	$C_{70,100}$	322	1	83	$C_{70,122}$	368	5	53
$C_{70,79}$	230	5	27	$C_{70,101}$	322	1	84	$C_{70,123}$	368	5	72
$C_{70,80}$	230	5	36	$C_{70,102}$	322	3	22	$C_{70,124}$	368	5	79
$C_{70,81}$	230	5	41	$C_{70,103}$	322	3	54	$C_{70,125}$	368	5	85
$C_{70,82}$	230	5	55	$C_{70,104}$	322	3	60				

a generator matrix:

$$L' = \left(\begin{array}{ccc} e_1(x) & 0 & \alpha_1^{t_1}(x) \\ 0 & e_1(x) & \alpha_1^{t_2}(x) \\ \alpha_1^{t_1}(x^{-1}) & \alpha_1^{t_2}(x^{-1}) & e_2(x) \end{array} \right), \quad (2.3)$$

where $t_1 = 0, 1, 3, 5, 13$, $t_2 = 0, 1, \ldots, 88$.

Then the generator matrix of $E_\sigma(C)^*$ is:

$$A = \left(\begin{array}{ccc} u & o & r_1 \\ o & u & r_2 \\ r_1' & r_2' & v \end{array} \right), \quad (2.4)$$

where o is the all-zero 11×23 matrix; the cells u, v, r_1 ,r_2, r_1' and r_2' are 11×23 circulant matrices with first rows the vectors which correspond to 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 2.1. *Any binary* [70,35,12] *self-dual code* C *with an automorphism of order* 23 C *has a generator matrix of the form:*

$$G_i = \left(\begin{array}{cc} \multicolumn{2}{c}{X_i} \\ A & O \end{array} \right), i = 1, 2, 3, \quad (2.5)$$

where O *is the all zero column of length* 33.

A computer test showed that 469 of the all 3×445 matrices (2.5) generate a $[70, 35, 12]$ code C. By transformations i), ii) and iii) we obtain that among them there are only 156 nonequivalent codes. All those have weight enumerator (1.1) with parameters $\gamma = 0$ and β=1 012, 184, 276, 138, 230, 322, 414, 460 or 368.

The values of t_1,t_2 and the parameter β for the obtained codes are given in the Table 1 and Table 2. It occurred that all codes generated by G_3 are equivalent to some of the codes found by G_1 or G_2.

To prove the nonequivalence of the above codes we use the method described in [6]. The result is that the all 156 codes C are nonequivalent.

Table 2. Codes generated by G_2

Code	β	t_1	t_2	*Code*	β	t_1	t_2	*Code*	β	t_1	t_2
$C_{70,126}$	184	1	4	$C_{70,137}$	138	0	5	$C_{70,148}$	230	13	60
$C_{70,127}$	184	1	5	$C_{70,138}$	230	1	8	$C_{70,149}$	322	1	13
$C_{70,128}$	184	3	7	$C_{70,139}$	230	1	68	$C_{70,150}$	322	1	15
$C_{70,129}$	184	13	53	$C_{70,140}$	230	3	16	$C_{70,151}$	322	1	16
$C_{70,130}$	276	0	3	$C_{70,141}$	230	3	17	$C_{70,152}$	322	1	40
$C_{70,131}$	276	1	7	$C_{70,142}$	230	3	20	$C_{70,153}$	322	3	51
$C_{70,132}$	276	1	32	$C_{70,143}$	230	3	23	$C_{70,154}$	322	5	6
$C_{70,133}$	276	3	5	$C_{70,144}$	230	3	26	$C_{70,155}$	368	5	53
$C_{70,134}$	276	3	10	$C_{70,145}$	230	3	35	$C_{70,156}$	460	13	52
$C_{70,135}$	276	5	8	$C_{70,146}$	230	3	71				
$C_{70,136}$	276	5	11	$C_{70,147}$	230	5	51				

Theorem 2.1. *Up to equivalence there exist* 156 *self-dual* [70,35,12] *codes with an automorphism of order* 23.

All codes found in Theorem 2.1 are new.

Acknowledgment. The author would like to thank Professor S. Dodunekov for helpful discussion and Professor M. Harada for sending a copy of [2].

REFERENCES

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

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

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

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

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

[5] S. Topalova. Hadamart matrices of order 44 with automorphism of order 7. Intern. Workshop ACCT, Bansko 2000, 305–310.

Radinka A. Dontcheva
Konstantin Preslavsky University
Faculty of Mathematics and Computer Science
9712 Shoumen, Bulgaria

ВЪРХУ ДВОИЧНИ САМОДУАЛНИ КОДОВЕ С ДЪЛЖИНА 70

Радинка А. Дончева

Конструирани са всички двоични [70,35,12] самодуални кодове с автоморфизъм от ред 23. С точност до еквивалентност съществуват 156 такива кода и всички те са неизвестни до сега.