Fourteenth International Workshop on Algebraic and Combinatorial Coding Theory
September 7–13, 2014, Svetlogorsk (Kaliningrad region), Russia *pp. 97–102*

On the Classificaton of the Binary Self-Dual Codes of Length 40 [1]

Iliya Bouyukliev iliyab@math.bas.bg
Institute of Mathematics and Informatics,
Bulgarian Academy of Sciences, Veliko Tarnovo, Bulgaria
Mariya Dzhumalieva-Stoeva mdzhumalieva@gmail.com
Institute of Mathematics and Informatics,
Bulgarian Academy of Sciences, Veliko Tarnovo, Bulgaria
Venelin Monev venelinmonev@gmail.com
Faculty of Mathematics and Informatics, Veliko Tarnovo University, Bulgaria

Abstract. The results of the complete classification of all binary self-dual codes of length 40 are presented. It is given some additional information about the automorphism groups and the possible weight enumerators of the codes.

1 Introduction

The classification of all binary self-dual codes for a given length is one of the most important problems in constructive coding theory, because self-dual codes have good algebraic properties and they have close connection to combinatorial structures, such as block designs, Hadammard matrices and graphs.

The first classification of binary self-dual codes of length $n \leq 20$ was made by Vera Pless [12]. Later Pless, Conway and Sloane classified the self-dual codes of length $n \leq 30$ [6]. The classification for length 32 is completed by Bilous and Van Rees [3], and the classification of the codes of length 34 was given by Bilous [2]. Melchor and Gaborit classified the optimal self-dual codes of length 36 [11]. Harada and Munemasa completed the classification of the codes of length 36 [7, 8]. Recently the self-dual codes of length 38 were classified by I. Bouyukliev and S. Bouyuklieva [4]. Together with Harada they classified the optimal self-dual codes of length 40 [5]. Betsumiya, Harada and Munemasa gave the classification of the doubly even self-dual codes of length 40 [1].

The main methods for classification are based on a building up construction, which proceeds from smaller to larger length, and test for equivalence of the obtained objects [9]. But the self-dual codes of length 38 and the optimal self-dual codes of length 40 are classified by one new approach, using isomorph free generation [10]. The constructive part of the algorithm for classification is not different from the previous constructions, but it is combined with a parent

[1] This research is supported by the Bulgarian Science Fund under Contract I01/0003/2012.

test (instead of test for equivalence) to take only one representative of any equivalence class.

For the classification of all binary self-dual codes of length 40, we considered two subproblems - classification of the codes with minimum distance ≥ 6, and classification of all self-dual $[40, 20, 4]$ codes. The codes with minimum distance 6 and 8 are classified with the algorithm presented in [4]. The algorithm for classification of the self-dual $[40, 20, 4]$ codes is of the same type but another construction and parent test are implemented.

Throughout this paper all codes are assumed to be binary. Two binary codes are called *equivalent* if one can be obtained from the other by a permutation of coordinates. The permutation $\sigma \in S_n$ is an *automorphism* of C, if $C = \sigma(C)$ and the set of all automorphisms of C forms a group called the *automorphism group* of C, which is denoted by $Aut(C)$ in this paper. If C has length n, then the number of codes equivalent to C is $n!/|Aut(C)|$.

There exists a formula for the number of all self-dual codes of length n, called a mass formula. The number of all self-dual codes of length n is $N(n) = \prod_{i=1}^{n/2-1}(2^i + 1)$. To classify self-dual codes of length n, it is necessary to find inequivalent self-dual codes $C_1, C_2, \ldots, C_r$ so that the following mass formula holds $\sum_{i=1}^{r} n!/|Aut(C_i)| = N(n)$.

2 The constructions

We use two algorithms, based on two different constructions, to obtain the complete classification of the self-dual codes of length 40. The first construction (Theorem 1) is implemented in a recursive algorithm. The same algorithm was used for the classification of self-dual codes of length 38 [4]. It takes as an input the set of the self-dual codes of dimension $k < 19$ and gives as a result all inequivalent self-dual codes of dimension k', $k < k' \leq 20$ (here $k' = 20$).

Theorem 1. *If C is a binary self-dual $[n = 2k > 2, k, d]$ code and the last two coordinates of C are not equal, then C is equivalent to a code with a generator matrix in the form*

$$G = \left(\begin{array}{cccc} x_1 \ldots x_{k-1} & 00\ldots0 & 1 & 0 \\ & & x_1 & x_1 \\ I_{k-1} & A & \vdots & \vdots \\ & & x_{k-1} & x_{k-1} \end{array}\right)$$

and the matrix $(I_{k-1}|A)$ generates a self-dual $[n-2, k-1]$ code.

All inequivalent self-dual $[38, 19]$ and $[36, 18]$ codes are 38 682 183 and 519 492, respectively. More than 70 percent of them have minimum distance 4. Moreover, performing a parent test is a difficult and time consuming process, because these codes don't have trivial automorphism groups. That's why the classification of the self-dual $[40, 20, 4]$ codes separately decreases drastically the complexity of the full classification. Therefore another construction (Theorem 2) is used and another type of parent test is developed.

Theorem 2. *[2] Let C be a binary self-dual $[n, k = n/2, 4]$ code and $x = (110\ldots011)$ be a codeword of weight 4. Then C has a generator matrix in the form*

$$G = \begin{pmatrix} 11 & 00\cdots0 & 00\cdots0 & 1 & 1 \\ 01 & 00\cdots0 & v & 0 & 1 \\ 00 & I_{k-2} & A & a^T & a^T \end{pmatrix}$$

where a and v are binary vectors of length $k-2$. The matrix $(I_{k-2}|A)$ generates a self-dual $[n-4, n/2-2]$ code.

This construction is implemented in the second algorithm, which uses as an input the set of the self-dual codes of dimension k and gives as a result all inequivalent $[2k + 4, k + 2, 4]$ self-dual codes.

The combination of the two algorithms gives us the possibility to classify all binary self-dual codes of length 40.

3 The results

The first algorithm is implemented with *C* programming language in the program *GenSelfDualAllD*. The algorithm for the construction of self-dual codes with minimum distance 4, presented in the previous section, is implemented in the program *GenSelfDualD4*. These two programs, as well as detailed manuals, will be available soon on the web-page `http://www.moi.math.bas.bg/~iliya/`, so anyone could repeat our calculations.

We use a computer with two CPU Intel(R) Xeon(R) E5, 6 Core, and a computer with CPU Intel(R) Core(TM) i7, 4 Core. The complete result for classification of the self-dual codes of length 40, is obtained by the two programs for about a month. As an input of both of the programs the codes of length 36 with their generator matrices are used. There are 519 492 inequivalent $[36, 18]$ self-dual codes. They are separated into 52 intervals with 10000 codes each, except the last one, which is smaller. Each program runs on each interval and produces four files with information about the codes obtained during the calculation on the interval. The first file contains five values for each code - the numbers of codewords with minimum distances $d = 2$, $d = 4$, $d = 6$ and $d = 8$ (partial weight enumerator), as well as the orders of the automorphism groups of the codes. The second file contains mass formulas. The third file contains the number of the self-dual $[40, 20]$ codes, constructed from codes of the given input interval. In the last file we print generator matrices of those self-dual codes, which have order of automorphism group greater than a fixed number. The size of all files, generated during the classification, is 122 GB.

After generalizing the information, we obtained the following results: the number of all self-dual $[40, 20, 4]$ codes is 4 329 329 746. The number of all codes, considered by the program GenSelfDualD4 is 20 614 314 107, for 5 226 244 513 of them, a canonical form is computed. Further, the number of the self-dual codes of length 40 with minimum distances 6 and 8 is 3 882 046 152. 131 822 097 145 codes are considered by the program GenSelfDualAllD, and for 6 563 895 920 of them the canonical form is computed.

The number of the self-dual codes of length 40 is 8 250 058 081. In Table 1 we give the number of all codes by minimum distances, and how many of them are doubly-even. The number of the different partial weight enumerators and the number of the different orders of automorphism groups for each minimum distance d are listed. In Table 2 the smallest order of an automorphism group Aut_s and the largest order of an automorphism group Aut_l are given, again for each minimum distance d.

Table 1: Number of inequivalent codes of length 40

d	4	6	8
# codes	4 329 329 746	3 871 829 027	10 217 125
# doubly-even codes [1]	77 873		16 470
# partial weight enumerators	18 460	199	10
# orders of $Aut(C)$	1 112	94	91

Table 2: Orders of the automorphism groups

d	4	6	8
Aut_s	4	1	1
Aut_l	1275541328062914232320000	14745600	82575360

In the next tables we give some more information about the properties of the self-dual codes of length 40.

We would like to point out two codes as exceptions. They are the unique codes with the correspomding weight enumerators and automorphism groups. The first code C_1 is singly-even and the second one C_2 is doubly-even. They have very big automorphism groups: $|Aut(C_1)| = 1316348119775969280000$ and $|Aut(C_2)| = 1275541328062914232320000$. Their weight enumerators are

Table 3: The most common orders of automorphism groups

$d = 2$	# codes	10537172	10140257	6864707
	$\vert Aut(C)\vert$	8	2	32
$d = 4$	# codes	2532173617	1066608320	365208531
	$\vert Aut(C)\vert$	4	16	64
$d = 6$	# codes	3841168936	28685425	1621556
	$\vert Aut(C)\vert$	1	2	4
$d = 8$	# codes	9987996	189687	24717
	$\vert Aut(C)\vert$	1	2	4

Table 4: The most common partial weight enumerators

$d = 2$	# codes	1084280	1068254	1007808
	$W'(z)$	$z^2 + 9z^6 + 189z^8$	$z^2 + 10z^6 + 191z^8$	$z^2 + 8z^6 + 187z^8$
$d = 4$	# codes	183734248	179135519	173643537
	$W'(z)$	$z^4 + 8z^6 + 149z^8$	$z^4 + 9z^6 + 151z^8$	$z^4 + 7z^6 + 147z^8$
$d = 6$	# codes	358251949	348080056	333531803
	$W'(z)$	$7z^6 + 139z^8$	$6z^6 + 137z^8$	$8z^6 + 141z^8$
$d = 8$	# codes	4674608	3597997	1511827
	$W'(z)$	$141z^8$	$125z^8$	$157z^8$

$W_1(y) = 1 + 126y^4 + 128y^6 + 2541y^8 + 4480y^{10} + 19048y^{12} + 34944y^{14} + 62738y^{16} + 222592y^{18} + 355380y^{20} + 222592y^{22} + 62738y^{24} + 34944y^{26} + 19048y^{28} + 4480y^{30} + 2541y^{32} + 128y^{34} + 126y^{36} + y^{40}$.

$W_2(y) = 1 + 190y^4 + 4845y^8 + 38760y^{12} + 125970y^{16} + 709044y^{20} + 125970y^{24} + 38760y^{28} + 4845y^{32} + 190y^{36} + y^{40}$.

References

[1] K. Betsumiya, M. Harada, A. Munemasa, A complete classification of doubly even self-dual codes of length 40, *Electronic J. Combin.,* **19**, P18, 2012.

[2] R.T. Bilous, Enumeration of the binary self-dual codes of length 34, *J.Combin. Math. Combin. Comput.,* **59**, 173-211, 2006.

[3] R.T. Bilous, G.H.J. Van Rees, An enumeration of binary self-dual codes of length 32, Designs, Codes and Cryptography, **26**, 61-68, 2002.

Table 5: Number of partial weight enumerators and orders of Aut(C) with unique representatives

d	2	4	6	8
# orders of $Aut(C)$	268	241	27	26
# partial weight enumerators	2597	3600	15	0^*

* For $d = 8$ the smallest number is 120 for $W'(z) = 253z^8$

[4] S. Bouyuklieva and I. Bouyukliev, An algorithm for classification of binary self-dual codes, *IEEE Trans. Inform. Theory,* **58**, 3933-3940, 2012.

[5] S. Bouyuklieva, I. Bouyukliev and M. Harada, Some extremal self-dual codes and unimodular lattices in dimension 40, *Finite Fields Appl.,* **21**, 67-83, 2013.

[6] J. H. Conway, V. Pless, N.J.A.Sloane, The binary self-dual codes of length up to 32: a revised enumeration, *Journ. Combin. Theory, ser. A,* **60**, 183-195, 1992.

[7] M. Harada and A. Munemasa, Classification of self-dual codes of length 36, *Advances Math. Communications,* **6**, 229-235, 2012.

[8] M. Harada and A. Munemasa, Database of Self-Dual Codes, Online available at http://www.math.is.tohoku.ac.jp/ munemasa/selfdualcodes.htm

[9] W.C.Huffman, On the Classification and enumeration of self-dual codes, *Finite Fields Appl.* **11**, 451-490, 2005.

[10] B. D. McKay, Isomorph-free exhaustive generation, *J. Algorithms,* **26**, 306–324, 1998.

[11] C.A.Melchor, P.Gaborit, On the classification of extremal [36,18,8] binary self-dual codes, *IEEE Trans. Inform. Theory*, **54**, 4743-4750, 2008.

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