SAT-1.405B-1-MIP-01

EXTENDING RESULTS FOR SOME BINARY SELF-DUAL CODES OF LENGTHS 62 AND 64*

Milena Nikolova, Assist.
Faculty of Mathematics and Informatics, Shumen University,
E- mail: nicolova_m@abv.bg

Nikolay Yankov, Assoc. Prof. DSc.
Faculty of Mathematics and Informatics, Shumen University
E-mail: n.yankov@shu-bg.net

Abstract: *The aim of this paper is to try to find new optimal self-dual codes of lengths 64 and 66 using previously known codes. We begin with an outline of the previous results regarding codes of these lengths. We then extend some known binary self-dual codes of length 62 to singly-even binary self-dual* $[64,32,12]$ *codes using a known method of Harada and Kimura. As a result we find 8 new singly-even binary self-dual* $[64,32,12]$ *codes and discuss their connection to the codes of length 62. We conclude with another result by extending the doubly-even* $[64,32,12]$ *self-dual codes with an automorphism of type 31-(2, 2) to 35 new* $[66,33,12]$ *self-dual codes. Two of these new codes that we obtain have an automorphism of type 5-(12, 6) and codes with this type of automorphism previously were not known to exist.*

Keywords: *automorphism; extension; code; self-dual code.*

INTRODUCTION

A *linear* $[n,k]$ *code C* is a *k*-dimensional subspace of the vector space F_q^n, where F_q is the finite field of *q* elements. The elements of *C* are called *codewords* and the (Hamming) *weight* of a codeword is the number of its nonzero coordinate positions. The *minimum weight d* of *C* is the smallest weight among all nonzero code words of *C*, and *C* is called an $[n,k,d]$ code.

A matrix which rows form a basis of *C* is called a *generator matrix* of this code. The weight enumerator $W(y)$ of a code *C* is given by $W(y)=\sum_{i=0}^{n} A_i y^i$, where A_i is the number of codewords of weight *i* in *C*. Let $(u,v): F_q^n \times F_q^n \to F_q$ be an inner product in the linear space F_q^n. The *dual code* of *C* is $C^{\perp}=\left\{u \in F_q^n : (u,v)=0 \text{ for all } v \in C\right\}$. The dual code $C^{\perp}$ is a linear $[n,n-k]$ code. We call the code *C self-orthogonal* if $C \subseteq C^{\perp}$. If $C=C^{\perp}$ then the code *C* is termed *self-dual*.

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 congruent 2 modulo 4. Self-dual doubly-even codes exist only when *n* is divisible by eight.

The codes with the largest possible minimum weight among all self-dual codes of a given length are named *optimal* self-dual codes. For self-dual codes, Rains [8] provided new upper bounds for the minimum weight

$$d \le \begin{cases} 4\left\lfloor \frac{n}{24} \right\rfloor + 4, \text{when } n \not\equiv 22 (\text{mod } 24) \\ 4\left\lfloor \frac{n}{24} \right\rfloor + 6, \text{when } n \equiv 22 (\text{mod } 24) \end{cases}$$

* This paper is supported by Shumen University under Grants RD-08-144/08.02.2016 and RD-08-103/-05.02.2016.

Two binary codes are *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 $C = \sigma(C)$. We say that a permutation $\sigma \in S_n$ is of type $p-(c,f)$ if there are c cycles of length p and f fixed points in its decomposition into disjoint cycles. The set of all automorphisms of C forms a group, called the *automorphism group* $\mathrm{Aut}(C)$ of C. Some researchers on self-dual codes work towards full classification of all inequivalent codes for a given length. The last results in this regards are for length 38 by Bouyuklieva and Bouyukliev [1] and for length 40 by Bouyukliev et al. [3]. In both of these cases a complete classification is given.

Most of the possible weight enumerators for optimal binary self-dual codes of smaller lengths are known however for the larger lengths the results are scarce. The largest n for which there are integer parameters in the weight enumerators of an optimal singly-even binary self-dual $[2n,n,d]$ code and all possible parameter values are known is $n = 52$ (see [10]). Thus an interesting question is to find new values of the integer parameters in the weight enumerators of optimal singly-even binary self-dual codes. One possible approach is to classify all such codes that possess certain automorphism of odd prime order. However it is possible that some of the values of these parameters may be achieved only by codes with trivial automorphism group. This means that we need to look also for optimal binary self-dual codes with trivial automorphism group. Next we look at the weight distributions of the optimal binary self-dual codes for the code lengths we will consider.

There is one possible weight enumerator for a doubly-even binary self-dual $[64,32,12]$ code: $W_{64}(y) = 1 + 2976y^{12} + 454956y^{16} + 18275616y^{20} + \cdots,$

and two possible weight enumerators for a singly-even code (see [4]):

$$W_{64,1}(y) = 1 + (1312 + 16\beta)y^{12} + (22016 - 64\beta)y^{14} + \cdots,$$

where $14 \le \beta \le 104$ and

$$W_{64,2}(y) = 1 + (1312 + 16\beta)y^{12} + (23040 - 64\beta)y^{14} + \cdots,$$

where $0 \le \beta \le 277.$

Codes exist with all three weight enumerators and it is interesting to find all possible values of the parameter β for which there exists a singly-even code with either $W_{64,1}(y)$ or $W_{64,2}(y)$. Currently the following values for β are known:

- in $W_{64,1}(y)$: 14, 18, 20, 22, 24, 25, 26, 29, 30, 32, 34, 36, 38, 39, 44, 46, 53, 59, 60, 64, and 74.
- in $W_{64,2}(y)$: 0,..,18, 20,..,30, 32, 33, 35, 36, 37, 38, 40, 41, 44, 48, 51, 52, 56, 58, 64, 65, 72, 80, 88, 96, 104, 108, 112, 114, 118, 120, and 184.

Next, we give the three possible weight enumerators for a binary self-dual $[66,33,12]$ codes, which were first published also in [4]:

$$W_{66,1}(y) = 1 + 1690y^{12} + 7990y^{14} + 302705y^{16} + 867035y^{18} + 13196014y^{20} + \ldots,$$

$$W_{66,2}(y) = 1 + (858 + 8\beta)y^{12} + (18678 - 24\beta)y^{14} + (201201 - 48\beta)y^{16} + \ldots,$$

where $0 \le \beta \le 778$ and

$$W_{66,3}(y) = 1 + (858 + 8\beta)y^{12} + (18166 - 24\beta)y^{14} + (205809 - 48\beta)y^{16} + \ldots,$$

where $14 \le \beta \le 756.$

There are a total of 102 known codes with $W_{66,1}$: two with an automorphism of type 5-(12,6) from [9] and 100 with trivial automorphism group from [6]; with $W_{66,2}$ for $\beta = 0$, 1,2,3,5,6,8,...,11,14,..., 39, 40,..., 56, 59,...,69,71,...,90,92,94,100,101,115; and with $W_{66,3}$ for $\beta = 28$,...,38,44,...,64,66,67,70,71, 73,...,88,90,92 (see [12], and [7])

I. CONSTRUCTION METHOD

In this paper, we are using a technique due to Harada and Kimura [5] which allows us to obtain new binary self-dual codes of length 2*n*+2 using known codes of length 2*n*.

Theorem 1 [5] Let *G* be a generator matrix of a self-dual code *C* of length 2*n*, and let $x = (x_1,\ldots,x_n,x_{n+1},\ldots,x_{2n})$ be a vector in F_2^{2n} such that $(x,x) = 1$, where (,) denotes the Euclidean inner product. Let $y_i = (x,r_i)$ for $1 \le i \le n$, where r_i is the *i*-th row vector of *G*. Then the following matrix $G' = \begin{pmatrix} 1 & 0 & x_1 & \ldots & x_i & \ldots & x_{2n} \\ y_1 & y_1 & & & & & \\ \vdots & \vdots & & & G & & \\ y_n & y_n & & & & & \end{pmatrix}$ generates a self-dual code *C′* of length $2n+2$.

Corollary 1 [5] Let *S* be a subset of the set $1,2,\ldots,n$ such that $|S|$ is odd if $2n \equiv 0 \pmod 4$ and $|S|$ is even if $2n \equiv 2 \pmod 4$. Let $G = (I_n \mid A)$ be a generator matrix in standard form of a self-dual code *C* of length 2*n*. Suppose that $x_i = 1$ if $i \in S$ and $x_i = 0$ if $i \notin S$ and that $y_i = x_i + 1$ for $1 \le i \le n$. Then the following matrix:

$$G' = \begin{pmatrix} 1 & 0 & x_1 & \ldots & x_n & 1 & \ldots & 1 \\ y_1 & y_1 & & & & & & \\ \vdots & \vdots & & & I_n & & & A \\ y_n & y_n & & & & & & \end{pmatrix}$$

generates a self-dual code *C′* of length 2*n*+2.

II. EXTENDING [62, 31, 12] CODES TO NEW SELF-DUAL [64, 32, 12] CODES

According to [11] there are exactly 8 inequivalent binary self-dual $[62,31,12]$ codes having an automorphism of type 7–(8, 6). Denote these codes by $C_{62,i}, i = 1,\ldots,8.$ For the next code length: there are 44465 doubly-even and 557 singly-even $[64,32,12]$ self-dual codes having an automorphism of type 7–(8, 8).

We start with the generator matrices of the 8 self-dual $[62,31,12]$ codes in the standard form in order to use Corollary 1 for all possible subsets *S* of the set $1,2,\ldots,31$. In our case $2n \equiv 2 \pmod 4$ so we consider only sets with even cardinality thus we need to calculate all $\frac{1}{2}2^{31} = 2^{30} = 1\,073\,741\,824$ self-dual codes of length 64 and consider only the ones with minimum distance $d = 12.$

Proposition 1 There exist exactly 8 inequivalent singly-even binary self-dual [64, 32, 12] codes obtained via extending the binary self-dual $[62,31,12]$ codes having an automorphism of

type 7–(8, 6). Conversely, only 8 of the singly-even $[64,32,12]$ self-dual codes having an automorphism of type 7–(8, 8) can be shortened to 7 of the binary self-dual $[62,31,12]$ codes.

We give the results from the previous statement in Table 1.

III. EXTENDING [64, 32, 12] CODES TO NEW SELF-DUAL [66, 33, 12] CODES

In this section we use the 35 binary $[64,32,12]$ self-dual codes $C_{64,i}, i=1,\ldots,35$ with an automorphism of type 31-(2,2) from [13] (note that 3 of the 38 codes in this paper are actually equivalent to other codes). Our goal is to extend these codes using again Corollary 1. We summarize our results in the following.

Proposition 2 There exist exactly 35 inequivalent singly-even binary self-dual $[66,33,12]$ codes obtained via extending the doubly-even binary self-dual $[64,32,12]$ codes having an automorphism of type 31–(2, 2). Two of the binary self-dual $[66,33,12]$ codes have automorphism of type 5-(12, 6) and all others have trivial automorphism group.

Table 1. Results on extending binary self-dual [62, 31, 12] codes to binary self-dual [64, 32, 12] codes

	Number of codes obtained	$\lvert \mathrm{Aut}(C) \rvert$	$W_{64,i}(y),\beta$
$C_{62,1}$	1	14	$i=1,\beta=18$
$C_{62,2}$	1	14	$i=1,\beta=18$
$C_{62,3}$	2	28	$i=1,\beta=18$
		168	$i=2,\beta=37$
$C_{62,4}$	1	42	$i=2,\beta=16$
$C_{62,5}$	1	14	$i=1,\beta=32$
$C_{62,6}$	–	–	–
$C_{62,7}$	1	42	$i=2,\beta=30$
$C_{62,8}$	1	14	$i=1,\beta=18$

Table 2. Generators of the new $[66,33,12]$ codes obtained via extending the $[64,32,12]$ codes with an automorphism of type 31-(2,2)

code	number of codes obtained	generators $(x_1,\ldots,x_{32})$ in hexadecimal
$C_{64,1}$	1	0B0AA252
$C_{64,2}$	1	06D4DD5E
$C_{64,5}$	1	025087D4
$C_{64,6}$	2	04F2CCDA, 0AE639D2
$C_{64,7}$	1	03BF1B84
$C_{64,8}$	2	01523F1A, 06F159F0
$C_{64,15}$	1	052876B4

$C_{64,16}$	4	007FFE6E, 029655A6, 056D8B56, 12461BA0
$C_{64,17}$	2	02C32A4C, 0E1D9AD8
$C_{64,18}$	1	005D753E
$C_{64,19}$	1	07218EF6
$C_{64,21}$	1	06E468B8
$C_{64,23}$	3	0039B6F0, 00860E80, 072BCECE
$C_{64,25}$	2	042260B2, 0A8D58A6
$C_{64,29}$	1	00D492F6
$C_{64,31}$	6	01E0A034, 03AE2D9C, 05770316, 07FAB26A, 08613FA8, 0F0DBAB6
$C_{64,33}$	3	0004A238, **00077E42**, 001AFC36
$C_{64,34}$	2	0018487C, **003C907C**

Remark 1 All binary self-dual $[66,33,12]$ codes that we have constructed in this research have weight enumerator $W_{66,1}(y)$. The two codes (for $C_{64,33}$ with 00077E42 and $C_{64,34}$ with 003C907C) with nontrivial automorphism group have automorphism group of order 5, automorphism of type 5-(12, 6), and are the first known codes with such automorphism group. None of the codes we obtain are equivalent to the codes from [9] and [6] therefore are new. We give the generating vectors for all new codes from this section in Table 2.

Remark 2 In this research all code constructions and minimum distance tests were achieved using own programs in Delphi. For equivalence check we use the software system Q-extensions by Iliya Bouyukliev [2]

REMARK

Remark 1 All binary self-dual $[66,33,12]$ codes that we have constructed in this research have weight enumerator $W_{66,1}(y)$. The two codes (for $C_{64,33}$ with 00077E42 and $C_{64,34}$ with 003C907C) with nontrivial automorphism group have automorphism group of order 5, automorphism of type 5-(12, 6), and are the first known codes with such automorphism group. None of the codes we obtain are equivalent to the codes from [9] and [6] therefore are new. We give the generating vectors for all new codes from this section in Table 2.

Remark 2 In this research all code constructions and minimum distance tests were achieved using own programs in Delphi. For equivalence check we use the software system Q-extensions by Iliya Bouyukliev [2]

REFERENCES

[1] Bouyuklieva S., I. Bouyukliev, An Algorithm for Classification of Binary Self-Dual Codes, IEEE Trans. Inf. Theory, vol. 58(6), pp. 3933–3940, 2012.

[2] Bouyukliev, I. About the code equivalence, Advances in Coding Theory and Cryptography. Series on coding theory and cryptology, vol. 3. World Scientific Publishing, pp. 126–151, 2007.

[3] Bouyukliev I., M. Dzhumalieva-Stoeva, and V. Monev, Classification of Binary Self-Dual Codes of Length 40, IEEE Trans. Inf. Theory, vol. 61(8), pp. 4253–4258, 2015.

[4] Dougherty, S.T., T.A. Gulliver, M. Harada, Extremal binary self-dual codes, IEEE Transactions on Information Theory, vol. 43(6), pp. 2036–2047, 1997.

[5] Harada, M., H. Kimura, On extremal self-dual codes, Math. J. Okayama Univ., vol. 37, pp. 1–14, 1995.

[6] Harada, M. T. Nishimura, and R. Yorgova, New Extremal Self-Dual Codes of Length 66, Math. Balk. (N. S.), vol. 21, no. 1–2, pp. 113–121, 2007.

[7] Kaya, A., New extremal binary self-dual codes of lengths 64 and 66 from bicubic planar graphs, arXiv:1604.00486, 2016.

[8] Rains E.M., Shadow bounds for self-dual codes. IEEE Trans. Inform. Theory, vol. 44(1), pp. 134–139, 1998.

[9] Tsai, H.-P., Extremal self-dual codes of lengths 66 and 68, IEEE Transactions on Information Theory, vol. 45(6), pp. 2129–2133, 1999.

[10] Yankov, N., M.-H. Lee, New binary self-dual codes of lengths 50–60, Designs, Codes and Cryptography, vol. 73 (3), pp. 983–996, 2014.

[11] Yankov, N. Self-dual [62, 31, 12] and [64, 32, 12] codes with an automorphism of order 7, Advances in Mathematics of Communications, Vol. 8, No. 1, pp. 73–81, 2014.

[12] Yankov, N., M.-H. Lee, M. Gurel, M. Ivanova, Self-dual codes with an automorphism of order 11, IEEE Transactions on Information Theory, vol. 61(3), pp. 1188–1193, 2015.

[13] Yorgov, V.Y., Binary self-dual codes with an automorphism of odd order, Problems Information Transmission, vol. 4, pp. 13–24 (in Russian), 1983.

