ISBN 89-88081-90-0
ISSN 1975-5635

The 19th International Workshop on

Multimedia Signal Processing & Transmission

MSPT

World Class University



20 Feb. 2013

Chonbuk National University. Korea

WCU-Ⅱ Center of MIMO-OFDM Coded Cooperative Wireless Networks

Mid-career Research Program (MEST)

IT Convergence Research Center

Chonbuk National University

New [54,27,10] Binary Self-Dual Codes Obtained via Extending Technique

Nikolay I. Yankov
Shumen University, Bulgaria
Moon Ho Lee
Chonbuk National University, Korea

New $[54, 27, 10]$ binary self-dual codes obtained via extending technique

Nikolay I. Yankov
Faculty of Mathematics and Informatics
Shumen University
Shumen, 9700, Bulgaria
Email: jankov_niki@yahoo.com

Moon Ho Lee
Institute of Information and Communication
Chonbuk National University
Jeonju, 561-756, R. Korea
Email: moonho@chonbuk.ac.kr

Abstract

Using a method for extending self-dual codes, applied on optimal binary self-dual codes of length 52 with an automorphism of type $5-(10,2)$, we obtain new $[54, 27, 10]$. There are exactly 1503 inequivalent singly-even binary self-dual $[54, 27, 10]$ codes with both weight enumerators $W_{54,1}$ and $W_{54,2}$ for $\beta \geq 20$, most of which are new. We have obtained codes with new value of the parameter in their weight enumerators for the second type of enumerator. This new values is $\beta = 25$. This brings the open values of the parameter β to: $\beta = 23, 24, 25$ or $27 \leq \beta \leq 43$ for $W_{54,1}$; and $28 \leq \beta \leq 43$ for $W_{54,2}$.

Index Terms

automorphisms; block codes; extending; self-dual codes; weight enumerator

I. Introduction

Let $\mathbb{F}_q^n$ be the n-dimensional vector space over the field $\mathbb{F}_q$ of q elements. A linear $[n,k]_q$ *code* C is a k-dimensional subspace of $\mathbb{F}_q^n$. An element of C is called a *codeword*. The *Hamming weight* of a vector $v \in \mathbb{F}_q^n$ (denoted by $\mathrm{wt}(v)$) is the number of its non-zero coordinates. The *minimum weight* d of a code C is the smallest weight among its nonzero codewords. A code with minimum weight d is called an $[n,k,d]$ code. A generator matrix of a code C is a matrix whose rows form a basis of C. We say that a generator matrix G is in *standard form* if $G = (I_k|A)$, where I_k denotes the $k \times k$ identity matrix.

The *weight enumerator* $W(y)$ of a code C is given by $W(y) = \sum_{i=0}^{n} A_i y^i$ where $A_i = |\{v \in C | \mathrm{wt}(v) = i\}|$. 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 $\mathrm{Aut}(C)$ in this paper.

Let $(u,v) \in \mathbb{F}_q$ for $u, v \in \mathbb{F}_q^n$ be an inner product in $\mathbb{F}_q^n$. We study binary self-dual codes and when the base field is $\mathbb{F}_2$ we have for $u = (u_1, \ldots, u_n)$, $v = (v_1, \ldots, v_n) \in \mathbb{F}_2^n$ the following Euclidean inner product: $(u,v) = \sum_{i=0}^{n} u_i v_i \in \mathbb{F}_2$.

The *dual code* of an $[n,k]$ code C is defined as

$$C^{\perp} = \left\{ u \in \mathbb{F}_q^n | (u,v) = 0 \text{ for all } v \in C \right\}.$$

The dual $C^{\perp}$ is a linear $[n, n-k]$ code. If $C \subseteq C^{\perp}$, C is termed *self-orthogonal*, and if $C = C^{\perp}$, C is *self-dual*. Every self-dual code C have dimension $k = \frac{n}{2}$. The largest possible minimum weights of singly even self-dual codes of lengths up to 72 are determined in [6]. It was also shown [10] that the minimum weight d of a binary self-dual code of length n is bounded by

$$d \leq \begin{cases} 4\lfloor \frac{n}{24} \rfloor + 4, & \text{if } n \not\equiv 22 \pmod{24}; \\ 4\lfloor \frac{n}{24} \rfloor + 6, & \text{if } n \equiv 22 \pmod{24}. \end{cases} \tag{1}$$

We call a self-dual code meeting this upper bound *extremal*. A self-dual code is called *optimal* iff it is not extremal but has the largest minimum weight for its length. The weight enumerators of the optimal self-dual codes of lengths from 52 and 54 are known [6] and [1]:

- $[52, 26, 10]$: There are two possible forms for the weight enumerator

  $$W_{52,1} = 1 + 250y^{10} + 7980y^{12} + 42800y^{14} + \cdots,$$

  and

  $$W_{52,2} = 1 + (442 - 16\beta)y^{10} + (6188 + 64\beta)y^{12} + \cdots,$$

  where $0 \leq \beta \leq 12, \beta \neq 11$.
  Codes exist for $W_{52,1}$ and for $W_{52,2}$ for all values of β (see [14]).
- $[54, 27, 10]$: There are two possible forms for the weight enumerator

  $$W_{54,1} = 1 + (351 - 8\beta)y^{10} + (5031 + 24\beta)y^{12} + \cdots,$$

  where $0 \leq \beta \leq 43$, and

  $$W_{54,2} = 1 + (351 - 8\beta)y^{10} + (5543 + 24\beta)y^{12} + \cdots,$$

  where $12 \leq \beta \leq 43$.
  Codes exist for $W_{54,1}$ when $0 \leq \beta \leq 22, \beta = 26$ and for $W_{54,2}$ when $\beta = 12, \ldots, 24, 26, 27$ (see [8] and [12]).

The classification of binary self-dual codes started with a paper from V. Pless [9], were all codes are classified up to length 20. Since then the classification of self-dual codes has been one of the most active research topics (see [11], [8]). Recently in [2], Bouyuklieva and Bouyukliev have classified all binary self-dual $[38, 19]$ codes. Optimal self-dual codes with automorphism of odd prime order is also extensively studied subject, for example, all such codes are classified: for length 42 in [3] and for length 44 in [4]. Very recently in [5] it was proved that the order of the automorphism group of a binary self-dual $[48, 24, 10]$ code is: 2^s with $s \geq 0$; $2^s 3^t$ with $s, t \geq 0$; or the group is trivial. Also there, all binary self-dual $[48, 24, 10]$ codes with an automorphism of odd prime order were classified. In [13] a

full classification of all $[50, 25, 10]$ codes possessing an automorphism of odd prime order was given. In [14] a full classification of all optimal binary self-dual $[50 + 2t, 25 + t]$ codes having an automorphism of order 5 for $t = 0, \ldots, 5$. As a consequence, also in [14] the weight enumerators for which there is an optimal binary self-dual $[52, 26, 10]$ code was determined.

Even if the problem of classifying all binary self-dual codes of a given length is not solved (and is very difficult) for $n \geq 40$ still an interesting question is what are the possible weight enumerators (or rather possible values of the parameters in this enumerators) for which there exist a self-dual code. The first length for which this question is still unsolved is $n = 54$. This is the reason we will focus on this question for binary self-dual $[54, 27, 10]$ codes.

II. Construction method

In this paper, we extend binary self-dual codes of length 52 having an automorphism of order 5 to self-dual codes of length 54 using a technique due to Harada and Kimura [7].

Theorem 2.1: [7] Let G be a generator matrix of a self-dual code C of length $2n$, and let $x = (x_1, \ldots, x_n, x_{n+1}, \ldots, x_{2n})$ be a vector in $\mathbb{F}_2^{2n}$ such that $(x, x) = 1$, where $(,)$ denotes the Euclidean inner product. Let $y_i = (x, r_i)$ for $1 \leq i \leq n$, where r_i is the i-th row vector of G. Then the following matrix

$$G' = \begin{pmatrix} 1 & 0 & x_1 & & x_i & \ldots & x_{2n} \\ y_1 & y_1 & & & & & \\ \vdots & \vdots & & & G & & \\ y_n & y_n & & & & & \end{pmatrix}$$

generates a self-dual code C' of length $2n + 2$.

Since we will extend $[52, 26, 10]$ binary self-dual codes, i.e. $n = 26$ the number of all vectors $x = (x_1, \ldots, x_n, x_{n+1}, \ldots, x_{2n})$ satisfying the condition of Theorem 2.1 is 2^{51} is too big to be applied even on one code of length 52. Thus we need the following.

Corollary 2.2: [7] Let S be a subset of the set $1, 2, \ldots, n$ such that $|S|$ is odd if $2n \equiv 0 (\text{mod } 4)$ and $|S|$ is even if $2n \equiv 2 (\text{mod } 4)$. Let $G = (I_n | A)$ be a generator matrix in standard form of a self-dual code C of length $2n$. 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 $1 \leq i \leq n$. 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 $2n + 2$.

III. The minimum weight algorithm

We continue with an effective algorithm for computing the minimum weight of a binary self-dual code with a generator matrix in standard form. Let C be an $[n, \frac{n}{2}, d]$, for an even n, binary self-dual code.

Denote by $k = \frac{n}{2}$. We assume that the generator matrix is in the form $G = (I_k|A)$, where is a $k \times k$ binary matrix. Since, in general, we need to compute the minimum weight of all codewords in C, that is we have to find all $|C| = 2^k$ codewords, the problem of computing the minimum weight is effectively approximated by $O(2^k)$. But self-dual codes are not general codes and have additional properties which we will explore here, in order to scale down the complexity of the algorithm to finding the minimum weight of just $2(k + \binom{k}{2} + \cdots + \binom{k}{d-1})$ codewords.

The main idea of the algorithm is that if an codewords $c \in C$ with $\mathrm{wt}(c) < d$ then it has either d nonzero coordinates in the first $\frac{n}{2} = k$ coordinate positions or in the last $\frac{n}{2} = k$ coordinate positions. Thus we only need to check, at most, the linear combinations of at most d rows of the generator matrix G for codewords of weight $< d$. Let $1 \leq l \leq d$ is the number of rows we use for linear combinations.

Let the rows are $1 \leq r_{i_1} < r_{i_1} < \cdots < r_{i_l} \leq k$. We have linear the combinations

$$c = \lambda_1 r_{i_1} + \lambda_2 r_{i_2} + \ldots \lambda_1 r_{i_l}, \lambda_s \neq 0,$$

so $c = \lambda_t = 1$ and

$$c = r_{i_1} + r_{i_2} + \ldots r_{i_l}.$$

But since the first k coordinates of c are composed of all zeroes, except the coordinates $i_1, i_2, \ldots, i_l$ then the weight of the codewords c is

$$\mathrm{wt}(c) = l + \mathrm{wt}(c|\Omega),$$

where $\mathrm{wt}(c|\Omega)$ is the weight of the codeword c in the last k coordinate positions. Thus we only compute the weight of the linear combination in the columns with numbers $k+1, \ldots, n$ and add the number l. A Borland Delphi 7.0 program that computes the weights was created.

IV. Results

As a general rule, the more codewords of weight 10 are in the $[52, 26, 10]$ code that we are extending, the more such words will be in the result code, leading to a higher chance of obtaining codes with higher values of β. Since we are interested in obtaining values of $\beta \geq 20$ we will try to extend the following codes with automorphism of type $5 - (10, 2)$ (see [14]):

- 147 codes with weight enumerator $W_{52,1}$;
- 1 code with weight enumerator $W_{52,2}$ for $\beta = 10$;
- 520 codes with weight enumerator $W_{52,2}$ for $\beta = 7$.

1) New codes from codes with weight enumerator $W_{52,1}$: If C is one of the 147 $[52, 26, 10]$ code with weight enumerator $W_{52,1}$, possessing an automorphism of type $5 - (10, 2)$ which was constructed in [14]. Extending these codes using Corollary 2.2 we obtain exactly 1434 inequivalent $[54, 27, 12]$ binary self-dual codes. All of these codes have weight enumerator $W_{54,2}$ for different values of the parameter β, listed it Table I. The code with $W_{54,2}$ for $\beta = 25$ is the first known example of a code with this value of the parameter. The cardinality of the automorphism groups of the constructed codes are listed in Table II.

TABLE I
NEW CODES EXTENDED FROM CODES WITH WEIGHT ENUMERATOR $W_{52,1}$

number	A_{10}	A_{12}	β	type
1291	191	6023	20	$W_{54,2}$
103	183	6047	21	$W_{54,2}$
37	175	6071	22	$W_{54,2}$
1	167	6095	23	$W_{54,2}$
1	**151**	**6143**	**25**	$W_{54,2}$
1	135	6191	27	$W_{54,2}$

TABLE II
CARDINALITY OF AUT(C) FOR THE CODES OBTAINED FROM CODES WITH $W_{52,1}$

$\lvert\mathrm{Aut}(C)\rvert$	1	2	5	10
number of codes	1401	1	21	1

Since the codes with automorphism groups of order 5 and 10 are known from [14] all other 1402 codes are new.

We give the generator matrix $G = (I_{24}|A)$ of the new code with weight enumerator $W_{54,2}$ for $\beta = 25$, where $A = 332620031; 617107724; 656542227; 720212740; 437175230; 570406444; 503273370; 651632062; 723566661; 426607261; 564377461; 515103661; 371643113; 214526244; 116057120; 047223450; 023511624; 713330206; 752523751; 762222036; 416361146; 610307331; 710540074; 743217767; 776570120; 332550146; 360007603$. Here every row of A is written in octal (exchange 0 with 000, 1 with 001, ..., 7 with 111) and all rows are separated by semicolon.

2) New codes from a code with weight enumerator $W_{52,2}$ with $\beta = 10$: Let C be the unique $[52, 26, 10]$ code with weight enumerator $W_{52,2}$ with $\beta = 10$, possessing an automorphism of type $5-(10, 2)$ which was constructed in [14]. Extending this code using Corollary 2.2 we obtain exactly 3 inequivalent $[54, 27, 12]$ binary self-dual codes. All code have weight enumerator $W_{54,2}$ for $\beta = 20$. Of the 3 codes there is one with trivial automorphism group and two with $|\mathrm{Aut}(C)| = 10$. The code with the trivial automorphism group is new.

3) New codes from codes with weight enumerator $W_{52,2}$ with $\beta = 7$: Here C is one of the 520 $[52, 26, 10]$ codes with weight enumerator $W_{52,2}$ for $\beta = 7$, possessing an automorphism of type $5-(10, 2)$ which was constructed in [14]. Using Corollary 2.2 we obtain exactly 66 inequivalent $[54, 27, 12]$ binary self-dual codes with both weight enumerators $W_{54,1}$ and $W_{52,2}$ for different values of β listed in Table III. Of the 66 codes there are 61 with trivial automorphism group, two with $|\mathrm{Aut}(C)| = 5$ and three with $|\mathrm{Aut}(C)| = 10$. The codes with the trivial automorphism group are new.

Proposition 4.1: Up to equivalence, there exist exactly 1503binary self-dual $[54, 27, 10]$ codes with $W_{54,1}$ and $W_{54,2}$ for $\beta \geq 20$, obtained via extending of the binary self-dual $[52, 26, 10]$ with an automorphism of order 5 with $W_{52,1}$ and $W_{52,2}$ for $\beta \geq 7$.

Open problem: Construct or prove the nonexistence of optimal binary self-dual $[54, 27, 10]$ codes having an weight distribution:

TABLE III
NEW CODES EXTENDED FROM CODES WITH WEIGHT ENUMERATOR $W_{52,2}$ FOR $\beta = 7$

number	A_{10}	A_{12}	β	type
45	191	6023	20	$W_{54,2}$
12	183	6047	21	$W_{54,2}$
5	175	5559	22	$W_{54,1}$
2	175	6071	22	$W_{54,2}$
2	167	6095	23	$W_{54,2}$

- $W_{54,1}$ for $\beta = 23, 24, 25$ or $27 \leq \beta \leq 43$;
- $W_{54,2}$ when $28 \leq \beta \leq 43$.

V. ACKNOWLEDGMENTS

This work was also supported by World Class University Project (WCU) R-32-2012-000-20014-0, Basic Science Research Program 2010-0020942, NRF Korea, and MEST 2012-002521, NRF Korea.

REFERENCES

[1] S. Bouyuklieva, M. Harada, A. Munemasa, Restrictions on the weight enumerators of binary self-dual codes of length $4m$, *Proceedings of the International Workshop OCRT*, White Lagoon, Bulgaria, pp. 40–44, 2007.

[2] S. Bouyuklieva and I. Bouyukliev, An algorithm for classification of binary self-dual codes, *IEEE Transactions on Information Theory*, vol. 58, no. 6, pp. 3933–3940, 2012.

[3] S. Bouyuklieva, N. Yankov, and R. Russeva, Classification of the Binary Self-Dual $[42, 21, 8]$ Codes having an Automorphism of Order 3, *Finite Fields and Their Applications*, vol. 13, pp. 605–615, 2007.

[4] S. Bouyuklieva, N. Yankov, and R. Russeva, On the classification of binary self-dual $[44, 22, 8]$ codes with an automorphism of order 3 or 7, *International Journal of Information and Coding Theory*, vol. 2, no. 1, pp. 21–37, 2011.

[5] S. Bouyuklieva, N. Yankov, and J.-L. Kim, Classification of binary self-dual $[48, 24, 10]$ codes with an automorphism of odd prime order, *Finite Fields and Their Applications*, vol. 18(6), pp. 1104–1113, 2012.

[6] J. H. Conway, N.J.A. Sloane, A new upper bound on the minimal distance of self-dual codes, *IEEE Transactions on Information Theory*, vol. 36, no. 6, pp. 1319–1333, 1990.

[7] M Harada, H. Kimura, On extremal self-dual codes, *Mathematical Journal of Okayama University*, vol. 37, pp. 1–14, 1995.

[8] W. C. Huffman, On the classification and enumeration of self-dual codes, *Finite Fields and Their Applications*, vol. 11(3), pp. 451–490, 2005.

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

[10] E. M. Rains, Shadow bounds for self-dual-codes, *IEEE Transactions on Information Theory*, vol. 44, pp. 134–139, 1998.

[11] E. Rains and N. Sloane, *Self-dual codes, in: V.S. Pless, W.C. Huffman (Eds.), Handbook of Coding Theory*. Elsevier, Amsterdam, 1998.

[12] N. Yankov, New self-dual $[54, 27, 10]$ codes extended from $[52, 26, 10]$ codes, *Proceedings of Conference 40 Year Shumen University (1971-2011)*, pp. 36–41, 2011.

[13] N. Yankov, Moon Ho Lee, Classification of self-dual codes of length 50 with an automorphism of odd prime order, preprint.

[14] N. Yankov, Moon Ho Lee, New binary self-dual codes of lengths 50 to 60, preprint.