NEW SELF-DUAL [54, 27, 10] CODES EXTENDED FROM [52, 26, 10] CODES [1]

Nikolay I. Yankov

ABSTRACT: *Using [52, 26, 10] binary self-dual codes, possesing an automorphism of order 3, we construct new [54, 27, 10] binary self-dual codes. We do this by applying a technique for extending a [2k, k, d] self-dual code to a [2k+2, k+1] self-dual code. Most of the constructed codes have new values of the parameter in their weight numerators,. We construct new codes with $\beta = 20, 21, 22$ for the first weight function and with $\beta = 22, 23$ for the second.*

KEYWORDS: *codes, automorphisms, self-dual codes, weight enumerator*

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 $G = (I_k \mid A)$, 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 $A_i = \left|\{v \in C \mid \mathrm{wt}(v) = i\}\right|$. 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

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

[1] This research is supported by Shumen Univesity under Project RD-05-157/25.02.2011

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 [1]. It was also shown [2] that the minimum weight d of a binary self-dual code of length n is bounded by

$$d \le \begin{cases} 4\left\lfloor \frac{n}{24} \right\rfloor + 4, & \text{if } n \not\equiv 22 (\text{mod } 24); \\ 4\left\lfloor \frac{n}{24} \right\rfloor + 6, & \text{if } n \equiv 22 (\text{mod } 24). \end{cases} \quad (1)$$

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 [3], [4]:

- [52, 26, 10]: There are two possible forms for the weight enumerator ,
  $W_{52,1} = 1 + 250y^{10} + 7980y^{12} + 42800y^{14} + \cdots$,
  $W_{52,2} = 1 + (442 - 16\beta)y^{10} + (6188 + 64\beta)y^{12} + \cdots$, where
  $0 \le \beta \le 12, \beta \ne 11$. Codes exist for $W_{52,1}$ and for $W_{52,2}$ when $\beta = 0, \ldots, 9, 12$ (see [5]).
- [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 $0 \le \beta \le 43$,
  $W_{54,2} = 1 + (351 - 8\beta)y^{10} + (5543 + 24\beta)y^{12} + \cdots$, where $12 \le \beta \le 43$.
  Codes exist for $W_{54,1}$ when $0 \le \beta \le 19, \beta = 26$ and for $W_{54,2}$ when $\beta \in [12..21], 24, 26, 27$ (see [6]).

CONSTRUCTION METHOD

In this paper, we extend binary self-dual codes of length 52 having an automorphism of order 3 to self-dual codes of length 54 using a technique due to Harada and Kimura [7].

Theorem 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 $1 \le i \le n$, 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 [7] 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 $2n$. 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 $1 \le i \le n$. Then the following matrix:

$$G' = \begin{pmatrix} 1 & 0 & x_1 & \ldots & x_n & 1 & \ldots & 1 \\ y_1 & y_1 & & & & & & \\ \vdots & \vdots & & I_n & & & A & \\ y_n & y_n & & & & & & \end{pmatrix} \tag{2}$$

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

EXTENDING LENGTH 52 CODES TO LENGTH 54

In [5] we constructed some new $[52, 26, 10]$ self-dual codes with automorphism of types $3-(14,10)$ and $3-(16,4)$. We use construction (2) and an exhaustive search on all odd cardinality sets S. The base codes which we extend are the following:

- **Case I:** 640 codes with $\beta = 8$ having an automorphism of type $3-(14,10)$. We have found 228 inequivalent $[54, 27, 10]$ codes with weight enumerators $W_{54,1}$ and $W_{54,2}$ for different values of β. The codes with $W_{52,1}$ for $\beta = 20, 21, 22$, and $W_{52,2}$ for $\beta = 22, 23$ are the first known codes with these weight functions. We give the number of codes for different values of β (for all codes with $\beta \ge 20$) in Table 1 (the new codes are in bolds).

Number of codes	A_{10}	A_{12}	β	$W_{54,i}$
14	**191**	**5511**	**20**	**1**
126	191	6023	20	2
7	**183**	**5535**	**21**	**1**
59	183	6047	21	2
6	**175**	**5559**	**22**	**1**
14	**175**	**6071**	**22**	**2**
2	**167**	**6095**	**23**	**2**

Table 1: [54, 27, 10] self-dual codes with $\beta \ge 20$ from case I

- **Case II:** 36 codes with $\beta = 9$ having an automorphism of type $3-(16,4)$. We have found 35 inequivalent $[54, 27, 10]$ codes with weight enumerators $W_{54,1}$ and $W_{54,2}$ for different values of β. The codes with $W_{52,1}$ for $\beta = 20, 22$, and

$W_{52,2}$ for $\beta = 22, 23$ are the first known codes with these weight functions. We give the number of codes for different values of β in Table 2.

Number of codes	A_{10}	A_{12}	β	$W_{54,i}$
12	**191**	**5511**	**20**	**1**
14	183	6047	21	2
2	**175**	**5559**	**22**	**1**
5	**175**	**6071**	**22**	**2**
1	**167**	**6095**	**23**	**2**
1	159	6119	24	2

Table 2: [54, 27, 10] self-dual codes with $\beta \geq 20$ from case II

- **Case III:** 1 code with $\beta = 12$ having an automorphism of type $3-(16,4)$. We have found 75 inequivalent new codes. The codes with $W_{54,1}$ for $\beta = 20, 21$ are the first known codes with these weight functions. We give the number of codes for different values of β in Table 3.

Number of codes	A_{10}	A_{12}	β	$W_{54,i}$
72	**191**	**5511**	**20**	**1**
1	**183**	**5535**	**21**	**1**
2	143	6167	26	2

Table 3: [54, 27, 10] self-dual codes with $\beta \geq 20$ from case III

We conclude with examples of codes for each new weight distribution obtained. To construct a generator matrix of a code with $W_{52,i}$ for $\beta = j$ use $G = (I_{27} \mid {G_{i,j}}^T)$ (removing the last column of ${G_{i,j}}^T$ consisting of zeroes), where the matrices

$$G_{1,20} = \begin{pmatrix} 0926452e36caf599907cb681000 \\ 081767e1697a5fbed4a93032930 \\ 01ed2a6c5befd2ed39753175307 \\ 3c8bc300066a3a416cefec1583c \\ c0797a34d2cf24dce2e12792ab0 \\ 7e47b33fa9a148cc598423d446f \\ c0ee8aec622cac40446424eee66 \end{pmatrix}, \quad G_{1,21} = \begin{pmatrix} 0a8ce5273659cf0000df6110100 \\ 0bacd7e969f96436541a0b29830 \\ 0c57ed65a37b7e7b2fa8e8ac0e0 \\ 0296e303c964eb4ea0310ea733f \\ 37e04a6f99cb9e97f27625a2bea \\ fa33d069d5cfe92ad90f69119fe \\ ea2c848cc4ca6460e4c82eaa68a \end{pmatrix},$$

$$G_{1,22} = \begin{pmatrix} 09bfdcb7af536c9990e52618900 \\ 089fef69e1f2d7bed421b0ba130 \\ 0e7bcd8b4d79529b2f642e84200 \\ 30b7c000c965c94da32320da73f \\ d2ac3157a9f49e9cbe8202a91a9 \\ 7a4c967ec801faf34ac5e9600bd \\ 468e24622ca66ae62eea64244ca \end{pmatrix}, \; G_{2,22} = \begin{pmatrix} 6ea64527bedb650088fdae19100 \\ 908767e9f06bdf36cd3829bb830 \\ cfdd2a7d69ddd3ec1a461376117 \\ 9208f0cf81dd367d2457a82dcfc \\ 89e6d51f63b9573f4bf9dc681c2 \\ 9bc80c034efbe16ab1a988a071e \\ 6c62668ecce06ee0ccca8ae0c2a \end{pmatrix},$$

$$G_{2,23} = \begin{pmatrix} 6ea64527bedb650088fdae19100 \\ 908767e9f06bdf36cd3829bb830 \\ cfdd2a7d69ddd3ec1a461376117 \\ 9208f0cf81dd367d2457a82dcfc \\ 89e6d51f63b9573f4bf9dc681c2 \\ 9bc80c034efbe16ab1a988a071e \\ 6c62668ecce06ee0ccca8ae0c2a \end{pmatrix}$$ are in hexadecimal form.

Proposition There exist optimal binary self-dual [54, 27, 10] codes having an weight distribution $W_{54,1}$ when $0 \le \beta \le 22, \beta = 26$ and for $W_{54,2}$ when $12 \le \beta \le 27$, $\beta \ne 25.$

Open problem Construct or prove the nonexistence of optimal binary self-dual [54, 27, 10] codes having an weight distribution $W_{54,1}$ with $\beta = 23, 24, 25$ and for $W_{54,2}$ when $\beta = 25.$

REFERENCES

1. **Conway J.H. and Sloane N.J.A.**, A new upper bound on the minimal distance of self-dual codes. // IEEE Trans. Inform. Theory 36, pp. 1319–1333, 1990.
2. **Rains E.M.,** Shadow bounds for self-dual-codes. // IEEE Trans. Inform. Theory, vol. 44, pp. 134-139, 1998.
3. **Bouyuklieva St., Harada M., Munemasa A.**, Restrictions on the weight enumerators of binary self-dual codes of length 4*m*. // Proceedings of the International Workshop OCRT, White Lagoon, Bulgaria, pp. 40-44, 2007.
4. **Huffman W.C.**, Automorphisms of codes with application to extremal doubly-even codes of length 48. // IEEE Trans. Inform. Theory, vol. 28, pp. 511-521, 1982.
5. **N. Yankov,** New optimal [52, 26, 10] self-dual codes. // to appear.

6. **Yankov N., Russeva R.**, Binary self-dual codes of lengths 52 to 60 with an automorphism of order 7 or 13. // to appear in IEEE Trans. Inform. Theory.
7. **Harada M., Kimura H.,** On extremal self-dual codes. // Math. J. Okayama Univ., vol. 37, pp. 1-14, 1995.

ABOUT THE AUTOR

assist. prof. Nikolay I. Yankov, PhD, Konstantin Preslavski University of Shumen, 140 Saedinenie Str, 9700 Shumen, Bulgaria, e-mail: jankov_niki@yahoo.com