Annual of Konstantin Preslavsky University of Shumen
vol. XXIII C, 2022, pp. 3 – 9, https://doi.org/10.46687/NQCW1165

ON BINARY LCD CODES POSSESSING AN AUTOMORPHISM OF ORDER 13*

STEFKA H. BOUYUKLIEVA, NIKOLAY I. YANKOV, RADKA P. RUSSEVA, EMINE A. KARATASH, MILENA N. IVANOVA

ABSTRACT: *In this work we apply the method for constructing binary LCD codes via an automorphism of prime order described in [3] and [4]. Thus we obtain all optimal LCD codes of lengths 26, 27 and 28 possessing an automorphism of order 13 with two cycles.*

KEYWORDS: *LCD codes, automorphism*

2020 Math. Subject Classification: *94B05*

1 Introduction

Let $\mathbb{F}_q$ be a finite field with q elements and $\mathbb{F}_q^n$ be the n-dimensional vector space over $\mathbb{F}_q$. The (Hamming) *distance* $d(x,y)$ between two vectors $x,y \in \mathbb{F}_q^n$ is the number of coordinate positions in which they differ. The (Hamming) *weight* $\mathrm{wt}(x)$ of a vector $x \in \mathbb{F}_q^n$ is the number of its nonzero coordinates. A linear $[n,k,d]$ code C is a k-dimensional subspace of the vector space $\mathbb{F}_q^n$, where d is the smallest weight among all non-zero codewords of C is called the minimum weight (or minimum distance) of the code. A matrix which rows form a basis of C is called a generator matrix of this code. Let $(u,v) : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$ be an inner product in the linear space $\mathbb{F}_q^n$. The dual code of C is $C^\perp = \{u \in \mathbb{F}_q^n : (u,v) = 0$ for all $v \in C\}$. $C^\perp$ is a linear $[n,n-k]$ code. If C and $C^\perp$ are equivalent codes, C is termed isodual and if $C = C^\perp$, C is self-dual. A code C is a linear complementary dual (LCD) code if $C \cap C^\perp = \{0\}$.

LCD codes over finite fields were introduced by Massey [7] in

*This paper is (partially) supported by Scientific Research Grant RD-08-148/02.03.2022 of Shumen University

1992 and they are an important class of codes for both theoretical and practical reasons [6]. The classification of LCD $[n,k]$ codes and determination of the largest minimum weight among all LCD $[n,k]$ codes, denoted by $d_{LCD}(n,k)$, are fundamental problems. A LCD $[n,k]$ code with the largest minimum weight among all LCD $[n,k]$ codes is an *optimal* code. The optimal binary LCD codes of length $n \leq 16$ are presented in [6] and all values of $d_{LCD}(n,k)$ for binary codes of lengths $n \leq 40$ are known [2].

Different methods have been used to study, construct and classify LCD codes with different parameters over different finite fields (see [6] and [5]). A method for constructing LCD binary codes via their automorphism is presented in [2] and [3]. In Section 2, applying this method we construct all optimal binary LCD codes with an automorphism of order 13 with two cycles of lengths 26, 27 and 28.

2 Automorphisms of order 13

Let C be a binary LCD code of length $n = 13c + f$ and dimension k, invariant under the action of the group generated by $\sigma \in S_n$, where

$$\sigma = (1,2,\ldots,13)\ldots(13c-12,13c-11,\ldots,13c)$$

is a permutation of order 13 with c independent cycles. Then the code C is a direct sum of its subcodes $F_\sigma(C) = \{v \in C : v\sigma = v\}$ and

$$E_\sigma(C) = \{v \in C : \mathrm{wt}(v|\Omega_i) \equiv 0 \pmod 2, i = 1,\ldots,c+f\},$$

where $v|\Omega_i$ is the restriction of v on Ω_i. According to [3, Theorem 2], the two subcodes are also LCD codes.

If $\pi : F_\sigma(C) \to \mathbb{F}_2^{c+f}$ is the projection map, i.e., $(\pi(v))_i = v_j$ for some $j \in \Omega_i$, $i = 1,2,\ldots,c+f$, then $C_\pi = \pi(F_\sigma(C))$ is a binary LCD $[c+f,k_\pi,d_\pi]$ code [3, Lemma 3].

Denote by $E_\sigma(C)^*$ the code obtained from $E_\sigma(C)$ by deleting the last f coordinates. For $v \in E_\sigma(C)^*$ we identify $v|\Omega_i = (v_0,v_1,\cdots,v_{12})$ with the polynomial $v_0 + v_1x + \cdots + v_{12}x^{12}$ from $\mathscr{P}$, where $\mathscr{P}$ is the set of even-weight polynomials in $\mathbb{F}_2[x]/(x^{13}-1)$. Thus we obtain the map $\varphi : E_\sigma(C)^* \to \mathscr{P}^c$. We have that $\mathscr{P}$ is a field with $2^{12} = 4096$ elements and $\mathscr{P}^* = \{\beta^i\gamma^j | 0 \le i \le 64, 0 \le j \le 62\}$, where $e = x + x^2 + \cdots + x^{12}$ is the identity element, $\alpha = xe = 1 + x^2 + \cdots + x^{12}$, is a primitive element, and $\beta = \alpha^{65}, \gamma = \alpha^{63}$. We take $\delta = \gamma^{13}$ so δ is an element of order 5.

On $\mathscr{P}^c$, we use the Hermitian inner product, namely

$$\langle u, v\rangle = \sum_{j=1}^{c} u_j v_j^{64}, \tag{1}$$

where $u = (u_1, \ldots, u_c)$, $v = (v_1, v_2, \ldots, v_c) \in \mathscr{P}^c$. The code $C_\varphi = \varphi(E_\sigma(C)^*)$ is a $[c, k_\varphi, d_\varphi]$ LCD code over the field $\mathscr{P}$ with respect to the Hermitian inner product (1). Obviously, $k = 12k_\varphi + k_\pi$.

Consider the case $c = 2$. Then C_φ must be a LCD code of length 2 over the field $\mathscr{P}$. Up to equivalence, if $k_\varphi = 1$, we can take the generator matrix of C_φ in the form (δ^i, β^j), where $0 \le i \le 4$, $0 \le j \le 62$, and $e + \beta^{2j} \ne 0$, so $j \ge 1$.

There is a total of 20 codes C_φ, namely $C_0 = \{(0,0)\}$, the codes with generators $\langle(e, \beta^j)\rangle$ for $j = 1, 3, 5, 7, 9, 11, 21$ (denoted by $C_1, \ldots, C_7$); the codes with generators $\langle(\delta, \beta^j)\rangle$ for $j = 1, 2, 3, 5, 6, 7, 9, 10, 11, 21, 22$ (denoted by $C_8, \ldots, C_{18}$); and $C_{19} = \mathscr{P}^2$.

The cases for the generator matrix of the code $F_\sigma(C)$, up to equivalence, are:

- $(O|A)$, where A is a generator matrix of a $[f, k_\pi, d]$ binary LCD code;
- $\begin{pmatrix} \mathbf{1}_{13}\mathbf{0}_{13} & x \\ O & A \end{pmatrix}$, where A is a $(k_\pi - 1) \times f$ matrix and $x \in \mathbb{F}_2^f$, $k_\pi \ge 1$;
- $\begin{pmatrix} \mathbf{1}_{13}\mathbf{1}_{13} & x \\ O & A \end{pmatrix}$, where A is a $(k_\pi - 1) \times f$ matrix and $x \in \mathbb{F}_2^f$, $k_\pi \ge 1$;

- $\begin{pmatrix} \mathbf{1}_{13}\mathbf{0}_{13} & x \\ \mathbf{0}_{13}\mathbf{1}_{13} & y \\ O & A \end{pmatrix}$, where A is a $(k_\pi - 2) \times f$ matrix and $x, y \in \mathbb{F}_2^f$, $k_\pi \geq 2$.

In all cases O is the zero matrix of appropriate size, and $\mathbf{0}_s, \mathbf{1}_s$ denotes the all-zero or all-ones vector of length s, respectively.

If $k_\varphi = 2$ then $d(E_\sigma(C)) = 2$ and so C is a binary LCD code of length $26 + f$ and minimum distance at most 2. Therefore we will not consider these codes, they are not optimal. If $k_\varphi = 0$ then $C = F_\sigma(C)$. The optimal LCD code of dimension 1 is $\langle(11\ldots10)\rangle$ for even n and $\langle(11\ldots1)\rangle$ for odd n and σ is an automorphism of these codes for all $n \geq 27$.

Next we consider the cases $f = 0, 1$ and 2.

$f = 0)$ Then C is a LCD $[26, k]$ code with $k = 12k_\varphi + k_\pi$. Since C_π is a binary code of length 2, $k_\pi \leq 2$.

- $k_\varphi = 0)$ Then $k = k_\pi \leq 2$. Hence $C = \{0\}, C = \langle(\mathbf{1}_{13}\mathbf{0}_{13})\rangle$ or $C = \left\langle \begin{pmatrix} \mathbf{1}_{13}\mathbf{0}_{13} \\ \mathbf{0}_{13}\mathbf{1}_{13} \end{pmatrix} \right\rangle$.

- $k_\varphi = 1)$ Then $k = 12 + k_\pi = 12$, 13 or 14. From C_7 we obtain 3 optimal LCD codes $C_{26,1}, C_{26,2}$ and $C_{26,3}$ with parameters $[26, 12, 8]$, $[26, 13, 7]$ and $[26, 14, 6]$, respectively from $C_\pi = \{0\}$, $C_\pi = \langle \mathbf{0}_{13}\mathbf{1}_{13} \rangle$ and $C_\pi = \left\langle \begin{pmatrix} \mathbf{1}_{13} & \mathbf{0}_{13} \\ \mathbf{0}_{13} & \mathbf{1}_{13} \end{pmatrix} \right\rangle$. These codes have automorphism groups of orders 78, 78 and 156, respectively. The LCD code $C_{26,2}$ is an isodual code, too.

- $k_\varphi = 2)$ Then $k = 24 + k_\pi$. The obtained LCD codes C are dual to the codes constructed in the case $k_\varphi = 0$.

$f = 1)$ Then C_π is a binary $[3, k_\pi, d_\pi]$ LCD code. There are 6 such codes, namely $\{(000)\}$, $\langle(100)\rangle$, $\langle(111)\rangle$, $\langle(100), (010)\rangle$, $\langle(101), (011)\rangle$, and $\mathbb{F}_2^3$. The optimal among the constructed LCD codes are:

- $k_\varphi = 0$) The $[27,1,27]$ and $[27,2,14]$ codes with generator matrices $(\mathbf{1}_{13}\mathbf{1}_{13}1)$ and $\begin{pmatrix} \mathbf{1}_{13}\mathbf{0}_{13}1 \\ \mathbf{0}_{13}\mathbf{1}_{13}1 \end{pmatrix}$, respectively. If $k_\pi = 1$ we have two optimal $[27,13,7]$ LCD codes when $C_\pi = \langle(111)\rangle$ and $C_\pi = \langle(100)\rangle$, with $|\mathrm{Aut}(C)| = 156$ and 78, respectively.

  If $k_\pi = 2$ we have found 14 optimal $[27,14,6]$ LCD codes given in Table 1.

C_φ	C_π	$\lvert\mathrm{Aut}(C)\rvert$
C_7	$\langle(100),(010)\rangle$	156
C_1	$\langle(101),(011)\rangle$	26
C_5	$\langle(101),(011)\rangle$	52
C_6	$\langle(101),(011)\rangle$	26
C_7	$\langle(101),(011)\rangle$	156
C_8	$\langle(101),(011)\rangle$	13
C_9	$\langle(101),(011)\rangle$	13
C_{10}	$\langle(101),(011)\rangle$	13
C_{12}	$\langle(101),(011)\rangle$	13
C_{13}	$\langle(101),(011)\rangle$	13
C_{14}	$\langle(101),(011)\rangle$	13
C_{15}	$\langle(101),(011)\rangle$	13
C_{16}	$\langle(101),(011)\rangle$	13
C_{18}	$\langle(101),(011)\rangle$	13

Table 1: $[27,14,6]$ LCD codes

$f = 2$) Then C_π is a binary $[4,k_\pi,d_\pi]$ LCD code. The binary LCD codes of length 4 are $A_0 = \{(0000)\}$, $A_1 = \langle(1000)\rangle$, $A_2 = \langle(1110)\rangle$, $A_3 = \langle(1000),(0100)\rangle$, $A_4 = \langle(1000),(0111)\rangle$, $A_5 = \langle(1010),(0110)\rangle$, $A_6 = \langle(1010),(0111)\rangle$, $A_1^\perp$, $A_2^\perp$, and $\mathbb{F}_2^4$. The optimal among the constructed LCD codes are:

- $k_\varphi = 0)$ Only the $[28,1,27]$ code with a generator matrix $(\mathbf{1}_{27}0)$ is optimal in this case.

- $k_\varphi = 1)$ If $k_\pi = 1$ we have one optimal $[28,13,8]$ LCD code when $C_\pi = \langle(1011)\rangle$ and $C_\varphi = C_7$.

  If $k_\pi = 2$ we have 2 optimal $[28,14,7]$ LCD codes all with $C_\varphi = C_7$ for $C_\pi = \langle(1000),(0111)\rangle$ and $C_\pi = \langle(1010),(0111)\rangle$, having automorphism groups of orders 156 and 78, respectively.

For cumputer calculations of equivalences and automorphism groups of the constructed codes we have used the software package Q-EXTENTION [1].

REFERENCES:

[1] Bouyukliev I., What is Q-EXTENSION?, Serdika J. Computing, **1**, (2007), 115-130.

[2] Bouyuklieva S., Optimal binary LCD codes, Des. Codes Cryptogr. 89, (2021), 2445–2461. https://doi.org/10.1007/s10623-021-00929-w

[3] Bouyuklieva S., Russeva R., Binary LCD Codes Having an Automorphism of Odd Prime Order, Proc. 17th International Workshop on Algebraic and Combinatorial Coding Theory, Oct. 11–17, (2020), Bulgaria, IEEE Xplore, 2021, 32-36.

[4] Bouyuklieva S. and J. De la Cruz, On the Structure of Binary LCD Codes having an Automorphism of Odd Prime Order, IEEE Transactions on Information Theory, vol. 68, no. 10, (2022), 6426–6433.

[5] Galvez L., Kim J.-L., Lee N., Roe Y.G. and Won B.-S., Some bounds on binary LCD codes, Cryptogr. Commun. vol. 10, (2018), 719–728.

[6] Harada M., Saito K., Binary linear complementary dual codes, Cryptogr. Commun. vol. 11, (2019), 677–696.

[7] Massey J.L., Linear codes with complementary duals, Discrete Math. 106/107 (1992), 337–342.

Stefka Bouyuklieva
Faculty of Mathematics and Informatics
St. Cyril and St. Methodius University of Veliko Tarnovo
Veliko Tarnovo, Bulgaria
e-mail: stefka@ts.uni-vt.bg

Nikolay Yankov
College in Dobrich
Shumen University
Dobrich, Bulgaria
e-mail: n.yankov@shu.bg

Radka Russeva
Faculty of Mathematics and Informatics
Shumen University
Shumen, Bulgaria
e-mail: russeva@shu.bg

Emine Karatash
Faculty of Mathematics and Informatics
Shumen University
Shumen, Bulgaria
e-mail: e.karatash@shu.bg

Milena Ivanova
Faculty of Mathematics and Informatics
Shumen University
Shumen, Bulgaria
e-mail: m.ivanova@shu.bg