Defence Science Journal, Vol. 70, No. 6, November 2020, pp. 626-632, DOI : 10.14429/dsj.70.15691

Constacyclic and Linear Complementary Dual Codes Over $\mathbb{F}_q + u\mathbb{F}_q$

Om Prakash*, Shikha Yadav, and Ram Krishna Verma

Department of Mathematics, Indian Institute of Technology Patna, Patna - 801 106, India
**E-mail: om@iitp.ac.in*

ABSTRACT

This article discusses linear complementary dual (LCD) codes over $\mathfrak{R} = \mathbb{F}_q + u\mathbb{F}_q$ $(u^2 = 1)$, where q is a power of an odd prime p. Authors come up with a new Gray map from $\mathfrak{R}^n$ to $\mathbb{F}_q^{2n}$ and define a new class of codes obtained as the gray image of constacyclic codes over $\mathfrak{R}$. Further, we extend the study over Euclidean and Hermitian LCD codes and establish a relation between reversible cyclic codes and Euclidean LCD cyclic codes over $\mathfrak{R}$. Finally, an application of LCD codes in multisecret sharing scheme is given.

Keywords: Linear codes; Cyclic codes; Gray map; Constacyclic codes; Euclidean LCD codes; Hermitian LCD codes; Reversible codes

1. INTRODUCTION

The class of cyclic codes is an important subclass of linear codes because of their rich algebraic structure. The study of such codes over finite rings, after the pioneering work by Hammons[1], *et al.* over $\mathbb{Z}_4$, have been attracting many researchers. Interestingly, non-linear codes over Galois fields can also be derived from codes over finite rings with the help of Gray maps[2]. Recently, many works have been reported on codes over finite ring $\mathbb{F}_q + u\mathbb{F}_q, u^2 = 1$ for different values of q[3-8]. Meanwhile, constacyclic codes are generalization of the cyclic codes and often have good parameters than cyclic codes. These codes have been studied in many papers[9-13]. Nevertheless, to say that main target behind the study of linear codes (cyclic codes, constacyclic codes and their generalizations) over finite rings is to obtain new and better MDS (optimal) codes over finite field.

Linear complementary dual (LCD) codes were introduced by Massey[14]. These codes were shown to be supreme linear coding solution to the two-user binary adder channel. Yang & Massey[15] derived conditions for a cyclic code over finite field to have a complementary dual. The relation between reversible and LCD cyclic codes over finite field was also provided when length of the code is coprime to the characteristics of the field. Sendrier[16] showed that LCD codes over finite field meet Gilbert-Varshamov bound. Liu & Liu[17] obtained some results for linear codes over a finite chain ring to be LCD under certain conditions. Li[18] provided a construction of Hermitian LCD cyclic codes over finite fields and investigated their parameters. Later, Hui[19], *et al*. obtained LCD codes over finite field from linear codes over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q$, by means of a Gray map. Recently, Liu & Wang[20] studied LCD codes over finite rings.

Received : 08 May 2020, Revised : 28 June 2020
Accepted : 27 July 2020, Online published : 12 October 2020

Inspired from above works, authors studied LCD codes over $\mathfrak{R} = \mathbb{F}_q + u\mathbb{F}_q$ $(u^2 = 1)$, where $q = p^m$, for an odd prime p, $m \geq 1$ and establish a relation between reversible cyclic codes and LCD cyclic codes over $\mathfrak{R}$. Further, we provide a criterion based on defining set to check whether a constacyclic code is Hermitian LCD and study Gray images of these codes. Note that the LCD codes have many applications in Cryptography and these are playing an important role in secret sharing scheme (SSS), implementations against side-channel attack (SCA) and fault injection attack (FIA)[21]. Author also showed the applications of LCD codes in the multisecret sharing scheme. Therefore, the LCD codes that we provide here can be used to send secret information through a channel.

2. PRELIMINARIES

For an odd prime p and positive integer m, let $\mathbb{F}_q$ be a finite field where $q = p^m$, and $\mathfrak{R} := \mathbb{F}_q + u\mathbb{F}_q$ $(u^2 = 1)$. Thus $\mathfrak{R}$ is a finite non-chain ring with characteristic p. Any $\mathfrak{R}-$ submodule of the module $\mathfrak{R}^n$ is referred as linear code and throughout the manuscript we denote it by Z. For a unit $\lambda \in \mathfrak{R}$, the code Z is said to be $\lambda-$ constacyclic if for each code word $z = (z_0, z_1, ..., z_{n-1}) \in \mathrm{Z}$, the vector $\sigma(z) = (\lambda z_{n-1}, z_0, ..., z_{n-2}) \in \mathrm{Z}$. Notice that the constacyclic code is negacyclic if $\lambda = -1$ and cyclic if $\lambda = 1$. A $\lambda-$ constacyclic code Z of length n over $\mathfrak{R}$ is also considered as an ideal of $\mathrm{K}_n = \mathfrak{R}[y]/\langle y^n - \lambda \rangle$ on identifying $(z_0, z_1, ..., z_{n-1})$ by $z_0 + z_1 y + ... + z_{n-1} y^{n-1}$. The generator matrix G of a linear code over $\mathbb{F}_q$ with parameters $[n, k, d]$ is a $k \times n$ matrix whose rows forms a basis for the code where symbols n, k and d represent length, dimension and minimum distance of the code, respectively. The Euclidean inner product of vectors $z = (z_0, z_1 ..., z_{n-1})$ and $t = (t_0, t_1 ..., t_{n-1})$

is defined by $z \cdot t = \sum_{i=0}^{n-1} z_i t_i$. The Euclidean dual of a linear code Z over the ring $\mathfrak{R}$ is denoted by $Z^{\perp}$ and defined as $Z^{\perp} = \{r \in \mathfrak{R}^n : r \cdot z = 0, \text{ for all } z \in Z\}$. A linear code Z is said to be Euclidean LCD code if and only if $Z \cap Z^{\perp} = \{0\}$. Throughout this article, LCD code stands for Euclidean LCD code until and unless specified. The Hamming weight w_H of a codeword is the number of non-zero components in it and the Hamming distance d_H between any two codewords is number of components in which these two differ. The Hamming distance of a linear code is the minimum of Hamming distances between any pair of codewords. For a monic polynomial $r(y)$ of degree n, with $r(0) = s \neq 0$, its monic reciprocal polynomial is given by $\tilde{r}(y) = s^{-1} y^n r(1/y)$. If $r(y) = \tilde{r}(y)$, then $r(y)$ is called self-reciprocal.

3. THE STRUCTURE OF CYCLIC CODES OVER $\mathfrak{R}$

Let $\gamma \in \mathbb{F}_q$ such that $2\gamma \equiv 1 (\text{mod } p)$. Consider $\varepsilon_1 = \gamma(1+u)$ and $\varepsilon_2 = \gamma(1-u)$ where $u \in \mathfrak{R}$ such that $u^2 = 1$. Then $\varepsilon_1 + \varepsilon_2 = 1$, $\varepsilon_i^2 = \varepsilon_i$ and $\varepsilon_i \varepsilon_j = 0$, for $i \neq j$, where $i, j \in \{1, 2\}$. By the orthogonal idempotent decomposition, we have $\mathfrak{R} = \varepsilon_1 \mathbb{F}_q \oplus \varepsilon_2 \mathbb{F}_q$. Now, we define $\Theta : \mathfrak{R}^n \to \mathbb{F}_q^{2n}$ by

$$\Theta(r) = \Theta(y_1 + uz_1, y_2 + uz_2, ..., y_n + uz_n)$$
$$= (y_1 - z_1, y_2 - z_2, ..., y_n - z_n, y_1 + z_1, y_2 + z_2, ..., y_n + z_n).$$

Then Θ is a ring isomorphism with inverse

$$\Theta^{-1}(s) = \Theta^{-1}(a_1, a_2, ..., a_n, b_1, b_2, ..., b_n)$$
$$= (\gamma(a_1 + b_1) + u\gamma(b_1 - a_1), ..., \gamma(a_n + b_n) + u\gamma(b_n - a_n)).$$

Definition 3.1 The Lee weight of an element $r = (r_0, r_1, ..., r_n) \in \mathfrak{R}^n$ is defined by $w_L(r) = w_H(\Theta(r))$ and the Lee distance between *r, s* in R^n is $d_H(\Theta(r), \Theta(s))$.

It can be easily verified that Θ is a distance preserving isometry, i.e., a Gray map. Also, the following result holds.

Theorem 3.1 If Z is an (n, q^k, d_L) linear code (having q^k elements) over the ring $\mathfrak{R}$, then $\Theta(Z)$ is a linear code over $\mathbb{F}_q$ with parameters $[2n, k, d_L]$. Moreover, if $Z^{\perp}$ is the dual of Z, then $\Theta(Z^{\perp}) = \Theta(Z)^{\perp}$.

For a linear code Z of length n over $\mathfrak{R}$, we define

$$A_1 = \{b_1 \in \mathbb{F}_q^n : \exists\ b_2 \in \mathbb{F}_q^n \,|\, \varepsilon_1 b_1 + \varepsilon_2 b_2 \in Z\},$$

$$A_2 = \{b_2 \in \mathbb{F}_q^n : \exists\ b_1 \in \mathbb{F}_q^n \,|\, \varepsilon_1 b_1 + \varepsilon_2 b_2 \in Z\}.$$

It is easy to verify that A_1 and A_2 are linear codes of length n over $\mathbb{F}_q$. Also, $Z = \varepsilon_1 A_1 \oplus \varepsilon_2 A_2 = \{\varepsilon_1 b_1 + \varepsilon_2 b_2 : b_1 \in A_1, b_2 \in A_2\}$ and $|Z| = |A_1||A_2|$. Further, Z is a cyclic code if and only if both A_1 and A_2 are cyclic codes of length n over $\mathbb{F}_q$.

Theorem 3.2 Let $Z = \varepsilon_1 A_1 \oplus \varepsilon_2 A_2$ be a cyclic code over $\mathfrak{R}$, where A_1 and A_2 are cyclic codes over $\mathbb{F}_q$ generated by $f_1(y)$ and $f_2(y)$, respectively. Then there exists a unique polynomial $f(y) = \varepsilon_1 f_1(y) + \varepsilon_2 f_2(y)$ such that $Z =< f(y) >$.

Proof. Same procedure follows as given in Theorem 3.6 of Cengellenmis[4].

Theorem 3.3 For any linear code $Z = \varepsilon_1 A_1 \oplus \varepsilon_2 A_2$ of length n over $\mathfrak{R}$, its dual is $Z^{\perp} = \varepsilon_1 A_1^{\perp} \oplus \varepsilon_2 A_2^{\perp}$. Moreover, if Z is cyclic, then $Z^{\perp}$ is a cyclic code over $\mathfrak{R}$.

Proof. Same procedure follows as given in Corollary 3.2 of Cengellenmis[4].

4. CONSTACYCLIC CODES OVER $\mathfrak{R}$ AND THEIR GRAY IMAGES

In this section, we find the image of λ-constacyclic codes under the Gray map Θ (defined in section 3), for different values of λ. Now, we provide some definitions which are essential for further study in this section.

Definition 4.1 Let α, α' are units in $\mathfrak{R}$. Then a linear code Z of length n over $\mathfrak{R}$ is called an $(\alpha, \alpha') -$ constacyclic code of length (r, s) where $n = r + s$, if for any

$$z = (z_1, z_2, ..., z_r, z_{r+1}, z_{r+2}, ..., z_{r+s}) \in Z,$$

the vector given by

$$\tau_1(z) = (\alpha z_r, z_1, ..., z_{r-1}, \alpha' z_{r+s}, z_{r+1}, ..., z_{r+s-1}),$$

is also in Z. If $\alpha' = 1$, then Z is called an α-constacyclic code of length (r, s) in addition $\alpha = -1$, then Z is said to be negacyclic code of length (r, s). Further, if $\alpha = \alpha'$, then we call Z as a double α-constacyclic code of length (r, s).

For rest of the results in this section, consider $\lambda = l + um$, a unit in $\mathfrak{R}$.

Theorem 4.1 Let $Z = \varepsilon_1 A_1 \oplus \varepsilon_2 A_2$ be a linear code of length n over $\mathfrak{R}$ and $\lambda \in \mathfrak{R}$ be a unit. Then Z is a λ-constacyclic code if and only if A_1, A_2 are $(l+m)$ and $(l-m)$-constacyclic codes over $\mathbb{F}_q$, respectively.

Proof: Let Z be a λ-constacyclic code of length n over $\mathfrak{R}$. Then $z \in Z$ implies $\sigma(z) \in Z$. Let $a = (a_0, a_1, ..., a_{n-1}) \in A_1$ and $b = (b_0, b_1, ..., b_{n-1}) \in A_2$ be arbitrary. For $z = \varepsilon_1 a \oplus \varepsilon_2 b$, we have

$$\sigma(z) = (\lambda(\varepsilon_1 a_{n-1} + \varepsilon_2 b_{n-1}), \varepsilon_1 a_0 + \varepsilon_2 b_0, ..., \varepsilon_1 a_{n-2} + \varepsilon_2 b_{n-2})$$
$$= (((l+m)\varepsilon_1 a_{n-1} + \varepsilon_2 (l-m) b_{n-1}), \varepsilon_1 a_0 + \varepsilon_2 b_0, ..., \varepsilon_1 a_{n-2} + \varepsilon_2 b_{n-2})$$
$$= \varepsilon_1((l+m)a_{n-1}, a_0, ..., a_{n-2}) + \varepsilon_2((l-m)b_{n-1}, b_0, ..., b_{n-2}) \in Z.$$

Therefore, A_1 is $(l+m)$-constacyclic code and A_2 is $(l-m)$-constacyclic code over $\mathbb{F}_q$.

Conversely, let $z = (z_0, z_1, ..., z_{n-1}) \in Z$ where $z_i = \varepsilon_1 a_i + \varepsilon_2 b_i$. For $(a_0, a_1, ..., a_{n-1}) \in A_1$, $(b_0, b_1, ..., b_{n-1}) \in A_2$, we have

$((l+m)a_{n-1}, a_0, ..., a_{n-2}) \in A_1$ and $((l-m)b_{n-1}, b_0, ..., b_{n-2}) \in A_2$.

Also, $\sigma(z) = \varepsilon_1((l+m)a_{n-1}, a_0, ..., a_{n-2}) + \varepsilon_2((l-m)b_{n-1}, b_0, ..., b_{n-2}) \in Z$.

This implies that Z is a λ-constacyclic code over $\mathfrak{R}$.

Corollary 4.1 The linear code Z of length n over $\mathfrak{R}$ is a u-constacyclic code if and only if A_1 is cyclic and A_2 is negacyclic code over $\mathbb{F}_q$.

Theorem 4.2 If Z is a λ-constacyclic code over $\mathfrak{R}$ of length n, then $\Theta(Z)$ is $(l-m, l+m)$-constacyclic code of

length (n,n) over $\mathbb{F}_q$.

Proof: Let $\overline{z} \in \Theta(\mathrm{Z})$, i.e., $\overline{z} = \Theta(z)$ for some $z = (x_1 + uy_1, x_2 + uy_2, ..., x_n + uy_n) \in \mathrm{Z}$. As Z is a λ -constacyclic code of length n over $\mathfrak{R}$, we have $\sigma(z) = (\lambda(x_n + uy_n), x_1 + uy_1, ..., x_{n-1} + uy_{n-1}) \in \mathrm{Z}$. Now,

$$\sigma(z) = (lx_n + my_n + u(mx_n + ly_n), x_1 + uy_1, ..., x_{n-1} + uy_{n-1}) \text{ and}$$

$$\begin{aligned}\Theta(\sigma(z)) &= ((lx_n + my_n) - (mx_n + ly_n), x_1 - y_1, ..., x_{n-1} - y_{n-1}, lx_n \\ &\quad + my_n + (mx_n + ly_n),\ x_1 + y_1, ..., x_{n-1} + y_{n-1}) \\ &= ((l-m)(x_n - y_n), x_1 - y_1, ..., x_{n-1} - y_{n-1}, (l+m)(x_n + y_n), \\ &\quad x_1 + y_1, ..., x_{n-1} + y_{n-1}) = \tau_1(\overline{z}).\end{aligned}$$

Then $\tau_1(\overline{z}) \in \Theta(\mathrm{Z})$. Hence $\Theta(\mathrm{Z})$ is $(l-m, l+m)$ -constacyclic code over $\mathbb{F}_q$ of length (n,n).

Corollary 4.2 If Z is a u - constacyclic code over $\mathfrak{R}$ of length n, then $\Theta(\mathrm{Z})$ is negacyclic code over $\mathbb{F}_q$ of length (n, n).

5. LCD CODES OVER $\mathfrak{R}$

This section is devoted to the study of Euclidean LCD codes over $\mathfrak{R}$ and establish some important results here. We would like to point out that a result on LCD cyclic codes over $\mathfrak{R}$ of Dinh[22], et al. [Proposition 6.9] is not valid for cyclic codes of an arbitrary length n. Hence, we modify that result and present the corrected version in [Theorem 5.1] for cyclic code of arbitrary length n.

Definition 5.1 For a linear code Z of length n over the ring $\mathfrak{R}$, we say it is reversible if for any codeword $z = (z_0, z_1, ..., z_{n-1}) \in \mathrm{Z}$ implies $z^r = (z_{n-1}, z_{n-2}, ..., z_0) \in \mathrm{Z}$.

Lemma 5.1 [15] If Z is an $[n,k]$-cyclic code over $\mathbb{F}_q$ with generator polynomial $f(y)$, then it is an LCD code if and only if $f(y) = \tilde{f}(y)$ and all the monic irreducible factors of $f(y)$ has same multiplicity in $y^n - 1$ and $f(y)$. In particular, for $\gcd(n,q) = 1$, Z is an LCD code if and only if it is a reversible code.

Lemma 5.2 [23, Theorem 1] Let Z be a cyclic code over a finite field $\mathbb{F}_q$ having generator polynomial $f(y)$. Then Z is reversible code if and only if $f(y) = \tilde{f}(y)$.

Proposition 5.1 Let $\mathrm{Z} = \varepsilon_1 A_1 \oplus \varepsilon_2 A_2$ be any linear code of length n over $\mathfrak{R}$. Then Z is an LCD code if and only if A_1, A_2 both are LCD codes over $\mathbb{F}_q$.

Proof: It can be derived by using Theorem 3.3.

Theorem 5.1 Let $\mathrm{Z} = \varepsilon_1 A_1 \oplus \varepsilon_2 A_2$ be a cyclic code of arbitrary length n over $\mathfrak{R}$. Then Z is an LCD code if and only if the generator polynomial $f_i(y)$ of A_i for $i = 1,2$ is self-reciprocal and multiplicity of each monic irreducible factor of $f_i(y)$ is same in $f_i(y)$ and $y^n - 1$.

Proof: Follows from the Lemma 5.1 and Proposition 5.1.

Theorem 5.2 Let $\gcd(n, p) = 1$ and $\mathrm{Z} = \varepsilon_1 A_1 \oplus \varepsilon_2 A_2$ be a cyclic code over $\mathfrak{R}$ of length n. Then Z is an LCD code if and only if it is reversible.

Proof. Suppose Z is an LCD code over $\mathfrak{R}$. Then A_1, A_2 are LCD codes over $\mathbb{F}_q$, i.e., A_1 and A_2 are reversible codes over $\mathbb{F}_q$ (by Lemma 5.1). This implies $\mathrm{Z} = \varepsilon_1 A_1 \oplus \varepsilon_2 A_2$ is also a reversible code over $\mathfrak{R}$.

Conversely, let Z be a reversible code over $\mathfrak{R}$. Then, $z = \varepsilon_1 x + \varepsilon_2 y \in Z$ implies that $z^r \in \mathrm{Z}$, where $x = (x_0, x_1, ..., x_{n-1}) \in A_1$ and $y = (y_0, y_1, ..., y_{n-1}) \in A_2$. Consider

$$\begin{aligned}z^r &= (\varepsilon_1 x_0 + \varepsilon_2 y_0, \varepsilon_1 x_1 + \varepsilon_2 y_1, ..., \varepsilon_1 x_{n-1} + \varepsilon_2 y_{n-1})^r \\ &= (\varepsilon_1 x_{n-1} + \varepsilon_2 y_{n-1}, \varepsilon_1 x_{n-2} + \varepsilon_2 y_{n-2}, ..., \varepsilon_1 x_0 + \varepsilon_2 y_0) \\ &= \varepsilon_1 x^r + \varepsilon_2 y^r.\end{aligned}$$

This implies that A_1 and A_2 are reversible codes over $\mathbb{F}_q$ and hence LCD codes over $\mathbb{F}_q$. Therefore, Z is an LCD code over $\mathfrak{R}$.

Lemma 5.3 Let Z be a cyclic code over $\mathfrak{R}$ and $\Theta : \mathfrak{R}^n \to \mathbb{F}_q^{2n}$ be the Gray map defined in Section 3. Then $\Theta(\mathrm{Z}) \cap \Theta(\mathrm{Z}^\perp) = \Theta(\mathrm{Z} \cap \mathrm{Z}^\perp)$.

Proof: It can be easily proved.

Theorem 5.3 If Z is a linear code of length n over $\mathfrak{R}$, then Z is an LCD code over $\mathfrak{R}$ if and only if $\Theta(\mathrm{Z})$ is an LCD code over $\mathbb{F}_q$.

Proof: Since Θ is injective and $\Theta(0) = 0$, the result follows from the Lemma 5.3 and Theorem 3.1.

According to the database for linear codes[24] available online and the Gray map defined in Section 3, we present some LCD codes over finite fields with best possible parameters as Gray images of LCD codes over $\mathfrak{R}$. The Magma software[25] has been used to carry out all the computations.

Example 1. The factorization of $y^8 - 1$ over $\mathbb{F}_3$ is

$$y^8 - 1 = (y+1)(y+2)(y^2+1)(y^2+y+2)(y^2+2y+2).$$

The codes $A_1 = \langle y+1 \rangle$, $A_2 = \langle y+2 \rangle$ and $A_3 = \langle y^2+1 \rangle$ are LCD cyclic codes with A_1, A_2 having the parameters [8,7,2] and parameters of A_3 are [8,6,2]. Therefore, $\mathrm{Z} = \varepsilon_1 A_1 + \varepsilon_2 A_2$ and $\overline{\mathrm{Z}} = \varepsilon_1 A_1 + \varepsilon_2 A_3$ are LCD cyclic codes of length 8 over $\mathbb{F}_3 + u\mathbb{F}_3$. Also, $\Theta(\mathrm{Z})$ and $\Theta(\overline{\mathrm{Z}})$ are [16,14,2] and [16,13,2], respectively LCD cyclic codes over $\mathbb{F}_3$. These are the best-known linear codes (BKLC) over $\mathbb{F}_3$ for given length and dimension as shown in Table 1.

Example 2. The factorization of $y^8 - 1$ over $\mathbb{F}_9 = \mathbb{F}_3[\omega]$ is $y^8 - 1 = (y+1)(y+2)(y+\omega)(y+\omega^2)(y+\omega^3)(y+\omega^5)(y+\omega^6)(y+\omega^7)$.

Consider $A_1 = \langle y+1 \rangle$ and $A_2 = \langle y+2 \rangle$. Then A_1 and A_2 are cyclic LCD codes over $\mathbb{F}_8$. Here, both codes have the same parameters [8,7,2]. Also $\mathrm{Z} = \langle \varepsilon_1(y+1) + \varepsilon_2(y+2) \rangle$ is an LCD cyclic code of length 8 over $\mathbb{F}_9 + u\mathbb{F}_9$ with 9^{14} codewords. Moreover, $\Theta(\mathrm{Z})$ is [16,14,2] LCD cyclic code over $\mathbb{F}_9$, which is the best known linear code (BKLC) over $\mathbb{F}_9$ for given length and dimension as shown in Table 1.

Table 1. LCD Code from cyclic code $Z = \langle \varepsilon_1 f_1(y) + \varepsilon_2 f_2(y) \rangle$ over $\mathbb{F}_q + u\mathbb{F}_q$.

q	$f_1(y)$	$f_2(y)$	$\Theta(Z)$	Remark
3	$(y+1)(y+2)$	$(y+2)$	[20,17,2]	BKLC
3	$y+2$	$y+2$	[22,20,2]	BKLC
3	$y+2$	$(y+1)(y+2)$	[22,19,2]	BKLC
3	$y+1$	$y+1$	[28,26,2]	BKLC
3	$y+1$	$y+2$	[16,14,2]	BKLC
3	$y+1$	y^2+1	[16,13,2]	BKLC
3	$(y+1)(y+2)$	$y+1$	[28,25,2]	BKLC
3	y^2+1	$y+2$	[32,29,2]	BKLC
3	$y+1$	$y+2$	[32,30,2]	BKLC
5	$y+4$	$y+1$	[12,10,2]	BKLC
5	$y+1$	$y+4$	[16,14,2]	BKLC
5	$y+4$	$y+1$	[24,22,2]	BKLC
5	$(y+1)(y+4)$	$y+4$	[32,29,2]	BKLC
5	$y+4$	$y+1$	[32,30,2]	BKLC
5	y^2+4y+1	$y+1$	[36,33,2]	BKLC
5	y^2+y+1	$y+4$	[36,33,2]	BKLC
5	$y+1$	$y+4$	[36,34,2]	BKLC
7	$y+6$	$y+1$	[16,14,2]	BKLC
7	$y+6$	$y+6$	[22,20,2]	BKLC
9	$y+1$	$y+2$	[16,14,2]	BKLC
9	$y+2$	$y+2$	[14,12,2]	BKLC

6. HERMITIAN LCD CODES OVER $S = \mathbb{F}_{p^2} + u\mathbb{F}_{p^2}$

This section contains the study of the Hermitian LCD α-constacyclic codes over $\mathbb{F}_{p^2} + u\mathbb{F}_{p^2}$ of length n, where $\alpha \in \mathbb{F}_{p^2} \setminus \{0\}$ and p is an odd prime such that $\gcd(p,n) = 1$. The results that we provide here are also valid for any power of p, in place of p. For any $x + uy \in S$ where $x, y \in \mathbb{F}_{p^2}$, we use $\overline{x+uy} = \bar{x} + u\bar{y} = x^p + uy^p$.

The Hermitian inner product of two elements $z = (z_0, z_1, ..., z_{n-1})$ and $t = (t_0, t_1, ..., t_{n-1})$ in S^n is defined as $\langle z, t \rangle_H = \sum_{i=0}^{n-1} z_i \overline{t_i}$. For any linear code Z over S of length n, its Hermitian dual $Z^{\perp_H}$ is defined as $Z^{\perp_H} = \{s \in S^n : \langle s, z \rangle_H = 0, \forall z \in Z\}$.

Definition 6.1 A linear code Z over S is said to be Hermitian LCD code if and only if $Z \cap Z^{\perp_H} = \{0\}$.

Let ω be a primitive element of $\mathbb{F}_{p^2}$ and μ be a primitive rn^{th} root of unity in an extension field of $\mathbb{F}_{p^2}$ satisfying $\mu^n = \alpha$. Consider $\xi = \mu^r$, it is a primitive n^{th} root of unity and $\mu\xi^j$ are the roots of $y^n - \alpha$ for $j \in \{0,1,...,n-1\}$. Let $F = \{1 + ir \mid 0 \le i \le n-1\}$ and Υ_j denote the p^2-cyclotomic coset modulo rn containing $j \in F$. Then any monic irreducible divisor of $y^n - \alpha$ is of the form $m_j(y) = \prod_{a \in \Upsilon_j} (y - \mu^a)$, i.e., each monic irreducible divisor of $y^n - \alpha$ corresponds to Υ_j, for some $j \in F$. Therefore, the generator polynomial of an α-constacyclic code Z over $\mathbb{F}_{p^2}$ is given by $g(y) = \prod_{w \in W} (y - \mu^w)$, where W is the union of some p^2-cyclotomic cosets modulo rn.

Definition 6.2 Let Z be an α-constacyclic code over $\mathbb{F}_{p^2}$ and $W := \{j \in F \mid g(\mu^j) = 0\}$ where $g(y)$ is the generator polynomial of Z. Then the set W is called the defining set of C.

In fact, the defining set of any α-constacyclic code Z over $\mathbb{F}_{p^2}$ is a union of some Υ_i. Based on the concept of generator polynomials of an α-constacyclic code and its Hermitian dual given in[26], we have the following two lemmas:

Lemma 6.1 If W is a defining set of an α-constacyclic code Z, then the defining set of $Z^{\perp_H}$ is $W' = \{w \in F \mid -pw (\mathrm{mod}\, rn) \notin W\}$.

Lemma 6.2 If the generator polynomial of an α-constacyclic code Z over $\mathbb{F}_{p^2}$ is $g(y) = \prod_{w \in W} (y - \mu^w)$, then the Hermitian dual of Z is $Z^{\perp_H} = \langle h_\perp(y) \rangle$, where, $h_\perp(y) = \prod_{w \in F \setminus W} (y - \mu^{-pw})$.

Lemma 6.3 Let Z be an α-constacyclic code over $\mathbb{F}_{p^2}$ of length n, generated by $g(y)$ and $Z^{\perp_H}$ be its Hermitian dual, generated by $h_\perp(y)$. Then Z is a Hermitian LCD code if and only if $\gcd(g(y), h_\perp(y)) = 1$.

Proof: Let $Z = \langle g(y) \rangle$ be an α-constacyclic code and $Z^{\perp_H} = \langle h_\perp(y) \rangle$ be the Hermitian dual of Z. Then $Z \cap Z^{\perp_H} = \langle r(y) \rangle$, where, $r(y) = lcm(g(y), h_\perp(y))$ i.e.,

$$\deg(r(y)) \le \deg(h_\perp(y)) + \deg(g(y)) = n.$$

Therefore, $Z \cap Z^{\perp_H} = \{0\}$ if and only if $\deg(r(y)) = n$. Since $g(y)$ and $h_\perp(y)$, both divide $y^n - \alpha$, therefore, $r(y)$ divides $y^n - \alpha$. This implies that $Z \cap Z^{\perp_H} = \{0\}$ if and only if $r(y) = y^n - \alpha$. Hence, Z is an Hermitian LCD codes if and only if $\gcd(g(y), h_\perp(y)) = 1$.

Note that the above result can also be proved for Euclidean LCD codes in the similar way.

Proposition 6.1 Let Z be a $p^2 - ary$ α-constacyclic code of length n with defining set W and $W_\perp = \{w \in F \mid -pw (\mathrm{mod}\, rn) \notin W\}$ be the defining set of $Z^{\perp_H}$. Then Z is a Hermitian LCD code if and only if $W \cap W_\perp = \varphi$.

Proof. Trivially follows from Lemma 6.2 and Lemma 6.3.

Theorem 6.1 Let $Z = \varepsilon_1 A_1 \oplus \varepsilon_2 A_2$ be a linear code over S of length n. Then the Hermitian dual of Z is $Z^{\perp_H} = \varepsilon_1 A_1^{\perp_H} + \varepsilon_2 A_2^{\perp_H}$. Moreover, Z is a Hermitian LCD code if and only if A_1, A_2 both are Hermitian LCD codes over $\mathbb{F}_{p^2}$.

Proof. Same procedure follows as given in Corollary 3.2 of Cengellenmis [4] and Proposition 5.1.

Corollary 6.1 Let $Z = \varepsilon_1 A_1 \oplus \varepsilon_2 A_2$ be an α-constacyclic code over S where A_1 and A_2 both are α-constacyclic code over $\mathbb{F}_{p^2}$ with defining sets W^1 and W^2, respectively. Then Z is a Hermitian LCD code if and only if $W^1 \cap W^1_{\perp} = \varphi$ and $W^2 \cap W^2_{\perp} = \varphi$ where $W^1_{\perp}$ and $W^2_{\perp}$ are defining sets for the Hermitian duals of A_1 and A_2, respectively.

Lemma 6.4 Let Z be a linear code over S and $\Theta : S^n \to \mathbb{F}_q^{2n}$ be the Gray map defined in Section 3. Then $\Theta(Z) \cap \Theta(Z)^{\perp_H} = \Theta(Z \cap Z^{\perp_H})$.

Proof. It can be seen that $\Theta(Z^{\perp_H}) = \Theta(Z)^{\perp_H}$ and rest of the proof is similar to Lemma 5.3.

Theorem 6.2 Let $Z = \varepsilon_1 A_1 \oplus \varepsilon_2 A_2$ be a linear code of length n over S. Then Z is a Hermitian LCD code over S if and only if $\Theta(Z)$ is a Hermitian LCD code over $\mathbb{F}_{p^2}$.

Proof. Follows from Lemma 6.4, as Θ is injective and $\Theta(0) = 0$.

Here, authors provided some examples of Hermitian LCD codes to elaborate our main results of this section as shown in Table 2.

Table 2. Hermitian LCD Code from Cyclic Code $Z = \langle \varepsilon_1 g_1(y) + \varepsilon_2 g_2(y) \rangle$ over $\mathbb{F}_{p^2} + u\mathbb{F}_{p^2}$ In this table, " * " represents a BKLC code over $\mathbb{F}_{p^2}$.

P^2	$g_1(y)$	$g_2(y)$	Z	Θ(Z)
9	$(y+1)$	$y+2$	$(16,9^{30},2)$	$[32,30,2]^*$
9	$y+2$	$y+2$	$(17,9^{32},2)$	$[34,32,2]^*$
9	$y+\omega^6$	$y+\omega^2$	$(20,9^{38},2)$	$[40,38,2]^*$
9	$y+2$	$y+1$	$(22,9^{42},2)$	$[44,42,2]^*$
9	$y+2$	$y+2$	$(19,9^{36},2)$	$[38,36,2]^*$
9	$(y+\omega^6)$ $(y+2)$	$y+1$ $(y+1)$	$(8,9^{14},2)$	$[16,14,2]^*$
9	$(y^2+\omega^7 y+1)$ $(y^2+\omega^5 y+1)$	$(y^2+\omega^3 y+1)$ $(y^2+\omega y+1)$	$(10,9^{10},4)$	$[20,10,4]$
9	$(y+2)$	$(y+2)$	$(11,9^{20},2)$	$[22,20,2]^*$
9	$(y+1)$	$(y+2)$	$(14,9^{26},2)$	$[28,26,2]^*$
25	$(y+4)(y+1)$ $(y+\omega^4)(y+\omega^{20})$	$(y+1)$ $(y+\omega^4)(y+\omega^{20})$	$(6,25^5,4)$	$[12,5,4]$
25	$(y+\omega^8)(y+\omega^{16})$	$(y+\omega^4)(y+\omega^{20})$	$(6,25^8,2)$	$[12,8,2]$
25	$y+1$	$(y+2)(y+3)$	$(16,25^{29},2)$	$[32,29,2]$
25	$y+1$	$y+1$	$(16,25^{30},2)$	$[32,30,2]$
49	$y+6$	$y+1$	$(8,49^{14},2)$	$[16,14,2]$
49	$y+1$	$y+1$	$(10,49^{18},2)$	$[20,18,2]$
49	$y+6$	$y+6$	$(9,49^{16},2)$	$[18,16,2]$
49	$(y+\omega^6)(y+\omega^{12})$ $(y+\omega^{36})(y+\omega^{42})$	$(y+1)(y+\omega^6)(y+\omega^{12})$ $(y+\omega^{36})(y+\omega^{42})$	$(8,49^7,4)$	$[16,7,4]$
49	$(y+1)(y+\omega^6)$ $(y+\omega^{12})(y+\omega^{36})$ $(y+\omega^{42})$	$(y+1)(y+6)$ $(y+\omega^6)(y+\omega^{12})$ $(y+\omega^{36})(y+\omega^{42})$	$(8,49^5,6)$	$[16,5,6]$

7. APPLICATIONS

In this section, we explain the importance of LCD codes in sharing secret information through a channel. Secret sharing scheme (SSS) is a method in which dealer distributes the pieces of the secret information among participants. This method is basically used when we cannot trust a single person owing the secret. Therefore, the secret is distributed among participants. Now, we define some basic terms.

Dealer: Distributer of the pieces of the secret information.

Encryption: It is a process of converting information into a suitable form (called encrypted message) so that only authorized parties can read the information.

Shares: These are the pieces of the information.

Decryption: It is the process of retrieving back the information from the encrypted message.

7.1 Multisecret Sharing Scheme

Multisecret Sharing Scheme is an important class of secret sharing scheme. In this scheme, participants do not transmit the secret share but a pseudo-share which is computed from their secret share. We use the method used Alahmadi[27], *et al.* with slight modification to elaborate our approach for Hermitian LCD code.

Let Z be a Hermitian LCD code of length n over $\mathbb{F}_{p^2}$ with generator matrix G and the generator matrix of its Hermitian dual $Z^{\perp_H}$ be D. Then $G\overline{D}^t = 0$, where $\overline{D}^t = [\overline{d_{ij}}]^t$ and $\overline{d_{ij}} = d_{ij}^p$.

Encryption: Given that the secret $K = (k_1, k_2, ..., k_n) \in Z$ then the share ℓ corresponding to x is computed by $\ell = x\overline{K}^t$. Now, the secret K is encrypted as $L = (\ell_1, \ell_2, ..., \ell_k)$ and distributed among the participants, where ℓ_i is the share corresponding to the i^{th} row of G.

Decryption: The secret K can be recovered by solving the following system of equations:

$$G\overline{K}^t = L \text{ and } D\overline{K}^t = 0$$

where $L = (\ell_1, \ell_2, ..., \ell_k)$ is the received encrypted message. Since Z is an LCD code, $\begin{bmatrix} G \\ D \end{bmatrix}$ is an invertible matrix and the secret K can be retrieved uniquely.

Example 3: Consider $a\,[12,5,4]$ code over $\mathbb{F}_{25}$ with the generator matrix

$$G = \begin{bmatrix} 1&0&0&0&0&1&1&0&0&0&0&1 \\ 0&1&0&0&0&4&0&1&0&0&0&4 \\ 0&0&1&0&0&1&0&0&1&0&0&1 \\ 0&0&0&1&0&4&0&0&0&1&0&4 \\ 0&0&0&0&1&1&0&0&0&0&1&1 \end{bmatrix} = \begin{bmatrix} g_1 \\ g_2 \\ g_3 \\ g_4 \\ g_5 \end{bmatrix}.$$

It is a Hermitian LCD code with the generator matrix of $Z^{\perp_H}$ as

$$D = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 1 & 4 & 1 & 4 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 4 & 1 & 4 & 1 & 4 \end{bmatrix} = \begin{bmatrix} h_1 \\ h_2 \\ h_3 \\ h_4 \\ h_5 \\ h_6 \\ h_7 \end{bmatrix},$$

i.e., $G\overline{D}^t = 0$.

Assume that our secret vector is $K = (010004010004) \in Z$. Then the shares for the participants are calculated as

$$\ell_1 = g_1\overline{K}^t = 3,\ \ell_2 = g_2\overline{K}^t = 4,\ \ell_3 = g_3\overline{K}^t = 3,\ \ell_4 = g_4\overline{K}^t = 2,\ \ell_5 = g_5\overline{K}^t = 3.$$

i.e., the received encrypted message is

$$L = \begin{bmatrix} \ell_1 \\ \ell_2 \\ \ell_3 \\ \ell_4 \\ \ell_5 \end{bmatrix}.$$

To retrieve back the secret, we solve the system

$$\begin{bmatrix} G \\ D \end{bmatrix} X = \begin{bmatrix} L \\ 0 \end{bmatrix}.$$

and get $X = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 4 & 0 & 1 & 0 & 0 & 0 & 4 \end{bmatrix}^t$.

Therefore, the secret is $K = \overline{X}^t$.

Note that we can also use Euclidean LCD code in above scheme with slight modification. Also, we have not used the concept of minimum distance in this scheme. Therefore, the $[n,k,d]$ Euclidean or Hermitian LCD codes that we provide even with very small minimum distance are of great significance.

8. CONCLUSION

In this paper, we examined LCD codes over $\mathfrak{R}$ of arbitrary length n and obtained some best known LCD codes over finite field as Gray image of these codes. We have provided generator polynomials for cyclic codes over $\mathfrak{R}$ and also some results on constacyclic codes over $\mathfrak{R}$ along with their Gray images. Further, we discussed Hermitian LCD codes and some related results. Finally, some examples related to Euclidean and Hermitian LCD codes (some of them are BKLC) are also provided along with their applications. Interested readers are cordially invited to further obtain more examples of LCD codes with better parameters by using our results (specially, on Hermitian LCD). A possible direction for the future work could be studying LCD codes considering different rings are still open.

REFERENCES

1. Hammons, A. R.; Kumar, P. V.; Calderbank, A. R.; Slone, N. J. A. & Sole, P. The $\mathbb{Z}_4$-linearity of Kerdock Preparata Goethals and related codes. *IEEE T. Inform. Theory,* 1994, **40**(2), 301-319. doi: 10.1109/18.312154
2. Greferath, M. & Schmidt, S. E. Gray isometries for finite chain rings and a nonlinear ternary (36, 3^{12}, 15) code. *IEEE T. Inform. Theory*, 1999, **45**(7), 2522-2524. doi: 10.1109/18.796395
3. Ashraf, M. & Mohammad, G. On skew cyclic codes over a semi-local ring. *Discrete Math. Algorithms Appl.*, 2015, **7**(4), 1550042(10 pages). doi: 10.1142/S17938309155004
4. Cengellenmis, Y. On the Cyclic Codes over $\mathbb{F}_3 + v\mathbb{F}_3$. *Int. J. Algebra,* 2010, **4**(6), 253- 59.
5. Gao, J. & Wang, Y. u-Constacyclic codes over $\mathbb{F}_p + u\mathbb{F}_p$ and their applications of constructing new non-binary quantum codes. *Quantum Inf. Process.,* 2018, **17**(4), 1-9. doi: 10.1007/s11128-017-1775-8
6. Sharma, A. & Bhaintwal, M. A class of 2D skew-cyclic codes over $\mathbb{F}_q + u\mathbb{F}_q$. *Appl. Algebra Eng. Comm.*, 2019, **30**(6), 471-90. doi: 10.1007/s00200-019-00388-w
7. Shi, M.; Yang, S. & Zhu, S. Good $p-ary$ quasi-cyclic codes from cyclic codes over $\mathbb{F}_p + v\mathbb{F}_p$. *J. Syst. Sci. Complex*, 2012, **25**(2), 375-84. doi: 10.1007/s11424-012-0076-7
8. Ashraf, M. & Mohammad, G. *Quantum codes from cyclic codes Over* $\mathbb{F}_3 + v\mathbb{F}_3$. *Int. J. Quantum Inf.,* 2014, **12**(6), 1450042(8 pages). doi: 10.1142/S0219749914500427
9. Abualrub, T. & Siap, I. Constacyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$. *J. Franklin Inst.*, 2009, **346**(5), 520-29. doi: 101016/jjfranklin.2009.02.001
10. Cengellenmis, Y.; Dertli, A. & Aydin, N. Some Constacyclic Codes over $\mathbb{Z}_4/(u^2)$, New Gray maps and New quaternary code. *Algebra Colloq.,* 2018, **25**(3), 369-76. doi: 10.1142/S1005386718000263
11. Islam, H. & Prakash, O. A class of constacyclic codes over the ring $\mathbb{Z}_4[u,v]/(u^2, v^2, uv - vu)$ and their Gray images. *Filomat*, 2019, **33**(8), 2237-248. doi: 10.2298/FIL1908237I
12. Islam, H.; Bag, T. & Prakash, O. A class of constacyclic codes over $\mathbb{Z}_4[u]/\langle u^k \rangle$. *J. Appl. Math. Comput.*, 2019, **60**(1-2), 237-251. doi: 10.1007/s12190-018-1211-y
13. Shi, M.; Qian, L.; Sok, L.; Aydin, N. & Sole, P. On constacyclic codes over $\mathbb{Z}_4[u]/(u^2-1)$ and their Gray images. *Finite Fields Appl.,* 2017, **45**, 86-95. doi: 10.1016/j.ffa.2016.11.016
14. Massey, J. L. Linear codes with complementary duals. *Discrete Mathematics*, 1992, **106/107**, 337-342. doi: 10.1016/0012-365X(92)90563-U
15. Yang, X. & Massey, J. L. The condition for a cyclic code to have a complementary dual. *Discrete Mathematics*,1994 **126**, 391-393. doi: 10.1016/0012365X (94)90283-6
16. Sendrier, N. Linear codes with complementary duals meet the Gilbert-Varshamov bound. Discrete Math.,2004, **285**(1-3), 345-347. doi: 10.1016/j.disc.2004.05.005
17. Liu, X. & Liu, H. LCD codes over finite chain rings.

Finite Fields Appl., 2015, **34**, 1-19.
doi: 10.1016/j.ffa.2015.01.004

18. Li, C. Hermitian LCD codes from cyclic codes. *Design Code. Cryptogr.*, 2018, **86**, 2261-278. doi: 10.1007/s10623-017-0447-0
19. Liu, H.; Peng, H. & Liu, X. Skew cyclic and LCD codes over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q$. *J. Math. (PRC)*, 2018, **38**(3), 459-66.
20. Liu, Z. & Wang, J. Linear complementary dual codes over rings. *Design Code. Cryptogr.*, 2019, **87**, 3077-086. doi: 10.1007/s10623-019-00664-3
21. Carlet, C. & Guilley, S. Complementary dual codes for counter-measures to side-channel attacks. *Adv. Math. Commun*., 2016, **10**(1), 131-150. doi: 10.3934/amc.2016.10.131
22. Dinh, H. Q.; Bag, T.; Upadhyay, A. K.; Bandi, R. & Chinnakum, W. On the structure of cyclic codes over $\mathbb{F}_q RS$ and applications in quantum and LCD codes constructions. *IEEE Access*, 2020, **8**, 18902-18914. doi: 10.1109/ACCESS.2020.2966542
23. Massey, J. L. Reversible codes. *Inform. Control,* 1964, **7**(3), 369-80. doi: 10.1016/S0019-9958(64)90438-3
24. Grassl, M. Table of bounds on linear codes. http://www.codetables.de.
25. Bosma, W. & Cannon, J. Handbook of magma functions, Univ. of Sydney, Sydney, 1995.
26. Kai, X.; Zhu, S. & Li, P. Constacyclic Codes and Some New Quantum MDS Codes. *IEEE T. Inform. Theory*, 2014, **60**(4), 2080−086. doi: 10.1109/TIT .2014.2308180
27. Alahmadi, A.; Altassan, A.; AlKenani, A.; Calkavur, S.; Shoaib, H. & Sole, P. A Multisecret-Sharing Scheme Based on LCD Codes. *Mathematics*, 2020, **8**(2), 272-82. doi: 10.3390/math8020272

ACKNOWLEDGEMENT

The authors are thankful to the Indian Institute of Technology Patna for providing financial support and research facilities. The authors would also like to thank the Editor and anonymous referee(s) for careful reading and constructive suggestions to improve the presentation of the manuscript.

CONTRIBUTORS

Dr Om Prakash has completed his MSc from Patna University, Patna, in 1999, and PhD from Banasthali University, Rajasthan, in 2010. Currently working as an Associate Professor at the Department of Mathematics, Indian Institute of Technology Patna. His main research interest includes rings and modules, algebraic coding theory, algebraic graph theory, and algebraic number theory. He has the credit of publishing more than 45 research articles in the journals.
In the current study, he has suggested the problem, provided guidance to develop the results on LCD codes and reviewed the final manuscript.

Ms Shikha Yadav completed her BSc and MSc in Mathematics from the University of Delhi in 2015 and 2017, respectively. Currently, pursuing her PhD at the Department of Mathematics, Indian Institute of Technology Patna and her research field includes algebraic coding theory and cryptography.
In the current study, she has developed all the results of the manuscript and constructed suitable examples based on the developed results and finally prepared the manuscript.

Mr Ram Krishna Verma received his BSc and MSc from University of Lucknow, in 2012 and 2014, respectively. He is currently pursuing his PhD from the Department of Mathematics, Indian Institute of Technology Patna. His research interest includes information theory and algebraic coding theory.
In the current study, he has prepared the manuscript and also helped in examples and applications during discussion.