LCD and ACD codes over a non commutative non-unital ring with four elements

Minjia Shi, Shitao Li, Jon-Lark Kim, Patrick Solé

LCD and ACD codes over a noncommutative non-unital ring with four elements*

Minjia Shi[†], Shitao Li[‡], Jon-Lark Kim[§], Patrick Solé[¶‖]

Abstract

We study LCD (linear complementary dual) and ACD (additive complementary dual) codes over a noncommutative non-unital ring E with four elements. This is the first attempt to construct LCD codes over a noncommutative non-unital ring. We show that free LCD codes over E are directly related to binary LCD codes. We introduce ACD codes over E. They include free LCD codes over E as a special case. These facts imply that LCD and ACD codes over E are worth studying. In particular, we characterize a free LCD E-code C in terms of a binary generator matrix G. We also define an ACD code over E, called a left-ACD code. We give several conditions for the existence of left-ACD codes.

keywords additive codes, LCD codes, non-unitary ring

MSC(2010): Primary 94 B05, Secondary 16 L 30.

*This research is supported by National Natural Science Foundation of China (12071001, 61672036), Excellent Youth Foundation of Natural Science Foundation of Anhui Province (1808085J20), the Academic Fund for Outstanding Talents in Universities (gxbjZD03).

[†]smjwcl.good@163.com

[‡]lishitao0216@163.com

[§]jlkim@sogang.ac.kr

[¶]sole@enst.fr

[‖]Minjia Shi and Shitao Li are with School of Mathematical Sciences, Anhui University, Hefei, 230601, China. Jon-Lark Kim is with Department of Mathematics, Sogang University, Seoul, South Korea. Patrick Solé is with Aix Marseille Univ, CNRS, Centrale Marseille, I2M, Marseille, France.

1 Introduction

Algebraic coding theory has been developed extensively since the inception of error-correcting codes by Hamming and Shannon in the late 1940s. The most well-known constructions are linear codes including Reed-Solomon codes, Reed-Muller codes, BCH codes, quadratic residue codes, Algebraic Geometry codes, and self-dual codes. Recently, LCD (linear complementary dual) codes have been very popular due to their connection to side channel attacks.

We recall that a *linear* $[n, k]$ *code* over a finite field $GF(q)$ or $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$. The *dual* of C is denoted by $C^\perp$ which is the set of vectors orthogonal to C under the usual inner product. A linear code $\mathcal{C}$ is called *self-orthogonal* if $C \subset C^\perp$. A linear code C is called an *LCD code* (linear complementary dual code) if $C \cap C^\perp = \{0\}$. Hence being LCD is the opposite concept of self-orthogonality.

An LCD code was first introduced by [8] as a reversible code in 1964 in order to provide an optimum linear coding solution for the two-user binary adder channel. Massey [9] showed that there exist asymptotically good LCD codes. Sendrier [12] showed that LCD codes meet the asymptotic Gilbert-Varshamov bound using the hull dimension spectra of linear codes. In 2014, Carlet and Guilley [2] introduced several constructions of LCD codes and investigated an application of LCD codes against Side-Channel Attacks (SCA) and Fault Injection Attacks (FIA). SCA consist in passively recording some leakage, that is the source of information to retrieve the key. FIA consist in actively perturbing the computation so as to obtain exploitable differences at the output.

In the Carlet-Guilley's Boolean masking approach, the direct sum $C \oplus C^\perp = \mathbb{F}_q^n$ is essential, the minimum distance of C (resp. $C^\perp$) acting as a performance criterion for SCA (resp. FIA). Since this model does not use the linearity of C but only its additivity, it makes sense to study Additive Complementary Dual (ACD) codes over finite fields or finite rings. Moreover, since additive codes include linear codes, ACD codes include LCD codes.

On the other hand, Alahmadi, et al. [1] considered the finite noncommutative non-unital ring E with four elements in the notation of Fine [4] and studied Type IV codes over this ring. Later, Kim and Ohk showed that the ring E has the complement map and GC-content map so that it can be used to construct DNA codes [6].

These two aspects motivate the current paper. Here, we consider LCD and additive complementary dual (ACD) codes over E. The ring E is not

a Frobenius ring. Thus this is the first nontrivial attempt to study LCD codes over such a ring. We show that free LCD codes over E contain binary LCD codes while ACD codes over E include free LCD codes over E as a special case. These facts imply that LCD codes over E are worth studying. In particular, we characterize a free LCD E-code C in terms of a binary generator matrix G. We also define an ACD code over E, called a left-ACD code. We give several conditions for the existence of left-ACD codes over E.

We remark that little is known about ACD over $\mathbb{F}_4$,. We reserve the study of ACD codes over $\mathbb{F}_4$, which is algebraically easier but computationally more demanding, for a companion paper [11]. Hence one may compare ACD codes over E with Hermitian LCD codes over $\mathbb{F}_4$ [7]. Based on Examples in Section 3 and the fact that ACD codes over E are additive groups, the minimum distances of ACD codes over E seem as good as those of Hermitian LCD codes over $\mathbb{F}_4$.

The material is arranged as follows. The next section is dedicated to LCD codes over E. Section 3 studies ACD codes over E. Section 4 concludes the paper.

2 Codes over a finite ring with four elements

Recall that the ring E is defined as a ring on two generators a and b with the following relations.

$$E = \langle a, b \,|\, 2a = 2b = 0, a^2 = a, b^2 = b, ab = a, ba = b \rangle.$$

The addition table is immediate to derive, writing 0 for the neutral element of the addition law, and c for the sum $a + b$. Its multiplication table is given as follows. Note that E does not have a unity or a unit. Nevertheless, we have $xa = x$ for all $x \in E$.

$\times$	0	a	b	c
0	0	0	0	0
a	0	a	a	0
b	0	b	b	0
c	0	c	c	0

Table 1: Multiplication table of the ring E

The ring E is local with maximal ideal $J = \{0, c\}$, and residue field $E/J = \mathbb{F}_2 = \{0, 1\}$, the finite field of order 2.

Denote by $\alpha : E \to E/J = \mathbb{F}_2$, the map of reduction modulo J. Thus $\alpha(0) = \alpha(c) = 0$, and $\alpha(a) = \alpha(b) = 1$. This map is extended in the natural way in a map (still denoted by α) from E^n to $\mathbb{F}_2^n$.

If $e \in E$ and $b \in \mathbb{F}_2$ then $eb = e$ if $b = 1$ and zero otherwise. This convention is extended naturally to vectors $\mathbf{b} \in \mathbb{F}_2^n$. Alahmadi et al. [1] introduced linear codes over E. A *linear E-code C of length n* is a left E-submodule of E^n. An *additive code* of length n over E is any additive subgroup of E^n. The parameters of such a code with minimum distance d are written compactly as $(n, |C|, d)$. Two codes A and B over E are called *permutation-equivalent* if and only if there is a coordinate permutation that maps on the other. Let C be a linear E-code of length n. With that code we associate two binary codes of length n :

(1) the **residue code** defined by $Res(C) = \{\alpha(\mathbf{y}) \mid \mathbf{y} \in C\}$,

(2) the **torsion code** defined by $Tor(C) = \{\mathbf{u} \in \mathbb{F}_2^n \mid c\mathbf{u} \in C\}$.

Following a well-established tradition [1, 10], we denote by k_1 (resp. k_1+k_2) the dimension of $Res(C)$ (resp. $Tor(C)$).

The *left dual* $C^{\perp_L}$ of C is the left module defined by

$$C^{\perp_L} = \{\mathbf{y} \in E^n \mid \forall\ \mathbf{x} \in C,\ (\mathbf{y}, \mathbf{x}) = 0\},$$

where $(\mathbf{y}, \mathbf{x}) = \sum_{i=1}^{n} y_i x_i$ for $\mathbf{y} = (y_1, \ldots, y_n)$ and $\mathbf{x} = (x_1, \ldots, x_n)$.

Similarly, the *right dual* $C^{\perp_R}$ of C is the right module defined by

$$C^{\perp_R} = \{\mathbf{y} \in E^n \mid \forall\ \mathbf{x} \in C,\ (\mathbf{x}, \mathbf{y}) = 0\}.$$

Definition 1. A linear E-code C is called *left-nice* if

$$|C||C^{\perp_L}| = 4^n.$$

Definition 2. A linear E-code C is *self-orthogonal* if $C \subset C^{\perp_L}$.

Definition 3. A linear E-code C is *left-LCD* if it is left-nice and $C \cap C^{\perp_L} = \{\mathbf{0}\}$.

Therefore, C is *left-LCD* if and only if $C \oplus C^{\perp_L} = E^n$.

Remark 1. We remark that there is no right-LCD linear E-code. If $C \neq \{\mathbf{0}\}$ is a linear E-code, then there is a codeword $\mathbf{y} = c\mathbf{v}$ in C, where $\mathbf{v}$ is a binary vector. Now $\mathbf{y}$ is also in $C^{\perp_R}$ since $(\mathbf{x}, \mathbf{y}) = 0$ for any $\mathbf{x} \in C$. Thus $C \cap C^{\perp_R} \neq \{\mathbf{0}\}$. Hence there is no need to consider right-LCD E-code. From now on, we will call left-LCD as LCD.

From now on we only consider a left-dual of a linear E-code C.

Definition 4. Let C be a linear E-code. Let $S = \{\mathbf{s}_1, \ldots, \mathbf{s}_m\}$ be a subset of C. The (left) E-span of S is defined by $\langle S \rangle_E := \{\alpha_1\mathbf{s}_1 + \cdots + \alpha_m\mathbf{s}_m \mid \alpha_i \in E \text{ for any } i\}$. The additive span of S is defined by $\langle S \rangle_{\mathbb{F}_2} := \{\gamma_1\mathbf{s}_1 + \cdots + \gamma_m\mathbf{s}_m \mid \gamma_i = 0 \text{ or } 1 \text{ for any } i\}$. Since there is no unitary in E, $\langle S \rangle_E$ does not necessarily contain $\langle S \rangle_{\mathbb{F}_2}$.

A subset $S = \{\mathbf{s}_1, \ldots, \mathbf{s}_m\}$ of C is called a *generating set for* C if $\langle S \rangle_E \cup \langle S \rangle_{\mathbb{F}_2}$ is equal to C. If $S = \{\mathbf{s}_1, \ldots, \mathbf{s}_m\}$ of C is a generating set for C, then a *generator matrix* G_E for C is an $m \times n$ matrix whose rows are $\mathbf{s}_1, \ldots, \mathbf{s}_m$ so that $\langle G \rangle_E$ means $\langle S \rangle_E \cup \langle S \rangle_{\mathbb{F}_2}$. A linear E-code C is *free* if C is a finite direct sum of E (E as a left E-module), that is, $C = E \oplus \cdots \oplus E$, where $E = \langle \mathbf{s}_i \rangle_E$ for some $\mathbf{s}_i \in E$.

Lemma 1. *If C is a free linear E-code with generator matrix G_E, then*

(1) $C = \langle aG \rangle_E$ for some binary matrix G.

(2) $C^{\perp_L} = \langle aH \rangle_E$ for some binary parity check matrix H.

Proof. We first show (1). Since C is free, there exists a generating set $S = \{\mathbf{s}_1, \ldots, \mathbf{s}_m\} \subset C$ such that $C = \langle \mathbf{s}_1 \rangle_E \oplus \cdots \oplus \langle \mathbf{s}_m \rangle_E$, where $\langle \mathbf{s}_i \rangle_E = E$ for each i. Note that $\langle \mathbf{s}_i \rangle_E = \langle a\mathbf{s}_i \rangle_E$ for any $i = 1, \ldots, m$. Let G_E consist of the rows $a\mathbf{s}_i = a\mathbf{s}_i'$, where $\mathbf{s}_i'$ is a binary vector. Therefore, by applying elementary row operations on G_E and by permuting columns of G_E, we may assume that its generator matrix $G_E = [aI|aA]$, where aI is a diagonal matrix with a's on the diagonal and A is a binary matrix. Thus $C = \langle aG \rangle_E$ for some binary matrix G.

Next we show (2), that is,

$$C^{\perp_L} = \langle aH \rangle_E , \tag{1}$$

for some binary parity check matrix H related to G. Noting that $(aH)(aG)^T = aHG^T = 0$, we have $\langle aH \rangle_E \subset C^{\perp_L}$. It remains to show that $C^{\perp_L} \subset \langle aH \rangle_E$.

Suppose $\mathbf{y} = (y_1, y_2, \ldots, y_n) \in C^{\perp_L}$. We may assume that G is of the standard form $G = [I|A]$. Let

$$aG = a[I|A] = \begin{bmatrix} a\mathbf{r}_1 \\ a\mathbf{r}_2 \\ \vdots \\ a\mathbf{r}_k \end{bmatrix},$$

where $\mathbf{r}_i$'s are the binary rows of G. Then $(\mathbf{y}, a\mathbf{r}_i) = 0$ for $1 \le i \le k$. That is, for each $1 \le i \le k$, $y_{i_1}a + \cdots + y_{i_j}a = (y_{i_1} + \cdots + y_{i_j})a = 0$ for some $1 \le j \le k$. Then $y_{i_1} + \cdots + y_{i_j} = 0$ by the multiplication table. More precisely, since G is of the standard form, we have the following k equations.

$$\begin{gathered} y_1 + 0 + 0 + \cdots + 0 + y_{k+i_1} + \cdots + y_{i_{s_1}} = 0 \\ 0 + y_2 + 0 + \cdots + 0 + y_{k+i_2} + \cdots + y_{i_{s_2}} = 0 \\ \vdots \\ 0 + 0 + \cdots + 0 + y_k + y_{k+i_k} + \cdots + y_{s_k} = 0 \end{gathered}$$

where for each $j = 1, \ldots, k$, the indices $k + i_j, \ldots, i_{s_j}$ of y correspond to the nonzero positions of $a\mathbf{r}_j$. Since there are at most $n - k$ free variables in the above k equations, there are at most 4^{n-k} solutions for $\mathbf{y}$, that is, $|C^{\perp_L}| \le 4^{n-k}$. Since there are already $|\langle aH \rangle_E| = 4^{n-k}$ elements in $C^{\perp_L}$, we can conclude that $C^{\perp_L} = \langle aH \rangle_E$. □

Corollary 1. *Any linear E-code C is permutation-equivalent to an additive E-code with an additive generator matrix of the form*

$$\begin{bmatrix} aI_{k_1} & aX & aY \\ bI_{k_1} & bX & bY \\ \boldsymbol{0} & cI_{k_2} & cZ \end{bmatrix}, \tag{2}$$

where I_j denotes the identity matrix of order j, the matrices X, Y, Z are binary matrices. Therefore, $C = \langle aG \rangle_E$ for some binary matrix G.

Proof. Let $C' = \langle C \rangle_E$. Then C' is free. By Lemma 1, $C' = \langle aG_1 \rangle$ for some binary matrix G_1. We may assume that G_1 is of the form $[I_{k_1}|A]$. For any $\mathbf{x} \in C \backslash C'$, we may assume $\mathbf{x} = (\underbrace{0, \cdots, 0}_{k_1}, \mathbf{x}')$. Since $\mathbf{x} + a\mathbf{x} = c\mathbf{x}_2$ for some binary vector $\mathbf{x}_2$, where $a\mathbf{x} \in C', c\mathbf{x}_2 \notin C'$, we have $\mathbf{x} = a\mathbf{x} + c\mathbf{x}_2$. Therefore, we can find a set $S_2 = \{c\mathbf{x}_2^1, \ldots, c\mathbf{x}_2^{k_2} \mid \mathbf{x}_2^j \text{ is a binary vector for any } j\}$ such

that they are $\mathbb{F}_2$-linearly independent and $C = C' \oplus \langle S_2 \rangle_{\mathbb{F}_2}$. This completes the proof. □

We define a map $\phi : E \to E$, $\phi(0) = 0, \phi(a) = c, \phi(b) = b, \phi(c) = a$. For $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in E^n$, define $\phi(\mathbf{x}) = (\phi(x_1), \phi(x_2), \ldots, \phi(x_n))$. It is easy to check that $\phi(z)x = \phi(zx)$ and $\phi(x + y) = \phi(x) + \phi(y)$, for $x, y, z \in E$. Hence for $z \in E, \mathbf{x}, \mathbf{y} \in E^n$, we have

$$\phi(z)\mathbf{x} = \phi(z\mathbf{x}), \ \phi(\mathbf{x} + \mathbf{y}) = \phi(\mathbf{x}) + \phi(\mathbf{y}).$$

Lemma 2. *If C is a linear E-code, then C is free if and only if for any $c\boldsymbol{u} \in C$ with $\boldsymbol{u}$ is a binary vector, we have $a\boldsymbol{u} \in C$.*

Proof. Since C is free, there exists a generating set $S = \{\mathbf{s}_1, \ldots, \mathbf{s}_m\} \subset C$ such that $C = \langle \mathbf{s}_1 \rangle_E \oplus \cdots \oplus \langle \mathbf{s}_m \rangle_E$. If $c\mathbf{u} = \alpha_1\mathbf{s}_1 + \cdots + \alpha_m\mathbf{s}_m$, we have

$$\begin{aligned} a\mathbf{u} = a(a\mathbf{u}) = \phi(c)a\mathbf{u} = \phi(ca\mathbf{u}) = \phi(c\mathbf{u}) &= \phi(\alpha_1\mathbf{s}_1 + \cdots + \alpha_m\mathbf{s}_m) \\ &= \phi(\alpha_1)\mathbf{s}_1 + \cdots + \phi(\alpha_m)\mathbf{s}_m. \end{aligned}$$

Hence $a\mathbf{u} \in C$. Conversely, it is easy to check $k_2 = 0$. Hence C is free. □

Lemma 3. *If C is a linear E-code, then $C = (C^{\perp_L})^{\perp_L}$ if and only if C is free.*

Proof. By Corollary 1, we can assume C has an additive generator matrix

$$G = \begin{bmatrix} aI_{k_1} & aX & aY \\ bI_{k_1} & bX & bY \\ \mathbf{0} & cI_{k_2} & cZ \end{bmatrix}.$$

Let $G_1 = \begin{bmatrix} aI_{k_1} & aX & aY \\ bI_{k_1} & bX & bY \end{bmatrix}$ and B be a linear E-code with generator matrix G_1. Obvious, B is free and $B \subseteq C$. Clearly, $C^{\perp_L} \subseteq B^{\perp_L}$. To prove the opposite direction, suppose v is in $B^{\perp_L}$. By definition, v is orthogonal to any row of G_1. Since c is an annihilator if multiplied on the right, v is also orthogonal to any row of the matrix $\begin{bmatrix} 0 & cI_{k_2} & cZ \end{bmatrix}$. Hence v is orthogonal to any row of G_1, so $B^{\perp_L} \subseteq C^{\perp_L}$, which implies that $B^{\perp_L} = C^{\perp_L}$. Hence $(B^{\perp_L})^{\perp_L} = (C^{\perp_L})^{\perp_L}$.

Since $B^{\perp_L}, (B^{\perp_L})^{\perp_L}$ are free by Lemma 1, we know that $B, B^{\perp_L}$ are left-nice. Since $|B| = 4^{k_1}$ and $|B^{\perp_L}| = 4^{n-k_1}$, we have $|(B^{\perp_L})^{\perp_L}| = 4^{n-(n-k_1)} =$

4^{k_1}, which implies that $|B| = |(B^{\perp_L})^{\perp_L}|$. Since B and $B^{\perp_L}$ are free, for any $\mathbf{x} \in B, \mathbf{y} \in B^{\perp_L}$ we may assume that $\mathbf{x} = a\mathbf{u}, \mathbf{y} = a\mathbf{v}$, where $\mathbf{u}, \mathbf{v}$ are binary vectors. Since

$$(\mathbf{x}, \mathbf{y}) = (a\mathbf{u}, a\mathbf{v}) = a(\mathbf{u}, \mathbf{v}) = a(\mathbf{v}, \mathbf{u}) = (a\mathbf{v}, a\mathbf{u}) = (\mathbf{y}, \mathbf{x}) = 0,$$

$\mathbf{x} \in (B^{\perp_L})^{\perp_L}$. Hence $B \subseteq (B^{\perp_L})^{\perp_L}$, which implies that $B = (B^{\perp_L})^{\perp_L}$. Hence $(C^{\perp_L})^{\perp_L} = (B^{\perp_L})^{\perp_L} = B \subseteq C$. Therefore, $C = (C^{\perp_L})^{\perp_L}$ if and only if $B = C$, that is to say, C is free. □

Proposition 1. *If C is a non-free linear E-code, then it is not left-nice.*

Proof. Let us assume that C is a non-free linear E-code with generator matrix G_E. We may assume that G_E is of the form $G_E = \begin{bmatrix} aI_{k_1} & aX & aY \\ bI_{k_1} & bX & bY \\ \mathbf{0} & cI_{k_2} & cZ \end{bmatrix}$, where $k_2 \neq 0$. By the proof process of Lemma 3, we have

$$|C||C^{\perp_L}| = 4^{k_1} 2^{k_2} 4^{n-k_1} = 4^n 2^{k_2} > 4^n,$$

which implies that C is not left-nice. □

Corollary 2. *There is no non-free LCD E-code.*

Proof. By Proposition 1, any non-free linear E-code is not left-nice. Hence it is not an LCD E-code. □

We first describe a method to construct LCD codes over E from binary LCD codes.

Proposition 2. *Suppose that B is a binary LCD code with generator matrix G of size $k \times n$. Then the E-span of aG, $\langle aG \rangle_E$ is LCD.*

Proof. Let $C = \langle aG \rangle_E = \{\mathbf{x}(aG) \mid \mathbf{x} \in E^k\}$. Let H be a binary parity check matrix for B.

By Lemma 1 (2), we know

$$C^{\perp_L} = \langle aH \rangle_E . \tag{3}$$

This shows that $|C||C^{\perp_L}| = |C||\langle aH \rangle_E| = 4^k 4^{n-k} = 4^n$, which implies that C is left-nice.

Now it remains to show that

$$C \cap C^{\perp_L} = \{\mathbf{0}\}.$$

Suppose that $\mathbf{x} \in C \cap C^{\perp_L}$ and $\mathbf{x} \neq 0$.

Assume that $\mathbf{x}$ is not a multiple of a binary vector by c. Then for some nonzero α_i's and β_j's in E, we have

$$\begin{aligned} \mathbf{x} &= \sum \alpha_i a\mathbf{r}_i, \quad a\mathbf{r}_i \text{ is a row of } aG \text{ for some distinct } i \\ &= \sum \beta_t a\mathbf{r}_t, \quad a\mathbf{r}_t \text{ is a row of } aH \text{ for some distinct } t. \end{aligned}$$

Here since $c = a + b$, we may assume that α_i's are a or b and that β_t's are a or b.

Furthermore, since $aa = a$, $ab = a$, and $a\mathbf{x} \neq \mathbf{0}$, we have

$$\begin{aligned} a\mathbf{x} &= \sum a\mathbf{r}_{i_j}, \quad \mathbf{r}_{i_j} \text{ is a row of } G \text{ for some distinct } i_j \\ &= \sum a\mathbf{r}_{t_s}, \quad \mathbf{r}_{t_s} \text{ is a row of } H \text{ for some distinct } t_s. \end{aligned}$$

Therefore $\mathbf{0} = \sum a\mathbf{r}_{i_j} - \sum a\mathbf{r}_{t_s} = (\sum \mathbf{r}_{i_j} - \sum \mathbf{r}_{t_s})a$. Hence $\sum \mathbf{r}_{i_j} - \sum \mathbf{r}_{t_s} = 0$, that is, $\sum \mathbf{r}_{i_j} = \sum \mathbf{r}_{t_s}$. Then $\sum \mathbf{r}_{i_j} = 0$ since $B \cap B^{\perp} = \{\mathbf{0}\}$. This implies that the rows $\mathbf{r}_{i_j}$ of G are zero vectors. This is a contradiction since $x \neq \mathbf{0}$ is a nontrivial linear combination of $\mathbf{r}_i$'s.

We need to prove the case when $\mathbf{x}$ is a multiple of a binary vector by c. Suppose that $\mathbf{x}$ is a multiple of a binary vector $\mathbf{u}$ by c. Let $\mathbf{x} = c\mathbf{u}$. By looking at the generator matrix aG with G in standard form, we see that $\mathbf{u}$ is a linear combination of some rows of G, hence $\mathbf{u}$ is a codeword of B. In the same manner, we see that $\mathbf{u}$ is a codeword of $B^{\perp_L}$. Since $\mathbf{u} \in B \cap B^{\perp_L} = \{\mathbf{0}\}$, $\mathbf{u} = \mathbf{0}$. Hence $\mathbf{x} = c\mathbf{u} = \mathbf{0}$. This is a contradiction since $\mathbf{x} \neq \mathbf{0}$.

In both case, we have $\mathbf{x} = 0$ as desired. Therefore, we conclude that C is LCD. □

Then the converse of Proposition 2 is partially true as follows.

Proposition 3. *If C is a free LCD E-code with generator matrix G_E, then C is spanned by the rows of aG_2, where G_2 is a binary matrix of a binary LCD code B.*

Proof. By Lemma 1, C is spanned by the rows of aG_2 for some generator matrix G_2 of a binary code B. By Lemma 1, $C^{\perp_L} = \langle aH_2 \rangle_E$ for some parity check matrix H_2 of B. Since $C \cap C^{\perp_L} = \{\mathbf{0}\}$, it follows that $B \cap B^{\perp} = \{\mathbf{0}\}$ because if $\mathbf{u}$ is a nonzero vector in $B \cap B^{\perp}$ then $a\mathbf{u} \neq 0$ will be in $C \cap C^{\perp_L}$, which is a contradiction. Therefore, B is a binary LCD code. □

Corollary 3. *If C is an LCD E-code of length n, then $Res(C)$ and $Tor(C)$ are binary LCD codes.*

Proof. Since C is an LCD E-code, C is free by Corollary 2. By Proposition 3, then C is spanned by the rows of aG_2, where G_2 is a binary matrix of a binary LCD code. Obviously, $Res(C) = Tor(C)$ are binary codes with generator matrix G_2. Hence $Res(C)$ and $Tor(C)$ are binary LCD codes. □

Next, we characterize a necessary and sufficient condition for a linear E-code to be LCD. An LCD code over a finite field has a useful characterization as follows.

Lemma 4. ([9]) *Let G be a generator matrix for a code over $GF(q)$. Then $\det(GG^T) \neq 0$ if and only if G generates an LCD code.*

Proposition 4. *Let C be a linear E-code with an additive generator matrix which is of the form (2), and let $G = \begin{bmatrix} I_{k_1} & X & Y \end{bmatrix}$. Then C is an LCD E-code if and only if $k_2 = 0$ and $\det(GG^T) \neq 0$.*

Proof. If $\det(GG^T) \neq 0$. By Lemma 4, G generates a binary LCD code. By Proposition 2, C is an LCD E-code. Conversely, suppose that C is an LCD E-code. Then we know that C is free by Corollary 2, hence $k_2 = 0$. If $\det(GG^T) = 0$, let B be a binary linear code with generator matrix G. By Lemma 4, B is not a binary LCD code, it follows that $B \cap B^{\perp} \neq \{\mathbf{0}\}$, say $\mathbf{u} \in B \cap B^{\perp}$. Hence $a\mathbf{u} \in C \cap C^{\perp_L} \neq \{\mathbf{0}\}$. Thus C is not a linear LCD E-code, which is a contradiction. Therefore, $\det(GG^T) \neq 0$. □

3 ACD E-codes

An *additive E-code* of length n is an additive subgroup of E^n. It is a free $\mathbb{F}_2$-module with 2^k elements, where $0 \leq k \leq 2n$. An additive E-code C is called *left-nice* (resp. *right-nice*) if $|C||C^{\perp_L}| = 4^n$ (resp. $|C||C^{\perp_R}| = 4^n$).

Definition 5. An additive E-code C is *left-ACD* (resp. *right-ACD*) if it is left-nice (resp. right-nice) and $C \cap C^{\perp_L} = \{\mathbf{0}\}$ (resp. $C \cap C^{\perp_R} = \{\mathbf{0}\}$).

Lemma 5. *If C is an additive E-code of length n, then $C^{\perp_L}$ is a free linear E-code and $C^{\perp_R}$ is a non-free linear E-code.*

Proof. Obviously, $C^{\perp_L}$ is a left E-submodule of E^n. For any $\mathbf{x} \in C$ and $\mathbf{y} \in C^{\perp_R}$, we have $a\mathbf{y}, b\mathbf{y} \in C^{\perp_R}$ since $(\mathbf{x}, a\mathbf{y}) = (\mathbf{x}, b\mathbf{y}) = (\mathbf{x}, \mathbf{y}) = 0$. Hence $C^{\perp_R}$ is also a left E-submodule of E^n. Hence they are linear E-codes. So let us prove that $C^{\perp_L}$ is free and that $C^{\perp_R}$ is not free.

(1) Assume $C^{\perp_L}$ has an additive generator matrix

$$H_L = \begin{bmatrix} aI_{k_1} & aX & aY \\ bI_{k_1} & bX & bY \\ \mathbf{0} & cI_{k_2} & cZ \end{bmatrix}.$$

If $k_2 \neq 0$, then there is a codeword $\mathbf{x} = c\mathbf{u} \in C^{\perp_L}$, where $\mathbf{u} = (\underbrace{0, \ldots, 0}_{k_1}, \mathbf{u}')$ is a binary vector. Then for any $\mathbf{z} \in C$, $(\mathbf{x}, \mathbf{z}) = mc = 0$. So m is even. Let $\mathbf{y} = a\mathbf{u} \notin C^{\perp_L}$. Then $(\mathbf{y}, \mathbf{z}) = ma = 0$. Hence $\mathbf{y} \in C^{\perp_L}$, which is a contradiction. Therefore, $C^{\perp_L}$ is free.

(2) Assume $C^{\perp_R}$ is free. Then it has an additive generator matrix

$$H_R = \begin{bmatrix} aI_{k_1} & aX & aY \\ bI_{k_1} & bX & bY \end{bmatrix}.$$

Since c is a right zero divisor, $\langle cI_n \rangle_{\mathbb{F}_2} \subseteq C^{\perp_R}$. Since $C^{\perp_R}$ is free, we have $\langle aI_n \rangle_{\mathbb{F}_2} \subseteq C^{\perp_R}$ and $\langle bI_n \rangle_{\mathbb{F}_2} \subseteq C^{\perp_R}$. Hence $|C^{\perp_R}| \geq 2^n \times 2^n = 4^n$. Since $C^{\perp_R} \subseteq E^n$, we know $|C^{\perp_R}| \leq 4^n$. Hence $C^{\perp_R} = E^n$. From this we can get $H_R = \begin{bmatrix} aI_n \\ bI_n \end{bmatrix}$. Hence $C = \{\mathbf{0}\}$, which is a contradiction. Therefore, $C^{\perp_R}$ is not free. □

Proposition 5. *Let C be an additive E-code of length n with 2^k elements. If C is a left-ACD additive E-code, then k is even.*

Proof. By Lemma 5, $C^{\perp_L}$ is a free linear E-code. Hence $|C^{\perp_L}| = 4^{k_1} = 2^{2k_1}$. If C is a left-ACD additive E-code, $|C||C^{\perp_L}| = 4^n = 2^{2n}$. Hence $|C| = 2^k = 2^{2n-2k_1}$, we have $k = 2n - 2k_1$. Therefore, k is even. □

Remark 2. Let C be an additive E-code of length n with additive generator matrix $G = [aI_n]$. Then $C^{\perp_R}$ has an additive generator matrix $H_R = [cI_n]$. Obviously, both C and $C^{\perp_R}$ have parameters $(n, 2^n, 1)$. Since $|C||C^{\perp_R}| = 2^n \times 2^n = 4^n$ and $C \cap C^{\perp_R} = \{\mathbf{0}\}$, C is a right-ACD additive E-code. Therefore, for any integer k, we can find a right-ACD additive E-code with 2^k elements.

Next we construct left-ACD E-codes.

Lemma 6. *Let C be an additive E-code. If $|C||C^{\perp_L}| < 4^n$, $C \cap C^{\perp_L} = \{\mathbf{0}\}$, and $cC \cap C^{\perp_L} = \{\mathbf{0}\}$, then for any nonzero element $\boldsymbol{z} = \boldsymbol{x} + c\boldsymbol{y} \in C + cC$, if $\boldsymbol{z} \in C^{\perp_L}$, then $\boldsymbol{x} \neq \mathbf{0}, c\boldsymbol{y} \neq \mathbf{0}$, $\boldsymbol{x}$ is a multiple of a binary vector by c, and $\boldsymbol{x} \in C \backslash cC$.*

Proof. For any $\mathbf{z} \in C + cC$ and $\mathbf{z} \neq \mathbf{0}$, we can assume that $\mathbf{z} = \mathbf{x} + c\mathbf{y}$, where $\mathbf{x}, \mathbf{y} \in C$.

(i) When $\mathbf{x} = \mathbf{0}$ and $c\mathbf{y} \neq \mathbf{0}$, then $\mathbf{z} = c\mathbf{y} \in cC$. Since $cC \cap C^{\perp_L} = \{\mathbf{0}\}$, we have $\mathbf{z} = c\mathbf{y} \notin C^{\perp_L}$.

(ii) When $\mathbf{x} \neq \mathbf{0}$ and $c\mathbf{y} = \mathbf{0}$, then $\mathbf{z} = \mathbf{x} \in C$. Since $C \cap C^{\perp_L} = \{\mathbf{0}\}$, we have $\mathbf{z} = \mathbf{x} \notin C^{\perp_L}$.

(iii) When $\mathbf{x} \neq \mathbf{0}$ and $c\mathbf{y} \neq \mathbf{0}$, then $\mathbf{z} = \mathbf{x} + c\mathbf{y}$. Suppose that $\mathbf{x}$ is not a multiple of a binary vector by c. By Lemma 5, $C^{\perp_L}$ is a free linear E-code. If $\mathbf{z} \in C^{\perp_L}$, we have $c\mathbf{z} = c(\mathbf{x} + c\mathbf{y}) = c\mathbf{x} \in C^{\perp_L}$, which is a contradiction. If $\mathbf{x} \in C \cap cC$, $\mathbf{z} \in cC$, which is a contradiction.

By (i), (ii), and (iii), we know that if $\mathbf{z} = \mathbf{x} + c\mathbf{y} \in C^{\perp_L}$, $\mathbf{z} \neq \mathbf{0}$, then $\mathbf{x} \neq \mathbf{0}, c\mathbf{y} \neq \mathbf{0}$, $\mathbf{x}$ is a multiple of a binary vector by c, and $\mathbf{x} \in C \backslash cC$.

□

Proposition 6. *Let C be an additive E-code. If $|C||C^{\perp_L}| < 4^n$, $C \cap C^{\perp_L} = \{\mathbf{0}\}$, and $cC \cap C^{\perp_L} = \{\mathbf{0}\}$, then we can add some codewords of cC to C to make C be a left-ACD code.*

Proof. (a) We first show $cC \nsubseteq C$. Let

$$C_1 = \langle C \rangle_E = aC + cC = \{a\mathbf{x} + c\mathbf{y} \mid \mathbf{x}, \mathbf{y} \in C \backslash cC\},$$

where since c is a right zero divisor, we may assume that $\mathbf{x}, \mathbf{y}$ are not multiples of binary vectors by c. Obviously, C_1 is a free linear E-code and $C^{\perp_L} = C_1^{\perp_L}$. By Lemma 1 and Proposition 2, we have $|C_1||C_1^{\perp_L}| = 4^n$. If $cC \subset C$, we define a map $\tau_1 : C \to C_1$ by

$$\tau_1(\mathbf{x}) = a\mathbf{x}, \tau_1(c\mathbf{x}) = c\mathbf{x}, \tau_1(\mathbf{0}) = \mathbf{0}, \text{ for any } \mathbf{x} \in C \backslash cC.$$

Let $\tau_1(\mathbf{x}_1 + \mathbf{x}_2) = \tau_1(\mathbf{x}_1) + \tau_1(\mathbf{x}_2)$, for $\mathbf{x}_1, \mathbf{x}_2 \in C$. Obviously, τ_1 is a $\mathbb{F}_2$-linear mapping and it is a surjection. Hence $|C| \geq |C_1|$, which implies that

$$|C||C^{\perp_L}| \geq |C_1||C_1^{\perp_L}| = 4^n,$$

which is a contradiction. Therefore, we can add some codewords of cC to C to make C be left-nice.

(b) We show that there exists $c\mathbf{y} \in cC\backslash C$ such that for all $\mathbf{x} \in C$, $\mathbf{x}+c\mathbf{y} \notin C^{\perp_L}$. Suppose not. Then for all $c\mathbf{y} \in cC\backslash C$, there exists $\mathbf{x} \in C$ such that $\mathbf{x} + c\mathbf{y} \in C^{\perp_L}$. By Lemma 6, $\mathbf{x}$ is a multiple of a binary vector by c and $\mathbf{x} \in C\backslash cC$. For $c\mathbf{y}_1, c\mathbf{y}_2 \in cC\backslash C$ and $c\mathbf{y}_1 \neq c\mathbf{y}_2$, there exists $\mathbf{x}_1, \mathbf{x}_2 \in C$ such that $\mathbf{x}_1 + c\mathbf{y}_1, \mathbf{x}_2 + c\mathbf{y}_2 \in C^{\perp_L}$. We have $\mathbf{x}_1 \neq \mathbf{x}_2$, otherwise, $\mathbf{x}_1 = \mathbf{x}_2$, hence $(\mathbf{x}_1 + c\mathbf{y}_1) + (\mathbf{x}_2 + c\mathbf{y}_2) = c(\mathbf{y}_1 + \mathbf{y}_2) \in C^{\perp_L}$, which is a contradiction. We define a map $\tau_2 : C_1 \to C$. For any $\mathbf{y} \in C\backslash cC$, if $c\mathbf{y} \in cC\backslash C$,

$$\tau_2(a\mathbf{y}) = \mathbf{y}, \tau_2(c\mathbf{y}) = \mathbf{x}, \tau_2(\mathbf{0}) = \mathbf{0},$$

where $\mathbf{x}$ is the vector mentioned above such that $\mathbf{x} + c\mathbf{y} \in C^{\perp_L}$. If $c\mathbf{y} \in C$,

$$\tau_2(a\mathbf{y}) = \mathbf{y}, \tau_2(c\mathbf{y}) = c\mathbf{y}, \tau_2(\mathbf{0}) = \mathbf{0}.$$

Let $\tau_2(\mathbf{z}_1 + \mathbf{z}_2) = \tau_2(\mathbf{z}_1) + \tau_2(\mathbf{z}_2)$, for $\mathbf{z}_1, \mathbf{z}_2 \in C_1$. If $\mathbf{z}_1 = \mathbf{z}_2$, let $\tau_2(\mathbf{z}_1) = \tau_2(\mathbf{z}_2)$. Obviously, τ_2 is a $\mathbb{F}_2$-linear mapping and it is an injection. Hence $|C||C^{\perp_L}| \geq |C_1||C_1^{\perp_L}| = 4^n$, which is a contradiction. Therefore, there exists $c\mathbf{y} \in cC\backslash C$ such that for all $\mathbf{x} \in C$, $\mathbf{x} + c\mathbf{y} \notin C^{\perp_L}$.

At this time, we get C' by adding $c\mathbf{y}$ to C, obviously, $C' \cap C'^{\perp_L} = \{\mathbf{0}\}$. If C' is left-nice, then C' is an ACD code. Otherwise, repeat steps (a) and (b) for C'. □

The definition of the residue code and the torsion code of a linear E-code in Section 2 can be naturally extended to an additive E-code C. Obviously, $Res(C)$ and $Tor(C)$ are binary linear codes. We let $m_1 = \dim(Res(C))$ and $m_2 = \dim(Tor(C))$.

If C is a linear E-code, consider the generator matrix G for C in Equation (2) in Section 2. Then $Res(C) = k_1 = m_1$ and $Tor(C) = m_2 = m_1 + k_2$, where k_2 is the $\mathbb{F}_2$-dimension of the set of codewords of C which is a scalar multiple of $c \in E$ and which cannot be obtained from the top two blocks of the generator matrix G.

Write an arbitrary codeword in c-adic decomposition form as $a\mathbf{u} + c\mathbf{v}$, with $\mathbf{u}, \mathbf{v}$ are binary vectors, so that $\alpha(a\mathbf{u} + c\mathbf{v}) = \mathbf{u}$.

Lemma 7. *Let C be an additive E-code of length n. Then we have $C^{\perp_L} = \langle Res(C)^{\perp} \rangle_E$, and $|C^{\perp_L}| = 4^{n-\dim(Res(C))} = 4^{n-m_1}$.*

Proof. For any $\mathbf{y} \in C$, there exists $\mathbf{v} \in Res(C)$ such that $a\mathbf{y} = a\mathbf{v}$. For any $\mathbf{u} \in Res(C)^{\perp}$,

$$(a\mathbf{u}, \mathbf{y}) = (a\mathbf{u}, a\mathbf{y}) = (a\mathbf{u}, a\mathbf{v}) = a(\mathbf{u}, \mathbf{v}) = 0,$$

$$(b\mathbf{u}, \mathbf{y}) = (b\mathbf{u}, a\mathbf{y}) = (b\mathbf{u}, a\mathbf{v}) = b(\mathbf{u}, \mathbf{v}) = 0,$$

which imply $a\mathbf{u}, b\mathbf{u} \in C^{\perp_L}$. Hence $\left\langle Res(C)^{\perp} \right\rangle_E \subseteq C^{\perp_L}$. Conversely, it is easy to see that $\left\langle Res(C)^{\perp} \right\rangle_E = \langle Res(C) \rangle_E^{\perp_L}$. For any $\mathbf{u} \in Res(C)$, there exists $a\mathbf{u} + c\mathbf{v} \in C$ such that $\alpha(a\mathbf{u} + c\mathbf{v}) = \mathbf{u}$. For any $\mathbf{z} \in C^{\perp_L}$, since c is an annihilator, we have

$$(\mathbf{z}, a\mathbf{u}) = (\mathbf{z}, a\mathbf{u} + c\mathbf{v}) = 0, (\mathbf{z}, b\mathbf{u}) = (\mathbf{z}, a\mathbf{u}) = 0,$$

which implies $\mathbf{z} \in \langle Res(C) \rangle_E^{\perp_L}$. Hence $C^{\perp_L} \subseteq \langle Res(C) \rangle_E^{\perp_L}$, that is, $C^{\perp_L} \subseteq \left\langle Res(C)^{\perp} \right\rangle_E$. Therefore, $C^{\perp_L} = \left\langle Res(C)^{\perp} \right\rangle_E$. And $|C^{\perp_L}| = |\left\langle Res(C)^{\perp} \right\rangle_E| = 4^{n-\dim(Res(C))} = 4^{n-m_1}$. □

We describe a sufficient condition for an additive E-code to be left-ACD in what follows.

Proposition 7. *Let C be an additive E-code of length n. If $Res(C)$ is binary LCD, $cTor(C) \cap C^{\perp_L} = \{\mathbf{0}\}$, and $2^{m_1} \cdot 2^{m_2} \cdot 4^{n-m_1} = 4^n$ (that is, $m_1 = m_2$), then C is left-ACD.*

Proof. Since $|C| = |Res(C)||Tor(C)| = 2^{m_1} \cdot 2^{m_2}$ and $|C^{\perp_L}| = 4^{n-m_1}$, C is left-nice. Suppose that $\mathbf{x} = (x_1, x_2, \cdots, x_n) \in C \cap C^{\perp_L}$ and $\mathbf{x} \neq \mathbf{0}$, since $cTor(C) \cap C^{\perp_L} = \{\mathbf{0}\}$, $\mathbf{x}$ is not a multiple of a binary nonzero vector by c. Implying that $\alpha(\mathbf{x})$ is a binary nonzero vector. Since $\mathbf{x} \in C \cap C^{\perp_L}$, for any $\mathbf{y} = (y_1, y_2, \cdots, y_n) \in C$, we have $(\mathbf{x}, \mathbf{y}) = 0$, since α is a ring morphism,

$$\alpha(\mathbf{x}) \cdot \alpha(\mathbf{y}) = \sum_{i=1}^{n} \alpha(x_i)\alpha(y_i) = \sum_{i=1}^{n} \alpha(x_i y_i) = \alpha(\sum_{i=1}^{n} x_i y_i) = \alpha((\mathbf{x}, \mathbf{y})) = 0.$$

Hence, $\alpha(\mathbf{x}) \in Res(C) \cap Res(C)^{\perp}$, which is a contradiction. Implying that $\mathbf{x} = \mathbf{0}$. Therefore, C is left-ACD. □

In what follows, we prove that the converse of Corollary 3 is true.

Corollary 4. *Suppose that C is a free linear E-code of length n. If $Res(C)$ is a binary LCD, then C is a LCD E-code.*

Proof. Since $Res(C)$ is a binary LCD, it suffices to check the two conditions of Proposition 7. Since C is a free linear E-code, $Res(C) = Tor(C)$. Hence $k_1 = k_2$. Furthermore by Lemma 7, $cTor(C) \cap C^{\perp_L} = cTor(C) \cap \langle Res(C)^{\perp} \rangle_E = cRes(C) \cap \langle Res(C)^{\perp} \rangle_E = cRes(C) \cap cRes(C)^{\perp} = c(Res(C) \cap Res(C)^{\perp}) = \mathbf{0}$, where the last equality follows since $Res(C)$ is a binary LCD code. Hence C is left-ACD, that is, C is an LCD E-code.

□

Lemma 8. *If C be an additive E-code of length n, then $Res(C^{\perp_L}) = Res(C)^{\perp}$.*

Proof. For any $a\mathbf{x} + c\mathbf{y} \in C^{\perp_L}$, $\alpha(a\mathbf{x} + c\mathbf{y}) = \mathbf{x}$ is an arbitrary vector in $Res(C^{\perp_L})$. For any $a\mathbf{x}' + c\mathbf{y}' \in C$, $\alpha(a\mathbf{x}' + c\mathbf{y}') = \mathbf{x}'$ is an arbitrary vector in $Res(C)$. Since $(a\mathbf{x} + c\mathbf{y}, a\mathbf{x}' + c\mathbf{y}') = 0$ and α is a ring morphism,

$$\alpha((a\mathbf{x} + c\mathbf{y}, a\mathbf{x}' + c\mathbf{y}')) = \alpha(a\mathbf{x} + c\mathbf{y}) \cdot \alpha(a\mathbf{x}' + c\mathbf{y}') = \mathbf{x} \cdot \mathbf{x}' = 0,$$

which implies $\mathbf{x} \in Res(C)^{\perp}$. Hence $Res(C^{\perp_L}) \subseteq Res(C)^{\perp}$. By definition of the residue code and Lemma 5, we know $|C^{\perp_L}| = 4^{n-m_1}$ and $C^{\perp_L}$ is a free linear E-code, which implies $|Res(C^{\perp_L})| = 2^{n-m_1}$. Since $|Res(C)^{\perp}| = 2^n/|Res(C)| = 2^{n-m_1}$, $|Res(C^{\perp_L})| = |Res(C)^{\perp}|$. Therefore, $Res(C^{\perp_L}) = Res(C)^{\perp}$. □

Corollary 5. *If C is a linear E-code of length n, then $Tor(C)^{\perp} \subseteq Tor(C^{\perp_L})$.*

Proof. By [1, Lemma 1], we know $Res(C) \subseteq Tor(C)$ and $Res(C^{\perp_L}) \subseteq Tor(C^{\perp_L})$, hence $Tor(C)^{\perp} \subseteq Res(C)^{\perp}$. By Lemma 8, $Res(C^{\perp_L}) = Res(C)^{\perp}$, hence $Tor(C)^{\perp} \subseteq Res(C^{\perp_L}) \subseteq Tor(C^{\perp_L})$. This completes the proof. □

A partial converse of Proposition 7 can be true by the following proposition.

Proposition 8. *Let C be an additive E-code of length n. If C is left-ACD and $cC \cap C^{\perp_L} = \{\mathbf{0}\}$, then $Res(C)$ is a binary LCD, $cTor(C) \cap C^{\perp_L} = \{\mathbf{0}\}$, and $2^{m_1} \cdot 2^{m_2} \cdot 4^{n-m_1} = 4^n$ (that is, $m_1 = m_2$).*

Proof. Since $|C| = |Res(C)||Tor(C)| = 2^{m_1} \cdot 2^{m_2}$, $|C^{\perp_L}| = 4^{n-m_1}$ and C is left-ACD, we have $2^{m_1} \cdot 2^{m_2} \cdot 4^{n-m_1} = 4^n$, that is, $m_1 = m_2$. Also, $cTor(C) \cap C^{\perp_L} = \{\mathbf{0}\}$ is obvious.

For any $\mathbf{u} \in Res(C) \cap Res(C)^{\perp}$, $\mathbf{u} \in Res(C^{\perp_L})$, by Lemma 8, so there are $a\mathbf{u} + c\mathbf{v} \in C$ and $a\mathbf{u} + c\mathbf{v}' \in C^{\perp_L}$ such that $\alpha(a\mathbf{u} + c\mathbf{v}) = \alpha(a\mathbf{u} + c\mathbf{v}') = \mathbf{u}$. Since $C^{\perp_L}$ is linear E-codes, $c(a\mathbf{u} + c\mathbf{v}') = c\mathbf{u} \in C^{\perp_L}$. In addition, $c(a\mathbf{u} + c\mathbf{v}) = c\mathbf{u} \in cC$, so $c\mathbf{u} \in cC \cap C^{\perp_L} = \{\mathbf{0}\}$. Hence $c\mathbf{u} = \mathbf{0}$, implying that $\mathbf{u} = \mathbf{0}$. Therefore, $Res(C)$ is a binary LCD. □

In what follows, we describe Propositions 6 and 7 using examples.

Example 1. Let C be an additive E-code with an additive generator matrix

$$G = \begin{bmatrix} a & b & 0 \\ 0 & a & b \end{bmatrix}.$$

Then $C^{\perp_L}$ has an additive generator matrix

$$G_L = \begin{bmatrix} a & a & a \\ b & b & b \end{bmatrix}.$$

Hence $|C||C^{\perp_L}| = 2^2 2^2 = 4^2 < 4^3$, $C \cap C^{\perp_L} = \{\mathbf{0}\}$, and $cC \cap C^{\perp_L} = \{\mathbf{0}\}$. We add $c(a, b, 0) = (c, c, 0)$ and $c(0, a, b) = (0, c, c)$ to G, so that we get

$$G' = \begin{bmatrix} a & b & 0 \\ 0 & a & b \\ c & c & 0 \\ 0 & c & c \end{bmatrix}.$$

Let C' be an additive E-code with an additive generator matrix G'. Then by Proposition 6, C' is a left-ACD code with parameters $(3, 2^4, 2)$.

On the other hand, this example satisfies the condition of Proposition 7 so that C' is really left-ACD as follows. Note that $Res(C')$ and $Tor(C')$ have generator matrices, respectively

$$Res(G') = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}, \quad Tor(G') = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}.$$

Clearly $m_1 = 2 = m_2$. We also have that $Res(C')$ is a binary LCD codes since $Res(C')^{\perp} = \{(0, 0, 0), (1, 1, 1)\}$. By Lemma 7, $C^{\perp_L} = \langle \mathbf{1} \rangle_E$, whose additive generator matrix is the same as G_L above. Finally, $cTor(C) \cap C^{\perp_L} = \{\mathbf{0}\}$.

Example 2. Let C be an additive E-code with an additive generator matrix

$$G = \begin{bmatrix} a & 0 & a & b & 0 \\ 0 & a & 0 & a & b \\ b & 0 & b & c & a \\ 0 & c & c & c & c \end{bmatrix}.$$

Then $C^{\perp_L}$ has an additive generator matrix

$$G_L = \begin{bmatrix} a & 0 & 0 & a & a \\ b & 0 & 0 & b & b \\ 0 & 0 & a & a & a \\ 0 & 0 & b & b & b \end{bmatrix}.$$

Hence $|C||C^{\perp_L}| = 2^4 2^4 = 4^4 < 4^5$, $C \cap C^{\perp_L} = \{\mathbf{0}\}$, and $cC \cap C^{\perp_L} = \{0\}$. We add $c(a,0,a,b,0) = (c,0,c,c,0)$ and $c(b,0,b,c,a) = (c,0,c,0,c)$ to G, so that we get

$$G' = \begin{bmatrix} a & 0 & a & b & 0 \\ 0 & a & 0 & a & b \\ b & 0 & b & c & a \\ 0 & c & c & c & c \\ c & 0 & c & c & 0 \\ c & 0 & c & 0 & c \end{bmatrix}.$$

Let C' be an additive E-code with an additive generator matrix G'. Therefore, by Proposition 6, C' is a left-ACD code with parameters $(5, 2^6, 2)$.

On the other hand, this example satisfies the condition of Proposition 7 so that C' is really left-ACD as follows. Note that $Res(C')$ and $Tor(C')$ have generator matrices, respectively

$$Res(G') = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 \end{bmatrix}, \quad Tor(G') = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

Clearly $m_1 = 3 = m_2$. We also have that $Res(C')$ is a binary LCD codes since

$$Res(G')Res(G')^T = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

is invertible. By looking at G_L, we see that $C^{\perp_L}$ has only two codewords $(c,0,0,c,c)$ and $(0,0,c,c,c)$ which are multiples of a binary vector by c. Because $cTor(C)$ does not contain any of these, we have finally $cTor(C) \cap C^{\perp_L} = \{\mathbf{0}\}$.

4 Conclusion and open problems

We have introduced LCD and ACD codes over a noncommutative non-unital ring E with four elements. We have shown that free LCD codes over E are directly related to binary LCD codes. We have also characterized (left-) additive complementary dual codes over E in terms of their residue codes and their torsion codes. They form a natural generalization of LCD codes over E. As future work, it will be interesting to find a family of left-ACD codes over E with large minimum distances.

References

[1] Alahmadi, A., Altassan, A., Basaffar, W., Bonnecaze, A., Shoaib, H., Solé P.: Type IV codes over a non-unital ring. to appear in J. of Algebra and Its Applications (`https://doi.org/10.1142/S0219498822501420`) with preprint in `https://hal.archives-ouvertes.fr/hal-02433480/document`(2021)

[2] Carlet, C., Guilley, S.: Complementary dual codes for counter-measures to side-channel attacks. Coding Theory and Applications. Raquel Pinto, Paula Rocha-Malonek, Paolo Vettori eds, Springer, CIMSMS, **3**, 97–105 (2015)

[3] Dougherty, S.T., Kim, J.-L., Ozkaya. B., Sok, L., Solé, P.: The combinatorics of LCD codes : Linear Programming bound and orthogonal matrices. Int. J. of Information and Coding Theory. **4**(2/3) 116-128 (2015)

[4] Fine, B.: Classification of finite rings of order p^2. Mathematics Magazine. **66**(4), 248–252 (1993)

[5] Huffman, W.C., Pless, V.: *Fundamentals of Error-Correcting Codes*. Cambridge University Press, Cambridge (2003)

[6] Kim, J.-L., Ohk, D. E.: DNA codes over two noncommutative rings of order four. To appear in J. of Applied Mathematics and Computing, `https://doi.org/10.1007/s12190-021-01598-7`

[7] Lu L., Zhan X., Yang S., Cao H. Optimal Quaternary Hermitian LCD codes, preprint, `https://arxiv.org/abs/2010.10166` (2020)

[8] Massey J. L.: Reversible codes. Information and Control. **7**(3), 369-380 (1964)

[9] Massey, J. L.: Linear codes with complementary duals, Discrete Math. **106-107**, 337-342 (1992)

[10] Sendrier, N.: Linear codes with complementary duals meet the Gilbert-Varshamov bound. Discrete Math. **285**(1), 345–347 (2004)

[11] Shi M., Alahmadi A., Solé P., *Codes and Rings; theory and practice*, Wiley (2017).

[12] Shi M., Liu, N., Kim J-L., Solé P. , Additive complementary dual codes over $\mathbb{F}_4$, in preparation.

[13] Shi, M., Wang, S., Kim, J.-L., Solé, P.: Self-orthogonal codes over a non-unital ring and combinatorial matrices.
`https://arxiv.org/abs/2106.07124` (2021)