On Linear Complementary Pair Of nD Cyclic Codes

Cem Güneri, Buket Özkaya and Selcen Sayıcı

***Abstract*—The security parameter for a linear complementary pair (C, D) of codes is defined to be the minimum of the minimum distances $d(C)$ and $d(D^\perp)$. Recently, Carlet et al. showed that if C and D are both cyclic or both two-dimensional (2D) cyclic linear complementary pair of codes, then C and $D^\perp$ are equivalent codes. Hence, the security parameter for cyclic and 2D cyclic linear complementary pair of codes is simply $d(C)$. We extend this result to nD cyclic linear complementary pair of codes. The proof of Carlet et al. for the 2D cyclic case is based on the trace representation of the codes, which is technical and nontrivial to generalize. Our proof for the generalization is based on the zero sets of the ideals corresponding to nD cyclic codes.**

***Index Terms*—LCP of codes, nD cyclic codes, abelian codes, code equivalence.**

I. Introduction

A pair of linear codes (C, D) over $\mathbb{F}_q$ of length n is called a linear complementary pair (LCP) of codes if $C \cap D = \{0\}$ and $C + D = \mathbb{F}_q^n$. In the case $C = D^\perp$, C is referred to as a linear complementary dual (LCD) code. Note that the dual in this paper will be relative to the Euclidean inner product, although such codes are also of interest with respect to other inner products (see [4], for instance).

The interest in LCP of codes stems from cryptography, although the problems that arise in their study are interesting solely from coding theory point of view as well. In fact, LCD codes were introduced by Massey [9], long before the recent cryptographic applications. Revived interest in LCP of codes is due to their use in protection against side channel and fault injection attacks ([1], [2]). In this context, the security parameter of an LCP (C, D) is defined to be $\min\{d(C), d(D^\perp)\}$. For the LCD case, this parameter is simply $d(C)$, since $D^\perp = C$. So, the goal is to construct LCP of codes with big security parameter.

It has recently been shown by Carlet et al. ([3]) that if the supplementary codes C and D are both cyclic or both 2D cyclic, then C is equivalent to $D^\perp$. Therefore, $d(C) = d(D^\perp)$, just as in the case of LCD codes. In other words, there is an LCP of cyclic codes, which has as good a security parameter as the cyclic code with the best minimum distance (for a fixed length and dimension). The same also holds for 2D cyclic codes. It is also shown in the same paper that an LCP of quasi-cyclic codes does not have this property, i.e., there is an example of quasi-cyclic complementary pair (C, D) for which $d(C) \neq d(D^\perp)$.

If C_a denotes the cyclic group of order a, for any positive integer a, then a length n cyclic code is an ideal in $\mathbb{F}_q[C_n]$ and a length $n \times m$ (see Section II for the notation) 2D cyclic code is an ideal in $\mathbb{F}_q[C_n \times C_m]$. This naturally brings up the question whether there is a similar result for the security parameter of more general "ideal codes", which are better known with the names nD cyclic codes or abelian codes ([7], [8]). Here, we answer this question positively for abelian codes that lie in a group algebra $\mathbb{F}_q[G]$ with $\gcd(q, |G|) = 1$. The proof in [3] for cyclic codes is rather simple and is based on polynomial arithmetic, since ideals of $\mathbb{F}_q[C_n]$ are principal ideals. The proof for 2D cyclic codes in [3] is based on the Chinese Remainder Decomposition and the trace representation of 2D cyclic codes. This proof is technical and nontrivial to generalize. The proof for the abelian codes given in the current work uses the correspondence between ideals in the group algebra and their zero sets.

We recall basic results on nD cyclic codes in Section II. The main result is proved in Section III.

II. nD Cyclic Codes

We refer to [6] and [7] for details of the results presented in this Section.

Let $m_1, \ldots, m_n$ be positive integers all of which are relatively prime to q. Denote the cyclic group of order m_i by C_{m_i} and consider the abelian group

$$G = C_{m_1} \times \cdots \times C_{m_n}.$$

Then there is a natural isomorphism between the group algebra $\mathbb{F}_q[G]$ and the quotient ring

$$R_n = \mathbb{F}_q[x_1, \ldots, x_n]/\langle x_1^{m_1} - 1, \ldots, x_n^{m_n} - 1\rangle.$$

An ideal in $\mathbb{F}_q[G]$ or in R_n is called an abelian code or an nD cyclic code ([7], [8]). When $n = 1$, these are simply cyclic codes.

Let us denote an $m_1 \times \cdots \times m_n$ array over $\mathbb{F}_q$ by $(a_{i_1,i_2,\ldots,i_n})$. Here, we understand that the index i_j runs over the set $\{0, 1, \ldots, m_j - 1\}$ for all $1 \leq j \leq n$. In other words, such an array is simply a vector over $\mathbb{F}_q$ of length $m_1 \cdots m_n$. One can identify the $\mathbb{F}_q$-space $\mathbb{F}_q^{m_1 \times \cdots \times m_n}$ of all $m_1 \times \cdots \times m_n$ arrays with R_n via the map

$$\begin{aligned} \mathbb{F}_q^{m_1 \times \cdots \times m_n} &\longrightarrow R_n \\ (a_{i_1,\ldots,i_n}) &\longmapsto \sum_{j=1}^{n} \sum_{i_j=0}^{m_j-1} a_{i_1,\ldots,i_n} {x_1}^{i_1} \cdots {x_n}^{i_n}. \end{aligned} \quad \text{(II.1)}$$

C. Güneri and S. Sayıcı are with Sabancı University, Faculty of Engineering and Natural Sciences, 34956, İstanbul, Turkey (e-mail: guneri@sabanciuniv.edu, selcensayici@sabanciuniv.edu).

B. Özkaya is with Nanyang Technological University, School of Physical and Mathematical Sciences, Division of Mathematical Sciences, 21 Nanyang Link, Singapore 637371 (e-mail: buketozkaya@ntu.edu.sg).

Manuscript received ; revised .

Note that, for simplicity, we denote the element of R_n not as a coset but just as a polynomial representing a coset in R_n. Under this identification, an nD cyclic code C becomes an $\mathbb{F}_q$-linear code of size (length) $m_1 \times \cdots \times m_n$ which satisfies the condition

$$(a_{i_1,i_2,\ldots,i_n}) \in C \implies (a_{i_1+s_1,i_2+s_2,\ldots,i_n+s_n}) \in C,$$

for all $s_1, \ldots, s_n$, where $i_j + s_j$ is computed modulo m_j for each j. Note that, for $n = 1$, this is equivalent to the usual vectorial representation of cyclic codes and the code's invariance under cyclic shift. Let us also note that the dual $C^\perp$ of an nD cyclic code of size $m_1 \times \cdots \times m_n$ is also an nD cyclic code of the same size.

Let α_j be a primitive m_j^{th} root of unity for $1 \le j \le n$. Note that all α_j's lie in a field $\mathbb{F}_{q^s}$ with the property that every m_j divides $q^s - 1$. Define the set

$$\Omega = \left\{(\alpha_1{}^{i_1}, ..., \alpha_n{}^{i_n}) : \ 0 \le i_j \le m_j - 1, \ 1 \le j \le n\right\}.$$

The $\mathbb{F}_q$-conjugacy class containing $(\alpha_1{}^{i_1}, \ldots, \alpha_n{}^{i_n})$ in Ω is defined as

$$\left[(\alpha_1{}^{i_1}, ..., \alpha_n{}^{i_n})\right] = \left\{(\alpha_1{}^{i_1 q^t}, \ldots, \alpha_n{}^{i_n q^t}) : 0 \le t \le \delta - 1\right\},$$

where

$$\delta = \operatorname{lcm}\left\{\left[\mathbb{F}_q(\alpha_j{}^{i_j}) : \mathbb{F}_q\right], 1 \le j \le n\right\}.$$

Ω is a disjoint union of such $\mathbb{F}_q$-conjugacy classes.

Note that an ideal C of R_n (nD cyclic code) is of the form $\mathcal{C} + \langle x_1^{m_1} - 1, \ldots, x_n^{m_n} - 1\rangle$ for an ideal $\mathcal{C}$ of the polynomial ring $\mathbb{F}_q[x_1, \ldots, x_n]$. Therefore, $\mathcal{C} \supset \langle x_1^{m_1} - 1, \ldots, x_n^{m_n} - 1\rangle$. We define the zero set $Z(C)$ of an nD cyclic code C as the common zeros of all of the polynomials in $\mathcal{C}$ and observe that $Z(C) \subset \Omega$. In fact, $Z(C)$ is a union of $\mathbb{F}_q$-conjugacy classes.

Conversely, for a subset $U \subset \Omega$, the nD cyclic code C_U in R_n corresponding to U is defined to be $\mathcal{C}_U + \langle x_1^{m_1} - 1, \ldots, x_n^{m_n} - 1\rangle$, where

$$\mathcal{C}_U = \{f(x_1, x_2, \ldots, x_n) \in \mathbb{F}_q[x_1, x_2, \ldots, x_n] : f(a_1, \ldots, a_n) = 0, \text{ for all } (a_1, \ldots, a_n) \in U\}.$$

If $\bar{U}$ denotes the smallest union of $\mathbb{F}_q$-conjugacy classes in Ω that contains U, then it can be seen that $C_U = C_{\bar{U}}$. Moreover, there is a one-to-one correspondence between subsets of Ω which are unions of $\mathbb{F}_q$-conjugacy classes and nD cyclic codes in R_n, given via the assignment $U \leftrightarrow C_U$. In other words, we have $Z(C_U) = U$ for any $U \subset \Omega$, which is a union of $\mathbb{F}_q$-conjugacy classes, and $C_{Z(C)} = C$ for any ideal (nD cyclic code) C of R_n.

The following important facts will be used throughout, so we collect them in the next result. Let us note that these results are stated for 2D cyclic codes in [6, Theorem 3.4, Proposition 3.5] and for general nD cyclic codes in [7, Proposition 2.2].

Proposition II.1. *Let $U = Z(C)$ be the zero set of the nD cyclic code $C \subset R_n$. Then,*

i. $\dim_{\mathbb{F}_q}(C) = |\Omega - U|$,

ii. $Z(C^\perp) = \Omega - U^{-1}$,

where $U^{-1} = \left\{(a_1^{-1}, \ldots, a_n^{-1}) : (a_1, \ldots, a_n) \in U\right\}$.

Example II.2. The class of nD cyclic codes contains some good codes. We give an example of a good 2D cyclic code here. Consider the extension $\mathbb{F}_9$ over $\mathbb{F}_3$ and let α be a primitive element of $\mathbb{F}_9$ satisfying $\alpha^2 + \alpha - 1 = 0$. Let C be the 2D cyclic code over $\mathbb{F}_3$ of size 8×8 (i.e., length 64) whose dual $C^\perp$ has the zero set

$$Z(C^\perp) = [(\alpha, \alpha)] \cup [(\alpha, \alpha^2)].$$

In other words, C and $C^\perp$ are ideals of $\mathbb{F}_3[x_1, x_2]/\langle x_1^8 - 1, x_2^8 - 1\rangle$. It is easy to observe that the $\mathbb{F}_3$-conjugacy classes of (α, α) and (α, α^2) both have two elements. Hence, by Proposition II.1, $\dim_{\mathbb{F}_3}(C^\perp) = 64 - 4 = 60$ and $\dim_{\mathbb{F}_3}(C) = 4$. It is shown in [6, Example 6.2] that the minimum distance of C is 42. This is the best minimum distance for a code of length 64 and dimension 4 over $\mathbb{F}_3$ according to [5].

III. LCP of nD Cyclic Codes

Recently, Carlet et al. showed that if (C, D) is an LCP of codes where both C and D are cyclic or 2D cyclic, then C and $D^\perp$ are equivalent ([3, Theorems 2.4 and 3.4]). We extend this result to nD cyclic codes (for any n) in this section. As in Section II, we let $R_n = \mathbb{F}_q[x_1, \ldots, x_n]/\langle x_1^{m_1} - 1, \ldots, x_n^{m_n} - 1\rangle$ and assume that $\gcd(q, m_i) = 1$ for all $1 \le i \le n$.

We start by recalling a basic ring theoretic fact. For the sake of completeness, a short proof is provided below. Note that the sum and product of ideals I and J in a ring R are defined as

$$I + J := \{u + v : \ u \in I, v \in J\},$$

$$IJ := \left\{\sum_{i=1}^{n} u_i v_i : \ n \in \mathbb{N}, u_i \in I, v_i \in J \text{ for } 1 \le i \le n\right\}.$$

Proposition III.1. *If I and J are ideals in a commutative ring R with identity such that $I + J = R$, then $I \cap J = IJ$.*

Proof: In general $IJ \subset I \cap J$, so we just need to show the opposite implication. Let a be an element of the intersection and write $1 = u + v$ for some $u \in I$ and $v \in J$. Then, $a = a(u + v) = au + av$. Since R is commutative, both au and av are elements of the ideal IJ. Hence, $a \in IJ$. ∎

The next result collects important information on the zero sets of complementary nD cyclic codes and it will be essential in the proof of the main result.

Proposition III.2. *Let (C, D) be an nD cyclic LCP of codes in R_n. Then,*

i. $Z(C) \cup Z(D) = Z(C \cap D) = \Omega$.

ii. $Z(C) \cap Z(D) = \emptyset$.

Proof: Since (C, D) is LCP, we have $C \cap D = CD$ in R_n by Proposition III.1. So it suffices to show that $Z(C) \cup Z(D) = Z(CD)$.

i. Let a be in $\in Z(C) \cup Z(D)$ and assume without loss of generality that $a \in Z(C)$. So $f(a) = 0$ for all $f \in C$, and hence $f(a)g(a) = 0$ for any $g \in D$. Therefore, a is also a root of summation of such products, which implies that $a \in Z(CD)$.

Conversely, let a be an element of $Z(CD)$. If a does not belong to $Z(C) \cup Z(D)$, then there exist $f \in C$ and $g \in D$ such that $f(a) \neq 0$ and $g(a) \neq 0$. So, $h(a) \neq 0$ for $h = fg \in CD$, which is a contradiction.

Hence, we proved that $Z(C) \cup Z(D) = Z(CD) = Z(C \cap D)$. Since $C \cap D = \{0\}$, the corresponding zero set is Ω.

ii. Note that $|\Omega| = m_1 \cdots m_n = \dim_{\mathbb{F}_q}(R_n)$. Since $C \oplus D = R_n$, we obtain

$$|\Omega| = \dim_{\mathbb{F}_q}(C) + \dim_{\mathbb{F}_q}(D).$$

Then by Proposition II.1, we have

$$|\Omega| = (|\Omega| - |Z(C)|) + (|\Omega| - |Z(D)|),$$

and hence

$$|\Omega| = |Z(C)| + |Z(D)|. \tag{III.1}$$

By part i, we also have

$$|\Omega| = |Z(C) \cup Z(D)| = |Z(C)| + |Z(D)| - |Z(C) \cap Z(D)|. \tag{III.2}$$

Equations III.1 and III.2 imply that $|Z(C) \cap Z(D)| = 0$, which proves the result. ∎

Remark III.3. Proposition III.2 implies that Ω is a disjoint union of $Z(C)$ and $Z(D)$. Carlet et al. showed in [3, Theorem 2.1] that if C and D are complementary cyclic codes with the generating polynomials $g(x)$ and $u(x)$ (in $R_1 = \mathbb{F}_q[x]/\langle x^{m_1} - 1\rangle$), then $u(x) = (x^{m_1} - 1)/g(x)$ (this is their statement in the case $\gcd(q, m_1) = 1$). Hence, the zero sets (or the defining sets in the terminology of cyclic codes) of C and D partition $\{0, 1, \ldots, m_1 - 1\}$. Therefore, Proposition II.1 extends their result to nD cyclic codes for all n.

The next observation is on the relation between $Z(C)$ and $Z(D^\perp)$ for an LCP (C, D) of nD cyclic codes.

Proposition III.4. *If (C, D) is an LCP of nD cyclic codes in R_n, then $Z(D^\perp) = Z(C)^{-1}$.*

Proof: Since Ω is a disjoint union of $Z(C)$ and $Z(D)$ (cf. Remark III.3), and $\Omega^{-1} = \Omega$, the same is true for $Z(C)^{-1}$ and $Z(D)^{-1}$. We have $Z(D^\perp) = \Omega - Z(D)^{-1}$ by Proposition II.1. By the preceding observation, this set is simply $Z(C)^{-1}$. ∎

Remark III.5. Note that Proposition III.4 also extends the analogous result for LCP of cyclic codes to LCP of nD cyclic codes.

We are ready to prove the main result.

Theorem III.6. *Let (C, D) be an nD cyclic LCP of codes in R_n. Then C and $D^\perp$ are equivalent.*

Proof: Consider the following map:

$$\begin{aligned} \psi : C &\longrightarrow D^\perp \\ f(x_1, \ldots, x_n) &\longmapsto x_1^{m_1 - 1} \cdots x_n^{m_n - 1} f(x_1^{-1}, \ldots, x_n^{-1}). \end{aligned}$$

Note that $\psi(f)$ is a polynomial for any f whose degree in x_j is less than m_j (for all $j = 1, \ldots, n$). For $f \in C$, we have $f(a_1, \ldots, a_n) = 0$, for all $(a_1, \ldots, a_n) \in Z(C)$. Therefore, $\psi(f)(a_1^{-1}, \ldots, a_n^{-1}) = 0$ for any such n-tuple, meaning that $\psi(f)$ vanishes on $Z(C)^{-1} = Z(D^\perp)$ (cf. Proposition III.4). Hence, ψ indeed takes values in $D^\perp$.

The map is clearly one-to-one. Since the dimensions of C and $D^\perp$ are equal (by Propositions II.1 and III.4), ψ is a bijection between C and $D^\perp$.

More explicitly, if

$$f(x_1, \ldots, x_n) = \sum_{j=1}^{n} \sum_{i_j=0}^{m_j - 1} a_{i_1, \ldots, i_n} x_1^{i_1} \ldots x_n^{i_n},$$

then

$$\begin{aligned} \psi(f) &= \sum_{j=1}^{n} \sum_{i_j=0}^{m_j - 1} a_{i_1, \ldots, i_n} x_1^{m_1 - 1 - i_1} \ldots x_n^{m_n - 1 - i_n} \\ &= \sum_{j=1}^{n} \sum_{i_j=0}^{m_j - 1} a_{m_1 - 1 - i_1, \ldots, m_n - 1 - i_n} x_1^{i_1} \ldots x_n^{i_n}. \end{aligned}$$

Under the correspondence (II.1) between $\mathbb{F}_q^{m_1 \times \cdots \times m_n}$ and R_n, the map ψ sends the array (codeword) $(a_{i_1, \ldots, i_n})$ to $(a_{m_1 - 1 - i_1, \ldots, m_n - 1 - i_n})$. In other words, if we set $A_j := \{0, 1, \ldots, m_j - 1\}$ and a permutation

$$\begin{aligned} \sigma_j : A_j &\longrightarrow A_j \\ i_j &\longmapsto m_j - 1 - i_j \end{aligned}$$

for each $j = 1, \ldots, n$, then

$$\begin{aligned} \sigma : A_1 \times \cdots \times A_n &\longrightarrow A_1 \times \cdots \times A_n \\ (i_1, \ldots, i_n) &\longmapsto (\sigma_1(i_1), \ldots, \sigma_n(i_n)) \end{aligned}$$

yields the explicit equivalence between the codewords (as arrays or vectors) of C and $D^\perp$ via $(a_{\sigma(i_1, \ldots, i_n)}) = (a_{\sigma_1(i_1), \ldots, \sigma_n(i_n)})$. ∎

Remark III.7. The proof of the analogous result in [3, Theorem 2.4] for cyclic codes is based on polynomial representation, where the equivalence is shown by using the fact that the ideals in $R_1 \cong \mathbb{F}_q[C_n]$ are principal ideals, and any LCP pair of such ideals (i.e., cyclic codes) are generated by polynomials that are reciprocal to each other. Observe that the bijection ψ in the proof above maps a polynomial f to its reciprocal for $n = 1$ and the permutation σ represents the corresponding reversion of coefficients.

ACKNOWLEDGMENT

C. Güneri is supported by the TÜBİTAK Project under Grant 215E200, which is associated with the SECODE Project in the scope of the CHIST-ERA Program. B. Özkaya is supported by NTU Research Grant M4080456.

REFERENCES

[1] S. Bhasin, J.-L. Danger, S. Guilley, Z. Najm and X. T. Ngo, "Linear complementary dual code improvement to strengthen encoded circuit against hardware Trojan horses", *IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, May 5-7, 2015.

[2] J. Bringer, C. Carlet, H. Chabanne, S. Guilley, and H. Maghrebi, "Orthogonal direct sum masking - a smartcard friendly computation paradigm in a code, with builtin protection against side-channel and fault attacks", in WISTP, Springer, Heraklion, 40-56, 2014.

[3] C. Carlet, C. Güneri, F. Özbudak, B. Özkaya and P. Solé, "On linear complementary pairs of codes", *IEEE Trans. Inform. Theory*, to appear.

[4] C. Carlet, S. Mesnager, C. Tang and Y. Qi "Euclidean and Hermitian LCD MDS codes", *Des. Codes Cryptogr.*, to appear.

[5] M. Grassl, "Bounds on the minimum distance of linear codes and quantum codes", online available at http://www.codetables.de. Accessed on 2018-08-30.

[6] C. Güneri, "Artin-Schreier curves and weights of two-dimensional cyclic codes", *Finite Fields Appl.*, vol. 10, 481-505, 2004.

[7] C. Güneri and F. Özbudak, "Multidimensional cyclic codes and Artin-Schreier type hypersurfaces over finite fields", *Finite Fields Appl.*, vol. 14, 44-58, 2008.
[8] J. Jensen, "The concatenated structure of cyclic and Abelian codes", *IEEE Trans. Inform. Theory*, vol. 31, 788-793, 1985.
[9] J.L. Massey, "Linear codes with complementary duals", *Discrete Math.*, vol. 106/107, 337-342, 1992.