ON LINEAR COMPLEMENTARY PAIRS OF CODES

Claude Carlet[1], Cem Güneri[2], Ferruh Özbudak[3], Buket Özkaya[2], Patrick Solé[4]

[1] Department of Mathematics, University of Paris VIII and University of Paris XIII, LAGA, UMR 7539, CNRS, France

[2] Sabancı University, Faculty of Engineering and Natural Sciences, 34956 İstanbul, Turkey

[3] Department of Mathematics and Institute of Applied Mathematics, Middle East Technical University, Ankara, Turkey

[4] CNRS/LAGA, University of Paris 8, 93 526 Saint-Denis, France

Abstract. We study linear complementary pairs (LCP) of codes (C, D), where both codes belong to the same algebraic code family. We especially investigate constacyclic and quasi-cyclic LCP of codes. We obtain characterizations for LCP of constacyclic codes and LCP of quasi-cyclic codes. Our result for the constacyclic complementary pairs extends the characterization of linear complementary dual (LCD) cyclic codes given by Yang and Massey. We observe that when C and D are complementary and constacyclic, the codes C and $D^\perp$ are equivalent to each other. Hence, the security parameter $\min(d(C), d(D^\perp))$ for LCP of codes is simply determined by one of the codes in this case. The same holds for a special class of quasi-cyclic codes, namely 2D cyclic codes, but not in general for all quasi-cyclic codes, since we have examples of LCP of double circulant codes not satisfying this conclusion for the security parameter. We present examples of binary LCP of quasi-cyclic codes and obtain several codes with better parameters than known binary LCD codes. Finally, a linear programming bound is obtained for binary LCP of codes and a table of values from this bound is presented in the case $d(C) = d(D^\perp)$. This extends the linear programming bound for LCD codes.

Keywords: Constacyclic code, quasi-cyclic code, LCP of codes, linear programming bound.

1. Introduction

This paper is devoted to the study of the parameters of pairs of supplementary linear codes, whose motivation comes from cryptography, and which have their own interest in coding. Until the end of the 90's, the security models for block ciphers (in symmetric cryptography) assumed that the attacker had access only to a so-called black box. According to the model considered, they could see ciphertexts or pairs (plaintext, ciphertext), possibly of particular forms, corresponding to a same algorithm and to a same secret key. But they were supposed to have no access to the data implemented inside the algorithm. Since then, it has been shown that the implementations of block ciphers are prone to side-channel attacks (SCA) and to fault injection attacks (FIA), which, when no countermeasure is implemented in the algorithm, are able to extract the secret key from the access to the noisy data which can be read when the algorithm is running over some device, or from the perturbation of this implementation.

These attacks which can be non-invasive (i.e. do not damage the system) are a special concern since they leave no evidence that they have been perpetrated. The most generic and efficient known protection against SCA is achieved with masking: every sensitive data (that is, every data processed by the algorithm from which a part of the secret key can be deduced) is bitwise added with a uniformly distributed random vector of the same length or several ones, called globally a mask. If the sensitive data and the mask belong respectively to two supplementary subspaces C and D of a larger vector space, it is possible to deduce the sensitive data from the resulting masked data. And it is shown that the level of resistance against both SCA and FIA depends on $\min(d(C), d(D^{\perp}))$, where $d(C)$ is the minimum distance of the code C and $d(D^{\perp})$ is the dual distance of the code D. This method is called *Direct Sum Masking* (DSM), and the pair (C, D) is called a complementary pair of codes. The masks are the codewords of the code D and the sensitive data are codewords of the code C. By the rank-nullity theorem, if the dimension of C is k and the ambient space is of dimension n, then the dimension of D is $n-k$. If C and D are subspaces in $\mathbb{F}_q^n$, and their generator matrices are G and G', respectively, then every vector $z \in \mathbb{F}_q^n$ can be written in a unique way as $z = xG + yG'$, for $x \in \mathbb{F}_q^k, y \in \mathbb{F}_q^{n-k}$. We refer to [1] for further information on complementary pairs of codes and their uses.

To summarize the coding theoretic setting, we are interested in two linear codes C and D of length n over $\mathbb{F}_q$, which are supplementary (i.e. have trivial intersection and direct sum equal to the whole space $\mathbb{F}_q^n$). We call such (C, D) a linear complementary pair (LCP) of codes. Note that the linear complementary dual (LCD) codes amount to the special case when $D = C^{\perp}$, in which case the "security parameter" is simply the minimum distance of C. There has been quite an activity in recent years on the algebraic study of LCD codes but LCP of codes are not as well-studied yet.

The aim of this work is to study LCP of codes (C, D), where both codes belong to the same family of algebraic codes. Namely, we will be interested in LCP of codes (C, D), where C, D are both constacyclic codes or both quasi-cyclic codes. These code families are fundamental objects in coding theory. We present characterizations of constacyclic and quasi-cyclic LCP of codes. The characterization result in the constacyclic case extends the characterization of LCD cyclic codes due to Yang and Massey ([10]). In the case of constacyclic LCP of codes (C, D), we prove that the codes C and $D^{\perp}$ are equivalent. Hence, the security parameter is simply the minimum distance of C in this case. In particular, finding the best constacyclic code and finding the best constacyclic LCP of codes are equivalent problems. We show that the same result does not hold in the case of quasi-cyclic codes (i.e. C and $D^{\perp}$ need not be equivalent). However, equivalence of C and $D^{\perp}$ is valid for some particular quasi-cyclic codes, namely 2D cyclic codes. We also prove a linear programming bound for binary LCP of codes, extending the analogous result for LCD codes in [3].

Constacyclic LCP of codes are studied in Section 2, which is then followed by the study of quasi-cyclic LCP of codes in Section 3. Examples of LCP of codes from quasi-cyclic codes are presented in Section 4 and LCP of codes with better security parameters than comparable LCD codes, as well as optimal LCP of codes in the category of linear codes, are found. Section 5 presents the linear programming bound for binary LCP of codes.

2. Constacyclic LCP of Codes

Let $\lambda \in \mathbb{F}_q$ be a nonzero element. A linear code C over $\mathbb{F}_q$ of length n is said to be λ-constacyclic if the following holds:

$$(c_0, c_1, \ldots, c_{n-1}) \in C \implies (\lambda c_{n-1}, c_0, \ldots, c_{n-2}) \in C.$$

Note that $\lambda = 1$ amounts to cyclic codes and $\lambda = -1$ amounts to negacyclic codes.

We recall some basic information on constacyclic codes and refer to [8, 9] for further reading. A λ-constacyclic code of length n can be viewed, in the usual manner, as an ideal of $\mathbb{F}_q[x]/\langle x^n - \lambda \rangle$. Observe that a λ-constacyclic code is an ideal of $\mathbb{F}_q[x]/\langle x^n - \lambda \rangle$, hence has a unique monic generating polynomial $g(x)$, which divides $x^n - \lambda$. Clearly, the dimension of C is $n - \deg g$. The dual of a λ-constacyclic code is λ^{-1}-constacyclic. Moreover, if $C = \langle g(x) \rangle$ is λ-constacyclic with $\deg g = k$, then for $h(x) = (x^n - \lambda)/g(x)$, the dual constacyclic code $C^\perp$ has the generating polynomial

$$h^*(x) = h(0)^{-1} x^{n-k} h(x^{-1}) \quad \text{(see [9, Lemma 2.1]) or [8, Fact 3]).}$$

The polynomial $h^*(x)$ is called the reciprocal polynomial of $h(x)$. Let us note these facts are valid for both separable ($\gcd(q, n) = 1$) and repeated root ($\gcd(q, n) \neq 1$) constacyclic codes.

Throughout the text, we denote the sum of two vector subspaces C and D (linear codes) in an ambient space by $C + D$, which is the collection of all possible sums of vectors in C and D. Note that the sum of subspaces is also equal to the subspace generated by their union. When the subspaces intersect trivially, the sum is said to be direct and it is denoted by $C \oplus D$.

Theorem 2.1. *Let C and D be q-ary λ-constacyclic codes of length n with the generating polynomials $g(x)$ and $u(x)$, respectively. Then (C, D) is LCP if and only if $u(x) = (x^n - \lambda)/g(x)$ and* $\gcd(u(x), g(x)) = 1$.

Proof. The intersection of C and D has the generating polynomial $\operatorname{lcm}(g(x), u(x))$. For trivial intersection, the least common multiple must be $x^n - \lambda$. If $C + D = \mathbb{F}_q^n = \mathbb{F}_q[x]/\langle x^n - \lambda \rangle$, then $1 \equiv a(x)g(x) + b(x)u(x) \mod (x^n - \lambda)$ for some $a(x), b(x) \in \mathbb{F}_q[x]$. A common divisor for g and u would contradict this congruence, hence $\gcd(g(x), u(x)) = 1$. These two observations combined implies in particular that $u(x) = (x^n - \lambda)/g(x)$. For the converse, g and u being relatively prime implies that $C + D = \mathbb{F}_q[x]/\langle x^n - \lambda \rangle$. This, combined with the assumption $u(x) = (x^n - \lambda)/g(x)$ implies that $\operatorname{lcm}(g(x), u(x)) = x^n - \lambda$, which yields $C \cap D = \{0\}$. □

Remark 2.2. In the case $\gcd(q, n) = 1$, the polynomial $x^n - \lambda$ is separable and hence $\gcd((x^n - \lambda)/g(x), g(x)) = 1$ holds. Therefore the condition for (C, D) as above to be LCP reduces simply to $u(x) = (x^n - \lambda)/g(x)$.

Remark 2.3. Theorem 2.1 generalizes the result of Yang and Massey on the characterization of LCD cyclic codes ([10]). Note that $\lambda = 1$ in this case. A cyclic code C being LCD means $(C, C^\perp)$ is LCP. If C has the generating polynomial $g(x)$, then the generating polynomial of $C^\perp$ is $h^*(x)$ for $h(x) = (x^n - 1)/g(x)$. Theorem 2.1 yields $\left(\frac{x^n-1}{g(x)}\right)^* = \frac{x^n-1}{g(x)}$, which is equivalent to g being self-reciprocal (as stated in [10]). Moreover, relative primeness of $(x^n - 1)/g(x)$ and $g(x)$ amounts to irreducible factors of $g(x)$ having the same multiplicity in $g(x)$ and in $(x^n - 1)/g(x)$ (again, as stated in [10]).

The observations made so far allow us to make the following important conclusion.

Theorem 2.4. *If (C, D) is a q-ary λ-constacyclic LCP of codes, then C and $D^\perp$ are equivalent.*

Proof. By Theorem 2.1, if $g(x) = g_0 + g_1 x + \cdots + x^k$ is the generating polynomial of C, then the dual $D^\perp$ of the complementary λ-constacyclic code is generated by

$$g^*(x) = g_0^{-1} x^k g(x^{-1}).$$

Generating matrices of C and $D^\perp$ are as follows:

$$G_C = \begin{pmatrix} g_0 & g_1 & \dots & 1 & 0 & \dots & \\ 0 & g_0 & g_1 & \dots & 1 & 0 & \dots \\ \vdots & & \vdots & & & \vdots & \\ 0 & \dots & 0 & g_0 & g_1 & \dots & 1 \end{pmatrix}$$

$$G_{D^\perp} = g_0^{-1} \begin{pmatrix} 1 & g_{k-1} & \dots & g_1 & g_0 & 0 & \dots & & \\ 0 & 1 & g_{k-1} & \dots & g_1 & g_0 & 0 & \dots & \\ \vdots & & \vdots & & & & \vdots & & \\ 0 & \dots & 0 & & 1 & g_{k-1} & \dots & g_1 & g_0 \end{pmatrix}$$

Codes generated by these matrices are equivalent (up to a nonzero scalar multiplication in each coordinate) under the coordinate permutation that sends the ith coordinate to the $(n - 1 - i)$th coordinate (for $0 \leq i \leq n - 1$). □

Hence, finding the "best" λ-constacyclic LCP of codes (C, D) and finding the best λ-constacyclic code are equivalent problems.

3. Quasi-Cyclic LCP of Codes

A linear code over $\mathbb{F}_q$ is called a quasi-cyclic (QC) code of index ℓ if it is closed under shifting codewords by ℓ units, and ℓ is the smallest positive integer with this property. So, cyclic codes amount to the special case $\ell = 1$. It is well-known that the index of a QC code divides its length. So, we let C be a QC code of length $m\ell$, index ℓ over $\mathbb{F}_q$. We assume throughout that m and q are relatively prime. If we let $R := \mathbb{F}_q[x]/\langle x^m - 1\rangle$, then the code C can be viewed as an R-module in R^ℓ ([6, Lemma 3.1]). We will recall the Chinese Remainder Theorem (CRT) decomposition of QC codes, following [6].

Assume the following factorization into irreducible polynomials in $\mathbb{F}_q[x]$

$$x^m - 1 = g_1 \cdots g_s h_1 h_1^* \cdots h_t h_t^*, \tag{3.1}$$

where g_i's are self-reciprocal and h_j^* denotes the reciprocal of h_j. Let ξ be a primitive m^{th} root of unity over $\mathbb{F}_q$. Assume that $g_i(\xi^{u_i}) = 0$ and $h_j(\xi^{v_j}) = 0$ (for all i, j). Then we also have $h_j^*(\xi^{-v_j}) = 0$. By CRT, R decomposes into direct sum of fields as

$$\left(\bigoplus_{i=1}^{s}\mathbb{F}_q[x]/\langle g_i\rangle\right)\oplus\left(\bigoplus_{j=1}^{t}\Big(\mathbb{F}_q[x]/\langle h_j\rangle\oplus\mathbb{F}_q[x]/\langle h_j^*\rangle\Big)\right) \;=\; \left(\bigoplus_{i=1}^{s}\mathbb{F}_q(\xi^{u_i})\right)\oplus\left(\bigoplus_{j=1}^{t}\Big(\mathbb{F}_q(\xi^{v_j})\oplus\mathbb{F}_q(\xi^{-v_j})\Big)\right).$$

Let $G_i = \mathbb{F}_q[x]/\langle g_i\rangle$, $H'_j = \mathbb{F}_q[x]/\langle h_j\rangle$ and $H''_j = \mathbb{F}_q[x]/\langle h_j^*\rangle$ for simplicity. The CRT isomorphism is given by

$$a(x)\mapsto\left(\bigoplus_{i=1}^{s}a(\xi^{u_i})\right)\oplus\left(\bigoplus_{j=1}^{t}\Big(a(\xi^{v_j})\oplus a(\xi^{-v_j})\Big)\right). \tag{3.2}$$

Let us denote the CRT isomorphism (3.2) and its natural extension to R^ℓ by ϕ. So, $C \subset R^\ell$ decomposes as

$$C=\left(\bigoplus_{i=1}^{s}C_i\right)\oplus\left(\bigoplus_{j=1}^{t}\Big(C'_j\oplus C''_j\Big)\right), \tag{3.3}$$

where each component code is a length ℓ linear code over the base field (G_i, H'_j or H''_j) it is defined over ([6, Section IV]). Component codes C_i, C'_j, C''_j are called the constituents of C.

It was shown in [7] that for a QC code C with the above CRT decomposition, the (Euclidean) dual in $\mathbb{F}_q^{m\ell}$ is of the form

$$C^\perp=\left(\bigoplus_{i=1}^{s}C_i^{\perp_h}\right)\oplus\left(\bigoplus_{j=1}^{t}\Big(C_j''^{\perp_e}\oplus C_j'^{\perp_e}\Big)\right). \tag{3.4}$$

Here, $\perp_h$ denotes the Hermitian dual on $G_i^\ell = \mathbb{F}_q(\xi^{u_i})^\ell$, which is an extension field of $\mathbb{F}_q$ of even degree (for all $1 \le i \le s$).

We have the following characterization of QC LCP of codes via their constituents.

Theorem 3.1. *Let C and D be q-ary QC codes of length $m\ell$ and index ℓ. Suppose that the CRT decomposition of C and D are as follows:*

$$\begin{aligned} C &= (\textstyle\bigoplus_{i=1}^{s}C_i)\oplus\left(\bigoplus_{j=1}^{t}\Big(C'_j\oplus C''_j\Big)\right),\\ D &= (\textstyle\bigoplus_{i=1}^{s}D_i)\oplus\left(\bigoplus_{j=1}^{t}\Big(D'_j\oplus D''_j\Big)\right). \end{aligned}$$

Then (C, D) is LCP if and only if (C_i, D_i) is LCP in G_i^ℓ (for all $1 \le i \le s$), (C'_j, D'_j) is LCP in $H_j'^\ell$ (for all $1 \le j \le t$) and (C''_j, D''_j) is LCP in $H_j''^\ell$ (for all $1 \le j \le t$).

Proof. As R-modules in R^ℓ, being LCP for C and D amounts to $C \oplus D = R^\ell$. This means, via the CRT isomorphism, that

$$\phi(C)\oplus\phi(D)=\bigoplus_{i=1}^{s}G_i^\ell\oplus\left(\bigoplus_{j=1}^{t}\Big(H_j'^\ell\oplus H_j''^\ell\Big)\right), \tag{3.5}$$

where $\phi(C)$ and $\phi(D)$ are simply constituent descriptions of C and D. If (3.5) holds, then we have

$$C_i + D_i = G_i^{\ell} \quad (1 \leq i \leq s), \quad C'_j + D'_j = H_j'^{\ell} \text{ and } C''_j + D''_j = H_j''^{\ell} \quad (1 \leq j \leq t).$$

Hence, sum of the dimensions for all pair of constituents over the same field is greater or equal to ℓ. For instance,

$$\ell = \dim(C_i + D_i) = \dim C_i + \dim D_i - \dim(C_i \cap D_i). \tag{3.6}$$

Note that the dimensions are over the base field G_i. On the other hand, $\dim_{\mathbb{F}_q}(C) + \dim_{\mathbb{F}_q}(D) = m\ell$ (since they are complementary) and we have

$$\begin{aligned}
\dim_{\mathbb{F}_q}(C) &= \deg f_1 \dim C_1 + \cdots + \deg f_s \dim C_s + \deg h_1(\dim C'_1 + \dim C''_1) + \cdots + \deg h_t(\dim C'_t + \dim C''_t) \\
\dim_{\mathbb{F}_q}(D) &= \deg f_1 \dim D_1 + \cdots + \deg f_s \dim D_s + \deg h_1(\dim D'_1 + \dim D''_1) + \cdots + \deg h_t(\dim D'_t + \dim D''_t)
\end{aligned}$$

Summing up the right and left hand sides above yields

$$m\ell = \sum_{i=1}^{s} \deg f_i(\dim C_i + \dim D_i) + \sum_{j=1}^{t} \deg h_j \left[(\dim C'_j + \dim D'_j) + (\dim C''_j + \dim D''_j)\right].$$

As

$$m = \sum_{i=1}^{s} \deg f_i + \sum_{j=1}^{t} 2 \deg h_j,$$

this forces sum of the dimensions of each pair of corresponding constituents of C and D to be ℓ, which is equivalent to trivial intersection of these constituents by (3.6), or their LCP'ness.

Assuming LCP'ness of all the constituents of C and D, the converse statement follows essentially with similar arguments. □

We will see that unlike constacyclic LCP of codes, QC LCP of codes C and D need not satisfy $d(C) = d(D^{\perp})$. For this, we recall double circulant (DC) codes. These are one-generator, index 2 QC codes. More concretely, a DC code is a one-generator module $\langle(1, a(x))\rangle \in R^2$. The following characterizes DC LCP of codes.

Proposition 3.2. *Let $C = \langle(1, a(x))\rangle$ and $D = \langle(1, b(x))\rangle$ be DC codes in R^2. Then (C, D) is LCP of codes if and only if* $\gcd(a(x) - b(x), x^m - 1) = 1$.

Proof. Constituents of a DC code are 1-dimensional subspaces in 2-dimensional ambient spaces. Hence, constituents of C and D, lying in the same ambient space, satisfy the LCP condition in Proposition 3.1 if and only if they intersect trivially. This amounts to trivial intersection of the spaces $\langle(1, a(\xi^u))\rangle$ and $\langle(1, b(\xi^u))\rangle$, for any root ξ^u of the polynomial $x^m - 1$. Note that such spaces have nontrivial intersection if and only if $a(\xi^u) = b(\xi^u)$, or equivalently, an irreducible factor of $x^m - 1$ (corresponding to the minimal polynomial of ξ^u over $\mathbb{F}_q$) divides $a(x) - b(x)$. Hence the result follows. □

Example 3.3. Let $q = 2$, $m = 3$, $a(x) = x + 1$ and $b(x) = x^2 + x + 1$. Note that $a(x) - b(x) = x^2$ and $x^3 - 1$ are relatively prime, hence the condition in Proposition 3.2 is satisfied. Therefore, length 6 binary DC codes $C = \langle(1, a(x))\rangle$ and $D = \langle(1, b(x))\rangle$ are LCP. Parameters of C and D are $[6, 3, 3]$

and $[6,3,2]$, respectively. On the other hand, $D^{\perp}$ is a $[6,3,2]$ DC code. Hence, the analogue of Theorem 2.4 does not apply to QC codes in general.

A 2D cyclic code is a QC code with cyclic constituents (e.g. see [4]). In this case, the code is not only an R-submodule of R^{ℓ} but it is also closed under cyclic shift in R^{ℓ}. Moreover, when m and ℓ are relatively prime to q and each other, then a 2D cyclic code is equivalent to a cyclic code ([4, Remark 3.6]). Next, we show that 2D cyclic LCP of codes (C,D) satisfies the analogue of Theorem 2.4.

Theorem 3.4. *Let (C,D) be a q-ary 2D cyclic LCP of codes of length $m\ell$ and index ℓ. Then C and $D^{\perp}$ are equivalent.*

Proof. Let C be as in (3.3) and let the complementary code D decompose as

$$D = \left(\bigoplus_{i=1}^{s} D_i\right) \oplus \left(\bigoplus_{j=1}^{t} \Big(D'_j \oplus D''_j\Big)\right).$$

Then by (3.4), $D^{\perp}$ is of the form

$$D^{\perp} = \left(\bigoplus_{i=1}^{s} D_i^{\perp_h}\right) \oplus \left(\bigoplus_{j=1}^{t} \Big(D_j''^{\perp_e} \oplus D_j'^{\perp_e}\Big)\right).$$

Let us set the generating polynomials for the cyclic constituents of C as follows:

$$\begin{aligned} C_i &= \langle a_i(x)\rangle \subseteq G_i[x]/\langle x^{\ell}-1\rangle, & 1 \le i \le s\\ C'_j &= \langle a'_j(x)\rangle \subseteq H'_j[x]/\langle x^{\ell}-1\rangle, & 1 \le j \le t\\ C''_j &= \langle a''_j(x)\rangle \subseteq H''_j[x]/\langle x^{\ell}-1\rangle, & 1 \le j \le t. \end{aligned}$$

We set $|G_i| = q^{e_i}$ and $|H'_j| = |H''_j| = q^{f_j}$ (for all i,j) and note that each e_i is even as the polynomial g_i that defines G_i is self-reciprocal (see (3.1)). The constituents of $D^{\perp}$ have the following generating polynomials (by Section 2 for the Euclidean dual constituents $D_j'^{\perp_e}, D_j''^{\perp_e}$'s and by [5, Section 4] for the the Hermitian dual constituents $D_i^{\perp_h}$'s):

$$\begin{aligned} D_i^{\perp_h} &= \langle \bar{a}_i^{*}(x)\rangle \subseteq G_i[x]/\langle x^{\ell}-1\rangle, & 1 \le i \le s\\ D_j''^{\perp_e} &= \langle a_j''^{*}(x)\rangle \subseteq H'_j[x]/\langle x^{\ell}-1\rangle, & 1 \le j \le t\\ D_j'^{\perp_e} &= \langle a_j'^{*}(x)\rangle \subseteq H''_j[x]/\langle x^{\ell}-1\rangle, & 1 \le j \le t. \end{aligned}$$

Here, $\bar{a}_i^{*}(x)$ denotes the polynomial obtained from the reciprocal of $a_i(x)$ by raising each coefficient to exponent $q^{e_i/2}$. Raising elements of G_i to the exponent $q^{e_i/2}$ will be denoted similarly below.

Let σ denote the permutation of $\{0,1,\ldots,\ell-1\}$ that sends μ to $\ell-1-\mu$. If $\gamma_i, \alpha_j, \beta_j$ denote the constant coefficients of $a_i(x), a'_j(x), a''_j(x)$ respectively (for all $1 \le i \le s$ and $1 \le j \le t$), then by the proof of Theorem 2.4 and its easy extension to the Hermitian dual of cyclic codes, we have the following bijections:

$$\begin{aligned} C_i &\longrightarrow D_i^{\perp_h}\\ (c_{i,0}, c_{i,1}, \ldots, c_{i,\ell-1}) &\longmapsto \bar{\gamma}_i^{\,-1}\left(\bar{c}_{i,\sigma(0)}, \bar{c}_{i,\sigma(1)}, \ldots, \bar{c}_{i,\sigma(\ell-1)}\right), \end{aligned} \tag{3.7}$$

$$\begin{array}{rcl} C'_j & \longrightarrow & D'^{\perp_e}_j \\ (d_{j,0}, d_{j,1}, \ldots, d_{j,\ell-1}) & \longmapsto & \alpha_j^{-1}\left(d_{j,\sigma(0)}, d_{j,\sigma(1)}, \ldots, d_{j,\sigma(\ell-1)}\right), \end{array} \tag{3.8}$$

$$\begin{array}{rcl} C''_j & \longrightarrow & D''^{\perp_e}_j \\ (e_{j,0}, e_{j,1}, \ldots, e_{j,\ell-1}) & \longmapsto & \beta_j^{-1}\left(e_{j,\sigma(0)}, e_{j,\sigma(1)}, \ldots, e_{j,\sigma(\ell-1)}\right). \end{array} \tag{3.9}$$

We now utilize the trace representation of QC codes via constituents. Let ξ denote a primitive mth root of unity, and u_i and v_j be such that

$$G_i = \mathbb{F}_q(\xi^{u_i}), \quad H'_j = \mathbb{F}_q(\xi^{v_j}), \quad H''_j = \mathbb{F}_q(\xi^{-v_j}).$$

Let Tr_i denote the trace map from G_i to $\mathbb{F}_q$ and Tr'_j denote the trace map from $H'_j = H''_j$ to $\mathbb{F}_q$ (for all i, j). If we view a codeword $d^\perp \in D^\perp$ as an $m \times \ell$ array, then by [6, Theorem 5.1] and the bijections (3.7), (3.8) and (3.9), the kth row of $d^\perp$ (for $0 \le k \le m-1$) is of the form

$$\begin{aligned} d_k^\perp \;=\; & \Big(\underbrace{\cdots + \left(\mathrm{Tr}_i(\bar{\gamma_i}^{-1}\bar{c}_{i,\sigma(0)}\xi^{-ku_i}), \ldots, \mathrm{Tr}_i(\bar{\gamma_i}^{-1}\bar{c}_{i,\sigma(\ell-1)}\xi^{-ku_i})\right) + \cdots}_{1 \le i \le s} \\ & \underbrace{\cdots + \left(\mathrm{Tr}'_j(\beta_j^{-1}e_{j,\sigma(0)}\xi^{-kv_j}), \ldots, \mathrm{Tr}'_j(\beta_j^{-1}e_{j,\sigma(\ell-1)}\xi^{-kv_j})\right) + \left(\mathrm{Tr}'_j(\alpha_j^{-1}d_{j,\sigma(0)}\xi^{kv_j}), \ldots, \mathrm{Tr}'_j(\alpha_j^{-1}d_{j,\sigma(\ell-1)}\xi^{kv_j})\right) + \cdots}_{1 \le j \le t}\Big) \end{aligned}$$

for some codewords $(c_{i,0}, \ldots, c_{i,\ell-1}) \in C_i$, $(d_{j,0}, d_{j,1}, \ldots, d_{j,\ell-1}) \in C'_j$ and $(e_{j,0}, e_{j,1}, \ldots, e_{j,\ell-1}) \in C''_j$ (for $1 \le i \le s$, $1 \le j \le t$). Note that $\mathrm{Tr}_i(\bar{z}) = \mathrm{Tr}_i(z)$ for any $z \in G_i$. Moreover, it is not difficult to see that $\bar{\xi}^{u_i} = \xi^{-u_i}$. Hence,

$$\begin{aligned} d_k^\perp \;=\; & \Big(\underbrace{\cdots + \left(\mathrm{Tr}_i(\gamma_i^{-1}c_{i,\sigma(0)}\xi^{ku_i}), \ldots, \mathrm{Tr}_i(\gamma_i^{-1}c_{i,\sigma(\ell-1)}\xi^{ku_i})\right) + \cdots}_{1 \le i \le s} \\ & \underbrace{\cdots + \left(\mathrm{Tr}'_j(\beta_j^{-1}e_{j,\sigma(0)}\xi^{-kv_j}), \ldots, \mathrm{Tr}'_j(\beta_j^{-1}e_{j,\sigma(\ell-1)}\xi^{-kv_j})\right) + \left(\mathrm{Tr}'_j(\alpha_j^{-1}d_{j,\sigma(0)}\xi^{kv_j}), \ldots, \mathrm{Tr}'_j(\alpha_j^{-1}d_{j,\sigma(\ell-1)}\xi^{kv_j})\right) + \cdots}_{1 \le j \le t}\Big). \end{aligned}$$

Now, consider the codeword $c \in C$ which is obtained from the codewords $\gamma_i^{-1}(c_{i,0}, \ldots, c_{i,\ell-1}) \in C_i$, $\alpha_j^{-1}(d_{j,0}, d_{j,1}, \ldots, d_{j,\ell-1}) \in C'_j$ and $\beta_j^{-1}(e_{j,0}, e_{j,1}, \ldots, e_{j,\ell-1}) \in C''_j$ (for $1 \le i \le s$, $1 \le j \le t$). Then the kth row of c is

$$\begin{aligned} c_k \;=\; & \Big(\underbrace{\cdots + \left(\mathrm{Tr}_i(\gamma_i^{-1}c_{i,0}\xi^{-ku_i}), \ldots, \mathrm{Tr}_i(\gamma_i^{-1}c_{i,\ell-1}\xi^{-ku_i})\right) + \cdots}_{1 \le i \le s} \\ & \underbrace{\cdots + \left(\mathrm{Tr}'_j(\alpha_j^{-1}d_{j,0}\xi^{-kv_j}), \ldots, \mathrm{Tr}'_j(\alpha_j^{-1}d_{j,\ell-1}\xi^{-kv_j})\right) + \left(\mathrm{Tr}'_j(\beta_j^{-1}e_{j,0}\xi^{kv_j}), \ldots, \mathrm{Tr}'_j(\beta_j^{-1}e_{j,\ell-1}\xi^{kv_j})\right) + \cdots}_{1 \le j \le t}\Big). \end{aligned}$$

If τ denotes the permutation of $\{0, 1, \ldots, m-1\}$ that fixes 0 and sends all other μ to $m - \mu$, then $d_k^\perp$ and $c_{\tau(k)}$ are two rows of $d^\perp \in D^\perp$ and $c \in C$ (length ℓ vectors) which are obtained from each other by the permutation σ. In other words, codewords of C and $D^\perp$ in $m \times \ell$ array form are equivalent via σ-column and τ-row permutations. This proves the claim. □

4. Examples

For Table 1, random pair of LCP constituents C_i and D_i (of length ℓ and of dimension 1 and $\ell - 1$, respectively) over extensions of $\mathbb{F}_2$, satisfying the conditions in Theorem 3.1, are searched by Magma [2]. Note that the resulting binary QC codes C and D have length $m\ell$ and the dimension of C is m. Then, the value $\min(d(C), d(D^\perp))$ is determined and presented as $\mathbf{d_{LCP}}$. The distances

$\mathbf{d_{LCP}}$, $\mathbf{d_{LCD}}$ and $\mathbf{d}^*$ are shown in Table 1, respectively, for each choice of m and ℓ. The values $\mathbf{d_{LCD}}$ correspond to the best distances for LCD codes from [5, Table 1], where the binary LCD code C has dimension m. The parameter $\mathbf{d}^*$ represents the optimal distance for binary linear codes of length $m\ell$ and dimension m. Note that there are many instances in Table 1 where $\mathbf{d_{LCP}} > \mathbf{d_{LCD}}$.

ℓ/**m**	**3**			**5**			**7**			**9**			**11**			**13**			**15**			**17**		
2	3^*	2	3	4^*	3	4	4^*	4^*	4	4	4	6	5	5	7	7^*	6	7	6	6	8	6	6	8
3	4^*	3	4	6	5	7	8^*	7	8	8	8	10	9	9	12	10	10	12	12	11	14			
5	8^*	7	8	11	10	12	14	13	16	16	15	18												
7	12^*	10	12																					

TABLE 1. Binary QC LCP of codes

Table 2 presents results for binary double-circulant LCP of codes $C = \big\langle\big(1, a(x)\big)\big\rangle \subset R^2$ and $D = \big\langle\big(1, b(x)\big)\big\rangle \subset R^2$, where $R = \mathbb{F}_2[x]/\langle x^m - 1\rangle$. The codes C and D are QC of length $2m$ and dimension m. The search is done in Magma for random $a(x), b(x) \in R$ satisfying the condition in Proposition 3.2. In the table, $\mathbf{d_{LCP}}$ denotes the maximum value of $\min(d(C), d(D^\perp))$ among all such LCP of double-circulant codes C and D. Next, we present the best possible distances $\mathbf{d_{LCD}}$ which can be attained by a LCD DC code C of length $2m$ and dimension m (see [5, Table 2]). Note again that there are examples where $\mathbf{d_{LCP}} > \mathbf{d_{LCD}}$. On the last line, $\mathbf{d}^*$ represents optimal distances for binary linear codes of length $2m$ and dimension m. Let us note that these types of QC codes were excluded from Table 1, as was the case for Tables 1 and 2 in [5]. This is evident when the first row ($\ell = 2$) of Table 1 is compared with Table 2. For $m = 9, 11, 15, 17$, $\mathbf{d_{LCP}}$ in Table 2 is better than $\mathbf{d_{LCP}}$ in Table 1.

m	**3**	**5**	**7**	**9**	**11**	**13**	**15**	**17**
$\mathbf{d_{LCP}}$	2	4^*	4^*	5	6	7^*	7	8^*
$\mathbf{d_{LCD}}$	1	3	4^*	3	6	7^*	5	8^*
$\mathbf{d}^*$	3	4	4	6	7	7	8	8

TABLE 2. Binary DC LCP of codes

For both tables, the distances attaining the optimal value for linear codes are marked by "*".

5. A Linear Programming Bound for Binary LCP of Codes

In this section, we will derive an upper bound on the size of the binary LCP of codes, which is analogous to the bound derived for LCD codes in [3]. More precisely, for binary LCP of codes C and D of common length n, the aim is to maximize the dimension of C for a given minimum distance of C and dual distance of D.

Let $\{A_i\}$ and $\{B_i\}$ denote the weight distributions of C and D, respectively. Let $d = d(C)$. Then we have $A_0 = B_0 = 1$ and

$$A_1 = \cdots = A_{d-1} = 0,\ A_i \geq 0 \text{ for } d \leq i \leq n \tag{5.1}$$

$$B_i \geq 0 \text{ for } 1 \leq i \leq n. \tag{5.2}$$

Let $P_i(x)$ be the Krawtchouk polynomial of degree i given by the following generating function:

$$\sum_{i=0}^{n} P_i(x)z^i = (1+z)^{n-x}(1-z)^x,\ \text{where } P_i(0) = \binom{n}{i}.$$

Recall the so-called Delsarte inequality for C:

$$\sum_{j=1}^{n} P_i(j)A_j \geq -\binom{n}{i}. \tag{5.3}$$

Suppose $d' = d(D^\perp)$ and let $\{B_i^\perp\}$ denote the weight distribution of $D^\perp$. By MacWilliams formula we know that

$$B_i^\perp = 2^{-k}\sum_{j=0}^{n} B_j P_i(j),$$

where

$$B_0^\perp = 1, B_1^\perp = \cdots = B_{d'-1}^\perp = 0,\ B_i^\perp \geq 0 \text{ for } d' \leq i \leq n.$$

Hence we obtain the following by combining the two identites above.

$$\sum_{j=1}^{n} P_i(j)B_j = -\binom{n}{i} \text{ for } 1 \leq i \leq d'-1 \tag{5.4}$$

$$\sum_{j=1}^{n} P_i(j)B_j \geq -\binom{n}{i} \text{ for } d' \leq i \leq n \tag{5.5}$$

For all $1 \leq i \leq n$, we have by the definition of LCP of codes

$$A_i + B_i \leq \binom{n}{i}. \tag{5.6}$$

If the dimension of C is k, then by using the facts $2^k - 1 = \sum_{i=1}^n A_i$, and $2^{n-k} - 1 = \sum_{i=1}^n B_i$, we obtain the following bounds.

Proposition 5.1. *If $k \geq k_0$, then we have*

$$\sum_{i=1}^{n} -A_i \leq 1 - 2^{k_0}. \tag{5.7}$$

$$\sum_{i=1}^{n} B_i \leq 2^{n-k_0} - 1. \tag{5.8}$$

If M is an $m \times r$ matrix and x, h are column vectors of length r and m, respectively, we denote by $U(M, h)$ the maximum of $\sum_{i=1}^{r} x_i$ for non-negative rationals x_i subject to m linear constraints $Mx \leq h$. We need the following auxiliary matrices:

- $P = (P_i(j))$ for $i, j \in \{1, \ldots, n\}$,
- I_n : the $n \times n$ identity matrix,
- Z_n : the $n \times n$ zero matrix,
- 1_n : all 1 vector of length n,
- 0_n : all 0 vector of length n,
- Δ : the vector of length n with $\Delta_i = \binom{n}{i}$ for $1 \leq i \leq n$.

Now let $U(n, k_0, d, d')$ be the maximum of $\sum_{i=1}^{n} A_i$ over $A_i, B_i \geq 0$, $i \in \{1, \ldots, n\}$ satisfying the constraints (5.1), (5.2), (5.3),(5.4),(5.5), (5.6), (5.7) and (5.8). For $m = 5n + 2$ and $r = 2n$, let us set

$$M = \begin{bmatrix} -I_n & | & Z_n \\ Z_n & | & -I_n \\ -P & | & Z_n \\ Z_n & | & -P \\ I_n & | & I_n \\ 0_n & | & 1_n \\ -1_n & | & 0_n \end{bmatrix} \text{ and } h^T = [0_n, 0_n, \Delta, \Delta, \Delta, 2^{n-k_0} - 1, 1 - 2^{k_0}].$$

After this preparation, the following result is immediate.

Theorem 5.2. *If $k \geq k_0$, the minimum distance of C is at least d and the dual distance of D is d', then*

$$2^k \leq 1 + U(n, k_0, d, d').$$

Given a complementary pair C and D, the special case $d = d'$ is of particular interest in practice (see [1]). The following table obtained by using Magma [2] presents the results in comparison with the classical linear programming (LP) bound and LP bound for LCD codes in [3].

n/d=d'	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**
1	1																													
2	2	0*																												
3	3	2	1																											
4	4	2*	1	0*																										
5	5	4	2	1	1																									
6	6	4*	3	2	1	0*																								
7	7	6	4	3	1	1	1																							
8	8	6*	4	3*	2	1	1	0*																						
9	9	8	5	4	2	2	1	1	1																					
10	10	8*	6	5	3	2	1	1	1	0*																				
11	11	10	7	6	4	3	2	1	1	1	1																			
12	12	10*	8	7	5	4	2	2	1	1	1	0*																		
13	13	12	9	8	6	5	3	2	1	1	1	1	1																	
14	14	12*	10	9	7	6	4	3	2	1	1	1	1	0*																
15	15	14	11	10	8	7	5	4	2	2	1	1	1	1	1															
16	16	14*	11	10*	8	8(7)	5	4*	2	2	1	1	1	1	1	0*														
17	17	16	12	11	9	8	6	5	3	2	2	1	1	1	1	1	1													
18	18	16*	13	12	10	9	7	6	4	3	2	2	1	1	1	1	1	0*												
19	19	18	14	13	11	10	8	7	5	4	2	2	1	1	1	1	1	1	1											
20	20	18*	15	14	12	11	9	8	6	5	3	2	2	1	1	1	1	1	1	0*										
21	21	20	16	15	12	12	10	9	6	6	3	3	2	2	1	1	1	1	1	1	1									
22	22	20*	17	16	13	12	11	10	7	6	4	3	2	2	1	1	1	1	1	1	1	0*								
23	23	22	18	17	14	13	12	11	8	7	5	4	2	2	2	1	1	1	1	1	1	1	1							
24	24	22*	19	18	15	14	12	12(11)	9	8	6	5	3	2	2	2	1	1	1	1	1	1	1	0*						
25	25	24	20	19	16	15	13	12	10	9	6	6	3	3	2	2	1	1	1	1	1	1	1	1	1					
26	26	24*	21	20	17	16	14	13	10	10	7	6	4	3	2	2	2	1	1	1	1	1	1	1	1	0 *				
27	27	26	22	21	18	17	14	14	11	10	8	7	5	4	3	2	2	2	1	1	1	1	1	1	1	1	1			
28	27*	27(26)	23(22)	22(21)	19(18)	18(17)	15(14)	14	12(11)	11(10)	9(8)	8(7)	6(5)	5(4)	3	3(2)	2	2	1	1	1	1	1	1	1	1	1	0*		
29	28*	27	24	23	20	19	16	15	13	12	10	9	7	6	4	3	2	2	2	1	1	1	1	1	1	1	1	1	1	
30	29*	29(28)	25	24	20	20	17	16	14	13	10	10	7	7	5	4	2	2	2	2	1	1	1	1	1	1	1	1	1	0*

Table 3. The values in paranthesis are from the LP bound for LCD codes, if different. The starred values differ from classical LP bound, $a*$ implies that classical LP bound gives $a+1$.

6. Acknowledgment

Güneri and Özbudak are supported by the TÜBİTAK project 215E200, which is associated with the SECODE project in the scope of the CHIST-ERA Program. Carlet and Solé are also supported by the SECODE Project.

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 57, 2015.

[2] W. Bosma, J. Cannon and C. Playoust, "The Magma algebra system. I. The user language", *J. Symb. Comput.*, vol. 24, 235265, 1997.

[3] S. T. Dougherty, J.-L. Kim, B. Özkaya, L. Sok and P. Solé, "The combinatorics of LCD codes: Linear programming bound and orthogonal matrices", *Int. J. Inf. and Coding Theory*, vol. 4, no. 2/3, 116-128, 2017.

[4] C. Güneri and F. Özbudak, "A relation between quasi-cyclic codes and 2-D cyclic codes", *Finite Fields Appl.*, vol. 18, 123-132, 2012.

[5] C. Güneri, B. Özkaya and P. Solé, "Quasi-cyclic complementary dual codes", *Finite Fields Appl.*, vol. 42, 67-80, 2016.

[6] S. Ling and P. Solé, "On the algebraic structure of quasi-cyclic codes I: finite fields", *IEEE Trans. Inform. Theory*, vol. 47, 2751-2760, 2001.

[7] S. Ling and P. Solé, "On the algebraic structure of quasi-cyclic codes III: generator theory", *IEEE Trans. Inform. Theory*, vol. 51, 2692-2700, 2005.

[8] J.P. Pedersen and C. Dahl, "Classification of pseudo-cyclic MDS codes", *IEEE Trans. Inform. Theory*, vol. 37, 365-370, 1991.

[9] Y. Yang and W. Cai, "On self-dual constacyclic codes over finite fields", *Des. Codes Cryptogr.*, vol. 74, 355-364, 2015.

[10] X. Yang and J.L. Massey, "The condition for a cyclic code to have a complementary dual", *Discrete Math.*, vol. 126, 391-393, 1994.