Communications in Mathematics and Applications
Vol. 13, No. 2, pp. 493–500, 2022
ISSN 0975-8607 (online); 0976-5905 (print)
Published by RGN Publications
DOI: 10.26713/cma.v13i2.1756

http://www.rgnpublications.com

Research Article

Linear Complementary Pairs of Multi-twisted Codes and their Characterizations

Rubayya*, K.S. Mansoor Ali and M. Sumanth Datt

School of Mathematics and Statistics, University of Hyderabad, Hyderabad 500046, India
***Corresponding author:** rubayyayusuf@gmail.com

Received: December 2, 2021 **Accepted:** March 8, 2022

Abstract. The linear complementary pairs (LCP) of codes is studied mainly due to their application in cryptography. It is used in the protection against physical attacks such as the side channel and fault injection. In this paper, we study the LCP of codes which belong to the class of multi-twisted codes. We give characterizations for the multi-twisted LCP of codes via their constituents and in terms of the generator polynomial of the code.

Keywords. Linear complementary pair, Multi-twisted code, Finite field, Constituents

Mathematics Subject Classification (2020). 94B05, 94B15

1. Introduction

Cyclic codes were introduced by E. Prange in 1957 [8]. Thereafter various families of codes were discovered as generalisations of cyclic codes. These codes have good algebraic structures and contain various optimal codes. One such family is multi-twisted codes which was introduced by Aydin and Halilovic [1]. It is a generalisation of already known quasi-twisted codes as well. They have given various methods to construct multi-twisted codes and studied some of the basic properties of these codes. They have shown that there are codes with better parameters in this class compared to the other known linear codes. Later, Sharma *et al*. [9] described the algebraic structure of multi-twisted codes and its dual codes. They have obtained some conditions under which the multi-twisted code is a linear complementary dual (LCD). The LCD codes were

introduced by Massey [6] in 1992. Later, Yang and Massey obtained characterisation for LCD of cyclic codes in [10] using the generator polynomial. Due to the application in cryptography ([2, 7]), there was a renewed interest in studying LCD and LCP of codes. The work of Yang and Massey was extended by Carlet *et al*. [3] for characterisation of LCP of constacyclic codes. In the same paper, the authors have also obtained characterisation for the quasi-cyclic LCP of codes. In this work, we obtain characterisations for LCP of multi-twisted codes in terms of its constituents and generator polynomial.

2. Preliminaries

Let q be a power of a prime p and $\mathbb{F}_q$ denote the finite field of order q. Let $n, m_1, m_2, \ldots, m_d$ be natural numbers such that $(m_i, p) = 1$, for all $1 \le i \le d$ and $n = m_1 + m_2 + \cdots + m_d$. Let $\mathbb{F}_q^n$ denote the vector space which consists of all n-tuples over $\mathbb{F}_q$. Let $\mu_1, \mu_2, \ldots, \mu_d$ be non-zero elements of $\mathbb{F}_q$. Let $\mathbb{F}_q[x]$ be the polynomial ring over $\mathbb{F}_q$ and $M_i = \mathbb{F}_q[x]/\langle x^{m_i} - \mu_i \rangle$ for $1 \le i \le d$. The $\mathbb{F}_q[x]$-module M_i is also a vector space over $\mathbb{F}_q$ of dimension m_i. Let $M = \prod_{i=1}^{d} M_i$. The map $T : \mathbb{F}_q^n \to M$, given by

$$T(c_{1,0}, c_{1,1}, \ldots, c_{1,m_1-1}; c_{2,0}, \ldots, c_{2,m_2-1}; \ldots; c_{d,0}, \ldots, c_{d,m_d-1}) = (c_1(x), c_2(x), \ldots, c_d(x)),$$

where $c_i(x) = \sum_{j=0}^{m_i-1} c_{i,j} x^j \in M_i$ for $1 \le i \le d$ defines a vector space isomorphism.

By a multi-twisted code $\mathscr{C}$ of length n over $\mathbb{F}_q$, we mean a non-zero $\mathbb{F}_q[x]$-submodule of M. This is equivalent to a linear code (a non-zero subspace of $\mathbb{F}_q^n$) satisfying:
if $c = (c_{1,0}, c_{1,1}, \ldots, c_{1,m_1-1}; c_{2,0}, c_{2,1}, \ldots, c_{2,m_2-1}; \ldots; c_{d,0}, c_{d,1}, \ldots, c_{d,m_d-1}) \in \mathscr{C}$, then the multi-twisted shift of c given by

$$T(c) = (\mu_1 c_{1,m_1-1}, c_{1,0}, \ldots, c_{1,m_1-2}; \mu_2 c_{2,m_2-1}, c_{2,0}, \ldots, c_{2,m_2-2}; \ldots; \mu_d c_{d,m_d-1}, c_{d,0}, \ldots, c_{d,m_d-2})$$

is also an element of $\mathscr{C}$.

Let $f_1(x), f_2(x), \ldots, f_r(x)$ be the factors of $x^{m_i} - \mu_i$, for $1 \le i \le d$, which are distinct and irreducible. For $1 \le j \le r$ and $1 \le i \le d$, define

$$l_{ji} = \begin{cases} 1 & \text{if } f_j(x) \text{ divides } x^{m_i} - \mu_i \text{ in } \mathbb{F}_q[x] \\ 0 & \text{otherwise.} \end{cases}$$

Then for $1 \le i \le d$, we have $x^{m_i} - \mu_i = \prod_{j=1}^{r} f_j(x)^{l_{ji}}$. Let $F_j = \frac{\mathbb{F}_q[x]}{\langle f_j(x) \rangle}$. As $f_j(x)$ is irreducible, we have F_j is a field. As $(m_i, p) = 1$, from [9] we have $M_i = \prod_{j=1}^{r} l_{ji} F_j$, where $l_{ji} F_j = (0)$ if $l_{ji} = 0$ and $l_{ji} F_j = F_j$ otherwise. Hence, we have

$$M \cong \bigoplus_{j=1}^{r} \left(\prod_{i=1}^{d} l_{ji} F_j \right). \tag{2.1}$$

Let $l_j = \sum_{i=1}^{d} l_{ji}$ for each $1 \le j \le r$, then $N_j = \prod_{i=1}^{d} l_{ji} F_j$ is an l_j-dimensional vector space over F_j.

Recall that the reciprocal polynomial of a non-zero $f(x)$ of degree k is defined as $f^*(x) = x^k f(1/x)$ (see [4, p. 88]). A polynomial $f(x)$ is said to be self-reciprocal if $f(x) = f^*(x)$ and a pair $(f(x), g(x))$ of polynomials is called a reciprocal pair if $g(x) = f^*(x)$. Let $X = \{f_1(x), f_2(x), \ldots, f_r(x)\}$, $A = \{f(x) \in X \mid f(x) \text{ is self reciprocal}\}$, $B = \{f(x) \in X \mid f(x)$ has a reciprocal in X different from $f(x)\}$ and $C = \{f(x) \in X \mid f(x)$ has no reciprocal in $X\}$. By reordering the set X if necessary, we may assume that $A = \{f_1(x), f_2(x), \ldots, f_{r_0}(x)\}$, $B = \{f_{r_0+1}(x), f^*_{r_0+1}(x), \ldots, f_{r_1}(x), f^*_{r_1}(x)\}$ and $C = \{f_{r_1+1}(x), f_{r_1+2}(x), \ldots, f_{r'}(x)\}$ where $r' = r - (r_1 - r_0)$. Let

$$F_\alpha = \frac{\mathbb{F}_q[x]}{\langle f_\alpha(x)\rangle}, \qquad 1 \le \alpha \le r_0,$$

$$F_\beta = \frac{\mathbb{F}_q[x]}{\langle f_\beta(x)\rangle},\ F'_\beta = \frac{\mathbb{F}_q[x]}{\langle f^*_\beta(x)\rangle}, \quad r_0 + 1 \le \beta \le r_1, \text{ and}$$

$$F_\gamma = \frac{\mathbb{F}_q[x]}{\langle f_\gamma(x)\rangle}, \qquad r_1 + 1 \le \gamma \le r'.$$

Let $N_\alpha = (l_{\alpha 1}F_\alpha, l_{\alpha 2}F_\alpha, \ldots, l_{\alpha d}F_\alpha)$ for $1 \le \alpha \le r_0$, $N_\beta = (l_{\beta 1}F_\beta, l_{\beta 2}F_\beta, \ldots, l_{\beta d}F_\beta)$, $N'_\beta = (l'_{\beta 1}F'_\beta, l'_{\beta 2}F'_\beta, \ldots, l'_{\beta d}F'_\beta)$ for $r_0 + 1 \le \beta \le r_1$ and $N_\gamma = (l_{\gamma 1}F_\gamma, l_{\gamma 2}F_\gamma, \ldots, l_{\gamma d}F_\gamma)$ for $r_1 + 1 \le \gamma \le r'$, where for $r_0 + 1 \le \beta \le r_1$ and $1 \le i \le d$,

$$l'_{\beta i} = \begin{cases} 1 & \text{if } f^*_\beta(x) \text{ divides } x^{m_i} - \mu_i \text{ in } \mathbb{F}_q[x], \\ 0 & \text{otherwise.} \end{cases}$$

By (2.1), we have an isomorphism ϕ from M to

$$\left(\bigoplus_{\alpha=1}^{r_0} N_\alpha\right) \oplus \left(\bigoplus_{\beta=r_0+1}^{r_1} [N_\beta \oplus N'_\beta]\right) \oplus \left(\bigoplus_{\gamma=r_1+1}^{r'} N_\gamma\right).$$

Let $\mathscr{C}$ be a multi-twisted code of M over $\mathbb{F}_q$. From (2.2), M is a semi-simple $\mathbb{F}_q[x]$-module. The multi-twisted code $\mathscr{C}$, being a submodule of a semi-simple $\mathbb{F}_q[x]$-module M, is also semi-simple (see [3, Proposition 2.2]). Hence, $\mathscr{C}$ is also a direct sum of simple $\mathbb{F}_q[x]$-modules. That is, we have

$$M \simeq \left(\bigoplus_{\alpha=1}^{r_0} N_\alpha\right) \oplus \left(\bigoplus_{\beta=r_0+1}^{r_1} [N_\beta \oplus N'_\beta]\right) \oplus \left(\bigoplus_{\gamma=r_1+1}^{r'} N_\gamma\right) \tag{2.2}$$

and hence we have

$$\mathscr{C} \cong \left(\bigoplus_{\alpha=1}^{r_0} \mathscr{C}_\alpha\right) \oplus \left(\bigoplus_{\beta=r_0+1}^{r_1} [\mathscr{C}_\beta \oplus \mathscr{C}'_\beta]\right) \oplus \left(\bigoplus_{\gamma=r_1+1}^{r'} \mathscr{C}_\gamma\right),$$

where $\mathscr{C}_\alpha = \phi(\mathscr{C}) \cap N_\alpha$ for $1 \le \alpha \le r_0$, $\mathscr{C}_\beta = \phi(\mathscr{C}) \cap N_\beta$ and $\mathscr{C}'_\beta = \phi(\mathscr{C}) \cap N'_\beta$ for $r_0 + 1 \le \beta \le r_1$ and $\mathscr{C}_\gamma = \phi(\mathscr{C}) \cap N_\gamma$ for $r_1 + 1 \le \gamma \le r'$. We call $\mathscr{C}_\alpha$, $\mathscr{C}_\beta$, $\mathscr{C}'_\beta$ and $\mathscr{C}_\gamma$ as the constituents of $\mathscr{C}$.

3. Linear Complementary Pairs(LCP) of Codes

When $m_1 = m_2 = \cdots = m_d = m$ and $\mu_1 = \mu_2 = \cdots = \mu_d = 1$, then the code $\mathscr{C}$ is a quasi-cyclic code of length $n (= md)$ over $\mathbb{F}_q$. Two linear codes $\mathscr{C}$ and $\mathscr{D}$ of length n over $\mathbb{F}_q$ are said to

be linear complementary pairs (LCP) of codes if $\mathscr{C} \oplus \mathscr{D} = \mathbb{F}_q^n$. In a paper by Carlet *et al*. [3], a characterisation for quasi cyclic LCP of codes is obtained via their constituents. We shall consider in this paper LCP of multi-twisted codes of M. Two multi-twisted codes $\mathscr{C}$ and $\mathscr{D}$ are said to be LCP of codes of M if $\mathscr{C} \oplus \mathscr{D} = M$. From the above section, $\mathscr{C}$ and $\mathscr{D}$ can be expressed as

$$\left.\begin{aligned} \mathscr{C} &\cong \left(\bigoplus_{\alpha=1}^{r_0} \mathscr{C}_\alpha\right) \oplus \left(\bigoplus_{\beta=r_0+1}^{r_1} [\mathscr{C}_\beta \oplus \mathscr{C}'_\beta]\right) \oplus \left(\bigoplus_{\gamma=r_1+1}^{r'} \mathscr{C}_\gamma\right) \\ \mathscr{D} &\cong \left(\bigoplus_{\alpha=1}^{r_0} \mathscr{D}_\alpha\right) \oplus \left(\bigoplus_{\beta=r_0+1}^{r_1} [\mathscr{D}_\beta \oplus \mathscr{D}'_\beta]\right) \oplus \left(\bigoplus_{\gamma=r_1+1}^{r'} \mathscr{D}_\gamma\right) \end{aligned}\right\} \tag{3.1}$$

We prove the following theorem.

Theorem 3.1. *The pair $(\mathscr{C}, \mathscr{D})$ is an LCP in M if and only if $(\mathscr{C}_\alpha, \mathscr{D}_\alpha)$ is LCP in N_α for $1 \le \alpha \le r_0$, $(\mathscr{C}_\beta, \mathscr{D}_\beta)$ and $(\mathscr{C}'_\beta, \mathscr{D}'_\beta)$ are LCP in N_β and N'_β respectively for $r_0 + 1 \le \beta \le r_1$ and $(\mathscr{C}_\gamma, \mathscr{D}_\gamma)$ is LCP in N_γ for $r_1 + 1 \le \gamma \le r'$.*

Proof. Assume that $(\mathscr{C}, \mathscr{D})$ is LCP in M. Therefore $M = \mathscr{C} \oplus \mathscr{D}$. From (2.2) and (3.1) we have

$$\phi(\mathscr{C}) \oplus \phi(\mathscr{D}) = \left(\bigoplus_{\alpha=1}^{r_0} N_\alpha\right) \oplus \left(\bigoplus_{\beta=r_0+1}^{r_1} [N_\beta \oplus N'_\beta]\right) \oplus \left(\bigoplus_{\gamma=r_1+1}^{r'} N_\gamma\right). \tag{3.2}$$

Therefore, for $1 \le \alpha \le r_0$, $r_0 + 1 \le \beta \le r_1$ and $r_1 + 1 \le \gamma \le r'$, we have

$$\mathscr{C}_\alpha + \mathscr{D}_\alpha \subseteq N_\alpha,\ \mathscr{C}_\beta + \mathscr{D}_\beta \subseteq N_\beta,\ \mathscr{C}'_\beta + \mathscr{D}'_\beta \subseteq N'_\beta \text{ and } \mathscr{C}_\gamma + \mathscr{D}_\gamma \subseteq N_\gamma$$

By (3.2) and since $N_\alpha, N_\beta, N'_\beta$ and N_γ are finite dimensional vector spaces over their corresponding fields, we have

$$\mathscr{C}_\alpha + \mathscr{D}_\alpha = N_\alpha,\ \mathscr{C}_\beta + \mathscr{D}_\beta = N_\beta,\ \mathscr{C}'_\beta + \mathscr{D}'_\beta = N'_\beta \text{ and } \mathscr{C}_\gamma + \mathscr{D}_\gamma = N_\gamma.$$

Then,

$$\dim N_\alpha = \dim(\mathscr{C}_\alpha + \mathscr{D}_\alpha) = \dim \mathscr{C}_\alpha + \dim \mathscr{D}_\alpha - \dim(\mathscr{C}_\alpha \cap \mathscr{D}_\alpha).$$

Therefore, for each α, $\dim \mathscr{C}_\alpha + \dim \mathscr{D}_\alpha$ is greater than or equal to $\dim N_\alpha$. Similarly, it follows for the addition of dimensions of every constituent pair in β and γ. Since $(\mathscr{C}, \mathscr{D})$ is LCP, we have

$$\begin{aligned} n = &\sum_{\alpha=1}^{r_0} \deg f_\alpha (\dim \mathscr{C}_\alpha + \dim \mathscr{D}_\alpha) + \sum_{\beta=r_0+1}^{r_1} \deg f_\beta [(\dim \mathscr{C}_\beta + \dim \mathscr{D}_\beta) \\ &+ (\dim \mathscr{C}'_\beta + \dim \mathscr{D}'_\beta)] + \sum_{\gamma=r_1+1}^{r'} \deg f_\gamma (\dim \mathscr{C}_\gamma + \dim \mathscr{D}_\gamma). \end{aligned}$$

By (2.2), it follows that

$$n = \sum_{\alpha=1}^{r_0} \deg f_\alpha \dim N_\alpha + \sum_{\beta=r_0+1}^{r_1} \deg f_\beta (\dim N_\beta + \dim N'_\beta) + \sum_{\gamma=r_1+1}^{r'} \deg f_\gamma \dim N_\gamma.$$

Hence for each α,

$$\dim \mathscr{C}_\alpha + \dim \mathscr{D}_\alpha = \dim N_\alpha$$

and similarly, it follows for the addition of dimensions of every constituent pair in β and γ.

Therefore, $(\mathscr{C}_\alpha, \mathscr{D}_\alpha)$ is LCP in N_α for $1 \le \alpha \le r_0$, $(\mathscr{C}_\beta, \mathscr{D}_\beta)$ and $(\mathscr{C}'_\beta, \mathscr{D}'_\beta)$ are LCP in N_β and N'_β respectively for $r_0+1 \le \beta \le r_1$ and $(\mathscr{C}_\gamma, \mathscr{D}_\gamma)$ is LCP in N_γ for $r_1+1 \le \gamma \le r'$.

To prove the converse, we can follow similar arguments and conclude that $(\mathscr{C}, \mathscr{D})$ is LCP in M. □

A multi-twisted code $\mathscr{C}$ of length n over $\mathbb{F}_q$ is said to be a k-generator code if k is the least positive integer such that there exists k number of codewords in $\mathscr{C}$ say, $a_1(x), a_2(x) \ldots, a_k(x)$ with the property that every $c(x) \in \mathscr{C}$ can be expressed as $c(x) = g_1(x)a_1(x) + g_2(x)a_2(x) + \cdots + g_k(x)a_k(x)$ for some $g_1(x), g_2(x), \ldots g_k(x) \in \mathbb{F}_q[x]$ and we denote $\mathscr{C} = \langle a_1(x), a_2(x), \ldots, a_k(x)\rangle$ where $a_t(x) = (a_{t,1}(x), a_{t,2}(x), \ldots, a_{t,d}(x))$ for $1 \le t \le k$.

When $k = 1$, $\mathscr{C}$ is said to be a 1-generator multi-twisted code. Let $\mathscr{C} = \langle a(x)\rangle$ be a 1-generator multi-twisted code where $a(x) = (a_1(x), a_2(x) \ldots, a_d(x))$. By (2.1) we have $M \cong \bigoplus_{j=1}^{r} \left(\prod_{i=1}^{d} l_{ji} F_j \right)$ and $F_j \cong \mathbb{F}_q(\zeta_j)$, where ζ_j is a root of $f_j(x)$ for $1 \le j \le r$. Thus we have an isomorphism from M to $\bigoplus_{j=1}^{r} \left(\prod_{i=1}^{d} l_{ji} \mathbb{F}_q(\zeta_j) \right)$ given by $(a_1(x), a_2(x), \ldots, a_d(x)) \mapsto \sum_{j=1}^{r} (l_{j1}a_1(\zeta_j), l_{j2}a_2(\zeta_j), \ldots, l_{jd}a_d(\zeta_j))$. Therefore, for a 1-generator multi-twisted code $\mathscr{C} = \langle (a_1(x), a_2(x), \ldots, a_d(x))\rangle$ its constituents are of the form $\mathscr{C}_j = \langle (l_{j1}a_1(\zeta_j), l_{j2}a_2(\zeta_j), \ldots, l_{jd}a_d(\zeta_j))\rangle$ for $1 \le j \le r$.

Let $\mu_1, \mu_2, \ldots, \mu_d \in \mathbb{F}_q^*$ and $\{f_1, f_2, \ldots, f_r\}$ be the collection of all irreducible factors of $x^{m_i} - \mu_i$, $1 \le i \le d$. Now consider that each irreducible factor divides $x^{m_i} - \mu_i$ for exactly two distinct i's, in that case we prove the following for 1-generator multi-twisted codes.

Theorem 3.2. *Let $\mu_1, \mu_2, \ldots, \mu_d$ be such that for each $1 \le j \le r$, $f_j(x)$ divides $x^{m_i} - \mu_i$ for exactly two distinct i's, say u, v. Suppose $\mathscr{C} = \langle (a_1(x), a_2(x), \ldots, a_d(x))\rangle$ and $\mathscr{D} = \langle (b_1(x), b_2(x), \ldots, b_d(x))\rangle$ are 1-generator multi-twisted codes of length n. Then the pair $(\mathscr{C}, \mathscr{D})$ is LCP if and only if for every $j, 1 \le j \le r$ and any $s \in F_j^*$, we have*

$$\gcd(f_j(x), a_i(x) - s b_i(x)) = 1, \quad \text{for } i = u, v.$$

Proof. Let $\mathscr{C} = \langle (a_1(x), a_2(x), \ldots, a_d(x))\rangle$ and $\mathscr{D} = \langle (b_1(x), b_2(x), \ldots, b_d(x))\rangle$ be 1-generator multi-twisted codes. Here all the constituents $\mathscr{C}_j$ and $\mathscr{D}_j$ of $\mathscr{C}$ and $\mathscr{D}$ respectively are 1-dimensional subspaces of 2-dimensional space N_j over F_j. Therefore, to prove that the pair $(\mathscr{C}, \mathscr{D})$ is LCP, it is enough to show that $\mathscr{C}_j \cap \mathscr{D}_j = \{0\}$ for $1 \le j \le r$. Since $f_j(x)$ divides $x^{m_i} - \mu_i$ for exactly two distinct i's, say u, v, we have $l_{ji} = 1$ if $i = u, v$ and $l_{ji} = 0$ otherwise. Therefore, we have $\mathscr{C}_j = \langle (0, \ldots, a_u(\zeta_j), \ldots, a_v(\zeta_j), \ldots, 0)\rangle$ and $\mathscr{D}_j = \langle (0, \ldots, b_u(\zeta_j), \ldots, b_v(\zeta_j), \ldots, 0)\rangle$, where ζ_j is a root of $f_j(x)$. Then $\mathscr{C}_j \cap \mathscr{D}_j \ne \{0\}$ if and only if there exists $s \in F_j^*$ such that $f_j(x)$ divides $a_i(x) - s b_i(x)$, for $i = u, v$. Therefore, $\mathscr{C}_j \cap \mathscr{D}_j = \{0\}$ if and only if for any $s \in F_j^*$,

$$\gcd(f_j(x), a_i(x) - s b_i(x)) = 1, \quad \text{for } i = u, v.$$

Hence $(\mathscr{C}, \mathscr{D})$ is LCP if and only if for every j, $1 \le j \le r$ and any $s \in F_j^*$ we have

$$\gcd(f_j(x), a_i(x) - s b_i(x)) = 1, \quad \text{for } i = u, v.$$ □

Corollary 3.1. *Let $\mu_1,\mu_2,\ldots,\mu_d \in \mathbb{F}_q^*$ be such that $x^{m_1}-\mu_1, x^{m_2}-\mu_2,\ldots,x^{m_{d-1}}-\mu_{d-1}$ are pairwise coprime polynomials in $\mathbb{F}_q[x]$ and $x^{m_d}-\mu_d = \prod_{i=1}^{d-1} x^{m_i}-\mu_i$. Let $\prod_{i=1}^{d-1} x^{m_i}-\mu_i = f_1(x)f_2(x)\ldots f_r(x)$, where f_i's are distinct irreducible polynomials. Suppose $\mathscr{C} = \langle (a_1(x),\ldots,a_{d-1}(x),1)\rangle$ and $\mathscr{D} = \langle (b_1(x),\ldots,b_{d-1}(x),1)\rangle$ are 1-generator multi-twisted codes of length n. Then the pair $(\mathscr{C},\mathscr{D})$ is LCP if and only if for every j, $1\le j\le r$ we have $\gcd(f_j(x),a_i(x)-b_i(x))=1$ for i such that $l_{ji}=1$.*

Proof. The constituents of $\mathscr{C}$ and $\mathscr{D}$ are of the form $\mathscr{C}_j = \langle (0,\ldots,a_i(\zeta_j),\ldots,1)\rangle$ and $\mathscr{D}_j = \langle (0,\ldots,b_i(\zeta_j),\ldots,1)\rangle$ for i such that $l_{ji}=1$, and ζ_j is a root of $f_j(x)$. Then, $\mathscr{C}_j\cap\mathscr{D}_j \neq \{0\}$ if and only if $f_j(x)$ divides $a_i(x)-b_i(x)$. Therefore, $\mathscr{C}_j\cap\mathscr{D}_j=\{0\}$ if and only if $\gcd(f_j(x),a_i(x)-b_i(x))=1$. Since $\mathscr{C}_j$ and $\mathscr{D}_j$ are 1-dimensional subspaces of the 2-dimensional space $N_j = \prod_{i=1}^{d} l_{ji}F_j$ for $1\le j\le r$, we have the pair $(\mathscr{C}_j,\mathscr{D}_j)$ is LCP if and only if $\mathscr{C}_j\cap\mathscr{D}_j=\{0\}$.

Hence, $(\mathscr{C},\mathscr{D})$ is LCP if and only if for every j, $1\le j\le r$ we have $\gcd(f_j(x),a_i(x)-b_i(x))=1$ for i such that $l_{ji}=1$. □

When $x^{m_1}-\mu_1, x^{m_2}-\mu_2,\ldots,x^{m_d}-\mu_d$ are pairwise coprime polynomials in $\mathbb{F}_q[x]$, we have

$$M = \prod_{i=1}^{d} M_i = \prod_{i=1}^{d} \frac{\mathbb{F}_q[x]}{\langle x^{m_i}-\mu_i\rangle} = \frac{\mathbb{F}_q[x]}{\left\langle \prod_{i=1}^{d} x^{m_i}-\mu_i \right\rangle}.$$

Clearly, M is a ring and any multi-twisted code can be considered as an ideal of M. Since M is a principle ideal ring, the multi-twisted codes are generated by monic polynomials. Then we have the following theorem.

Theorem 3.3. *Let $\mu_1,\mu_2,\ldots,\mu_d \in \mathbb{F}_q^*$ be such that $x^{m_1}-\mu_1, x^{m_2}-\mu_2,\ldots,x^{m_d}-\mu_d$ are pairwise coprime polynomials in $\mathbb{F}_q[x]$. Let $\mathscr{C}$ and $\mathscr{D}$ be multi-twisted codes of M over $\mathbb{F}_q$ generated by monic polynomials $a(x)$ and $b(x)$, respectively. Then the pair $(\mathscr{C},\mathscr{D})$ is LCP in M if and only if $a(x)b(x) = \prod_{i=1}^{d} x^{m_i}-\mu_i$.*

Proof. By our assumption, $\{x^{m_i}-\mu_i \mid 1\le i\le d\}$ are pairwise coprime polynomials in $\mathbb{F}_q[x]$. First, let us assume that the pair $(\mathscr{C},\mathscr{D})$ is LCP. Then $\mathscr{C}\oplus\mathscr{D} \cong \mathbb{F}_q^n \cong \frac{\mathbb{F}_q[x]}{\left\langle \prod_{i=1}^{d} x^{m_i}-\mu_i \right\rangle}$ and $\gcd(a(x),b(x))=1$. Since $\mathscr{C}\cap\mathscr{D}$ has the generating polynomial $\operatorname{lcm}(a(x),b(x))$ and $\mathscr{C}\cap\mathscr{D}=\{0\}$, we get $\operatorname{lcm}(a(x),b(x)) = \prod_{i=1}^{d} x^{m_i}-\mu_i$. As $\gcd(a(x),b(x))=1$, we have $a(x)b(x) = \prod_{i=1}^{d} x^{m_i}-\mu_i$.

Conversely, suppose $a(x)b(x) = \prod_{i=1}^{d} x^{m_i}-\mu_i$. Since $(m_i,q)=1$ for $1\le i\le d$, the irreducible factors of the polynomials $x^{m_i}-\mu_i$ are distinct. Therefore, $\gcd(a(x),b(x)) = 1$. Then $\operatorname{lcm}(a(x),b(x)) = \prod_{i=1}^{d} x^{m_i}-\mu_i$ which implies that $\mathscr{C}\cap\mathscr{D}=\{0\}$. Now, $\gcd(a(x),b(x))=1$ implies that $\mathscr{C}+\mathscr{D} = \frac{\mathbb{F}_q[x]}{\prod_{i=1}^{d} x^{m_i}-\mu_i}$. Hence, the pair $(\mathscr{C},\mathscr{D})$ is LCP in M. □

4. Conclusion

In this paper we obtained characterisations of linear complementary pairs of multi-twisted codes using their constituents and generator polynomial. The characterisation obtained via their constituents extends the characterisation of LCP of quasi-cyclic codes due to Carlet *et al*. [3]. Further it will be interesting to obtain characterisations for the linear complementary dual of skew multi-twisted codes, which are generalisations of multi-twisted codes.

Competing Interests

The authors declare that they have no competing interests.

Authors' Contributions

All the authors contributed significantly in writing this article. The authors read and approved the final manuscript.

References

[1] N. Aydin and A. Halilović, A generalization of quasi-twisted codes: Multi-twisted codes, *Finite Fields and Their Applications* **45** (2017), 96 – 106, DOI: 10.1016/j.ffa.2016.12.002.

[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 2014: Information Security Theory and Practice. Securing the Internet of Things*, Springer, Heraklion, pp. 40 – 56, 2014, DOI: 10.1007/978-3-662-43826-8_4.

[3] C. Carlet, C. Güneri, F. Özbudak, B. Özkaya and P. Solé, On linear complementary pairs of codes, *IEEE Transactions on Information Theory* **64**(10) (2018), 6583 – 6589, DOI: 10.1109/tit.2018.2796125.

[4] S. Lang, *Algebra*, revised third edition, Springer-Verlag New York (2002), DOI: 10.1007/978-1-4613-0041-0.

[5] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd edition, Cambridge University Press (2009), DOI: 10.1017/CBO9780511525926.

[6] J.L. Massey, Linear codes with complementary duals, *Discrete Mathematics* **106/107** (1992), 337 – 342, DOI: 10.1016/0012-365x(92)90563-u.

[7] X.T. Ngo, S. Bhasin, J.-L. Danger, S. Guilley and Z. Najm, Linear complementary dual code improvement to strengthen encoded circuit against hardware Trojan horses, *2015 IEEE International Symposium on Hardware Oriented Security and Trust* (HOST), May 5-7, 2015, pp. 82 – 87, DOI: 10.1109/hst.2015.7140242.

[8] E. Prange, Cyclic error correcting codes in two symbols, Air Force Cambridge Research Center (1957), p. 103.

[9] A. Sharma, V. Chauhan and H. Singh, Multi-twisted codes over finite fields and their dual codes, *Finite Fields and Their Applications* **51** (2018), 270 – 297, DOI: 10.1016/j.ffa.2018.01.012.

[10] X. Yang and J.L. Massey, The condition for a cyclic code to have a complementary dual, *Discrete Mathematics* **126** (1994), 391 – 393, DOI: 10.1016/0012-365x(94)90283-6.