J. Algebra Comb. Discrete Appl.
12(1) • 19–29

Received: 5 July 2024
Accepted: 13 October 2024

Journal of Algebra Combinatorics Discrete Structures and Applications

Mixed skew cyclic codes over rings

Research Article

Nabil Bennenni, Nasreddine Benbelkacem, Nuh Aydin, Peihan Liu

Abstract: This paper explores different types of skew cyclic codes by generating special subclasses with additional desirable properties. Specifically, we are interested in skew cyclic codes over mixed rings. We study some algebraic and structural properties of these codes and their constructions. We study skew cyclic codes over the mixed alphabet ring $\mathbb{F}_q(\mathbb{F}_q + v\mathbb{F}_q)$ under a mixed automorphism $(\theta, \tilde{\theta})$ and we give the structure of these codes for an arbitrary length via the non-commutative ring $\mathbb{F}_q[x,\theta](\mathbb{F}_q + v\mathbb{F}_q)[x,\tilde{\theta}]$. A condition for the existence of linear complementary dual (LCD) codes (which play an important role in practical applications such as armoring implementations against side-channel attacks and fault injection attacks) are explored specifically for skew cyclic codes.

2020 MSC: 94B05, 94B15, 16S36

Keywords: Skew cyclic codes, LCD skew cyclic codes, Computational results

1. Introduction

The algebraic theory of error-correcting codes has traditionally taken place over finite fields, especially the binary field. The theory of codes over finite rings was first developed in the early 1970s and study of codes over various finite rings has received a lot of attention in the last few decades. The study of codes over finite rings has significantly expanded the tools of coding theorists and yielded new useful results. Among other results, new ways of constructing some of the best known or optimal classical codes have been discovered, as well as quantum codes and DNA codes. For example, an optimal binary linear code was obtained from the Gray image of a constacyclic code over $\mathbb{F}_2 + u\mathbb{F}_2$ in [3]. In [8], new quantum codes with better parameters have been obtained from cyclic codes over the ring $\mathbb{Z}_2[u]\mathbb{Z}_2[u]/\langle u^4\rangle$. A method of constructing reversible codes over the ring $\mathbb{F}_2[u]/\langle u^{2k}-1\rangle$ for various values of k is given in [20].

Nabil Bennenni (Corresponding Author), Nasreddine Benbelkacem; Faculty of Mathematics, Department of Algebra, ATN Laboratory, University of Science and Technology Houari Boumediene, BP 32 El Alia, Bab Ezzouar, 1611 Algeries, Algeria (email: nabil.bennenni@gmail.com, nasreddine.benbelkacem@usthb.edu.dz).
Nuh Aydin; Department of Mathematics and Statistics, Kenyon College, Gambier, OH 43022, United States of America (email: aydinn@kenyon.edu).
Peihan Liu; John A. Paulson School Of Engineering and Applied Sciences, Harvard University, Cambridge, MA 02134, United States of America (email: peihanliu@fas.harvard.edu).

This allows us more freedom than the classical method of generating cyclic codes using self-reciprocal polynomials, and more freedom in constructing DNA codes. The era of intensive research on codes over rings started with the discovery in 1992 ([14]) and subsequent comprehensive development in 1994 ([18]) that some of the best binary nonlinear codes can be obtained as images of $\mathbb{Z}_4$-linear codes. Cyclic codes are one of the most important classes of codes in coding theory for both theoretical and practical reasons. Some of the best-known codes are cyclic or related to cyclic codes such as BCH codes, Reed-Solomon codes, Golay codes, many Hamming codes, quadratic residue codes and more. They also have many useful generalizations such as constacyclic codes, quasi-cyclic (QC) codes, and quasi-twisted (QT) codes. Hundreds of best-known linear have been obtained from these generalizations of cyclic codes. A more recent generalization of cyclic codes is skew (or theta) cyclic codes introduced in [10]. The algebraic structure of skew cyclic codes over a field $\mathbb{F}_q$ gives rise to the skew polynomial ring $\mathbb{F}_q[x,\theta]$, where θ is an automorphism of $\mathbb{F}_q$, which is a non-commutative ring. Factorizations of polynomials in a skew polynomial ring is not unique. For example, the polynomial x^n-1 has many different factorizations in $\mathbb{F}_q[x,\theta]$. Therefore, there are usually more skew cyclic codes of a given length over $\mathbb{F}_q$ than ordinary cyclic codes over $\mathbb{F}_q$ of the same length. This increases the possibility of obtaining new linear codes with better parameters from skew cyclic codes. Indeed, researchers have found new linear codes from skew cyclic codes [10], [5] and from skew quasi-cyclic codes [2]. Boucher *et al.* ([10]) constructed skew cyclic codes with the property that the order of automorphism divides the length of skew cyclic codes so that the left ideal (x^n-1) in $\mathbb{F}_q[x,\theta]$ generated by x^n-1 is a two-sided ideal. The same result was given by Abualrub et al. [1] over the ring $\mathbb{F}_2+v\mathbb{F}_2$. Siap et al [23] constructed skew cyclic codes without the requirement that the order of automorphism divides the length of skew cyclic code. In the general case, the left ideal (x^n-1) in $\mathbb{F}_q[x,\theta]$ generated by (x^n-1) is not necessarily a two-sided ideal and the set (the quotient space) $R_n=\mathbb{F}_q[x,\theta]/(x^n-1)$ is not ring but it is a left $\mathbb{F}_q[x,\theta]-$submodule.
The study of codes over mixed alphabet rings was introduced by Borger *et al.* in [9]. It has been shown that codes over mixed alphabets have some applications in stenography and data hiding [21]. In [4] Abualrub *et al.* give the structure of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes and their generators. In [7, 22], skew cyclic codes over various mixed alphabet rings are studied. In [7] it is shown that the skew cyclic codes over $\mathbb{F}_4R$ are left $R[x,\theta]$-submodules of $R_{\alpha,\beta}=\mathbb{F}_4[x]/(x^\alpha-1)\times R[x;\theta]/(x^\beta-1)$, where the order of the automorphism θ does not have to divide the length of the codes and their generators are determined. Similar results are given in [22]. In this paper, we study skew cyclic codes over a mixed alphabet ring using a mixed automorphism θ over a finite field $\mathbb{F}_q$ and an automorphism $\tilde{\theta}$ of the ring $\mathbb{F}_q+v\mathbb{F}_q$. This is different from the cases given in [4, 7, 9, 10, 22]. If $|\langle\theta\rangle|=m$ does not divide α and $|\langle\tilde{\theta}\rangle|=m$ does not divide β, then skew cyclic codes obtained are left $(\mathbb{F}_q+v\mathbb{F}_q)[x,\theta]$-submodules of $R_{\alpha,\beta}=(\mathbb{F}_q[x,\theta]/(x^\alpha-1))((\mathbb{F}_q+v\mathbb{F}_q)[x;\tilde{\theta}]/(x^\beta-1))$. If $|\langle\theta\rangle|\big|\alpha$ and if $|\langle\tilde{\theta}\rangle|\big|\beta$, then skew cyclic codes that are generated by the mixed ideal $((x^\alpha-1),(x^\beta-1))$ in the mixed ring $\mathbb{F}_q[x,\theta](\mathbb{F}_q+v\mathbb{F}_q)[x;\tilde{\theta}]$ are two-sided ideals of the ring $R_{\alpha,\beta}=(\mathbb{F}_q[x,\theta]/(x^\alpha-1))((\mathbb{F}_q+v\mathbb{F}_q)[x;\tilde{\theta}]/(x^\beta-1))$. We investigate a relationship between the mixed ring $\mathbb{F}_q[x,\theta](\mathbb{F}_q+v\mathbb{F}_q)[x;\tilde{\theta}]$ and the mixed ring $\mathbb{F}_q[x,\theta,\delta_a](\mathbb{F}_q+v\mathbb{F}_q)[x;\tilde{\theta},\tilde{\delta}_c]$, where δ_a is an additive map such that for any $b,b'\in\mathbb{F}_q$, $\delta_a(bb')=\theta(b)\delta_a(b')+\delta_a(b)b'$ and $\tilde{\delta}_c$ is an additive map such that for any $d,d'\in\mathbb{F}_q+v\mathbb{F}_q$, $\tilde{\delta}_c(dd')=\tilde{\theta}(d)\tilde{\delta}_c(d')+\tilde{\delta}_c(d)d'$. In construction codes over these rings, we potentially have more skew cyclic codes and hence greater chances to find new codes compared to the constructions given in [4, 7, 9, 10, 17, 22]. There are several motivations for studying codes over the mixed alphabet ring $\mathbb{F}_q(\mathbb{F}_q+v\mathbb{F}_q)$ with mixed automorphisms, including:

- The factorization of $(x^\alpha-1)$ and $(x^\beta-1)$ over $\mathbb{F}_q[x,\theta,\delta_a]$ and $(\mathbb{F}_q+v\mathbb{F}_q)[x;\tilde{\theta},\tilde{\delta}_c]$, respectively, is not unique and this leads to potentially more skew codes compared to ordinary cyclic codes.
- The existence of more skew cyclic codes increases the chances of finding new codes compared to the constructions given in the articles [4, 7, 9, 10, 22].

We also consider skew cyclic codes that are linear complementary dual (LCD), aiming to construct skew cyclic codes with an additional desirable property. We refer to such codes as LCD-codes. Self dual codes have been intensively studied in coding theory for many decades. Compared to self-dual codes, LCD codes have an opposite property in terms of the size of their hulls (the intersection of a code with its dual) and they have received much attention recently. Hence, it is natural to study LCD codes from a mathematical

point of view. Massey [19] first introduced them in 1992, the motivation being their application to the so-called two-user binary adder channel. Massey showed that the unique decodability problem for this scenario is overcome if one uses an LCD code. These codes have attracted a lot of attention since the discovery by Carlet and Guilley [12] in 2015 of their use in counter-measures against side-channel attacks (SCA) and fault injection attacks (FIA) in the context of direct sum masking (DSM). In this paper, we present a condition for the existence of LCD-codes.
The paper is organized as follows. In section 2, we present some basic facts about the ring $\mathbb{F}_q(\mathbb{F}_q + v\mathbb{F}_q)$ and introduce skew cyclic codes over this ring. In section 3, we study the algebraic structure of skew cyclic codes with an arbitrary length and determine their generators in $\mathbb{F}_q[x, \theta, \delta_a](\mathbb{F}_q + v\mathbb{F}_q)[x; \tilde{\theta}, \tilde{\delta}_c]$. In section 4 we study a necessary and sufficient condition for a skew cyclic code to be an LCD code over the ring $\mathbb{F}_q(\mathbb{F}_q + v\mathbb{F}_q)$. In section 5, we give examples of optimal and best-known linear codes obtained from skew polynomial rings with derivation over the fields $GF(4), GF(8)$ and $GF(9)$.

2. Preliminaries

Let $\mathbb{F}_q$ be the finite field with $q = p^m$ elements where p is a prime. We consider the noncommutative ring $\mathbb{F}_q[x, \theta, \delta_a] = \{a_\alpha x^\alpha + \cdots + a_1 x + a_0 : a_i \in \mathbb{F}_q\}$ where p is the characteristic of $\mathbb{F}_q$, the automorphism θ is a power of the Frobenius map $(z \to z^p)$, and $\delta_a(b) = a(\theta(b) - b)$ is a θ-derivation, where $a, b \in \mathbb{F}_q$, also called an inner derivation. The addition in this ring is the usual addition of polynomials. The multiplication is as given in [11] for a skew polynomial ring with derivation. It is defined iteratively starting with $x \cdot b = \theta(b)x + \delta_a(b)$, for all $b \in \mathbb{F}_q$. Then it is extended to all elements of $\mathbb{F}_q[x, \theta, \delta_a]$ recursively by associativity and distributivity.

The non-commutative ring $\mathbb{F}_q[x, \theta, \delta_a]$ is called a skew polynomial ring with derivation, and its elements are skew polynomials. It is a left and right Euclidean ring whose left and right ideals are principal. A skew cyclic code $\mathcal{C}$ over $\mathbb{F}_q$ is a linear code with the property that if $c = (c_0, c_1, \cdots, c_{\alpha-1}) \in \mathcal{C}$ then $(\theta(c_{\alpha-1}), \theta(c_0), \cdots, \theta(c_{\alpha-2})) \in \mathcal{C}$. The quotient space $R_\alpha = \mathbb{F}_q[x, \theta, \delta_a]/(x^\alpha - 1)$ is a ring if the ideal $(x^\alpha - 1)$ is a two-sided ideal which happens if $x^\alpha - 1$ is in the center of the ring $\mathbb{F}_q[x, \theta, \delta_a]$. For any $f(x) + (x^\alpha - 1) \in R_\alpha$ and $r(x) \in \mathbb{F}_q[x, \theta, \delta_a]$, one can define a multiplication $\star$ from the left as follows $r(x) \star (f(x) + (x^\alpha - 1)) = r(x)f(x) + (x^\alpha - 1)$. As usual, we consider the map

$$\xi : \mathbb{F}_q^\alpha \to \mathbb{F}_q[x, \theta, \delta_a]/(x^\alpha - 1)$$

$$(c_0, c_1, \cdots, c_{\alpha-1}) \to c_0 + c_1 x + c_2 x^2 + \cdots + c_{\alpha-1} x^{\alpha-1}$$

which is an $\mathbb{F}_q[x, \theta, \delta_a]$-module isomorphism, that enables us to identify vectors with polynomials.

We now consider the ring $\mathbb{F}_q + v\mathbb{F}_q = \{a + vb : a, b \in \mathbb{F}_q\}$ where $v = v^2$. This is a non-chain ring with q^2 elements. It is a semi local ring with maximal ideals $\langle v \rangle$ and $\langle 1 - v \rangle$ making $(\mathbb{F}_q + v\mathbb{F}_q)/\langle v \rangle$ and $(\mathbb{F}_q + v\mathbb{F}_q)/\langle 1 - v \rangle$ isomorphic to $\mathbb{F}_q$. A subset $\tilde{C}$ of $(\mathbb{F}_q + v\mathbb{F}_q)^\beta$ is a linear code over $\mathbb{F}_q + v\mathbb{F}_q$ if $\tilde{C}$ is an $(\mathbb{F}_q + v\mathbb{F}_q)$-submodule. Any linear code $\tilde{C}$ over $\mathbb{F}_q + v\mathbb{F}_q$ can be expressed as $\tilde{C} = vC_1 \bigoplus (1 - v)C_2$ where C_1 and C_2 are linear codes over $\mathbb{F}_q$. For more details on skew codes over $\mathbb{F}_q + v\mathbb{F}_q$ see [16].

Let an automorphism $\tilde{\theta}$ over $\mathbb{F}_q + v\mathbb{F}_q$ be defined by

$$\tilde{\theta} : \mathbb{F}_q + v\mathbb{F}_q \to \mathbb{F}_q + v\mathbb{F}_q$$

$$a + vb \to a^p + (1 + v)b^p$$

We define the skew polynomial ring $(\mathbb{F}_q + v\mathbb{F}_q)[x, \tilde{\theta}, \tilde{\delta}_c] = \{b_0 + b_1 x + \cdots + b_{n-1} x^{\beta-1} : b_i \in \mathbb{F}_q + v\mathbb{F}_q\}$ where $\tilde{\theta}$-derivation must be an inner derivation $\tilde{\delta}_c$ such that $\tilde{\delta}_c(d) = c(\tilde{\theta}(d) - d)$, where $c, d \in \mathbb{F}_q + v\mathbb{F}_q$. The multiplication is defined by $xd = \tilde{\theta}(d)x + \tilde{\delta}_c(d)$ and addition is defined to be the usual addition of polynomials. This ring is not commutative unless the automorphism $\tilde{\theta}$ is trivial. The ideal $(x^\beta - 1)$ of

$(\mathbb{F}_q+v\mathbb{F}_q)[x,\tilde{\theta},\tilde{\delta}_c]$ is a two sided ideal if and only if $|\langle\tilde{\theta}\rangle||\beta$, in which case the set $(\mathbb{F}_q+v\mathbb{F}_q)[x,\tilde{\theta},\tilde{\delta}_c]/(x^\beta-1)$ is a residue class ring. For an arbitrary β, $(\mathbb{F}_q+v\mathbb{F}_q)[x,\tilde{\theta},\tilde{\delta}_c]/(x^\beta-1)$ is a left $(\mathbb{F}_q+v\mathbb{F}_q)[x,\tilde{\theta},\tilde{\delta}_c]$ module with a multiplication defined by

$$r(x)(f(x)+(x^\beta-1))=r(x)f(x)+(x^\beta-1)$$

We define an $(\mathbb{F}_q+v\mathbb{F}_q)$-module isomorphism from $(\mathbb{F}_q+v\mathbb{F}_q)^\beta$ to $(\mathbb{F}_q+v\mathbb{F}_q)[x,\tilde{\theta},\tilde{\delta}_c]/(x^\beta-1)$ as

$$\tilde{\xi}:(\mathbb{F}_q+v\mathbb{F}_q)^\beta\to(\mathbb{F}_q+v\mathbb{F}_q)[x;\tilde{\theta},\tilde{\delta}_c]/(x^\beta-1)$$

$$(\tilde{c}_0,\tilde{c}_1,\cdots,\tilde{c}_{\beta-1})\to\tilde{c}_0+\tilde{c}_1x+\tilde{c}_2x^2+\cdots+\tilde{c}_{\beta-1}x^{\beta-1}.$$

Theorem 2.1. *([16, Theorem 5]) Let C_1 and C_2 be skew cyclic codes over $\mathbb{F}_q$ and g_1,g_2 be the monic generator polynomials of these codes respectively. Suppose that $C=(1-v)C_1\oplus vC_2$. Then there is a unique polynomial $g(x)\in(\mathbb{F}_q+v\mathbb{F}_q)[x;\theta_i]$ such that $C=\langle g(x)\rangle$ and $g(x)$ is a right divisor of x^n-1 where $g(x)=(1-v)g_1(x)+vg_2(x)$.*

Next, we extend the notion of skew cyclic codes over $\mathbb{F}_q[x,\theta,\delta_a]$ to the ring $(\mathbb{F}_q+v\mathbb{F}_q)[x,\tilde{\theta},\tilde{\delta}_c]$. We first define the ring $\mathbb{F}_q(\mathbb{F}_q+v\mathbb{F}_q)=\{(c,a+vb):a,b,c\in\mathbb{F}_q\}$. It is a commutative ring of characteristic p. The finite ring $\mathbb{F}_q(\mathbb{F}_q+v\mathbb{F}_q)$ is not a chain ring and it is not local because it has three maximal ideals $\langle(0,1)\rangle,\langle(1,v)\rangle$ and $\langle(1,1-v)\rangle$. We consider the natural homomorphism:

$$\Psi:(\mathbb{F}_q+v\mathbb{F}_q)\to\mathbb{F}_q$$

$$a+vb\to b.$$

It is straightforward to verify that the ring $\mathbb{F}_q(\mathbb{F}_q+v\mathbb{F}_q)$ is an $(\mathbb{F}_q+v\mathbb{F}_q)$-module under the multiplication

$$d*(a,b)=(\Psi(d)a,db)\text{ with }d\in(\mathbb{F}_q+v\mathbb{F}_q)\text{ and }(a,b)\in\mathbb{F}_q(\mathbb{F}_q+v\mathbb{F}_q).\tag{1}$$

This scalar multiplication extends naturally to $\mathbb{F}_q^\alpha(\mathbb{F}_q+v\mathbb{F}_q)^\beta$. Let $\mathbf{x}=(a_0,a_1,...,a_{\alpha-1},b_0,b_1,...,b_{\beta-1})\in\mathbb{F}_q^\alpha(\mathbb{F}_q+v\mathbb{F}_q)^\beta$, for α and $\beta\in\mathbb{N}$, and $d\in(\mathbb{F}_q+v\mathbb{F}_q)$. Then

$$d*\mathbf{x}=(\Psi(d)a_0,\Psi(d)a_1,...,\Psi(d)a_{\alpha-1},db_0,db_1,...,db_{\beta-1}).\tag{2}$$

Definition 2.2. *A nonempty subset C of $\mathbb{F}_q^\alpha(\mathbb{F}_q+v\mathbb{F}_q)^\beta$ is called an $\mathbb{F}_q(\mathbb{F}_q+v\mathbb{F}_q)$-linear code if it is an $(\mathbb{F}_q+v\mathbb{F}_q)$-submodule of $\mathbb{F}_q^\alpha(\mathbb{F}_q+v\mathbb{F}_q)^\beta$ with respect to the scalar multiplication in equation (2).*

An inner product of $\mathbf{x}=(a_0,a_1,\ldots,a_{\alpha-1},b_0,b_1,\ldots,b_{\beta-1})$ and $\mathbf{y}=(d_0,d_1,\ldots,d_{\alpha-1},e_0,e_1,...,e_{\beta-1})$ in $\mathbb{F}_q^\alpha(\mathbb{F}_q+v\mathbb{F}_q)^\beta$ is given by

$$\langle\mathbf{x},\mathbf{y}\rangle=(1-v)\sum_{i=0}^{\alpha-1}a_id_i+\sum_{j=0}^{\beta-1}b_je_j\in\mathbb{F}_q+v\mathbb{F}_q.\tag{3}$$

The dual code of an $\mathbb{F}_q(\mathbb{F}_q+v\mathbb{F}_q)$-linear code C, denoted by $C^\perp$, is also $\mathbb{F}_q(\mathbb{F}_q+v\mathbb{F}_q)$-linear and is defined in the usual way as

$$C^\perp:=\{\mathbf{y}\in\mathbb{F}_q^\alpha(\mathbb{F}_q+v\mathbb{F}_q)^\beta\mid\langle\mathbf{x},\mathbf{y}\rangle=0\text{ for all }\mathbf{x}\in C\}.$$

Let

$$f(x)=a_0+a_1x+\ldots+a_{\alpha-1}x^{\alpha-1}\in\mathbb{F}_q[x,\theta,\delta_a]/\langle x^\alpha-1\rangle\text{ and}$$
$$\tilde{f}(x)=b_0+b_1x+\ldots+b_{\beta-1}x^{\beta-1}\in(\mathbb{F}_q+v\mathbb{F}_q)[x,\tilde{\theta},\tilde{\delta}_c]/\langle x^\beta-1\rangle.$$

Then any codeword $\mathbf{x} = (a_0, a_1, ..., a_{\alpha-1}, b_0, b_1, ..., b_{\beta-1}) \in \mathbb{F}_q^{\alpha}(\mathbb{F}_q + v\mathbb{F}_q)^{\beta}$ can be identified with a module element consisting of two polynomials such that

$$c(x) = (f(x), \tilde{f}(x)). \tag{4}$$

This identification gives a one-to-one correspondence between $\mathbb{F}_q^{\alpha}(\mathbb{F}_q + v\mathbb{F}_q)^{\beta}$ and

$$R_{\alpha,\beta} := \mathbb{F}_q[x, \theta, \delta_a]/\langle x^{\alpha} - 1\rangle(\mathbb{F}_q + v\mathbb{F}_q)[x, \tilde{\theta}, \tilde{\delta}_c]/\langle x^{\beta} - 1\rangle. \tag{5}$$

The product of $r(x) = r_0 + r_1x + \ldots + r_tx^t \in (\mathbb{F}_q + v\mathbb{F}_q)[x, \tilde{\theta}, \tilde{\delta}_c]$ and $(f(x), \tilde{f}(x)) \in R_{\alpha,\beta}$ is

$$r(x) * (f(x), \tilde{f}(x)) = (\Psi(r(x))f(x), r(x)\tilde{f}(x)), \tag{6}$$

where $\Psi(r(x)) = \Psi(r_0) + \Psi(r_1)x + \ldots + \Psi(r_t)x^t \in \mathbb{F}_q[x, \theta]$. Here, $\Psi(r(x))f(x)$ is the polynomial multiplication in $\mathbb{F}_q[x, \theta]/\langle x^{\alpha} - 1\rangle$ while $r(x)\tilde{f}(x)$ is the polynomial multiplication in $(\mathbb{F}_q + v\mathbb{F}_q)[x, \tilde{\theta}, \tilde{\delta}_c]/\langle x^{\beta} - 1\rangle$ where $x(a + vb) = (a^p + (1 + v)b^p)\, x + \tilde{\delta}_c(a + vb)$.
We define a Gray map

$$\varphi : \mathbb{F}_q + v\mathbb{F}_q \to \mathbb{F}_q^2$$

$$a + vb \to (a, a + b)$$

As usual, the Hamming weight of a vector $\mathbf{x} \in \mathbb{F}_q^{\alpha}$ is the number of non-zero coordinates. The Lee weight on $(\mathbb{F}_q + v\mathbb{F}_q)$ is $w_L(a + vb) = w_H(a, a + b)$. The Lee distance $d_L(\mathbf{x}, \mathbf{y})$ between $\mathbf{x}$ and $\mathbf{y}$ is $w_L(\mathbf{x} - \mathbf{y})$ and the Hamming distance $d_H(\mathbf{x}, \mathbf{y})$ is $w_H(\mathbf{x} - \mathbf{y})$. The weight of $\mathbf{x} = (\mathbf{x}_{\alpha}, \tilde{\mathbf{x}}_{\beta})$ in $\mathbb{F}_q(\mathbb{F}_q + v\mathbb{F}_q)$ is defined to be $w(\mathbf{x}) = w_H(\mathbf{x}_{\alpha}) + w_L(\tilde{\mathbf{x}}_{\beta})$. The map φ can be extended to vectors $\mathbf{x} = (\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{\alpha-1}, \tilde{\mathbf{x}}_0, \tilde{\mathbf{x}}_1, \ldots, \tilde{\mathbf{x}}_{\beta-1}) \in \mathbb{F}_q^{\alpha} \times (\mathbb{F}_q + v\mathbb{F}_q)^{\beta}$. A Gray map is defined by

$$\varphi : \mathbb{F}_q^{\alpha}(\mathbb{F}_q + v\mathbb{F}_q)^{\beta} \to \mathbb{F}_q^{\alpha+2\beta}$$

$$(\mathbf{x}_{\alpha}, \tilde{\mathbf{x}}_{\beta}) \to (\mathbf{x}_{\alpha}, \varphi(\tilde{\mathbf{x}}_{\beta}))$$

3. Skew cyclic codes over the ring $\mathbb{F}_q(\mathbb{F}_q + v\mathbb{F}_q)$

In this section we study algebraic properties of skew cyclic codes over $\mathbb{F}_q(\mathbb{F}_q + v\mathbb{F}_q)$ which depend on the elements of finite field $\mathbb{F}_q$, the finite ring $(\mathbb{F}_q + v\mathbb{F}_q)$, and the pair of automorphisms $(\theta, \tilde{\theta})$ over $\mathbb{F}_q(\mathbb{F}_q + v\mathbb{F}_q)$ where

$$\Theta : \mathbb{F}_q(\mathbb{F}_q + v\mathbb{F}_q) \to \mathbb{F}_q(\mathbb{F}_q + v\mathbb{F}_q)$$

$$(c, a + vb) \to (c^p, a^p + (1 + v)b^p)$$

For any a vector $c = (c_0, c_1, \cdots, c_{\alpha-1}, \tilde{c_0}, \tilde{c_1}, \cdots, \tilde{c}_{\beta-1})$, we define its $\alpha\beta$-skew cyclic shift

$$\tau_{\alpha\beta} : \mathbb{F}_q^{\alpha}(\mathbb{F}_q + v\mathbb{F}_q)^{\beta} \to \mathbb{F}_q^{\alpha}(\mathbb{F}_q + v\mathbb{F}_q)^{\beta}$$

by

$$\tau_{\alpha\beta}(c) = (\theta(c_{\alpha-1}), \theta(c_1), \cdots, \theta(c_0), \tilde{\theta}(\tilde{c}_{\beta-1}), \tilde{\theta}(\tilde{c_1}), \cdots, \tilde{\theta}(\tilde{c_0}))$$

We investigate a relationship between the mixed ring $\mathbb{F}_q[x, \theta](\mathbb{F}_q + v\mathbb{F}_q)[x, \tilde{\theta}]$ and $\mathbb{F}_q[x, \theta, \delta_a](\mathbb{F}_q + v\mathbb{F}_q)[x, \tilde{\theta}, \tilde{\delta}_c]$ using the change of variables $z = x + a$ and $y = x + b$ to transform the ring $\mathbb{F}_q[x, \theta, \delta_a](\mathbb{F}_q + v\mathbb{F}_q)[x, \tilde{\theta}, \tilde{\delta}_c]$ into the pure-automorphism ring $\mathbb{F}_q[z, \theta](\mathbb{F}_q + v\mathbb{F}_q)[y, \tilde{\theta}]$. If $\delta_a = \tilde{\delta}_c = 0$, then these two rings become the same. For more details see [13]. In the following theorem we determine the centre $Z\left(\mathbb{F}_q[x, \theta](\mathbb{F}_q + v\mathbb{F}_q)[x, \tilde{\theta}]\right)$ of the mixed skew polynomial ring with $\delta_a = \tilde{\delta}_c = 0$.

Theorem 3.1. *The center $Z(\mathbb{F}_q[x,\theta](\mathbb{F}_q+v\mathbb{F}_q)[x,\tilde{\theta}])$ of $\mathbb{F}_q[x,\theta](\mathbb{F}_q+v\mathbb{F}_q)[x,\tilde{\theta}])$ is $(\mathbb{F}_q[x^m],\mathbb{F}_q+v\mathbb{F}_q[x^m])$ where m is the order of the mixed automorphism $(\theta,\tilde{\theta})$.*

Proof. Let m be the order of the mixed automorphism $(\theta,\tilde{\theta})$. For any element $a\in(\mathbb{F}_q+v\mathbb{F}_q)$, we have $(x^m,x^m)a=(x^m\psi(a),x^ma)=(\theta^m(\psi(a))x^m,\tilde{\theta}^m(a)x^m)=(\psi(a)x^m,ax^m)=a(x^m,x^m)$. Therefore, (x^m,x^m) is in the center $Z(\mathbb{F}_q[x,\theta](\mathbb{F}_q+v\mathbb{F}_q)[x,\tilde{\theta}])$ of $\mathbb{F}_q[x,\theta](\mathbb{F}_q+v\mathbb{F}_q)[x,\tilde{\theta}])$. Similarly, for any $f(x)=a_0+a_1x+\cdots a_\alpha x^\alpha,\tilde{f}(x)=\tilde{a}_0+\tilde{a}_1x+\cdots+\tilde{a}_\beta x^\beta$ is in the center where $(a_i,\tilde{a}_i)\in\mathbb{F}_q(\mathbb{F}_q+v\mathbb{F}_q)$.
Conversely, for any $(f,\tilde{f})\in Z(\mathbb{F}_q[x,\theta](\mathbb{F}_q+v\mathbb{F}_q)[x,\tilde{\theta}])$ and $a\in(\mathbb{F}_q+v\mathbb{F}_q)$, if $a(f,\tilde{f})=(f,\tilde{f})a$ and $x(f,\tilde{f})=(f,\tilde{f})x$. Then $(f,\tilde{f})\in(\mathbb{F}_q[x^m],\mathbb{F}_q+v\mathbb{F}_q[x^m])$. □

In the following theorem, we give a necessary and sufficient condition for $(x^\alpha-1,x^\beta-1)$ to be in $Z(\mathbb{F}_q[x,\theta](\mathbb{F}_q+v\mathbb{F}_q)[x,\tilde{\theta}])$, with $\delta_a=\tilde{\delta}_c=0$.

Theorem 3.2. *$(x^\alpha-1,x^\beta-1)\in Z(\mathbb{F}_q[x,\theta](\mathbb{F}_q+v\mathbb{F}_q)[x,\tilde{\theta}])$ if and only if $|\langle\theta\rangle|\big|\alpha$ and $|\langle\tilde{\theta}\rangle|\big|\beta$ where $Z(\mathbb{F}_q[x,\theta](\mathbb{F}_q+v\mathbb{F}_q)[x,\tilde{\theta}])$ is the centre of $\mathbb{F}_q[x,\theta](\mathbb{F}_q+v\mathbb{F}_q)[x,\tilde{\theta}])$.*

Proof. Let $f(x)=a_0+a_1x+\cdots+a_rx^r\in(\mathbb{F}_q+v\mathbb{F}_q)[x,\tilde{\theta}]$. Since $|\langle\theta\rangle|\big|\alpha$ and $|\langle\tilde{\theta}\rangle|\big|\beta$, we have

$$\begin{aligned}
(x^\alpha-1,x^\beta-1)f(x)=&((x^\alpha-1)\Psi(f(x)),(x^\beta-1)f(x))\\
=&(x^\alpha\Psi(a_0)+x^\alpha\Psi(a_1)x+\cdots+x^\alpha\Psi(a_r)x^r-f(x),x^\beta(a_0)+\\
&x^\beta(a_1)x+\cdots+x^\beta(a_r)x^r-f(x))\\
=&(\theta^\alpha(\Psi(a_0))x^\alpha+\theta^\alpha(\Psi(a_1))x^\alpha x+\cdots+\theta^\alpha(\Psi(a_r))x^\alpha x^r-f(x),\\
&\tilde{\theta}^\beta(a_0)x^\beta+\tilde{\theta}^\beta(a_1)x^\beta x+\cdots+\tilde{\theta}^\beta(a_r)x^\beta x^r-f(x))\\
=&(\Psi(a_0)x^\alpha+\Psi(a_1)x^\alpha x+\cdots+\Psi(a_r)x^\alpha x^r-f(x),a_0x^\beta+\\
&a_1x^\beta x+\cdots+a_rx^\beta x^r-f(x))\\
=&(\Psi(f(x))x^\alpha-f(x),f(x)x^\beta-f(x))\\
=&(\Psi(f(x))(x^\alpha-1),(f(x))(x^\beta-1))\\
=&f(x)(x^\alpha-1,x^\beta-1)
\end{aligned}$$

Hence, $(x^\alpha-1,x^\beta-1)\in Z(\mathbb{F}_q[x,\theta](\mathbb{F}_q+v\mathbb{F}_q)[x,\tilde{\theta}])$.
Conversely suppose that $(x^\alpha-1,x^\beta-1)\in Z(\mathbb{F}_q[x,\theta](\mathbb{F}_q+v\mathbb{F}_q)[x,\tilde{\theta}])$. Then we have $(x^\alpha-1,x^\beta-1)ax^m=ax^m(x^\alpha-1,x^\beta-1)$ where $a\in(\mathbb{F}_q+v\mathbb{F}_q)$. We have that

$$\begin{aligned}
(x^\alpha-1,x^\beta-1)ax^m&=((x^\alpha-1)\Psi(a)x^m,(x^\beta-1)ax^m)\\
&=(\theta^\alpha(\Psi(a))x^{\alpha+m}-\Psi(a)x^m,\tilde{\theta}^\beta(a)x^{\beta+m}-ax^m)
\end{aligned}$$

and

$$ax^m(x^\alpha-1,x^\beta-1)=(\Psi(a)x^m(x^\alpha-1),ax^m(x^\beta-1))=(\Psi(a)x^{m+\alpha}-\Psi(a)x^m,ax^{p+\beta}-ax^m).$$

It follows that $\theta^\alpha(a)=a$ for each $a\in\mathbb{F}_q$ and $\tilde{\theta}^\beta(a+bv)=a+bv$ for all $a+bv\in\mathbb{F}_q+v\mathbb{F}_q$, which implies $|\langle\theta\rangle|\big|\alpha$ and $|\langle\tilde{\theta}\rangle|\big|\beta$. □

From Theorem 3.1 and Theorem 3.2 we have that $R_{\alpha,\beta}:=\mathbb{F}_q[x,\theta]/\langle x^\alpha-1\rangle(\mathbb{F}_q+v\mathbb{F}_q)[x,\tilde{\theta}]/\langle x^\beta-1\rangle$ is a ring, therefore we have the following theorem.

Theorem 3.3. *Let $|\langle\theta\rangle|\big|\alpha$, $|\langle\tilde{\theta}\rangle|\big|\beta$ and let $(C,\tilde{C})$ be a skew cyclic code of length $\alpha+\beta$ over $R_{\alpha,\beta}$ where C and $\tilde{C}$ are skew cyclic codes over $\mathbb{F}_q[x,\theta]/\langle x^\alpha-1\rangle$ and $(\mathbb{F}_q+v\mathbb{F}_q)[x,\tilde{\theta}]/\langle x^\beta-1\rangle$, respectively. Then $(C,\tilde{C})$ is a left ideal of $R_{\alpha,\beta}:=\mathbb{F}_q[x,\theta]/\langle x^\alpha-1\rangle(\mathbb{F}_q+v\mathbb{F}_q)[x,\tilde{\theta}]/\langle x^\beta-1\rangle$.*

Proof. Since $(C, \tilde{C})$ is a linear code, $(C, \tilde{C})$ is an additive group. Let $(a(x), b(x)) \in (C, \tilde{C})$ where $a(x) = a_0 + a_1x + \cdots + a_{\alpha-1}x^{\alpha-1} \in C$ and $b(x) = b_0 + b_1x + \cdots + b_{\beta-1}x^{\beta-1} \in \tilde{C}$

$$\begin{aligned} x \star (a(x), b(x)) =& x \star (a_0 + a_1x + \cdots + a_{\alpha-1}x^{\alpha-1}, b_0 + b_1x + \cdots + b_{\beta-1}x^{\beta-1}) \\ =& (\theta(a_{\alpha-1}) + \theta(a_0)x + \cdots + \theta(a_{\alpha-2})x^{\alpha-1}, \tilde{\theta}(b_{\beta-1}) + \tilde{\theta}(b_0)x + \\ & \cdots + \tilde{\theta}(b_{\beta-2})x^{\beta-1}) \end{aligned}$$

Hence, $(C, \tilde{C})$ is a skew cyclic code, and $x \star (a(x), b(x)) \in (C; \tilde{C})$. Moreover, by linearity and iteration we have $r(x) \star (a(x), b(x)) \in (C, \tilde{C})$, for any $r(x) \in (\mathbb{F}_q + v\mathbb{F}_q)[x, \tilde{\theta}]/\langle x^\beta - 1\rangle$. Therefore, $(C, \tilde{C})$ is a left ideal of $R_{\alpha,\beta}$. □

Let C be an $\mathbb{F}_q^\alpha(\mathbb{F}_q + v\mathbb{F}_q)^\beta$-skew cyclic code. Let $\mathbf{0}$ denote the zero polynomial. The factorization of $(x^\alpha - 1)$ and $(x^\beta - 1)$ over $\mathbb{F}_q[x, \theta, \delta_a]$ and $(\mathbb{F}_q + v\mathbb{F}_q)[x, \tilde{\theta}, \tilde{\delta}_c]$ respectively are not unique. We use the change of variables $z = x + a$ and $y = x + b$ to transform the rings $\mathbb{F}_q[x, \theta, \delta_a], (\mathbb{F}_q + v\mathbb{F}_q)[x, \tilde{\theta}, \tilde{\delta}_c]$ into the pure-automorphism rings $\mathbb{F}_q[z, \theta], (\mathbb{F}_q + v\mathbb{F}_q)[y, \tilde{\theta}]$. We then obtain the factorizations of $(z^\alpha - 1)$ and $(y^\beta - 1)$ over the new rings and they are the same as the factorizations of $(x^\alpha - 1)$ and $(x^\beta - 1)$ over $\mathbb{F}_q[x, \theta, \delta_a]$ and $(\mathbb{F}_q + v\mathbb{F}_q)[x, \tilde{\theta}, \tilde{\delta}_c]$ respectively. For this correspondence, we define the ring homomorphism Ψ by:

$$\begin{aligned} \psi : \mathbb{F}_q[x, \theta, \delta_a](\mathbb{F}_q + v\mathbb{F}_q)[x, \tilde{\theta}, \tilde{\delta}_c] &\to \mathbb{F}_q[Z, \theta](\mathbb{F}_q + v\mathbb{F}_q)[Y, \tilde{\theta},] \\ \left(\sum a_i x^i, \sum b_i x^i\right) &\mapsto \left(\sum a_i (z-a)^i, \sum b_i (y-b^i)\right) \end{aligned}$$

The ring homomorphism ψ induces a map from a $(\theta, \tilde{\theta}, \delta_a, \tilde{\delta}_c)$- linear code over the ring $\mathbb{F}_q[x, \theta, \delta_a](\mathbb{F}_q + v\mathbb{F}_q)[x, \tilde{\theta}, \tilde{\delta}_c]$ to a $(\theta, \tilde{\theta})$-linear code over the ring $\mathbb{F}_q[z, \theta](\mathbb{F}_q + v\mathbb{F}_q)[y, \tilde{\theta}]$. From the result is given in [[7], Theorem 3.3] and the ring homomorphism ψ, we have the following corollary which classifies all $\mathbb{F}_q(\mathbb{F}_q + v\mathbb{F}_q)$-skew cyclic codes with mixed automorphism $(\theta, \tilde{\theta})$-derivation.

Corollary 3.4. *Let C be an $\mathbb{F}_q(\mathbb{F}_q + v\mathbb{F}_q)$-skew cyclic code generated by $C := \langle (f(x), \mathbf{0}), (\ell(x), g(x))\rangle$, where $\ell(x)$ is an element in $\mathbb{F}_q[x, \theta, \delta_a]/\langle x^\alpha - 1\rangle$, $f(x)$ and $g(x)$ are right divisors of $(x^\alpha - 1)$ and $(x^\beta - 1)$ over $\mathbb{F}_q[x, \theta, \tilde{\delta}_c]/(x^\alpha - 1)$ and $(\mathbb{F}_q + v\mathbb{F}_q)[x, \tilde{\theta}, \tilde{\delta}_c]/(x^\beta - 1)$, respectively. Then C is a skew cyclic code over $\mathbb{F}_q[z, \theta](\mathbb{F} + v\mathbb{F})[y, \tilde{\theta}]$ generated by $\langle (f(z), \mathbf{0}), (\ell(z), g(y))\rangle$ where $\ell(z)$ is an element in $\mathbb{F}_q[z, \theta]/\langle z^\alpha - 1\rangle$, $z = x + a$, $y = x + b$ and $f(z)$ and $g(y)$ are right divisors of $z^\alpha - 1$ and $y^\beta - 1$ over $\mathbb{F}_q[z, \theta]/(z^\alpha - 1)$ and $(\mathbb{F}_q + v\mathbb{F}_q)[y; \tilde{\theta}]/(y^\beta - 1)$, respectively.*

Example 3.5. *Let $C := \langle (f(x), \mathbf{0}), (\ell(x), g(x))\rangle$ be the skew cyclic code over $\mathbb{F}_4(\mathbb{F}_4 + v\mathbb{F}_4)$ of the length 18 where $f(x) = x^2 + wx + w$, $\ell(x) = 0$ in $\mathbb{F}_4[x, \theta, \delta_w]$ and $g(x) = x^3 + (v + w)x^2 + (v + w)x + 1$ in $(\mathbb{F}_4 + v\mathbb{F}_4)[x, \tilde{\theta}, \delta_v]$.*
By the ring homomorphism Ψ, we obtain $f(z) = z^2 + w^2z + w$, $\ell(z) = 0$ in $\mathbb{F}_4[z, \theta]$ and $g(y) = y^3 + (v + 1)y^2 + wy + w^2v + 1$ in $(\mathbb{F}_4 + v\mathbb{F}_4)[y, \tilde{\theta}]$ where $z = x + w$ and $y = x + v$. By Corollary 3.4 we get $\tilde{C} := \langle (f(z), \mathbf{0}), (\ell(z), g(y))\rangle$, a skew cyclic code over $\mathbb{F}_4[z, \theta](\mathbb{F}_4 + v\mathbb{F}_4)[x, \tilde{\theta}]$.

In the table below, we give a few examples of skew cyclic codes with their parameters (length n and minimum distance d) over the ring $\mathbb{F}_2(\mathbb{F}_2 + v\mathbb{F}_2)$.

4. LCD-skew cyclic codes

In this section we give the definition of a LCD-skew cyclic code and a necessary and sufficient condition for an skew cyclic code to be an LCD code over the ring $\mathbb{F}_q(\mathbb{F}_q + v\mathbb{F}_q)$.

Definition 4.1. *A linear code over the ring $\mathbb{F}_q(\mathbb{F}_q + v\mathbb{F}_q)$ is LCD if $C \cap C^\perp = \{0\}$.*

Table 1. Construction of skew cyclic codes with the mixed automorphism over $\mathbb{F}_2(\mathbb{F}_2 + v\mathbb{F}_2)$ obtained by Corollary 3.4.

The code $\mathcal{C}$	n	d
$\langle(x^3+x^2+1,0),(0,x^4+(v+1)x^3+x^2+vx+1)\rangle$	15	7
$\langle(x^3+x+1,0),(0,x^5+1)\rangle$	17	5
$\langle(x^4+x^3+1,0),(0,x^7+x^6+x^5+x^4+x+1)\rangle$	29	7
$\langle(x^4+x+1,0),(0,x^{12}+x^{11}+x^9+(1+v)x^7+vx^5+x^3+(1+v)x^2+x+1)\rangle$	39	11

In the following theorem, we generalize the result from [6, Lemma 3] to $\mathbb{F}_q(\mathbb{F}_q + v\mathbb{F}_q)$ and the condition for the existence of the LCD skew cyclic codes over the rings $\mathbb{F}_q(\mathbb{F}_q + v\mathbb{F}_q)$.

Theorem 4.2. *Let C be a skew cyclic code over $\mathbb{F}_q(\mathbb{F}_q + v\mathbb{F}_q)$ of length $n = \alpha + \beta$. Then we have*

(i) $\varphi(C) = C_1 \otimes C_2 \otimes C_3$ is a skew cyclic code over $\mathbb{F}_q$ of length $\alpha + 2\beta$ where C_1 and (C_2, C_3) are skew cyclic codes over $\mathbb{F}_q$ of lengths α and 2β respectively.

(ii) $\varphi(C^\perp) = \varphi(C)^\perp$. Moreover $\varphi(C^\perp) = C_1^\perp \otimes C_2^\perp \otimes C_3^\perp$.

(iii) $\varphi(C)$ is an LCD skew cyclic code if and only if C_1, C_2 and C_3 are LCD skew cyclic codes over $\mathbb{F}_q$.

Proof. (i) Let C be a skew cyclic code over $\mathbb{F}_q(\mathbb{F}_q + v\mathbb{F}_q)$ of length $n = \alpha + \beta$. Any codeword of C can be written as $c = (c_0, c_1, \ldots, c_{\alpha-1}, a_0 + vb_0, a_1 + vb_1, \ldots, a_{\beta-1} + vb_{\beta-1})$. Applying θ, we have

$$\theta(c) = (c_{\alpha-1}^p, c_0^p, \ldots, c_{\alpha-2}^p, a_{\beta-1}^p + (1-v)b_{\beta-1}^p, a_0^p + (1-v)b_0^p, \ldots, a_{\beta-2}^p + (1-v)b_{\beta-2}^p) \in C.$$

Next, applying the Gray map φ, we have $\varphi(\theta(c)) = (c_{\alpha-1}, c_1, \ldots, c_0, \varphi(a_{\beta-1} + vb_{\beta-1}, a_1 + vb_1, \ldots, a_0 + vb_0) = (c_{\alpha-1}, c_1, \ldots, c_0, a_{\beta-1}, a_1 \ldots a_0, b_{\beta-1}, b_1, \ldots b_0) \in C_1 \otimes C_2 \otimes C_3$.

(ii) $\varphi(C^\perp) = \varphi(C)^\perp$ is a generalisation of the result given in [6, Lemma 3] over $\mathbb{F}_q(\mathbb{F}_q + v\mathbb{F}_q)$ and we get $\varphi(C^\perp) = \varphi(C)^\perp$. Moreover $\varphi(C^\perp) = (C_1 \otimes C_2 \otimes C_3)^\perp = C_1^\perp \otimes C_2^\perp \otimes C_3^\perp$.

(iii) Let $\varphi(C) = C_1 \otimes C_2 \otimes C_3$ be a skew cyclic code of length $\alpha + 2\beta$ over $\mathbb{F}_q$. By (ii) we have that $\varphi(C^\perp) = C_1^\perp \otimes C_2^\perp \otimes C_3^\perp$. By the definition of direct product, we have $\varphi(C \cup C^\perp) = (C_1 \cup C_1^\perp) \otimes (C_2 \cup C_2^\perp) \otimes (C_3 \cup C_3^\perp)$. $\varphi(C) \cap \varphi(C)^\perp = \{0\}$. Therefore $\varphi(C)$ is an LCD skew cyclic code.

□

5. Computational Results

In this section, we present examples of good linear codes obtained from skew polynomial rings with derivation over the fields $GF(4), GF(8)$ and $GF(9)$. These codes are either optimal or have the same parameters as best known linear codes available in the database [15]. These codes are principally generated in the form $C = \langle g(x)\rangle$ where $g(x)$ divides $x^n - 1$ in $\mathbb{F}_q[x, \theta, \delta_a]$.

Table 2. Examples of best known and optimal linear codes over $GF(4)$ where z below denotes a root of $x^2+x+1 \in \mathbb{F}_4[x]$

$[n,k,d]$	$\theta(x)$	$g(x)$	derivation's a
$[6,2,4]_4$	$\theta(x)=x^2$	$x^4+zx^3+zx^2+z^2x$	z^2
$[7,3,4]_4$	$\theta(x)=x^2$	$x^4+x^2+z^2x+z^2$	z
$[14,11,3]_4$	$\theta(x)=x^2$	x^3+zx^2+zx+z	1
$[18,14,3]_4$	$\theta(x)=x^2$	x^4+zx^3+x+z	z
$[21,18,3]_4$	$\theta(x)=x^2$	$x^3+z^2x^2+z^2x+z^2$	z^2

Table 3. Examples of best known and optimal linear codes $GF(8)$ where z below denotes a root of $x^3+x+1 \in \mathbb{F}_2[x]$

$[n,k,d]$	$\theta(x)$	$g(x)$	derivation's a
$[6,3,4]_8$	$\theta(x)=x^4$	$x^3+z^5x^2+z^6x+z^5$	z
$[10,6,4]_8$	$\theta(x)=x^4$	$x^4+zx^3+z^6x^2+z^6$	z^3
$[10,5,5]_8$	$\theta(x)=x^4$	$x^5+z^6x^4+z^6x^3+z^6x^2+z^6x+z^2$	z^4
$[12,8,4]_8$	$\theta(x)=x^4$	$x^4+az^2x^3+z^4x^2+z^5x+z$	z
$[16,12,4]_8$	$\theta(x)=x^4$	$x^4+x^3+z^4x+z^4$	z^2
$[10,4,6]_8$	$\theta(x)=x^2$	$x^6+z^2x^5+zx^4+z^4x^3+x^2+z^4x+z^6$	z^6
$[20,14,5]_8$	$\theta(x)=x^2$	$x^9+z^6z^8+x^7+x^6+z^6x^4+zx^3+z^2x^2+z^2x+z^3$	z^3
$[20,11,7]_8$	$\theta(x)=x^2$	$x^6+z^4x^5+zx^4+z^6x^3+z^5x^2+zx+z^2$	z^3

Table 4. Examples of best known and optimal linear codes $GF(9)$ where z below denotes a root of $x^2+x+2 \in \mathbb{F}_3[x]$

$[n,k,d]$	$\theta(x)$	$g(x)$	derivation's a
$[13,9,4]_9$	$\theta(x)=x^3$	$x^4+z^2x^3+z^5x^2+2x+z^3$	z
$[18,12,5]_9$	$\theta(x)=x^3$	$x^6+z^2x^4+z^3x^3+z^6x^2+z^2x+z^3$	z^2
$[22,17,4]_9$	$\theta(x)=x^3$	$x^5+zx^4+z^7x^3+z^7x^2+2x+2$	z^2
$[24,16,6]_9$	$\theta(x)=x^3$	$x^8+z^2x^7+z^7x^6+2x^5+z^3x^4+z^2x^3+z^3x^2+zx+z$	z^3
$[24,19,4]_9$	$\theta(x)=x^3$	$x^5+z^5x^4+z^2x^3+z^7x^2+zx+z$	z^6

6. Conclusion

In this paper, we presented our study on mixed skew cyclic codes over rings . We investigated the structural and algebraic properties of these codes, highlighting their potential for practical applications, particularly in strengthening the defense against cryptographic attacks such as side-channel and fault injection attacks. Additionally, we demonstrated that under a mixed automorphism, a condition for the existence of linear complementary dual (LCD) codes can be specifically developed for skew cyclic codes, further enhancing their utility in secure communication systems.

References

[1] T. Abualrub, N. Aydin, P. Seneviratne, On θ-cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$, The Australasian Journal of Combinatorics 54 (2012) 115–126.
[2] T. Abualrub, A. Ghrayeb, N. Aydin, I. Siap, On the construction of skew quasi-cyclic codes, IEEE Transactions on Information Theory 56(5) (2010) 2081–2090.
[3] T. Abualrub, I. Siap, Constacyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$, Journal of the Franklin Institute 346(5) (2009) 520–529.
[4] T. Abualrub, I. Siap, N. Aydin, $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes, IEEE Transactions on Information Theory 60(3) (2014) 1508–1514.
[5] N. Aydin, Some new linear codes from skew cyclic codes and computer algebra challenges, Applicable Algebra in Engineering, Communication and Computing 30(3) (2019) 1855–191.
[6] N. Benbelkacem, M. F. Ezerman, T. Abualrub, Linear codes over $\mathbb{F}_4R$ and their MacWilliams identity, Discrete Mathematics, Algorithms and Applications 12(06) (2020) 2050085.
[7] N. Benbelkacem, M. F. Ezerman, T. Abualrub, A. Batoul, Skew cyclic codes over $\mathbb{F}_4R$, Journal of Algebra and Its Applications 21(4) (2022) 2250065.
[8] S. Biswas, M. Bhaintwal, Quantum codes from $\mathbb{Z}_2\mathbb{Z}_2[u]/\langle u^4\rangle$-cyclic codes, Designs, Codes and Cryptography 90(2) (2022) 343–366.
[9] J. Borges, C. Fernandez-Cordoba, R. Ten-Valls, On $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic codes, Advances in Mathematics of Communications 12(1) (2018) 169-179.
[10] D. Boucher, W. Geiselmann, F. Ulmer, Skew-cyclic codes, Applicable Algebra in Engineering, Communication and Computing 18(4) (2007) 379–389.
[11] D. Boucher, F. Ulmer, Linear codes using skew polynomials with automorphisms and derivations, Designs, Codes and Cryptography 70(3) (2014) 405–431.
[12] C. Carlet, S. Guilley, Complementary dual codes for counter-measures to side-channel attacks, Advances in Mathematics of Communications 10(1) (2016) 131–150.
[13] P. Cohn, Free rings and their relations, Bulletin of the American Mathematical Society 21(1) (1989) 139–142.
[14] G. D. Forney Jr, N. J. Sloane, M. D. Trott, The Nordstrom-Robinson code is the binary image of the octacode, In Coding and Quantization, DIMACS/IEEE workshop, American Mathematical Society (1993) 19–26.
[15] M. Grassl, Code tables, Bounds on the parameters of codes.
[16] F. Gursoy, I. Siap, B. Yildiz, Construction of skew cyclic codes over $\mathbb{F}_q + v\mathbb{F}_q$, Advances in Mathematics of Communications 8(3) (2014) 313–322.
[17] F Gursoy, I. Aydogdu, On $\mathbb{Z}_2\mathbb{Z}_4[\xi]$-skew cyclic codes, Journal of Applied Mathematics and Computing 68 (2022) 1613–1633
[18] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. Sloane, P. Solé, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes, IEEE Transactions on Information Theory 40(2) (1994) 301–319.
[19] J. L. Massey, Linear codes with complementary duals, Discrete Mathematics 106–107 (1992) 337–342.
[20] E. S. Oztas, B. Yildiz, I. Siap, A novel approach for constructing reversible codes and applications

to DNA codes over the ring $\mathbb{F}_2[u]/(u^{2k}-1)$, Finite Fields and Their Applications 46 (2017) 217–234.
[21] H. Rifá-Pous, J. Rifá, L. Ronquillo, $\mathbb{Z}_2\mathbb{Z}_4$-additive perfect codes in steganography, Advances in Mathematics of Communications 5(3) (2011) 425–433.
[22] A. Sharma, M. Bhaintwal, $\mathbb{F}_3R$-skew cyclic codes, International Journal of Information and Coding Theory 3(3) (2016) 234–251.
[23] I. Siap, T. Abualrub, N. Aydin, P. Seneviratne, Skew cyclic codes of arbitrary length, International Journal of Information and Coding Theory 2(1) (2011) 10–20.