Skew cyclic codes over $\mathbb{F}_p + u\mathbb{F}_p$

R. Dastbasteh

Department of Mathematics,
Simon Fraser University,
Vancouver, V5A 1S6, Canada
Email: dastbasteh@sabanciuniv.edu

H. Mousavi

Department of Electrical Engineering,
Shiraz University of Technology,
Shiraz, 71557-13876, Iran
Email: h.moosavi@sutech.ac.ir

T. Abualrub

Department of Mathematics and Statistics,
American University of Sharjah,
Sharjah, 61485, UAE
Email: abualrub@aus.edu

N. Aydin

Department of Mathematics and Statistics,
Kenyon College,
Gambier, Ohio, 43022, USA
Email: aydinn@kenyon.edu

J. Haghighat*

Department of Electrical Engineering,
Shiraz University of Technology,
Shiraz, 71557-13876, Iran
Email: haghighat@sutech.ac.ir
*Corresponding author

Abstract: In this paper, we study skew cyclic codes with arbitrary length over the ring $R = \mathbb{F}_p + u\mathbb{F}_p$ where p is an odd prime and $u^2 = 0$. We characterise all skew cyclic codes of length n as left $R[x;\theta]$-submodules of $R_n = R[x;\theta]/\langle x^n - 1\rangle$. We find all generator polynomials for these codes and describe their minimal spanning sets. Moreover, an encoding algorithm is presented for skew cyclic codes over the ring R. Finally, based on the theory we developed in this paper, we provide examples of codes with good parameters over F_p with different odd primes p. In fact, example 6 in our paper is a new ternary code in the class of quasi-twisted codes. We also present several examples of optimal codes.

Keywords: skew cyclic codes; optimal codes; codes over rings.

Reference to this paper should be made as follows: Dastbasteh, R., Mousavi, H., Abualrub, T., Aydin, N. and Haghighat, J. (2018) 'Skew cyclic codes over $\mathbb{F}_p + u\mathbb{F}_p$', *Int. J. Information and Coding Theory*, Vol. 5, No. 1, pp.81–99.

Biographical notes: R. Dastbasteh received his BSc and MSc in Mathematics from Shiraz University and Sabanci University, respectively. Currently, he is a PhD student at Simon Fraser University. His main research interests include coding theory, algebraic geometry, and algebraic function fields.

H. Mousavi received his BSc in Mathematics from Shiraz University, in Iran in 2013, and his first MSc in Communication Engineering from Shiraz University of Technology, in Iran in 2015. He earned his second MSc in Mathematics from Sabanci University, in Turkey in 2017. Currently, he is a PhD student in Mathematics at the Georgia Institute of Technology. His research interests primarily focus on number theory, in addition to working on algebraic coding theory.

T. Abualrub is a Professor of Mathematics at the American University of Sharjah. He received his Master and PhD degrees in Mathematics from The University of Iowa, USA, in August 1994 and May 1998, respectively. In 1998, he joined The American University of Sharjah (AUS) as an Assistant Professor in the Department of Mathematics and Statistics. Currently, he is a Professor of Mathematics at AUS. His research interests include error correcting codes, DNA computing, wavelet theory, and control theory. He is on the editorial board of *Mathematical Sciences and Applications E-Notes Journal* and *Journal of Algebra Combinatorics Discrete Structures and Applications*.

N. Aydin received his PhD in mathematics and MS in Computer Science from The Ohio State University. His primary area of research is algebraic coding theory, and he is particularly interested in constructing codes with best possible parameters. He has been teaching at Kenyon College since 2002 where he has supervised a number of undergraduate research projects in coding theory.

J. Haghighat received his MSc in Electrical Engineering from University of Tehran in 2002, and his PhD in Electrical Engineering from Concordia University in 2007. He is currently with the Department of Electrical Engineering, Shiraz University of Technology, Shiraz, Iran as an assistant professor. His research interests include source coding, channel coding, cooperative communications, and wireless sensor networks.

1 Introduction

Cyclic codes are an important class of codes from both theoretical and practical points of view. Traditionally, cyclic codes were studied over finite fields. Recently, finite rings and their ideals are employed to construct cyclic codes with good error detection and error correction capabilities (Calderbank and Sloane, 1995; Pless and Qian, 1996; Kanwar and Lopez-Permouth, 1997; Bonnecaze and Parampalli, 1999; Wolfmann, 2001). These codes have found applications in various areas including wireless sensor networks, steganography and burst errors (Mandelbaum, 1969; Tokiwa et al., 1983).

Delphine et al. (2007) generalised the notion of cyclic codes. They used generator polynomials in a non-commutative polynomial ring called skew polynomial ring. They gave examples of skew cyclic codes with Hamming distances larger than previously best known linear codes of the same length and dimension. Abualrub et al. (2010) generalised the concept of skew cyclic codes to skew quasi-cyclic codes. They constructed several new codes with Hamming distances exceeding the Hamming distances of the previously best known linear codes with comparable parameters. Other papers have appeared that make use of various non-commutative rings to construct linear codes with good parameters (Boucher et al., 2008; Boucher and Ulmer, 2011; Jian, 2013; Bhaintwal, 2012).

Let p be an odd prime number. In this paper, we are interested in studying skew cyclic codes over the ring $R = \mathbb{F}_p + u\mathbb{F}_p$ where $u^2 = 0$. Note that if we let $p = 2$, then the ring $\mathbb{F}_2 + u\mathbb{F}_2$ has only the trivial automorphism, and therefore skew cyclic codes over this ring are exactly the classical cyclic codes studied in Abualrub and Siap (2007). One motivation behind studying skew cyclic codes over this specific ring is that compared to the class of cyclic codes over R, the class of skew cyclic codes is larger. This suggests that there may be a better possibility of finding codes with good parameters from skew cyclic codes over R.

The paper is organised as follows: In Section 2, we discuss some properties of the skew polynomial ring $R[x;\theta]$. In Section 3, we find the set of generator polynomials for skew cyclic codes over the ring R. Section 4 studies minimal generating sets for these codes and their cardinality. Section 5 includes an encoding algorithm for these codes. Section 6 includes examples of linear codes over $\mathbb{F}_p$ obtained from skew cyclic codes over R by the help of a Gray map. Section 7 includes the conclusion of our work and suggestions for future work.

2 Preliminaries

Let p be an odd prime number. Consider the Galois field $\mathbb{F}_p$ of order p and the ring $R = \mathbb{F}_p + u\mathbb{F}_p = \left\{a + ub \mid a, b \in \mathbb{F}_p, \text{ with } u^2 = 0\right\} = \mathbb{F}_p[u] / \left\langle u^2 \right\rangle$. Denote the set of units of $\mathbb{F}_p$ by $\mathbb{F}_p^* = \mathbb{F}_p - \{0\}$. Let θ be an automorphism of the ring R with order $o(\theta) = |\langle\theta\rangle| = e > 1$. Then, every element in the finite field $\mathbb{F}_p$ is fixed under θ. Hence, $\theta(a) = a$ for any $a \in \mathbb{F}_p$. The next Lemma characterises the elements of the group $Aut(R)$.

Lemma 1: *Let* $\theta \in Aut(R)$ *and* $a + ub \in R$. *Then* $\theta(a + ub) = a + usb$ *for some* $s \in \mathbb{F}_p^*$.

Proof: Let $\theta \in Aut(R)$ and suppose that $\theta(u) = r + us$ for some $r, s \in \mathbb{F}_p$. Then $u^2 = 0$ and

$$
\begin{aligned}
0 &= \theta\left(u^2\right) = \theta(u)\theta(u) \\
0 &= (r + us)(r + us) = r^2 + 2urs \\
0 &= r^2.
\end{aligned}
$$

Hence $r = 0$ and $\theta(u) = us$ for some $s \in \mathbb{F}_p^*$. Now, let $a + ub \in R$. Then

$$\begin{aligned}\theta(a + ub) &= \theta(a) + \theta(u)\theta(b) \\ &= a + usb.\end{aligned}$$

□

One can show by induction that if $\theta(a + ub) = a + usb$, then $\theta^i(a + ub) = a + us^ib$ for any positive integer i.

Definition 2.1: Let θ be an automorphism on R. Define the skew polynomial set $R[x;\theta]$ to be

$$R[x;\theta] = \left\{ \begin{array}{c} f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n | \\ a_i \in \ R \text{ for all } i = 0, 1, \ldots, n \end{array} \right\}$$

where the addition of these polynomials is defined in the usual way while multiplication $*$ is defined using the distributive law and the rule

$$(ax^i) * (bx^j) = a\theta^i(b)x^{i+j}. \tag{1}$$

The set $R[x;\theta]$ is a non-commutative ring called the skew polynomial ring with the usual addition of polynomials and multiplication defined as above. Note that if $a, b \in \mathbb{F}_p$, then $(ax^i) * (bx^j) = a\theta^i(b)x^{i+j} = abx^{i+j}$ because $\theta(b) = b$ for all $b \in \mathbb{F}_p$. Hence, the ring $\mathbb{F}_p[x]$ is a subring of $R[x;\theta]$.

Note that throughout the paper we might right $f * g$ as fg.

Theorem 2 (Mcdonald, 1974) (The Right Division Algorithm)**:** *Let f and g be two polynomials in $R[x;\theta]$ with the leading coefficient of f being a unit. Then there exist unique polynomials q and r such that*

$$g = q * f + r \text{ where } r = 0 \text{ or } \deg(r) < \deg(f).$$

The above result is called a division on the right by f. A similar result can be proved regarding division on left by f.

Theorem 3: *The centre of $R[x;\theta]$ is the set $Z(R[x;\theta]) = \mathbb{F}_p[x^e]$ for any $\theta \in Aut(R)$ of order e.*

Proof: The proof is similar to Lemma 1.1 in Jian (2013). □

As a result of this Theorem, the following corollary is clear.

Corollary 4: $x^n - 1 \in Z(R[x;\theta])$ *if and only if* $e|n$.

The above corollary shows that the polynomial $(x^n - 1)$ is in the centre $Z(R[x;\theta])$ of the ring $R[x;\theta]$, hence generates a two-sided ideal if and only if the $e|n$. Consequently, the quotient space $R_n = R[x;\theta]/\langle x^n - 1\rangle$ is a ring if and only if $e|n$. In this case, skew cyclic codes can be regarded as (left) ideals in R_n. In this paper, we are interested in skew cyclic codes for any length n regardless of whether $e|n$ or not. We show that regarding them as modules rather than ideals gives us the flexibility to handle skew cyclic codes of all lengths in the same way.

Let $r(x) \in R[x;\theta]$ and $(f(x) + \langle x^n - 1\rangle) \in R_n$. Define

$$r(x) * (f(x) + \langle x^n - 1\rangle) = r(x) * f(x) + \langle x^n - 1\rangle.$$

This multiplication with the usual addition leads to the following Lemma

Lemma 5: *The quotient space R_n is a left $R[x;\theta]$ module.*

Definition 2.2: Let R be the ring $\mathbb{F}_p + u\mathbb{F}_p$ and θ be an automorphism of R with $|\langle\theta\rangle| = e$. A subset C of R^n is called a skew cyclic code of length n if C satisfies the following conditions:

- C is a submodule of R^n
- If $c = (c_0, c_1, \ldots, c_{n-1}) \in C$, then so is its skew cyclic shift, i.e., $(\theta(c_{n-1}), \theta(c_0), \ldots, \theta(c_{n-2})) \in C$.

We have the usual representation of vectors $(c_0, c_1, \ldots, c_{n-1}) \in R^n$ by polynomials $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$. With this identification, the skew cyclic shift of a codeword $c(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1}x^{n-1} \in C$ corresponds to $x * c(x) \bmod (x^n - 1)$ which is equal to $\theta(c_{n-1}) + \theta(c_0)x + \cdots + \theta(c_{n-2})\, x^{n-1}$.

As is common in the discussion of cyclic codes, we can regard codewords of a skew cyclic code C as vectors or as polynomials interchangeably. In either case, we use the same notation C to denote the set of all codewords. We follow this convention in the definition below and in the rest of the paper.

Definition 2.3 (Polynomial definition of skew cyclic codes)**:** A subset $C \subseteq R_n$ is called a skew cyclic code if C satisfies the following conditions:

- C is an R-submodule of R^n
- If $c(x) = \left(a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}\right) \in C$, then $x * c(x) = \left(\theta(a_{n-1}) + \theta(a_0)x + \cdots + \theta(a_{n-2})x^{r-1}\right) \in C$.

As a result of this definition, we get the following Lemma.

Lemma 6: *C is a skew cyclic code of length n over R if and only if C is a left $R[x;\theta]-$submodule of $R_n = R[x;\theta]/\langle x^n - 1\rangle$.*

3 Generator polynomials of skew cyclic codes over R

In this section we are interested in studying algebraic structures of skew cyclic codes over R. Using Lemma 6, our goal is to find the generator polynomials of these codes as left $R[x;\theta]$-submodules of $R_n = R[x;\theta]/\langle x^n - 1\rangle$.

Lemma 7: *For any $g(x) \in R[x;\theta]$, there exists a unique $g'(x) \in \mathbb{F}_p[x]$ of the same degree as $g(x)$ such that $g(x) * u = ug(x)'$.*

Proof: Let $g(x) = \sum_{i=0}^{n} g_i x^i \in R[x, \theta]$. Since $g_i \in R$ for each i, there exist $g_i', g_i'' \in \mathbb{F}_p$ such that $g_i = g_i' + ug_i''$. So $g(x) = \sum (g_i' + ug_i'')x^i$.

It follows from Lemma 1 that $us^i = \theta^i(u)$. Hence we have

$$\begin{aligned} g(x) * u &= \left(\sum (g_i' + ug_i'')x^i\right) * u = \left(\sum g_i' x^i\right) * u + \left(\sum ug_i'' x^i\right) * u \\ &= \sum g_i' \theta^i(u) x^i + \sum ug_i'' \theta^i(u) x^i = \sum g_i' us^i x^i + \sum ug_i'' us^i x^i. \end{aligned}$$

Obviously, the second sum is 0 (it contains a factor of u^2). Therefore, we have

$$g(x) * u = \sum g_i' us^i x^i = u \sum g_i' s^i x^i = ug'(x). \tag{2}$$

The uniqueness of g' in $\mathbb{F}_p[x]$ is clear by this proof. □

Notation. For a fixed element $g \in \mathbb{F}_p[x]$, the element $g' \in \mathbb{F}_p[x]$ in Lemma 7 is unique and hence we call it the *partaker* of g. Also note that if $g = g_1 + ug_2 \in R[x;\theta]$, then $ug = u\,(g_1 + ug_2) = ug_1 = g'u$.

Example 1: Suppose $g(x) = 1 + x + x^2 \in (\mathbb{F}_p + u\mathbb{F}_p)[x;\theta]$ where $\theta(a + ub) = a + sub$ for $s \in \mathbb{F}_p$. Then $g(x) * u = (1 + x + x^2) * u = u + x * u + x^2 * u = u + \theta(u)x + \theta^2(u)x^2 = u + sux + s^2ux^2$. Therefore, $g(x)u = u(1 + sx + s^2x^2)$. So $g' = s^2x^2 + sx + 1$.

Note that there are infinitely many elements $h \in R[x;\theta]$ such that $gu = uh$. It is sufficient to define $h = g' + ul$ for every $l \in \mathbb{F}_p[x]$.

Lemma 8: *The polynomial $x^n - 1$ factors in the ring $\mathbb{F}_p[x]$ as $x^n - 1 = f_1(x)g_1(x)$ if and only if $x^n - 1 = f(x) * g(x)$ in the ring $R\,[x;\theta]$ where $f(x) = f_1(x) + uf_2(x)$ and $g(x) = g_1(x) + ug_2(x)$ for some polynomials $f_2(x),\ g_2(x)$ in $\mathbb{F}_p[x]$.*

Proof: For the forward direction, suppose $x^n - 1 = f_1(x)g_1(x)$ in the ring $\mathbb{F}_p[x]$. Since $\mathbb{F}_p\,[x]$ is a subring of $R[x;\theta]$, $x^n - 1 = f_1(x)g_1(x)$ in $R[x;\theta]$. Hence, we let $f_2(x) = g_2(x) = 0$.

For the backward direction, suppose $x^n - 1 = f(x) * g(x)$ in the ring $R\,[x;\theta]$ where $f(x) = f_1(x) + uf_2(x)$ and $g(x) = g_1(x) + ug_2(x)$ for some polynomials $f_2(x),\ g_2(x)$ in $\mathbb{F}_p[x]$. Then

$$\begin{aligned} x^n - 1 &= f(x) * g(x) \\ &= (f_1(x) + uf_2(x)) * (g_1(x) + ug_2(x)) \\ &= f_1(x)g_1(x) + f_1(x) * ug_2(x) + uf_2(x)g_1(x). \end{aligned}$$

Using Lemma 7, we know that $f_1(x)u = uk(x)$ for some $k(x) \in \mathbb{F}_p[x]$. Hence,

$$\begin{aligned} x^n - 1 &= f(x) * g(x) \\ &= f_1(x)g_1(x) + f_1(x) * ug_2(x) + uf_2(x)g_1(x) \\ &= f_1(x)g_1(x) + uk(x)g_2(x) + uf_2(x)g_1(x) \\ &= f_1(x)g_1(x) + u\left(k(x)g_2(x) + f_2(x)g_1(x)\right). \end{aligned}$$

Suppose $x^n - 1 = f_1(x)g_1(x) + r_1(x)$ in the ring $\mathbb{F}_p[x]$. Since $\mathbb{F}_p[x]$ is a subring of $R\,[x;\theta]$, $x^n - 1 = f_1(x)g_1(x) + r_1(x)$ in the ring $R\,[x;\theta]$ as well. Hence,

$$\begin{aligned} x^n - 1 &= f_1(x)g_1(x) + u\,(k(x)g_2(x) + f_2(x)g_1(x)) \\ &= x^n - 1 - r_1(x) + u\,(k(x)g_2(x) + f_2(x)g_1(x)) \\ r_1(x) &= u\,(k(x)g_2(x) + f_2(x)g_1(x))\,. \end{aligned}$$

But $r_1(x) \in \mathbb{F}_p[x]$. This is a contradiction unless $r_1(x) = 0$ and then $x^n - 1 = f_1(x)g_1(x)$ in the ring $\mathbb{F}_p[x]$. □

Note that in the above Lemma $f_1(x)$ and $g_1(x)$ are unique polynomials because the ring $\mathbb{F}_p[x]$ is a unique factorisation ring; however, $f_2(x)$ and $g_2(x)$ are not unique. This is justified by noting that the ring $R\,[x;\theta]$ is not a unique factorisation ring. We know that $U(R) = \mathbb{F}_p^* + u\mathbb{F}_p$. Based on this fact, we find $U(R[x;\theta])$.

Lemma 9: $U\,(R\,[x;\theta]) = \left\{a + uh(x) | a \in \mathbb{F}_p^*,\ \textit{and}\ h(x) \in \mathbb{F}_p\,[x]\right\}$

Proof: Let $a + uh(x) \in R\,[x;\theta]$ where $a \in \mathbb{F}_p^*$ and $h(x) \in \mathbb{F}_p\,[x]$. Then

$$\begin{aligned} (a + uh) * \left(a^{-1} - a^{-1}uha^{-1}\right) &= 1 - uha^{-1} + uha^{-1} - uh * a^{-1}uha^{-1} \\ &= 1 - uh * a^{-1}uha^{-1} \\ &= 1 - u^2h_1a^{-1}ha^{-1} \text{ (by Lemma 7)} \\ &= 1. \end{aligned}$$

Hence, $a + uh(x) \in U\,(R\,[x;\theta])$. Conversely, let $f \in U\,(R\,[x;\theta])$. Then, there exists $g \in R\,[x;\theta]$ such that $f * g = g * f = 1$. Let $f = f_1 + uf_2$ and $g = g_1 + ug_2$ for $f_i, g_i \in \mathbb{F}_p[x]$. Then, $f * g = (f_1 + uf_2) * (g_1 + ug_2) = 1$ implies that $f_1g_1 = 1$ and $uf_2g_1 + f_1ug_2 = 0$. Hence, f_1 is a non-zero constant polynomial. That is, $f_1 \in \mathbb{F}_p^*$. Thus, $f = f_1 + uf_2$, where $f_1 \in \mathbb{F}_p^*$ and $f_2 \in \mathbb{F}_p[x]$. □

Let C be be a nonzero skew cyclic code over R and let $c(x) = \left(a_0 + a_1x + \cdots + a_{n-1}x^{n-1}\right) \in C$. If a_{n-1} is a unit in R with inverse w then $wc(x)$ is a monic polynomial in C. Hence, for any nonzero skew cyclic code we have the following cases to consider:

Case 1: C has no monic polynomials.

Case 2: C has at least one monic polynomial.

The next lemma classifies all skew cyclic codes that satisfy Case 1.

Lemma 10: *Let C be a nonzero skew cyclic code that has no monic polynomials. Then $C = \left\langle u\overline{a(x)}\right\rangle$ where $\overline{a(x)}$ is a polynomial of minimal degree in C and $x^n - 1 = \overline{b(x)}\,\overline{a(x)}$ in $\mathbb{F}_p[x]$.*

Proof: Suppose C is a nonzero skew cyclic code that has no monic polynomials and supposes that

$$\theta\,(a + ub) = a + usb \text{ where } s \in \mathbb{F}_p^*.$$

Let

$$a(x) = a_0 + a_1 x + \cdots + u\overline{a_r} x^r$$

be a polynomial of a minimal degree in C where $\overline{a_r} \in \mathbb{F}_p^*$ and $a_i \in R$ for all $i = 0, 1, \ldots, r-1$. Note that

$$ua(x) = ua_0 + ua_1 x + \cdots + ua_{r-1} x^{r-1} \in C.$$

Since $a(x)$ is of minimal degree in C, $ua(x) = 0$ and

$$a(x) = u\overline{a(x)},$$

where $\overline{a(x)} \in \mathbb{F}_p[x]$ and $a_i = u\overline{a_i}$ for all $i = 0, 1, \ldots, r$. Let $c(x)$ be any codeword in C. Then, $c(x)$ is not monic. Hence, $c(x) = c_0 + c_1 x + \cdots + u\overline{c_t} x^t$ where $t \leq n-1$, $\overline{c_t} \in \mathbb{F}_p^*$ and $c_i \in R$. for all $i = 0, 1, \ldots, t-1$. We want to prove that $c(x) = u\overline{c(x)}$. Write $c(x) = c_1(x) + c_2(x)$ where all terms in $c_1(x)$ have powers less than r while all terms in $c_2(x)$ have powers larger than or equal r. Suppose c_{t-1} is a unit. Note that $\theta^i(u) = us^i$. Consider the polynomial $Z(x) = z_1(x) - z_2(x) \in C$, where

$$\begin{aligned}
z_1(x) &= \left(s^{t-r}\right)^{-1} (\overline{a_r})^{-1} x^{t-r} a(x) \\
&= \left(s^{t-r}\right)^{-1} (\overline{a_r})^{-1} \overline{a_0} \theta^{t-r}(u) x^{t-r} + \left(s^{t-r}\right)^{-1} (\overline{a_r})^{-1} \overline{a_1} \theta^{t-r}(u) x^{t-r+1} \\
&\quad + \ldots + \left(s^{t-r}\right)^{-1} (\overline{a_r})^{-1} \overline{a_{r-1}} \theta^{t-r}(u) x^{t-1} + \left(s^{t-r}\right)^{-1} (\overline{a_r})^{-1} \overline{a_r} \theta^{t-r}(u) x^t \\
&= \left(s^{t-r}\right)^{-1} (\overline{a_r})^{-1} \overline{a_0} \theta^{t-r}(u) x^{t-r} + \left(s^{t-r}\right)^{-1} (\overline{a_r})^{-1} \overline{a_1} \theta^{t-r}(u) x^{t-r+1} \\
&\quad + \ldots + \left(s^{t-r}\right)^{-1} (\overline{a_r})^{-1} \overline{a_{r-1}} \theta^{t-r}(u) x^{t-1} + ux^t,
\end{aligned}$$

and

$$z_2(x) = (c_t)^{-1} c(x) = (c_t)^{-1} c_0 + (c_t)^{-1} c_1 x + \cdots + (c_t)^{-1} c_{t-1} x^{t-1} + ux^t.$$

Hence, $Z(x) = z_1(x) - z_2(x)$ is a polynomial of degree $t-1$ in C where the coefficient of x^{t-1} is $z_{t-1} = \left(s^{t-r}\right)^{-1} (\overline{a_r})^{-1} \overline{a_{r-1}} \theta^{t-r}(u) - (c_t)^{-1} c_{t-1} = \eta u - (c_t)^{-1} c_{t-1}$ where $(c_t)^{-1} c_{t-1}$ is a unit. By Lemma 9, z_{t-1} is a unit and hence C has a monic polynomial. This is a contradiction since C has no monic polynomials. Using the same procedure we can show that c_i is not a unit for all $c_i \in c_2(x)$. Suppose that c_i is a unit for some i in $c_1(x)$. Then $uc(x) = uc_1(x) \in C$ and $uc_1(x)$ is a nonzero polynomial with $\deg uc_1(x) < \deg a(x)$. Again, this is a contradiction. Hence,

$$c(x) = u\overline{c(x)},$$

where $\overline{c(x)} \in \mathbb{F}_p[x]$ and $c_i = u\overline{c_i}$ for all $i = 0, 1, \ldots, t$. Since $\overline{a(x)}$ and $\overline{c(x)}$ are two polynomials in $\mathbb{F}_p[x]$, by the division algorithm, there exist polynomials $q(x), r(x)$ in $\mathbb{F}_p[x]$ such that

$$\overline{c(x)} = q(x)\overline{a(x)} + r(x)$$

where $r(x) = 0$ or $\deg r(x) < \deg \overline{a(x)} = \deg a(x)$. Hence, using Lemma 7, we get

$$\begin{aligned} u\overline{c(x)} &= uq(x)\overline{a(x)} + ur(x) \\ &= q'(x)u\overline{a(x)} + ur(x). \end{aligned}$$

This implies that

$$ur(x) = u\overline{c(x)} - q'(x)u\overline{a(x)} \in C.$$

This is a contradiction because $\deg ur(x) < \deg \overline{a(x)} = \deg a(x)$. Therefore, $ur(x) = 0$. Since $r(x) \in \mathbb{F}_p[x]$, then $r(x) = 0$ and

$$u\overline{c(x)} = q'(x)u\overline{a(x)}.$$

Hence, $C = \left\langle u\overline{a(x)} \right\rangle$. Again, since $\overline{a(x)}$ and $x^n - 1$ are polynomials in $\mathbb{F}_p[x]$, by the division algorithm, there exist polynomials $\overline{b(x)}, r_1(x)$ in $\mathbb{F}_p[x]$ such that

$$x^n - 1 = \overline{b(x)}\ \overline{a(x)} + r_1(x),$$

where $r_1(x) = 0$ or $\deg r_1(x) < \deg \overline{a(x)} = \deg a(x)$. Hence,

$$\begin{aligned} u\left(x^n - 1\right) &= u\ \overline{b(x)}\ \overline{a(x)} + ur_1(x) \\ &= q_1'(x)u\overline{a(x)} + ur_1(x). \end{aligned}$$

In the ring $R_n = R[x;\theta]/\langle x^n - 1\rangle$, we get

$$0 = q_1'(x)u\overline{a(x)} + ur_1(x)$$

or,

$$ur_1(x) = -q_1'(x)u\overline{a(x)} \in C.$$

A contradiction. Hence, $ur_1(x) = 0$. Since $r_1(x) \in \mathbb{F}_p[x]$, $r_1(x) = 0$ and

$$x^n - 1 = \overline{b(x)}\ \overline{a(x)}.$$

$\square$

Lemma 11: *Let C be a nonzero skew cyclic code that has at least one monic polynomial and let $g(x)$ be a polynomial of minimal degree in C. Suppose that $g(x)$ is monic. Then $C = \langle g(x)\rangle$ where $x^n - 1 = k(x)g(x)$ in R_n.*

Proof: The proof is a straightforward application of Theorem 2. $\square$

Lemma 12: *Let C be a nonzero skew cyclic code that has at least one monic polynomial. Moreover, suppose that all polynomials of minimal degree are not monic. Let $a(x)$ be a polynomial of minimal degree in C. Let $g(x)$ be a monic polynomial in C of minimal degree among all monic polynomials in C. Then, $C = \langle g(x) + up(x), a(x)\rangle = \left\langle g(x) + up(x), u\overline{a(x)}\right\rangle$, where $x^n - 1 = k(x) * g(x)$ in $R[x; \theta]$, $x^n - 1 = \overline{b(x)}\,\overline{a(x)}$ in $\mathbb{F}_p[x]$ and $\deg a(x) < \deg g(x)$.*

Proof: Let C be a skew cyclic code that has at least one monic polynomial and let $a(x)$ be a polynomial of minimal degree in C. Since $a(x)$ is not monic and of minimal degree in C, as in the proof of Lemma 10, we can show that $a(x) = u\overline{a(x)}$ where $\overline{a(x)} \in \mathbb{F}_p[x]$. Suppose that $c(x)$ is a codeword in C. Let $f(x)$ be a monic polynomial of minimal degree in C. Then using Theorem 2, there exist two polynomials $q_2(x)$ and $r_2(x)$ in R_n such that

$$c(x) = q_2(x) * f(x) + r_2(x)$$

where $r_2(x) = 0$ or $\deg r_2(x) < \deg f(x)$. Then

$$r_2(x) = c(x) - q_2(x) * f(x) \in C.$$

Since $f(x)$ is a monic polynomial of minimal degree in C, $r_2(x)$ is not monic. In fact, as in the proof of Lemma 10, one can easily show that $r_2(x) = ur_3(x)$ for some polynomial $r_3(x) \in \mathbb{F}_p[x]$. Now, apply the division algorithm on $\overline{a(x)}$ and $r_3(x)$ to obtain

$$r_3(x) = q_3(x)\overline{a(x)} + r_4(x),$$

where $r_4(x) = 0$ or $\deg r_4(x) < \deg \overline{a(x)}$. Hence,

$$\begin{aligned} r_2(x) &= ur_3(x) = uq_3(x)\overline{a(x)} + ur_4(x) \\ &= q_4u\overline{a(x)} + ur_4(x). \end{aligned}$$

Thus, $ur_4(x) \in C$. Since $\deg r_4(x) < \deg a\bar{(x)} = \deg a(x)$, $ur_4(x) = 0$. Since $r_4(x) \in \mathbb{F}_p[x]$, then $r_4(x) = 0$ and

$$r_2(x) = ur_3(x) = uq_3(x)a\bar{(x)} = q_4ua\bar{(x)}.$$

Therefore,

$$\begin{aligned} c(x) &= q_2(x)f(x) + r_2(x) \\ &= q_2(x)f(x) + q_4u\overline{a(x)}. \end{aligned}$$

Thus $C = \langle f, a(x)\rangle = \left\langle f, u\overline{a(x)}\right\rangle$. Note that $x^n - 1$ and $\overline{a(x)}$ are polynomials in $\mathbb{F}_p[x]$. Hence, by the division algorithm we can write

$$x^n - 1 = q_5\overline{a(x)} + r_5$$

where $r_5(x) = 0$ or $r_5(x)$ is a polynomial in $\mathbb{F}_p[x]$ with $\deg r_5(x) < \deg \overline{a(x)}$. Then we have

$$u(x^n - 1) = uq_5\overline{a(x)} + ur_5$$
$$= q_5' u\overline{a(x)} + ur_5.$$

In R_n, we obtain

$$ur_5(x) = -q_5' u\overline{a(x)} \in C$$

with $\deg ur_5(x) = \deg r_5(x) < \deg \overline{a(x)}$. This is a contradiction unless $ur_5(x) = 0$. Since $r_5(x) \in \mathbb{F}_p[x]$, we have $r_5(x) = 0$ and

$$x^n - 1 = q_5\overline{a(x)}.$$

Moreover, let $f(x) = f_1(x) + uf_2(x)$ where $f_1(x),\ f_2(x) \in \mathbb{F}_p[x]$. Then using Theorem 2, we have

$$x^n - 1 = q_3(x)\left(f_1(x) + uf_2(x)\right) + R(x),$$

where $R(x) = 0$ or $\deg R(x) < \deg f(x) = \deg f_1(x)$. This implies that $R(x) \in C$. Since $f(x)$ is a monic polynomial of minimal degree in C, we conclude that $R(x)$ is not monic. Hence, $R(x) = w(x)u\overline{a(x)} = uw_1(x)\overline{a(x)}$ (by Lemma 7). Thus

$$\begin{aligned} x^n - 1 &= q_3(x)\left(f_1(x) + uf_2(x)\right) + uw_1(x)\overline{a(x)} \\ &= q_3(x)f_1(x) + q_3(x)uf_2(x) + uw_1(x)\overline{a(x)} \\ &= q_3(x)f_1(x) + uq_4(x)f_2(x) + uw_1(x)\overline{a(x)}. \end{aligned}$$

Hence, in the ring $\mathbb{F}_p[x]$, we have

$$x^n - 1 = q_3(x)f_1(x).$$

By Lemma 8, there must be a polynomial $g(x)$ in $R[x;\theta]$ of degree $f_1(x)$ such that $g(x)$ is a right divisor of $x^n - 1$ in $R[x;\theta]$. Hence, $g(x) = f_1(x) + ul_1(x)$ where $l_1(x)$ is a polynomial in $\mathbb{F}_p[x]$ of degree less than the degree of $f_1(x)$. Thus,

$$\begin{aligned} f(x) &= f_1(x) + uf_2(x) \\ &= g(x) - ul_1(x) + uf_2(x) \\ &= g(x) + u\left(f_2(x) - l_1(x)\right). \end{aligned}$$

Therefore, $C = \langle f, a(x)\rangle = \left\langle f, u\overline{a(x)}\right\rangle = \left\langle g(x) + u\left(f_2(x) - l_1(x)\right), u\overline{a(x)}\right\rangle$ with $x^n - 1 = k(x)g(x)$ in $R[x;\theta]$ and $x^n - 1 = \overline{b(x)}\ \overline{a(x)}$ in $\mathbb{F}_p[x]$ and $\deg \overline{a(x)} < \deg g(x)$. $\square$

Lemma 13: *Let $C = \langle g(x) + up(x), a(x)\rangle = \left\langle g(x) + up(x), u\overline{a(x)}\right\rangle$ as in Lemma 12. Then $\overline{a(x)} | g(x) \operatorname{mod} u$ and $\dfrac{x^n - 1}{g} up \in \langle ua\rangle$.*

Proof: Suppose $C = \langle g(x) + up(x), a(x)\rangle = \left\langle g(x) + up(x), u\overline{a(x)}\right\rangle$ as in Lemma 12. Let $uc(x) \in C$ where $c(x) \in \mathbb{F}_p[x]$. Using the division algorithm one can write

$$c(x) = q(x)\overline{a(x)} + r(x),$$

where $r(x) = 0$ or $\deg r(x) < \deg \overline{a(x)}$. Hence,

$$\begin{aligned} uc(x) &= uq(x)\overline{a(x)} + ur(x) \\ &= q'(x)u\overline{a(x)} + ur(x). \end{aligned}$$

This implies that $ur(x) \in C$. This is a contradiction since $\deg ur(x) = \deg r(x) < \deg a(x) = \deg \overline{a(x)}$. Hence, $ur(x) = 0$ and $r(x) = 0$ because $r(x) \in \mathbb{F}_p[x]$. This implies $uc(x) = uq(x)\overline{a(x)} = q'(x)u\overline{a(x)} \in \langle u\overline{a}\rangle$. Therefore, for any polynomial of the form $uc(x) \in C$, we have $c(x) = q(x)\overline{a(x)}$ and $uc(x) \in \langle ua\rangle$. Since $u\,(g(x) + up(x)) = ug(x) \in C$, we get that $\overline{a(x)}|g(x)\text{mod}u$. Also $\frac{x^n-1}{g}\,(g(x) + up(x)) = \frac{x^n-1}{g}up(x) = u\left(\frac{x^n-1}{g}\right)' p(x) \in C$. Hence $\frac{x^n-1}{g}up \in \langle ua\rangle$. □

We summarise the results of Lemmas 10–13 in the following theorem that classifies all skew cyclic codes over the ring R.

Theorem 14: *Let C be a nonzero skew cyclic code over the ring R. Then C satisfies one of the following cases:*

- *C has no monic polynomials. Then $C = \left\langle u\overline{a(x)}\right\rangle$ where $\overline{a(x)}$ is a polynomial of minimal degree in C and $x^n - 1 = \overline{b(x)}\ \overline{a(x)}$ in $\mathbb{F}_p[x]$.*
- *C has a monic polynomial $g(x)$ of minimal degree in C. Then $C = \langle g(x)\rangle$ where $g(x)$ is a polynomial of minimal degree in C and $x^n - 1 = k(x) * g(x)$ in R_n.*
- *All monic polynomials in C are not of minimal degree. Then we have $C = \langle g(x) + up(x), a(x)\rangle = \left\langle g(x) + up(x), u\overline{a(x)}\right\rangle$, where $a(x)$ is a polynomial of minimal degree in C which is not monic, $g(x)$ is a monic polynomial in C of minimal degree among all monic polynomials in C, $x^n - 1 = k(x) * g(x)$ in $R[x;\theta]$, $x^n - 1 = \overline{b(x)}\ \overline{a(x)}$ in $\mathbb{F}_p[x]$, $\overline{a(x)}|g(x)\text{mod}u$ and $\frac{x^n-1}{g}up \in \langle ua\rangle$.*

Proof: The proof follows from Lemmas 10–13. □

4 Minimal spanning sets for skew cyclic codes over R

In this section, we provide minimal generating sets for skew cyclic codes over R. The generating sets will help in finding the cardinality of each code. Moreover, they will be useful in describing an encoding algorithm for these codes.

Theorem 15: *Let C be a nonzero skew cyclic code over the ring R.*

- *If $C = \left\langle u\overline{a(x)} \right\rangle$ where $\overline{a(x)}$ is a polynomial of minimal degree r in C and $x^n - 1 = \overline{b(x)}\ \overline{a(x)}$ in $\mathbb{F}_p[x]$, then*

  $$\beta = \left\{ u\overline{a(x)}, xu\overline{a(x)}, \ldots, x^{n-r-1}u\overline{a(x)} \right\},$$

  forms a minimal generating set for C and $|C| = p^{n-r}$.

- *If $C = \langle g(x) \rangle$ where $g(x)$ is a polynomial of minimal degree r in C and $x^n - 1 = k(x) * g(x)$ in R_n, then*

  $$\beta = \left\{ g(x), x * g(x), \ldots, x^{n-r-1} * g(x) \right\},$$

  forms a minimal generating set for C and $|C| = \left(p^2\right)^{n-r}$.

- *If $C = \langle g(x) + up(x), a(x) \rangle = \left\langle g(x) + up(x), u\overline{a(x)} \right\rangle$, where $a(x)$ is a polynomial of minimal degree t in C which is not monic, $g(x)$ is a monic polynomial in C of minimal degree r among all monic polynomials in C, $x^n - 1 = k(x) * g(x)$ in $R[x;\theta]$, $x^n - 1 = \overline{b(x)}\ \overline{a(x)}$ in $\mathbb{F}_p[x]$, $\overline{a(x)} | g(x) \bmod u$ and $\dfrac{x^n - 1}{g} up \in \langle ua \rangle$. Then*

  $$\beta = \left\{ \begin{array}{c} g(x) + up(x),\ x * (g(x) + up(x)), \ldots, x^{n-r-1} * (g(x) + up(x)), \\ u\overline{a(x)},\ xu\overline{a(x)}, \ldots,\ x^{r-t-1}u\overline{a(x)} \end{array} \right\},$$

  forms a minimal generating set for C and $|C| = \left(p^2\right)^{n-r} p^{r-t}$.

Proof: We will prove Cases 1 and 3. Case 2 has a similar proof.

- Suppose $c(x) \in \left\langle u\overline{a(x)} \right\rangle$ where $\overline{a(x)}$ is a polynomial of minimal degree r in C and $x^n - 1 = \overline{b(x)}\ \overline{a(x)}$ in $\mathbb{F}_p[x]$. Then $c(x) = s(x)u\overline{a(x)}$. Note that if $s(x) = s_1(x) + us_2(x)$, then $s(x)u\overline{a(x)} = (s_1(x) + us_2(x))\, u\overline{a(x)} = s_1(x)u\overline{a(x)} + us_2(x)u\overline{a(x)} = s_1(x)u\overline{a(x)} + u^2 s_3(x)\overline{a(x)} = s_1(x)u\overline{a(x)}$. Hence, we may assume that $s(x) = s_1(x) \in \mathbb{F}_p[x]$ and $c(x) = s_1(x)u\overline{a(x)} = us_3(x)\overline{a(x)}$ (by Lemma 7) where $\deg s_1(x) = \deg s_3(x)$. If $\deg s_1(x) \leq n - r - 1$, then $c(x) = s(x)u\overline{a(x)}$ $\in$span(β). Otherwise, by the division algorithm there are unique polynomials $q(x),\ r(x)$ such that

  $$s_3(x) = q(x)\frac{x^n - 1}{\overline{a(x)}} + r(x),$$

  where $r(x) = 0$ or $\deg r(x) < \deg \dfrac{x^n - 1}{\overline{a(x)}} = n - r$. Hence,

  $$\begin{aligned} c(x) &= s(x)u\overline{a(x)} = s_1(x)u\overline{a(x)} = us_3(x)\overline{a(x)} \\ &= u\left(q_1(x)\frac{x^n - 1}{\overline{a(x)}} + r(x) \right)\overline{a(x)} \end{aligned}$$

$$= uq_1(x)\frac{x^n-1}{\overline{a(x)}}\overline{a(x)} + ur(x)\overline{a(x)}$$
$$= ur(x)\overline{a(x)}$$
$$= r'(x)\overline{ua(x)},$$

where $\deg r'(x) = \deg r(x) < \deg \frac{x^n-1}{\overline{a(x)}} = n-r$. Hence, β spans the code C. From the construction of the elements in the set β, it is clear that none of the elements is a linear combination of the others. Therefore, β forms a minimal generating set for C. Since $s_1(x) \in \mathbb{F}_p[x]$, we get that $|C| = p^{n-r}$.

- The proof is similar to Case 1.
- Suppose that $c(x) \in C = \langle g(x) + up(x), a(x)\rangle = \left\langle g(x) + up(x), u\overline{a(x)}\right\rangle$. Then $c(x) = s_1(x) * (g(x) + up(x)) + s_2(x) * u\overline{a(x)}$. If $\deg s_1(x) \leq n-r-1$, then $s_1(x) * (g(x) + up(x)) \in$ span(β). Otherwise, by Theorem 2

$$s_1(x) = q(x)\left(\frac{x^n-1}{g(x)}\right) + r(x),$$

where $r(x) = 0$ or $\deg r(x) \leq n-r-1$. Hence,

$$\begin{aligned} s_1(x) * (g(x) + up(x)) &= \left(q(x)\left(\frac{x^n-1}{g(x)}\right) + r(x)\right) * (g(x) + up(x)) \\ &= q(x)\left(\frac{x^n-1}{g(x)}\right) * (g(x) + up(x)) \\ &\quad + r(x) * (g(x) + up(x)) \\ &= q(x)\left(\frac{x^n-1}{g(x)}\right) * up(x) + r(x) * (g(x) + up(x)) \\ &= uq_1(x)p(x) + r(x) * (g(x) + up(x)). \end{aligned}$$

Hence,

$$\begin{aligned} c(x) &= s_1(x) * (g(x) + up(x)) + s_2(x) * u\overline{a(x)} \\ &= uq_1(x)p(x) + r(x) * (g(x) + up(x)) + s_2(x) * u\overline{a(x)} \\ &= uq_1(x)p(x) + r(x) * (g(x) + up(x)) + us_2'(x)\overline{a(x)} \\ &= u\left(q_1(x)p(x) + s_2'(x)\overline{a(x)}\right) + r(x) * (g(x) + up(x)) \end{aligned}$$

Since $r(x) = 0$ or $\deg r(x) \leq n-r-1$, $r(x) * (g(x) + up(x)) \in$ span(β). Hence, we only need to show that $uk(x) \in$ span(β) for any $uk(x) \in C$. Suppose that $uk(x) \in C$. Then

$$k(x) = q_2(x)g(x) + r_2(x),$$

where $r_2(x) = 0$ or $\deg r_2(x) < \deg g(x)$ and $\deg q_2(x) = \deg k(x) - r \leq n-r-1$. Hence $uk(x) = uq_2(x)g(x) + ur_2(x) =$

$q_2'(x)ug(x) + ur_2(x) = q_2'(x)u\left(g(x) + up(x)\right) + ur_2(x)$. Since $q_2'(x)u\left(g(x) + up\right)$ $\in$span(β), it suffices to show that $ur_2(x)$ $\in$span(β) where $r_2(x) = 0$ or $\deg r_2(x) < \deg g(x)$ and $\deg r_2(x) \geq \deg \overline{a(x)}$. By the proof of Lemma 13, we know that any element of the form $ur_2(x)$ belongs to $\langle ua(x)\rangle$. Hence, $ur_2(x) = \underline{s_4(x)}ua(x)$ and $\deg ur_2(x) < \deg g(x)$ and $\deg ur_2(x) \geq \deg \overline{a(x)}$. Thus

$$ur_2(x) = \alpha_0 u\overline{a(x)} + \alpha_1 xu\overline{a(x)} + \cdots + \alpha_{r-t-1}x^{r-t-1}u\overline{a(x)}.$$

Therefore, β spans C. Since none of the elements in β is a linear combination of the other elements, we conclude that β is a minimal generating set for the code C and $|C| = \left(p^2\right)^{n-r} p^{r-t}$.

□

5 The encoding of the codes

Based on Theorem 15, we can develop an encoding algorithm for these codes as follows:

Theorem 16: *Let C be a nonzero skew cyclic code over the ring R.*

- *If $C = \left\langle u\overline{a(x)}\right\rangle$ where $\overline{a(x)}$ is a polynomial of minimal degree r in C and $x^n - 1 = \overline{b(x)}\,\overline{a(x)}$ in $\mathbb{F}_p[x]$, then any codeword $c(x)$ in C is encoded as*

$$c(x) = i(x)u\overline{a(x)},$$

  where $i(x) \in \mathbb{F}_p[x]$ is a polynomial of degree $\leq n - r - 1$.

- *If $C = \langle g(x)\rangle$ where $g(x)$ is a polynomial of minimal degree r in C and $x^n - 1 = k(x)g(x)$ in R_n, then any codeword $c(x)$ in C is encoded as*

$$c(x) = (i(x) + uq(x))g(x),$$

  where $i(x) + uq(x) \in R[x;\theta]$ is a polynomial of degree $\leq n - r - 1$.

- *Let $C = \langle g(x) + up(x), a(x)\rangle = \left\langle g(x) + up(x), u\overline{a(x)}\right\rangle$, where $a(x)$ is a polynomial of minimal degree τ in C which is not monic, $g(x)$ is a monic polynomial in C of minimal degree r among all monic polynomials in C, $x^n - 1 = k(x)g(x)$ in $R[x;\theta]$, $x^n - 1 = \overline{b(x)}\,\overline{a(x)}$ in $\mathbb{F}_p[x]$, $\overline{a(x)}|g(x)\mathrm{mod}u$ and $\dfrac{x^n-1}{g}up \in \langle ua\rangle$. Then, any codeword $c(x)$ in C is encoded as*

$$c(x) = \left(i\left(x\right) + uq(x)\right)\left(g(x) + up(x)\right) + j(x)u\overline{a(x)},$$

  where $i(x) + uq(x) \in R[x;\theta]$ is a polynomial of degree $\leq n - r - 1$ and $j(x) \in \mathbb{F}_p[x]$ is a polynomial of degree$\leq r - \tau - 1$.

Proof: The proof follows from Theorem 15. □

Suppose that a string of $r-\tau$ symbols $J=(j_0,j_1,\cdots,j_{r-\tau-1})\in\mathbb{F}_p^{r-\tau}$ and a string of symbols $I=\big((i_0+uq_0),\cdots,(i_{n-r-1}+uq_{n-r-1})\big)\in\big(\mathbb{F}_p+u\mathbb{F}_p\big)^{n-r}$ are the inputs of the encoder. So, according to Theorem 16, the encoding process will be as follows

$$encod(J,I)=\Big(uj(x)\overline{a(x)}+\big(i(x)+uq(x)\big)\big(g(x)+up(x)\big)\Big)(mod \quad x^n-1). \qquad (3)$$

The encoded string is of length n symbols $v+uw$ over $\mathbb{F}_p+u\mathbb{F}_p$ which is transmitted through the channel.

Example 2: In this example, we see the steps to encode with the proposed algorithm. Let $n=6,r=3,\tau=1$, $C=<x^3+2x^2+(2+u)x+1+u,u(x+1)>$, and $\theta(u)=u$. In polynomial point of view, we have two input polynomial; one is of degree at most 2 over $\mathbb{F}_p+u\mathbb{F}_p$. As this polynomial needs 3 coefficients, we need 6 symbols in $\mathbb{F}_p$. The second polynomial is of degree 1 over $\mathbb{F}_p$. So it needs 2 symbols in $\mathbb{F}_p$. Hence, the number of symbols in $\mathbb{F}_p$ of the input of encoding is 8. For the output, it is a polynomial of degree 5 over $\mathbb{F}_p+u\mathbb{F}_p$. So the encoded string has 12 symbols over $\mathbb{F}_p$. Suppose that the encoder wants to transmit two strings $I=(4+2u,3u,1+u)\in(\mathbb{F}_5+u\mathbb{F}_5)^3$ and $J=(2,2)\in(\mathbb{F}_5+u\mathbb{F}_5)^2$. So

$$\begin{aligned}&Encode((4+2u,3u,1+u),(2,2))=\\&\quad((1+u)x^2+3ux+(4+2u))(x^3+2x^2+(2+u)x+1+u)+u(2x+2)(x+1)\\&\quad=(1+u)x^5+2x^4+(1+u)x^3+(4+4u)x^2+3x+4+3u.\end{aligned}$$

So the encoder sends $(4+3u,3,4+4u,1+u,2,1+u)$ through the channel.

Example 3: We show examples of principal skew cyclic codes with length 4 over F_3+uF_3 with $\theta(u)=-u$. For this, one can see that the factorisation of x^4-1 over F_3 is as follows.

$$x^4-1=(x+2)(x+1)(x^2+1) \quad (4)$$

There are two types of principal codes. If the generator is not monic, then $C=\langle u\bar{a}(x)\rangle$. Therefore, all of the nontrivial codes in this form are as follows.

$$\begin{aligned}&C_1=<u(x+2)> \quad or \quad C_2=<u(x+1)> \quad or \quad C_3=<u(x^2+1)>\\&C_4=<u(x^2+2)> \quad or \quad C_5=<u(x^3+x^2+x+1)>\\&C_6=<u(x^3+2x^2+x+2)>.\end{aligned}$$

The generator matrix G and the parity check matrix H of the code C_4 are as follows.

$$G=\begin{bmatrix}2u&0&u&0\\0&u&0&2u\end{bmatrix} \qquad H=\begin{bmatrix}0&1&0&1\\1&0&1&0\end{bmatrix}$$

On the other hand, if the generator of the code is monic, then $C=\langle g(x)+up(x)\rangle$ where $x^n-1=k*(g+up)$ for some $k\in R_n$. An example of such code is $C=\langle x^3+(u+1)*x^2+x+u+1\rangle$. The generator matrix and parity check matrix of this code are as follows.

$$G=\begin{bmatrix}u+1&1&u+1&1\end{bmatrix} \qquad H=\begin{bmatrix}1&2-u&0&0\\0&1&u+2&0\\0&0&1&2-u\end{bmatrix}$$

6 Gray images and codes with good parameters

One of our goals in this study was to obtain codes with good parameters over $\mathbb{F}_p$ from skew cyclic codes over R. To this end, we need a map from R to $\mathbb{F}_p^{\ell}$ for some positive integer ℓ. We use the map given in Zhu et al. (2017). For any integer ℓ, $1 \le \ell \le p$, define the Gray mapping as

$$\varphi_{\ell} \;:\; R \rightarrow \mathbb{F}_p^{\ell}$$
$$\varphi_{\ell}\left(a + ub\right) = \left(b, b + a, b + 2a, \ldots b + \left(\ell - 1\right) a\right).$$

This map is naturally extended to a map φ_{ℓ} from R^n to $\mathbb{F}_p^{\ell n}$.

For $c = a + ub \in R$, define the Gray weight of c to be

$$w\left(c\right) = \begin{cases} 0 & \text{if } c = 0 \\ \ell - 1 & \text{if } c = x - u\lambda x,\ x \in \mathbb{F}_p^{*},\ 0 \le \lambda \le \ell - 1 \\ \ell & \text{otherwise} \end{cases}$$

It is shown in Zhu et al. (2017) that φ_{ℓ} is a linear, distance preserving map from R^n to $\mathbb{F}_p^{\ell n}$. It is one-to-one if $\ell \ge 2$. Therefore, if C is a linear code over R with parameters (n, M, d) where d is the minimum Gray weight of C, then for $\ell \ge 2$ $\varphi_{\ell}(C)$ is a linear code over $\mathbb{F}_p$ with parameters $(n\ell, M, d)$. If C is a free code of dimension k over R, then $\varphi_{\ell}(C)$ is a linear code of dimension $2k$ over $\mathbb{F}_p$.

We searched over skew cyclic codes for $p = 3$ and $p = 5$ with generators of the form (2) in Theorem 14. Hence they are free codes over R with dimension $k = n - \deg(g(x))$ where $g(x)$ is a divisor of $x^n - 1$ in $R[x; \theta]$. Then we applied the Gray map described above to obtain linear codes over $\mathbb{F}_3$ and $\mathbb{F}_5$. For $p = 3$, there is only one non-trivial automorphism of R which is $\theta(a + ub) = a + 2ub$. For $p = 5$, there are three non-trivial automorphisms of R: $\theta(a + ub) = a + sub$, where $s = 2, 3$ or 4. We chose $s = 4$, so $\theta(a + ub) = a + 4ub$. As a result of a computer search which is carried out using Magma software, we obtained a number of codes with optimal or near optimal parameters. We list below a sample of these codes.

Example 4: Let $p = 3, n = 8$. The polynomial $g = x^3 + ux^2 + x + 1$ divides $x^8 - 1$ over $R = \mathbb{F}_3 + u\mathbb{F}_3$, hence it generates a free cyclic code of dimension 5 over R. Its image $\varphi_2(C)$ is a ternary linear code with parameters $[16, 10, 4]$ which, according to the database (http://www.codetables.de), is an optimal code over $\mathbb{F}_3$.

Example 5: Let $p = 3, n = 6$. The polynomial $g = x^4 + 2x^3 + 2ux^2 + x + u + 2$ divides $x^6 - 1$ over $R = \mathbb{F}_3 + u\mathbb{F}_3$, hence it generates a free cyclic code of dimension 2 over R. Its image $\varphi_2(C)$ is a ternary linear code with parameters $[12, 4, 6]$ and $\varphi_3(C)$ is a ternary linear code with parameters $[18, 4, 11]$. Both of these codes are optimal according to Code Tables (http://www.codetables.de).

Example 6: Let $p = 3, n = 11$. The polynomial $g = x^6 + x^4 + 2x^3 + 2x^2 + 2x + 1$ divides $x^{11} - 1$ over $R = \mathbb{F}_3 + u\mathbb{F}_3$, hence it generates a free cyclic code of dimension 5 over R. Its image $\varphi_2(C)$ is a ternary linear code with parameters $[22, 10, 6]$ which turns out to be a quasi-cyclic code. According to the database of best known quasi-twisted codes (which includes quasi-cyclic codes as a special case) (http://www.tec.hkr.se/∼chen/research/codes/searchqc2.htm), this is a new code in the class of quasi-twisted codes.

Example 7: Let $p = 3, n = 12$. The polynomial $g = x^5 + (u+1)x^4 + ux^3 + 2ux^2 + (2u+2)x + 2u + 2$ divides $x^{12} - 1$ over $R = \mathbb{F}_3 + u\mathbb{F}_3$, hence it generates a free cyclic code of dimension 7 over R. Its image $\varphi_2(C)$ is a ternary linear code with parameters $[24, 14, 6]$ which, according to Code Tables (http://www.codetables.de), has the parameters of a best known ternary linear code.

Example 8: Let $p = 5, n = 6$. The polynomial $g = x^4 + (3u+4)x^3 + 4ux^2 + (2u+1)x + u + 4$ divides $x^6 - 1$ over $R = \mathbb{F}_5 + u\mathbb{F}_5$, hence it generates a free cyclic code of dimension 2 over R. Its image $\varphi_3(C)$ is a linear code with parameters $[18, 4, 12]$ over $\mathbb{F}_5$. According to the database (http://www.codetables.de), this is an optimal linear code.

Example 9: Let $p = 5, n = 10$. The polynomial $g = x^8 + 3x^7 + (4u+3)x^6 + x^5 + 3ux^4 + 4x^3 + (2u+2)x^2 + 2x + u + 4$ divides $x^{10} - 1$ over $R = \mathbb{F}_5 + u\mathbb{F}_5$, hence it generates a free cyclic code of dimension 2 over R. Its images $\varphi_2(C)$, $\varphi_3(C)$, $\varphi_4(C)$, and $\varphi_5(C)$ are linear codes over $\mathbb{F}_5$ with parameters $[20, 4, 12]$, $[30, 4, 20]$, $[40, 4, 28]$ and $[50, 4, 37]$ respectively. Their minimum distances are within 1 or 2 units of the best known linear codes for their parameters. Moreover, for $g = x^8 + (4u+2)x^7 + (4u+3)x^6 + (3u+4)x^5 + 3ux^4 + (2u+1)x^3 + (2u+2)x^2 + (u+3)x + u + 4$, $\varphi_4(C)$ has parameters $[40, 4, 29]$.

7 Conclusion

In this paper, we studied skew cyclic codes over the ring $R = \mathbb{F}_p + u\mathbb{F}_p$ where p is an odd prime and $u^2 = 0$. We have classified all skew cyclic codes of arbitrary lengths as left $R[x;\theta]$-submodules of $R_n = R[x;\theta]/\langle x^n - 1\rangle$. Our classification is general and works for any value of n. Then we constructed generators for these codes. We also provided an encoding algorithm for skew cyclic codes over R. Additionally, we presented examples of skew cyclic codes whose Gray images are linear codes over $\mathbb{F}_p$ with optimal or near optimal parameters. One of these codes is a new code in the class of quasi-twisted codes.

References

Abualrub, T. and Siap, I. (2007) 'Cyclic codes over the rings $\mathbb{Z}_2 + u\mathbb{Z}_2$ and $\mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2$', *Designs, Codes and Cryptography*, Vol. 42, No.3, pp.273–287.

Abualrub, T., Ghrayeb, A., Aydin, N. and Siap, I. (2010) 'On the construction of skew quasi-cyclic codes', *IEEE Transactions on Information Theory*, Vol. 56, No. 5, pp.2081–2090.

Abualrub, T., Siap, I. and Aydin, N. (2014) '$\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes', *IEEE Transactions on Information Theory*, Vol. 60, No. 3, pp.1508–1514.

Bhaintwal, M. (2012) 'Skew quasi-cyclic codes over Galois rings', *Designs, Codes and Cryptography*, Vol. 62, No. 1, pp.85–101.

Bonnecaze, A. and Parampalli, U. (1999) 'Cyclic codes and self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$', *IEEE Transactions on Information Theory*, Vol. 45, No. 4, pp.1250–1255.

Boucher, D. and Ulmer, F. (2011) 'A note on the dual codes of module skew codes' *Cryptography and coding*, Springer Berlin Heidelberg, Oxford, UK, pp.230–243.

Boucher, D., Sole, P. and Ulmer, F. (2008) 'Skew constacyclic codes over Galois rings', *Advances in Mathematics of Communications*, Vol. 2, pp.273–292.

Calderbank, A.R. and Sloane, N.J. (1995) 'Modular and p-adic cyclic codes', *Designs, Codes and Cryptography*, Vol. 6, No. 1, pp.21–35.

Casavola, A., Famularo, D. and Franze, G. (2002) 'A feedback min-max MPC algorithm for LPV systems subject to bounded rates of change of parameters', *IEEE Transactions on Automatic Control*, Vol. 47, No. 7, pp.1147–1153.

Delphine, B., Geiselmann, W. and Ulmer, F. (2007) 'Skew-cyclic codes', *Applicable Algebra in Engineering, Communication and Computing* Vol. 18, No. 4, pp.379–389.

Jian, G. (2013) 'Skew cyclic codes over $\mathbb{F}_p + v\mathbb{F}_p$' *Journal of Applied Mathematics and Informatics*, Vol. 31, Nos. 3–4, pp.337–342.

Kanwar, P. and Lopez-Permouth, S.R. (1997) 'Cyclic codes over the integers modulo p_m', *Finite Fields and Their Applications*, Vol. 3, No. 4, pp.334–352.

Mandelbaum, D. (1969) 'An application of cyclic coding to message identification. *IEEE Transactions on Communication Technology*, Vol. 17, No. 1, pp.42–48.

McDonald, B.R. (1974) *Finite Rings with Identity*, Marcel Dekker Inc., New York.

Pless, V.S. and Qian, Z. (1996) 'Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$', *IEEE Transactions on Information Theory*, Vol. 42, No. 7, pp.1594–1600.

Tokiwa, K., Kasahara, M. and Namekawa, T. (1983) 'Burst-error-correction capability of cyclic codes', *Electronics and Communications in Japan (Part I: Communication6s)*, Vol. 66, No.11, pp.60–66.

Wolfmann, J. (2001) 'Binary images of cyclic codes over $\mathbb{Z}_4$', *IEEE Transactions on Information Theory*, Vol. 47, No. 5, pp.1773–1779.

Zhu, S-X., Kai, X-S. and Xu, X-Q. (2017) *Cyclic and 1-generator quasi-cyclic codes over* $\mathbb{F}_q + u\mathbb{F}_q$, http://media.paper.edu.cn/uploads/original_pdf/2012/02/15/A201202-617_1329311935.pdf (Accessed 12 December 2017).

Websites

Code Tables: Bounds on the parameters of various types of codes, http://www.codetables.de (Accessed 12 December, 2017).

Chen, E., Online Database of Quasi-Twisted Codes, http://www.tec.hkr.se/∼chen/research/codes/searchqc2.htm (Accessed 12 December, 2017).