Cyclic codes of arbitrary length over 
\[ F_q + uF_q + u^2 F_q + \ldots + u^{k-1} F_q \]

Mohammed M. Al-Ashker and Jianzhang Chen

Communicated by Ayman Badawi

MSC 2010 Classifications: 94B15.

Keywords and phrases: Cyclic codes, Codes over rings, Self-dual codes.

Abstract. In this paper, we study the structure of cyclic codes of an arbitrary length \( n \) over the ring \( F_q + uF_q + u^2 F_q + \ldots + u^{k-1} F_q \), where \( u^k = 0 \) and \( q \) is a power of prime. Also we study the rank for these codes, and we find their minimal spanning sets. This study is a generalization and extension of the works in references [9] and [12], the dual codes over the ring \( F_q + uF_q + u^2 F_q \), where \( u^3 = 0 \) are studied as well.

1 Introduction

Among the four rings of four elements, the Galois field \( F_4 \) and more recently the ring of integers modulo four \( Z_4 \) are the most used in coding theory. \( Z_4 \)-codes are renowned for producing good nonlinear codes by the Gray map, namely Kerdok, preparata or Goethals codes. The structure of cyclic codes over rings of odd length \( n \) has been discussed in Bonnecaze and Udaya [4], Calderbank [5], Dougherty and Shiromoto [8], and van Lint [13]. Calderbank and Sloane [6], and Pless [11] presented a complete structure of cyclic codes over \( Z_4 \) of odd length. In [3], Blackford studied cyclic codes of length \( n = 2k \) when \( k \) is odd. The cyclic codes over \( Z_4 \) of length a power of 2 are studied in [2]. They showed that the ring \( Z_4/N \) is not a principal ideal ring and hence ideals may have more than one generator. Ping Li and Shixin Zhu in [12], studied cyclic codes of arbitrary length over the ring \( F_q + uF_q \), with \( u^2 = 0 \) and \( F_q \) is a finite field of order \( q \) where \( q \) is a power of prime.

Let \( R_k \) be the ring \( F_q + uF_q + u^2 F_q + \ldots + u^{k-1} F_q \) with \( u^k = 0 \), where \( q \) is a power of prime \( p \).

In [1], Abualrub and Siap studied cyclic codes of an arbitrary length \( n \) over \( F_2 + uF_2 = \{ 0, 1, u, u + 1 \} \) where \( u^2 = 0 \) and over \( F_2 + uF_2 + u^2 F_2 = \{ 0, 1, u, u + 1, u^2, 1 + u^2, 1 + u, u + u^2 \} \) where \( u^3 = 0 \) and \( F_2 = \{ 0, 1 \} \). In [9], the authors Mohammed Al-Ashker and Mohammed Hamoudeh extend these results to rings of the form \( F_2 + uF_2 + u^2 F_2 + \ldots + u^{k-1} F_2 \) where \( u^k = 0 \).

A. Singh and P. kewat in [14] extend some of the results in [9] to the ring \( F_p + uF_p + u^2 F_p + \ldots + u^{k-1} F_p \) where \( u^k = 0 \), and \( F_p = \{ 0, 1, 2, \ldots, p - 1 \} \). In this paper, we study cyclic codes of an arbitrary length over \( F_q + uF_q + u^2 F_q + \ldots + u^{k-1} F_q \), where \( q \) is a power of prime \( p \) and \( u^k = 0 \), we also study their dual codes and find their properties over these rings. We give a unique set of generators for these codes as ideals in the ring \( R_k = R_k[x]/(x^n - 1) \). For this purpose, it is useful to obtain the divisors of \( x^n - 1 \), but this becomes difficult when the characteristic of the ring is not relatively prime to the length of the code, because then \( x^n - 1 \) does not factor uniquely over the ring \( F_q + uF_q + u^2 F_q + \ldots + u^{k-1} F_q \).

We show that the results of [12] concerning the codes over the ring \( F_q + uF_q \) with \( u^2 = 0 \) and of [9] concerning the codes over the ring \( F_2 + uF_2 + u^2 F_2 + \ldots + u^{k-1} F_2 \) with \( u^k = 0 \) are valid for \( R_k = F_q + uF_q + u^2 F_q + \ldots + u^{k-1} F_q \) with \( u^k = 0 \). The proofs of lemmas and Theorems in this paper are some what similar to those discussed in [12], [9] and slightly different from those discussed in [14].

The remaining part of this paper is organized as follows: In section 2, we give some basic definitions and results that are used in the sequel of this paper. In section 3, we study cyclic codes of an arbitrary length \( n \) over \( F_q + uF_q + u^2 F_q + \ldots + u^{k-1} F_q \). We find a unique set of generators for these codes. In section 4, we study the rank and find minimal spanning sets for these codes. In section 5, we study the dual codes of the codes over the ring \( F_q + uF_q + u^2 F_q \). In section 6, we include some examples of cyclic codes over \( R_k \).
2 Preliminaries

Let $F_q^n$ denote the vector space of all $n$-tuples over the finite field $F_q$. An $(n, M)$ code $C$ over $F_q$ is a subset of $F_q^n$ of size $M$. If $C$ is a $k$-dimensional subspace of $F_q^n$, then we will called an $[n, k]$ linear code over $F_q$.

A linear code $C$ of length $n$ over $F_q$ is cyclic provided that for each vector $c = (c_0c_1 \ldots c_{n-2}c_{n-1})$ in $C$, the vector $(c_{n-1}c_0 \ldots c_{n-2})$ obtained from $c$ by the cyclic shift of coordinates $i \mapsto i+1$ (mod $n$), is also in $C$.

A code of length $n$ over a commutative ring $R$ is a nonempty subset of $R^n$, and a code is linear over $R$ if it is an $R$-submodule of $R^n$.

A free module $C$ is a module with a basis (a linearly independent spanning set for $C$).

A linear code of length $n$ is cyclic if it is invariant under the automorphism $\sigma$ which is given by $\sigma(c_0, c_1, \ldots, c_{n-1}) = (c_{n-1}, c_0, \ldots, c_{n-2})$.

Definition 2.1. [7] An ideal $I$ of a ring $R$ is called principal if it is generated by one element. A ring $R$ is a principal ideal ring if its ideals are principal. $R$ is called a local ring if $R$ has a unique maximal right (left) ideal. Furthermore, a ring $R$ is called a right (left) chain ring if the set of all right (left) ideals of $R$ is a chain under set-theoretic inclusion. If $R$ is both a right and a left chain ring, we simply call $R$ a chain ring.

Definition 2.2. The ring $R_k = F_q[u]/\langle u^k \rangle = F_q + uF_q + u^2F_q + \ldots + u^{k-1}F_q$ is a commutative ring of $u^k$ elements with maximal ideal $uR_k$, where $u^k = 0$.

Since $u$ is nilpotent with nilpotent index $k$, we have

$$R_k \supset uR_k \supset u^2R_k \supset \ldots \supset u^kR_k = 0.$$ 

Moreover $R_k/uR_k \cong F_q$ is the residue field and $|uR_k| = q^{k−i}$, $0 \leq i \leq (k-1)$.

Denote $R_1 = F_q$, $R_2 = F_q + uF_q$, $R_3 = F_q + uF_q + u^2F_q$, etc.

Definition 2.3. Let $C_k$ be a code of length $n$ over the ring $R_k = F_q + uF_q + u^2F_q + \ldots + u^{k-1}F_q$ with $u^k = 0$, we mean an additive submodule of the $R_k$-module $R_k^n$.

A cyclic code of length $n$ over $R_k$ is an ideal in the ring $R_{k,n} = R_k[x]/\langle x^n − 1 \rangle$.

Definition 2.4. [1] Let $c = (c_0, \ldots, c_{n-1})$ and $u = (u_0, \ldots, u_{n-1})$ be any two vectors over a ring.

We define their inner product by

$$c \cdot u = c_0u_0 + \ldots + c_{n-1}u_{n-1}.$$ 

If $c \cdot u = 0$, then $c$ and $u$ are said to be orthogonal. We define the dual of a cyclic code $C$ to be the set

$$C^\perp = \{c \in R_k^n : c \cdot u = 0 \text{ for all } u \in C\}.$$ 

Notation: We write $a$ for $a(x)$, $g$ for $g(x)$, etc.

Proposition 2.1. [7] Let $R$ be a finite commutative ring, then the following conditions are equivalent:

(i) $R$ is a local ring and the maximal ideal $M$ of $R$ is principal.

(ii) $R$ is a local principal ideal ring.

(iii) $R$ is a chain ring.

Notation: all rings studied in this paper are commutative chain rings.

3 A generator Construction

The structure of cyclic codes over $R_i$ depends on cyclic codes over $R_{i-1}$ for $i = 2, 3, \ldots, k$ and the structure of cyclic codes over $R_2$ depends on cyclic codes over $R_1 = F_q$.

By following results in [1] and [9], let $C_1$ be a cyclic code in $R_{k,n} = R_k[x]/\langle x^n − 1 \rangle$.

Define $\psi_1 : R_k \to R_{k-1}$ by $\psi_1(a) = a$, where $a^k = 0 \mod q$. $\psi_1$ is a ring homomorphism that can be extended to a homomorphism $\phi_1 : C_1 \to R_{k-1,n} = R_{k-1}[x]/\langle x^n − 1 \rangle$ defined by

$$\phi_1(c_0 + c_1x + \ldots + c_{n-1}x^{n-1}) = \psi_1(c_0) + \psi_1(c_1)x + \ldots + \psi_1(c_{n-1})x^{n-1}.$$ 

Let $J_1 = \{r(x) : u^{k-1}r(x) \in \ker \phi_1\}$, $J_1$ is an ideal in $R_{1,n} = R_1[x]/\langle x^n − 1 \rangle = F_q[x]/\langle x^n − 1 \rangle$ and and hence a cyclic code in $F_q[x]/\langle x^n − 1 \rangle$. So $J_1 = \langle a_{k-1}(x) \rangle$ and $\ker \phi_1 = \langle u^{k-1}a_{k-1}(x) \rangle$.
with \(a_{k-1}(x)|(x^n - 1)\).

Let \(C_0\) be a cyclic code in \(R_{k-1,n} = R_{k-1}[x]/(x^n - 1)\).

Define \(\psi_2 : R_{k-1} \to R_{k-2}\) by \(\psi_2(a) = a\). \(\psi_2\) is a ring homomorphism that can be extended to a homomorphism \(\phi_2 : C_2 \to R_{k-2}[x]/(x^n - 1)\) defined by

\[
\phi_2(c_0 + c_1 x + \ldots + c_{n-1} x^{n-1}) = \psi_2(c_0) + \psi_2(c_1)x + \ldots + \psi_2(c_{n-1})x^{n-1}.
\]

\[\ker \phi_2 = \{u^{k-2}r(x) : r(x) \in F_q[x]\}.
\]

Let \(J_2 = \{r(x) = u^{k-2}r(x) \in \ker \phi_2\}\) is an ideal in \(R_{1,n} = F_q[x]/(x^n - 1)\) and hence a cyclic code in \(F_q[x]/(x^n - 1)\). So \(J_2 = \langle a_{k-2}(x) \rangle\) and hence \(\ker(\phi_2) = \langle u^{k-2}a_{k-2}(x) \rangle\) with \(a_{k-2}(x)|(x^n - 1)\).

Let \(C_1\) be a cyclic code in \(R_{k-2,n} = R_{k-2}[x]/(x^n - 1)\).

Define \(\psi_3 : R_{k-2} \to R_{k-3}\) by \(\psi_3(a) = a\). \(\psi_3\) is a ring homomorphism that can be extended to a homomorphism \(\phi_3 : C_3 \to R_{k-3}[x]/(x^n - 1)\). Continue in the same way as above until we define \(\psi_{k-1} : R_2 \to R_1 = F_q\) by \(\psi_{k-1}(a) = a^q\). \(\psi_{k-1}\) is a ring homomorphism because \((a + b)^q = a^q + b^q\) in \(R_2\) and in \(F_q\).

Extend \(\psi_{k-1}\) to a homomorphism \(\phi_{k-1} : C_{k-1} \to F_q[x]/(x^n - 1) = R_{1,n}\) defined by

\[
\phi_{k-1}(c_0 + c_1 x + \ldots + c_{n-1} x^{n-1}) = \psi_{k-1}(c_0) + \psi_{k-1}(c_1)x + \ldots + \psi_{k-1}(c_{n-1})x^{n-1} - \psi_{k-1}(c_0) + c_1 x + c_2 x^2 + \ldots + c_{n-1} x^{n-1} = c_0 + c_1 x + c_2 x^2 + \ldots + c_{n-1} x^{n-1},
\]

where \(C_{k-1}\) is a cyclic code in \(R_{2,n} = R_{2}[x]/(x^n - 1)\), where \(R_2 = F_q + uF_q\) with \(u^2 = 0\) mod \(q\).

\[
\ker \phi_{k-1} = \{ur(x) : r(x) \text{ is a polynomial in } F_q[x]/(x^n - 1)\}
\]

\[= \langle(ua_1(x)) \rangle \text{ with } (ua_1(x)) \langle x^n - 1 \rangle.
\]

The image of \(\phi_{k-1}\) is also an ideal and hence a cyclic code over \(F_q\) generated by \(g(x)\) with \(g(x)|(x^n - 1)\). The cyclic code over \(R_2 = F_q + uF_q\) have the form in the following lemma:

**Lemma 3.1.** [12] Let \(C_{k-1}\) an arbitrary ideal of ring \(R_{2,n}\) (i.e., it’s an arbitrary cyclic code of arbitrary length \(n\) over ring \(R_2\)), then there only exits \(a_1(x)|g(x)|x^n - 1\), and the polynomials \(g(x), a_1(x), p(x)\) in \(F_q[x]\) with \(\deg a_1 > \deg p\), such that \(C_{k-1} = \langle g(x) + up(x), ua_1(x) \rangle\).

Note that \(a_1\langle p^{x^n - 1}/g \rangle\) because

\[
\phi_{k-1}(x^n - 1) = \phi_{k-1}(up(\frac{x^n - 1}{g})) = 0.
\]

\[
\Rightarrow (up\frac{x^n - 1}{g}) \in \ker \phi_{k-1} = \langle(ua_1(x)) \rangle g(x).
\]

**Lemma 3.2.** If \(C_{k-1} = \langle g(x) + up(x), ua_1(x) \rangle\) over \(R_2 = F_q + uF_q\) with \(u^2 = 0\) mod \(q\), and \(g(x) = a_1(x)\) with \(\deg g(x) = r\), then \(C_{k-1} = \langle g(x) + up(x) \rangle\) and \(\langle g + up \rangle \langle x^n - 1 \rangle\) in \(R_2[x]\).

**Proof.** Since \(u(g + up) = u\) and \(g = a\) with \(\deg g(x) = r\), then \(C_{k-1} = \langle g(x) + up \rangle\) and \(\langle g + up \rangle \langle x^n - 1 \rangle\) in \(R_2[x]\).

**Lemma 3.3.** (1) Let \(C_{k-2}\) be a cyclic code in \(R_{3,n}\), then \(C_{k-2} = \langle g + up_1 + u^2p_2, ua_1 + u^2q_1, u^2a_2 \rangle\) with \(a_2|a_1|g|(x^n - 1)\), \(a_1(x)|p_1(x)|\langle 2^{n-1}/g(x) \rangle \mod q\), \(a_2|q_1(x^{n-1}/g), a_2|p_1(x^{n-1}/g)\) and \(a_2|p_2(\frac{x^n - 1}{g})\). We may assume that \(\deg p_2 < \deg a_2\), \(\deg q_1 < \deg a_2\), \(\deg p_1 < \deg a_1\).

(2) A cyclic code over the ring \(R_{3,n}\) can be written uniquely as \(C_{k-2} = \langle g + up_1 + u^2p_2, ua_1 + u^2q_1, u^2a_2 \rangle\). (3) If \(C_{k-2} = \langle g + up_1 + u^2p_2, ua_1 + u^2q_1, u^2a_2 \rangle\) over \(R_3 = F_q + uF_q + u^2F_q\) with \(u^3 = 0\), and \(a_2 = g\), then \(C_{k-2} = \langle g + up_1 + u^2p_2 \rangle\) and \(\langle g + up_1 + u^2p_2 \rangle \langle x^n - 1 \rangle\) in \(R_3\).

(4) If \(n\) is relatively prime to \(q\), then \(C_{k-2} = \langle g, ua_1, u^2a_2 \rangle = \langle g + ua_1 + u^2a_2 \rangle\) over \(R_3\).

**Proof.** (1) Since the image of \(\phi_{k-2}\) is an ideal in \(R_{2,n} = R_2[x]/(x^n - 1)\) (where \(R_2 = F_q + uF_q\) with \(u^2 = 0\)), then \(\im(\phi_{k-2}) = \langle g(x) + up_1(x), ua_1(x) \rangle\) with \(\langle a_1(x)g(x)|(x^n - 1)\), and \(a_1(x)|p_1(x)|\langle 2^{n-1}/g(x) \rangle\). Also, \(\ker(\phi_{k-2}) = \langle u^2a_2(x) \rangle\) with \(a_2(x)\langle x^n - 1 \rangle\). Since \(a_2|a_1\) in \(\ker(\phi_{k-2}) = \langle u^2a_2 \rangle\), then the cyclic code \(C_{k-2}\) over \(R_3 = F_q + uF_q + u^2F_q\) with \(u^3 = 0\) is \(C_{k-2} = \langle g + up_1 + u^2p_2, ua_1 + u^2q_1, u^2a_2 \rangle\) with \(a_2|a_1|g|(x^n - 1)\), \(a_1(x)|p_1(x)|\langle 2^{n-1}/g(x) \rangle \mod q\). Since \(\phi_{k-2}(\frac{x^n - 1}{g}(ua_1 + u^2q_1)) = \phi_{k-2}(u^2q_1\frac{x^n - 1}{g}) = 0\). Hence \((u^2q_1\frac{x^n - 1}{g}) \in \ker \phi_{k-2} = \langle u^2a_2 \rangle\).
This implies that $a_2(x)|(q_1 \frac{x^n-1}{g(x)})$. Similarly, we have $a_1(x)|p_1(x)(\frac{x^n-1}{g(x)})$ mod $q$. Further, 
$\phi_k-2\left( \left( \frac{x^n-1}{g(x)} \right) (g+up_1+u^2p_2) \right) = \phi_k-2\left( \left( \frac{x^n-1}{g(x)} \right) u^2p_2 \right) = 0$. Thus, $a_2|p_2(\frac{x^n-1}{g(x)})(\frac{x^n-1}{a_1(x)})$.

We may assume that $\deg p_2 < \deg a_2$, $\deg q_1 < \deg a_2$, $\deg p_1 < \deg a_1$ because if $e = (a,b)$, then $e = (a,b + de)$ for any $d$.

(2) The proof is similar to Lemma 6 in [1].

(3) Since $a_2 = g$, then $a_1 = a_2 = g$. From Lemma 3.1 we get that $(g + up_1)(x^n - 1)$ in $R_2$ and $C_{k-2} = (g + up_1 + u^2p_2, u^2a_2)$.

(4) The proof is similar to Lemma 8 in [1].

Following the same process we find the cyclic code $C_{k-3}$ over $R_4 = F_q + uF_q + u^2F_q + u^3F_q$ with $(u^4 = 0)$. So, since the image of $\phi_k-3$ is an ideal in $R_{3,n} = R_3[x]/(x^n - 1)$ (where $R_3 = F_q + uF_q + u^2F_q$ with $u^3 = 0$), then $Im(\phi_{k-3}) = \langle g(x) + up_1(x) + u^2p_2(x), u_1(x) + u^2q_1(x), u^2a_2(x) \rangle$ with $a_2|p_2(\frac{x^n-1}{g(x)})(\frac{x^n-1}{a_1(x)})$ and $a_2|p_2(\frac{x^n-1}{a_1(x)})(\frac{x^n-1}{g(x)})$. Also $\ker(\phi_{k-3}) = \langle u^3a_3(x) \rangle$ with $a_3(x)|p_3(x)(\frac{x^n-1}{g(x)})(\frac{x^n-1}{a_1(x)})$. Moreover $\deg p_3 < \deg a_3$, $\deg q_2 < \deg a_2$, $\deg l_1 < \deg a_2$, $\deg p_2 < \deg a_2$, $\deg q_1 < \deg a_1$.

**Lemma 3.4.** If $C_{k-3} = \langle g + up_1 + u^2p_2 + u^3a_1, u_1 + u^2q_1 + u^3q_2 + u^2a_2 + u^3a_3 \rangle$ over $R_4 = F_q + uF_q + u^2F_q + u^3F_q$ with $(u^4 = 0)$, and $a_3 = g$, then $C_{k-3} = \langle g + up_1 + u^2p_2 + u^3a_3 \rangle$ and $(g + up_1 + u^2p_2 + u^3a_3)(x^n - 1)$ in $R_4$.

**Proof.** Since $a_3 = g$, then $a_1 = a_2 = a_3 = g$. From Lemma 3.3 we get that $(g + up_1 + u^2p_2)(x^n - 1)$ in $R_2$ and $C_{k-3} = \langle g + up_1 + u^2p_2 + u^3a_1, u_1 + u^2q_1 + u^3q_2, u^2a_2 + u^3a_3 \rangle$. The rest of the proof is similar to Lemma 3.3.

**Lemma 3.5.** If $n$ is relatively prime to $q$, then the cyclic code $C_{k-3}$ over $R_4$ can be written as

$$C_{k-3} = \langle g, ua_1, u^2a_2, u^3a_3 \rangle = \langle g + ua_1 + u^2a_2 + u^3a_3 \rangle$$

**Proof.** The proof is similar to Lemma 3.5 in [9].

From all the above discussion, we can construct any cyclic code $C_1$ over $R_k$, $k \geq 4$ by using the same process and induction on $k$ to get the following theorem:

**Theorem 3.6.** Let $C_1$ be a cyclic code in $R_k, n = R_k[x]/(x^n - 1)$, $R_k = F_q + uF_q + u^2F_q + \ldots + u^{k-1}F_q$ with $u^k = 0$.

1. If $n$ is relatively prime to $q$, then $R_k, n$ is a principal ideal ring and $C_1 = \langle g, ua_1, u^2a_2, \ldots, u^{k-1}a_{k-1} \rangle = \langle g, ua_1 + u^2a_2 + \ldots + u^{k-1}a_{k-1} \rangle$ where $g(x), a_1(x), a_2(x), \ldots, a_{k-1}(x)$ are polynomials over $F_q$ with $a_{k-1}(x)|a_{k-2}(x) \ldots |a_2(x)|a_1(x)|g(x)$.

2. If $n$ is not relatively prime to $q$, then
   a. $C_1 = \langle g + up_1 + u^2p_2 + \ldots + u^{k-1}p_{k-1} \rangle$ where $g(x), p_1(x)$ are polynomials over $F_q$.

   b. $C_1 = \langle g + up_1 + u^2p_2 + \ldots + u^{k-1}p_{k-1}, u^{k-1}a_{k-1} \rangle$ where $a_{k-1}|p_1(x)(x^n - 1), (g + up_1)(x^n - 1)$ in $R_k$, $p_1(x)|p_1(x)(x^n - 1)$ and $\deg p_1 < \deg p_{k-1}$ for all $2 \leq i \leq k - 1$.

   OR

   c. $C_1 = \langle g + up_1 + u^2p_2 + \ldots + u^{k-1}p_{k-1}, u_1 + u^2q_1 + \ldots + u^{k-1}q_{k-1}, u^2a_2 + u^3a_3 \rangle$
u^{k-1}a_k-3, \ldots, u^k-2a_{k-2} + u^{k-1}a_{k-1} \) with \( a_k-1|a_{k-2} \mid \ldots \mid a_2|a_1|g|(x^n - 1), \\
a_k-2|p_1(x^n - 1), a_k-1|\ldots, a_2|a_1|p_{k-1}(x^{n-1} - 1) \ldots (x^{n-1} - 1).

Moreover \( \deg p_{k-1} < \deg a_{k-1}, \ldots, \deg t_1 < \deg a_{k-1}, \ldots \) and \( \deg p_1 < \deg a_{k-2} \).

Motivated by the work in [7], [10], the structure of cyclic codes over \( R_k \) of length \( n \) relatively prime to \( q \) can be given in another way as follows: Let \( R_k \) be a finite chain ring with the maximal ideal \( < u > \) and \( k \) be the nilpotent index of \( u \). Assume that \( n \) is not divisible by the characteristic of the residue field \( \mathbb{F}_q \), so that \( x^n - 1 \) has a unique decomposition as a product of basic irreducible pairwise coprime polynomials in \( R_k[x] \) (cf. proposition 2.7 in [7]).

**Theorem 3.7.** Let \( C \) be a cyclic code of length \( n \) relatively prime to \( q \) over \( R_k \), which has maximal ideal \( < u > \) and \( k \) is the nilpotent index of \( u \). Then there exist polynomials \( g_0, g_1, \ldots, g_{k-1} \) in \( R_k[x] \) such that \( C = \langle g_0, g_1, \ldots, u^{k-1}g_{k-1} \rangle \) and \( g_{k-1}|g_{k-2} \ldots |g_0 |(x^n - 1) \).

**Theorem 3.8.** Let \( C \) be a cyclic code of length \( n \) relatively prime to \( q \) over \( R_k \), which has maximal ideal \( < u > \) and \( k \) is the nilpotent index of \( u \), \( F = F_1 + uF_2 + \ldots + u^{k-1}F_k \), where \( F_i(x) \) is a factor of \( x^n - 1 \), \( F_i(x) = \frac{x^{n_i} - 1}{x - 1} \). Then \( C = \langle F \rangle \).

**Corollary 3.9.** The ring \( R_k[x]/\langle x^n - 1 \rangle \) with \( n \) relatively prime to \( q \) is a principal ideal ring.

## 4 Ranks and minimal spanning sets for cyclic codes over \( R_k \)

In this section we will discuss the ranks and minimal spanning sets for cyclic codes over \( R_k \). In [9], the authors have shown the following Theorem:

**Lemma 4.1.** [9] Let \( C \) be a cyclic code of even length \( n \) over \( R_k = Z_2 + uZ_2 + u^2Z_2 + \ldots + u^{k-1}Z_2 \) with \( u^k = 0 \). The generators on the polynomial algebras as in theorem 3.6.

1. If \( C_1 = \langle g + up_1 + u^2p_2 + \ldots + u^{k-1}p_{k-1} \rangle \), \( \deg g(x) = r \), then \( C_1 \) is a free module with \( \gcd(x) = n - r \) and basis \( \beta = \langle g + up_1 + u^2p_2 + \ldots + u^{k-1}p_{k-1}, x^{n-r}g - u^r + u^{2r} + \ldots + u^{k-1}p_{k-1} \rangle \).

2. If \( C_1 = \langle g + up_1 + u^2p_2 + \ldots + u^{k-1}p_{k-1}, a_1 + u^2a_1 + \ldots + u^{k-1}a_1, u^{-1}a_1 \rangle \) with \( \deg g(x) = r, \deg a_1(x) = r, \deg a_2(x) = r_3 \), \( \gcd(x) = n - r \) and a minimal spanning set given by \( \chi = \langle x^{r_1} - 1, x^{r_2} - 1, x^{r_3} - 1, x^{r_4} - 1 \rangle \).

3. If \( C_1 = \langle g + up_1 + u^2p_2 + \ldots + u^{k-1}p_{k-1}, a_1 - 1 \rangle \) with \( \deg g(x) = r, \deg a_1 - 1 = t \) then \( C_1 \) has rank \( \gcd(x) = n - t \) and a minimal spanning set given by \( \Gamma = \langle x^{r_1} - 1, x^{r_2} - 1, x^{r_3} - 1 \rangle \).

Now we use the technology to obtain the similar results:

**Theorem 4.2.** Let \( C_1 \) be a cyclic code of length \( n \) not relatively prime to \( q \) over \( R_k = F_q + uF_q + u^2F_q + \ldots + u^{k-1}F_q \) with \( u^k = 0 \). The constraints on the generator polynomials as in theorem 3.6.

1. If \( C_1 = \langle g + up_1 + u^2p_2 + \ldots + u^{k-1}p_{k-1} \rangle \), \( \deg g(x) = r \), then \( C_1 \) is a free module with \( \gcd(x) = n - r \) and basis \( \beta = \langle g + up_1 + u^2p_2 + \ldots + u^{k-1}p_{k-1}, x^{n-r}g - u^r + u^{2r} + \ldots + u^{k-1}p_{k-1} \rangle \).

2. If \( C_1 = \langle g + up_1 + u^2p_2 + \ldots + u^{k-1}p_{k-1}, a_1 + u^2a_1 + \ldots + u^{k-1}a_1, u^{-1}a_1 \rangle \) with \( \deg g(x) = r_1, \deg a_1(x) = r_2, \deg a_2(x) = r_3 \), \( \gcd(x) = n - r \) and a minimal spanning set given by \( \Gamma = \langle x^{r_1} - 1, x^{r_2} - 1, x^{r_3} - 1 \rangle \).
\[ \chi = \left\{ (g + up_1 + u^2p_2 + \ldots + u^{k-1}p_{k-1}), \ x(g + up_1 + u^2p_2 + \ldots + u^{k-1}p_{k-1}), \ \ldots, \ x^{n-r-1}(g + up_1 + u^2p_2 + \ldots + u^{k-1}p_{k-1}), \ \right\} \]

(3) If \( C = \langle g + up_1 + u^2p_2 + \ldots + u^{k-1}p_{k-1} \rangle \) with \( \deg g(x) = r, \deg ak_1 - t \) then \( C \) has rank \( C(n) = n - t \) and a minimal spanning set given by

\[ \Gamma = \left\{ (g + up_1 + u^2p_2 + \ldots + u^{k-1}p_{k-1}), \ x(g + up_1 + u^2p_2 + \ldots + u^{k-1}p_{k-1}), \ \ldots, \ x^{n-r-1}(g + up_1 + u^2p_2 + \ldots + u^{k-1}p_{k-1}), \ \right\} \]

\[ \text{Proof. The proof is similar to the prove of lemma (4.1) in [9].} \]

5 Dual codes over rings \( F_q + uF_q + u^2F_q \)

This section studies the dual codes of cyclic codes over \( R_3 = F_q + uF_q + u^2F_q \). Let \( I \) be the ideal of \( R_{3,n} = R_3[x]/\langle x^n - 1 \rangle \), where \( 2 \leq i \leq k \), then the set \( A(I) = \{ g(x) : f(x)g(x) = \langle 0 \rangle, \forall f(x) \in I \} \) is called the annihilator of \( I \) in \( R_{3,n} \); reciprocal polynomial of degree \( r \) of the polynomial \( f(x) = c_0 + c_1x + \cdots + c_0x^r \) is defined as \( f^*(x) = c_r + c_{r-1}x + \cdots + c_0x^r \). It's obvious that if \( C \) is a cyclic code with associated ideal \( I \) then the associate ideal of \( C^\perp \) is

\[ A(I)^* = \{ g^*(x) : \forall g(x) \in I \}. \]

**Lemma 5.1.** [12] If \((n, p) \neq 1\), let \( C_{k-2} \) be an arbitrary ideal of the ring \( R_{2,n} = R_2[x]/\langle x^n - 1 \rangle \) (i.e., it's an arbitrary cyclic code of arbitrary length \( n \) over ring \( R_2 \)), then there only exits \( a_1(x) \mid g(x) \mid x^n - 1 \), and the polynomials \( g(x), a_1(x), p_1(x) \) in \( F_q[x] \) with \( \deg g_1 > \deg p_1 \), such that

\[ C_{k-2} = \langle g(x) + up_1, u_1 \rangle \]

(1) If \( a(x) = g(x) \), then \( C_{k-1} = \langle g + up \rangle, \) and \( (g + up) \mid x^n - 1 \) in \( R_2[x] \), thus \( A(C_{k-1}) = \langle x^{n-1} \rangle \), also have \( C_{2,k-1} = \left((\frac{x^{n-1}}{a})^*\right) \), \( u(x^{n-1})^* \)

(II) Otherwise, \( C_{2,k-1} \) is a cyclic code in \( R_{3,n} \), then

(1) If \((n, p) \neq 1 \) and \( C_{k-2} = \langle g + up_1 + u^2p_2 \rangle \) with \( a_2 | g | (x^{n-1}) \) mod \( q \), \( (g + up) \mid x^n - 1 \), and \( \deg p_2 < \deg p_1 \), then \( A(C_{k-2}) = \langle \frac{x^{n-1}}{a} \rangle \), also have \( C_{2,k-2} = \left((\frac{x^{n-1}}{a})^*\right) \)

(II) If \((n, p) \neq 1 \) and \( C_{k-2} = \langle g + up_1 + u^2p_2, u_1 a_2 \rangle \) with \( a_2 | g | (x^{n-1}) \) mod \( q \), \( (g + up) \mid x^n - 1 \), \( g(x) \mid p_1(x) \mid x^{n-1} \), \( a_1(x) \mid p_1(x) \mid x^{n-1} \), and \( \deg g_2 < \deg g_2 \), then

\[ A(C_{k-2}) = \langle \frac{x^{n-1}}{a_2} \rangle \]

Also have \( C_{2,k-2} = \left((\frac{x^{n-1}}{a_2})^*\right) \)

(III) \( C_{2,k-2} = \langle g + up_1 + u^2p_2, u_1 a_2 \rangle \) with \( a_2 | g | (x^{n-1}) \), \( a_1(x) \mid p_1(x) \mid x^{n-1} \) mod \( q \), \( \deg g_2 < \deg g_2 \), \( \deg q_1 < \deg q_2 \), \( \deg q_1 < \deg q_2 \), then

\[ A(C_{k-2}) = \langle \frac{x^{n-1}}{a_2} \rangle \]

Also have \( C_{2,k-2} = \left((\frac{x^{n-1}}{a_2})^*\right) \)

\[ \text{Proof. (I) Since } (g + up_1 + u^2p_2) \mid (x^n - 1), \text{ the proof of the conclusion is similar to the generator of dual codes in the ring } R_1. \]

\[ \text{(II) Let } D = \langle \frac{x^{n-1}}{a_2} \rangle \text{, it is easy to prove that } \]

\[ \frac{x^{n-1}}{a_2} \text{, } u(x^{n-1})^* \in A(C_{k-2}), \text{ } u \in A(C_{k-2}). \]

Since \( A(C_{k-2}) \) is an ideal of the ring of \( R_{3,n} \), we assume that \( A(C_{k-2}) = \langle h + uv_1 + u^2v_2, u^2d_2 \rangle \)

\[ \text{Since } (h + uv_1 + u^2v_2)(g + up_1 + u^2p_2) = 0, \text{ and } (h + uv_1 + u^2v_2)(u^2a_2) = 0, \text{ then } \]

\[ a_2h = 0, gh = 0, gv_1 + p_1h = 0, gv_2 + p_1v_1 + p_2h = 0. \]
From the above equalities, we assume that 

\[ h = \varphi(x) \frac{(x^{n-1})^3}{ga_2}, \]

and we can obtain that 

\[ v_1 = -p_1 \varphi(x) \frac{(x^{n-1})^3}{g^2 a_2}, \quad v_2 = \varphi \frac{p_1(x^{n-1})^3}{ga_2} - \varphi \frac{p_2(x^{n-1})^3}{a_2}. \]

we also can get 

\[ v_2 - \varphi \frac{p_1(x^{n-1})^3}{ga_2} + \varphi \frac{p_1(x^{n-1})^3}{a_2} = x^{n-1} \frac{g}{g}, \text{ i.e. } v_2 = \varphi \frac{p_1(x^{n-1})^3}{ga_2} - \varphi \frac{p_1(x^{n-1})^3}{a_2} + x^{n-1} \frac{g}{g}. \]

Then

\[
h + u v_1 + u^2 v_2 = \varphi(x) \frac{(x^{n-1})^2}{ga_2} - up_1 \varphi(x) \frac{(x^{n-1})^2}{g^2 a_2} + u^2 \varphi \frac{p_1(x^{n-1})^2}{ga_2} - u^2 \varphi \frac{p_2(x^{n-1})^2}{a_2} + u^2 x^{n-1} \frac{g}{g},
\]

which implies that \( h + u v_1 + u^2 v_2 \in D \), it is easy to prove that \( u^2 d_2 \in D \), then \( A(C_{k-2}) \in D \).

Hence \( A(C_{k-2}) = \langle \langle (x^{n-1})^3 - u \frac{p_1(x^{n-1})^3}{a_2} + u^2 \frac{p_1(x^{n-1})^3}{a_2} - u^2 \frac{p_2(x^{n-1})^3}{a_2}, u \frac{x^{n-1}}{g} \rangle \rangle \),

and \( C_{k-2} = \langle \langle (x^{n-1})^3 - u \frac{p_1(x^{n-1})^3}{a_2} + u^2 \frac{p_1(x^{n-1})^3}{a_2} - u^2 \frac{p_2(x^{n-1})^3}{a_2}, u \frac{x^{n-1}}{g} \rangle \rangle, (x^{n-1})^3 \rangle \).

(III)Let \( D_1 = \langle \langle (x^{n-1})^3 - u \frac{p_1(x^{n-1})^3}{a_2} + u^2 \frac{p_1(x^{n-1})^3}{a_2} - u^2 \frac{p_2(x^{n-1})^3}{a_2}, u \frac{x^{n-1}}{g} \rangle \rangle \),

it is easy to prove that 

\[
(\frac{(x^{n-1})^3}{ga_2} - u \frac{p_1(x^{n-1})^3}{a_2} + u^2 \frac{p_1(x^{n-1})^3}{a_2} - u^2 \frac{p_2(x^{n-1})^3}{a_2} \in A(C_{k-2}), (x^{n-1})^3 \rangle \rangle = \frac{\delta x^{n-1}}{g}.
\]

Since \( A(C_{k-2}) = \langle \langle (x^{n-1})^3 \rangle \rangle, (x^{n-1})^3 \rangle \rangle \) is an ideal of the ring of \( R_{3, n} \), we assume that \( A(C_{k-2}) = \langle \langle h + u v_1 + u^2 v_2, u d_1 + u^2 l_1, u^2 d_2 \rangle \rangle \).

Since \( (h + u v_1 + u^2 v_2)(g + p_1 + u^2 p_2) = 0, (h + u v_1 + u^2 v_2)(u a_1 + u^2 g_1) = 0, (h + u v_1 + u^2 v_2)(u a_2) = 0, (g + p_1 + u^2 p_2)(u d_1 + u^2 l_1) = 0, (u a_1 + u^2 q_1)(u d_1 + u^2 l_1) = 0 \)

and \( (h + u v_1 + u^2 v_2)(u a_2) = 0 \), then

\[
a_2 h = 0, h a_1 = 0, h q_1 + a_1 v_1 = 0, gh = 0, g v_1 + p_1 h = 0, g v_2 + p_1 v_1 + p_2 h = 0.
\]

From the above equalities, we assume that \( h = \eta(x) \frac{(x^{n-1})^3}{ga_2} \),

and we can obtain that 

\[ v_1 = -p_1 \eta(x) \frac{(x^{n-1})^3}{g a_2} + \varphi \frac{p_1(x^{n-1})^3}{a_2} - \eta(x) \frac{p_1(x^{n-1})^3}{g a_2} \]

We also can get 

\[ v_2 = -\eta(x) \frac{p_1(x^{n-1})^3}{g a_2} + \varphi \frac{p_1(x^{n-1})^3}{a_2} = \delta x^{n-1} \frac{g}{g}, \text{ i.e. } v_2 = \eta(x) \frac{p_1(x^{n-1})^3}{g a_2} - \eta(x) \frac{p_1(x^{n-1})^3}{g a_2} + \delta x^{n-1} \frac{g}{g}. \]

Then

\[
h + u v_1 + u^2 v_2 = \eta(x) \frac{(x^{n-1})^3}{ga_2} - up_1 \eta(x) \frac{(x^{n-1})^3}{g^2 a_2} + u^2 \eta(x) \frac{p_1(x^{n-1})^3}{ga_2} - u^2 \eta(x) \frac{p_2(x^{n-1})^3}{a_2} + u^2 x^{n-1} \frac{g}{g},
\]

which implies that \( h + u v_1 + u^2 v_2 \in D \), it is easy to prove that \( u d_1 + u^2 l_1 \in D \), and \( u^2 d_2 \in D \),

then \( A(C_{k-2}) \in D \).

Hence \( A(C_{k-2}) = \langle \langle (x^{n-1})^3 - u \frac{p_1(x^{n-1})^3}{a_2} + u^2 \frac{p_1(x^{n-1})^3}{a_2} - u^2 \frac{p_2(x^{n-1})^3}{a_2}, u \frac{(x^{n-1})^3}{g_1} - u^2 \frac{p_1(x^{n-1})^3}{a_1}, u^3 \frac{x^{n-1}}{g} \rangle \rangle \),

and \( C_{k-2} = \langle \langle (x^{n-1})^3 - u \frac{p_1(x^{n-1})^3}{g a_2} + u^2 \frac{p_1(x^{n-1})^3}{g a_2} - u^2 \frac{p_2(x^{n-1})^3}{g a_2}, (u \frac{(x^{n-1})^3}{g a_2} - u^2 \frac{p_1(x^{n-1})^3}{a_1})^*, (u^3 \frac{x^{n-1}}{g})^* \rangle \rangle. \]

6 Examples

Example 6.1. Cyclic codes of length 3 over \( F_3 + u F_3 + u^2 F_3 + u^3 F_3 \) with \( u^4 = 0 \).

Now, \( x^3 - 1 = (x + 2)^3 - g(x)^3 \).

The Nonzero cyclic codes of length 3 over \( F_3 + u F_3 + u^2 F_3 + u^3 F_3 \) with generator polynomials are on the following table 1:
The nonzero free/non free module cyclic codes over $x^2, 3$:

Example 6.2. If $n = 4$ over $F_3 + uF_3 + u^2F_3 + u^3F_3$, with $u^3 = 0$, then $x^4 - 1 = (x + 1)(x + 2)(x^2 + 1) = f_1(x)f_2(x)f_3(x)$. The nonzero free/non free module cyclic codes over $F_3 + uF_3 + u^2F_3$ are on the following tables 2,3:

<table>
<thead>
<tr>
<th>Non zero generator polynomial(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(1), (f_1), (f_2), (f_1 + u), (f_1 + u), (f_1 + u), (f_1 + u), (f_1 + u), (f_1 + u)$</td>
</tr>
<tr>
<td>$(f_2 + u(c_0 + c_1x + c_2x^2)), (f_1f_2 + u(c_0 + c_1x + c_2x^2))$</td>
</tr>
<tr>
<td>$(f_2f_3 + u(c_0 + c_1x + c_2x^2), (f_2f_3 + u(c_0 + c_1x + c_2x^2))$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Non zero Free module cyclic codes of length 4 over $F_3 + uF_3 + u^2F_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(u, (u^i))$ for $i = 1, 2, 3$.</td>
</tr>
<tr>
<td>$(u, f_1f_2), (u, f_1f_3), (u, f_2f_3)$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Non zero Free module cyclic codes of length 4 over $F_3 + uF_3 + u^2F_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(u, (u^i))$ for $i = 1, 2, 3$.</td>
</tr>
<tr>
<td>$(u, f_1f_2), (u, f_1f_3), (u, f_2f_3)$</td>
</tr>
</tbody>
</table>

7 Conclusion

In this paper, we studied cyclic codes of an arbitrary length over the ring $F_q + uF_q + u^2F_q + \ldots + u^{k-1}F_q$, with $u^k = 0$. The rank and minimum spanning of this family of codes are studied as well. We also study dual codes and find their properties over the ring $F_q + uF_q + u^2F_q$.

References


**Author information**

Mohammed M. Al-Ashker, Department of Mathematics, Islamic University of Gaza, Gaza, Palestine.
E-mail: mashker@iugaza.edu.ps

Jianzhang Chen, School of Computer Science and Engineering, University of Electronic Science and Technology of China, China.
E-mail: chenyouqing66@gmail.com

Received: June 2, 2012
Accepted: August 27, 2012