TÜBİTAK

Turk J Math
35 (2011) , 737 – 749.

doi:10.3906/mat-1001-71

Cyclic codes over $Z_2 + uZ_2 + u^2Z_2 + \ldots + u^{k-1}Z_2$

Mohammed Al-Ashker, Mohammed Hamoudeh

Abstract

In this paper, we study the structure of cyclic codes of an arbitrary length n over the ring $Z_2 + uZ_2 + u^2Z_2 + \ldots + u^{k-1}Z_2$, where $u^k = 0$. Also we study the rank for these codes, and we find their minimal spanning sets. This study is a generalization and extension of the work in reference [1].

Key Words: Cyclic codes, Codes over rings, Hamming weight

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. On the other hand, the ring Z_4 admits a linear Gray map which does not give good binary 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 [11]. Calderbank and Sloane [6], and Pless [10] 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 Abualrub and Oehmke [2]. They showed that the ring $Z_4[x]/\langle x^n - 1\rangle$ is not a principal ideal ring and hence ideals may have more than one generator. Let R_k be the ring $Z_2 + uZ_2 + u^2Z_2 + \ldots + u^{k-1}Z_2$ with $u^k = 0$, where $Z_2 = \{0, 1\}$.

In [1], Abualrub and Siap studied cyclic codes of an arbitrary length n over $Z_2 + uZ_2 = \{0, 1, u, u + 1\}$ where $u^2 = 0$ and over $Z_2 + uZ_2 + u^2Z_2 = \{0, 1, u, u + 1, u^2, 1 + u^2, 1 + u + u^2, u + u^2\}$ where $u^3 = 0$. In this paper, we extend these results to more general rings of the form $Z_2 + uZ_2 + u^2Z_2 + \ldots + u^{k-1}Z_2$ where $u^k = 0$.

We give a unique set of generators for these codes as ideals in the ring $R_{k,n} = R_k[x]/\langle x^n - 1\rangle$. 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. For codes over $Z_2 + uZ_2 + u^2Z_2 = \{0, 1, u, u + 1, u^2, 1 + u^2, 1 + u + u^2, u + u^2\}$, with $u^k = 0$, this case corresponds to the case, when the length is even. Also, we study the rank of these codes and give a minimal spanning set for them.

2000 *AMS Mathematics Subject Classification:* 94B15.

We show that the results of [1] concerning the codes over the rings $F_2 + uF_2$ with $u^2 = 0$ and $Z_2 + uZ_2 + u^2Z_2$ with $u^3 = 0$ are valid for $R_k = Z_2 + uZ_2 + u^2Z_2 + \ldots + u^{k-1}Z_2$ with $u^k = 0$.

The remains 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 R_k. 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 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-dimentional 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 σ 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 $R_k = Z_2[u]/\langle u^k \rangle = Z_2 + uZ_2 + u^2Z_2 + \ldots + u^{k-1}Z_2$ is a commutative chain ring of 2^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 $R_k/uR_k \cong Z_2$ is the residue field and $|u^iR_k| = 2|(u^{i+1}R_k)| = 2^{k-i}$, $i = 0, 1, 2, \ldots, k-1$.

Denote $R_1 = Z_2 = \{0, 1\}$, $R_2 = Z_2 + uZ_2$, $R_3 = Z_2 + uZ_2 + u^2Z_2, \ldots$ etc.

Definition 2.3 *A linear code C_k of length n over the ring $R_k = Z_2 + uZ_2 + u^2Z_2 + \ldots + u^{k-1}Z_2$ with $u^k = 0$ is defined to be an additive submodule of the R_k-module R_k^n.*

Remark 2.1 *A cyclic code C_k of length n over R_k can be considered as 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*

$$c \cdot u = c_0 u_0 + \ldots + c_{n-1} u_{n-1}.$$

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

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

Definition 2.5 [1] *The Hamming weight of a codeword c is defined by*

$$w_H(c) = |\{i : c_i \neq 0\}|.$$

The minimum Hamming weight $d_H(C)$ of a linear code C is given by

$$d_H(C) = \min\{w_H(c) : c \in C \text{ and } c \neq 0\}.$$

Following Abualrub and Siap [1, p.p. 274], the parameters of an R_2-code C with $4^{k_1}2^{k_2}$ code words, where k_1 refers to the free part and k_2 refers to non free part u-multiple generator of C), and minimum distance d is denoted by $(n, 4^{k_1}2^{k_2}, d)$. Such codes are often referred to as codes of type $\{k_1, k_2\}$. Similarly, the parameters of an R_3-code C with $8^{k_1}4^{k_2}2^{k_3}$ code words, where k_1 refers to the free part and k_2, k_3 refer to non free part (u and u^2 multiple generators of C), and minimum distance d is denoted by $(n, 8^{k_1}4^{k_2}2^{k_3}, d)$. Such codes are often referred to as codes of type $\{k_1, k_2, k_3\}$.

We define the rank of a code C over R_2 of type $\{k_1, k_2\}$, denoted by $\text{rank}(C)$, by the minimum number of generators of C, and define the free rank of C, denoted by $\text{f-rank}(C)$, by the maximum of the ranks of R_2-free submodules of C. A code C of type $\{k_1, k_2\}$ has a rank $(k_1 + k_2)$ and a f-rank k_1. We define the rank of a code C over R_3 of type $\{k_1, k_2, k_3\}$, denoted by $\text{rank}(C)$, by the minimum number of generators of C, and define the free rank of C, denoted by $\text{f-rank}(C)$, by the maximum of the ranks of R_3-free submodules of C. A code C of type $\{k_1, k_2, k_3\}$ has a rank $(k_1 + k_2 + k_3)$ and a f-rank k_1.

Following the same procedure, we can define the ranks and free ranks of a code C over $R_k \ \forall\ k \geq 4$.

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.

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 $R_1 = Z_2$.

By following results in [1], 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 $\psi_1(a) = a$. ψ_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 $R_{1,n} = R_1[x]/\langle x^n - 1\rangle = Z_2[x]/\langle x^n - 1\rangle$ and hence a cyclic code in $Z_2[x]/\langle x^n - 1\rangle$. So $J_1 = \langle a_{k-1}(x)\rangle$ and $\ker\phi_1 = \langle u^{k-1}a_{k-1}(x)\rangle$ with $a_{k-1}(x)|(x^n - 1) \mod 2$.

Let C_2 be a cyclic code in $R_{k-1,n} = R_{k-1}[x]/\langle x^n - 1\rangle$.

Define $\psi_2 : R_{k-1} \to R_{k-2}$ by $\psi_2(a) = a$. ψ_2 is a ring homomorphism that can be extended to a homomorphism $\phi_2 : C_2 \to R_{k-2}[x]/\langle x^n - 1\rangle$ defined by

$$\phi_2(c_0 + c_1x + \ldots + c_{n-1}x^{n-1}) = \psi_2(c_0) + \psi_2(c_1)x + \ldots + \psi_2(c_{n-1})x^{n-1}.$$

Let $J_2 = \{r(x) = u^{k-2}r(x) \in \ker\phi_2\}$ is an ideal in $R_{1,n} = Z_2[x]/\langle x^n - 1\rangle$ and hence a cyclic code in $Z_2[x]/\langle x^n - 1\rangle$. So $J_2 = \langle a_{k-2}(x)\rangle$ and hence $\ker(\phi_2) = \langle u^{k-2}a_{k-2}(x)\rangle$ with $a_{k-2}(x)|(x^n - 1) \mod 2$.

Let C_3 be a cyclic code in $R_{k-2,n} = R_{k-2}[x]/\langle x^n - 1\rangle$.

Define $\psi_3 : R_{k-2} \to R_{k-3}$ by $\psi_3(a) = a$. ψ_3 is a ring homomorphism that can be extended to a homomorphism $\phi_3 : C_3 \to R_{k-3}[x]/\langle x^n - 1\rangle$. Continue in the same way as above until we define $\psi_k : R_2 \to R_1 = F_2$ by $\psi_k(a) = a^2$. ψ_k is a ring homomorphism because $(a + b)^2 = a^2 + b^2$ in R_2 and in Z_2.

Extend ψ_k to a homomorphism $\phi_k : C_k \to Z_2[x]/\langle x^n - 1\rangle = R_{1,n}$ defined by

$$\phi_k(c_0 + c_1x + \ldots + c_{n-1}x^{n-1}) = \psi_k(c_0) + \psi_k(c_1)x + \ldots + \psi_k(c_{n-1})x^{n-1}$$

$$= c_0^2 + c_1^2x + \ldots + c_{n-1}^2x^{n-1} \mod 2,$$

where C_k be a cyclic code in $R_{2,n} = R_2[x]/\langle x^n - 1\rangle$, where $R_2 = Z_2 + uZ_2$ with $u^2 = 0 \mod 2$.

$$\ker\phi_k = \langle ua_1(x)\rangle \text{ with } a_1(x)\big|\big(x^n - 1\big) \mod 2.$$

The image of ϕ_k is also an ideal and hence a binary cyclic code generated by $g(x)$ with $g(x)\big|\big(x^n - 1\big)$. So the cyclic code over $R_2 = Z_2 + uZ_2$ would be in the form:

$C_k = \langle g(x) + up(x), ua_1(x)\rangle$ for some binary polynomial $p(x)$. Note that $a_1\big|\big(p\frac{x^n-1}{g}\big)$ because

$$\phi_k\big(\frac{x^n - 1}{g}[g + up]\big) = \phi_k\big(up\frac{x^n - 1}{g}\big) = 0$$

$\Rightarrow \big(up\frac{x^n-1}{g}\big) \in \ker\phi_k = \langle ua_1\rangle$. Also $ug \in \ker\phi_k$ implies $a_1(x)\big|g(x)$.

Lemma 3.1 *[1] If $C_k = \langle g(x) + up(x), ua_1(x)\rangle$ over $R_2 = Z_2 + uZ_2$ with ($u^2 = 0 \mod 2$), and $g(x) = a_1(x)$ with $\deg g(x) = r$, then*

$$C_k = \langle g(x) + up(x)\rangle \text{ and } (g + up)\big|\big(x^n - 1\big) \text{ in } R_2.$$

Now since the image of ϕ_{k-1} is an ideal in $R_{2,n} = R_2[x]/\langle x^n - 1\rangle$ (where $R_2 = Z_2 + uZ_2$ with $u^2 = 0$), then $\mathrm{Im}(\phi_{k-1}) = \langle g(x) + up_1(x), ua_1(x)\rangle$ with $a_1(x)\big|g(x)|(x^n - 1)$ and $a_1(x)\big|p_1(x)\big(\frac{x^n-1}{g(x)}\big)$. Also, $\ker(\phi_{k-1}) = \langle u^2 a_2(x)\rangle$ with $a_2(x)\big|(x^n - 1) \mod 2$. Since $u^2 a_1 \in \ker(\phi_{k-1}) = \langle u^2 a_2\rangle$, then the cyclic code C_{k-1} over $R_3 = Z_2 + uZ_2 + u^2 Z_2$ with $u^3 = 0$ is

$$C_{k-1} = \langle g + up_1 + u^2 p_2, ua_1 + u^2 q_1, u^2 a_2\rangle \text{ with } a_2|a_1|g|(x^n - 1),\ a_1(x)\big|p_1(x)\big(\frac{x^n-1}{g(x)}\big) \mod 2, a_2|q_1\big(\frac{x^n-1}{a_1}\big),$$

$a_2|p_1\big(\frac{x^n-1}{g}\big)$ and $a_2\big|p_2\big(\frac{x^n-1}{g}\big)\big(\frac{x^n-1}{a_1}\big)$. 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.

Lemma 3.2 *[1] If $C_{k-1} = \langle g + up_1 + u^2 p_2, ua_1 + u^2 q_1, u^2 a_2\rangle$ over $R_3 = Z_2 + uZ_2 + u^2 Z_2$ with $(u^3 = 0)$, and $a_2 = g$, then $C_{k-1} = \langle g + up_1 + u^2 p_2\rangle$ and $\big(g + up_1 + u^2 p_2\big)\big|(x^n - 1)$ in R_3.*

Lemma 3.3 *[1] If n is odd, then $C_{k-1} = \langle g, ua_1, u^2 a_2\rangle = \langle g + ua_1 + u^2 a_2\rangle$ over R_3.*

Following the same process we find the cyclic code C_{k-2} over $R_4 = Z_2 + uZ_2 + u^2 Z_2 + u^3 Z_2$ with $(u^4 = 0)$. So, since the image of ϕ_{k-2} is an ideal in $R_{3,n} = R_3[x]/\langle x^n - 1\rangle$ (where $R_3 = Z_2 + uZ_2 + u^2 Z_2$ with $u^3 = 0$), then $\mathrm{Im}(\phi_{k-2}) = \langle g(x) + up_1(x) + u^2 p_2(x), ua_1(x) + u^2 q_1(x), u^2 a_2(x)\rangle$ with $a_2|a_1|g|(x^n - 1)$, $a_1(x)\big|p_1(x)\big(\frac{x^n-1}{g(x)}\big)$, $a_2|q_1(x)\Big(\frac{(x^n-1)}{a_1(x)}\Big)$ and $a_2\big|p_2(x)\big(\frac{x^n-1}{g(x)}\big)\big(\frac{x^n-1}{a_1(x)}\big)$. Also, $\ker(\phi_{k-2}) = \langle u^3 a_3(x)\rangle$ with $a_3(x)\big|(x^n - 1)$.

Since $u^3 a_2 \in \ker(\phi_{k-2}) = \langle u^3 a_3(x)\rangle$, then the cyclic code C_{k-2} over $R_4 = Z_2 + uZ_2 + u^2 Z_2 + u^3 Z_2$ with $(u^4 = 0)$ is $C_{k-2} = \langle g + up_1 + u^2 p_2 + u^3 p_3, ua_1 + u^2 q_1 + u^3 q_2, u^2 a_2 + u^3 l_1, u^3 a_3\rangle$ with

$$a_3|a_2|a_1|g|(x^n - 1) \mod 2,\ a_1(x)|p_1(x)\big(\frac{x^n-1}{g(x)}\big),$$

$$a_2|q_1(x)\Big(\frac{(x^n-1)}{a_1(x)}\Big),\ a_2|p_2(x)\big(\frac{x^n-1}{g(x)}\big)\big(\frac{x^n-1}{a_1(x)}\big),$$

$$a_3\big|l_1(x)\Big(\frac{(x^n-1)}{a_2(x)}\Big),\ a_3|q_2(x)\big(\frac{x^n-1}{q_1(x)}\big)\big(\frac{x^n-1}{a_1(x)}\big)$$

and $a_3(x)\big|p_3(x)\big(\frac{x^n-1}{g(x)}\big)\big(\frac{x^n-1}{a_2(x)}\big)\big(\frac{x^n-1}{a_1(x)}\big)$. Moreover , $\deg p_3 < dega_3$, $\deg q_2 < dega_3$, $\deg l_1 < dega_3$, $\deg p_2 < dega_2$, $\deg q_1 < dega_2$, $\deg p_1 < dega_1$.

Lemma 3.4 *If $C_{k-2} = \langle g + up_1 + u^2 p_2 + u^3 p_3, ua_1 + u^2 q_1 + u^3 q_2, u^2 a_2 + u^3 l_1, u^3 a_3\rangle$ over $R_4 = Z_2 + uZ_2 + u^2 Z_2 + u^3 Z_2$ with $(u^4 = 0)$, and $a_3 = g$, then $C_{k-2} = \langle g + up_1 + u^2 p_2 + u^3 p_3\rangle$ and $\big(g + up_1 + u^2 p_2 + u^3 p_3\big)\big|(x^n - 1)$ in R_4.*

Proof. Since $a_3 = g$, then $a_1 = a_2 = a_3 = g$. From lemma 3.2 we get that $(g + up_1 + u^2 p_2)\big|(x^n - 1)$ in R_3 and $C_{k-2} = \langle g + up_1 + u^2 p_2 + u^3 p_3, ua_1 + u^2 q_1 + u^3 q_2, u^3 a_3\rangle$. Rest of the proof is similar to lemma 3.2. □

Lemma 3.5 *If n is odd, then the cyclic code C_{k-2} over R_4 can be written as*

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

Proof. Since n is odd, then (x^n-1) factors uniquely into a product of distinct irreducible polynomials. So, $\gcd\left(a_1, \frac{x^n-1}{g(x)}\right) = \gcd\left(a_2, \frac{x^n-1}{a_1(x)}\right) = \gcd\left(a_2, \frac{x^n-1}{g(x)}\right) = \gcd\left(a_3, \frac{x^n-1}{a_2(x)}\right) = \gcd\left(a_3, \frac{x^n-1}{g(x)}\right) = 1$.

Since $a_1 \big| p_1(x)\left(\frac{x^n-1}{g(x)}\right)$, then $a_1 \big| p_1$. But $\deg p_1 < \deg a_1$. Hence $p_1 = 0$, since $a_2 \big| q_1(x)\left(\frac{x^n-1}{a_1(x)}\right)$ and $a_2(x) \big| p_2(x)\left(\frac{x^n-1}{g(x)}\right)\left(\frac{x^n-1}{a_1(x)}\right)$, then $a_2 \big| q_1$ and $a_2 \big| p_2$. But $\deg q_1 < \deg a_2$ and $\deg p_2 < \deg a_2$. Hence, $p_2 = q_1 = 0$. Similarly, $p_3 = q_2 = l_1 = 0$. So $C_{k-2} = \langle g, ua_1, u^2a_2, u^3a_3\rangle$. Let $h = g + ua_1 + u^2a_2 + u^3a_3$. Then, $u^3h = u^3g$, $\frac{x^n-1}{a_2}h = \frac{x^n-1}{a_2}u^3a_3$ and $u^2\frac{x^n-1}{g}h = \frac{x^n-1}{g}u^3a_2 \in \langle h\rangle$. Since n is odd, we have $\left(\frac{x^n-1}{g}, g\right) = \left(\frac{x^n-1}{a_2}, a_2\right) = 1$. Hence $1 = f_1\frac{x^n-1}{g} + f_2g$ for some polynomials f_1 and f_2, and $1 = m_1\frac{x^n-1}{a_2} + m_2a_2$ for some polynomials m_1 and m_2.

$u^3a_2 = u^3a_2f_1\frac{x^n-1}{g} + u^3a_2f_2g \in \langle h\rangle$. Also,

$$u^3a_3 = u^3a_3m_1\frac{x^n-1}{a_2} + u^3a_3m_2a_2 \in \langle h\rangle$$

and $u^2a_2 = u^3m_2a_2^3 \in C_{k-2}$ and hence $g \in \langle h\rangle$. Similarly, $ua_1 \in \langle h\rangle$. Therefore $C_{k-2} = \langle g, ua_1, u^2a_2, u^3a_3\rangle = \langle g + ua_1 + u^2a_2 + u^3a_3\rangle$. □

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 $R_{k,n} = R_k[x]/\langle x^n - 1\rangle$, $R_k = Z_2 + uZ_2 + u^2Z_2 + \ldots + u^{k-1}Z_2$ with $u^k = 0$.*

(1) *If n is odd, 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 binary polynomials with $a_{k-1}(x) \big| a_{k-2}(x) \big| \ldots \big| a_2(x) \big| a_1(x) \big| g(x) \mod 2$.

(2) *If n is not odd, then*

(a) *$C_1 = \langle g + up_1 + u^2p_2 + \ldots + u^{k-1}p_{k-1}\rangle$ where $g(x)$, $p_i(x)$ are binary polynomials $\forall i = 1, 2, \ldots, k-1$ with $g(x) \big| (x^n - 1) \mod 2$, $(g + up_1 + u^2p_2 + \ldots + u^{k-1}p_{k-1}) \big| (x^n - 1)$ in R_k and $\deg\ p_i < deg\ p_{i-1}$ for all $2 \leq i \leq k-1$.* OR

(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 $a_{k-1} | g | (x^n - 1)$ mod 2, $(g+up) | (x^n - 1)$ in R_2, $g(x) | p_1\left(\frac{x^n-1}{g(x)}\right)$ and $a_{k-1} | p_1\left(\frac{x^n-1}{g(x)}\right)$, $a_{k-1} | p_2\left(\frac{x^n-1}{g(x)}\right)\left(\frac{x^n-1}{g(x)}\right), \ldots$ and $a_{k-1} | p_{k-1}\left(\frac{x^n-1}{g(x)}\right) \ldots \left(\frac{x^n-1}{g(x)}\right)(k-1, times)$ and deg $p_{k-1} <$ deg a_{k-1}.* OR

(c) *$C_1 = \langle g + up_1 + u^2p_2 + \ldots + u^{k-1}p_{k-1}, ua_1 + u^2q_1 + \ldots + u^{k-1}q_{k-2}, u^2a_2 + u^3l_1 + \ldots + u^{k-1}l_{k-3}, \ldots, u^{k-2}a_{k-2} + u^{k-1}t_1, u^{k-1}a_{k-1}\rangle$ with $a_{k-1} \big| a_{k-2} \big| \ldots \big| a_2 \big| a_1 \big| g | (x^n - 1) \mod 2$, $a_{k-2} | p_1\left(\frac{x^n-1}{g}\right), \ldots, a_{k-1} | t_1\left(\frac{x^n-1}{a_{k-2}}\right)$,*

$\ldots, a_{k-1}|p_{k-1}\big(\frac{x^n-1}{g}\big)\ldots\big(\frac{x^n-1}{a_{k-2}}\big)$. *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], [9], the structure of cyclic codes over R_k of odd length n 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 Z_2, 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 (n odd) 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 $C = \langle g_0, ug_1, \ldots, u^{k-1}g_{k-1}\rangle$ and $g_{k-1}|g_{k-2}|\ldots|g_1|g_0|(x^n-1)$.*

Theorem 3.8 *Let C be a cyclic code of length n (n odd) over R_k, which has maximal ideal $< u >$ and k is the nilpotent index of u, $F = \hat{F}_1 + u\hat{F}_2 + \ldots + u^{k-1}\hat{F}_k$, where $F_i(x)$ is a factor of $x^n - 1$, $\hat{F}_i(x) = \frac{x^n-1}{F_i(x)}$. Then $C = \langle F\rangle$.*

Corollary 3.9 *$R_k[x]/\langle x^n - 1\rangle$, ($n$ odd) is a principal ideal ring.*

4. Ranks and minimal spanning sets for cyclic codes over R_k

Theorem 4.1 [*1*] *Let C be a cyclic code of even length n over $R_2 = Z_2 + uZ_2$ with $u^2 = 0$.*

(1) *If $C = \langle g(x) + up(x)\rangle$ with* deg $g(x) = r$ *and $\big(g(x) + up(x)\big)\big|(x^n - 1)$, then C is a free module with* rank$(C) = n - r$ *and basis $\beta = \Big\{g + up(x),\ xg(x) + up(x), \ldots, x^{n-r-1}(g(x) + up(x))\Big\}$, and $|C| = 4^{n-r}$.*

(2) *If $C = \langle g(x) + up(x), ua(x)\rangle$ with* deg $g(x) = r$, deg $a(x) = t$, *then C has* rank$(C) = n - t$ *and a minimal spanning set given by $\chi = \Big\{g(x)+up(x), x(g(x)+up(x))+\ldots+x^{n-r-1}\big(g(x)+up(x)\big), ua(x), xua(x), \ldots, x^{r-t-1}ua(x)\Big\}$.*

By following the same process, we find the rank and the minimal spanning set for any cyclic code over the ring R_i for $i = 2, 3, \ldots, k$. To do this, let us consider the cyclic code C_{k-2} of even length n over the ring $R_4 = Z_2 + uZ_2 + u^2Z_2 + u^3Z_2$ with $u^4 = 0$.

(1) If $C_{k-2} = \langle g + up_1 + u^2p_2 + u^3p_3\rangle$ as in lemma 3.4., deg $g(x) = r$, then C_{k-2} is a free module with rank$(C_{k-2}) = n - r$ and basis $\beta = \Big\{(g + up_1 + u^2p_2 + u^3p_3),\ x(g + up_1 + u^2p_2 + u^3p_3), \ldots,\ x^{n-r-1}(g + up_1 + u^2p_2 + u^3p_3)\Big\}$.

(2) If $C_{k-2} = \langle g+up_1+u^2p_2+u^3p_3, ua_1+u^2q_1+u^3q_2, u^2a_2+u^3l_1, u^3a_3\rangle$, where $a_3\big|a_2\big|a_1\big|g\big|(x^n-1) \mod 2$ with deg $g(x) = r$, deg $a_1(x) = s$, deg $a_2(x) = t$ and deg $a_3(x) = b$, then C_{k-2} has rank$(C_{k-2}) = n-b$ and a

minimal spanning set given by $\chi = \Big\{\big(g+up_1+u^2p_2+u^3p_3\big),\ x(g+up_1+u^2p_2+u^3p_3),\ \ldots,\ x^{n-r-1}(g+up_1+u^2p_2+u^3p_3),\ (ua_1+u^2q_1+u^3q_2),\ x(ua_1+u^2q_1+u^3q_2),\ \ldots,\ x^{r-s-1}(ua_1+u^2q_1+u^3q_2),\ (u^2a_2+u^3l_1),\ x(u^2a_2+u^3l_1),\ \ldots,\ x^{s-t-1}(u^2a_2+u^3l_1),\ (u^3a_3(x)),\ x(u^3a_3(x)),\ \ldots,\ x^{t-b-1}(u^3a_3(x))\Big\}$.

(3) If $C_{k-2} = \langle g+up_1+u^2p_2+u^3p_3, u^3a_3\rangle$ where deg $g(x) = r$, deg $a_3(x) = t$, then C_{k-2} has rank$(C_{k-2}) = n-t$ and a minimal spanning set given by

$\Gamma = \Big\{(g+up_1+u^2p_2+u^3p_3),\ x(g+up_1+u^2p_2+u^3p_3),\ldots,\ x^{n-r-1}(g+up_1+u^2p_2+u^3p_3), u^3a_3,\ xu^3a_3,\ldots,\ x^{r-t-1}u^3a_3\Big\}$.

Continue in the same way as above to get the following theorem as is a generalization of the results in [1].

Theorem 4.2 *Let C_1 be a cyclic code of even length n over*

$$R_k = Z_2 + uZ_2 + u^2Z_2 + \ldots + u^{k-1}Z_2 \text{ with } u^k = 0.$$

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* rank$(C_1) = n-r$ *and basis* $\beta = \Big\{(g+up_1+u^2p_2+\ldots+u^{k-1}p_{k-1}),\ x(g+up_1+u^2p_2+\ldots+u^{k-1}p_{k-1}),\ \ldots,\ x^{n-r-1}(g+up_1+u^2p_2+\ldots+u^{k-1}p_{k-1})\Big\}$.

(2) *If* $C_1 = \langle g+up_1+u^2p_2+\ldots+u^{k-1}p_{k-1}, ua_1+u^2q_1+\ldots+u^{k-1}q_{k-2}, u^2a_2+u^3l_1+\ldots+u^{k-1}l_{k-3},\ldots,u^{k-2}a_{k-2}+u^{k-1}t_1, u^{k-1}a_{k-1}\rangle$ *with* deg $g(x) = r_1$, deg $a_1(x) = r_2$, deg $a_2(x) = r_3,\ldots,$ deg $a_{k-1} = r_k$, *then C_1 has* rank$(C_1) = n-r_k$ *and a minimal spanning set given by* $\chi = \Big\{\big(g+up_1+u^2p_2+\ldots+u^{k-1}p_{k-1}\big),\ x\big(g+up_1+u^2p_2+\ldots+u^{k-1}p_{k-1}\big),\ \ldots,\ x^{n-r_1-1}\big(g+up_1+u^2p_2+\ldots+u^{k-1}p_{k-1}\big),\ \big(ua_1+u^2q_1+\ldots+u^{k-1}q_{k-2}\big),\ x\big(ua_1+u^2q_1+\ldots+u^{k-1}q_{k-2}\big),\ \ldots,\ x^{r_1-r_2-1}\big(ua_1+u^2q_1+\ldots+u^{k-1}q_{k-2}\big),\ (u^2a_2+u^3l_1+\ldots+u^{k-1}l_{k-3}),\ x(u^2a_2+u^3l_1+\ldots+u^{k-1}l_{k-3}),\ \ldots,\ x^{r_2-r_3-1}(u^2a_2+u^3l_1+\ldots+u^{k-1}l_{k-3}),\ \ldots,\ u^{k-1}a_{k-1}(x),\ xu^{k-1}a_{k-1}(x),\ \ldots,\ x^{r_{k-1}-r_k-1}u^{k-1}a_{k-1}(x)\Big\}$.

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

Proof. (1) Let C_1 be a cyclic code of even length over $R_k = Z_2 + uZ_2 + u^2Z_2 + \ldots + u^{k-1}Z_2$ with $u^k = 0$. Suppose

$$x^n - 1 = \big(g+up_1+u^2p_2+\ldots+u^{k-1}p_{k-1}\big)\big(h+up_1+u^2p_2+\ldots+u^{k-1}p_{k-1}\big) \text{ over} R_k.$$

Let $c(x) \in C_1 = \big\langle g(x)+up_1(x)+u^2p_2(x)+\ldots+u^{k-1}p_{k-1}(x)\big\rangle$, then $c(x) = \big(g(x)+up_1(x)+u^2p_2(x)+\ldots+u^{k-1}p_{k-1}(x)\big)f(x)$ for some polynomial $f(x)$.

If $\deg(f(x) \leq n-r-1,$ then we are done, otherwise by division algorithm there exist two polynomials $q(x), s(x)$ such that

$$f(x) = \left(\frac{x^n-1}{g+up_1+u^2p_2+\ldots+u^{k-1}p_{k-1}}\right)q(x)+s(x)$$

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

Now, $\Big(g(x)+up_1(x)+u^2p_2(x)+\ldots+u^{k-1}p_{k-1}(x)\Big)f(x)$

$= \Big(g(x)+up_1(x)+u^2p_2(x)+\ldots+u^{k-1}p_{k-1}(x)\Big)\left(\frac{x^n-1}{g+up_1+u^2p_2+\ldots+u^{k-1}p_{k-1}}q(x)+s(x)\right)$

$= \Big(g(x)+up_1(x)+u^2p_2(x)+\ldots+u^{k-1}p_{k-1}(x)\Big)s(x)$. Since $\deg(s(x)) \leq n-r-1,$ then β spans C_1. Now we only need to show that β is linearly independent. Let $g(x)=1+g_1x+\ldots+x^r,$ $p_1(x)=p_{1,0}+p_{1,1}x+\ldots+p_{1,l}x^l,$ $p_2(x)=p_{2,0}+p_{2,1}x+\ldots+p_{2,b}x^b,\ldots,$ $p_{k-1}(x)=p_{k-1,0}+p_{k-1,1}x+\ldots+p_{k-1,d}x^d$. Suppose $\big(g(x)+up_1(x)+u^2p_2(x)+\ldots+u^{k-1}p_{k-1}(x)\big)c_0+x\big(g(x)+up_1(x)+u^2p_2(x)+\ldots+u^{k-1}p_{k-1}(x)\big)c_1+\ldots+x^{n-r-1}\big(g(x)+up_1(x)+u^2p_2(x)+\ldots+u^{k-1}p_{k-1}(x)\big)c_{n-r-1}=0$. Comparing coefficients in the above equation we get that $\big(1+up_{1,0}+u^2p_{2,0}+\ldots+u^{k-1}p_{k-1,0}\big)c_0=0$ (constant coefficient). Since $\big(1+up_{1,0}+u^2p_{2,0}+\ldots+u^{k-1}p_{k-1,0}\big)$ is a unit, then $c_0=0$.

Hence, $x\big(g(x)+up_1(x)+u^2p_2(x)+\ldots+u^{k-1}p_{k-1}(x)\big)c_1+\ldots+x^{n-r-1}\big(g(x)+up_1(x)+u^2p_2(x)+\ldots+u^{k-1}p_{k-1}(x)\big)c_{n-r-1}=0$.

Again, comparing coefficients, we get that $\big(1+up_{1,0}+u^2p_{2,0}+\ldots+u^{k-1}p_{k-1,0}\big)c_1=0$ (coefficient of x). This implies that $c_1=0$. Similarly we get that $c_i=0$ for all $i=0,1,\ldots,n-r-1$. Therefore, β is linearly independent and hence a basis for C_1.

(2) Suppose $C_1=\langle g+up_1+u^2p_2+\ldots+u^{k-1}p_{k-1}, ua_1+u^2q_1+\ldots+u^{k-1}q_{k-2}, u^2a_2+u^3l_1+\ldots+u^{k-1}l_{k-3},\ldots,u^{k-1}a_{k-1}\rangle$ with $\deg(g+up_1+\ldots+u^{k-1}p_{k-1})=r_1,$ $\deg(ua_1+u^2q_1+\ldots+u^{k-1}q_{k-2})=r_2,$ $\deg(u^2a_2+u^3l_1+\ldots+u^{k-1}l_{k-3})=r_3,\ldots,$ $\deg(u^{k-1}a_{k-1})=r_k.$ Since the lowest degree polynomial in C_1 is $u^{k-1}a_{k-1}(x)$, then it's suffices to show that χ spans $\gamma=\Big\{\big(g+up_1+u^2p_2+\ldots+u^{k-1}p_{k-1}\big),\ x\big(g+up_1+u^2p_2+\ldots+u^{k-1}p_{k-1}\big),\ \ldots,\ x^{n-r_1-1}\big(g+up_1+u^2p_2+\ldots+u^{k-1}p_{k-1}\big),\ \big(ua_1+u^2q_1+\ldots+u^{k-1}q_{k-2}\big),\ x\big(ua_1+u^2q_1+\ldots+u^{k-1}q_{k-2}\big),\ldots,\ x^{r_1-r_2-1}\big(ua_1+u^2q_1+\ldots+u^{k-1}q_{k-2}\big),\ (u^2a_2+u^3l_1+\ldots+u^{k-1}l_{k-3}),\ x(u^2a_2+u^3l_1+\ldots+u^{k-1}l_{k-3}),\ \ldots,\ x^{r_2-r_3-1}(u^2a_2+u^3l_1+\ldots+u^{k-1}l_{k-3}),\ \ldots,\ u^{k-1}a_{k-1}(x),\ xu^{k-1}a_{k-1}(x),\ldots,x^{n-r_k-1}u^{k-1}a_{k-1}(x)\Big\}$. Similarly, it suffices to show that $u^{k-1}x^{r_{k-1}-r_k}a_{k-1}\in \text{span}\gamma.$ $u^{k-1}x^{r_{k-1}-r_k}a_{k-1}(x)=u^{k-1}\big(g(x)+up_1(x)+u^2p_2(x)+\ldots+u^{k-1}p_{k-1}(x)\big)+u^{k-1}m(x),$ where $u^{k-1}m(x)$ is a polynomial in C_1 of degree less than r_{k-1}.

Since any polynomial in C_1 must have degree greater or equal to $\deg(u^{k-1}a_{k-1}(x))=r_k,$ then $r_k \leq \deg(m(x))<r_{k-1}$. Hence $u^{k-1}m(x)=\alpha_0u^{k-1}a_{k-1}(x)+\alpha_1xu^{k-1}a_{k-1}(x)+\ldots+\alpha_{r_{k-1}-r_k-1}x^{r_{k-1}-r_k-1}u^{k-1}a_{k-1}(x)$.

Hence, χ is a generating set. By comparing coefficients as in (1) we get that non of elements in χ is a linear combination of the others. Therefore χ is a minimal generating set.

(3) This case is a special case of case (2); so the proof is similar to case (2). □

Definition 4.1 [1] *Let* $C = \langle g + up(x), ua(x) \rangle$ *be a cyclic code of even length* n *over* $R_2 = Z_2 + uZ_2$. *We define* $C_u = \{k(x) : uk(x) \in C\}$ *in* $R_{2,n} = R_2[x]/\langle x^n - 1 \rangle$.

Remark 4.1 [1] C_u *is a cyclic code over* $Z_2 = \{0, 1\} = R_1$.

Definition 4.2 [1] *Let* $C = \langle g + up_1 + u^2p_2, ua_1 + u^2q_1, u^2a_2 \rangle$ *be a cyclic code of even length over* $R_3 = Z_2 + uZ_2 + u^2Z_2$ *with* $(u^3 = 0)$. *We define* $C_{u^2} = \{k(x) : u^2k(x) \in C\}$ *in* $R_{3,n} = R_3[x]/\langle x^n - 1 \rangle$.

Remark 4.2 [1] C_{u^2} *is a cyclic code over* $R_1 = \{0, 1\} = Z_2$.

By following the same process, we define $C_{u^{i-1}}$ over the ring R_i for $i = 2, 3, \ldots, k$. So, if $i = 4$, then we let $C = \langle g + up_1 + u^2p_2 + u^3p_3, ua_1 + u^2q_1 + u^3q_2, u^2a_2 + u^3l_1, u^3a_3 \rangle$ be a cyclic code of even length over $R_4 = Z_2 + uZ_2 + u^2Z_2 + u^3Z_2$ with $(u^4 = 0) \Rightarrow C_{u^3} = \{R(x) : u^3k(x) \in C\}$ is a cyclic code over Z_2.

Hence, we generalize these definitions to more general ring R_k as follows.

Definition 4.3 *Let* $C = \langle g + up_1 + \ldots + u^{k-1}p_{k-1}, ua_1 + u^2q_1 + \ldots + u^{k-1}q_{k-2}, u^2a_2 + u^3l_1 + \ldots + u^{k-1}l_{k-3}, \ldots, u^{k-2}u_{k-2} + u^{k-1}t_1, u^{k-1}a_{k-1} \rangle$ *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* $u^k = 0$. *We define* $C_{u^{k-1}} = \{k(x) : u^{k-1}k(x) \in C\}$ *in* $R_{k,n}$.

Remark 4.3 $C_{u^{k-1}}$ *is a cyclic code over* $Z_2 = \{0, 1\}$.

Proof. Let $k(x) \in C_{u^{k-1}}$, we need to show that $xk(x) \in C_{u^{k-1}}$. Now, since $k(x) \in C_{u^{k-1}} \Rightarrow u^{k-1}k(x) \in C$, but C is cyclic code over $R_k \Rightarrow xu^{k-1}k(x) \in C \Rightarrow xk(x) \in C_{u^{k-1}}$. □

Theorem 4.3 [1] *Let* $C = \langle g + up_1 + u^2p_2, ua_1 + u^2q_1, u^2a_2 \rangle$. *Then* $C_{u^2} = \langle a_2(x) \rangle$ *and* $w_H(C) = w_H(C_{u^2})$.

According to Theorem 4.3, if $C = \langle g + up_1 + u^2p_2 + u^3p_3, ua_1 + u^2q_1 + u^3q_2, u^2a_2 + u^3l_1, u^3a_3 \rangle$ over $R_4 = Z_2 + uZ_2 + u^2Z_2 + u^3Z_2$ with $(u^4 = 0)$. Then $C_{u^3} = \langle a_3(x) \rangle$ and $w_H(C) = w_H(C_{u^3})$.

Continue in the same way as above we have the following theorem:

Theorem 4.4 *If* $C = \langle g + up_1 + \ldots + u^{k-1}p_{k-1}, ua_1 + u^2q_1 + \ldots + u^{k-1}q_{k-2}, u^2a_2 + u^3l_1 + \ldots + u^{k-1}l_{k-3}, \ldots, u^{k-2}u_{k-2} + u^{k-1}t_1, u^{k-1}a_{k-1} \rangle$ *is a cyclic code of even length over* $R_k = Z_2 + uZ_2 + u^2Z_2 + \ldots + u^{k-1}Z_2$ *with* $u^k = 0$. *Then* $C_{u^{k-1}} = \langle a_{k-1} \rangle$ *and* $w_H(C) = w_H(C_{u^{k-1}})$.

Proof. Since $u^{k-1}a_{k-1} \in C$, then $\langle a_{k-1}(x) \rangle \subseteq C_{u^{k-1}}$. Now given an $b(x) \in C_{u^{k-1}}$, then $u^{k-1}b(x) \in C$ and hence there exist polynomials $c_1(x), c_2(x), \ldots, c_t(x) \in Z_2[x]$ such that $u^{k-1}b(x) = c_1(x)u^{k-1}g(x) + c_2(x)u^{k-1}a_1(x) + c_3(x)u^{k-1}a_2(x) + \ldots + c_t(x)u^{k-1}a_{k-1}(x)$. Since $a_{k-1}(x) \big| a_{k-2}(x) \big| \ldots \big| a_2(x) \big| a_1(x) \big| g(x)$, we have $u^{k-1}b(x) = u^{k-1}m(x)a_{k-1}(x)$ for some $m(x)$. So $C_{u^{k-1}} \subseteq \langle a_{k-1}(x) \rangle$ and hence $C_{u^{k-1}} = \langle a_{k-1}(x) \rangle$.

Further, given a codeword $m(x) = m_0(x_0) + um_1(x) + u^2m_2(x) + \ldots + u^{k-1}m_{k-1}(x) \in C$, where $m_0(x),\ m_1(x),\ m_2(x),\ \ldots,\ m_{k-1}(x) \in F_2[x]$, since $u^{k-1}m(x) = u^{k-1}m_0(x) \in C$ and $w_H(u^{k-1}m(x)) \leq w_H(m(x))$ and $u^{k-1}C$ is a subcode of C with $w_H(u^{k-1}C) \leq w_H(C)$ it is sufficient to focus on the subcode $u^{k-1}C$ in order to compute the Hamming weight of C. Since $u^{k-1}C = \langle u^{k-1}a_{k-1}(x)\rangle$, thus $w_H(C) = w_H(C_{u^{k-1}})$. □

5. Examples

Example 5.1 *Cyclic codes of length 5 over* $R_4 = Z_2 + uZ_2 + u^2Z_2 + u^3Z_2$ *with* $u^4 = 0$. *Now,* $x^5 - 1 = (x+1)(x^4+x^3+x^2+x+1) = g_1g_2 \Rightarrow$ *The Nonzero cyclic codes of length 5 over* R_4 *with generator polynomials in Table 1.*

Table 1. Cyclic codes of length 5 over $R_4 = Z_2 + uZ_2 + u^2Z_2 + u^3Z_2$.

Non zero generator polynomials
$\langle 1\rangle,\ \langle g_1\rangle,\ \langle g_2\rangle$
$\langle u\rangle,\ \langle ug_1\rangle,\ \langle ug_2\rangle$
$\langle u^2\rangle,\ \langle u^2g_1\rangle,\ \langle u^2g_2\rangle$
$\langle u^3\rangle,\ \langle u^3g_1\rangle,\ \langle u^3g_2\rangle$
$\langle g_1, u\rangle,\ \langle g_2, u\rangle,\ \langle g_1, u^2\rangle,\ \langle g_2, u^2\rangle$
$\langle g_1, u^3\rangle,\ \langle g_2, u^3\rangle$
$\langle ug_1, u^2\rangle,\ \langle ug_2, u^2\rangle$
$\langle u^2g_1, u^3\rangle,\ \langle u^2g_2, u^3\rangle$

Example 5.2 *If* $n = 8$ *over* $R_3 = Z_2 + uZ_2 + u^2Z_2$ *with* $u^3 = 0$. $x^8 - 1 = (x-1)^8 = \big(g(x)\big)^8$ *over* $Z_2 = \{0, 1\}$. *The nonzero free/non free module cyclic codes over* R_3 *given in Table 2, and 3.*

Table 2. Non zero Free module cyclic codes of length 8 over $R_3 = F_2 + uF_2 + u^2F_2$.

Non zero generator polynomial(s): g=x+1
$\langle 1\rangle,\ \langle g\rangle,\ \langle g+u\rangle,\ \langle g+u^2\rangle$
$\langle g + u(c_0 + c_1x)\rangle,\ \langle g + u^2(c_0 + c_1x)\rangle$
$\langle g^3 + u(c_0 + c_1x + c_2x^2)\rangle,\ \langle g^3 + u^2(c_0 + c_1x + c_2x^2)\rangle$
$\langle g^4 + u(c_0 + c_1x + c_2x^2 + c_3x^3)\rangle,\ \langle g^4 + u^2(c_0 + c_1x + c_2x^2 + c_3x^3)\rangle$
$\langle g^5 + u(x^2+1)(c_0 + c_1x + c_2x^2)\rangle,\ \langle g^5 + u^2(x^2+1)(c_0 + c_1x + c_2x^2)\rangle$
$\langle g^6 + u(x+1)^4(c_0 + c_1x)\rangle,\ \langle g^6 + u^2(x+1)^4(c_0 + c_1x)\rangle$
$\langle g^7 + uc_0\rangle,\ \langle g^7 + u^2c_0\rangle$

Table 3. Non Free module cyclic codes of length 8 over $R_3 = Z_2 + uZ_2 + u^2Z_2$

Non zero generator polynomial(s): g=x+1
$\langle u \rangle,\ \langle u^2 \rangle$
$\langle ug^i \rangle,\ i = 1, \ldots, 7,\ \langle u^2 g^i \rangle,\ i = 1, \ldots, 7.$
$\langle g^i, u \rangle,\ i = 1, 2, \ldots, 7,\ \langle g^i, u^2 \rangle,\ i = 1, \ldots, 7.$
$\langle g^2 + uc_0, ug \rangle,\ \langle g^2 + u^2 c_0, u^2 g \rangle$
$\langle g^3 + uc_0, ug) \rangle,\ \langle g^3 + u^2 c_0, u^2 g) \rangle$
$\langle g^3 + u(c_0 + c_1 x), ug^2 \rangle,\ \langle g^3 + u^2(c_0 + c_1 x), u^2 g^2 \rangle$
$\langle g^4 + uc_0, ug \rangle,\ \langle g^4 + u^2 c_0, u^2 g \rangle$
$\langle g^4 + u(c_0 + c_1 x), ug^2 \rangle,\ \langle g^4 + u^2(c_0 + c_1 x), u^2 g^2 \rangle$
$\langle g^4 + u(c_0 + c_1 x + c_2 x^2), ug^3 \rangle,\ \langle g^4 + u^2(c_0 + c_1 x + c_2 x^2), u^2 g^3 \rangle$
$\langle g^5 + uc_0, ug \rangle,\ \langle g^5 + u^2 c_0, u^2 g \rangle$
$\langle g^5 + u(c_0 + c_1 x), ug^2 \rangle,\ \langle g^5 + u^2(c_0 + c_1 x), u^2 g^2 \rangle$
$\langle g^5 + u(c_0 + c_1 x + c_2 x^2), ug^3 \rangle,\ \langle g^5 + u^2(c_0 + c_1 x + c_2 x^2), u^2 g^3 \rangle$
$\langle g^5 + u(x+1)(c_0 + c_1 x + c_2 x^2), ug^4 \rangle,\ \langle g^5 + u^2(x+1)(c_0 + c_1 x + c_2 x^2), u^2 g^4 \rangle$
$\langle g^6 + uc_0, ug \rangle,\ \langle g^6 + u^2 c_0, u^2 g \rangle$
$\langle g^6 + u(c_0 + c_1 x), ug^2 \rangle,\ \langle g^6 + u^2(c_0 + c_1 x), u^2 g^2 \rangle$
$\langle g^6 + ug(c_0 + c_1 x), ug^3 \rangle,\ \langle g^6 + u^2 g(c_0 + c_1 x), u^2 g^3 \rangle$
$\langle g^6 + ug^2(c_0 + c_1 x), ug^4 \rangle,\ \langle g^6 + u^2 g^2(c_0 + c_1 x), u^2 g^4 \rangle$
$\langle g^6 + ug^3(c_0 + c_1 x), ug^5 \rangle\ \langle g^6 + u^2 g^3(c_0 + c_1 x), u^2 g^5 \rangle$
$\langle g^7 + uc_0, ug \rangle,\ \langle g^7 + u^2 c_0, u^2 g \rangle$
$\langle g^7 + ugc_0, ug^2 \rangle,\ \langle g^7 + u^2 gc_0, u^2 g^2 \rangle$
$\langle g^7 + ug^2 c_0, ug^3 \rangle,\ \langle g^7 + u^2 g^2 c_0, u^2 g^3 \rangle$
$\langle g^7 + ug^3 c_0, ug^4 \rangle,\ \langle g^7 + u^2 g^3 c_0, u^2 g^4 \rangle$
$\langle g^7 + ug^4 c_0, ug^5 \rangle,\ \langle g^7 + u^2 g^4 c_0, u^2 g^5 \rangle$
$\langle g^7 + ug^5 c_0, ug^6 \rangle,\ \langle g^7 + u^2 g^5 c_0, u^2 g^6 \rangle$

6. Conclusion

In this paper, we studied cyclic codes of an arbitrary length over the ring $Z_2 + uZ_2 + u^2Z_2 + \ldots + u^{k-1}Z_2$, with $u^k = 0$. The rank and minimum spanning of this family of codes are studied as well. Open problem include the study of cyclic codes of an arbitrary length over $Z_p + uZ_p + u^2Z_p + \ldots + u^{k-1}Z_p$, where p is a prime integer, $u^k = 0$, and also the study of dual and self-dual codes and their properties over these rings.

References

[1] Abualrub, T. and Saip, I.: Cyclic codes over the rings $Z_2 + uZ_2$ and $Z_2 + uZ_2 + u^2Z_2$, Designs Codes and Cryptography. Vol.42, No.3, 273-287(2007).

[2] Abualrub, T. and Oehmke, R.: On the generators of Z_4 cyclic codes, IEEE Trans. Inform. Theory. Vol.49, No.9, 2126-2133(2003).

[3] Blackford, T.: Cyclic codes over Z_4 of oddly even length, Discrete Applied Mathematics. Vol.128, 27-46(2003).

[4] Bonnecaze, A. and Udaya, P.: Cyclic codes and self-dual codes over $F_2 + uF_2$, IEEE Trans. Inform. Theory. Vol.45, No.4, 1250-1255(1999).

[5] Calderbank, A., Rains, E., Shor, P., Neil, J. and Sloane, N.J.A.: Quantum error corrections via codes over GF(4), IEEE Transactions on Information Theory. Vol.4, No.4, 1369-1387(1998).

[6] Calderbank, A. and Sloane, N.J.A.: Modular and P-adic cyclic codes, Des. Codes Crypt. Vol.37, No.6, 21-35(1995).

[7] Dinh, H. and Lopez-Permouth, S.: Cyclic and negacyclic codes over finite chain rings, IEEE Trans. Inform. Theory. Vol.50, No.8, 1728-1744(2004).

[8] Dougherty, ST. and Shiromoto, K.: Maximum distance codes over rings of order 4, IEEE Trans. Inform. Theory. Vol.47, No.1, 400-404 (2001).

[9] Noton, G. and Salagean, A.: On the structure of linear and cyclic codes over a finite chain ring, Applicable Algebra Engineering Communication and Computing. Vol.10, No.6, 489-506 (2000).

[10] Pless, V. and Qian, Z.: Cyclic codes and quadratic residue codes over Z_4, IEEE Trans. Inform. Theory. Vol.45, No.5, 1594-1600 (1996).

[11] Van Lint, J.: Repeated-root cyclic codes, IEEE Trans. Inform. Theory. Vol.37, No.2, 343-345(1977).

Mohammed AL-ASHKER
Department of Mathematics,
Islamic University of Gaza-PALESTINE
e-mail: mashker@iugaza.edu.ps

Mohammed HAMOUDEH
Ministry of education, Gaza-PALESTINE
e-mail: mamh_73@hotmail.com

Received: 04.01.2010