Des. Codes Cryptogr. (2015) 74:1–13
DOI 10.1007/s10623-013-9843-2

On cyclic codes over the ring $\mathbb{Z}_p[u]/\langle u^k \rangle$

Abhay Kumar Singh · Pramod Kumar Kewat

Received: 21 June 2012 / Revised: 3 November 2012 / Accepted: 5 June 2013 /
Published online: 25 June 2013

Abstract In this paper, we study cyclic codes over the ring $\mathbb{Z}_p[u]/\langle u^k \rangle$. We find a set of generators for these codes. We also study the rank and the Hamming distance of these codes.

Keywords Cyclic codes · Hamming distance

Mathematics Subject Classification 94B15

1 Introduction

Let R be a ring. A linear code of length n over R is a R submodule of R^n. A linear code C of length n over R is cyclic if $(c_{n-1}, c_0, \ldots, c_{n-2}) \in C$ whenever $(c_0, c_1, \ldots, c_{n-1}) \in C$. We can consider a cyclic code C of length n over R as an ideal in $R[x]/\langle x^n - 1 \rangle$ via the following correspondence

$$R^n \longrightarrow R[x]/\langle x^n - 1 \rangle, \quad (c_0, c_1, \ldots, c_{n-1}) \mapsto c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}.$$

In recent time, cyclic codes over rings have been studied extensively because of their important role in algebraic coding theory. The structure of cyclic codes of odd length over rings has been discussed in a series of papers [6,8,11,14]. In [7,9,13], a complete structure of cyclic codes of odd length over $\mathbb{Z}_4$ has been presented. In [5], Blackford studied cyclic codes of length $n = 2k$, when k is odd. The cyclic codes of length a power of 2 over $\mathbb{Z}_4$ are studied in [1,3]. The structures of cyclic codes of length n over a finite chain ring R has been discussed

Communicated by J.-L. Kim.

A. K. Singh · P. K. Kewat (✉)
Department of Applied Mathematics, Indian School of Mines,
Dhanbad 826 004, Jharkhand, India
e-mail: pramodkewat@gmail.com; kewat.pk.am@ismdhanbad.ac.in

A. K. Singh
e-mail: singh.ak.am@ismdhanbad.ac.in

in [10] when n is not divisible by the characteristic of the residue field $\bar{R}$. Bonnecaze and Udaya [6] studied cyclic codes of odd length over $R_{2,2} = \mathbb{Z}_2 + u\mathbb{Z}_2,\ u^2 = 0$. In [2], Abualrub and Siap studied cyclic codes of an arbitrary length over $R_{2,2} = \mathbb{Z}_2 + u\mathbb{Z}_2,\ u^2 = 0$ and over $R_{3,2} = \mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2,\ u^3 = 0$. Al-Ashker and Hamoudeh [4] extended some of the results in [2] to the ring $R_{k,2} = \mathbb{Z}_2 + u\mathbb{Z}_2 + \cdots + u^{k-1}\mathbb{Z}_2,\ u^k = 0$.

Let $R_{k,p} = \mathbb{Z}_p + u\mathbb{Z}_p + \cdots + u^{k-1}\mathbb{Z}_p$ where p is a prime number and $u^k = 0$. Note that the ring $R_{k,p}$ can also be viewed as the quotient ring $\mathbb{Z}_p[u]/\langle u^k\rangle$. In this paper, we discuss the structure of cyclic codes of arbitrary length over the ring $R_{k,p}$. We find a set of generators and a minimal spanning set for these codes. We also discuss about the rank and the Hamming distance of these codes. Recall that the Hamming weight of a codeword c is defined as the number of non-zero entries of c and the Hamming distance of a code C is the smallest possible weight among all its non-zero codewords. The minimum distance of a code is the minimum Hamming distance between two distinct codewords. When the code is linear, the minimum distance of the code is equal to the Hamming distance. The minimum distance determines the maximum number of errors that can be corrected under any decoding algorithm.

Let C be a cyclic code over the ring $R_{k,p} = \mathbb{Z}_p + u\mathbb{Z}_p + \cdots + u^{k-1}\mathbb{Z}_p,\ u^k = 0$. The line of arguments we have used to find a set of generators and a minimal spanning set of a code C are somewhat similar to those discussed in [2]. The idea to find a set of generators is as follows. We view the cyclic code C as an ideal in $R_{k,p,n} = R_{k,p}/\langle x^n - 1\rangle$. Then we define the projection map from $R_{i,p,n} \longrightarrow R_{i-1,p,n}$ for each $i > 1$. For $i = 2$, we have the projection map from $R_{2,p,n} \longrightarrow R_{1,p,n}$. Note that $R_{1,p,n}$ is nothing but $\mathbb{Z}_p[x]/\langle x^n - 1\rangle$ and an ideal in $R_{1,p,n}$ gives a cyclic code over $\mathbb{Z}_p$. The structure of cyclic codes over $\mathbb{Z}_p$ is well known. By pullback, we find a set of generators for a cyclic code over $R_{2,p}$ and inductively we get a set of generators for a cyclic code over $R_{k,p}$ for all k. Again, the line of arguments we have used to find minimum distance are similar to [2] but slightly different.

This paper is organized as follows. In Sect. 2, we give a set of generators for the cyclic codes C over the ring $R_{k,p} = \mathbb{Z}_p + u\mathbb{Z}_p + \cdots + u^{k-1}\mathbb{Z}_p,\ u^k = 0$. In Sect. 3, we find a minimal spanning set for these codes and discuss about the rank. In Sect. 4, we find the minimum distance of these codes. In Sect. 5, we discuss some of the examples of these codes.

2 Preliminaries

Let R be a finite commutative ring. We have the following equivalent conditions.

Proposition 2.1 [10, Proposition 2.1] *The following conditions are equivalent for a finite commutative ring R.*

(1) *R is a local ring and the maximal ideal M of R is principal*;
(2) *R is a local principal ideal ring*;
(3) *R is a chain ring.*

Let R be a finite commutative local ring with maximal ideal M. Let $\bar{R} = R/M$. Let $\mu : R[x] \longrightarrow \bar{R}[x]$ denote the natural ring homomorphism that maps $r \mapsto r + M$ and the variable x to x. We define the degree of the polynomial $f(x) \in R[x]$ as the degree of the polynomial $\mu(f(x))$ in $\bar{R}[x]$, i.e., $\deg(f(x)) = \deg(\mu(f(x))$ (see, for example, [12]). A polynomial $f(x) \in R[x]$ is called regular if it is not a zero divisor. The following proposition is well known.

Proposition 2.2 (cf. [12, Exercise XIII.2(c)]) *Let R be a finite commutative chain ring. Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$ be in $R[x]$, then the following are equivalent.*

(1) $f(x)$ *is regular*,
(2) $\langle a_0, a_1, \ldots, a_n\rangle = R$,
(3) a_i *is a unit for some* i, $0 \le i \le n$,
(4) $\mu(f(x)) \neq 0$.

The following version of the division algorithm holds true for polynomials over finite commutative local rings.

Proposition 2.3 (cf. [12, Exercise XIII.6]) *Let R be a finite commutative local ring. Let $f(x)$ and $g(x)$ be non-zero polynomials in $R[x]$. If $g(x)$ is regular, then there exist polynomials $q(x)$ and $r(x)$ in $R[x]$ such that $f(x) = g(x)q(x) + r(x)$ and $\deg(r(x)) < \deg(g(x))$.*

Let $R_{k,p} = \mathbb{Z}_p + u\mathbb{Z}_p + \cdots + u^{k-1}\mathbb{Z}_p$, $u^k = 0$. It is easy to see that the ring $R_{k,p}$ is a finite chain ring with unique maximal ideal $\langle u\rangle$. Let $g(x)$ be a non-zero polynomial in $\mathbb{Z}_p[x]$. By Proposition 2.2, it is also easy to see that the polynomial $g(x)+up_1(x)+u^2p_2(x)+\cdots+u^{k-1}p_{k-1}(x) \in R_{k,p}[x]$ is regular. Throughout the paper, we repeatedly make use of Proposition 2.3 for the polynomial $g(x)+up_1(x)+u^2p_2(x)+\cdots+u^{k-1}p_{k-1}(x) \in R_{k,p}[x]$. Note that $\deg(g(x) + up_1(x) + u^2p_2(x) + \cdots + u^{k-1}p_{k-1}(x)) = \deg(g(x))$.

3 A generator for cyclic codes over the ring $R_{k,p}$

Let p be a prime number. Let $R_{k,p} = \mathbb{Z}_p + u\mathbb{Z}_p + \cdots + u^{k-1}\mathbb{Z}_p$, $u^k = 0$ and $R_{k,p,n} = R_{k,p}[x]/\langle x^n-1\rangle$. Let C_k be a cyclic code of length n over $R_{k,p}$. We also consider C_k as an ideal in $R_{k,p,n}$. We define the map $\psi_{k-1} : R_{k,p} \longrightarrow R_{k-1,p}$ by $\psi_{k-1}(b_0+ub_1+\cdots+u^{k-1}b_{k-1}) = b_0 + ub_1 + \cdots + u^{k-2}b_{k-2}$, where $b_i \in \mathbb{Z}_p$. The map ψ_{k-1} is a ring homomorphism. We extend it to a homomorphism $\phi_{k-1} : C_k \longrightarrow R_{k-1,p,n}$ defined by

$$\phi_{k-1}\left(c_0 + c_1x + \cdots + c_{n-1}x^{n-1}\right) = \psi_{k-1}(c_0) + \psi_{k-1}(c_1)\,x + \cdots + \psi_{k-1}(c_{n-1})\,x^{n-1},$$

where $c_i \in R_{k,p}$. Let $J_{k-1} = \{r(x) \in \mathbb{Z}_p[x] : u^{k-1}r(x) \in \ker\phi_{k-1}\}$. It is easy to see that J_{k-1} is an ideal in $R_{1,p,n}$. Since $R_{1,p,n}$ is a principal ideal ring, we have $J_{k-1} = \langle a_{k-1}(x)\rangle$ for some $a_{k-1}(x) \in \mathbb{Z}_p[x]$, and $\ker\phi_{k-1} = \langle u^{k-1}a_{k-1}(x)\rangle$ with $a_{k-1}(x)|(x^n - 1) \bmod p$.

Let C_{k-1} be a cyclic code of length n over $R_{k-1,p}$. We define the map $\psi_{k-2} : R_{k-1,p} \longrightarrow R_{k-2,p}$ by $\psi_{k-2}(b_0 + ub_1 + \cdots + u^{k-2}b_{k-2}) = b_0 + ub_1 + \cdots + u^{k-3}b_{k-3}$, where $b_i \in \mathbb{Z}_p$. The map ψ_{k-2} is a ring homomorphism. We extend it to a homomorphism $\phi_{k-2} : C_{k-1} \longrightarrow R_{k-2,p,n}$ defined by

$$\phi_{k-2}\left(c_0 + c_1x + \cdots + c_{n-1}x^{n-1}\right) = \psi_{k-2}(c_0) + \psi_{k-2}(c_1)\,x + \cdots + \psi_{k-2}(c_{n-1})\,x^{n-1},$$

where $c_i \in R_{k-1,p}$. Let $J_{k-2} = \{r(x) \in \mathbb{Z}_p[x] : u^{k-2}r(x) \in \ker\phi_{k-2}\}$. We see that J_{k-2} is an ideal in $R_{1,p,n}$. As above, we have $J_{k-2} = \langle a_{k-2}(x)\rangle$ for some $a_{k-2}(x) \in \mathbb{Z}_p[x]$, and $\ker\phi_{k-2} = \langle u^{k-2}a_{k-2}(x)\rangle$ with $a_{k-2}(x)|(x^n - 1) \bmod p$.

We continue in the same way as above and define $\psi_{k-3}, \psi_{k-4}, \ldots, \psi_2$ and $\phi_{k-3}, \phi_{k-4}, \ldots, \phi_2$. We define $\psi_1 : R_{2,p} \longrightarrow R_{1,p} = \mathbb{Z}_p$ by $\psi_1(b_0 + ub_1) = b_0$, where $b_0, b_1 \in \mathbb{Z}_p$. The map ψ_1 is a ring homomorphism. We extend ψ_1 to a homomorphism $\phi_1 : C_2 \longrightarrow R_{1,p,n}$ defined by

$$\phi_1\left(c_0 + c_1x + \cdots + c_{n-1}x^{n-1}\right) = \psi_1(c_0) + \psi_1(c_1)\,x + \cdots + \psi_1(c_{n-1})\,x^{n-1},$$

where $c_i \in R_{2,p}$. As above, we have $\ker\phi_1 = \langle ua_1(x)\rangle$ for some $a_1(x) \in \mathbb{Z}_p[x]$, with $a_1(x)|(x^n - 1) \bmod p$. The image of ϕ_1 is an ideal in $R_{1,p,n}$ and hence a cyclic code in $\mathbb{Z}_p$.

Since $R_{1,p,n}$ is a principal ideal ring, the image of ϕ_1 is generated by some $g(x) \in \mathbb{Z}_p[x]$ with $g(x)|(x^n-1)$. Hence, we have $C_2 = \langle g(x)+up_1(x),\ ua_1(x)\rangle$ for some $p_1(x) \in \mathbb{Z}_p[x]$. We have

$$\phi_1\left(\frac{x^n-1}{g(x)}\left(g(x)+up_1(x)\right)\right) = \phi_1\left(up_1(x)\frac{x^n-1}{g(x)}\right) = 0.$$

Therefore, $up_1(x)\left(\frac{x^n-1}{g(x)}\right) \in \ker\phi_1 = \langle ua_1(x)\rangle$. Hence, $a_1(x)|p_1(x)\left(\frac{x^n-1}{g(x)}\right)$. Also we have $ug(x) \in \ker\phi_1$. This implies that $a_1(x)|g(x)$.

Lemma 3.1 *Let C_2 be a cyclic code over $R_{2,p} = \mathbb{Z}_p + u\mathbb{Z}_p$, $u^2 = 0$. If $C_2 = \langle g(x) + up_1(x),\ ua_1(x)\rangle$, and $g(x) = a_1(x)$ with $\deg g(x) = r$, then*

$$C_2 = \langle g(x) + up_1(x)\rangle \quad \textit{and} \quad (g(x) + up_1(x)) \mid \left(x^n - 1\right) \textit{ in } R_{2,p}.$$

Proof We have $u(g(x) + up_1(x)) = ug(x)$ and $g(x) = a_1(x)$. It is clear that $C_2 \subset \langle g(x) + up_1(x)\rangle$. Hence, $C_2 = \langle g(x) + up_1(x)\rangle$. By the division algorithm, we have

$$x^n - 1 = (g(x) + up_1(x))\, q(x) + r(x), \quad \text{where } r(x) = 0 \quad \text{or } \deg r(x) < r.$$

This implies that $r(x) = (x^n - 1) - (g(x) + up_1(x))q(x)$. This gives, $r(x) \in C_2$. Thus, we have $r(x) = 0$ and hence $(g(x) + up_1(x))|(x^n - 1)$ in $R_{2,p}$. □

Note that the image of ϕ_2 is an ideal in $R_{2,p,n}$, hence a cyclic code over $R_{2,p}$. Therefore, we have $\mathrm{Im}(\phi_2) = \langle g(x)+up_1(x),\ ua_1(x)\rangle$ with $a_1(x)|g(x)|(x^n-1)$ and $a_1(x)|p_1(x)\left(\frac{x^n-1}{g(x)}\right)$. Also, we have $\ker\phi_2 = \langle u^2a_2(x)\rangle$ with $a_2(x)|(x^n-1) \bmod p$ and $u^2a_1(x) \in \ker\phi_2$. As above, the cyclic code C_3 over $R_{3,p}$ is given by

$$C_3 = \left\langle g + up_1(x) + u^2p_2(x),\ ua_1(x) + u^2q_1(x),\ u^2a_2(x)\right\rangle,$$

for some $p_2(x),\ q_1(x) \in \mathbb{Z}_p[x]$, with $a_2(x)|a_1(x)|g(x)|(x^n-1)$, $a_1(x)|p_1(x)\left(\frac{x^n-1}{g(x)}\right) \bmod p$, $a_2(x)|q_1(x)\left(\frac{x^n-1}{a_1(x)}\right)$, $a_2(x)|p_1(x)\left(\frac{x^n-1}{g(x)}\right)$ and $a_2(x)|p_2(x)\left(\frac{x^n-1}{g(x)}\right)\left(\frac{x^n-1}{a_1(x)}\right)$. We may assume that $\deg p_2(x) < \deg a_2(x)$, $\deg q_1(x) < \deg a_2(x)$ and $\deg p_1(x) < \deg a_1(x)$ because g.c.d. $(a,\ b) = g.c.d.(a,\ b + da)$ for any d. We have the following lemma.

Lemma 3.2 *Let C_3 be a cyclic code over $R_{3,p} = \mathbb{Z}_p + u\mathbb{Z}_p + u^2\mathbb{Z}_p$, $u^3 = 0$. If $C_3 = \langle g + up_1(x) + u^2p_2(x),\ ua_1(x) + u^2q_1(x),\ u^2a_2(x)\rangle$, and $a_2(x) = g(x)$, then $C_3 = \langle g+up_1(x)+u^2p_2(x)\rangle$, $(g(x)+up_1(x))|(x^n-1)$ in $R_{2,p}$ and $(g+up_1(x)+u^2p_2(x))|(x^n-1)$ in $R_{3,p}$.*

Proof Since $a_2(x) = g(x)$, we get $a_1(x) = a_2(x) = g(x)$. We have $\phi_2(C_3) = \langle g + up_1(x),\ ua_1(x)\rangle$. From Lemma 3.1, we get $(g(x)+up_1(x))|(x^n-1)$ in $R_{2,p}$, and $\phi_2(C_3) = \langle g + up_1(x)\rangle$. This gives, $C_3 = \langle g + up_1(x) + u^2p_2(x),\ u^2a_2(x)\rangle$. The rest of the proof is similar to Lemma 3.1. □

If we continue in the same way as above, we can see that the image of ϕ_{k-1} is an ideal in $R_{k-1,p,n}$, hence a cyclic code over $R_{k-1,p}$. By induction hypothesis, we can assume that $\mathrm{Im}(\phi_{k-1}) = \langle g + up_1(x) + u^2p_2(x) + \cdots + u^{k-2}p_{k-2}(x),\ ua_1(x) + u^2q_1(x) + \cdots + u^{k-2}q_{k-3}(x),\ u^2a_2(x) + u^3l_1(x) + \cdots + u^{k-2}l_{k-4}(x), \ldots, u^{k-3}a_{k-3}(x) + u^{k-2}s_1(x),\ u^{k-2}a_{k-2}(x)\rangle$ with $a_{k-2}(x)|\cdots|a_2(x)|a_1(x)|g(x)|(x^n-1) \bmod p$, $a_{k-3}(x)|p_1(x)\left(\frac{x^n-1}{g(x)}\right), \ldots, a_{k-2}|s_1(x)\left(\frac{x^n-1}{a_{k-3}(x)}\right), \ldots, a_{k-2}|p_{k-2}\left(\frac{x^n-1}{g(x)}\right)\cdots\left(\frac{x^n-1}{a_{k-3}(x)}\right)$. Also, we have

$\ker\phi_{k-1} = \langle u^{k-1}a_{k-1}(x)\rangle$ with $a_{k-1}(x)|(x^n-1) \bmod p$ and $u^{k-1}a_{k-2}(x) \in \ker\phi_{k-1}$. Following the same process as above and by induction on k, we get the following theorem.

Theorem 3.3 *Let C_k be a cyclic code over $R_{k,p} = \mathbb{Z}_p + u\mathbb{Z}_p + u^2\mathbb{Z}_p + \cdots + u^{k-1}\mathbb{Z}_p$, $u^k = 0$. If n is not relatively prime to p, then*

(1) *$C_k = \langle g(x) + up_1(x) + u^2p_2(x) + \cdots + u^{k-1}p_{k-1}(x)\rangle$ where $g(x)$ and $p_i(x)$ are polynomials in $\mathbb{Z}_p[x]$ with $g(x)|(x^n-1)$ mod p, $(g(x) + up_1(x) + u^2p_2(x) + \cdots + u^{k-1}p_{i-1}(x))|(x^n-1)$ in $R_{i,p}$ and $\deg p_i < \deg p_{i-1}$ for all $1 < i \le k$.* Or

(2) *$C_k = \langle g + up_1(x) + u^2p_2(x) + \cdots + u^{k-1}p_{k-1}(x),\ ua_1(x) + u^2q_1(x) + \cdots + u^{k-1}q_{k-2}(x),\ u^2a_2(x) + u^3l_1(x) + \cdots + u^{k-1}l_{k-3}(x), \ldots, u^{k-2}a_{k-2}(x) + u^{k-1}t_1(x),\ u^{k-1}a_{k-1}(x)\rangle$ with $a_{k-1}(x)|a_{k-2}(x)|\cdots|a_2(x)|a_1(x)|g(x)|(x^n-1)$ mod p, $a_{k-2}(x)|p_1(x)\left(\frac{x^n-1}{g(x)}\right)$, $\ldots$, $a_{k-1}|t_1(x)\left(\frac{x^n-1}{a_{k-2}(x)}\right)$, $\ldots$, $a_{k-1}|p_{k-1}\left(\frac{x^n-1}{g(x)}\right)\cdots\left(\frac{x^n-1}{a_{k-2}(x)}\right)$. Moreover, $\deg p_{k-1}(x) < \deg a_{k-1}(x), \cdots, \deg t_1(x) < a_{k-1}(x), \cdots,$ and $\deg p_1(x) < \deg a_{k-2}(x)$.*

Note that if we have $a_{k-1}(x) = g(x)$ in part 2 of the above theorem then we get part 1. If we have $a_{k-1} \neq g(x)$ but $a_{k-2} = g(x)$ then $C_k = \langle g(x) + up_1(x) + u^2p_2(x) + \cdots + u^{k-1}p_{k-1}(x),\ u^{k-1}a_{k-1}(x)\rangle$ where $a_{k-1}(x)|g(x)|(x^n-1)$ mod p, $g(x) + up_1(x) + \cdots + u^{i-1}p_{i-1}|(x^n-1)$ in $R_{i,p}$ for $1 < i \le k-1$, $g(x)|p_1(x)\left(\frac{x^n-1}{g(x)}\right)$ and $a_{k-1}(x)|p_1(x)\left(\frac{x^n-1}{g(x)}\right)$, $a_{k-1}(x)|p_2(x)\left(\frac{x^n-1}{g(x)}\right)\left(\frac{x^n-1}{g(x)}\right), \ldots, a_{k-1}(x)|p_{k-1}(x)\underbrace{\left(\frac{x^n-1}{g(x)}\right)\cdots\left(\frac{x^n-1}{g(x)}\right)}_{k-1 \text{ times}}$ and $\deg p_{k-1}(x) < \deg a_{k-1}(x)$. Similarly we get the simpler form for C_k if we have $a_{k-1}, a_{k-2}, \ldots, a_i \neq g(x)$ but $a_{i-1} = g(x)$ for $i > 1$.

If n is relatively prime to p, then the following theorem follows from [10, Theorems 3.4–3.6].

Theorem 3.4 *Let C_k be a cyclic code over $R_{k,p} = \mathbb{Z}_p + u\mathbb{Z}_p + u^2\mathbb{Z}_p + \cdots + u^{k-1}\mathbb{Z}_p$, $u^k = 0$. If n is relatively prime to p, then we have $C_k = \langle g(x),\ ua_1(x),\ u^2a_2(x), \ldots, u^{k-1}a_{k-1}(x)\rangle = \langle g(x) + ua_1(x) + u^2a_2(x) + \cdots + u^{k-1}a_{k-1}(x)\rangle$ over $R_{k,p}$.*

4 Ranks and minimal spanning sets

Theorem 4.1 *Let n is not relatively prime to p. Let C_2 be a cyclic code of length n over $R_{2,p} = \mathbb{Z}_p + u\mathbb{Z}_p$, $u^2 = 0$.*

(1) *If $C_2 = \langle g(x) + up(x)\rangle$ with $\deg g(x) = r$ and $(g(x) + up(x))|(x^n-1)$, then C_2 is a free module with rank $n-r$ and a basis $B_1 = \{g(x) + up(x),\ x(g(x) + up(x)), \ldots, x^{n-r-1}(g(x) + up(x))\}$, and $|C_2| = p^{2n-2r}$.*

(2) *If $C_2 = \langle g(x) + up(x),\ ua(x)\rangle$ with $\deg g(x) = r$ and $\deg a(x) = t$, then C_2 has rank $n-t$ and a minimal spanning set $B_2 = \{g(x) + up(x),\ x(g(x) + up(x)), \ldots, x^{n-r-1}(g(x) + up(x)),\ ua(x),\ xua(x), \ldots, x^{r-t-1}ua(x)\}$, and $|C_2| = p^{2n-r-t}$.*

Proof (1) Suppose $x^n - 1 = (g(x) + up(x))(h(x) + uh_1(x))$ over $R_{2,p}$. Let $c(x) \in C_2 = \langle g(x) + up(x)\rangle$, then $c(x) = (g(x) + up(x))f(x)$ for some polynomial $f(x)$. If $\deg f(x) \le n - r - 1$, then $c(x)$ can be written as linear combinations of elements of B_1. Otherwise by the division algorithm there exist polynomials $q(x)$ and $r(x)$ such that

$$f(x) = \left(\frac{x^n - 1}{g(x) + up(x)}\right)q(x) + r(x) \quad \text{where } r(x) = 0 \text{ or } \deg r(x) \le n - r - 1.$$

This gives,

$$(g(x)+up(x))f(x) = (g(x)+up(x))\left(\left(\frac{x^n-1}{g(x)+up(x)}\right)q(x)+r(x)\right)$$
$$= (g(x)+up(x))r(x).$$

Since $\deg r(x) \leq n-r-1$, this shows that B_1 spans C_2. Now we only need to show that B_1 is linearly independent. Let $g(x) = g_0 + g_1x + \cdots + g_rx^r$ and $p(x) = p_0 + p_1x + \cdots + p_lx^l$, $g_0 \in \mathbb{Z}_p^{\times}$, $g_i,\ p_{i-1} \in \mathbb{Z}_p,\ i \geq 1$. Suppose

$$(g(x)+up(x))c_0 + x(g(x)+up(x))c_1 + \cdots + x^{n-r-1}(g(x)+up(x))c_{n-r-1} = 0.$$

By comparing the coefficients in the above equation, we get

$$(g_0+up_0)\,c_0 = 0 \text{ (constant coefficient)}.$$

Since (g_0+up_0) is unit, we get $c_0 = 0$. Thus,

$$x(g(x)+up(x))c_1 + \cdots + x^{n-r-1}(g(x)+up(x))c_{n-r-1} = 0.$$

Again comparing the coefficients, we get

$$(g_0+up_0)\,c_1 = 0 \text{ (coefficient of } x).$$

As above, this gives $c_1 = 0$. Continuing in this way we get that $c_i = 0$ for all $i = 0,\ 1, \ldots, n-r-1$. Therefore, the set B_1 is linearly independent and hence a basis for C_2.

(2) If $C_2 = \langle g(x)+up(x),\ ua(x)\rangle$ with $\deg g(x) = r$ and $\deg a(x) = t$. The polynomial $a(x)$ is the lowest degree polynomial such that $ua(x) \in C_2$. It is suffices to show that B_2 spans $B = \{g(x)+up(x),\ x(g(x)+up(x)), \ldots, x^{n-r-1}(g(x)+up(x)),\ ua(x),\ xua(x), \ldots, x^{n-t-1}ua(x)\}$. We first show that $ux^{r-t}a(x) \in \text{span}(B_2)$. Let the leading coefficients of $x^{r-t}a(x)$ be a_0 and of $g(x)+up(x)$ be g_0. There exists a constant $c_0 \in \mathbb{Z}_p$ such that $a_0 = c_0g_0$. Then we have

$$ux^{r-t}a(x) = uc_0(g(x)+up(x)) + um(x),$$

where $m(x)$ is a polynomial of degree less than r such that $um(x) \in C_2$. Since $C_2 = \langle g(x)+up(x),\ ua(x)\rangle$, any polynomial $p(x)$ such that $up(x)$ is in C_2 must have degree greater or equal to $\deg a(x) = t$. Hence, $t \leq \deg m(x) < r$ and

$$um(x) = \alpha_0 ua(x) + \alpha_1 xua(x) + \cdots + \alpha_{r-t-1}x^{r-t-1}ua(x).$$

Thus, $ux^{r-t}a(x) \in \text{span}(B_2)$. Inductively, we can show that $ux^{r-t+1}a(x), \ldots, ux^{n-t-1}a(x) \in \text{span}(B_2)$. Hence, B_2 is a generating set. As in (1), by comparing the coefficients we can see that B_2 is linearly independent. Therefore, B_2 is a minimal spanning set and $|C_2| = p^{2n-r-t}$. □

Following the same process as in the above theorem, we can find the rank and the minimal spanning set of any cyclic code over the ring $R_{k,p},\ k \geq 1$.

Theorem 4.2 *Let n is not relatively prime to p. Let C_k be a cyclic code of length n over $R_{k,p} = \mathbb{Z}_p + u\mathbb{Z}_p + \cdots + u^{k-1}\mathbb{Z}_p$, $u^k = 0$. We assume the constraints on the generator polynomials of C_k as in Theorem 3.3.*

(1) *If $C_k = \langle g(x)+up_1(x)+u^2p_2(x)+\cdots+u^{k-1}p_{k-1}(x)\rangle$ with $\deg g(x) = r$, then C_k is a free module with rank $n-r$ and a basis $B_1 = \{g(x)+up_1(x)+\cdots+u^{k-1}p_{k-1}(x),\ x(g(x)+up_1(x)+\cdots+u^{k-1}p_{k-1}(x)), \ldots, x^{n-r-1}(g(x)+up_1(x)+\cdots+u^{k-1}p_{k-1}(x))\}$.*

(2) If $C_k = < g(x) + up_1(x) + u^2p_2(x) + \cdots + u^{k-1}p_{k-1}(x), ua_1(x) + u^2q_1(x) + \cdots + u^{k-1}q_{k-2}(x), u^2a_2(x) + u^3l_1(x) + \cdots + u^{k-1}l_{k-3}(x), \ldots, u^{k-2}a_{k-2}(x) + u^{k-1}t_1(x), u^{k-1}a_{k-1}(x) >$ *with deg* $g(x) = r_1$, *deg* $a_1(x) = r_2$, *deg* $a_2(x) = r_3, \ldots,$ *deg* $a_{k-1}(x) = r_k$, *then* C_k *has rank* $n - r_k$ *and a minimal spanning set* $B_2 = \{g(x) + up_1(x) + \cdots + u^{k-1}p_{k-1}(x), x(g(x) + up_1(x) + \cdots + u^{k-1}p_{k-1}(x)), \ldots, x^{n-r_1-1}(g(x) + up_1(x) + \cdots + u^{k-1}p_{k-1}(x)), ua_1(x) + u^2q_1(x) + \cdots + u^{k-1}q_{k-2}(x), x(ua_1(x) + u^2q_1(x) + \cdots + u^{k-1}q_{k-2}(x)), \ldots, x^{r_1-r_2-1}(ua_1(x) + u^2q_1(x) + \cdots + u^{k-1}q_{k-2}(x)), u^2a_2(x) + u^3l_1(x) + \cdots + u^{k-1}l_{k-3}(x), x(u^2a_2(x) + u^3l_1(x) + \cdots + u^{k-1}l_{k-3}(x)), \ldots, x^{r_2-r_3-1}(u^2a_2(x) + u^3l_1(x) + \cdots + u^{k-1}l_{k-3}(x)), \ldots, u^{k-1}a_{k-1}(x), xu^{k-1}a_{k-1}(x), \ldots, x^{r_{k-1}-r_k-1}u^{k-1}a_{k-1}(x)\}$.

Proof (1) The proof is same as in Theorem 4.1. Suppose

$$x^n - 1 = \left(g(x) + up_1(x) + \cdots + u^{k-1}p_{k-1}(x)\right)\left(h(x) + uh_1(x) + \cdots + u^{k-1}h_{k-1}(x)\right),$$

over $R_{k,p}$. Suppose $x^n - 1 = (g(x) + up_1(x))(h(x) + uh_1(x))$ over $R_{2,p}$. Let $c(x) \in C_k = \langle g(x) + up_1(x) + u^2p_2(x) + \cdots + u^{k-1}p_{k-1}(x)\rangle$, then $c(x) = (g(x) + up_1(x) + u^2p_2(x) + \cdots + u^{k-1}p_{k-1}(x))f(x)$ for some polynomial $f(x)$. If $\deg f(x) \leq n - r - 1$, then $c(x)$ can be written as linear combinations of elements of B_1. Otherwise by the division algorithm there exist polynomials $q(x)$ and $r(x)$ such that

$$f(x) = \left(\frac{x^n - 1}{g(x) + up_1(x) + \cdots + u^{k-1}p_{k-1}(x)}\right)q(x) + r(x),$$

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

$$\left(g(x) + up_1(x) + \cdots + u^{k-1}p_{k-1}(x)\right)f(x) = \left(g(x) + up_1(x) + \cdots + u^{k-1}p_{k-1}(x)\right)r(x).$$

Since $\deg r(x) \leq n - r - 1$, this shows that B_1 spans C_k. Now we only need to show that B_1 is linearly independent. Let $g(x) = g_0 + g_1x + \cdots + g_rx^r$ and $p_1(x) = p_{1,0} + p_{1,1}x + \cdots + p_{1,l_1}x^{l_1}$, $p_2(x) = p_{2,0} + p_{2,1}x + \cdots + p_{2,l_2}x^{l_2}, \ldots, p_{k-1}(x) = p_{k-1,0} + p_{k-1,1}x + \cdots + p_{k-1,l_{k-1}}x^{l_{k-1}}$, $g_0 \in \mathbb{Z}_p^{\times}$, g_i, $p_{j,i-1} \in \mathbb{Z}_p$, i, $j \geq 1$. Suppose $(g(x) + up_1(x) + \cdots + u^{k-1}p_{k-1}(x))c_0 + x(g(x) + up_1(x) + \cdots + u^{k-1}p_{k-1}(x))c_1 + \cdots + x^{n-r-1}(g(x) + up_1(x) + \cdots + u^{k-1}p_{k-1}(x))c_{n-r-1} = 0$. By comparing the coefficients in the above equation, we get

$$\left(g_0 + up_{1,0} + \cdots + u^{k-1}p_{k-1,0}\right)c_0 = 0 \text{ (constant coefficient)}.$$

Since $(g_0 + up_{1,0} + \cdots + u^{k-1}p_{k-1,0})$ is unit, we get $c_0 = 0$. Thus, $x(g(x) + up_1(x) + \cdots + u^{k-1}p_{k-1}(x))c_1 + \cdots + x^{n-r-1}(g(x) + up_1(x) + \cdots + u^{k-1}p_{k-1}(x))c_{n-r-1} = 0$. Again comparing the coefficients, we get

$$\left(g_0 + up_{1,0} + \cdots + u^{k-1}p_{k-1,0}\right)c_1 = 0 \text{ (coefficient of } x).$$

As above, this gives $c_1 = 0$. Continuing in this way we get that $c_i = 0$ for all $i = 0, 1, \ldots, n - r - 1$. Therefore, the set B_1 is linearly independent and hence a basis for C_k.

(2) If $C_k = \langle g(x) + up_1(x) + \cdots + u^{k-1}p_{k-1}(x), ua_1(x) + u^2q_1(x) + \cdots + u^{k-1}q_{k-2}(x), u^2a_2(x) + u^3l_1(x) + \cdots + u^{k-1}l_{k-3}(x), \ldots, u^{k-2}a_{k-2}(x) + u^{k-1}t_1(x), u^{k-1}a_{k-1}(x)\rangle$ with $\deg(g(x) + up_1(x) + \cdots + u^{k-1}p_{k-1}(x)) = r_1$, $\deg(a_1(x)) = r_2$, $\deg(a_2(x)) = r_3, \ldots,$ and $\deg(a_{k-1}(x)) = r_k$. The polynomial $a(x)$ is the lowest degree polynomial such that $u^{k-1}a_{k-1}(x) \in C_k$. It is suffices to show that B_2 spans $B = \{g(x) + up_1(x) + \cdots + u^{k-1}p_{k-1}(x), x(g(x) + up_1(x) + \cdots + u^{k-1}p_{k-1}(x)), \ldots, x^{n-r_1-1}(g(x) + up_1(x) + \cdots + u^{k-1}p_{k-1}(x)), ua_1(x) + u^2q_1(x) + \cdots + u^{k-1}q_{k-2}(x), x(ua_1(x) + u^2q_1(x) +$

$\cdots + u^{k-1}q_{k-2}(x)), \ldots, x^{r_1-r_2-1}(ua_1(x) + u^2q_1(x) + \cdots + u^{k-1}q_{k-2}(x)),\ u^2a_2(x) + u^3l_1(x) + \cdots + u^{k-1}l_{k-3}(x),\ x(u^2a_2(x) + u^3l_1(x) + \cdots + u^{k-1}l_{k-3}(x)), \ldots, x^{r_2-r_3-1}(u^2a_2(x) + u^3l_1(x) + \cdots + u^{k-1}l_{k-3}(x)), \ldots, u^{k-1}a_{k-1}(x),\ xu^{k-1}a_{k-1}(x), \ldots, x^{n-r_k-1}u^{k-1}a_{k-1}(x)\}$. As in the proof of part 2 of Theorem 4.1, it is suffices to show that $u^{k-1}x^{r_{k-1}-r_k}a_{k-1}(x) \in \text{span}(B_2)$. Let the leading coefficients of $x^{r_{k-1}-r_k}a_{k-1}(x)$ be a_0 and of $g(x)+up_1(x)+\cdots+u^{k-1}p_{k-1}(x)$ be g_0. There exists a constant $c_0 \in \mathbb{Z}_p$ such that $a_0 = c_0g_0$. Then we have $u^{k-1}x^{r_{k-1}-r_k}a_{k-1}(x) = u^{k-1}c_0\left(g(x)+up_1(x)+\cdots+u^{k-1}p_{k-1}(x)\right) + u^{k-1}m(x)$, where $m(x)$ is a polynomial of degree less than r_{k-1} such that $u^{k-1}m(x) \in C_k$. Any polynomial $p(x)$ such that $u^{k-1}p(x)$ is in C_k must have degree greater or equal to $\deg(a_{k-1}(x)) = r_k$. Hence, $r_k \le \deg m(x) < r_{k-1}$ and $u^{k-1}m(x) = \alpha_0u^{k-1}a_{k-1}(x) + \alpha_1xu^{k-1}a_{k-1}(x) + \cdots + \alpha_{r_{k-1}-r_k-1}x^{r_{k-1}-r_k-1}u^{k-1}a_{k-1}(x)$. Thus, $u^{k-1}x^{r_{k-1}-r_k}a_{k-1}(x) \in \text{span}(B_2)$. Hence, B_2 is a generating set. As in (1), by comparing the coefficients we can see that B_2 is linearly independent. Therefore, B_2 is a minimal spanning set. □

5 Minimum distance

Let n is not relatively prime to p. Let $C_2 = \langle g(x)+up(x),\ ua(x)\rangle$ be a cyclic code of length n over $R_{2,p} = \mathbb{Z}_p + u\mathbb{Z}_p,\ u^2 = 0$. We define $C_{2,u} = \{k(x) \in R_{2,p,n} : uk(x) \in C_2\}$. It is easy to see that $C_{2,u}$ is a cyclic code over $\mathbb{Z}_p$. Let C_k be a cyclic code of length n over $R_{k,p} = \mathbb{Z}_p + u\mathbb{Z}_p + \cdots + u^{k-1}\mathbb{Z}_p,\ u^k = 0$. We define $C_{k,u^{k-1}} = \{k(x) \in R_{k,p,n} : u^{k-1}k(x) \in C_k\}$. Again it is easy to see that $C_{k,u^{k-1}}$ is a cyclic code over $\mathbb{Z}_p$.

Theorem 5.1 *Let n is not relatively prime to p. If $C_k = \langle g(x) + up_1(x) + u^2p_2(x) + \cdots + u^{k-1}p_{k-1}(x),\ ua_1(x) + u^2q_1(x) + \cdots + u^{k-1}q_{k-2}(x),\ u^2a_2(x) + u^3l_1(x) + \cdots + u^{k-1}l_{k-3}(x), \ldots, u^{k-2}a_{k-2}(x) + u^{k-1}t_1(x),\ u^{k-1}a_{k-1}(x)\rangle$ is a cyclic code of length n over $R_{k,p} = \mathbb{Z}_p + u\mathbb{Z}_p + \cdots + u^{k-1}\mathbb{Z}_p,\ u^k = 0$. Then $C_{k,u^{k-1}} = \langle a_{k-1}(x)\rangle$ and $w_H(C_k) = w_H(C_{k,u^{k-1}})$.*

Proof We have $u^{k-1}a_{k-1}(x) \in C_k$, thus $\langle a_{k-1}(x)\rangle \subseteq C_{k,u^{k-1}}$. If $b(x) \in C_{k,u^{k-1}}$, then $u^{k-1}b(x) \in C_k$ and hence there exist polynomials $b_1(x), \ldots, b_k(x) \in \mathbb{Z}_p[X]$ such that $u^{k-1}b(x) = b_1(x)u^{k-1}g(x) + b_2(x)u^{k-1}a_1(x) + b_2(x)u^{k-1}a_2(x) + \cdots + b_k(x)u^{k-1}a_{k-1}(x)$. Since $a_{k-1}(x)|a_{k-2}(x)|\cdots|a_2(x)|a_1(x)|g(x)$, we have $u^{k-1}b(x) = m(x)u^{k-1}a_{k-1}(x)$ for some polynomial $m(x) \in \mathbb{Z}_p[x]$. So, $C_{k,u^{k-1}} \in \langle a_{k-1}(x)\rangle$, and hence $C_{k,u^{k-1}} = \langle a_{k-1}(x)\rangle$. Let $m(x) = m_0(x) + um_1(x) + \cdots + u^{k-1}m_{k-1}(x) \in C_k$, where $m_0(x), m_1(x), \ldots, m_{k-1}(x) \in \mathbb{Z}_p[x]$. We have $u^{k-1}m(x) = u^{k-1}m_0(x)$, $w_H(u^{k-1}m(x)) \le w_H(m(x))$ and $u^{k-1}C_k$ is subcode of C_k with $w_H(u^{k-1}C_k) \le w_H(C_k)$. Therefore, it is sufficient to focus on the subcode $u^{k-1}C_k$ in order to prove the theorem. Since $u^{k-1}C_k = \langle u^{k-1}a_{k-1}(x)\rangle$, we get $w_H(C_k) = w_H(C_{k,u^{k-1}})$. □

Definition 5.2 Let $m = b_{l-1}p^{l-1} + b_{l-2}p^{l-2} + \cdots + b_1p + b_0,\ b_i \in \mathbb{Z}_p,\ 0 \le i \le l-1$, be the p-adic expansion of m.

(1) If $b_{l-i} \neq 0$ for all $1 \le i \le q,\ q < l$, and $b_{l-i} = 0$ for all $i,\ q+1 \le i \le l$, then m is said to have a p-adic length q zero expansion.
(2) If $b_{l-i} \neq 0$ for all $1 \le i \le q,\ q < l,\ b_{l-q-1} = 0$ and $b_{l-i} \neq 0$ for some $i,\ q+2 \le i \le l$, then m is said to have p-adic length q non-zero expansion.
(3) If $b_{l-i} \neq 0$ for $1 \le i \le l$, then m is said to have a p-adic length l expansion or p-adic full expansion.

Lemma 5.3 *Let C be a cyclic code over $R_{k,p}$ of length p^l where l is a positive integer. Let $C = \langle a(x)\rangle$ where $a(x) = (x^{p^{l-1}} - 1)^b h(x)$, $1 \le b < p$. If $h(x)$ generates a cyclic code of length p^{l-1} and minimum distance d then the minimum distance $d(C)$ of C is $(b+1)d$.*

Proof For $c \in C$, we have $c = (x^{p^{l-1}} - 1)^b h(x)m(x)$ for some $m(x) \in \frac{R_{k,p}[x]}{(x^{p^l}-1)}$. Since $h(x)$ generates a cyclic code of length p^{l-1}, we have $w(c) = w((x^{p^{l-1}} - 1)^b h(x)m(x)) = w(x^{p^{l-1}b}h(x)m(x)) + w({}^bC_1 x^{p^{l-1}(b-1)}h(x)m(x)) + \cdots + w({}^bC_{b-1}x^{p^{l-1}}h(x)m(x)) + w(h(x)m(x))$. Thus, $d(C) = (b+1)d$. □

Theorem 5.4 *Let C_k be a cyclic code over $R_{k,p}$ of length p^l where l is a positive integer. Then, $C_k = \langle g(x) + up_1(x) + u^2p_2(x) + \cdots + u^{k-1}p_{k-1}(x),\ ua_1(x) + u^2q_1(x) + \cdots + u^{k-1}q_{k-2}(x),\ u^2a_2(x) + u^3l_1(x) + \cdots + u^{k-1}l_{k-3}(x), \ldots, u^{k-2}a_{k-2}(x) + u^{k-1}t_1(x),\ u^{k-1}a_{k-1}(x)\rangle$ where $g(x) = (x-1)^{t_1}$, $a_1(x) = (x-1)^{t_2}, \cdots, a_{k-1}(x) = (x-1)^{t_k}$. for some $t_1 > t_2 > \cdots > t_k > 0$.*

(1) *If $t_k \le p^{l-1}$, then $d(C) = 2$.*
(2) *If $t_k > p^{l-1}$, let $t_k = b_{l-1}p^{l-1} + b_{l-2}p^{l-2} + \cdots + b_1p + b_0$ be the p-adic expansion of t_k and $a_{k-1}(x) = (x-1)^{t_k} = (x^{p^{l-1}} - 1)^{b_{l-1}}(x^{p^{l-2}} - 1)^{b_{l-2}} \cdots (x^{p^1} - 1)^{b_1}(x^{p^0} - 1)^{b_0}$.*
   (a) *If t_k has a p-adic length q zero expansion or full expansion ($l = q$). Then, $d(C_k) = (b_{l-1}+1)(b_{l-2}+1)\cdots(b_{l-q}+1)$.*
   (b) *If t_k has a p-adic length q non-zero expansion. Then, $d(C_k) = 2(b_{l-1}+1)(b_{l-2}+1)\cdots(b_{l-q}+1)$.*

Proof The first claim easily follows from Theorem 3.3. From Theorem 5.1, we see that $d(C_k) = d(u^{k-1}C_k) = d((x-1)^{t_k})$. hence, we only need to determine the minimum weight of $u^{k-1}C_k = (x-1)^{t_k}$.

(1) If $t_k \le p^{l-1}$, then $(x-1)^{t_k}(x-1)^{p^{l-1}-t_k} = (x-1)^{p^{l-1}} = (x^{p^{l-1}} - 1) \in C_k$. Thus, $d(C_k) = 2$.
(2) Let $t_k > p^{l-1}$.
   (a) If t_k has a p-adic length q zero expansion, we have $t_k = b_{l-1}p^{l-1} + b_{l-2}p^{l-2} + \cdots + b_{l-q}p^{l-q}$, and $a_{k-1}(x) = (x-1)^{t_k} = (x^{p^{l-1}} - 1)^{b_{l-1}}(x^{p^{l-2}} - 1)^{b_{l-2}} \cdots (x^{p^{l-q}} - 1)^{b_{l-q}}$. Let $h(x) = (x^{p^{l-q}} - 1)^{b_{l-q}}$. Then $h(x)$ generates a cyclic code of length p^{l-q+1} and minimum distance $(b_{l-q}+1)$. By Lemma 5.3, the subcode generated by $(x^{p^{l-q+1}} - 1)^{b_{l-q+1}}h(x)$ has minimum distance $(b_{l-q+1}+1)(b_{l-q}+1)$. By induction on q, we can see that the code generated by $a_{k-1}(x)$ has minimum distance $(b_{l-1}+1)(b_{l-2}+1)\cdots(b_{l-q}+1)$. Thus, $d(C_k) = (b_{l-1}+1)(b_{l-2}+1)\cdots(b_{l-q}+1)$.
   (b) If t_k has a p-adic length q non-zero expansion, we have $t_k = b_{l-1}p^{l-1} + b_{l-2}p^{l-2} + \cdots + b_1p + b_0,\ b_{l-q-1}$. Let $r = b_{l-q-2}p^{l-q-2} + b_{l-q-3}p^{l-q-3} + \cdots + b_1p + b_0$ and $h(x) = (x-1)^r = (x^{p^{l-q-2}} - 1)^{b_{l-q-2}}(x^{p^{l-q-3}} - 1)^{b_{l-q-3}} \cdots (x^{p^1} - 1)^{b_1}(x^{p^0} - 1)^{b_0}$. Since $r < p^{l-q-1}$, we have $p^{l-q-1} = r + j$ for some non-zero j. Thus, $(x-1)^{p^{l-q-1}-j}h(x) = (x^{p^{l-q-1}} - 1) \in C_k$. Hence, the subcode generated by $h(x)$ has minimum distance 2. By Lemma 5.3, the subcode generated by $(x^{p^{l-q}} - 1)^{b_{l-q}}h(x)$ has minimum distance $2(b_{l-q}+1)$. By induction on q, we can see that the code generated by $a_{k-1}(x)$ has minimum distance $2(b_{l-1}+1)(b_{l-2}+1)\cdots(b_{l-q}+1)$. Thus, $d(C_k) = 2(b_{l-1}+1)(b_{l-2}+1)\cdots(b_{l-q}+1)$. □

Table 1 Cyclic codes of length 5 over $R_{4,3} = \mathbb{Z}_3 + u\mathbb{Z}_3 + u^2\mathbb{Z}_3 + u^3\mathbb{Z}_3,\ u^4 = 0$

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

Table 2 Non-zero free module cyclic codes of length 5 over $\mathbb{Z}_5 + u\mathbb{Z}_5,\ u^2 = 0$

Non-zero generator polynomials	$d(C)$	Ranks
$\langle 1\rangle$	1	5
$\langle g + uc_0\rangle,\ c_0 \in \mathbb{Z}_5$	2	4
$\langle g^2 + u(c_0 + c_1x)\rangle,\ c_0,\ c_1 \in \mathbb{Z}_5$	3	3
$\langle g^3 + u(c_0 + c_1x - (c_0 + c_1)x^2)\rangle,\ c_0,\ c_1 \in \mathbb{Z}_5$	4	2
$\langle g^4 + uc_0(4x^3 + 3x^2 + 2x + 1)\rangle,\ c_0 \in \mathbb{Z}_5$	5	1

Table 3 Non-free module cyclic codes of length 5 over $\mathbb{Z}_5 + u\mathbb{Z}_5,\ u^2 = 0$

Non-zero generator polynomials	$d(C)$	Ranks
$\langle u\rangle,\ \langle g^i,\ u\rangle,\ 1 \le i \le 4$	1	5
$\langle ug\rangle$	2	4
$\langle ug^2\rangle$	3	3
$\langle ug^3\rangle$	4	2
$\langle ug^4\rangle$	5	1
$\langle g^2 + uc_0,\ ug\rangle,\ c_0 \in \mathbb{Z}_5$	2	4
$\langle g^3 + uc_0,\ ug\rangle,\ c_0 \in \mathbb{Z}_5$	2	4
$\langle g^3 + u(c_0 + c_1x),\ ug^2\rangle,\ c_0,\ c_1 \in \mathbb{Z}_5$	3	3
$\langle g^4 + uc_0,\ ug\rangle,\ c_0 \in \mathbb{Z}_5$	2	4
$\langle g^4 + uc_0g,\ ug^2\rangle,\ c_0 \in \mathbb{Z}_5$	3	3
$\langle g^4 + uc_0g^2,\ ug^3\rangle,\ c_0 \in \mathbb{Z}_5$	4	2

6 Examples

In this section, we give some examples of cyclic codes of different lengths over the ring $R_{k,p}$.

Example 6.1 Cyclic codes of length 5 over $R_{4,3} = \mathbb{Z}_3 + u\mathbb{Z}_3 + u^2\mathbb{Z}_3 + u^3\mathbb{Z}_3,\ u^4 = 0$: We have

$$x^5 - 1 = (x - 1)\left(x^4 + x^3 + x^2 + x + 1\right) \text{ over } R_{4,3}.$$

Let $g_1 = x - 1$ and $g_2 = x^4 + x^3 + x^2 + x + 1$. The non-zero cyclic codes of length 5 over $R_{4,3}$ with generator polynomial are given in Table 1.

Example 6.2 Cyclic codes of length 5 over $R_{2,5} = \mathbb{Z}_5 + u\mathbb{Z}_5,\ u^2 = 0$: We have

$$x^5 - 1 = (x - 1)^5 = g^5 \text{ over } R_{2,5}.$$

Table 4 Non-zero free module cyclic codes of length 9 over $\mathbb{Z}_3 + u\mathbb{Z}_3,\ u^2 = 0$

Non-zero generator polynomials	$d(C)$	Ranks
$\langle 1\rangle$	1	9
$\langle g + uc_0\rangle,\ c_0 \in \mathbb{Z}_3$	2	8
$\langle g^2 + u(c_0 + c_1x)\rangle,\ c_0,\ c_1 \in \mathbb{Z}_3$	2	7
$\langle g^3 + u(c_0 + c_1x + c_2x^2)\rangle,\ c_0,\ c_1,\ c_2 \in \mathbb{Z}_3$	2	6
$\langle g^4 + u(c_0 + c_1x + c_2x^2 + c_3x^3)\rangle,\ c_0,\ c_1,\ c_2 \in \mathbb{Z}_3$	4	5
$\langle g^5 + u(c_0 + c_1x + c_2x^2 + c_3x^3 - (c_0 + c_1 + c_2 + c_3)x^4)\rangle, c_0,\ c_1,\ c_2,\ c_3 \in \mathbb{Z}_3$	6	4
$\langle g^6 + u(c_0 + c_1x + c_2x^2 - c_0x^3 - c_1x^4 - c_2x^5)\rangle,\ c_0,\ c_1,\ c_2 \in \mathbb{Z}_3$	3	3
$\langle g^7 + u(c_0 + c_1x + c_1x^2 + (c_0 + c_1)x^3 - c_1x^4 - c_1x^5 + (c_0 - c_1)x^6)\rangle,\ c_0,\ c_1 \in \mathbb{Z}_3$	6	2
$\langle g^8 + uc_0(1 - x + x^3 - x^4 + x^6 - x^7)\rangle,\ c_0 \in \mathbb{Z}_3$	9	1

Table 5 Non-free module cyclic codes of length 9 over $\mathbb{Z}_3 + u\mathbb{Z}_3,\ u^2 = 0$

Non-zero generator polynomials	$d(C)$	Ranks
$\langle u\rangle,\ \langle g^i,\ u\rangle,\ 1 \le i \le 8$	1	9
$\langle ug\rangle,\ 1 \le i \le 3$	2	8
$\langle ug^2\rangle,\ 1 \le i \le 3$	2	7
$\langle ug^3\rangle,\ 1 \le i \le 3$	2	6
$\langle ug^4\rangle$	4	5
$\langle ug^5\rangle$	6	4
$\langle ug^6\rangle$	3	3
$\langle ug^7\rangle$	6	2
$\langle ug^8\rangle$	9	1
$\langle g^2 + uc_0,\ ug\rangle,\ c_0 \in \mathbb{Z}_3$	2	8
$\langle g^3 + uc_0,\ ug\rangle,\ c_0 \in \mathbb{Z}_3$	2	8
$\langle g^3 + u(c_0 + c_1x),\ ug^2\rangle,\ c_0,\ c_1 \in \mathbb{Z}_3$	2	7
$\langle g^4 + uc_0,\ ug\rangle,\ c_0 \in \mathbb{Z}_3$	2	8
$\langle g^4 + u(c_0 + c_1x),\ ug^2\rangle,\ c_0,\ c_1 \in \mathbb{Z}_3$	2	7
$\langle g^4 + u(c_0 + c_1x + c_2x^2),\ ug^3\rangle,\ c_0,\ c_1,\ c_2 \in \mathbb{Z}_3$	2	6
$\langle g^5 + uc_0,\ ug\rangle,\ c_0 \in \mathbb{Z}_3$	2	8
$\langle g^5 + u(c_0 + c_1x),\ ug^2\rangle,\ c_0,\ c_1 \in \mathbb{Z}_3$	2	7
$\langle g^5 + u(c_0 + c_1x + c_2x^2),\ ug^3\rangle,\ c_0,\ c_1,\ c_2 \in \mathbb{Z}_3$	2	6
$\langle g^5 + u(c_0 + c_1x + c_2x^2 + c_3x^3),\ ug^4\rangle,\ c_0,\ c_1,\ c_2,\ c_3 \in \mathbb{Z}_3$	4	5
$\langle g^6 + uc_0,\ ug\rangle,\ c_0 \in \mathbb{Z}_3$	2	8
$\langle g^6 + u(c_0 + c_1x),\ ug^2\rangle,\ c_0,\ c_1 \in \mathbb{Z}_3$	2	7
$\langle g^6 + u(c_0 + c_1x + c_2x^2),\ ug^3\rangle,\ c_0,\ c_1,\ c_2 \in \mathbb{Z}_3$	2	6
$\langle g^6 + u(c_0 + c_1x + c_2x^2)g,\ ug^4\rangle,\ c_0,\ c_1,\ c_2 \in \mathbb{Z}_3$	4	5
$\langle g^6 + u(c_0 + c_1x + c_2x^2)g^2,\ ug^5\rangle,\ c_0,\ c_1,\ c_2 \in \mathbb{Z}_3$	6	4

Table 5 continued

Non-zero generator polynomials	$d(C)$	Ranks
$\langle g^7 + uc_0,\ ug\rangle,\ c_0 \in \mathbb{Z}_3$	2	8
$\langle g^7 + u(c_0 + c_1x),\ ug^2\rangle,\ c_0,\ c_1 \in \mathbb{Z}_3$	2	7
$\langle g^7 + u(c_0 + c_1x)g,\ ug^3\rangle,\ c_0,\ c_1 \in \mathbb{Z}_3$	2	6
$\langle g^7 + u(c_0 + c_1x)g^2,\ ug^4\rangle,\ c_0,\ c_1 \in \mathbb{Z}_3$	4	5
$\langle g^7 + u(c_0 + c_1x)g^3,\ ug^5\rangle,\ c_0,\ c_1 \in \mathbb{Z}_3$	6	4
$\langle g^7 + u(c_0 + c_1x)g^4,\ ug^6\rangle,\ c_0,\ c_1 \in \mathbb{Z}_3$	3	3
$\langle g^8 + uc_0,\ ug\rangle,\ c_0 \in \mathbb{Z}_3$	2	8
$\langle g^8 + uc_0g,\ ug^2\rangle,\ c_0 \in \mathbb{Z}_3$	2	7
$\langle g^8 + uc_0g^2,\ ug^3\rangle,\ c_0 \in \mathbb{Z}_3$	2	6
$\langle g^8 + uc_0g^3,\ ug^4\rangle,\ c_0 \in \mathbb{Z}_3$	4	5
$\langle g^8 + uc_0g^4,\ ug^5\rangle,\ c_0 \in \mathbb{Z}_3$	6	4
$\langle g^8 + uc_0g^5,\ ug^6\rangle,\ c_0 \in \mathbb{Z}_3$	3	3
$\langle g^8 + uc_0g^6,\ ug^7\rangle,\ c_0 \in \mathbb{Z}_3$	6	2

The non-zero cyclic codes of length 5 over $R_{2,5}$ with generator polynomial and minimum distance are given in Tables 2 and 3.

Example 6.3 Cyclic codes of length 9 over $\mathbb{Z}_3 + u\mathbb{Z}_3,\ u^2 = 0$: We have

$$x^9 - 1 = (x - 1)^9 = g^9 \text{ over } R_{2,3}.$$

The non-zero cyclic codes of length 9 over $R_{2,3}$ with generator polynomial and minimum distance are given in Tables 4 and 5.

References

1. Abualrub T., Oehmke R.H.: On the generators of Z_4 cyclic codes of length 2^e. IEEE Trans. Inf. Theory **49**(9), 2126–2133 (2003).
2. Abualrub T., Siap I.: Cyclic codes over the rings $Z_2 + uZ_2$ and $Z_2 + uZ_2 + u^2Z_2$. Des. Codes Cryptogr. **42**(3), 273–287 (2007).
3. Abualrub T., Ghrayeb A., Oehmke R.H.: A mass formula and rank of Z_4 cyclic codes of length 2^e. IEEE Trans. Inf. Theory **50**(12), 3306–3312 (2004).
4. Al-Ashker M., Hamoudeh M.: Cyclic codes over $Z_2 + uZ_2 + u^2Z_2 + \cdots + u^{k-1}Z_2$. Turk. J. Math. **35**(4), 737–749 (2011).
5. Blackford T.: Cyclic codes over Z_4 of oddly even length. Discret. Appl. Math. **128**(1), 27–46 (2003). International Workshop on Coding and Cryptography (WCC 2001) (Paris).
6. Bonnecaze A., Udaya P.: Cyclic codes and self-dual codes over $F_2 + uF_2$. IEEE Trans. Inf. Theory **45**(4), 1250–1255 (1999).
7. Calderbank A.R., Sloane N.J.A.: Modular and p-adic cyclic codes. Des. Codes Cryptogr. **6**(1), 21–35 (1995).
8. Calderbank R.A., Rains E.M., Shor P.W., Sloane N.J.A.: Quantum error correction via codes over GF(4). IEEE Trans. Inf. Theory **44**(4), 1369–1387 (1998).
9. Conway J.H., Sloane N.J.A.: Self-dual codes over the integers modulo 4. J. Comb. Theory A **62**(1), 30–45 (1993).
10. Dinh H.Q., Lopez-Permouth S.: Cyclic and negacyclic codes over finite chain rings. IEEE Trans. Inf. Theory **50**(8), 1728–1744 (2004).
11. Dougherty S.T., Shiromoto K.: Maximum distance codes over rings of order 4. IEEE Trans. Inf. Theory **47**(1), 400–404 (2001).

12. McDonald B.R.: Finite rings with identity. In: Pure and Applied Mathematics, vol. 28. Marcel Dekker, New York (1974).
13. Pless V.S., Qian Z.: Cyclic codes and quadratic residue codes over Z_4. IEEE Trans. Inf. Theory **42**(5), 1594–1600 (1996).
14. van Lint J.H.: Repeated-root cyclic codes. IEEE Trans. Inf. Theory **37**(2), 343–345 (1991).