Self-dual Codes and Cyclic Codes over $F_p + vF_p$ *

Guanghui Zhang, Liangchen Li

Department of Mathematics, Luoyang Normal University,
Luoyang, Henan, 471022, China

Abstract

In this paper, we give a criterion to judge whether a linear code over the ring is self-dual. Moreover, we introduce the generating set in standard form for the cyclic codes over $F_p + vF_p$ and characterize the structure of cyclic codes over the ring. Then we prove that cyclic codes over the ring are principally generated and obtain the unique generating idempotent for cyclic codes of length n, where n is coprime to p.

Keywords: Cyclic codes, self-dual codes, $F_p + vF_p$.

2010 Mathematics Subject Classification: 94B05; 94B15

1 Introduction

Codes over finite rings have been studied in the early 1970s. They have received much attention recently after Hammons et al. showed that certain good nonlinear binary codes could be found as images of linear codes over $\mathbb{Z}_4$ under the Gray map [2]. However, these studies are concentrated on the situation in which the ground rings associated with codes are finite chain rings in general. In such cases, linear codes over certain finite rings have been characterized in several papers [1, 3, 5]. The case when the ground ring is not a finite chain ring seems to be more difficult. More recently, linear codes over the ring $F_p + vF_p$, where $v^2 = v$ and p is a prime, which is not a chain ring but a semi-local ring have been considered. In [8] Zhu et al. gave some results about cyclic codes over $F_2 + vF_2$, where it is shown that cyclic codes over the ring are principally generated; in [7] Zhu et al.

*E-mail addresses: zghui2012@126.com (G. Zhang); liangchen_li@163.com(L. Li).

studied $(1-2v)$-constacyclic codes over F_p+vF_p, where p is an odd prime. They determined the image of a $(1-2v)$-constacyclic code over F_p+vF_p under the Gray map and the generator polynomials of such constacyclic codes over F_p+vF_p and proved that constacyclic codes over the ring are principally generated.

In this paper, we extend previous works on the linear codes over ring F_p+vF_p in two directions. First, we explore the dual codes over the ring and under what conditions is a linear code over the ring self-dual, see Section 3. Second, we describe that the structure of cyclic codes and their duals over F_p+vF_p. Unlike the technique used in the mentioned papers, we first give the parity check matrices for linear codes over F_p+vF_p and the characterization of the torsion codes associated with the linear codes and their duals over F_p+vF_p; they are used as a tool to study linear codes over F_p+vF_p. In addition, by virtue of the generating set in standard form we try to characterize the structure of cyclic codes over F_p+vF_p, see Section 4. The necessary notations and some known results are provided in Section 2.

2 Preliminaries

Let F_p be a finite field with p elements, where p is an odd prime. Throughout this paper, let R be the commutative ring $F_p+vF_p=\{a+vb|a,b\in F_p\}$, where $v^2=v$. The ring R is a finite Frobenius ring. Let R^n be the R-module of n-tuples over R. A linear code C of length n over R is an R-submodule of R^n. For any linear code C of length n over R, the *dual code* $C^\perp$ is defined as $C^\perp=\{x\in R^n \mid x\cdot c=0,\forall c\in C\}$, where $x\cdot c$ denotes the standard Euclidean inner product x and c in R^n. Notice that $C^\perp$ is linear. If $C\subseteq C^\perp$, then C is called *self-orthogonal*. Moreover, if $C=C^\perp$, then C is called *self-dual*. In [6], it was proved that for any linear code C over a finite Frobenius ring $\widetilde{R}$, $|C||C^\perp|=|\widetilde{R}|^n$.

A linear code C of length n over R is *cyclic* if the code is invariant under the shift operator $(c_0,c_1,\cdots,c_{n-1})\mapsto(c_{n-1},c_0,\cdots,c_{n-2})$. Cyclic codes of length n over R can be identified as ideals in the quotient ring $R[x]/\langle x^n-1\rangle$ via the isomorphism from R^n to $R[x]/\langle x^n-1\rangle$ defined by $c=(c_0,c_1,\cdots,c_{n-1})\mapsto c(x)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}$. Then C is identified with the set of all polynomial representations of its codewords.

Recall some facts about the cyclic codes over finite field F_p. Every cyclic code C of length n over F_p is a principal ideal in $F_p[x]/\langle x^n-1\rangle$. Then there is a unique monic polynomial $g(x)$ of minimum degree in C. This polynomial generates C and divides x^n-1. This polynomial $g(x)$ is called the generator polynomial for C. Let $f(x)$ be a monic polynomial in $F_p[x]/\langle x^n-1\rangle$ and C a cyclic code. If $f(x)$ generates C, then $f(x)$ is the

generator polynomial in C if and only if $f(x)$ divides $x^n - 1$. It will be convenient to adopt the notation $C = \langle g(x) \rangle$ to denote the fact that C is the ideal generated by $g(x)$ and that $g(x)$ is the generator polynomial for C.

We know that the ring R has two maximal ideals $\langle v \rangle$ and $\langle 1 - v \rangle$. Their residue fields are both F_p. Thus we have two canonical projections defined as follows:

$$R = F_p + vF_p \longrightarrow R/\langle 1 - v \rangle = F_p$$

$$r + vq \longmapsto r + q;$$

and

$$R = F_p + vF_p \longrightarrow R/\langle v \rangle = F_p$$

$$r + vq \longmapsto r.$$

We simple denote these two projections by "$\widehat{\ }$" and "$-$", respectively. Denote by $\widehat{r}$ and $\overline{r}$ the images of an element $r \in R$ under these two projections, respectively. These two projections can be extended naturally from R^n to F_p^n or from $R[x]$ to $F_p[x]$.

For $k > 0$, I_k denotes the $k \times k$ identity matrix. Any nonzero linear code C over R is permutation-equivalent to a code generated by the following matrix:

$$G = \begin{pmatrix} I_{k_1} & (1-v)B_1 & vA_1 & vA_2 + (1-v)B_2 & vA_3 + (1-v)B_3 \\ 0 & vI_{k_2} & 0 & vA_4 & 0 \\ 0 & 0 & (1-v)I_{k_3} & 0 & (1-v)B_4 \end{pmatrix},$$

where A_i and B_j are matrices with entries in F_p for $i, j = 1, 2, 3, 4$. Such a code C is said to have type $p^{2k_1}p^{k_2}p^{k_3}$ and $|C| = p^{2k_1+k_2+k_3}$[4, 7]. For later convenience the above generator matrix can be written in the form:

$$G = \begin{pmatrix} I_{k_1} & (1-v)B_1 & vA_1 & vD_1 + (1-v)D_2 \\ 0 & vI_{k_2} & 0 & vC_1 \\ 0 & 0 & (1-v)I_{k_3} & (1-v)C_2 \end{pmatrix}, \qquad (*)$$

where $D_1 = (A_2, A_3), D_2 = (B_2, B_3), C_1 = (A_4, 0), C_2 = (0, B_4)$.

Note that any element c of R^n can be expressed as $c = a + vb$, where $a, b \in F_p^n$. Let C be a linear code of length n over R with generator matrix in form $(*)$. Define

$$C_1 = \{a \in F_p^n | a + vb \in C, \text{for some } b \in F_p^n\}$$

and

$$C_2 = \{a + b \in F_p^n | a + vb \in C\}.$$

Obviously, C_1 and C_2 are linear codes over F_p. The code C_1 is permutation-equivalent to a code with generator matrix of the form:

$$G_1 = \begin{pmatrix} I_{k_1} & B_1 & 0 & B_2 & B_3 \\ 0 & 0 & I_{k_3} & 0 & B_4 \end{pmatrix},$$

where B_i are p-ary matrices for $i \in \{1,2,3,4\}$. And the code C_2 is permutation-equivalent to a code with generator matrix of the form:

$$G_2 = \begin{pmatrix} I_{k_1} & 0 & A_1 & A_2 & A_3 \\ 0 & I_{k_2} & 0 & A_4 & 0 \end{pmatrix},$$

where A_i are p-ary matrices for $i \in \{1,2,3,4\}$. It is easy to see that $\dim C_1 = k_1 + k_3, \dim C_2 = k_1 + k_2$.

For a code C of length n over R, let $a \in R$. The submodule quotient is a linear code of length n over R, defined as follows:

$$(C : a) = \{x \in R^n | ax \in C\}.$$

The codes $\widehat{(C : v)}$ and $\overline{(C : (1-v))}$ over the field F_p are called the *torsion codes* associated with the code C over the ring R.

3 Self-dual codes over $F_p + vF_p$

We begin with a lemma about the torsion codes associated with the code over the ring R, which will be used throughout the paper.

Lemma 3.1. *With notations as above. Let C be a linear code of length n over R. Then (1) $\widehat{(C : v)} = C_2$; (2) $\overline{(C : (1-v))} = C_1$.*

Proof. (1) For any $y \in \widehat{(C : v)}$, there exists an $x \in (C : v)$ such that $y = \widehat{x}$. Let $x = r + vq$, where $r, q \in F_p^n$. Then $\widehat{x} = r + q$. Since $vx \in C$, we have $v(r+q) = v(r+vq) = vx \in C$, which implies that $r + q \in C_2$. Therefore $y = \widehat{x} = r + q \in C_2$. It follows that $\widehat{(C : v)} \subseteq C_2$.

Let $z \in C_2$. Then there exists an element $x + vy \in C$ such that $z = x + y$. Hence $v(x+y) = v(x+vy) \in C$ and $x + y \in (C : v)$. Thus we have that $z = x + y = \widehat{x+y} \in \widehat{(C : v)}$. Hence $\widehat{(C : v)} \supseteq C_2$. Therefore we get the desired result.

(2) Let y be an element of $\overline{(C : (1-v))}$, then there exists some $x \in (C : (1-v))$ such that $y = \overline{x}$. Suppose that $x = r + vq$, for $r, q \in F_p^n$. Then $\overline{x} = r$. From $(1-v)x \in C$ we have that $r - vr = (1-v)r = (1-v)(r+vq) = (1-v)x \in C$, which leads to $r \in C_1$. Hence $y = \overline{x} = r \in C_1$. Therefore we obtain that $\overline{(C : v)} \subseteq C_1$.

If r is an element of C_1, then we have that $r + vq \in C$ for some $q \in F_p^n$. Since $(1-v)r = (1-v)(r+vq) \in C$, which shows that $r \in (C : (1-v))$. Hence $r = \bar{r} \in \overline{(C : (1-v))}$, then $\overline{(C : (1-v))} \supseteq C_1$. Therefore $\overline{(C : (1-v))} = C_1$, as required. □

In the following, A^T denotes the transpose of the matrix A.

Theorem 3.2. *Let C be a linear code of length n over R with generator matrix in form $(*)$. Then*

(1)

$$H = \begin{pmatrix} vE_1 + (1-v)E_2 & P & Q & I_{n-k} \\ v(-A_1^T) & 0 & vI_{k_3} & 0 \\ (1-v)(-B_1^T) & (1-v)I_{k_2} & 0 & 0 \end{pmatrix},$$

where $E_1 = (-A_2, B_4A_1 - A_3)^T$, $E_2 = (A_4B_1 - B_2, -B_3)^T$, $P = (-A_4, 0)^T$, $Q = (0, -B_4)^T$; $k = k_1 + k_2 + k_3$, is a generator matrix for $C^\perp$ and a parity check matrix for C.

(2) $(\widehat{(C : v)})^\perp = (\widehat{C^\perp : v})$; $\overline{(\widehat{(C : (1-v))})}^\perp = \overline{(C^\perp : (1-v))}$.

Proof. (1) It is straightforward to check that $HG^T = 0$. Let D be the R-submodule generated by H, then $D \subseteq C^\perp$. Since R is a Frobenius ring, we have that $|C||C^\perp| = |R|^n$. It follows that

$$|C^\perp| = \frac{|R|^n}{|C|} = \frac{p^{2n}}{p^{2k_1+k_2+k_3}} = p^{2(n-k_1)-k_2-k_3}.$$

Note that $|D| = p^{2(n-k)+k_3+k_2} = p^{2(n-k_1)-k_2-k_3}$, and we obtain that $|D| = |C^\perp|$, hence $D = C^\perp$.

(2) We first prove that $(\widehat{C^\perp : v}) \subseteq (\widehat{(C : v)})^\perp$. Let $x \in (C^\perp : v)$ and $y \in (C : v)$. Then $vx \in C^\perp$ and $vy \in C$, so $(vx)(vy)^T = 0$, i.e., $v(xy^T) = 0$. Hence $xy^T \in (1-v)R$, and $\widehat{xy}^T = 0$, which implies that $(\widehat{C^\perp : v}) \subseteq (\widehat{(C : v)})^\perp$. On the other hand, by Lemma 3.1 and Theorem 3.2(1), we have that

$$\dim(\widehat{C^\perp : v}) = n - k + k_3 = n - k_1 - k_2;$$

$$\dim\overline{(\widehat{C : v})}^\perp = n - \dim\overline{(\widehat{C : v})} = n - (k_1 + k_2) = n - k_1 - k_2.$$

Hence $\dim(\widehat{C^\perp : v}) = \dim\overline{(\widehat{C : v})}^\perp$, which follows that $(\widehat{(C : v)})^\perp = (\widehat{C^\perp : v})$.

The proof of the second equality is similar to that of the first one and is left to the reader. □

Corollary 3.3. *Let C be a linear code of length n over R with generator matrix in form $(*)$. Then C is self-dual if and only if both the following two conditions are satisfied:*

(i) C is self-orthogonal;
(ii) $n = 2(k_1 + k_2), k_2 = k_3$.

Proof. Now suppose that both Conditions (i) and (ii) are satisfied. Then we have that

$$|C| = p^{2k_1+k_2+k_3} = p^{2(k_1+k_2)}, |C^\perp| = p^{2(n-k)+k_2+k_3} = p^{2(k_1+k_2)}.$$

Note that $C \subseteq C^\perp$, and then $C = C^\perp$, that is, C is self-dual.

Suppose that C is self-dual, then C is self-orthogonal. By Lemma 3.1 and Theorem 3.2(1), we have that

$$\dim(\widehat{(C : v)}) = k_1 + k_2; \dim(\widehat{(C^\perp : v)}) = n - k + k_3 = n - k_1 - k_2,$$

and

$$\dim\overline{(C : (1-v))} = k_1 + k_3; \dim\overline{(C^\perp : (1-v))} = n - k + k_2 = n - k_1 - k_3.$$

Since $C = C^\perp$, we have that $n = 2(k_1 + k_2), k_2 = k_3$. □

Let A, B be the codes over R. We denote that $A \oplus B = \{a + b | a \in A, b \in B\}$.

Theorem 3.4. *With the above notations, let C be a linear code of length n over R. Then C can be uniquely expressed as $C = vC_2 \oplus (1-v)C_1$. Moreover, we also have $C^\perp = vC_2^\perp \oplus (1-v)C_1^\perp$.*

Proof. We first prove the uniqueness of the expression of every element in $vC_2 \oplus (1-v)C_1$. Let $va_2 + (1-v)a_1 = vb_2 + (1-v)b_1$, where $a_2, b_2 \in C_2; a_1, b_1 \in C_1$. Then $v(a_2 - b_2) = (1-v)(b_1 - a_1)$, which implies that $a_1 = b_1$ and $a_2 = b_2$. Hence $|vC_2 \oplus (1-v)C_1| = |C_1||C_2| = p^{k_1+k_3}p^{k_1+k_2} = p^{2k_1+k_2+k_3} = |C|$.

Next we prove that $vC_2 \oplus (1-v)C_1 \subseteq C$. Let $a \in (C : v)$ and $b \in (C : (1-v))$. Then $va \in C; (1-v)b \in C$. Setting $a = a_1 + (1-v)a_2, b = b_1 + vb_2$, where $a_1, a_2, b_1, b_2 \in F_p^n$. Then $\widehat{a} = a_1 \in C_2, \overline{b} = b_1 \in C_1$. Thus $v\widehat{a} + (1-v)\overline{b} = va_1 + (1-v)b_1 = va + (1-v)b \in C$. Hence $vC_2 \oplus (1-v)C_1 \subseteq C$. Note that $|vC_2 \oplus (1-v)C_1| = |C|$, therefore $C = vC_2 \oplus (1-v)C_1$.

Finally, we prove that the second statement. By the first statement, Theorem 3.2(2) and Lemma 3.1 we have that

$$\begin{aligned} C^\perp &= v(\widehat{C^\perp : v}) \oplus (1-v)\overline{(C^\perp : (1-v))} \\ &= v(\widehat{(C : v)})^\perp \oplus (1-v)(\overline{(C : (1-v))})^\perp \\ &= vC_2^\perp \oplus (1-v)C_1^\perp, \end{aligned}$$

which is the desired result. □

4 Cyclic codes over $F_p + vF_p$

Let $R_n = R[x]/\langle x^n - 1\rangle$ and $f_1(x), f_2(x), \cdots, f_s(x) \in R_n$. The ideal generated by $f_1(x), f_2(x), \cdots, f_s(x)$ will be denoted by $\langle f_1(x), f_2(x), \cdots, f_s(x)\rangle$. Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1}$, where $a_i \in R$ for $0 \leq i \leq n-1$, and denote $\widehat{f(x)} = \widehat{a_0} + \widehat{a_1}x + \cdots + \widehat{a_{n-1}}x^{n-1}$; $\overline{f(x)} = \overline{a_0} + \overline{a_1}x + \cdots + \overline{a_{n-1}}x^{n-1}$.

Definition 4.1. *We say that the set $S = \{vg_1(x), (1-v)g_2(x)\}$ is a generating set in standard form for the cyclic code $C = \langle S\rangle$ if*

(1) For each $i \in \{1, 2\}$, $g_i(x)$ is either monic in $F_p[x]$ or equals to 0;

(2)If $g_i(x) \neq 0$, then $g_i(x)|(x^n - 1)$ for each $i \in \{1, 2\}$.

Lemma 4.2. *Let $S = \{vg_1(x), (1-v)g_2(x)\}$ be a generating set in standard form for the cyclic code $C = \langle vg_1(x), (1-v)g_2(x)\rangle$. Then*

(1) $\widehat{(C : v)} = \langle g_1(x)\rangle$; (2) $\overline{(C : (1-v))} = \langle g_2(x)\rangle$,

that is, $g_1(x)$ and $g_2(x)$ are the generator polynomials for cyclic codes $\widehat{(C : v)}$ and $\overline{(C : (1-v))}$, respectively.

Proof. (1)Obviously, $\widehat{(C : v)}$ and $\overline{(C : (1-v))}$ are cyclic codes over F_p. Since $vg_1(x) \in C$, we have that $g_1(x) \in (C : v)$. Then $g_1(x) = \widehat{g_1(x)} \in \widehat{(C : v)}$. Thus $\langle g_1(x)\rangle \subseteq \widehat{(C : v)}$.

Let $f(x) \in (C : v)$. Note that $vf(x) \in C$ and suppose that $vf(x) = h_1(x)vg_1(x) + h_2(x)(1-v)g_2(x)$, where $h_1(x), h_2(x) \in R_n$. Let $f(x) = f_1(x) + (1-v)f_2(x)$; $h_1(x) = h_{11}(x) + (1-v)h_{12}(x)$; $h_2(x) = h_{21}(x) + vh_{22}(x)$, where $f_1(x), f_2(x), h_{11}(x), h_{12}(x), h_{21}(x), h_{22}(x) \in F_p[x]$. Then

$$\begin{aligned} vf(x) &= vf_1(x) \\ &= [h_{11}(x) + (1-v)h_{12}(x)]vg_1(x) \\ &+ [h_{21}(x) + vh_{22}(x)](1-v)g_2(x) \\ &= vh_{11}(x)g_1(x) + (1-v)h_{21}(x)g_2(x) \\ &= v[h_{11}(x)g_1(x) - h_{21}(x)g_2(x)] + h_{21}(x)g_2(x). \end{aligned}$$

Hence $v[f_1(x) - h_{11}(x)g_1(x) + h_{21}(x)g_2(x)] = h_{21}(x)g_2(x)$, which implies that $h_{21}(x)g_2(x) = 0$ and $f_1(x) = h_{11}(x)g_1(x) - h_{21}(x)g_2(x) = h_{11}(x)g_1(x)$. So $\widehat{f(x)} = f_1(x) = h_{11}(x)g_1(x) \in \langle g_1(x)\rangle$, which shows that $\langle g_1(x)\rangle \supseteq \widehat{(C : v)}$. Therefore $\langle g_1(x)\rangle = \widehat{(C : v)}$.

(2) Since $(1-v)g_2(x) \in C$, $g_2(x) \in (C : (1-v))$. Then $g_2(x) = \overline{g_2(x)} \in \overline{(C : (1-v))}$. Hence $\langle g_2(x)\rangle \subseteq \overline{(C : (1-v))}$.

Let $f(x) \in (C : (1-v))$. Then $(1-v)f(x) \in C$ and suppose that $(1-v)f(x) = u_1(x)vg_1(x) + u_2(x)(1-v)g_2(x)$, where $u_1(x), u_2(x) \in R_n$.

Let $f(x) = f_1(x) + vf_2(x); u_1(x) = u_{11}(x) + (1-v)u_{12}(x); u_2(x) = u_{21}(x) + vu_{22}(x)$, where $f_1(x), f_2(x), u_{11}(x), u_{12}(x), u_{21}(x), u_{22}(x) \in F_p[x]$. Then

$$\begin{aligned}(1-v)f(x) &= (1-v)f_1(x) \\ &= [u_{11}(x) + (1-v)u_{12}(x)]vg_1(x) \\ &+ [u_{21}(x) + vu_{22}(x)](1-v)g_2(x) \\ &= vu_{11}(x)g_1(x) + (1-v)u_{21}(x)g_2(x) \\ &= v[u_{11}(x)g_1(x) - u_{21}(x)g_2(x)] + u_{21}(x)g_2(x).\end{aligned}$$

Hence $v[f_1(x) + u_{11}(x)g_1(x) - u_{21}(x)g_2(x)] = f_1(x) - u_{21}(x)g_2(x)$, which implies that $f_1(x) - u_{21}(x)g_2(x) = 0$ and $f_1(x) = u_{21}(x)g_2(x)$. So $\overline{f(x)} = f_1(x) = u_{21}(x)g_2(x) \in \langle g_2(x)\rangle$, which shows that $\langle g_2(x)\rangle \supseteq \overline{(C:(1-v))}$. Therefore $\langle g_2(x)\rangle = \overline{(C:(1-v))}$. □

Theorem 4.3. *Any nonzero cyclic code C over R has a unique generating set in standard form.*

Proof. We first prove the existence. From Lemma 3.1, $\overline{(C:(1-v))}$ and $\widehat{(C:v)}$ are not all zero. So we may suppose that $\overline{(C:(1-v))} \neq 0$ and $\widehat{(C:v)} \neq 0$. Since $\widehat{(C:v)}$ and $\overline{(C:(1-v))}$ are cyclic codes over F_p, we assume that $\widehat{(C:v)} = \langle g_1(x)\rangle; \overline{(C:(1-v))} = \langle g_2(x)\rangle$, where $g_1(x), g_2(x)$ are the generator polynomials for cyclic codes $\widehat{(C:v)}$ and $\overline{(C:(1-v))}$, respectively. We will show that $C = \langle vg_1(x), (1-v)g_2(x)\rangle$.

Since $g_1(x) \in \widehat{(C:v)}$, there is $f(x) \in (C:v)$ such that $g_1(x) = \widehat{f(x)}$. Let $f(x) = g_1(x) + (1-v)f_1(x), f_1(x) \in F_p[x]$. Since $vf(x) \in C, vg_1(x) \in C$; Similarly, $(1-v)g_2(x) \in C$. Hence $C \supseteq \langle vg_1(x), (1-v)g_2(x)\rangle$.

Let $f(x) \in C$. Then $vf(x) \in C, (1-v)f(x) \in C$. We write

$$f(x) = f_1(x) + (1-v)f_2(x) = [f_1(x) + f_2(x)] - vf_2(x),$$

where $f_1(x), f_2(x) \in F_p[x]$. Since $vf(x) \in C$, $f(x) \in (C:v)$, then $\widehat{f(x)} \in \widehat{(C:v)} = \langle g_1(x)\rangle$, i.e., $f_1(x) \in \langle g_1(x)\rangle$. Write $f_1(x) = u_1(x)g_1(x), u_1(x) \in F_p[x]$. Similarly, Since $(1-v)f(x) \in C$, $f(x) \in (C:(1-v))$, then $\overline{f(x)} \in \overline{(C:(1-v))} = \langle g_2(x)\rangle$, i.e., $f_1(x) + f_2(x) \in \langle g_2(x)\rangle$. Write $f_1(x) + f_2(x) = u_2(x)g_2(x), u_2(x) \in F_p[x]$. Thus $f_2(x) = u_2(x)g_2(x) - u_1(x)g_1(x)$. Hence

$$\begin{aligned}f(x) &= f_1(x) + (1-v)f_2(x) \\ &= [f_1(x) + f_2(x)] - vf_2(x) \\ &= u_2(x)g_2(x) - v[u_2(x)g_2(x) - u_1(x)g_1(x)] \\ &= u_1(x)[vg_1(x)] + u_2(x)[(1-v)g_2(x)],\end{aligned}$$

which shows that $C \subseteq \langle vg_1(x), (1-v)g_2(x)\rangle$.

Therefore $C = \langle vg_1(x), (1-v)g_2(x)\rangle$.

If $\widehat{(C:v)} = 0$, then we choose $g_1(x) = 0$; if $\overline{(C:(1-v))} = 0$, then $g_2(x) = 0$.

Next we prove the uniqueness of a generating set in standard form for C. It is obtained from Lemma 4.2 and the uniqueness of the generator polynomial for cyclic code over finite field F_p. □

Corollary 4.4. *The ring R_n is principal.*

Proof. Let C be an ideal of R_n. According to Theorem 4.3 we have $C = \langle vg_1(x), (1-v)g_2(x)\rangle$, where $\{vg_1(x), (1-v)g_2(x)\}$ is a generating set in standard set for C. Note that $vg_1(x) = v[vg_1(x) + (1-v)g_2(x)]$ and $(1-v)g_2(x) = (1-v)[vg_1(x) + (1-v)g_2(x)]$, which imply that $C = \langle vg_1(x) + (1-v)g_2(x)\rangle$. Then the ring R_n is principal. □

Proposition 4.5. *The dual $C^\perp$ of a cyclic code C over R is cyclic.*

Let $g_1(x)h_1(x) = x^n - 1, g_2(x)h_2(x) = x^n - 1$. Let

$$\widetilde{h}_1(x) = x^{\deg(h_1(x))}h_1(\frac{1}{x}), \quad \widetilde{h}_2(x) = x^{\deg(h_2(x))}h_2(\frac{1}{x})$$

be the reciprocal polynomials of $h_1(x)$ and $h_2(x)$, respectively. We write $h_1^*(x) = \frac{1}{h_1(0)}\widetilde{h}_1(x); h_2^*(x) = \frac{1}{h_2(0)}\widetilde{h}_2(x)$.

Theorem 4.6. *Let C be a cyclic code of length n over R with a generating set in standard form $\{vg_1(x), (1-v)g_2(x)\}$. Then the generating set in standard form for the dual code $C^\perp$ is*

$$\{vh_1^*(x), (1-v)h_2^*(x)\}.$$

Proof. It follows immediately from Theorem 3.2(2) and Lemma 4.2. □

Lemma 4.7. *With the above notations, let $C = vC_2 \oplus (1-v)C_1$ be a linear code of length n over R. Then C is a cyclic code if and only if C_1 and C_2 are both cyclic codes.*

Proof. ($\Longrightarrow$) By the fact that $\widehat{(C:v)}$ and $\overline{(C:(1-v))}$ are cyclic codes over F_p and Lemma 3.1, it is clear.

($\Longleftarrow$) Let C_1 and C_2 be two cyclic codes and π be the shift operator. For arbitrary element $c \in C$, since $C = vC_2 \oplus (1-v)C_1$, we may suppose that $c = vc_2 + (1-v)c_1, c_1 \in C_1, c_2 \in C_2$. Then $\pi(c) = \pi(vc_2 + (1-v)c_1) = v\pi(c_2) + (1-v)\pi(c_1) \in vC_2 \oplus (1-v)C_1 = C$. Hence C is a cyclic code. □

In the following, we explore another approach to describing cyclic code C over R, involving the generating idempotent which is both idempotent and generates C. We write $C = [\![e(x)]\!]$ to denote the fact that $e(x)$ is this unique generating idempotent of C.

Theorem 4.8. *If n is coprime to p, then every cyclic code C of length n over R contains a unique generating idempotent $e(x)$, that is, $C = [\![e(x)]\!]$.*

Proof. Since n is coprime to p, there exist two generating idempotents $e_1(x), e_2(x)$ in $F_p[x]/\langle x^n - 1\rangle$ such that $C_1 = [\![e_1(x)]\!], C_2 = [\![e_2(x)]\!]$. According to Theorem 3.4, we have that $C = vC_2 \oplus (1-v)C_1$. Let $f(x) \in C$. There exist $u_1(x), u_2(x) \in F_p[x]$ such that $f(x) = v[u_2(x)e_2(x)] + (1-v)[u_1(x)e_1(x)]$. Note that

$$\begin{aligned} f(x) &= v[u_2(x)e_2(x)] + (1-v)[u_1(x)e_1(x)] \\ &= [u_1(x) + v(u_2(x) - u_1(x))][e_1(x) + v(e_2(x) - e_1(x))]. \end{aligned}$$

On the other hand, for arbitrary element $u(x) \in R_n$, setting $u(x) = u_1(x) + vu_2(x)$, where $u_1(x), u_2(x) \in F_p[x]$. Then

$$\begin{aligned} u(x)[e_1(x) + v(e_2(x) - e_1(x))] &= u(x)[ve_2(x) + (1-v)e_1(x)] \\ &= v[u_1(x) + u_2(x)]e_2(x) \\ &+ (1-v)u_1(x)e_1(x) \\ &\in vC_2 \oplus (1-v)C_1 = C. \end{aligned}$$

Hence we obtain that $(1-v)e_1(x) + ve_2(x) = e_1(x) + v[e_2(x) - e_1(x)]$ generates C. Let $e(x) = e_1(x) + v[e_2(x) - e_1(x)]$. Then $(e(x))^2 = e(x)$, hence $C = [\![e(x)]\!]$. If there is another $d(x) \in C$ such that $C = [\![d(x)]\!]$. Since $d(x) \in C$ and $e(x)$ generates C, we have $d(x) = a(x)e(x)$ for some $a(x) \in R_n$, thus

$$d(x)e(x) = a(x)(e(x))^2 = a(x)e(x) = d(x).$$

Similarly, we can prove that $d(x)e(x) = e(x)$. Hence $d(x) = e(x)$. □

Theorem 4.9. *Let n be coprime to p and let $C = [\![e(x)]\!]$. Then $C^\perp$ has the generating idempotent $[1 - e(x^{n-1})] \bmod (x^n - 1)$.*

Proof. According to the proof of Theorem 4.8, if $e_1(x), e_2(x)$ is the generating idempotent of C_1 and C_2, respectively, then we have that $e(x) = e_1(x) + v[e_2(x) - e_1(x)]$ is the generating idempotent for C. Noting that the generating idempotents for $C_1^\perp, C_2^\perp$ are $[1 - e_1(x^{n-1})] \bmod (x^n - 1)$ and $[1 - e_2(x^{n-1})] \bmod (x^n - 1)$, by Theorem 3.4 we obtain the required result. □

Theorem 4.10. *Let $x^n - 1 = \prod_{i=1}^r p_i^{k_i}(x)$ be the factorization of $x^n - 1$ into monic pairwise different irreducible factors over F_p. Then the number of the cyclic codes of length n over R is $\prod_{i=1}^r (k_i + 1)^2$.*

Proof. The number of the cyclic codes of length n over F_p is $\prod_{i=1}^r (k_i + 1)$, so the result follows from Lemma 4.7. □

Acknowledgement The authors are grateful to the anonymous referees for valuable comments and suggestions which help to create an improved version. The first author is supported by the Natural Science Foundation of China (Grant No. 11171370) and the Youth Backbone Teacher Foundation of Henan University (Grant No. 2013GGJS-152). The second author is supported by Natural Science Foundation of China (Grant No. 11301254), the Natural Science Foundation of Henan Province (Grant No. 132300410313), the Natural Science Foundation of Education Bureau of Henan Province (Grant No. 13A110800) and the the Natural Science Foundation of Luoyang Normal University (Grant No. 2012-QNJJ-003).

References

[1] T. A. Gulliver, M. Harada, Codes over $F_3 + uF_3$ and improvements to the bounds on ternary linear codes, Des. Codes Cryptogr. 22(2001)89-96.

[2] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, P. Solé, The $\mathbb{Z}_4$ linearity of Kerdock, Preparata, Goethals and related codes, IEEE Trans. Inform. Theory 40(2)(1994) 301-319.

[3] S. Ling, J. Blackford, $\mathbb{Z}_{p^{k+1}}$-linear codes, IEEE Trans. Inform. Theory 48(2002)2592-2605.

[4] Z. X. Wan, Quaternary codes, World Scientific, Singapore, 1997.

[5] J. Wolfmann, Binary image of cyclic codes over $\mathbb{Z}_4$, IEEE Trans. Inform. Theory 47(5)(2001)1773-1779.

[6] J. Wood, Duality for modules over finite rings and applications to coding theory, Amer. J. Math. 121(1999) 555-575.

[7] S. Zhu, L. Wang, A class of constacyclic codes over $F_p + vF_p$ and its Gray image, Discrete Math.311(2011)2677-2682.

[8] S. Zhu, Y. Wang, M. Shi, Some results on cyclic codes over $F_2 + vF_2$, IEEE Trans. Inform. Theory 56(4)(2010)1680-1684.