Construction of Self-dual Codes over $F_p + vF_p$ *

Guanghui Zhang\textsuperscript{1}, Bocong Chen\textsuperscript{2}

1. School of Mathematical Sciences, Luoyang Normal University, Luoyang, Henan, 471022, China
2. School of Mathematics and Statistics, Central China Normal University, Wuhan, Hubei, 430079, China

Abstract

In this paper, we determine all self-dual codes over $F_p + vF_p$ ($v^2 = v$) in terms of self-dual codes over the finite field $F_p$ and give an explicit construction for self-dual codes over $F_p + vF_p$, where $p$ is a prime.

Keywords: Self-dual code; Permutation-equivalent; Generator matrix; Parity check matrix; Code over $F_p + vF_p$.

2010 Mathematics Subject Classification: 94B05; 94B15

1 Introduction

Codes over finite rings were initiated in the early 1970s \cite{1, 2}. They have received much attention since the seminal work \cite{13}, which showed that certain good nonlinear binary codes could be found as images of linear codes over $\mathbb{Z}_4$ under the Gray map.

Generally, most of the studies are concentrated on the situation when the ground rings associated with codes are finite chain rings (e.g. see \cite{5, 6, 11, 16-19, 24}). However, it has been proved that finite Frobenius rings are suitable for coding alphabets \cite{25}, which leads to many works on codes over non-chain rings.

In recent years, linear codes over the ring $F_p + vF_p$, with $v^2 = v$ and $p$ being a prime, which is not a chain ring but a Frobenius ring, have been considered by some authors. In \cite{27}, Zhu et al. gave some results on cyclic codes over $F_2 + vF_2$, where it is shown that cyclic codes over the ring are principally generated. In \cite{26}, Zhu et al. studied $(1 - 2v)$-constacyclic codes over $F_p + vF_p$, where $p$ is an odd prime. They determined the image of $(1 - 2v)$-constacyclic codes over $F_p + vF_p$ under the Gray map and the structures of such constacyclic codes over $F_p + vF_p$. In \cite{3}, Cengellenmis et al. generated the ring $F_2 + vF_2$ to the infinite family of rings $A_k = F_2[v_1, v_2, \cdots, v_k]/(v^2_i = v_i, v_iv_j = v_jv_i), 1 \leq i, j \leq k$, and studied codes over these rings by using Gray maps.

On the other hand, self-dual codes play a very significant role in coding theory both from practical and theoretical points of view. A vast number of papers have been devoted to the study of self-dual codes; e.g. see \cite{7-10, 12, 14-17, 20, 21}. In \cite{16}, Kim and Lee gave an efficient method to construct self-dual codes over finite fields from a given self-dual code of a smaller length. In \cite{10}, Dougherty et al. proved that self-dual codes exist over all finite commutative Frobenius rings and gave some building-up constructions for self-dual codes over these rings. More recently, Cengellenmis et al. \cite{3} studied Euclidean and Hermitian self-dual codes over $A_k = F_2[v_1, v_2, \cdots, v_k]/(v^2_i = v_i, v_iv_j = v_jv_i), 1 \leq i, j \leq k$, and gave a sufficient and necessary condition for the existence of self-dual codes over the rings.

In this paper, we determine all self-dual codes over $F_p + vF_p$ ($v^2 = v$) in terms of self-dual codes over the finite field $F_p$ and give an explicit construction for self-dual codes over $F_p + vF_p$, where $p$ is a prime.

*E-mail addresses: zg09@yahoo.com.cn (G. Zhang), b-c.\textsuperscript{2}chen@yahoo.com.cn (B. Chen)
Unlike the technique used in the mentioned papers, we first give the parity check matrices for linear codes over $F_p + v F_p$. Then we characterize the torsion codes associated with the linear codes, which are used as a tool to study self-dual codes over $F_p + v F_p$ and their explicit construction.

The organization of this paper is as follows. The necessary notations and some known results are provided in Section 2. In Section 3, we first characterize the torsion codes, and then give some criteria for a linear code over the ring to be self-dual. In Section 4, we determine all self-dual codes over $F_p + v F_p$ and give an explicit construction for self-dual codes over $F_p + v F_p$. In section 5, we give some examples to illustrate our main results.

2 Preliminaries

Let $F_p$ be a finite field with $p$ elements, where $p$ is a prime. Throughout this paper, $R$ denotes the commutative ring $F_p + v F_p = \{a + vb \mid a, b \in F_p\}$ with $v^2 = v$. Any element of $R$ can be uniquely expressed as $c = a + vb$, where $a, b \in F_p$. The Gray map $\Phi$ from $R$ to $F_p \times F_p$ is given by $\Phi(c) = (a, a + b)$. It is routine to check that $\Phi$ is a ring isomorphism, which means $R$ is isomorphic to the ring $F_p \times F_p$; so $R$ is a finite Frobenius ring. The ring $R$ is a semi-local ring with exactly two maximal ideals given by $(v) = \{av \mid a \in F_p\}$ and $(1 - v) = \{a(1 - v) \mid a \in F_p\}$. It is easy to verify that both $R/(v)$ and $R/(1 - v)$ are isomorphic to $F_p$.

A code $C$ of length $n$ over $R$ is a nonempty subset of $R^n$, and the ring $R$ is referred to the alphabet of the code. If this subset is also an $R$-submodule of $R^n$, then $C$ is called linear. For any code $C$ of length $n$ over $R$, the dual code of $C$ is defined as $C^\perp = \{u \in R^n \mid u \cdot v = 0, \text{for any } v \in C\}$, where $u \cdot v$ denotes the standard Euclidean inner product of $u$ and $v$ in $R^n$. Notice that $C^\perp$ is linear whether or not $C$ is linear. If $C \subseteq C^\perp$, then $C$ is called self-orthogonal. If $C = C^\perp$, then $C$ is called self-dual.

We have known that the ring $R$ has exactly two maximal ideals $(v)$ and $(1 - v)$. Their residue fields are both $F_p$. Thus we have two canonical projections defined as follows:

$$ R = F_p + v F_p \longrightarrow R/(v) = F_p $$
$$ a + vb \longrightarrow a; $$

and

$$ R = F_p + v F_p \longrightarrow R/(1 - v) = F_p $$
$$ a + vb \longrightarrow a + b. $$

We simple denote these two projections by "−" and "^\circ", respectively. Denote by $r$ and $\tilde{r}$ the images of an element $r \in R$ under these two projections, respectively.

Note that any element $c$ of $R^n$ can be uniquely expressed as $c = r + vq$, where $r, q \in F_p^n$. Let $C$ be a linear code of length $n$ over $R$. Define

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

and

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

Obviously, $C_1$ and $C_2$ are linear codes over $F_p$.

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

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

The codes $(C : v)$ and $(C : (1 - v))$ over the field $F_p$ is called the torsion codes associated with the code $C$ over the ring $R$.

For the case of odd prime $p$, any nonzero linear code $C$ over $R$ is permutation-equivalent to a code generated by the following matrix (see [20]):

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

2
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 $|C| = p^{2k_1+k_2+k_3}$. For later convenience the above generator matrix can be rewritten in the form:

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

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

For the case $p = 2$, a nonzero linear code $C$ over $R$ has a generator matrix which after a suitable permutation of the coordinates can be written in the form (see [23, 27]):

$$G = \begin{pmatrix}
I_{k_1} & A & B & D_1 + vD_2 \\
0 & vI_{k_2} & 0 & vC_1 \\
0 & 0 & (1+v)I_{k_3} & (1+v)E
\end{pmatrix},$$

where $A, B, C_1, D_1, D_2$ and $E$ are matrices with entries in $F_2$, and $|C| = 2^{2k_1}2^{k_2}2^{k_3}$.

For $k > 0$, $I_k$ denotes the $k \times k$ identity matrix. The code $C_1$ is permutation-equivalent to a code with generator matrix of the form (see [23, 27]):

$$G_1 = \begin{pmatrix}
I_{k_1} & B_1 & 0 & B_2 & B_3 \\
0 & 0 & I_{k_2} & 0 & B_4 \\
I_{k_1} & A & B & D_1
\end{pmatrix},$$

where $p$ is odd;

$$G_2 = \begin{pmatrix}
I_{k_1} & 0 & A_1 & A_2 & A_3 \\
0 & I_{k_2} & 0 & A_4 & 0 \\
I_{k_1} & A & B & D_1 + D_2
\end{pmatrix},$$

where $p = 2$, $A, B, C_1, D_1, D_2$ and $A_i$ 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 (see [23, 27]):

$$G_2 = \begin{pmatrix}
I_{k_1} & 0 & A_1 & A_2 & A_3 \\
0 & I_{k_2} & 0 & A_4 & 0 \\
I_{k_1} & A & B & D_1 + D_2
\end{pmatrix},$$

where $p = 2$, $A, B, C_1, D_1, D_2$ and $A_i$ are $p$-ary matrices for $i \in \{1, 2, 3, 4\}$. It is easy to see that $\dim C_1 = k_1 + k_3$ and $\dim C_2 = k_1 + k_2$.

## 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.** Assume the notation given above. Let $C$ be a linear code of length $n$ over $R$. Then

1. $(\widehat{C} : v) = C_2$.
2. $(\widehat{C} : (1-v)) = C_1$.

**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

$$z = x + y = \widehat{x + y} \in (C : \widehat{v}).$$

Hence $(C : v) \supseteq C_2$. Therefore we get the desired result.

(2) Let $y$ be an element of $(C : (1-v))$, then there exists some $x \in (C : (1-v))$ such that $y = \widehat{v}$. Suppose that $x = r + vq$, for $r, q \in F^n_p$. Then $\widehat{v} = r$. 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 $y = \widehat{v} = r \in C_1$. Therefore we obtain that $(C : v) \subseteq C_1$.

If $r$ is an element of $C_1$, then we have that $r + vq \in C$ for some $q \in F^n_q$. Since

$$(1-v)r = (1-v)(r+vq) \in C,$$

which shows that $r \in (C : (1-v))$. Hence $r \in (C : (1-v))$. Therefore we get the desired result.

In the following $A^T$ denotes the transpose of the matrix $A$. Suppose $C_1$ and $C_2$ are permutation equivalent linear codes over $R$ with $C_1P = C_2$ for some permutation matrix $P$. Then $C_1^\perp P = C_2^\perp$. Without loss of generality, we may assume that a linear code $C$ of length $n$ over $R$ is with generator matrix in the form $(\ast)$.

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

1. For $p$ being odd, let

$$H = \begin{pmatrix}
 vE_1 + (1-v)E_2 & P & Q & I_{n-k} \\
 v(-A_1^T) & 0 & vI_{k_3} & 0 \\
 (1-v)(-A_2^T) & (1-v)I_{k_2} & 0 & 0
\end{pmatrix},$$

where $E_1 = (-A_2 \mid A_1B_4 - A_3)^T$, $E_2 = (B_3A_4 - B_2 \mid -B_3)^T$, $P = (-A_4 \mid 0)^T$, $Q = (0 \mid -B_4)^T$ and $k = k_1 + k_2 + k_3$. Then $H$ is a generator matrix for $C^\perp$ and a parity check matrix for $C$.

2. For $p = 2$, let

$$H = \begin{pmatrix}
 E^T B^T + C_1^T A^T + (D_1 + vD_2)^T & C_1^T & E^T & I_{n-k} \\
 vB^T & 0 & vI_{k_3} & 0 \\
 (1+v)A^T & (1+v)I_{k_2} & 0 & 0
\end{pmatrix},$$

where $A, B, C_1, D_1, D_2$ and $E$ are matrices with entries in $F_2$ and $k = k_1 + k_2 + k_3$. Then $H$ is a generator matrix for $C^\perp$ and a parity check matrix for $C$.

3. $(\langle C : v \rangle)^\perp = (\langle C^\perp : v \rangle ; ((C : (1-v))}^\perp = (\langle C^\perp : (1-v)\rangle)$

**Proof.** (1) Since the verification of $HG_1 = 0$ is routine and somewhat tedious, we present a detail proof in the appendix. Let $D$ be the $R$-submodule generated by $H$, then $D \subseteq C^\perp$. Since $R$ is a Frobenius ring, we have $|C||C^\perp| = |R|^n$ (23). It follows that

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

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

(2) Similar to the proof of (1).

(3) We first prove that $(\langle C^\perp : v \rangle \subseteq (\langle C : v \rangle)^\perp$. Let $x \in (\langle C^\perp : v \rangle$ and $y \in (\langle C : v \rangle$. Then $vx \in C^\perp$ and $vy \in C$, so $(vx)(vy)^T = 0$, i.e., $(vx)^T = 0$. Hence $xy^T \in (1-v)R$, and $\widehat{xy}^T = 0$, which implies that $(\langle C^\perp : v \rangle \subseteq (\langle C : v \rangle)^\perp$. On the other hand, by Lemma 4.1 and Theorem 4.2(1)(2), we have that

$$\dim(\langle C^\perp : v \rangle) = n - k + k_3 = n - k_1 - k_2.$$
dim(\(C : v\)^⊥) = n - dim(\(C : v\)) = n - (k_1 + k_2) = n - k_1 - k_2.

Hence dim(\(C^\perp : v\)) = dim(\(C : v\))^⊥, which follows that ((\(C : v\))^⊥)^⊥ = (\(C^\perp : v\)).

The proof of the second equality is similar to that of the first one and is omitted here. \(\square\)

**Corollary 3.3.** Let \(C\) be a linear code of length \(n\) over \(R\). 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)(2), we have that

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

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

Let \(A, B\) be the codes over \(R.\) We denote by \(A \oplus B = \{a + b \mid a \in A, b \in B\}.\)

**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 \(a_2, b_2 \in C_2\) and \(a_1, b_1 \in C_1.\) 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 \(va \in C\) and \((1 - v)b \in C.\) Assume \(a = a_1 + (1 - v)a_2, b = b_1 + vb_2,\) where \(a_1, a_2, b_1, b_2 \in F_p^n.\) Then \(\hat{a} = a_1 \in C_2, \hat{b} = b_1 \in C_1.\) Thus

\(v\hat{a} + (1 - v)\hat{b} = va_1 + (1 - v)b_1 = va + (1 - v)b \in C.\)

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 the second statement. Combining the first statement, Theorem 3.2(3) with Lemma 3.1 we have

\(C^\perp = v(C^\perp : v) \oplus (1 - v)((C^\perp : (1 - v))^\perp)
= v((C : v))^\perp \oplus (1 - v)((C : (1 - v))^\perp)^\perp
= vC_2^\perp \oplus (1 - v)C_1^\perp,\)

which is the desired result. \(\square\)

**Corollary 3.5.** With the above notations, let \(C\) be a linear code of length \(n\) over \(R.\) Then \(C\) is a self-dual code if and only if \(C_1\) and \(C_2\) are both self-dual codes.
Proof. (⇒) Let \( C \) be a self-dual code. Then by Lemma 3.1 and Theorem 3.2, we have
\[
C_1^\perp = ((C^\perp : (1 - v))^\perp = (C^\perp : (1 - v)) = C_1
\]
and
\[
C_2^\perp = ((C : v))^\perp = (C : v) = C_2,
\]
that is, \( C_1 \) and \( C_2 \) are both self-dual codes.

(⇐) Let \( C_1 \) and \( C_2 \) be both self-dual codes. Then by Theorem 3.4,
\[
C^\perp = vC_2^\perp \oplus (1 - v)C_1^\perp = vC_2 \oplus (1 - v)C_1 = C.
\]
So \( C \) is self-dual.  

Remark 3.6. According to Theorem 3.4 and Corollary 3.5, it is clear that a self-dual code over \( R \) can be explicitly expressed via two self-dual codes over \( F_p \). We need to study the converse part, which is an interesting step.

4 Construction of self-dual codes over \( F_p + vF_p \)

The construction of self-dual codes over \( R \) depends on the following theorem.

Theorem 4.1. Suppose that \( C_1 \) and \( C_2 \) are linear codes of length \( n \) over \( F_p \) with generator matrices \( G_1 \) and \( G_2 \) respectively, and let \( l_1 \) and \( l_2 \) be the dimensions of \( C_1 \) and \( C_2 \) respectively. Then the code \( C \) over \( R \) generated by the matrix \( G \),
\[
G = \begin{cases} 
(vG_2) + (1 - v)G_1, & \text{if } l_1 > l_2; \\
vG_2 + \left( (1 - v)G_1 \right), & \text{if } l_1 < l_2; \\
vG_2 + (1 - v)G_1, & \text{if } l_1 = l_2.
\end{cases}
\]

satisfies
\[
C = vC_2 \oplus (1 - v)C_1, \quad (C : v) = C_2, \quad (C : (1 - v)) = C_1.
\]

Proof. We only prove the case \( l_1 > l_2 \) in the following, as the proof of the other cases are similar to this case. Assume that \( G_1 = (g_{11}, g_{12}, \cdots, g_{1,l_1})^T \), \( G_2 = (g_{21}, g_{22}, \cdots, g_{2,l_2})^T \), then
\[
G = \begin{pmatrix}
vg_{21} + (1 - v)g_{11} \\
v_{g_{22}} + (1 - v)g_{12} \\
\vdots \\
v_{g_{2,l_2}} + (1 - v)g_{1,l_2} \\
(1 - v)g_{1,l_2+1} \\
\vdots \\
(1 - v)g_{1,l_1}
\end{pmatrix}.
\]

Since \( vg_{2i} + (1 - v)g_{1i} \in C \), i.e. \( g_{1i} + v(g_{2i} - g_{1i}) \in C \), for every \( 1 \leq i \leq l_2 \), by Lemma 3.1 we have
\[
g_{2i} = g_{1i} + (g_{2i} - g_{1i}) \in \widehat{(C : v)},
\]
for every \( 1 \leq i \leq l_2 \). Therefore \( C_2 \subseteq \widehat{(C : v)} \).

Let \( y \in (C : v) \), then there exists \( x \in (C : v) \) such that \( y = \hat{x} \). Since \( vx \in C \), we may assume that
\[
vx = \sum_{i=1}^{l_2} (a_i + vs_i)[vg_{2i} + (1 - v)g_{1i}] + \sum_{i=l_2+1}^{l_1} (a_i + vs_i)[(1 - v)g_{1i}],
\]
where \( a_i + vs_i \in F_p + vF_p \), for \( 1 \leq i \leq l_1 \). So
\[
v x = v^2 x = v \cdot vx = v \sum_{i=1}^{l_2} (a_i + s_i)g_{2i}.
\]

Let \( x = x_1 + vx_2, x_1, x_2 \in F_p^n \). Then \( \hat{x} = x_1 + x_2 \). Thus
\[
v(x_1 + x_2) = vx = v \sum_{i=1}^{l_2} (a_i + s_i)g_{2i}.
\]
Hence \( x_1 + x_2 = \sum_{i=1}^{l_2} (a_i + s_i)g_{2i} \). Therefore we have
\[
y = \hat{x} = x_1 + x_2 = \sum_{i=1}^{l_2} (a_i + s_i)g_{2i} \in C_2,
\]
which gives \( \widetilde{(C : v)} \subseteq C_2 \). From the above facts we get that \( \widetilde{(C : v)} = C_2 \).

On the other hand, since
\[
v g_{2i} + (1 - v)g_{1i} \in C, i.e. \ g_{1i} + v(g_{2i} - g_{1i}) \in C,
\]
for every \( 1 \leq i \leq l_1 \). Here \( g_{2i} = 0 \), if \( i > l_2 \). By Lemma 3.1 we have \( g_{1i} \in \big(C : (1 - v)\big), \) for every \( 1 \leq i \leq l_1 \). Therefore \( C_1 \subseteq \big(C : (1 - v)\big) \).

Let \( z \in \big(C : (1 - v)\big) \), then there exists \( s \in (C : (1 - v)) \) such that \( z = \overrightarrow{s} \). Since \( (1 - v)s \in C \), we assume that
\[
(1 - v)s = \sum_{i=1}^{l_2} (b_i + vt_i)[v g_{2i} + (1 - v)g_{1i}] + \sum_{i=1}^{l_1} (b_i + vt_i)[(1 - v)g_{1i}]
\]
where \( b_i + vt_i \in F_p + vF_p \), for \( 1 \leq i \leq l_1 \). So
\[
(1 - v)s = (1 - v)^2 s = (1 - v) \cdot (1 - v)s = (1 - v) s \sum_{i=1}^{l_1} b_i g_{1i}.
\]

Let \( s = s_1 + vs_2, s_1, s_2 \in F_p^n \). Then \( \overrightarrow{s} = s_1 \). Thus
\[
(1 - v)s_1 = (1 - v)s = (1 - v) s \sum_{i=1}^{l_1} b_i g_{1i}.
\]
Hence \( s_1 = \sum_{i=1}^{l_1} b_i g_{1i} \). Therefore we have
\[
z = \overrightarrow{s} = s_1 = \sum_{i=1}^{l_1} b_i g_{1i} \in C_1,
\]
which gives \( \big(C : (1 - v)\big) \subseteq C_1 \). Thus we get \( \big(C : (1 - v)\big) = C_1 \).

Finally, by Lemma 3.1 and Theorem 3.3
\[
C = v\widetilde{(C : v)} \oplus (1 - v)\big(C : (1 - v)\big) = vC_2 \oplus (1 - v)C_1,
\]
which gives our desired result. Thus we complete the proof.

**Corollary 4.2.** Suppose that \( C_1 \) and \( C_2 \) are two self-dual codes of length \( n \) over \( F_p \) with generator matrices \( G_1 \) and \( G_2 \) respectively, then the code \( C \) over \( R \) generated by the matrix \( G \) as follows is also self-dual, where
\[
G = vG_2 + (1 - v)G_1.
\]
Proof. Note that $l_1 = l_2$ in this case. By Lemma 3.1, Theorem 3.4 and Theorem 4.1 we have
\[ C^\perp = v((C : v))^\perp \oplus (1 - v)((C : (1 - v))^\perp) \]
\[ = vC_2^\perp \oplus (1 - v)C_1^\perp \]
\[ = vC_2 \oplus (1 - v)C_1 \]
\[ = C. \]

So $C$ is self-dual. \qed

**Theorem 4.3.** All the self-dual codes over $R$ are given by
\[ vC_2 \oplus (1 - v)C_1, \]
where $C_1, C_2$ range over all the self-dual codes over $F_p$, respectively. Moreover, this expression is unique, i.e. if
\[ vC_2 \oplus (1 - v)C_1 = vC'_2 \oplus (1 - v)C'_1, \]
then $C_2 = C'_2$ and $C_1 = C'_1$, where $C_1, C_2, C'_1, C'_2$ are all self-dual codes over $F_p$.

**Proof.** First by Corollary 3.5 every self-dual code over $R$ can be explicitly expressed by two fixed self-dual codes over $F_p$ as in the above form.

Next, let $C_1, C_2$ be arbitrary two self-dual codes over $F_p$. Assume that $G_1$ and $G_2$ are generator matrices for $C_1, C_2$, respectively. Then according to Corollary 3.2 we know that the code $C$ generated by the matrix $vG_1 + (1 - v)G_2$ is self-dual and satisfies $C = vC_2 \oplus (1 - v)C_1$. This completes the proof of the first statement.

Let $x \in C_2$. Since $vC_2 \oplus (1 - v)C_1 = vC'_2 \oplus (1 - v)C'_1$, we have that
\[ vx \in vC_2 \subseteq vC_2 \oplus (1 - v)C_1 = vC'_2 \oplus (1 - v)C'_1. \]

Assuming $vx = vx' + (1 - v)y'$ where $x' \in C'_2, y' \in C'_1$, we get that $v(x - x') = (1 - v)y'$ and $v(x - x') = 0$, so $x = x'$. Therefore $C_2 \subseteq C'_2$. Similarly, we have $C'_2 \subseteq C_2$. Hence $C_2 = C'_2$.

Let $z \in C_1$. Since $vC_2 \oplus (1 - v)C_1 = vC'_2 \oplus (1 - v)C'_1$, we have that
\[ (1 - v)z \in (1 - v)C_1 \subseteq vC_2 \oplus (1 - v)C_1 = vC'_2 \oplus (1 - v)C'_1. \]

Setting $(1 - v)z = vz' + (1 - v)z'$, where $z' \in C'_2, z' \in C'_1$, we get that $(1 - v)(z - z') = vz'$ and $(1 - v)(z - z') = 0$, so $z = z'$. Therefore $C_1 \subseteq C'_1$. Similarly, we have $C'_1 \subseteq C_1$. Hence $C_1 = C'_1$. Thus we complete the proof. \qed

**Corollary 4.4.** Let $N(R)$ be the number of self-dual codes of length $n$ over $R$ and $N(F_p)$ the number of self-dual codes of length $n$ over $F_p$. Then
\[ N(R) = N(F_p)^2. \]

**Proof.** It follows immediately from Theorem 4.3. \qed

The following lemma is well known and can be found from [22].

**Lemma 4.5.** Let $F_q$ be a finite field with characteristic $p$. Then
(i) If $p = 2$ or $p \equiv 1 \pmod{4}$, then a self-dual code of length $n$ exists over $F_q$ if and only if $n \equiv 0 \pmod{2}$;  
(ii) If $p \equiv 3 \pmod{4}$, then a self-dual code of length $n$ exists over $F_q$ if and only if $n \equiv 0 \pmod{4}$.

Now combining Theorem 4.3 with Corollary 4.5, the following result is easily obtained.

**Theorem 4.6.** With the above notations. Then the following two statements hold:
(i) If $p = 2$ or $p \equiv 1 \pmod{4}$, then a self-dual code of length $n$ over $R$ exists if and only if $n \equiv 0 \pmod{2}$;  
(ii) If $p \equiv 3 \pmod{4}$, then a self-dual code of length $n$ over $R$ exists if and only if $n \equiv 0 \pmod{4}$.

**Remark 4.7.** For $p = 2$, the corresponding result has been obtained in [23, Corollary 5.5].
5 Examples

According to Corollary 4.2, the construction of self-dual codes over \( R \) hinges on constructing the self-dual codes over \( F_p \). See \([16]\) on the building-up construction of self-dual codes over \( F_p \). The following examples illustrate our results.

Example 5.1. Consider the construction of self-dual code of length 4 over \( R = F_5 + vF_5 \). Let \( c = 2 \) be in \( F_5 \) such that \( c^2 = -1 \) in \( F_5 \). Here \( l_1 = l_2 = 2 \) and

\[
G_1 = \begin{pmatrix} 1 & 0 & 3 & 0 \\ -3 & 1 & 1 & 2 \end{pmatrix};
\]

\[
G_2 = \begin{pmatrix} 0 & 2 & 0 & 1 \\ -2 & 4 & 1 & 2 \end{pmatrix}.
\]

Then the code \( C \) of length 4 over \( R = F_5 + vF_5 \) generated by the following matrix

\[
G = vG_2 + (1 - v)G_1 = \begin{pmatrix} 1 - v & 2v & 3 - 3v & v \\ -3 + v & 1 + 3v & 1 & 2 \end{pmatrix}
\]

is self-dual.

On the other hand, it is an elementary calculation to check that the above code \( C \) is permutation-equivalence to a code \( C \) generated by the following matrix:

\[
\begin{pmatrix} 1 & 0 & 2 + v & 0 \\ 0 & 1 & 0 & 2 + v \end{pmatrix} = (I_2 | vD_1 + (1 - v)D_2),
\]

where \( D_1 = \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix} \), \( D_2 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \). By the Corollary 3.3 it is easy to check that \( C \) is self-dual. So the code \( C \) is also self-dual.

Example 5.2. Consider the construction of self-dual code of length 6 over \( R = F_2 + vF_2 \). Here \( l_1 = l_2 = 3 \) and

\[
G_1 = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix};
\]

\[
G_2 = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.
\]

Then the code \( C \) of length 6 over \( R = F_2 + vF_2 \) generated by the following matrix

\[
G = vG_2 + (1 - v)G_1
\]

\[
= G_1 + v(G_2 - G_1)
\]

\[
= \begin{pmatrix} 1 & 0 & 1 + v & 1 & 0 & 1 + v \\ 1 + v & 1 + v & 1 & 0 & 1 + v & v \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}
\]

is self-dual.

Similarly, through an elementary calculation, the above code \( C \) is permutation-equivalence to a code \( C \) generated by the following matrix:

\[
\begin{pmatrix} 1 & 0 & 0 & v & 0 & 1 + v \\ 0 & 1 & 0 & 1 + v & 0 & v \\ 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix} = (I_3 | D_1 + vD_2),
\]

where \( D_1 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \), \( D_2 = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \). By the Corollary 3.3 it is easy to check that \( C \) is self-dual. Thus the code \( C \) is also self-dual.
Example 5.3. Consider the construction of self-dual code of length $12$ over $R = F_3 + vF_3$. Here $l_1 = l_2 = 6$ and

$$G_1 = (I_6 | B),$$

where $I_6$ denotes the $6 \times 6$ identity matrix, and

$$B = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 2 & 1 \\ 1 & 1 & 0 & 1 & 2 & 2 \\ 1 & 2 & 1 & 0 & 1 & 2 \\ 1 & 2 & 2 & 1 & 0 & 1 \\ 1 & 1 & 2 & 2 & 1 & 0 \end{pmatrix} ,$$

i.e. the code with generator matrix $G_1$ is the ternary Golay code:

$$G_2 = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 1 & 0 \\ 2 & 1 & 2 & 0 & 1 & 2 & 1 & 0 & 2 & 2 & 0 & 1 \end{pmatrix} .$$

Then the code $C$ of length $12$ over $R = F_3 + vF_3$ generated by the following matrix

$$G = vG_2 + (1-v)G_1 = G_1 + v(G_2 - G_1) =$$

$$\begin{pmatrix} 1+2v & v & v & v & 0 & 0 & 0 & 0 & 0 & 1+2v & 1+2v & 1+2v & 1+2v \\ v & 1+2v & 0 & 0 & v & 0 & 1 & 2v & 1+2v & 2+2v & 2+2v & 1+2v \\ 0 & 0 & 1+2v & 0 & 0 & v & 1 & 1 & 0 & 1+2v & 2+v & 2+v \\ 0 & 0 & 0 & 1+2v & v & 0 & 1+2v & 2+v & 1 & 0 & 1+v & 2+v \\ 0 & 0 & 0 & 0 & 1+2v & 0 & 1+2v & 2+v & 2+2v & 1+v & v & 1+2v \\ 2v & v & 2v & 0 & v & 1+v & 1 & 1+2v & 2 & 2 & 1+2v & v \end{pmatrix} ,$$

is self-dual.

Here we do the same thing as in the above examples and get the code $C$ is permutation-equivalence to a code $C$ generated by the following matrix:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 2 & v & 2 & 2v & 2 & 1+2v & 0 & 2+v \\ 0 & 1 & 0 & 0 & 0 & 2 & 0 & 1+2v & 2+v & 2 & 2v \\ 0 & 0 & 1 & 0 & 0 & 2v & 1+2v & 1+2v & 1+2v & 2+v & 2+2v \\ 0 & 0 & 0 & 1 & 0 & 1+2v & 2 & 2+v & 2+v & 2+v & 2+v \\ 0 & 0 & 0 & 0 & 1 & 1+2v & 2 & 2 & v & 1+2v & 2 & v \\ 0 & 0 & 0 & 0 & 0 & 1 & 2 & v & 1+2v & 1 & 1 & 0 \end{pmatrix} = (I_6 | vD_1 + (1-v)D_2) ,$$

where $D_1 = \begin{pmatrix} 0 & 1 & 2 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 & 2 \\ 2 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \end{pmatrix} , D_2 = \begin{pmatrix} 2 & 2 & 2 & 1 & 0 & 2 \\ 2 & 0 & 1 & 2 & 1 & 2 \\ 2 & 0 & 0 & 1 & 2 & 2 \\ 1 & 2 & 0 & 2 & 2 & 2 \\ 1 & 1 & 2 & 0 & 1 & 2 \\ 1 & 2 & 1 & 1 & 1 & 0 \end{pmatrix}$. By the Corollary 5.3, it is easy to check that $C$ is self-dual. So the code $C$ is also self-dual.

Acknowledgement This work is supported by the National Natural Science Foundation of China, Grant No. 11171370.

Appendix
We give a detail proof for $HG^T = 0$ in Theorem 3.2 below.

For $p$ being odd, we have that

$$HG^T = \begin{pmatrix}
vE_1 + (1-v)E_2 & P & Q & I_{n-k} \\
v(-A_1^T) & 0 & vI_{k_2} & 0 \\
(1-v)(-B_1^T) & (1-v)I_{k_2} & 0 & 0 \\
\end{pmatrix} \begin{pmatrix}
I_{k_1} & (1-v)B_1 & vA_1 & vD_1 + (1-v)D_2 \\
vA_1^T & 0 & 0 & vC_1 \\
(1-v)I_{k_3} & 0 & (1-v)I_{k_3} & (1-v)C_2 \\
\end{pmatrix}^T$$

$$= \begin{pmatrix}
(1-v)E_1 + (1-v)E_2 & P & Q & I_{n-k} \\
(1-v)(-A_1^T) & 0 & vI_{k_2} & 0 \\
(1-v)(-B_1^T) & (1-v)I_{k_2} & 0 & 0 \\
\end{pmatrix} \begin{pmatrix}
I_{k_1} & (1-v)B_1^T & vI_{k_2} & 0 \\
vA_1^T & 0 & vD_1 + (1-v)D_2 & vC_1^T \\
0 & (1-v)I_{k_2} & (1-v)I_{k_2} & (1-v)C_2 \\
\end{pmatrix}$$

$$= \begin{pmatrix}
(vE_1 + QA_1^T + D_1^T) + (1-v)(E_2 + PB_1^T + D_2^T) & v(P + C_1^T) & (1-v)(Q + C_2^T) \\
(1-v)(-B_1^T) + (1-v)^2B_1^T & v(1-v)I_{k_2} & 0 \\
\end{pmatrix}$$

$$= 0,$$

where

$$v(E_1 + QA_1^T + D_1^T) + (1-v)(E_2 + PB_1^T + D_2^T)$$

$$= v(\text{[} -A_2 \mid A_1B_4 - A_3\text{]}^T + (0 \mid -B_4)^T A_1^T + D_1^T) + (1-v)[(B_1A_4 - B_2 \mid -B_3)^T + (-A_4 \mid 0)^T B_1^T + D_2^T]$$

$$= v(\text{[} -A_2 \mid A_1B_4 - A_3\text{]} + A_1 (0 \mid -B_4) + D_1)^T + (1-v)[(B_1A_4 - B_2 \mid -B_3) + B_1 (-A_4 \mid 0) + D_2]^T$$

$$= v(\text{[} -A_2 \mid A_3 + D_1\text{]} + (1-v)\text{[} -B_2 \mid B_3 + D_2\text{]}^T$$

$$= v(-D_1 + D_1)^T + (1-v)(-D_2 + D_2)^T$$

$$= 0;$$

$$P + C_1^T = (-A_4 \mid 0)^T + (A_4 \mid 0)^T = 0;$$

$$Q + C_2^T = (0 \mid -B_4)^T + (0 \mid B_4)^T = 0.$$

For $p = 2,$

$$HG^T = \begin{pmatrix}
E^T B^T + C_1^T A_1^T + (D_1 + vD_2)^T & C_1^T & E^T & I_{n-k} \\
0 & 0 & vI_{k_2} & 0 \\
\end{pmatrix} \begin{pmatrix}
I_{k_1} & A & B & D_1 + vD_2 \\
vA_1^T & 0 & 0 & vC_1 \\
(1+v)I_{k_3} & 0 & (1+v)I_{k_3} & (1+v)E \\
\end{pmatrix}^T$$

$$= \begin{pmatrix}
E^T B^T + C_1^T A_1^T + (D_1 + vD_2)^T & C_1^T & E^T & I_{n-k} \\
0 & 0 & vI_{k_2} & 0 \\
\end{pmatrix} \begin{pmatrix}
I_{k_1} & A^T & vI_{k_2} & 0 \\
B^T & 0 & 0 & (1+v)I_{k_3} \\
D_1^T + vD_2^T & vC_1^T & (1+v)E^T & 0 \\
\end{pmatrix}$$

$$= 0.$$

Thus we complete the proof.

References

[1] I. F. Blake, Codes over certain rings, Inform. Control 20(1972), 396-404.
[2] I. F. Blake, Codes over integer residue rings, Inform. Control 29(1975), 295-300.
[3] Y. Cengellenmis, A. Dertli, S. T. Dougherty, Codes over an infinite family of rings with a Gray map, Des. Codes Cryptogr., DOI. 10.1007/s10623-012-9787-y, published online: 01 January 2013.
[4] A. R. Calderbank, N. J. A. Sloane, Modular and $p$-adic cyclic codes, Des. Codes Cryptogr. 6(1995), 21-35.

[5] H. Q. Dinh, S. R. Lópex-Permouth, Cyclic and negacyclic codes over finite chain rings, IEEE Trans. Inform. Theory 50(8)(2004), 1728-1744.

[6] H. Q. Dinh, Constacyclic codes of length $p^s$ over $F_{p^n} + uF_{p^n}$, J. Algebra 324(2010), 940-950.

[7] S. T. Dougherty, M. Harada, P. Solé, Self-dual codes over rings and the Chinese remainder theorem, Hokkaido Math. J. 28(1999), 253-283.

[8] S. T. Dougherty, J.-L. Kim, H. Kulosman, MDS codes over finite principal ideal rings, Des. Codes Cryptogr., 50(1)(2009), 77-92.

[9] S. T. Dougherty, J.-L. Kim, H. Liu, Constructions of self-dual codes over finite commutative chain rings, Int. J. Inform. Coding Theory, vol. 1(2)(2010), 171-190.

[10] S. T. Dougherty, J.-L. Kim, H. Kulosman, H. Liu, Self-dual codes over commutative Frobenius rings, Finite Fields Appl.16(2010), 14-26.

[11] 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.

[12] M. Greferath, S. R. Lopez-Permouth, On the role of rings and modules in algebraic coding theory, in: Groups, Rings and Group rings, in: Lect. Notes Pure Appl. Math., vol.248, Chapman & Hall/CRC, Boca Raton, FL, 2006, 205-216.

[13] A. R. Hammons , Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, P. Solé, The $Z_4$ linearity of Kerdock, Preparata, Goethals and related codes, IEEE Trans. Inform. Theory 40(2)(1994), 301-319.

[14] W. C. Huffman, V. Pless, Fundamentals of Error-correcting Codes, Cambridge University Press, Cambridge, 2003.

[15] M. Harada, P. Solé, P. Gaborit, Self-dual codes over $Z_4$ and unimodular lattices: A survey, in: Algebra and Combinatorices, 1997, Springer, Singapore, 1999, 255-275.

[16] J.-L. Kim, Y. Lee, Euclidean and Hermitian self-dual MDS codes over large finite fields, J. Combin. Theory, Ser. A, 105(2004), 79-95.

[17] J.-L. Kim, Y. Lee, Construction of MDS self-dual codes over Galois rings, Des. Codes Cryptogr., 45(2)(2007), 247-258.

[18] P. Kanwar, S. R. López-Permouth, Cyclic codes over the integers modulo $p^m$, Finite Fields Appl.3(1997), 334-352.

[19] S. Ling, J. Blackford, $Z_{p,b+1}$-linear codes, IEEE Trans. Inform. Theory 48(2002), 2592-2605.

[20] F. J. MacWilliams, N. J. A. Sloane, The Theory of Error-Correcting Codes, North-Holland Amsterdam, The Netherlands, 1977.

[21] V. S. Pless, W. C. Huffman(Eds.), Handbook of Coding Theory, Elsevier, Amsterdam, 1998.

[22] E. Rains and N. J. A. Sloane, Self-dual codes, in the Handbook of Coding Theory, V. S. Pless and W. C. Huffman, eds., Elsevier, Amsterdam, 1998, 177-294.

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

[24] J. Wolfmann, Binary image of cyclic codes over $Z_4$, IEEE Trans. Inform. Theory 47(5)(2001), 1773-1779.

[25] J. Wood, Duality for modules over finite rings and applications to coding theory, Amer. J. Math. 121(1999), 555-575.
[26] S. Zhu, L. Wang, A class of constacyclic codes over $F_p + vF_p$ and its Gray image, Discrete Math. 311(2011), 2677-2682.

[27] 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.