Let $\mathbb{R} = \mathbb{GR}(p^e, l)$ be a Galois ring of characteristic $p^e$ and cardinality $p^el$, where $p$ and $l$ are prime integers. First, we give a canonical form decomposition for additive cyclic codes over $\mathbb{R}$. This decomposition is used to construct additive cyclic codes and count the number of such codes, respectively. Then we give the trace dual code for each additive cyclic code over $\mathbb{R}$ from its canonical form decomposition and linear codes of length $l$ over some extension Galois rings of $\mathbb{Z}_{p^e}$.

© 2015 Elsevier B.V. All rights reserved.

1. Introduction

Algebraic coding theory deals with the design of error-correcting and error-detecting codes for the reliable transmission of information across noisy channel. It in general makes use of many algebra systems such as finite fields, groups, Galois rings, polynomial algebra, module theory and matrix theory over finite chain rings and areas of discrete mathematics.

Let $R = GR(p^e, l)$ be a Galois ring of characteristic $p^e$ and cardinality $p^el$, where $p$ and $l$ are prime integers. We can regard $\mathbb{Z}_{p^e}$ as a subring of $R$ in the usual sense. Let $n$ be a positive integer. A nonempty subset $C$ of the $R$-module $R^n$ is called an additive code over $R$ of length $n$ if $C$ is a subgroup of $R^n$ under addition. Then the minimal distance of an additive code $C$ is equal to $d = \min(w_H(c) \mid c \in C, c \neq 0)$, where $w_H(c) = \{i \mid c_i \neq 0, 0 \leq i \leq n-1\}$ is the Hamming weight of $c = (c_0, c_1, \ldots, c_{n-1}) \in R^n$ with $c_i \in R$. By the Singleton Bound, we have $|C| \leq |R|^{n-d+1}$. If $|C| = |R|^{n-d+1}$, $C$ is said to be MDS (maximal distance separable). It is clear that $C$ is an additive code over $R$ if and only if $C$ is a $\mathbb{Z}_{p^e}$-submodule of $R^n$. Furthermore, an additive code $C$ is said to be cyclic if $(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$ for all $(c_0, c_1, \ldots, c_{n-1}) \in C$.

When $e = 1$, $R = GR(p, l) = \mathbb{F}_p^l$, which is a finite field of characteristic $p$ and cardinality $p^l$. For the special case of $p = l = 2$, additive codes over the finite field $\mathbb{F}_4$ were first introduced in the year 1998 in [3] connecting these codes to binary quantum codes. One year later, for the special case of $l = 2$ additive codes over the finite field $\mathbb{F}_p^2$ were connected...
in [14] to nonbinary quantum codes. Additive codes over finite fields were also generalized and studied in many papers, for example [1,2,4,5].

Let \( l = rm \) and denote \( q = p^l \). Then \( \mathbb{F}_q \) has a unique subfield of cardinality \( q \), say \( \mathbb{F}_{q^m} \), and \( \mathbb{F}_{q^m} = \mathbb{F}_{q^m} \) which is an extension field of \( \mathbb{F}_q \) with degree \( m \). As a generalization of additive codes over \( \mathbb{F}_{q^m} \), a nonempty subset \( \mathcal{C} \) of the \( \mathbb{F}_{q^m} \)-linear space \( \mathbb{F}_{q^m} \) is called an \( \mathbb{F}_q \)-linear code over \( \mathbb{F}_{q^m} \) of length \( n \) if \( \mathcal{C} \) is closed under addition and multiplication with elements from \( \mathbb{F}_q \) (cf. [6,8–10]). Huffman presented a theory for constructing and counting additive cyclic codes and additive cyclic self-orthogonal codes over \( \mathbb{F}_q \) of odd length in [11]. And later, the author extended this work to even length in [12], and developed a general theory to \( \mathbb{F}_q \)-linear cyclic codes over \( \mathbb{F}_{q^m} \) in [8].

In the rest of this paper, let \( R \) = \( GR(p^l, l) \) where \( e \geq 2 \) and \( l \) is a prime number, and \( m \) is a positive integer satisfying \( \gcd(p, m) = 1 \). We plan to consider the following questions for additive cyclic codes over \( R \) of length \( n \):

- How many distinct additive cyclic codes over \( R \) of length \( n \) are there?
- How can we construct all additive cyclic code over \( R \) of length \( n \)?
- For each additive cyclic code \( \mathcal{C} \) over \( R \) of length \( n \) constructed above, how can we give an encoder (for example, a generator matrix) and obtain the dual code of \( \mathcal{C} \)?

Now, let \( R_n \) denote the group ring \( R[X]/(X^n - 1) \) where \( (X^n - 1) \) is the ideal in \( R[X] \) generated by \( X^n - 1 \), and \( R_n^{(p)} \) the group ring \( Z_{p^l}[X]/(X^n - 1) \) where \( (X^n - 1) \) is the ideal in \( Z_{p^l}[X] \) generated by \( X^n - 1 \). From now on, we regard \( R_n^{(p)} \) as a subring of \( R_n \) in the natural way, and identify \( \alpha(X) + (X^n - 1) \in R_n \) with \( \alpha(X) \) (mod \( X^n - 1 \)) for any \( \alpha(X) \in R[X] \). Then \( R_n^{(p)} \) is a \( R_n^{(p)} \)-module. Now, for any \( \alpha(X) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} \in R_n \), we define \( \gamma: \alpha(X) \mapsto a = (a_0, a_1, \ldots, a_{n-1}) \). Then \( \gamma \) is an \( R \)-module isomorphism from \( R_n \) onto \( R^{n} \). It is clear that \( \gamma \) is an additive cyclic code over \( R \) of length \( n \) if and only if there is a unique \( R_n^{(p)} \)-submodule \( D \) of \( R_n \) such that \( \gamma(D) = \mathcal{C} \). In this paper, we will identify \( \mathcal{C} \) with \( D \) for convenience.

The present paper is organized as follows. In Section 2, we investigate the structural properties of the ring \( R_n \) and \( R_n^{(p)} \) first, and then consider the relationship between the decompositions of \( R_n \) and \( R_n^{(p)} \). In Section 3, we present a canonical form decomposition of additive cyclic codes over \( R \) of length \( n \), and consider how to enumerate, construct and encode these codes respectively. In Section 4, we give the trace dual code of an additive cyclic code over \( R \) from its canonical form decomposition, and investigate the quasi-cyclic code over \( Z_{p^l} \) of length \( nl \) and index \( l \) corresponding to each additive cyclic code over \( R \) of length \( n \). Then we consider the construction of additive cyclic codes over the Galois ring \( GR(3^2, 2) \) of length 10 in Section 5.

2. Preliminaries

In this section, we consider decompositions for the rings \( R_n \) and \( R_n^{(p)} \) first. Let \( C_i^{(b)} = \{i, ib, ib^2, \ldots \} \) (mod \( n \)) be the \( b \)-cycloctomic coset containing \( i \) modulo \( n \) and denote the size of \( C_i^{(b)} \) by \( |C_i^{(b)}| \), where \( b \) is either \( p \) or \( p^l \). Since \( l \) is a prime integer, from [8] Lemma 1 we deduce the following.

**Lemma 2.1.**

(i) If \( \gcd(|C_i^{(b)}|, l) = 1 \), then \( C_i^{(p)} = C_i^{(p^l)} \).
(ii) If \( l \mid |C_i^{(p)}| \), then \( |C_i^{(p)}| = l|C_i^{(p^l)}| \) and \( C_i^{(p)} = C_i^{(p^l)} \cup C_i^{(p^l)} \cup \cdots \cup C_i^{(p^l)} \), where the union is disjoint.

Assume \( \nu = \min\{k \in \mathbb{Z}^+ | (p^l)^k \equiv 1 \pmod{n} \} \). By the theory of Galois rings (cf. Wan [15]), there is an extension Galois ring \( \widehat{R} \) of odd length \( n \) and an invertible element \( \xi \in \widehat{R} \) of multiplicative order \( p^n - 1 \). Denote \( \widehat{T} = \{0, 1, \xi, \ldots, \xi^{p^{n-2}} \} \), which is a Teichmüller set. Then any element \( a \in \widehat{R} \) can be uniquely expressed as \( a_0 + a_1p + \cdots + a_{p^{n-1}}X^{p^{n-1}}, a_0, a_1, \ldots, a_{p^{n-1}} \in \widehat{T} \). Define

\[
\widehat{\phi}(a) = a_0^p + a_1^pX + \cdots + a_{p^{n-1}}^pX^{p^{n-1}}
\]

and let \( \phi = \widehat{\phi}|_R \) be the restriction of \( \widehat{\phi} \) to \( R \). Then \( \phi \) is a ring automorphism of \( \widehat{R} \) satisfying \( \phi(b) = b \) for any \( b \in Z_{p^l} \) (cf. [15] Theorem 14.30). \( \hat{\phi} \) is called the generalized Frobenius automorphism of \( \hat{R} \) over \( Z_{p^l} \). Let \( X \) be an indeterminate over \( \hat{R} \) and extend \( \hat{\phi} \) to a ring automorphism of \( \hat{R}[X] \) by \( \hat{\phi}(\sum a_iX^i) = \sum \hat{\phi}(a_i)X^i \) (\( \forall a_i \in \hat{R} \)). In the rest of this paper, let \( \omega = \xi^{p^{n-2}} \) and denote \( T = \{0, 1, \omega, \ldots, \omega^{p^{n-2}} \} \). Then from Galois ring theory (cf. [15] Theorem 14.27 and Corollary 14.28) we deduce the following.

- \( \text{ord}(\omega) = p^{l-1} - 1 \).
- \( R = Z_{p^l} \{a \mid a \in \sum_{i=0}^{p^{l-1}-1} c_i \omega^i \} \), and each element \( a \in R \) can be uniquely expressed as \( a = \sum_{i=0}^{p^{l-1}-1} a_i \omega^i \) with \( a_i \in T \).
- \( \phi = \hat{\phi}|_R : R \rightarrow R \), given by \( \phi(a) = \sum a_i \omega^i \) for all \( a_0, a_1, \ldots, a_{p^{l-1}} \in T \), is a ring automorphism of \( R \) satisfying \( \phi(b) = b \) for any \( b \in Z_{p^l} \). In fact, \( \phi \) is the generalized Frobenius automorphism of \( R \) over \( Z_{p^l} \). Furthermore, by [15] Theorem 14.30 we have

\[
\phi(a) = \sum_{i=0}^{p^{l-1}-1} c_i \omega^i, \quad \forall a = \sum_{i=0}^{p^{l-1}-1} c_i \omega^i, \quad c_0, c_1, \ldots, c_{p^{l-1}-1} \in Z_{p^l}.
\]
\[ \hat{\phi} \] is a ring automorphism of \( \hat{R} \) satisfying \( \hat{\phi}(a) = a \) if and only if \( a \in R \).

For any \( f(X) \in R[X], f(X) \in R[X] \) if and only if \( \hat{\phi}(f(X)) = f(X) \) and \( f(X) \in \mathbb{Z}_{p^n} [X] \) if and only if \( \hat{\phi}(f(X)) = f(X) \).

For any \( f(X) \in R[X], f(X) \in R[X] \) if and only if \( \hat{\phi}(f(X)) = f(X) \).

Let \( \eta = \zeta_{p^n}^{\frac{1}{n}} \in \hat{R} \). Then \( \eta \) is a primitive \( n \)th root of unity, and \( \hat{\phi}(\eta) = \eta^p \) since \( \eta \in \hat{F} \). Assume that \( C_j^{(p)} = \{0\}, C_{j_1}^{(p)}, \ldots, C_{j_s}^{(p)} \) are all distinct \( p \)-cyclopolcosets modulo \( n \), where \( j_0 = 0 \) and \( 1 \leq j_1, \ldots, j_s \leq n - 1 \), such that \( \gcd(|C_j^{(p)}|, l) = 1 \) for \( 0 \leq i \leq r \) and \( l||C_j^{(p)}| \) for \( r + 1 \leq i \leq s \). Then we have

\[
X^n - 1 = \sum_{i=0}^{s} m_i(X), \quad \text{where } m_i(X) = \prod_{k \in C_{j_i}^{(p)}} (X - \eta^k), \ \forall 0 \leq i \leq s.
\]

It is known that each \( m_i(X) \) is a monic basic irreducible polynomial over \( \mathbb{Z}_{p^n} \) of degree \( |C_{j_i}^{(p)}| \), and \( m_0(X), m_1(X), \ldots, m_s(X) \) are pairwise coprime.

For each \( 0 \leq i \leq s \), in the rest of this paper we denote \( \kappa_i = |C_{j_i}^{(p)}| \),

\[
R_i = \mathbb{Z}_{p^n}[X] / (m_i(X)) \quad \text{and} \quad \varepsilon_i(X) = \frac{1}{n} \sum_{v=0}^{n-1} \sum_{k \in C_{j_i}^{(p)}} \eta^{-v}X^v.
\]

Then \( \kappa_i = \deg(m_i(X)) \) and \( R_i \) is a Galois ring of characteristic \( p^n \) and cardinality \( p^{\kappa_i} \), i.e., \( R_i = \mathbb{GR}(p^n, \kappa_i) \). By \( \hat{\phi}(\eta) = \eta^p \) it follows that \( \phi(\varepsilon_i(X)) = \varepsilon_i(X) \), which implies \( \varepsilon_i(X) \in \mathbb{Z}_{p^n}[X] \). Since \( \eta^j - \eta^k \) is an invertible element of \( R \) for any \( 0 \leq j \neq k \leq n - 1 \), from ring theory and a straightforward computation we deduce the following.

**Lemma 2.2.** Using the notations above, we denote \( \mathcal{K}_i = \varepsilon_i(X)^{\mathcal{R}_i^{(p)}} \) which is the ideal of \( \mathcal{R}_n^{(p)} \) generated by \( \varepsilon_i(X) \). The following hold.

(i) \( \varepsilon_i(X)^2 = \varepsilon_i(X) \) and \( \varepsilon_i(X) \varepsilon_j(X) = 0 \) for all \( 0 \leq i \neq j \leq s \), and \( \varepsilon_0(X) + \varepsilon_1(X) + \cdots + \varepsilon_s(X) = 1 \) in \( \mathcal{R}_n^{(p)} \).

(ii) \( \mathcal{R}_n^{(p)} = \mathcal{K}_0 \oplus \mathcal{K}_1 \oplus \cdots \oplus \mathcal{K}_s \), where \( \varepsilon_i(X) \) is the multiplicative identity of \( \mathcal{K}_i \) for each \( 0 \leq i \leq s \). This direct sum is a ring direct sum in that \( \mathcal{K}_i, \mathcal{K}_j = \{0\} \) if \( i \neq j \).

(iii) For each \( 0 \leq i \leq s \), the mapping \( \varphi_i : R_i \rightarrow \mathcal{K}_i \) defined by

\[
\varphi_i(f(X)) = \varepsilon_i(X)f(X) + (X^n - 1) \quad (\forall f(X) \in \mathbb{Z}_{p^n}[X])
\]

is a ring isomorphism. Hence \( \mathcal{K}_i \) is an extension Galois ring of \( \mathbb{Z}_{p^n} \). In particular, \( \mathcal{K}_i \) is a free \( \mathbb{Z}_{p^n} \)-module of rank \( \kappa_i \) with a basis \( \{\varepsilon_i(X)X^j \mid j = 0, 1, \ldots, \kappa_i - 1\} \), i.e., \( \mathcal{K}_i = \{\sum_{j=0}^{\kappa_i-1} a_j \varepsilon_i(X)X^j \mid a_0, a_1, \ldots, a_{\kappa_i-1} \in \mathbb{Z}_{p^n}\} \).

**Remark.** For any \( 0 \leq i \leq s \), by Lemma 2.2(iii) we can write \( \mathcal{K}_i \) as \( R_i \varepsilon_i(X) = \{\varepsilon_i(X)f(X) \mod (X^n - 1) \mid f(X) \in R_i\} \) in the following sections.

Then we examine the factorization of \( X^n - 1 \) over \( R \). For each \( 0 \leq i \leq r \), \( m_i(X) \) remains basic irreducible over \( R \) as the corresponding \( C_{j_i}^{(p)} = C_{j_i}^{(p)} \) by Lemma 2.1(i). For \( r + 1 \leq i \leq s \), by Lemma 2.1(ii), we have \( \mathcal{K}_j^{(p)} = \mathcal{K}_{j_1}^{(p)} \cup \mathcal{K}_{j_2}^{(p)} \cup \cdots \cup \mathcal{K}_{j_{s-1}}^{(p)} \).

Therefore, \( m_i(X) \) factors into \( l \) distinct monic basic irreducible polynomials \( m_{i,h}(X) \) over \( R \):

\[
m_i(X) = \prod_{h=0}^{l-1} m_{i,h}(X), \quad \text{where } m_{i,h}(X) = \prod_{k \in C_{j_i}^{(p)}} (X - \eta^k), \ 0 \leq h \leq l - 1.
\]

Hence \( X^n - 1 \) factors into \( r + l(s - r) \) distinct monic basic irreducible polynomials over \( R \):

\[
X^n - 1 = \prod_{i=r+1}^{s} \prod_{h=0}^{l-1} m_{i,h}(X) \prod_{i=0}^{r} \prod_{h=0}^{l-1} m_{i,h}(X).
\]

For each \( r + 1 \leq i \leq s \) and \( 0 \leq h \leq l - 1 \), in the rest of this paper we denote \( \kappa_{i,h} = |C_{j_{i+h}}^{(p)}| \) and

\[
\varepsilon_{i,h}(X) = \frac{1}{n} \sum_{v=0}^{n-1} \sum_{k \in C_{j_{i+h}}^{(p)}} \eta^{-v}X^v.
\]

Then \( \kappa_{i,h} = \deg(m_{i,h}(X)) = \frac{n}{p^h} \). By \( \hat{\phi}(\eta) = \eta^{p^h} \) it follows that \( \hat{\phi}(\varepsilon_{i,h}(X)) = \varepsilon_{i,h}(X) \), which implies \( \varepsilon_{i,h}(X) \in R[X] \). Then from \( \mathcal{K}_j^{(p)} = \cup_{h=0}^{p^h-1} C_{j_{i+h}}^{(p)} \) and classical ring theory, we deduce the following.

**Lemma 2.3.** Using the notations above, we denote \( I_i = \varepsilon_i(X)^{\mathcal{R}_i} \) for all \( 0 \leq i \leq s \) and \( I_{i,h} = \varepsilon_{i,h}(X)^{\mathcal{R}_i} \) for all \( r + 1 \leq i \leq s \) and \( 0 \leq h \leq l - 1 \). The following hold for the ring \( \mathcal{R}_n \).

(i) For any \( r + 1 \leq i \leq s \), we have \( \varepsilon_{i,h}(X)^2 = \varepsilon_{i,h}(X), \varepsilon_{i,h}(X)\varepsilon_{i,j}(X) = 0 \) for all \( 0 \leq h \neq j \leq l - 1 \), and \( \varepsilon_{i,0}(X) + \varepsilon_{i,1}(X) + \cdots + \varepsilon_{i,l-1}(X) = \varepsilon_i(X) \).
(ii) $R_n = I_0 \oplus I_1 \oplus \cdots \oplus I_s$, where $e_i(X)$ is the multiplicative identity of $I_i$ for each $0 \leq i \leq s$. This direct sum is a ring direct sum in that $I_i I_j = \{0\}$ if $i \neq j$.

(iii) For any $r + 1 \leq i \leq s$, we have $I_i = I_{i-r} \oplus I_{i-1} \oplus \cdots \oplus I_{i+1}$, where $e_{i,h}(X)$ is the multiplicative identity of $I_{i,h}$ for each $0 \leq h \leq i - 1$. This direct sum is a ring direct sum in that $I_{i,h} I_j = \{0\}$ if $h \neq j$.

(iv) For each $0 \leq i \leq r$, the mapping $\psi_i : R[X]/(m_i(X)) \to I_i$ defined by

$$f(X) + (m_i(X)) \mapsto e_i(X)f(X) + (X^n - 1) \quad (\forall f(X) \in R[X])$$

is a ring isomorphism. Hence $I_i$ is an extension Galois ring of $R$. In particular, $I_i$ is a free $R$-module of rank $\kappa_i$.

(v) For each $r + 1 \leq i \leq s$ and $0 \leq h \leq i - 1$, the mapping $\psi_{i,h} : R[X]/(m_{i,h}(X)) \to I_{i,h}$ defined by

$$f(X) + (m_{i,h}(X)) \mapsto e_{i,h}(X)f(X) + (X^n - 1) \quad (\forall f(X) \in R[X])$$

is a ring isomorphism. Hence $I_{i,h}$ is an extension Galois ring of $R$. In particular, $I_{i,h}$ is a free $R$-module of rank $\kappa_{i,h}$.

From now on, for any $a(X) = \sum_{k=0}^{n-1} a_k X^k \in R_n$ with $a_k \in R$, we define

$$\phi(a(X)) = \sum_{k=0}^{n-1} \phi(a_k) X^k, \quad \mu(a(X)) = \sum_{k=0}^{n-1} a_k X^{-k} = X^n a\left(\frac{1}{X}\right) = \sum_{k=0}^{n-1} a_k X^{n-k}.$$

Then we have the following results.

* $\phi$ is a ring automorphism of $R_n$ of multiplicative order $l$.
* $\mu$ is a ring automorphism of $R_n$ of multiplicative order $2$. For any $a(X) \in R_n$, we will denote $\widetilde{a}(X) = \mu(a(X))$ in some cases.
* $\phi \mu = \mu \phi$.
* $R^{(p)}_n$ is precisely the subring of $R_n$ whose elements are fixed by $\phi$; i.e., $R^{(p)}_n$ is the set of polynomials in $R_n$ with all coefficients in $\mathbb{Z}_{p^r}$.

In the rest of this paper, we denote

$$\varphi(Y) = (Y - \omega)(Y - \omega^2)(\cdots)(Y - \omega^{p^r-1}).$$

Then $\varphi(Y)$ is a monic basic primitive polynomial in $\mathbb{Z}_{p^r}[Y]$ of degree $l = \operatorname{ord}(\omega) = p^r - 1$, $R = \mathbb{Z}_{p^r}[\omega] \cong \mathbb{Z}_{p^r}[Y]/(\varphi(Y))$ and every element $c$ of $R$ can be uniquely expressed as $c_0 + c_1\omega + \cdots + c_{l-1}\omega^{l-1}$ where $c_0, c_1, \ldots, c_{l-1} \in \mathbb{Z}_{p^r}$ (cf. [15] Theorem 14.8). Therefore, $R$ is a free $\mathbb{Z}_{p^r}$-module of rank $1$ and $(1, \omega, \ldots, \omega^{l-1})$ is a $\mathbb{Z}_{p^r}$-basis of the Galois ring $R$. In the following, we gather some facts about the image of $I_i$ and $I_{i,h}$ under $\phi$, and about the relationship between $K_i$ and $I_i$.

**Theorem 2.4.** Using the notations above, the following hold.

(i) $\phi(e_i(X)) = e_i(X)$ for all $0 \leq i \leq s$, and $\phi(e_{i,h}(X)) = e_{i,h+1(\text{mod } l)}(X)$ for all $r + 1 \leq i \leq s$ and $0 \leq h \leq i - 1$.

(ii) $\phi(I_i) = I_i$ for all $0 \leq i \leq s$, and $\phi(I_{i,h}) = I_{i,h+1(\text{mod } l)}$ for all $r + 1 \leq i \leq s$ and $0 \leq h \leq i - 1$.

(iii) $K_i = I_i \cap R^{(p)}_n$ and hence $K_i$ is a $K_i$-module for all $0 \leq i \leq s$.

(iv) If $0 \leq i \leq r$, then $I_i$ is a free $K_i$-module of rank $1$ with a basis given by $\{e_i(X), \omega e_i(X), \ldots, \omega^{l-1} e_i(X)\}$.

(v) If $r + 1 \leq i \leq s$, then $I_i$ is a free $K_i$-module of rank $l$ with a basis given by $\{e_i(0, X), e_i(1, X), \ldots, e_i(l-1, X)\}$.

**Proof.** (i) Because $e_i(X) \in \mathbb{Z}_{p^r}[X], \phi(e_i(X)) = e_i(X)$. The remainder of (i) follows from the definitions of $e_i(X)$ and $\phi$.

(ii) It follows from (i) and the definitions of $I_i$ and $I_{i,h}$.

(iii) Obviously, $K_i = e_i(X) R^{(p)}_n \subseteq I_i \cap R^{(p)}_n$. Conversely, let $a(X) \in I_i \cap R^{(p)}_n$. Then $a(X) \in R^{(p)}_n$ and $a(X) \in I_i$. Since $e_i(X)$ is the multiplicative identity of $I_i$ by Lemma 2.3(ii), we have $a(X) = e_i(X)a(X) \in K_i$.

(iv) Let $0 \leq i \leq r$. Then $\gcd(k_i, l) = 1$. By Lemma 2.2, $K_i$ is a Galois ring of characteristic $p^r$ and cardinality $p^{|K_i|}$. Since $\omega$ is a primitive $(p^r - 1)$th root of unity, by $\omega \in R \subseteq R_n$ and Lemmas 2.2 and 2.3 $e_i(X)\omega$ is a primitive $(p^r - 1)$th root of unity contained in $I_i$. But $K_i$ is a subring of $I_i$, and the minimal polynomial of $e_i(X)\omega$ over $K_i$ is $g_i(Y) = \sum_{j=0}^{l-1}(Y - (e_i(X)\omega)^{p^j})$ where $d = \min\{a \in \mathbb{Z}^+ \mid (p^r)^a \equiv 1 \pmod{p^r - 1}\} = \frac{l}{\gcd(k_i, l)} = l$. From this we deduce that $K_i[e_i(X)\omega] \cong K_i[Y]/(g_i(Y))$ which is a Galois ring of characteristic $p^d$ and cardinality $|K_i|^l$. Therefore, a $K_i$-basis of $K_i[e_i(X)\omega]$ is given by $\{e_i(X), e_i(X)\omega, \ldots, e_i(X)\omega^{l-1}\}$. Obviously, we have $K_i[e_i(X)\omega] \subseteq I_i$. By Lemma 2.3(iv) it follows that $|K_i| = p^{sl} = |K_i[e_i(X)\omega]|$. Hence $I_i = K_i[e_i(X)\omega]$.

(v) Let $r + 1 \leq i \leq s$ and denote $S_i = \{\sum_{h=0}^{l-1} \phi^h(\alpha) \mid \alpha \in I_i\}$. First, we claim that $K_i = S_i$. In fact, for any $\alpha \in I_{i,0}$ we have $\phi^h(\alpha) \in I_{i,h}$ by (ii), which then implies $\sum_{h=0}^{l-1} \phi^h(\alpha) = \sum_{h=0}^{l-1} I_{i,h} = I_i$ by Lemma 2.3(iii), and so $S_i \subseteq I_i$. Since the multiplicative order of $\phi$ is $l$, we have $\phi^l(\alpha) = \sum_{h=0}^{l-1} \phi^h(\alpha) = \sum_{h=0}^{l-1} \phi^{h+1}(\alpha) = \sum_{h=0}^{l-1} \phi^h(\alpha)$, which implies $\sum_{h=0}^{l-1} \phi^h(\alpha) \in R_n^p$, and so $\sum_{h=0}^{l-1} \phi^h(\alpha) \in I_i \cap R_n^p = K_i$ by (iii). Hence $S_i \subseteq K_i$. Moreover, by Lemma 2.2(iii) we have $|K_i| = |R| = p^{sl}$. Since $\phi$ is a ring automorphism of $R_n$, by Lemma 2.3(v) and $\kappa_i, \chi = \frac{1}{\phi^s} X$ we have $|S_i| = |K_i|^l = |R_i|^l = p^{sl}$. As stated above, we conclude that $K_i = S_i$. 

925
Next we prove that $\varepsilon_{1,0}(X), \varepsilon_{1,1}(X), \ldots, \varepsilon_{i-1,i-1}(X)$ are linearly independent over $K_i$. Assume that $\alpha_0, \alpha_1, \ldots, \alpha_{i-1} \in I_{i,0}$ satisfy
\[
\left(\sum_{h=0}^{l-1} \phi^h(\alpha_0)\right) \varepsilon_{1,0}(X) + \left(\sum_{h=0}^{l-1} \phi^h(\alpha_1)\right) \varepsilon_{1,1}(X) + \cdots + \left(\sum_{h=0}^{l-1} \phi^h(\alpha_{i-1})\right) \varepsilon_{i-1,i-1}(X) = 0
\]
in $I_i$. For any $0 \leq h, j \leq i - 1$, by (ii) we have $\phi^h(\alpha_j) \in I_{j,h} = \varepsilon_{i,0}(X)R_n$, which then implies $(\sum_{h=0}^{l-1} \phi^h(\alpha_j))\varepsilon_{i,j}(X) = \sum_{h=0}^{l-1} \phi^h(\alpha_j)\varepsilon_{i,j}(X) = \phi^h(\alpha_j)$ by Lemma 2.3(i) and (iii). Therefore, we have $\phi^h(\alpha_0) + \phi^h(\alpha_1) + \cdots + \phi^h(\alpha_{i-1}) = 0$. From this by Lemma 2.3(iii) and $\phi^h(\alpha_j) \in I_{i,j}$, we deduce that $\phi^h(\alpha_0) + \phi^h(\alpha_1) + \cdots + \phi^h(\alpha_{i-1}) = 0$, which implies $\alpha_j = 0$ and so $\sum_{h=0}^{l-1} \phi^h(\alpha_j) = 0$ for all $j = 0, 1, \ldots, i - 1$. Hence $\varepsilon_{1,0}(X), \varepsilon_{1,1}(X), \ldots, \varepsilon_{i-1,i-1}(X)$ are linearly independent over $K_i$.

Now, let $M_i = \{\sum_{h=0}^{l-1} q_h(\alpha_j)\varepsilon_{h,j}(X) \mid q_0(\alpha_0), \alpha_1(X), \ldots, \alpha_{i-1}(X) \in K_i\}$. As stated above, we conclude that $M_i \subseteq I_i$ and $|M_i| = |K_i|^i = (p^{r\alpha_i})^i$. By Lemma 2.3(iii) and (v) it follows that $|I_i| = \prod_{h=0}^{l-1} |I_{h,h}| = \prod_{h=0}^{l-1} |R_i|^{\varepsilon_{h,h} = \prod_{h=0}^{l-1} (p^{r\alpha_i})^i = (p^{r\alpha_i})^i = |M_i|}$. Therefore, $I_i = M_i$ and hence $\{\varepsilon_{1,0}(X), \varepsilon_{1,1}(X), \ldots, \varepsilon_{i-1,i-1}(X)\}$ is a $K_i$-basis of $I_i$. \hfill $\Box$

3. Enumerating and constructing additive cyclic codes over $R$

In this section, we discuss how to enumerate, construct and encode additive cyclic codes over $R$ of length $n$. First, we give the following lemma.

**Lemma 3.1.** Let $C \subseteq R_n$. Then the following are equivalent.

(i) $C$ is an additive cyclic code over $R$ of length $n$.

(ii) $C$ is an $R_n^{(p)}$-submodule of $R_n$.

(iii) For each $0 \leq i \leq s$, there is a unique $K_i$-submodule $C_i$ of $I_i$, such that $C = \oplus_{i=0}^{s} C_i$. In this case, $|C| = \prod_{i=0}^{s} |C_i|$ and $C_i = C \cap I_i$ for all $0 \leq i \leq s$.

**Proof.** (i)$\Rightarrow$(ii) follows from Section 1; and (ii)$\iff$(iii) follows from Lemma 2.3(ii), Lemma 2.2(i), Theorem 2.4(iii) and classical ring theory. \hfill $\Box$

For any additive cyclic code $C$ over $R$ of length $n$, by Lemma 3.1 $C$ can be uniquely decomposed into $C = \oplus_{i=0}^{s} C_i$, where $C_i$ is a $K_i$-submodule of $I_i$ for $i = 0, 1, \ldots, s$. This decomposition is called the canonical form decomposition of $C$. In order to construct additive cyclic codes over $R$ of length $n$, by Lemma 3.1 it suffices to give a method to construct all $K_i$-submodules of $I_i$ for each $0 \leq i \leq s$.

**Notation 3.2.** Using the notations of Theorem 2.4, let
\[
B_i = (\varepsilon_{1,0}(X), \varepsilon_{1,1}(X), \ldots, \varepsilon_{i-1,i-1}(X)), \quad \text{for } 0 \leq i \leq r;
\]
\[
B_i = (\varepsilon_{i,0}(X), \varepsilon_{i,1}(X), \ldots, \varepsilon_{i-1,i-1}(X)), \quad \text{for } r + 1 \leq i \leq s.
\]

For $0 \leq i \leq s$ denote by $Sub_{K_i}(I_i)$ and $Sub_{R_i}(R_i)$ the set of all $K_i$-submodules of $I_i$ and all $R_i$-submodules of $R_i$ respectively, where $R_i = Z_{p^r}[X]/(m_i(X))$ and $R_i = \{\xi \mid \xi = (a_0(X), \ldots, a_{i-1}(X)) \mid a_j(X) \in R_i, j = 0, 1, \ldots, i - 1\}$.

**Lemma 3.3.** Let $0 \leq i \leq s$. For any $C \in Sub_{R_i}(R_i)$, define $\Gamma_i(C) = \{B_i\xi^i \pmod{X^{i-1}} \mid \xi \in C\}$, where $\xi^i$ is the transpose of the row vector $\xi$. Then $\Gamma_i(C) \subseteq Sub_{K_i}(I_i)$, and $\Gamma_i : C \mapsto \Gamma_i(C)$ is a bijection from $Sub_{R_i}(R_i)$ onto $Sub_{K_i}(I_i)$.

**Proof.** By Lemma 2.2(iii), the mapping $\phi_i : R_i \rightarrow K_i$ defined by $\phi_i(a(X)) = \varepsilon_{i}(X)a(X) (\pmod{X^{i-1}})$ ($\forall a(X) \in R_i$) is a ring isomorphism. Obviously, the inverse $\phi_i^{-1} : K_i \rightarrow R_i$ is given by $\phi_i^{-1}(b(X)) = b(X) (\pmod{m_i(X)}) (\forall b(X) \in K_i)$. Let $\xi = (a_0(X), \ldots, a_{i-1}(X)) \in R_i$ and $b(X) \in K_i$. We define
\[
b(X) \cdot \xi = \phi_i^{-1}(b(X)\xi) = (b(X)a_0(X)), \ldots, (b(X)a_{i-1}(X)) (\pmod{m_i(X)}).
\]

Then $R_i$ forms a $K_i$-module, and $C \subseteq Sub_{R_i}(R_i)$ if and only if $C$ is a $K_i$-submodule of $R_i$. Therefore, $\phi_i$ induces a $K_i$-module isomorphism from $R_i$ onto $K_i$ defined by
\[
\phi_i(\xi) = (\phi_i(a_0(X)), \ldots, \phi_i(a_{i-1}(X))) = (\varepsilon_{i}(X)a_0(X), \ldots, \varepsilon_{i}(X)a_{i-1}(X)) = \varepsilon_{i}(X)\xi (\pmod{X^{i-1}})
\]
($\forall \xi = (a_0(X), \ldots, a_{i-1}(X)) \in R_i$). Hence the mapping $\sigma_i : K_i \rightarrow I_i$ defined by $\sigma_i(\phi_i(\xi)) = B_i(\varepsilon_{i}(X)\xi^i) (\pmod{X^{i-1}})$ ($\forall \xi \in R_i$) is a $K_i$-module isomorphism by Theorem 2.4, where $(\phi_i(\xi))^i$ is the transpose of the row vector $\phi_i(\xi)$.

As stated above, we conclude that $\Gamma_i = \sigma_i \phi_i$ is a $K_i$-module isomorphism from $R_i$ onto $I_i$. Moreover, by Notation 3.2 and Lemma 2.3(ii) we have
\[
\Gamma_i(\xi) = \sigma_i(\phi_i(\xi)) = B_i(\varepsilon_{i}(X)\xi^i) = B_i\xi^i (\pmod{X^{i-1}}), \forall \xi \in R_i.
\]

Therefore, $\Gamma_i : C \mapsto \Gamma_i(C)$ is a bijection from $Sub_{R_i}(R_i)$ onto $Sub_{K_i}(I_i)$. \hfill $\Box$
For each $0 \leq i \leq s$, $R_i = \mathbb{Z}_{p^i}[X]/(m_i(X))$ is a Galois ring of characteristic $p^i$ and cardinality $p^{e+1}$. Hence for any $0 \neq a(X) \in R$, there is a unique integer $t$, $0 \leq t \leq e - 1$, such that $a(X) = p^t u(X)$ where $u(X)$ is an invertible element of $R_i$. In the rest of this paper, we will denote $\|a(X)\|_p = t$ and set $\|0\|_p = e$ for convenience. Furthermore, for any $\xi = (a_0(X), a_1(X), \ldots, a_{e-1}(X)) \in R^e_i$ we define $\|\xi\|_p = \min(\|a_i(X)\|_p : 0 \leq j \leq e - 1)$.

It is known that an $R_i$-submodule of $R^e_i$ is called a linear code over $R_i$ of length $l$. Hence Sub$_{R_i}(R^e_i)$ is in fact the set of all linear codes over $R_i$ of length $l$. Now, $R_i$ is a finite chain ring, its unique maximal ideal is $pR_i$, $|R_i/pR_i| = p^{e+1}$ and the nilpotency index of $p$ is equal to $e$. From Honold and Landjev [7], Theorems 2.1, 2.3 and 2.4 we deduce the following lemma.

**Lemma 3.4.** Using the notations above, the number of linear codes over the Galois ring $R_i$ of length $l$ is equal to

$$N_{l,p^{e+1},e} = 1 + \sum_{i=1}^{e} \sum_{h_i=0}^{\infty} \prod_{j=1}^{l} p^{e(h_i+1)} \left( h_i = h_j, h_i \neq h_j = 0 \right) ,$$

where $\binom{m}{k}$ is the Gaussian coefficient.

For example, if $e = 2$ and $l = 2, 3$, we have the following formulas

$$N_{2, p^{e+1}, 2} = p^{2e} + 3p^e + 5, \quad N_{3, p^{e+1}, 2} = 2p^{3e} + 4p^{2e} + 8p^e + 5p^e + 7.$$

Then by Lemmas 3.1, 3.3 and 3.4 we obtain the following theorem.

**Theorem 3.5.** Using the notations above, the number of all distinct additive cyclic codes over $R$ of length $n$ is equal to

$$\prod_{i=0}^{n} N_{l,p^{e+1},e}.$$

**Example 3.6.** Let $R = \text{GR}(9, 2) = \mathbb{Z}_{2^3}[Y]/(g(Y))$, where $g(Y)$ is a monic basic irreducible polynomial in $\mathbb{Z}_{2^3}[Y]$ of degree 2. We count the number of all distinct additive cyclic codes over $R$ of length 10, i.e., of length 10 and $n = 10$. Since all 3-cyclotomic cosets modulo 10 are given by: $C_0^{(3)} = \{0\}$, $C_5^{(3)} = \{5\}$, $C_1^{(3)} = \{1, 3, 7, 9\}$ and $C_2^{(3)} = \{2, 6, 4, 8\}$, using the notations of Section 2 we have $\kappa_0 = |C_0^{(3)}| = 1$, $\kappa_1 = |C_1^{(3)}| = 1$, $\kappa_2 = |C_2^{(3)}| = 4$ and $\kappa_3 = |C_3^{(3)}| = 4$. Then by Theorem 3.5, the number of all distinct additive cyclic codes over $R$ of length 10 is equal to

$$\prod_{i=0}^{3} N_{2, p^{e+1}, 2} = (3^2 \cdot 3^3 + 3 \cdot 3^4 + 3 \cdot 3^5 + 3^2 + 3^3 + 3^4 + 3^5) = 24, 525, 752, 449.$$ It is known that the number of all distinct $R_i$-linear cyclic codes over $R_i$ of length 10 is equal to $(2 + 1)^4 = 81$ (cf. [16]).

Next we consider how to construct all additive cyclic codes over $R_i$ of length $n$. For each $0 \leq i \leq s$, let $G_i$ be a linear code over $R_i$ of length $l$. By Norton [13] Definition 3.1, a matrix $G_i$ is called a generator matrix of $C_i$ if the rows of $G_i$ span $C_i$ and none of them can be written as a $R_i$-linear combination of the other rows of $G_i$. Furthermore, a generator matrix $G_i$ is said to be in standard form if there is a suitable permutation matrix $U$ of size $l \times l$ such that

$$G_i = \begin{pmatrix} k_0 & 0 & \ldots & 0 \\ M_{1,0} & p & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ M_{l-1,0} & p^{l-1} & \ldots & 0 \\ M_{0,1} & M_{1,1} & \ldots & M_{l-1,1} \\ pM_{0,1} & pM_{1,1} & \ldots & pM_{l-1,1} \\ \vdots & \vdots & \ddots & \vdots \\ p^{l-1}M_{0,e-1} & p^{l-1}M_{1,e-1} & \ldots & p^{l-1}M_{l-1,e-1} \end{pmatrix} U$$

where the columns are grouped into blocks of sizes $k_0, k_1, \ldots, k_{l-1}$, $k$ with $k_0 \geq 0$ and $k = l - \sum_{j=0}^{l-1} k_j$. Of course, if $k_j = 0$, the matrices $p^{l-1}k_j$ and $p^{l-1}M_{j,0}$ are suppressed in $G_i$ for all $i = 0, 1, \ldots, e - 1$. In this case, $C_i$ is called a $\rho$-generator linear code over $R_i$, where $\rho = \sum_{j=0}^{l-1} k_j$.

Let $G_{i,1}, \ldots, G_{i,e-1}$ be row vectors of the matrix $G_i$ in (1). Then it is clear that $\|G_{i,j}\|_p = t$ for all $\sum_{j=0}^{l-1} k_j + 1 \leq j \leq \sum_{j=0}^{l-1} k_j$, and $t = 0, 1, \ldots, e - 1$ where we set $k_{l-1} = 0$. From [13] Proposition 3.2 and Theorem 3.5, we deduce the following.

**Lemma 3.7.** For any nonzero linear code $C_i$ over $R_i$ of length $l$, the following hold.

(i) $C_i$ has a generator matrix in standard form as in (1).

(ii) Let $G_i$ be a generator matrix of $C_i$ in standard form with row vectors $G_{i,1}, \ldots, G_{i,e-1}$ satisfying $\|G_{i,j}\|_p = t_j$ where $0 \leq t_1 \leq \cdots \leq t_{e-1} \leq e - 1$. Then

(ii-a) Every codeword in $C_i$ can be uniquely expressed as $\sum_{j=0}^{e-1} b_j G_j$ with $b_j \in R_i/p^{a_j} R_i$ for all $j = 1, \ldots, e$.

(ii-b) The number of codewords in $C_i$ is equal to $|C_i| = p^{\sum_{j=0}^{e-1} t_j} \cdot p^{\sum_{j=0}^{e-1} (e-j)}$.

For any vectors $\alpha = (\alpha_1, \ldots, \alpha_l), \beta = (\beta_1, \ldots, \beta_l) \in R_i^l$, the Euclidean inner product of $\alpha$ and $\beta$ is defined by $(\alpha, \beta)_E = \sum_{l=1}^{l} \alpha_l \beta_l \in R_i$. For any linear code $C_i$ over $R_i$ of length $l$, the Euclidean dual code of $C_i$ is $C_i^{\perp E} = \{ c \in R_i^l | (\alpha, c)_E = 0, \forall \beta \in C_i \}$. 
Lemma 3.8 ([13] Theorem 3.10). Let \( C_i \) be a linear code over \( R_i \) of length \( l \) with generator matrix in standard form as in (1). Then

\[
H_i = \begin{pmatrix}
B_{0,e} & B_{0,e-1} & \cdots & B_{0,1} & I_{n-p}
\\
pB_{1,e} & pB_{1,e-1} & \cdots & pB_{1,1} & 0
\\
\vdots & \vdots & \ddots & \vdots & \vdots
\\
p^{l-1}B_{l-1,e} & p^{l-1}B_{l-1,e-1} & \cdots & 0 & 0
\end{pmatrix}(U^{-1})^v
\]

(2)

is a generator matrix for \( C_i^{\perp} \) and a parity check matrix for \( C_i \), where \( B_{v,j} = -\sum_{\lambda=v+1}^{j-1} B_{v,\lambda}M^{tr}_{\epsilon-j,\epsilon-\lambda} - M^{tr}_{\epsilon-j,\epsilon-v} \) for all \( 0 \leq v < j \leq \epsilon \), \( M^{tr} \) is the transpose of a matrix \( M \) and \( \rho = \sum_{v=0}^{l} v^k_i \).

Example 3.9. We consider the special case of \( \epsilon = l = 2 \). Then every linear code \( C_i \) and its Euclidean dual code \( C_i^{\perp} \) over the Galois ring \( R_i = GR(p^2, \kappa_i) \) of length 2 has one and only one of the following matrices \( G_i \) and \( H_i \), respectively, as their generator matrices in standard form:

1. \( G_i = (1, \alpha), H_i = (-\alpha, 1) \);
2. \( G_i = (p\beta_1, 1), H_i = (1, -p\beta_1) \);
3. \( G_i = (p, p\beta_2), H_i = \left( \begin{array}{c} -\beta_2 \\ 1 \\ 0 \end{array} \right) \);
4. \( G_i = (0, p), H_i = \left( \begin{array}{c} 1 \\ 0 \\ p \end{array} \right) \);
5. \( G_i = \left( \begin{array}{c} 0 \\ \gamma \\ p \end{array} \right), H_i = (-p\gamma, p) \);
6. \( G_i = \left( \begin{array}{c} 0 \\ 1 \\ 0 \end{array} \right), H_i = (p, 0) \);
7. \( G_i = \left( \begin{array}{c} p \\ 0 \\ 0 \end{array} \right), H_i = \); \( G_i = I_2 \) and \( H_i = 0 \), or \( G_i = 0 \) and \( H_i = I_2 \),

where \( I_2 \) is the identity matrix of size \( 2 \times 2 \), \( \alpha \in R_i \) and \( \beta_1, \beta_2, \gamma \in R_i/pR_i \) (with \( |R_i| = p^{2s_i} \) and \( |R_i/pR_i| = p^{s_i} \)).

Now, we give the program to construct all additive cyclic codes over \( R_i \) of length \( n \). By Lemmas 3.1, 3.3 and 3.7, we have the following theorem.

Theorem 3.10. Using the notations of Lemma 3.3, every additive cyclic code \( C_i \) over \( R_i \) of length \( n \) can be constructed by the following four steps:

1. For each \( 0 \leq i \leq s \), choose a linear code \( C_i \) over \( R_i \) of length \( l \) with a generator matrix \( G_i \in M_{p^d \times 1}(R_i) \) in standard form, and denote \( C_i = I_1(C_i) \).
2. For each \( 0 \leq i \leq s \), calculate \( g_i = (\epsilon_i(X), \epsilon_i(X)\omega, \ldots, \epsilon_i(X)\omega^{l-1})G_i^{tr} \) if \( 0 \leq i \leq r \) and \( g_i = (\epsilon_i, 0(X), \epsilon_i,1(X), \ldots, \epsilon_i,1(X))G_i^{tr} \) if \( r + 1 \leq i \leq s \), where \( G_i^{tr} \) is the transpose of the \( C_i \).
3. Assume \( g_i = (\beta_i, \beta_i, \ldots, \beta_i, \rho) \) where \( \beta_i, j_i \in I_i \) for all \( j = 1, \ldots, \rho_i \). Then \( C_i \) is the \( K_i \)-submodule of \( I_i \) generated by \( \beta_i, 1, \ldots, \beta_i, \rho \); in particular \( C_i = \sum_{j=0}^{\rho_i} K_i \beta_i, j_i \), for all \( i = 0, 1, \ldots, s \).
4. Let \( C = C_0 + C_1 + \cdots + C_s = C_0 \oplus C_1 \oplus \cdots \oplus C_s \).

Furthermore, if the row vectors \( G_i, 1, \ldots, G_i, \rho \) of \( G_i \) satisfy \( ||G_i||_p = t_i \), where \( 0 \leq t_1 \leq \cdots \leq t_i \leq \epsilon - 1 \) for all \( i = 0, 1, \ldots, s \), the number of codewords in \( C \) is equal to \( |C| = \prod_{i=0}^{s} |C_i| = p^{\sum_{s=0}^{s} \sum_{j=1}^{\rho_i} (\epsilon_i - \epsilon_i j_i)} \).

Finally, as every additive code over \( R_i \) of length \( n \) is in fact a \( Z_{p^s} \)-submodule of \( R^n \), we can give an encoder for each additive cyclic code over \( R_i \) of length \( n \) constructed by Theorem 3.10.

Theorem 3.11. For each \( 0 \leq i \leq s \), let \( C_i \) be a \( \rho_i \)-generator linear code over \( R_i \) of length \( l \) generated by \( G_i, 1, \ldots, G_i, \rho_i \in R_i^l \) with \( t_{i,j} = ||G_i||_p \) satisfying \( 0 \leq t_{i,1} \leq t_{i,2} \leq \cdots \leq t_{i,\rho_i} \leq \epsilon - 1 \), and \( E_i = I_1(C_i) \). Then a generator matrix \( \Phi(E_i) \) of the additive cyclic code \( C = \oplus_{i=0}^{s} E_i \) over \( R \) of length \( n \) is given by the following two steps:

**Step 1** For each \( (i, j) \) such that \( 0 \leq i \leq s \), \( 1 \leq j \leq \rho_i \), using the notations of Notation 3.2 we calculate \( \beta_i, j(X) = \beta_i G_i^{tr} \in E_i \), say \( \beta_i(X) = \sum_{k=0}^{l} g_{i,j,v}x^k \) with \( g_{i,j,v} \in R \). Then we form a \( \kappa_i \times n \) matrix over \( R \):

\[
\Phi_i = \begin{pmatrix}
g_{i,j,0} & g_{i,j,1} & \cdots & g_{i,j,n-2} & g_{i,j,n-1}
g_{i,j,n-1} & g_{i,j,0} & \cdots & g_{i,j,n-3} & g_{i,j,n-2}
\vdots & \vdots & \ddots & \vdots & \vdots
\end{pmatrix}
\]

**Step 2** Let \( \Phi_i = \begin{pmatrix} \phi_{i,1} \\ \phi_{i,2} \\ \vdots \\ \phi_{i,n} \end{pmatrix} \) for \( 0 \leq i \leq s \), and set \( \Phi = \begin{pmatrix} \phi_1 \\ \phi_2 \\ \vdots \\ \phi_n \end{pmatrix} \).

If we regard \( C \) as a \( Z_{p^s} \)-submodule of \( R^n \), then \( C = \{ w \Phi \mid w \in \mathbb{Z}_{p^s}^{\sum_{s=0}^{s} \epsilon_i j_i} \} \). Precisely, we have

\[
C = \left\{ \sum_{i=0}^{s} \sum_{j=1}^{\rho_i} v_{i,j} \phi_{i,j} \mid v_{i,j} \in \mathbb{Z}_{p^s}^{\epsilon_i j_i}, \ j = 1, \ldots, \rho_i, \ i = 0, 1, \ldots, s \right\}.
\]
Proof. Let $0 \leq i \leq s$. By Lemma 3.7(ii-a), every element in $C_i$ can be uniquely expressed as $c_i = \sum_{j=1}^{n_i} b_{ij} G_{ij}$ where $b_{ij} \in R_i/(p^{r_i} - 1)/R_i$ for $j = 1, \ldots, \rho_i$. Since $R_i = Z_{p^r} [X]/(m_i(X))$ and $\deg(m_i(X)) = \kappa_i$, every element $b_{ij}$ of $R_i/(p^{r_i} - 1)/R_i$ can be uniquely expressed as

$$b_{ij} = \sum_{d=0}^{\kappa_i-1} b_{ij,d} X^d, \quad \text{where } b_{ij,d} \in Z_{p^r - 1}, \quad d = 0, 1, \ldots, \kappa_i - 1.$$

From this and by Lemma 3.3 and its proof, we deduce that every codeword in $C_i = \Gamma_i(C_i)$ can be uniquely expressed as

$$\Gamma_i(c_i) = \sigma_i(\varphi_i(c_i)) = B_i \left( \sum_{d=0}^{\kappa_i-1} b_{ij,d} X^d G_{ij} \right)^{tr} = \sum_{d=0}^{\kappa_i-1} b_{ij,d} X^d (B_i G_{ij}^{tr})$$

$$= \sum_{j=1}^{\rho_i} \sum_{d=0}^{\kappa_i-1} b_{ij,d} (X^d \beta_{ij}) = \sum_{j=1}^{\rho_i} \sum_{d=0}^{\kappa_i-1} b_{ij,d} \left( X^d \sum_{v=0}^{n_1} g_{ij,v} X^v \right)$$

$$= \sum_{j=1}^{\rho_i} v_{ij} \Phi_{ij} = (v_{i1}, \ldots, v_{i\rho_i}) \Phi_i,$$

where $v_{ij} = (b_{ij,0}, b_{ij,1}, \ldots, b_{ij,\kappa_i-1}) \in Z_{p^r}^{\kappa_i}$ for all $j = 1, \ldots, \rho_i$, and $(v_{i1}, \ldots, v_{i\rho_i}) \in Z_{p^r}^{\rho_i}$. Then the conclusions follow from $C = \oplus_{i=0}^s C_i$. □

4. Dual codes of additive cyclic codes over $R$ of length $n$

Using the notations of Section 2, let $T = \{0, 1, \omega, \ldots, \omega^{p-2} \}$ be a Teichmüller set of $R$ and $\phi$ the generalized Frobenius automorphism of $R$ over $Z_{p^r}$. As defined in [15] & 14.7,

$$T : R \to Z_{p^r} \quad \text{via} \quad T : \alpha \mapsto \sum_{k=0}^{l-1} \phi^k(\alpha)$$

is the generalized trace of $\alpha \in R$ relative to $Z_{p^r}$. It is well known that $T$ is a surjective $Z_{p^r}$-homomorphism from $R$ onto $Z_{p^r}$ (cf. [15] Theorem 14.37). The trace inner product $\langle \cdot, \cdot \rangle_T$ of $R^n$ over $Z_{p^r}$, defined by

$$\langle x, y \rangle_T = \sum_{i=0}^{n-1} T(x_i y_i) = \sum_{i=0}^{n-1} \left( \sum_{k=0}^{l-1} \phi^k(x_i y_i) \right) = \sum_{k=0}^{l-1} \phi^k \left( \sum_{i=0}^{n-1} x_i y_i \right) \in Z_{p^r},$$

where $x = (x_0, x_1, \ldots, x_{n-1}), y = (y_0, y_1, \ldots, y_{n-1}) \in R^n$, is used to define self-orthogonality and self-duality of additive codes over $R$. If $C$ is an additive code over $R$ of length $n$, its dual code is defined by $C^{\perp}_T = \{ x \in R^n \mid \langle x, c \rangle_T = 0, \forall c \in C \}$. $C$ is self-orthogonal if $C \subseteq C^{\perp}_T$ and self-dual if $C = C^{\perp}_T$.

In the following, we consider how to obtain the dual code of an additive cyclic code over $R$ of length $n$ from its canonical form decomposition. First, we investigate properties of the ring automorphism $\mu$ on $R_n$ defined in Section 2: $\mu(a(X)) = \tilde{a}(X) = X^n a(X^{-1}) \forall a(X) \in K_n$.

For each $0 \leq i \leq s$, since $C^{(p)}_{-i}$ is also a $p$-cyclic coset modulo $n$, there exists a unique integer $0 \leq i' \leq s$ such that $C^{(p)}_{-i} = C^{(p)}_{-i'}$. We also use $\mu$ to denote this map $i \mapsto i'$; that is $C^{(p)}_{-i} = C^{(p)}_{-i'}$. Whether $\mu$ denotes the automorphism of $R_n$ or this map on the set $\{0, 1, \ldots, s\}$ is determined by the context. The next lemma shows the compatibility of the two uses of $\mu$.

Lemma 4.1. With the notations above, the following hold.

(i) $\mu$ is a permutation on $\{0, 1, \ldots, s\}$ satisfying $\mu^{-1} = \mu$.

(ii) $\mu(\varepsilon_i(X)) = \varepsilon_i(X) = \varepsilon_{\mu(i)}(X)$ in the ring $R_n$ for all $0 \leq i \leq s$.

(iii) $\mu(0) = 0, 1 \leq \mu(i) \leq r$ if $1 \leq i \leq r$ and $r+1 \leq \mu(i) \leq s$ if $r+1 \leq i \leq s$.

(iv) $\mu(K_i) = K_{\mu(i)}$ and $\mu(I_i) = I_{\mu(i)}$ for all $0 \leq i \leq s$.

Proof. (i) follows from $-C^{(p)}_{-i} = C^{(p)}_{-i}$; (ii) follows from $\mu(C^{(p)}_{-i}) = \mu(-C^{(p)}_{-i}) = |C^{(p)}_{-i}| = |C^{(p)}_{i}|$; and (iv) follows from (ii) and Lemmas 2.2 and 2.3. □

Let $0 \leq i \leq s$. By Lemma 4.1(iv), the ring isomorphism $\mu$ on $R_n$ induces a ring isomorphism from $K_i$ onto $K_{\mu(i)}$ given by $a(X) \mapsto \mu(a(X)) = X^n a(X^{-1}) \forall a(X) \in K_i$. From this and by Lemma 2.2(iii), we deduce that this ring isomorphism $\mu$ determines a ring isomorphism from $R_i$ onto $R_{\mu(i)}$ given by

$$f(X) \mapsto \mu^{-1}(\mu(f(X))) = f(X) \pmod{m_{\mu(i)}(X)}$$
where $\mu(f(X)) = X^nf(X^{-1})$ for any $f(X) \in R$. We also use $\mu$ to denote this ring isomorphism $R_i \to R_{\mu(i)}$, i.e., we will use $\mu(f(X))$ or $\tilde{f}(X)$ to denote $\mu(f(X)) \mod m_{\mu(i)}(X)$ for simplicity. Since $\mu^{-1} = \mu$ as a ring isomorphism on $R_n$, we also use $\mu$ to denote the inverse isomorphism from $R_{\mu(i)}$ onto $R_i$. Furthermore, for any $\xi = (b_0(X), b_1(X), \ldots, b_{l-1}(X)) \in R_l^{R_{\mu(i)}}$ we define

$$\mu(\xi) = (\mu(b_0(X)), \mu(b_1(X)), \ldots, \mu(b_{l-1}(X))) \in R_l^i.$$ 

**Lemma 4.2.** Using the notations of Section 2, let $\frac{\varphi(Y)}{T = \sum_{i=0}^{l-1} \gamma_i Y^i}$ where $\gamma_0, \gamma_1, \ldots, \gamma_{l-1} \in R$, and denote $\theta_j = \frac{\gamma_j}{\varphi(\epsilon)} \in R$ for $j = 0, 1, \ldots, l - 1$. The following hold.

(i) $\{\theta_0, \theta_1, \ldots, \theta_{l-1}\}$ is a $Z_{p^l}$-basis of $R$ satisfying $T(\omega^j \theta_j) = 1$ and $T(\omega^k \theta_j) = 0$ for all $0 \leq k \neq j \leq l - 1$.

(ii) If $0 \leq i \leq r$, $\{e_i(X) \theta_0, e_i(X) \theta_1, \ldots, e_i(X) \theta_{l-1}\}$ is a $K_i$-basis of $I_i$.

**Proof.** (i) By the definition of the automorphism $\phi$ in Section 2, we know that $\phi(\omega) = \omega^p$. Denote $b(Y) = \sum_{i=0}^{l-1} \theta_i Y^i \in R[Y]$. By $\varphi(Y) = (Y - \omega)(Y - \omega^p) \cdots (Y - \omega^{p^{l-1}})$, we have $\frac{\varphi(Y)}{T = \sum_{i=0}^{l-1} \gamma_i Y^i}$ and $\varphi'(\omega) = \sum_{i=0}^{l-1} (\omega - \omega^i)$. So $b(Y) = \frac{\varphi(Y)}{T} / \varphi'(\omega) = \prod_{i=0}^{l-1} Y - \omega^i$. Consider the following $l \times l$ matrices over $R$:

$$A = \begin{pmatrix}
1 & 1 & \cdots & 1 \\
\omega & \omega^p & \cdots & \omega^{p^{l-1}} \\
\omega^{l-1} & \omega^{1+p} & \cdots & \omega^{l-1+p^{l-1}}
\end{pmatrix}, \\
B = \begin{pmatrix}
\theta_0 & \theta_1 & \cdots & \theta_{l-1} \\
\phi(\theta_0) & \phi(\theta_1) & \cdots & \phi(\theta_{l-1}) \\
\phi^{-1}(\theta_0) & \phi^{-1}(\theta_1) & \cdots & \phi^{-1}(\theta_{l-1})
\end{pmatrix}.
$$

Let $0 \leq k, j \leq l - 1$. Then the element of $AB$ in the position $(k + 1, j + 1)$ is

$$(AB)_{k+1,j+1} = \omega^k \theta_j + \omega^p \phi(\theta_j) + \cdots + \omega^{p^{l-1}} \phi^{-1}(\theta_j) = T(\omega^k \theta_j).$$

Since $\phi$ is a ring automorphism of $R$, the element of $BA$ in the position $(k + 1, j + 1)$ is

$$(BA)_{k+1,j+1} = \phi^k(\theta_0) + \phi(\theta_1) \phi'(\omega) + \cdots + \phi(\theta_{l-1}) \phi^{-1}(\omega^{p^{l-1}}) = \phi(\theta_0 + \theta_1 \phi^k(\omega) + \cdots + \theta_{l-1} \phi^{-1}(\omega^{l-1}))$$

$$= \phi(\phi'(\omega) w) \quad (\text{where } w \equiv j - k \pmod{1}, \quad 0 \leq w \leq l - 1)$$

$$= \delta_{kj}.$$ 

Hence $BA = I_l$, which implies that $AB = I_l$. So $T(\omega^k \theta_j) = \delta_{kj}$ as required. If $\sum_{i=0}^{l-1} \alpha_i \theta_i = 0$ for $\alpha_i \in Z_{p^l}$, then $0 = T(\omega^k \sum_{i=0}^{l-1} \alpha_i \theta_i) = \alpha_0$. Hence $\{\theta_0, \theta_1, \ldots, \theta_{l-1}\}$ is a $Z_{p^l}$-basis of $R$.

(ii) Since $\{\omega^0, \omega^1, \ldots, \omega^{l-1}\}$ and $\{\theta_0, \theta_1, \ldots, \theta_{l-1}\}$ are two $Z_{p^l}$-bases of $R$, there is a unique $l \times l$ invertible matrix $U$ over $Z_{p^l}$ such that $\{\theta_0, \theta_1, \ldots, \theta_{l-1}\} = (\omega^0, \omega^1, \ldots, \omega^{l-1})U$, which implies that

$$(e_i(X) \theta_0, e_i(X) \theta_1, \ldots, e_i(X) \theta_{l-1}) = (e_i(X) \omega^0, e_i(X) \omega^1, \ldots, e_i(X) \omega^{l-1})U.$$

Since $\{e_i(X) \omega^0, e_i(X) \omega^1, \ldots, e_i(X) \omega^{l-1}\}$ is a $K_i$-basis of $I_i$ by Theorem 2.4(iv) and $U$ is also an invertible matrix over $K_i$, by $Z_{p^l} \subseteq K_i$, we conclude that $\{e_i(X) \theta_0, e_i(X) \theta_1, \ldots, e_i(X) \theta_{l-1}\}$ is a $K_i$-basis of $I_i$. \qed

Now, we give dual codes of additive cyclic codes over $R$ of length $n$.

**Theorem 4.3.** Let $C_i = \bigoplus_{i=0}^l C_i$ be an additive cyclic code over $R$ of length $n$ constructed by Theorem 3.10, where $C_i = I_l(C_i)$ and $C_i$ is a linear code over $R_i$ of length $l$ for all $i = 0, 1, \ldots, s$. Then $C^{\perp_{tr}} = \bigoplus_{i=0}^l D_i$, where

$$D_{\mu(i)} = \left\{ \nu_{\mu(i)}(X) \sum_{t=0}^{l-1} \gamma_t(X) \theta_t \mid \gamma_0(X) \mu(X), \gamma_1(X), \ldots, \gamma_{l-1}(X) \in C_{\mu(i)}^{\perp_{tr}} \right\}$$

when $0 \leq i \leq r$, and

$$D_{\mu(i)} = \left\{ \sum_{t=0}^{l-1} \gamma_t(X) \nu_{\mu(i)}(X) \mid \gamma_0(X) \mu(X), \gamma_1(X), \ldots, \gamma_{l-1}(X) \in C_{\mu(i)}^{\perp_{tr}} \right\}$$

when $r + 1 \leq i \leq s$, and $C_{\mu(i)}^{\perp_{tr}}$ is the Euclidean dual code of $C_i$ in $R_l^i$ for $i = 0, 1, \ldots, s$. Hence $C^{\perp_{tr}}$ is also an additive cyclic code over $R$ of length $n$.

**Proof.** Denote $D = \bigoplus_{i=0}^l D_i$. Let $a(X) \in C$ and $b(X) \in D$. Then there exist $a_i(X) \in C_i$ and $b_i(X) \in D_i$, $0 \leq i \leq s$, such that $a(X) = \sum_{i=0}^s a_i(X)$ and $b(X) = \sum_{i=0}^s b_i(X)$. We denote $\Omega(a(X), b(X)) = \sum_{i=0}^{l-1} \phi^i(a(X) \mu(b(X)))$. Since $\phi$ and $\mu$ are ring isomorphisms, we have $\Omega(a(X), b(X)) = \sum_{i=0}^{l-1} \sum_{j=0}^{l-1} \Omega(a_i(X), b_j(X))$. \qed
For any \(0 \leq i \leq s\), if \(j \neq \mu(i)\), i.e., \(i \neq \mu(j)\), by Lemma 4.1(iv) and Lemma 2.3(ii) it follows that \(a_i(X)\mu(b_j(X)) \in 1\), which implies \(a_i(X)\mu(b_j(X)) = 0\), and so \(\Omega(a_i(X),b_j(X)) = \sum_{\lambda=0}^{l-1} \phi^{\lambda}(a_i(X)\mu(b_j(X))) = 0\). Hence \(\Omega(a_i(X),b_j(X)) = \sum_{l=0}^{l-1} \Omega(a_i(X),b_{\mu(i)(X)}).

Let \(0 \leq i \leq r\). Then there exist \(\xi = \xi (0, X), \ldots, \xi_{r-1}(X) \in \mathcal{C}\) and \(\xi_2 = (g_0(X), \ldots, g_{l-1}(X)) \in \mathcal{C}_r^{k-1}\) such that \(a_i(X) = \sum_{h=0}^{l-1} f_h(X) g_0(X)\xi_2(h)\) and \(b_{\mu(i)}(X) = \sum_{h=0}^{l-1} \mu(g_0(X)\xi_2(h))\xi_0(h)\), respectively. Then \(\phi(f_i(X)) = f_i(X)\) and \(\phi(g_i(X)) = g_i(X)\) for all \(0 \leq h, t \leq l - 1\). Then from Example 3.9, Theorems 3.10 and 4.3 we deduce the following.

\[
\Omega(a_i(X), b_{\mu(i)}(X)) = \sum_{l=0}^{l-1} \phi^{\lambda}(a_i(X)\mu(b_{\mu(i)(X)}))
\]

\[
\sum_{l=0}^{l-1} \phi^{\lambda}(a_i(X)\mu(b_{\mu(i)(X)})) = \sum_{l=0}^{l-1} (f_h(X) g_0(X)\xi_2(h)\xi_0(h)) e_i(X)
\]

\[
\sum_{l=0}^{l-1} \sum_{h=0}^{l-1} (f_h(X) g_0(X)\xi_2(h)\xi_0(h)) e_i(X) = e_i(X) \sum_{h=0}^{l-1} f_h(X) g_0(X) = 0.
\]

Let \(r + 1 \leq i \leq s\). Then there exist \(\xi_1 = \xi (0, X), \ldots, \xi_{l-1}(X) \in \mathcal{C}\) and \(\xi_2 = (g_0(X), \ldots, g_{l-1}(X)) \in \mathcal{C}_r^{k-1}\) such that \(a_i(X) = \sum_{h=0}^{l-1} f_h(X) g_0(X)\xi_2(h)\) and \(b_{\mu(i)}(X) = \mu(g_0(X)\xi_2(h))\xi_0(h)\), respectively. Then \(\phi(f_i(X)) = f_i(X)\) and \(\phi(g_i(X)) = g_i(X)\) for all \(0 \leq h, t \leq l - 1\). Then from Example 3.9, Theorems 3.10 and 4.3 we deduce that.

\[
\Omega(a_i(X), b_{\mu(i)}(X)) = \sum_{l=0}^{l-1} \phi^{\lambda}(a_i(X)\mu(b_{\mu(i)(X)}))
\]

\[
\sum_{l=0}^{l-1} \phi^{\lambda}(a_i(X)\mu(b_{\mu(i)(X)})) = \sum_{l=0}^{l-1} (f_h(X) g_0(X)\xi_2(h)\xi_0(h)) e_i(X)
\]

\[
\sum_{l=0}^{l-1} (f_h(X) g_0(X)\xi_2(h)\xi_0(h)) e_i(X) = e_i(X) \sum_{h=0}^{l-1} f_h(X) g_0(X) = 0.
\]

As stated above, we conclude that \(\Omega(a_i(X), b_{\mu(i)}(X)) = 0\). Now, let \(a(X) = \sum_{j=0}^{n-1} a_j X^j\) and \(b(X) = \sum_{k=0}^{n-1} b_k X^k\), where \(a = (a_0, a_1, \ldots, a_{n-1}) \in \mathcal{C} \subseteq \mathbb{R}^n\) and \(b = (b_0, b_1, \ldots, b_{n-1}) \in \mathcal{D} \subseteq \mathbb{R}^n\). Then from \(\Omega(a(X), b(X)) \equiv 0 \mod X^n - 1\) as a polynomial, and

\[
\Omega(a(X), b(X)) = \sum_{l=0}^{l-1} \phi^{\lambda}(\left(\sum_{j=0}^{n-1} a_j X^j\right)\left(\sum_{k=0}^{n-1} b_k X^k\right))
\]

\[
\equiv \sum_{l=0}^{l-1} \phi^{\lambda}\left(\sum_{j=0}^{n-1} a_j b_j\right) + \sum_{l=0}^{n-1} c_l X^l \mod X^n - 1
\]

for some \(c_1, \ldots, c_{n-1} \in \mathbb{Z}_{p^n}\), we deduce that \((a, b)_\mathcal{C} = 0\) and \((a, b)_\mathcal{D} = 0\). Hence \(\mathcal{D} \subseteq \mathcal{C}^{1,\mathfrak{m}}\). On the other hand, since \(|\mathcal{C}| = |\mathcal{D}^{1,\mathfrak{m}}| = |\mathcal{C}|^{1,\mathfrak{m}} = |\mathcal{D}|^{1,\mathfrak{m}}\), by Theorem 3.10 it follows that \(|\mathcal{C}| \mathcal{D}| = \prod_{i=0}^{1} |\mathcal{C}|^{1,\mathfrak{m}} = \prod_{i=0}^{1} |\mathcal{C}_i|^{1,\mathfrak{m}} = 0\). Therefore, we conclude that \(\mathcal{C}^{1,\mathfrak{m}} = 0\).

\[\square\]

Then from Example 3.9, Theorems 3.10 and 4.3 we deduce the following.

**Corollary 4.4.** Let \(R = \mathbb{G}(p^2, 2)\) be a Galois ring of characteristic \(p^2\) and cardinality \(p^4\), and \(n\) a positive integer satisfying \(\gcd(p, n) = 1\). Using the notations of Section 2, all distinct additive cyclic codes and their dual codes over \(R\) of length \(n\) are given by \(\mathcal{E} = \mathcal{E}_0 = \mathcal{C}_1 = \mathcal{C}^{1,\mathfrak{m}} = \mathcal{D}^{1,\mathfrak{m}} = \mathcal{D}_0 = \mathcal{D}_1\), respectively, where \((\mathcal{C}, \mathcal{D}_0, \mathcal{D}_1)\) satisfy the following conditions in which \(a(X) \in \mathcal{R}_1 = \{\sum_{j=0}^{n-1} a_j X^j \mid a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}_{p^2}\}\) and \(\beta_1(X), \beta_2(X), \gamma(X) \in \mathcal{R}_1 \mathfrak{R}_1\) for any \(0 \leq i \leq r, 1, \ldots, s\):

(i) If \(0 \leq i \leq r\), then \((\mathcal{C}_i, \mathcal{D}_0, \mathcal{D}_1)\) satisfies one of the following eight conditions:

(i-1) \(\mathcal{C}_i = R_0 \mathfrak{e}_i(X)(1 + \alpha(X)\mathfrak{a}_0), \mathcal{D}_0 = R_0 \mathfrak{e}_0(X)(\mathfrak{a}(X)\mathfrak{b}_0 + \theta_1);\)
(i-2) \( C_i = R_i \varepsilon_i(X)(p \beta_1(X) + \omega) \), \( D_{\mu(i)} = R_{\mu(\varepsilon_1)}(\varepsilon_1(X) (\theta_0 - p \beta_1(X) \theta_1)) \);

(i-3) \( C_i = R_i \varepsilon_i(X)(p + p \beta_1(X) \omega) \), \( D_{\mu(i)} = R_{\mu(\varepsilon_1)}(\varepsilon_1(X) (-p \beta_2(X) \theta_0) + \theta_1) + R_{\mu(\varepsilon_1)}(\varepsilon_1(X)(p \theta_0)) \);

(i-4) \( C_i = R_i \varepsilon_i(X)(p \omega) \), \( D_{\mu(i)} = R_{\mu(\varepsilon_1)}(\varepsilon_1(X) (\theta_0) + R_{\mu(\varepsilon_1)}(\varepsilon_1(X)\theta_1)) \);

(i-5) \( C_i = R_i \varepsilon_i(X)(1 + \gamma(X) \omega) + R_i \varepsilon_i(X)(p \omega) \), \( D_{\mu(i)} = R_{\mu(\varepsilon_1)}(\varepsilon_1(X) (p \theta_0) - p \beta(X) \theta_0) \);

(i-6) \( C_i = R_i \varepsilon_i(X)(\omega) + R_i \varepsilon_i(X)(p) \), \( D_{\mu(i)} = R_{\mu(\varepsilon_1)}(\varepsilon_1(X)(p \theta_0)) \);

(i-7) \( C_i = p I, \ D_{\mu(i)} = p I_{\mu(i)} \);

(i-8) \( C_i = \mathcal{K}_i \), and \( D_{\mu(i)} = [0] \), or \( C_i = [0] \) and \( D_{\mu(i)} = \mathcal{K}_{\mu(i)} \).

(ii) If \( r + 1 \leq s \leq t \), then \( (C_i, D_{\mu(i)}) \) satisfies one of the following eight conditions:

(ii-1) \( C_i = R_i(\varepsilon_1(X) + \alpha \varepsilon(X)_1(X), D_{\mu(i)} = R_{\mu(\varepsilon_1)}(-\tilde{\alpha})R_1(X) + \tilde{\varepsilon}_1(X)) \);

(ii-2) \( C_i = R_i(p \beta_1(X) + \varepsilon_1(X) + \varepsilon_1(X)), D_{\mu(i)} = R_{\mu(\varepsilon_1)}(-p \beta(X) \tilde{R}_1(X) + \tilde{\varepsilon}_1(X) + \varepsilon_1(X)) \);

(ii-3) \( C_i = R_i(p \varepsilon_1(X) + p \beta_2(X) \varepsilon_1(X) \varepsilon_1(X)), D_{\mu(i)} = R_{\mu(\varepsilon_1)}(-p \beta(X) \varepsilon_1(X) \varepsilon_1(X) + \tilde{\varepsilon}_1(X)) + R_{\mu(\varepsilon_1)}(p \varepsilon_1(X)) \);

(ii-4) \( C_i = R_i(\varepsilon_1(X)), D_{\mu(i)} = R_{\mu(\varepsilon_1)}(\tilde{\varepsilon}_1(X)) + R_{\mu(\varepsilon_1)}(p \varepsilon_1(X)) \);

(ii-5) \( C_i = R_i(\varepsilon_1(X) + \gamma(X) \varepsilon_1(X) \varepsilon_1(X)) + R_i(\varepsilon_1(X) \varepsilon_1(X)), D_{\mu(i)} = R_{\mu(\varepsilon_1)}(p \varepsilon_1(X) + p \beta(X) \varepsilon_1(X)) \);

(ii-6) \( C_i = R_i(\varepsilon_1(X) + R_i(\varepsilon_1(X) \varepsilon_1(X)), D_{\mu(i)} = R_{\mu(\varepsilon_1)}(p \varepsilon_1(X)) \);

(ii-7) \( C_i = p I, D_{\mu(i)} = p I_{\mu(i)} \);

(ii-8) \( C_i = \mathcal{K}_i \), and \( D_{\mu(i)} = [0] \), or \( C_i = [0] \) and \( D_{\mu(i)} = \mathcal{K}_{\mu(i)} \).

Finally, using the notations of Section 2 we see that the mapping \( \tau : R \rightarrow Z_p^l \), defined by \( \tau(\sum_{j=0}^{l-1} a_j \omega^j) = (a_0, a_1, \ldots, a_{l-1}) \), is a \( Z_p^l \)-module isomorphism from \( R \) onto \( Z_p^l \), which then induces a \( Z_p^l \)-module isomorphism from \( R^n \) onto \( Z_p^l \), defined by

\[
\tau(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) = (\tau(\alpha_0), \tau(\alpha_1), \ldots, \tau(\alpha_{l-1})), \forall \alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in R.
\]

In the following, we denote

\[
\Lambda = \begin{pmatrix}
T(1) & T(\omega) & \ldots & T(\omega^{l-1}) \\
T(\omega) & T(\omega^2) & \ldots & T(\omega^l) \\
\vdots & \vdots & \ddots & \vdots \\
T(\omega^{l-1}) & T(\omega^l) & \ldots & T(\omega^{2l-2})
\end{pmatrix} \in M_{n \times 1}(Z_p^l),
\]

where \( T \) is the generalized trace function from \( R \) onto \( Z_p^l \). One can verify that the principal minors of \( \Lambda \) are all invertible elements in \( Z_p^l \). Now, for any vectors \( u = (a_0, a_1, \ldots, a_{l-1}) \) and \( v = (b_0, b_1, \ldots, b_{l-1}) \) in \( Z_p^l \), we define \( \langle u, v \rangle_A = u \Lambda v^T = \sum_{j=0}^{l-1} \sum_{k=0}^{l-1} a_j b_k T(\omega^{j+k}) \). Then one can verify that \( \langle \cdot, \cdot \rangle_A \) is a non-degenerate and symmetric bilinear form on the \( Z_p^l \)-module \( Z_p^l \). Obviously, \( \langle \cdot, \cdot \rangle_A \) can be extended to a non-degenerate and symmetric bilinear form on the \( Z_p^l \)-module \( Z_p^m \) by the following:

\[
\langle (u_0, u_1, \ldots, u_{n-1}), (v_0, v_1, \ldots, v_{n-1}) \rangle_A = \sum_{j=0}^{n-1} u_j A v_j^T, \forall u_j, v_j \in Z_p^l.
\]

Hence \( \langle \cdot, \cdot \rangle_A \) is an inner product on \( Z_p^m \). Then, for any linear code \( C \) over \( Z_p^l \) of length \( nl \), i.e., a \( Z_p^l \)-submodule \( Z_p^m \), we define the dual code of \( C \) with respect the inner product \( \langle \cdot, \cdot \rangle_A \) as

\[
C^\perp_A = \{ \xi \in Z_p^m \mid \langle \xi, \gamma \rangle_A = 0, \forall \gamma \in C \}.
\]

**Theorem 4.5.** Using notations above, let \( C \) be an additive cyclic code over \( R \) of length \( n \) and denote \( C = \tau(C) = \{ \tau(c) \mid c \in C \} \subseteq Z_p^m \). The following hold.

(i) \( C \) is a quasi-cyclic linear code over \( Z_p^l \) of length \( nl \) and index \( l \).

(ii) \( (C)^{\perp \perp} = C \).

(iii) \( C \) is a self-dual additive code over \( R \) of length \( n \) with respect to the trace inner product \( \langle \cdot, \cdot \rangle_T \) if and only if \( C \) is a self-dual linear code over \( Z_p^l \) of length \( nl \) with respect to the inner product \( \langle \cdot, \cdot \rangle_A \).

**Proof.** (i) follows from the definition of additive cyclic codes over \( R \) of length \( n \) and the definition of quasi-cyclic codes \( Z_p^l \) of length \( nl \) and index \( l \).

(ii) For any \( \alpha, \beta \in R \) where \( \alpha = \sum_{j=0}^{l-1} a_j \omega^j, \beta = \sum_{j=0}^{l-1} b_j \omega^j \) and \( a_j, b_j \in Z_p^l \) for all \( j = 0, 1, \ldots, l - 1 \), it is clear that \( T(\alpha \beta) = (a_0, a_1, \ldots, a_{l-1})A(b_0, b_1, \ldots, b_{l-1})^T \). From this we deduce that

\[
\langle (\alpha_0, \alpha_1, \ldots, \alpha_{n-1}), (\beta_0, \beta_1, \ldots, \beta_{n-1}) \rangle_T = \sum_{k=0}^{n-1} T(\alpha_k \beta_k) = \sum_{k=0}^{n-1} \tau(\alpha_k)\Lambda(\beta_k)^{T},
\]

for all \( \alpha_k, \beta_k \in R \) and \( k = 0, 1, \ldots, n - 1 \). Hence \( \tau(C^\perp_T) = C^\perp_A \).

(iii) follows from (ii) immediately. \( \square \)
5. An example

In this section, we consider the construction of additive cyclic codes over a Galois ring $GR(3^2, 2)$ of length 10. In this case, we have $p = 3$, $e = l = 2$ and $n = 10$.

Let $\varphi(Y) = Y^2 + 5Y + 8$. Then $\varphi(Y)$ is a basic primitive polynomial with degree 2 over the ring $Z_9$ and hence $R = Z_9[1/\varphi(Y)]$ is a Galois ring. Denote $\omega = Y + (\varphi(Y))$. Then $\omega$ is a basic primitive element of $R$, i.e., $\text{ord}(\omega) = 3^2 - 1$, and satisfies $\omega^2 + 5\omega + 8 = 0$ in $R$. Hence $\omega^2 = 1 + 4\omega$, $\omega^3 = \omega(1 + 4\omega) = 4 + 8\omega$ and $R = \{a + b\omega \mid a, b \in Z_9\}$.

Let $\phi$ be the generalized Frobenius automorphism of $R$ over $Z_9$ and $T$ the generalized trace function from $R$ onto $Z_9$. Then for any $a, b \in Z_9$,

$$\phi(a + b\omega) = a + b\omega^3 = (a + 4b) + 8b\omega, \quad T(a + b\omega) = a + b\omega + \phi(a + b\omega) = 2a + 4b.$$ 

Specifically, we have $T(1) = 2$, $T(\omega) = 4$ and $T(\omega^2) = 0$. From this we deduce that $\Lambda = \begin{pmatrix} T(1) & T(\omega) & T(\omega^2) \\ T(1) & T(\omega) & T(\omega^2) \end{pmatrix} = \begin{pmatrix} 2 & 4 & 0 \end{pmatrix}$.

Therefore, for any vectors $x = (a_0 + b_0\omega, \ldots, a_9 + b_9\omega)$ and $y = (c_0 + d_0\omega, \ldots, c_9 + d_9\omega)$ in $R^{10}$ where $a_i, b_i, c_i, d_i \in Z_9$ for all $i = 0, 1, \ldots, 9$, by Theorem 4.5 the trace inner product of $x$ and $y$ is equal to

$$\langle x, y \rangle_T = \sum_{i=0}^{9} T((a_i + b_i\omega)(c_i + d_i\omega)) = \sum_{i=0}^{9} (a_i, b_i) \Lambda (c_i, d_i)$$

$$= \langle (a_0, b_0, a_1, b_1, \ldots, a_9, b_9), (c_0, d_0, c_1, d_1, \ldots, c_9, d_9) \rangle \Lambda.$$ 

Step 1. Calculate $\nu = \min\{k \in Z^+ \mid 9^k \equiv 1(\text{mod} 10)\} = 2$. Then we choose a basic primitive polynomial $h(X) = X^2 + (2\omega + 6)X + 2\omega + 4$ with degree 2 over $R$, and set $R = R[X]/(h(X))$, which is a Galois extension ring of $R$ with degree 2. Let $\zeta = x + h(\omega) \in \tilde{R}$. Then $\text{ord} (\zeta) = 9^2 - 1 = 80$ and $\zeta^2 + (2\omega + 6)\zeta + 2\omega + 4 = 0$ in $\tilde{R}$. Denote $\eta = \zeta^8 = (4\omega + 1)\zeta + 7\omega + 1$. Then $\eta$ is a primitive 10th root of unity in $\tilde{R}$.

Step 2. First, we calculate all 3-cyclotomic cosets modulo 10: $C_{3h}^{(0)} = \{0\}, C_{3h}^{(1)} = \{5\}C_{3h}^{(1)} = \{1, 3, 7, 9\}$ and $C_{3h}^{(3)} = \{2, 6, 4, 8\}$, where $j_0 = 0, j_1 = 5, j_2 = 1$ and $j_3 = 2$. Using the notations of Section 2, we have $r = 1, s = 3, k_0 = k_1 = 1$ and $k_2 = k_3 = 4$.

Then we calculate $\epsilon_{3h}(X) = \frac{1}{10} \sum_{r=0}^{9} \sum_{k \in C_{3h}^{(1)}} \zeta^{-r}X^k \in Z_9[X]$ for $i = 0, 1, 2, 3$:

$$\epsilon_{3h}(X) = \sum_{i=0}^{9} T((a_i + b_i\omega)(c_i + d_i\omega)) = \sum_{i=0}^{9} (a_i, b_i) \Lambda (c_i, d_i)$$

$$= \langle (a_0, b_0, a_1, b_1, \ldots, a_9, b_9), (c_0, d_0, c_1, d_1, \ldots, c_9, d_9) \rangle \Lambda.$$ 

Step 3. First, we calculate all 9-cyclotomic cosets modulo 10: $C_{9h}^{(0)} = C_{9h}^{(3)}, C_{9h}^{(1)} = C_{9h}^{(3)}, C_{9h}^{(2)} = \{1, 9\}, C_{9h}^{(3)} = \{3, 7\}, C_{9h}^{(4)} = \{2, 8\}$ and $C_{9h}^{(5)} = \{4, 6\}$. Then we calculate $\epsilon_{9h,k}(X) = \frac{1}{10} \sum_{r=0}^{9} \sum_{k \in C_{9h}^{(1)}} \zeta^{-r}X^k \in R[X]$ for $i = 2, 3$ and $h = 0, 1$:

$$\epsilon_{2h}(X) = (5\omega + 3)X^9 + (4\omega + 5)X^8 + (4\omega + 5)X^7 + (5\omega + 3)X^6 + 2X^5 + (5\omega + 3)X^4 + (4\omega + 5)X^3 + (4\omega + 5)X^2 + (5\omega + 3)X + 2,$$

$$\epsilon_{2h}(X) = (4\omega + 5)X^8 + (5\omega + 3)X^7 + (4\omega + 5)X^6 + 2X^5 + (5\omega + 3)X^4 + (4\omega + 5)X^3 + (5\omega + 3)X^2 + (4\omega + 5)X + 2,$$

$$\epsilon_{3h}(X) = (7\omega^2 + (5\omega + 3)X^5 + (4\omega + 6)X^4 + (4\omega + 6)X^3 + (5\omega + 3)X^2 + (5\omega + 3)X + 2,$$

$$\epsilon_{3h}(X) = (4\omega + 6)X^9 + (4\omega + 5)X^8 + (5\omega + 3)X^7 + (5\omega + 3)X^6 + 7\omega^2 + (5\omega + 3)X^4 + (5\omega + 4)X^3 + (4\omega + 6)X^2 + (4\omega + 6)X + 2.$$ 

Then $R_{10} = R[X]/(X_{10} - 1) = I_0 + I_1 + I_2 + I_3$, where $I_j = R_{10} R_{10}$ for $i = 0, 1, 2, 3$. By Theorem 2.4(iv) and (v), we have the following

- $I_0$ is a free $\mathcal{K}_0$-module of rank 2 with a $\mathcal{K}_0$-basis $\{\epsilon_{3h}(X), \omega \epsilon_{3h}(X)\}$.
- $I_1$ is a free $\mathcal{K}_1$-module of rank 2 with a $\mathcal{K}_1$-basis $\{\epsilon_{3h}(X), \omega \epsilon_{3h}(X)\}$.
- $I_2$ is a free $\mathcal{K}_2$-module of rank 2 with a $\mathcal{K}_2$-basis $\{\epsilon_{2h}(X), \epsilon_{2h}(X)\}$.
- $I_3$ is a free $\mathcal{K}_3$-module of rank 2 with a $\mathcal{K}_3$-basis $\{\epsilon_{2h}(X), \epsilon_{2h}(X)\}$.

Step 4. By $\varphi(Y) = (Y - \omega)(Y - \omega^3) = Y^2 - (\omega + \omega^3)Y + \omega^2, \varphi'(Y) = Y - \omega^3$ and $\varphi'(\omega) = \omega - \omega^3$. Let $\gamma_0 = -\omega^3$ and $\gamma_1 = 1$.

Using the notations of Lemma 4.2, we calculate $\theta_0 = \frac{\gamma_0}{\varphi'(\omega)} = \frac{-\omega^3}{\omega - \omega^3} = \frac{\omega^2}{\omega^2 - 1} = 7\omega$ and $\theta_1 = \frac{\gamma_1}{\varphi'(\omega)} = \frac{1}{\omega - \omega^3} = \frac{\omega}{1 - \omega^2} = 7 + \omega$.

From this and by Lemma 4.2, we have the following:

...
• \{e_0(X)\theta_0, e_0(X)\theta_1\} is a \mathcal{K}_0\text{-}basis of \mathcal{I}_0,
• \{e_1(X)\theta_0, e_1(X)\theta_1\} is a \mathcal{K}_1\text{-}basis of \mathcal{I}_1.

It is clear that \(-C_{i,j}^{(3)} = C_{i,j}^{(3)}\) for all \(i = 0, 1, 2, 3,\) and \(-C_{j,h}^{(q)} = C_{j,h}^{(q)}\) for all \(j = 2, 3\) and \(h = 0, 1.\) From this and the definition of \(\mu,\) we deduce that \(\mu(i) = i\) for all \(i = 0, 1, 2, 3,\) and \(\mu(\epsilon_{i,h}(X)) = \tilde{\epsilon}_{i,h}(X) = \epsilon_{i,h}(X)\) for all \(j = 2, 3\) and \(h = 0, 1.\)

**Step 5.** By Corollary 4.4 and Example 3.6, all 24525752449 additive cyclic codes and their dual codes over \(R\) of length 10 are given by the following:

\[ C = C_0 \oplus C_1 \oplus C_2 \oplus C_3 \quad \text{and} \quad C^\perp = D_0 \oplus D_1 \oplus D_2 \oplus D_3, \]

where each \((C_i, D_i)\) is a pair of \(\mathcal{K}_i\text{-}submodules of \mathcal{I}_i\) given by the following:

(i) If \(i = 0, 1,\) then \((C_i, D_i)\) satisfies one of the following eight conditions:

(i-1) \(C_i = R\epsilon_i(X)(1 + \alpha \omega), D_i = R\epsilon_i(X)(-\alpha \theta_0 + \theta_1) = R\epsilon_i(X)(7 + (1 + 2 \alpha \omega)\omega);\)

(ii-2) \(C_i = R\epsilon_i(X)(3 \beta_1 + \omega), D_i = R\epsilon_i(X)(\theta_0 - 3 \beta_1 \theta_1) = R\epsilon_i(X)(6 \beta_1 + (7 + 6 \beta_1)\omega);\)

(i-3) \(C_i = R\epsilon_i(X)(3 + 3 \beta_2 \omega), D_i = R\epsilon_i(X)(-\beta_2 \theta_0 + \theta_1) + R\epsilon_i(X)(3 \theta_0) = R\epsilon_i(X)(7 + (1 + 2 \beta_2)\omega) + R\epsilon_i(X)(3 \omega);\)

(i-4) \(C_i = R\epsilon_i(X)(3 \omega), D_i = R\epsilon_i(X)(\theta_0) + R\epsilon_i(X)(3 \theta_1) = R\epsilon_i(X)(7 \omega) + R\epsilon_i(X)(3 + 3 \omega);\)

(ii-5) \(C_i = R\epsilon_i(X)(1 + \gamma \omega) + R\epsilon_i(X)(3 \omega), D_i = R\epsilon_i(X)(3 \theta_1 - 3 \gamma \theta_0) = R\epsilon_i(X)(3 + (3 + 6 \gamma \omega)\omega);\)

(ii-6) \(C_i = R\epsilon_i(X)(\omega) + R\epsilon_i(X)(3), D_i = R\epsilon_i(X)(3 \theta_0) = R\epsilon_i(X)(3 \omega);\)

(ii-7) \(C_i = 3I_1 = D_i;\)

(ii-8) \(C_i = I_1\) and \(D_i = \{0\}, \) or \(C_i = \{0\} \) and \(D_i = I_1,\)

where \(\alpha \in \mathbb{Z}_3 = \{0, 1, \ldots, 8\} \) and \(\beta_1, \beta_2, \gamma \in \mathbb{Z}_3 = \{0, 1, 2\}.\)

(ii) If \(i = 2, 3,\) then \((C_i, D_i)\) satisfies one of the following eight conditions:

(ii-1) \(C_i = R\epsilon_i(X)(1 + \alpha \omega), D_i = R\epsilon_i(X)(-\alpha \theta_0 + \theta_1) + R\epsilon_i(X)(3 \epsilon_{i,1}(X));\)

(ii-2) \(C_i = R\epsilon_i(X)(3 \beta_1 + \omega), D_i = R\epsilon_i(X)(\theta_0 - 3 \beta_1 \theta_1) + R\epsilon_i(X)(3 \epsilon_{i,1}(X));\)

(ii-3) \(C_i = R\epsilon_i(X)(3 + 3 \beta_2 \omega), D_i = R\epsilon_i(X)(-\beta_2 \theta_0 + \theta_1) + R\epsilon_i(X)(3 \theta_0) + R\epsilon_i(X)(3 \epsilon_{i,1}(X));\)

(ii-4) \(C_i = R\epsilon_i(X)(3 \omega), D_i = R\epsilon_i(X)(\theta_0) + R\epsilon_i(X)(3 \theta_1) + R\epsilon_i(X)(7 \omega) + R\epsilon_i(X)(3 \omega) + R\epsilon_i(X)(3 \epsilon_{i,1}(X));\)

(ii-5) \(C_i = R\epsilon_i(X)(1 + \gamma \omega) + R\epsilon_i(X)(3 \omega), D_i = R\epsilon_i(X)(3 \theta_1 - 3 \gamma \theta_0) + R\epsilon_i(X)(3 + (3 + 6 \gamma \omega)\omega);\)

(ii-6) \(C_i = R\epsilon_i(X)(\omega) + R\epsilon_i(X)(3), D_i = R\epsilon_i(X)(3 \theta_0) + R\epsilon_i(X)(3 \epsilon_{i,1}(X));\)

(ii-7) \(C_i = 3I_1 = D_i;\)

(ii-8) \(C_i = I_1\) and \(D_i = \{0\}, \) or \(C_i = \{0\} \) and \(D_i = I_1,\)

where \(\alpha(X) \in \{a_0 + a_2 X + a_3 X^2 + a_4 X^3 \mid a_0, a_1, a_2, a_3 \in \mathbb{Z}_3\}, \beta_1(X), \beta_2(X), \gamma(X) \in \{b_0 + b_1 X + b_2 X^2 + b_3 X^3 \mid b_0, b_1, b_2, b_3 \in \mathbb{Z}_3\}\)

and \(\tilde{f}(X) = \mu(f(X)) = X^{10} f(X^{-1}) = f_0 + f_2 X^2 + f_3 X^3 + f_4 X^5 \) (mod \(X^{10} - 1\),

for all \(f(X) = f_0 + f_1 X + f_2 X^2 + f_3 X^3 \in \{\alpha(X), \beta_1(X), \beta_2(X), \gamma(X)\}.\)

Finally, we consider self-dual additive cyclic codes over \(R\) of length 10. Let \(C = \oplus_{i=0}^3 C_i\) be any code constructed above. It is clear that \(C\) is self-dual, i.e., \(C = C^\perp,\) if and only if \(C_i = D_i\) for all \(i = 0, 1, 2, 3.\) From this we deduce that all self-dual additive cyclic codes over \(R\) of length 10 are given by

\[ C = C_0 \oplus C_1 \oplus C_2 \oplus C_3, \]

where \(C_i\) is determined by the following conditions:

(i) If \(i = 0, 1, C_i\) satisfies one of the following three conditions:

(i-1) \(C_i = R\epsilon_i(X)(1 + 2 \omega);\) (i-2) \(C_i = R\epsilon_i(X)(\omega);\) (i-3) \(C_i = 3I_1.\)

(ii) If \(i = 2, 3, C_i = 3I_1.\)

For example, we choose \(C_0 = \mathbb{Z}_3\epsilon_0(X)(1 + 2 \omega), C_i = 3I_1\) for \(i = 1, 2, 3,\) and set \(C = \sum_{i=0}^3 C_i.\) Then \(C\) is a self-dual additive cyclic code over \(R\) of length 10 and \(|C| = \sqrt{(9)^{10}} = 81^5.\) Moreover, using the notations of Theorem 3.11 we have \(C_i = G_i(C_i)\) for \(i = 0, 1, 2, 3,\)

• \(C_0\) is a linear code over \(R_0\) of length 2 generated by \(G_{0,1} = (1, 2),\) and

(\(\beta_{0,1} = (\epsilon_0(X), \epsilon_0(X)\omega)\))

\(C_{0,1}^\perp = \epsilon_0(X) + 2 \epsilon_0(X)\omega = (1 + 2 \omega)e_0(X).\)

• \(C_1\) is a linear code over \(R_1\) of length 2 generated by \(G_{1,1} = (3, 0)\) and \(G_{1,2} = (0, 3),\) and

(\(\beta_{1,1} = (\epsilon_1(X), \epsilon_1(X)\omega)\))

\(G_{1,1}^\perp = 3 \epsilon_1(X) + 3 X^2 + 6 X^3 + 3 X^4 + 6 X^5 + 3 X^6 + 6 X^7 + 3 X^8 + 6 X^9,\)

\(\beta_{1,2} = (\epsilon_1(X), \epsilon_1(X)\omega)\))

\(G_{1,2}^\perp = 3 \epsilon_1(X) + 3 X^2 + 6 X^3 + 3 X^4 + 6 X^5 + 3 X^6 + 6 X^7 + 3 X^8 + 6 X^9,\)
• $C_2$ is a linear code over $R_2$ of length 2 generated by $G_{2,1} = (3, 0)$ and $G_{2,2} = (0, 3)$, and

$$\beta_{2,1} = (\varepsilon_{2,0}(X), \varepsilon_{2,1}(X))\tilde{G}_{2,1} = 3\varepsilon_{2,0}(X)$$
$$= 6 + 6\omega X + (6 + 3\omega)X^2 + (6 + 3\omega)X^3 + 6\omega X^4 + 6X^5 + 6\omega X^6 + (6 + 3\omega)X^7 + (6 + 3\omega)X^8 + 6\omega X^9.$$

$$\beta_{2,2} = (\varepsilon_{2,0}(X), \varepsilon_{2,1}(X))\tilde{G}_{2,2} = 3\varepsilon_{2,1}(X)$$
$$= 6 + (6 + 3\omega)X + 6\omega X^2 + 6\omega X^3 + (6 + 3\omega)X^4 + 6X^5 + (6 + 3\omega)X^6 + 6\omega X^7 + 6\omega X^8 + (6 + 3\omega)X^9.$$

• $C_3$ is a linear code over $R_3$ of length 2 generated by $G_{3,1} = (3, 0)$ and $G_{3,2} = (0, 3)$, and

$$\beta_{3,1} = (\varepsilon_{3,0}(X), \varepsilon_{3,1}(X))\tilde{G}_{3,1} = 3\varepsilon_{3,0}(X)$$
$$= 6 + (3 + 6\omega)X + 6\omega X^2 + 3\omega X^3 + (6 + 3\omega)X^4 + 3X^5 + (6 + 3\omega)X^6 + 3\omega X^7 + 6\omega X^8 + (3 + 6\omega)X^9.$$

$$\beta_{3,2} = (\varepsilon_{3,0}(X), \varepsilon_{3,1}(X))\tilde{G}_{3,2} = 3\varepsilon_{3,1}(X)$$
$$= 6 + 3\omega X + (6 + 3\omega)X^2 + (3 + 6\omega)X^3 + 6\omega X^4 + 3X^5 + 6\omega X^6 + (3 + 6\omega)X^7 + (6 + 3\omega)X^8 + 3\omega X^9.$$

By $\kappa_0 = \kappa_1 = 1, \kappa_2 = \kappa_3 = 4, \rho_0 = 1, \rho_1 = \rho_2 = \rho_3 = 2$ and Theorem 3.11 we have

$$\phi_{0,1} = (((1, 2), (1, 2), (1, 2), (1, 2), (1, 2), (1, 2), (1, 2), (1, 2)));$$
$$\phi_{1,1} = (((3, 0), (6, 0), (3, 0), (6, 0), (3, 0), (6, 0), (3, 0), (6, 0)),$$
$$\phi_{1,2} = ((0, 0), (0, 3), (0, 3), (0, 0), (0, 3), (0, 0), (0, 3), (0, 0));$$

$$\phi_{2,1} = \begin{pmatrix}
(6, 0) & (0, 6) & (6, 3) & (6, 3) & (0, 6) & (6, 0) & (6, 3) & (6, 3) & (6, 0) \\
(6, 3) & (6, 0) & (6, 6) & (6, 6) & (6, 3) & (6, 0) & (6, 6) & (6, 6) & (6, 3)
\end{pmatrix};$$

$$\phi_{2,2} = \begin{pmatrix}
(6, 0) & (6, 3) & (0, 6) & (6, 3) & (6, 0) & (6, 3) & (0, 6) & (6, 3) & (6, 0)
\end{pmatrix};$$

$$\phi_{3,1} = \begin{pmatrix}
(6, 0) & (3, 6) & (0, 6) & (3, 6) & (3, 0) & (3, 6) & (0, 6) & (3, 6) & (3, 0)
\end{pmatrix};$$

$$\phi_{3,2} = \begin{pmatrix}
(6, 0) & (0, 3) & (6, 3) & (3, 6) & (0, 6) & (3, 0) & (6, 3) & (3, 0) & (6, 3)
\end{pmatrix};$$

where we write an element $a + b\omega \in R$ as $(a, b)$ for any $a, b \in \mathbb{Z}_9$, and the Hamming weight of $a + b\omega \in R$ is defined by: $w_h(a + b\omega) = 0$ when $a = b = 0$, and $w_h(a + b\omega) = 1$ otherwise. Then by Theorem 3.11 a generator matrix of $C$ is given by $\Phi = \begin{pmatrix} \phi_1 \\ \phi_2 \\ \phi_3 \end{pmatrix}$, where $\phi_0 = \Phi_{0,1}$ and $\phi_i = \begin{pmatrix} \phi_{i,1} \\ \phi_{i,2} \end{pmatrix}$ for all $i = 1, 2, 3$. Precisely, we have

$$C = \{(a, b_1, \ldots, b_{18})\Phi \mid a \in \mathbb{Z}_9, b_1, \ldots, b_{18} \in \mathbb{Z}_3\},$$

and the Hamming weight enumerator of $C$ is given by

$$W_C(Y) = 1 + 20Y + 990Y^2 + 20400Y^3 + 286860Y^4 + 2752344Y^5 + 18350220Y^6 + 83886000Y^7 + 251658270Y^8 + 447392420Y^9 + 2682436876Y^{10}.$$
Finally, by Theorem 4.5 we obtain a self-dual quasi-cyclic code $C = \tau(C)$ over $\mathbb{Z}_9$ of length 20 and index 2, with respect to the inner product $\langle \cdot, \cdot \rangle_\Lambda$, which is a $\mathbb{Z}_9$-submodule of $\mathbb{Z}_9^{20}$ and generated by the following matrix:

$$
\begin{pmatrix}
1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 \\
3 & 0 & 6 & 0 & 3 & 0 & 6 & 0 & 3 & 0 & 6 & 0 & 3 & 0 & 6 & 0 & 3 & 0 & 6 \\
0 & 3 & 0 & 6 & 0 & 3 & 0 & 6 & 0 & 3 & 0 & 6 & 0 & 3 & 0 & 6 & 0 & 3 & 0 \\
6 & 0 & 0 & 6 & 3 & 6 & 3 & 0 & 6 & 6 & 0 & 0 & 6 & 6 & 3 & 6 & 0 & 6 & 6 \\
0 & 6 & 6 & 0 & 0 & 6 & 6 & 3 & 6 & 3 & 0 & 6 & 6 & 0 & 0 & 6 & 6 & 3 & 6 \\
6 & 3 & 0 & 6 & 6 & 0 & 0 & 6 & 6 & 3 & 6 & 3 & 0 & 6 & 6 & 0 & 0 & 6 & 6 \\
6 & 3 & 6 & 3 & 0 & 6 & 6 & 0 & 0 & 6 & 6 & 3 & 6 & 3 & 0 & 6 & 6 & 0 & 0 \\
6 & 0 & 6 & 3 & 0 & 6 & 6 & 0 & 0 & 6 & 6 & 3 & 6 & 3 & 0 & 6 & 6 & 0 & 6 \\
0 & 6 & 3 & 0 & 6 & 3 & 0 & 6 & 6 & 3 & 0 & 6 & 6 & 3 & 0 & 6 & 6 & 3 & 0 \\
0 & 6 & 6 & 3 & 0 & 6 & 6 & 3 & 0 & 6 & 6 & 3 & 0 & 6 & 6 & 3 & 0 & 6 & 6 \\
0 & 6 & 0 & 6 & 6 & 3 & 6 & 0 & 6 & 6 & 0 & 6 & 6 & 3 & 6 & 0 & 6 & 6 & 0 \\
6 & 0 & 3 & 6 & 0 & 6 & 0 & 3 & 6 & 3 & 0 & 6 & 3 & 0 & 3 & 0 & 6 & 3 & 6 \\
3 & 6 & 6 & 0 & 3 & 6 & 0 & 6 & 3 & 6 & 3 & 0 & 6 & 3 & 3 & 0 & 6 & 3 & 0 \\
0 & 6 & 3 & 6 & 6 & 0 & 3 & 6 & 0 & 6 & 3 & 6 & 3 & 0 & 6 & 3 & 3 & 0 & 6 \\
0 & 3 & 0 & 6 & 3 & 6 & 6 & 0 & 3 & 6 & 0 & 6 & 3 & 6 & 3 & 3 & 0 & 6 & 3 \\
6 & 0 & 0 & 3 & 6 & 3 & 3 & 6 & 0 & 6 & 3 & 0 & 0 & 6 & 3 & 6 & 6 & 3 & 0 \\
0 & 3 & 6 & 0 & 0 & 3 & 6 & 3 & 3 & 6 & 0 & 6 & 3 & 0 & 0 & 6 & 3 & 6 & 6 \\
6 & 3 & 0 & 3 & 6 & 0 & 0 & 3 & 6 & 3 & 3 & 6 & 0 & 6 & 3 & 0 & 0 & 6 & 3 \\
3 & 6 & 6 & 3 & 0 & 3 & 6 & 0 & 0 & 3 & 6 & 3 & 3 & 6 & 0 & 6 & 3 & 0 & 6 \\
3 & 6 & 6 & 3 & 0 & 3 & 6 & 0 & 0 & 3 & 6 & 3 & 3 & 6 & 0 & 6 & 3 & 0 & 6
\end{pmatrix}
$$

The Hamming weight enumerator of $C$ is given by

$$W_C(Y) = 1 + 380Y^2 + 2280Y^3 + 29070Y^4 + 155040Y^5 + 852720Y^6 + 3255840Y^7 + 10833420Y^8 + 28553200Y^9 + 63186552Y^{10} + 114548720Y^{11} + 211629600Y^{12} + 28553200Y^{13} + 211707120Y^{14} + 169334688Y^{15} + 105843870Y^{16} + 49806600Y^{17} + 16602580Y^{18} + 3495240Y^{19} + 2324872460Y^{20}.$$

It is known that 9-ary codes with parameters $(20, 9^{10}, 11)$ are MDS codes with respect to the Singleton bound. The code $C$ satisfies $\frac{|\text{wt}_H(C, \geq 11)|}{|C|} = 3379915898348678401 > 96.935\%$, where $\text{wt}_H(C, \geq 11)$ is the set of codewords in $C$ having Hamming weight at least 11.

6. Conclusions and further research

Let $R = \text{GR}(p^e, l)$ be a Galois ring, where $p$ and $l$ are prime integers and $e, n$ are positive integers satisfying $\gcd(p, n) = 1$. We present a canonical form decomposition of additive cyclic codes over $R$ of length $n$, and obtain conclusions on the enumeration, construction and encoders of these codes. Then we give the dual code of each code from its canonical form decomposition, and get quasi-cyclic codes over $\mathbb{Z}_{p^e}$ of length $nl$ and index $l$ from additive cyclic codes over $R$ of length $n$. These codes enjoy a rich algebraic structure compared to arbitrary additive codes (which makes the search process much simpler). Obtaining some bounds for minimal distance such as BCH-like of an additive cyclic code over the ring $R$ by just looking at the canonical form decomposition would be rather interesting.

Acknowledgments

Part of this work was done when Yonglin Cao was visiting Chern Institute of Mathematics, Nankai University, Tianjin, China. Yonglin Cao would like to thank the institution for the kind hospitality. The research is supported by the National Key Basic Research Program of China (Grant No. 2013CB834204), and the National Natural Science Foundation of China (Grant Nos. 11471255, 61171082).

References