J. Appl. Math. Comput. (2016) 52:363–385
DOI 10.1007/s12190-015-0945-z

ORIGINAL RESEARCH

# The concatenated structure of cyclic codes over $\mathbb{Z}_{p^2}$

**Yuan Cao**[1] · **Yonglin Cao**[2] · **Qingguo Li**[1]

Received: 10 August 2015 / Published online: 12 October 2015


**Abstract** Let $N = p^k n$ where $p$ is a prime, and $k, n$ are positive integers satisfying $\gcd(p, n) = 1$. We present a canonical form decomposition for every cyclic code over $\mathbb{Z}_{p^2}$ of length $N$, where each subcode is concatenated by a basic irreducible cyclic code over $\mathbb{Z}_{p^2}$ of length $n$ as the inner code and a constacyclic code over a Galois extension ring of $\mathbb{Z}_{p^2}$ of length $p^k$ as the outer code. By determining their outer codes, we present a precise description for cyclic codes over $\mathbb{Z}_{p^2}$ when $p \neq 2$, give precisely dual codes and investigate self-duality for cyclic codes over $\mathbb{Z}_{p^2}$. We end by listing cyclic self-dual codes over $\mathbb{Z}_9$ of length 33.

**Keywords** Cyclic code · Concatenated structure · Constacyclic code · Dual code · Self-dual code

**Mathematics Subject Classification** 94B05 · 94B15 · 11T71

## 1 Introduction

Abualrub and Oehmke determined the generators for cyclic codes over $\mathbb{Z}_4$ for lengths of the form $2^k$ in [1], and Blackford presented the generators for cyclic codes over

✉ Yuan Cao
yuan_cao@hnu.edu.cn

Yonglin Cao
ylcao@sdut.edu.cn

Qingguo Li
liqingguo@hnu.edu.cn

1 College of Mathematics and Econometrics, Hunan University, Changsha 410082, China

2 School of Sciences, Shandong University of Technology, Zibo 255091, Shandong, China

$\mathbb{Z}_4$ of lengths of the form $2n$ where $n$ is odd in [2]. The case for odd $n$ follows from results in [3] and also appears in more detail in [6]. Dougherty and Ling [4] determined the structure of cyclic codes over $\mathbb{Z}_4$ of arbitrary even length by giving the generator polynomials for these codes, described the number and dual codes of cyclic codes for a given length and presented the form of cyclic codes that are self-dual. Moreover, [4] proposed an open problem: study the structure of cyclic codes of arbitrary lengths over $\mathbb{Z}_{p^e}$, where $p$ is a prime and $e \geq 2$ is a positive integer.

Kiah et al. [5] derived a method of representing cyclic codes of length $p^k$ over $\mathrm{GR}(p^2, m)$, classified all cyclic codes and analysed the dual codes and self-duality. Then Sobhani and Esmaeili investigated cyclic and negacyclic codes over the Galois ring $\mathrm{GR}(p^2, m)$ in [7], and their main contribution is an expression for each cyclic code of length $p^k$ over $\mathrm{GR}(p^2, m)$ and an algorithm to find a unique set of generators for cyclic and negacyclic codes over the Galois ring $\mathrm{GR}(p^2, m)$. To the best of our knowledge, the problem of determining precise expressions for cyclic codes and their dual codes of arbitrary length over $\mathrm{GR}(p^2, m)$ has not been solved completely.

A code over a ring $R$ of length $N$ is a nonempty subset $\mathcal{C}$ of $R^N$. The code $\mathcal{C}$ is said to be *linear* if $\mathcal{C}$ is an $R$-submodule. All codes in this paper are assumed to be linear unless otherwise specified. The ambient space $R^N$ is equipped with the usual Euclidean inner product, i.e., $[a, b] = \sum_{j=0}^{N-1} a_j b_j$, where $a = (a_0, a_1, \ldots, a_{N-1})$, $b = (b_0, b_1, \ldots, b_{N-1}) \in R^N$, and the *dual code* is defined by $\mathcal{C}^{\perp} = \{a \in R^N \mid [a, b] = 0, \forall b \in \mathcal{C}\}$. If $\mathcal{C}^{\perp} = \mathcal{C}$, then $\mathcal{C}$ is called a *self-dual code* over $R$. $\mathcal{C}$ is said to be $\zeta$-*constacyclic* if $(c_0, c_1, \ldots, c_{N-1}) \in \mathcal{C}$ implies $(\zeta c_{N-1}, c_0, c_1, \ldots, c_{N-2}) \in \mathcal{C}$, where $\zeta$ is an invertible element of $R$. Especially, $\mathcal{C}$ is called a *negacyclic code* if $\zeta = -1$, and $\mathcal{C}$ is called a *cyclic code* if $\zeta = 1$. We use the natural connection of $\zeta$-constacyclic codes to polynomial rings, where $c = (c_0, c_1, \ldots, c_{N-1})$ is viewed as $c(x) = \sum_{j=0}^{N-1} c_j x^j$ and the $\zeta$-constacyclic code $\mathcal{C}$ is an ideal in the polynomial residue ring $R[x]/\langle x^N - \zeta\rangle$.

In this paper, let $N = p^k n$ where $p$ is a prime, and $n, k$ are positive integers satisfying $\gcd(p, n) = 1$. Then cyclic codes over $\mathbb{Z}_{p^2}$ of length $N$ are viewed as ideals of the ring $\mathbb{Z}_{p^2}[x]/\langle x^N - 1\rangle$. In this paper, following [7] we attempt to give a precise description for cyclic codes over $\mathbb{Z}_{p^2}$ of length $N$ by use of concatenated structure of codes. It is clear that all the conclusions we obtained can be generalized to $\mathrm{GR}(p^2, m)$ directly.

The present paper is organized as follows. In Sect. 2, we overview properties for concatenated structure of codes over rings. In Sect. 3, we present a canonical form decomposition for every cyclic code over $\mathbb{Z}_{p^2}$ of length $N$, where each subcode is concatenated by a basic irreducible cyclic code over $\mathbb{Z}_{p^2}$ of length $n$ as the inner code and a constacyclic code over a Galois extension ring of $\mathbb{Z}_{p^2}$ of length $p^k$ as the outer code, and give a precise description for cyclic codes by determining their outer codes when $p \neq 2$. Using the canonical form decomposition, we present precisely dual codes and investigate the self-duality of cyclic codes over $\mathbb{Z}_{p^2}$ in Sect. 4. Finally, we list all cyclic self-dual codes over $\mathbb{Z}_9$ of length 33.

## 2 Preliminaries

In this section, we overview properties for concatenated structure of codes.

**Notation 2.1** In this paper, let $n$ be a positive integer satisfying $\gcd(p, n) = 1$, and assume

$$y^n - 1 = f_1(y),\ f_2(y), \ldots, f_r(y), \tag{1}$$

where $f_1(y),\ f_2(y), \ldots, f_r(y)$ are pairwise coprime monic basic irreducible polynomials in $\mathbb{Z}_{p^2}[y]$. For each $i$, $1 \le i \le r$, we assume $\deg(f_i(y)) = m_i$, and denote $R_i = \mathbb{Z}_{p^2}[y]/\langle f_i(y)\rangle = \mathbb{Z}_{p^2}[\zeta_i]$ where $\zeta_i = y + \langle f_i(y)\rangle \in R_i$ satisfying $f_i(\zeta_i) = 0$.

For each integer $i$, $1 \le i \le r$, It is known that $R_i$ is a GR of characteristic $p^2$ and cardinality $p^{2m_i}$. The Teichmüller set of $R_i$ is

$$\mathcal{T}_i = \left\{ \sum_{j=0}^{m_i-1} t_j y^j \mid t_0,\ t_1, \ldots, t_{m_i-1} \in \mathbb{Z}_p \right\} = \left\{ \sum_{j=0}^{m_i-1} t_j \zeta_i^j \mid t_0,\ t_1, \ldots, t_{m_i-1} \in \mathbb{Z}_p \right\},$$

and every element $\alpha$ of $R_i$ has a unique $p$-adic expression: $\alpha = r_0 + pr_1$, $r_0,\ r_1 \in \mathcal{T}_i$. Moreover, $\alpha$ is invertible if and only if $r_0 \neq 0$.

Denote $F_i(y) = \frac{y^n-1}{f_i(y)} \in \mathbb{Z}_{p^2}[y]$ in the following. Since $F_i(y)$ and $f_i(y)$ are coprime, there are polynomials $a_i(y),\ b_i(y) \in \mathbb{Z}_{p^2}[y]$ such that

$$a_i(y)F_i(y) + b_i(y)f_i(y) = 1.$$

In the rest of this paper, we set

$$\varepsilon_i(y) \equiv a_i(y)F_i(y) = 1 - b_i(y)f_i(y) \ \left(\bmod y^n - 1\right). \tag{2}$$

Then using classical ring theory, we deduce the following lemma.

**Lemma 2.2** *Denote $\mathcal{A} = \mathbb{Z}_{p^2}[y]/\langle y^n - 1\rangle$. The following hold in $\mathcal{A}$.*

(i) $\varepsilon_1(y) + \cdots + \varepsilon_r(y) = 1$, $\varepsilon_i(y)^2 = \varepsilon_i(y)$ *and* $\varepsilon_i(y)\varepsilon_j(y) = 0$ *for all* $1 \le i \neq j \le r$.

(ii) $\mathcal{A} = \mathcal{A}_1 \oplus \cdots \oplus \mathcal{A}_r$, *where* $\mathcal{A}_i = \varepsilon_i(y)\mathcal{A}$ *and its multiplicative identity is* $\varepsilon_i(y)$. *Moreover, this decomposition is a direct sum of rings in that* $\mathcal{A}_i\mathcal{A}_j = \{0\}$ *for all* $i$ *and* $j$, $1 \le i \neq j \le r$.

(iii) *For each* $1 \le i \le r$, *define a mapping* $\varphi_i\colon g(y) \mapsto \varepsilon_i(y)g(y)$ $(\forall g(y) \in R_i)$. *Then* $\varphi_i$ *is a ring isomorphism from* $R_i$ *onto* $\mathcal{A}_i$. *Hence* $|\mathcal{A}_i| = p^{2m_i}$.

(iv) *For each* $1 \le i \le r$, $\mathcal{A}_i$ *is a basic irreducible cyclic code over* $\mathbb{Z}_{p^2}$ *of length* $n$ *having parity check polynomial* $f_i(y)$ *and generator polynomial* $F_i(y)$.

For convenience and self-sufficiency of the paper, we restate the concatenated structure of codes over rings.

**Definition 2.3** Using notations above, let $C$ be a linear code over $R_i$ of length $l$, i.e., $C$ is an $R_i$-submodule of $R_i^l = \{(r_0, r_1, \ldots, r_{l-1}) \mid r_j \in R_i,\ j = 0, 1, \ldots, l-1\}$. The *concatenated code* of $\mathcal{A}_i$ and $C$ is defined by

$$\mathcal{A}_i \square_{\varphi_i} C = \{(\varphi_i(c_0), \varphi_i(c_1), \ldots, \varphi_i(c_{l-1})) \mid (c_0, c_1, \ldots, c_{l-1}) \in C\},$$

where the cyclic code $\mathcal{A}_i$ over $\mathbb{Z}_{p^2}$ of length $n$ is called the *inner code* and $C$ is called the *outer code*.

**Lemma 2.4** *$\mathcal{A}_i \square_{\varphi_i} C$ is a linear code over $\mathbb{Z}_{p^2}$ of length $nl$. The number of codewords in this concatenated code is equal to $|\mathcal{A}_i \square_{\varphi_i} C| = |C|$ and*

$$d_{\min}\left(\mathcal{A}_i \square_{\varphi_i} C\right) \geq d_{\min}(\mathcal{A}_i)\, d_{\min}(C),$$

*where $d_{\min}(\mathcal{A}_i)$ is the minimal distance of $\mathcal{A}_i$ as a linear code over $\mathbb{Z}_{p^2}$ of length $n$ and $d_{\min}(C)$ is the minimal distance of $C$ as a linear code over the GR $R_i$ of length $l$.*

By the following theorem, we see that a generator matrix of the concatenated code $\mathcal{A}_i \square_{\varphi_i} C$ as a $\mathbb{Z}_{p^2}$-submodule can be constructed from a generator matrix of the cyclic code $\mathcal{A}_i$ over $\mathbb{Z}_{p^2}$ and a generator matrix of the linear code $C$ over the GR $R_i$ straightforwardly.

**Theorem 2.5** *Let $\varepsilon_i(y) = \sum_{j=0}^{n-1} e_{i,j} y^j$ with $e_{i,j} \in \mathbb{Z}_{p^2}$, and $C$ be a linear code over the GR $R_i$ of length $l$ with a generator matrix $G_C \in \mathrm{M}_{t \times l}(R_i)$, i.e., $C$ is an $R_i$-submodule of $R_i^l$ generated by the row vectors of $G_C$. The following hold.*

(i) *A generator matrix of the cyclic code $\mathcal{A}_i$ is given by*

$$G_{\mathcal{A}_i} = \begin{pmatrix} e_{i,0} & e_{i,1} & \cdots & e_{i,n-2} & e_{i,n-1} \\ e_{i,n-1} & e_{i,0} & \cdots & e_{i,n-3} & e_{i,n-2} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ e_{i,n-m_i+1} & e_{i,n-m_i+2} & \cdots & e_{i,n-m_i-1} & e_{i,n-m_i} \end{pmatrix}.$$

(ii) *Assume $f_i(y) = \sum_{j=0}^{m_i} f_{i,j} y^j$ with $f_{i,j} \in \mathbb{Z}_{p^2}$ and $f_{i,m_i} = 1$, and let $M_{f_i} = \begin{pmatrix} 0 & I_{m_i-1} \\ -f_{i,0} & V_i \end{pmatrix}$ be the companion matrix of $f_i(y)$ where $I_{m_i-1}$ is the identity matrix of order $m_i - 1$ and $V_i = (-f_{i,1}, \ldots, -f_{i,m_i-1})$. For any $\alpha = \alpha(y) = \sum_{j=0}^{m_i-1} r_j y^j \in R_i$ with $r_j \in \mathbb{Z}_{p^2}$, denote $A_\alpha = \alpha(M_{f_i}) = \sum_{j=0}^{m_i-1} r_j M_{f_i}^j \in \mathrm{M}_{m_i \times m_i}(\mathbb{Z}_{p^2})$ in the rest of the paper. Then*

$$\alpha Y = A_\alpha Y, \quad \text{where} \quad Y = \begin{pmatrix} 1 \\ y \\ \cdots \\ y^{m_i-1} \end{pmatrix}.$$

(iii) *Let* $G_C = (\alpha_{j,s})_{1\leq j\leq t,\, 1\leq s\leq l}$ *with* $\alpha_{j,s} \in R_i$. *Then a generator matrix of the concatenated code* $\mathcal{A}_i\Box_{\varphi_i}C$ *is given by*

$$G_{\mathcal{A}_i\Box_{\varphi_i}C} = \begin{pmatrix} A_{\alpha_{1,1}}G_{\mathcal{A}_i} & \dots & A_{\alpha_{1,l}}G_{\mathcal{A}_i} \\ \dots & \dots & \dots \\ A_{\alpha_{t,1}}G_{\mathcal{A}_i} & \dots & A_{\alpha_{t,l}}G_{\mathcal{A}_i} \end{pmatrix}.$$

*Hence* $\mathcal{A}_i\Box_{\varphi_i}C = \{\underline{w}G_{\mathcal{A}_i\Box_{\varphi_i}C} \mid \underline{w} \in \mathbb{Z}_{p^2}^{m_it}\}$.

*Proof* (i) Since $f_i(y)$ is a monic basic irreducible polynomial in $\mathbb{Z}_{p^2}[y]$ of degree $m_i$, $\{1, y, \dots, y^{m_i-1}\}$ is a $\mathbb{Z}_{p^2}$-basis of the GR $R_i = \mathbb{Z}_{p^2}[y]/\langle f_i(y)\rangle$. As $\varphi_i$ is a $\mathbb{Z}_{p^2}$-module isomorphism from $R_i$ onto $\mathcal{A}_i$ by Lemma 2.2(iii), we conclude that $\{\varepsilon_i(y), y\varepsilon_i(y), \dots, y^{m_i-1}\varepsilon_i(y)\}$ is a $\mathbb{Z}_{p^2}$-basis of $\mathcal{A}_i$. Hence $G_{\mathcal{A}_i}$ is a generator matrix of $\mathcal{A}_i$ as a $\mathbb{Z}_{p^2}$-submodule of $\mathbb{Z}_{p^2}^n$.

(ii) It is obvious that $yY = M_{f_i}Y$, which then implies that $y^jY = M_{f_i}^jY$ for all $j = 0, 1, \dots, m_i - 1$. Hence $\alpha Y = \sum_{j=0}^{m_i-1} r_j(y^jY) = A_\alpha Y$.

(iii) Let $\mathcal{C}$ be the $\mathbb{Z}_{p^2}$-submodule of $\mathbb{Z}_{p^2}^{nl}$ generated by the row vectors of $G_{\mathcal{A}_i\Box_{\varphi_i}C}$, i.e., $\mathcal{C} = \{\underline{w}G_{\mathcal{A}_i\Box_{\varphi_i}C} \mid \underline{w} \in \mathbb{Z}_{p^2}^{m_it}\}$. By Definition 2.3, $\xi \in \mathcal{A}_i\Box_{\varphi_i}C$ if and only if there exists a unique codeword $c = (c_1, \dots, c_l) \in C$ such that $\xi = (\varphi_i(c_1), \dots, \varphi_i(c_l))$. Since $G_C$ is a generator matrix of $C$, $c \in C$ if and only if $c$ is an $R_i$-combination of the row vectors $(\alpha_{1,1}, \dots, \alpha_{1,l}), \dots, (\alpha_{t,1}, \dots, \alpha_{t,l})$ of $G_C$, which is equivalent that there exist $\beta_1, \dots, \beta_t \in R_i$ such that

$$\begin{aligned}\xi &= \left(\varphi_i\left(\beta_1\alpha_{1,1} + \dots + \beta_t\alpha_{t,1}\right), \dots, \varphi_i\left(\beta_1\alpha_{1,l} + \dots + \beta_t\alpha_{t,l}\right)\right) \\ &= \left(\varphi_i\left(\beta_1\alpha_{1,1}\right) + \dots + \varphi_i\left(\beta_t\alpha_{t,1}\right), \dots, \varphi_i\left(\beta_1\alpha_{1,l}\right) + \dots + \varphi_i\left(\beta_t\alpha_{t,l}\right)\right),\end{aligned}$$

since $\varphi_i$ is a $\mathbb{Z}_{p^2}$-module isomorphism. For each integer $j$, $1 \leq j \leq t$, by $\beta_j \in R_i$ there is a unique row vector $\underline{b}_j \in \mathbb{Z}_{p^2}^{m_i}$ such that $\beta_j = \underline{b}_jY$. From this and by (ii) we deduce that $\beta_j\alpha_{j,s} = \underline{b}_j(\alpha_{j,s}Y) = \underline{b}_jA_{\alpha_{j,s}}Y$ for all $s = 1, \dots, l$. Also, since $\varphi_i$ is a $\mathbb{Z}_{p^2}$-module isomorphism, we have

$$\begin{aligned}\xi &= \left(\underline{b}_1A_{\alpha_{1,1}}\varphi_i(Y) + \dots + \underline{b}_tA_{\alpha_{t,1}}\varphi_i(Y), \dots, \underline{b}_1A_{\alpha_{1,l}}\varphi_i(Y) + \dots + \underline{b}_tA_{\alpha_{t,l}}\varphi_i(Y)\right) \\ &= \underline{w}\begin{pmatrix} A_{\alpha_{1,1}}\varphi_i(Y) & \dots & A_{\alpha_{1,l}}\varphi_i(Y) \\ \dots & \dots & \dots \\ A_{\alpha_{t,1}}\varphi_i(Y) & \dots & A_{\alpha_{t,l}}\varphi_i(Y) \end{pmatrix},\end{aligned}$$

where $\underline{w} = (\underline{b}_1, \dots, \underline{b}_t) \in \mathbb{Z}_{p^2}^{m_it}$. Then by

$$\varphi_i(Y) = \begin{pmatrix} \varphi_i(1) \\ \varphi_i(y) \\ \dots \\ \varphi_i(y^{m_i-1}) \end{pmatrix} = \begin{pmatrix} \varepsilon_i(y) \\ y\varepsilon_i(y) \\ \dots \\ y^{m_i-1}\varepsilon_i(y) \end{pmatrix} = G_{\mathcal{A}_i}\begin{pmatrix} 1 \\ y \\ \dots \\ y^{n-1} \end{pmatrix},$$

and the identification of $\mathbb{Z}_{p^2}[y]\langle y^n-1\rangle$ with $\mathbb{Z}_{p^2}^n$, we deduce $\xi = \underline{w}G_{\mathcal{A}_i\Box_{\varphi_i}C} \in \mathcal{C}$. Therefore, $\mathcal{A}_i\Box_{\varphi_i}C = \mathcal{C}$. □

## 3 The concatenated structure of cyclic codes over $\mathbb{Z}_{p^2}$ of length $p^k n$

From now on, let $N = p^k n$ where $k$ is a positive integer. As usual, we will identify $\mathbb{Z}_{p^2}^N$ with $\mathbb{Z}_{p^2}[x]/\langle x^N-1\rangle$ under the natural $\mathbb{Z}_{p^2}$-module isomorphism: $(c_0, c_1, \ldots, c_{N-1}) \mapsto c_0+c_1x+\cdots+c_{N-1}x^{N-1}$ $(\forall c_j \in \mathbb{Z}_{p^2},\ j=0, 1, \ldots, N-1)$.

Using the notations of Lemma 2.2, each element of the ring $\mathcal{A}$ can be uniquely expressed as $a(y) = \sum_{j=0}^{n-1} a_j y^j$ with $a_j \in \mathbb{Z}_{p^2}$. Then each element of the quotient ring $\mathcal{A}[x]/\langle x^{p^k} - y\rangle$ can be uniquely expressed as

$$\alpha(x,\ y) = \left(1,\ y, \ldots, y^{n-1}\right) M \begin{pmatrix} 1 \\ x \\ \cdots \\ x^{p^k-1} \end{pmatrix},$$

where $M$ is a matrix over $\mathbb{Z}_{p^2}$ of size $n \times p^k$. Now, define

$$\Psi(\alpha(x,\ y)) = \alpha\left(x,\ x^{p^k}\right) = \left(1,\ x^{p^k}, \ldots, x^{p^k(n-1)}\right) M \begin{pmatrix} 1 \\ x \\ \cdots \\ x^{p^k-1} \end{pmatrix}.$$

It is clear that $\Psi$ is a ring isomorphism from $\mathcal{A}[x]/\langle x^{p^k} - y\rangle$ onto $\mathbb{Z}_{p^2}[x]/\langle x^N-1\rangle$. In the rest of this paper, we will identify $\mathcal{A}[x]/\langle x^{p^k} - y\rangle$ with $\mathbb{Z}_{p^2}[x]/\langle x^N-1\rangle$ under this isomorphism $\Psi$.

**Theorem 3.1** *Using the notations in Notation 2.1 and Lemma 2.2, and let $\mathcal{C} \subseteq \mathbb{Z}_{p^2}[x]/\langle x^N-1\rangle$. The following are equivalent*:

(i) *$\mathcal{C}$ is a cyclic code over $\mathbb{Z}_{p^2}$ of length $N$.*

(ii) *$\mathcal{C}$ is an ideal of the ring $\mathcal{A}[x]/\langle x^{p^k} - y\rangle$.*

(iii) *For each integer $i$, $1 \le i \le r$, there is a unique $\zeta_i$-constacyclic code $C_i$ over $R_i$ of length $p^k$, i.e., an ideal $C_i$ of the ring $R_i[x]/\langle x^{p^k} - \zeta_i\rangle$, such that $\mathcal{C} = (\mathcal{A}_1\Box_{\varphi_1}C_1) \oplus \cdots \oplus (\mathcal{A}_r\Box_{\varphi_r}C_r)$.*

*Proof* We only need to prove (ii)⇔(iii). By Lemma 2.2(ii) it follows that $\mathcal{A}[x]/\langle x^{p^k} - y\rangle = \oplus_{i=1}^r(\mathcal{A}_i[x]/\langle x^{p^k} - y\rangle)$. As $\mathbb{Z}_{p^2}[x]/\langle x^N-1\rangle = \mathcal{A}[x]/\langle x^{p^k} - y\rangle$, we see that $\mathcal{C}$ is an ideal of the ring $\mathbb{Z}_{p^2}[x]/\langle x^N-1\rangle$ if and only if for each integer $i$, $1 \le i \le r$, there is a unique ideal $\mathcal{C}_i$ of the ring $\mathcal{A}_i[x]/\langle x^{p^k} - y\rangle$ such that $\mathcal{C} = \oplus_{i=1}^r\mathcal{C}_i$.

By Lemma 2.2(iii), $\varphi_i\colon g(y) \mapsto \varepsilon_i(y)g(y)$ $(\forall g(y) \in R_i)$ is a ring isomorphism from $R_i$ onto $\mathcal{A}_i$. As $R_i = \mathbb{Z}_{p^2}[y]/\langle f_i(y)\rangle = \mathbb{Z}_{p^2}[\zeta_i]$ where $\zeta_i = y + \langle f_i(y)\rangle$, the inverse isomorphism $\psi_i$ of $\varphi_i$ is given by

$$\psi_i(h(y)) = h(y) \pmod{f_i(y)} \quad \text{or} \quad \psi_i(h(y)) = h(\zeta_i), \quad \forall h(y) \in \mathcal{A}_i.$$

Then $\psi_i$ induces a ring isomorphism from $\mathcal{A}_i[x]/\langle x^{p^k} - y\rangle$ onto $R_i[x]/\langle x^{p^k} - \zeta_i\rangle$ in the natural way:

$$\psi_i\left(\sum_{j=0}^{p^k-1} h_j(y)x^j\right) = \sum_{j=0}^{p^k-1} h_j(\zeta_i)x^j, \quad \forall h_0(y), h_1(y), \ldots, h_{p^k-1}(y) \in \mathcal{A}_i.$$

By $\varphi_i = \psi_i^{-1}$, $\varphi_i$ induces a ring isomorphism from $R_i[x]/\langle x^{p^k} - \zeta_i\rangle$ onto $\mathcal{A}_i[x]/\langle x^{p^k} - y\rangle$ by the following: $\forall g_0, g_1, \ldots, g_{p^k-1} \in R_i$,

$$\varphi_i\left(\sum_{j=0}^{p^k-1} g_j x^j\right) = \sum_{j=0}^{p^k-1} \varphi_i\left(g_j\right)x^j \leftrightarrow \left(\varphi_i(g_0), \varphi_i(g_1), \ldots, \varphi_i\left(g_{p^k-1}\right)\right) \in \mathcal{A}_i^{p^k}.$$

Therefore, for each integer $i$, $1 \le i \le r$, and the ideal $\mathcal{C}_i$ of $\mathcal{A}_i[x]/\langle x^{p^k} - y\rangle$, there is a unique ideal $C_i$ of $R_i[x]/\langle x^{p^k} - \zeta_i\rangle$ such that $\mathcal{C}_i = \varphi_i(C_i)$, which implies $\mathcal{C}_i = \mathcal{A}_i \Box_{\varphi_i} C_i$ by Definition 2.3. It is clear that $C_i$ is a $\zeta_i$-constacyclic code over $R_i$ of length $p^k$. □

By Theorem 3.1, in order to present all cyclic codes over $\mathbb{Z}_{p^2}$ of length $N$ it is sufficient to determine all ideals of the ring $R_i[x]/\langle x^{p^k} - \zeta_i\rangle$, where $R_i = \mathbb{Z}_{p^2}[\zeta_i]$ and $\zeta_i = y + \langle f_i(y)\rangle$ satisfies $f_i(\zeta_i) = 0$, for all $i = 1, \ldots, r$.

Since $\gcd(p, n) = 1$, there is a positive integer $v$, $1 \le v < n$, such that $p^k v \equiv 1 \pmod{n}$. By Eq. (1) it follows that $\zeta_i^n = 1$. From this we deduce $(\zeta_i^v)^{p^k} = \zeta_i$, which implies $(\zeta_i^e)^{p^k} = \zeta_i^{-1}$ where $e = n - v$.

**Lemma 3.2** *Using the notations above, define a mapping* $\sigma_i \colon R_i[z]/\langle z^{p^k} - 1\rangle \to R_i[x]/\langle x^{p^k} - \zeta_i\rangle$ *by*

$$\sigma_i(a(z)) = a\left(\zeta_i^e x\right), \quad \forall a(z) \in R_i[z]/\left\langle z^{p^k} - 1\right\rangle.$$

*Then* $\sigma_i$ *is a ring isomorphism from* $R_i[z]/\langle z^{p^k} - 1\rangle$ *onto* $R_i[x]/\langle x^{p^k} - \zeta_i\rangle$ *preserving Hamming weight.*

*Proof* It follows that $(\zeta_i^e x)^{p^k} - 1 = \zeta_i^{ep^k} x^{p^k} - 1 = \zeta_i^{-1}(x^{p^k} - \zeta_i)$. □

Recall that ideals of the ring $R_i[z]/\langle z^{p^k} - 1\rangle$ are in fact cyclic codes over the GR $R_i = \mathrm{GR}(p^2, m_i)$ of length $p^k$. This kind of cyclic codes have been researched in many literatures, for example Kiah et al. [5] and Sobhani and Esmaeili [7]. For purpose of application in this paper, we list some conclusions.

**Lemma 3.3** (cf. [7, Theorem 4.3]) *The number of ideals of* $R_i[z]/\langle z^{p^k}-1\rangle$, *where* $R_i=\mathrm{GR}(p^2, m_i)$, *is equal to*

$$N_{(p^2,m_i;k)}=4\left(\frac{p^{m_i p^{k-1}}-1}{p^{m_i}-1}\right)+\left(2(p-2)p^{k-1}+1\right)p^{m_i p^{k-1}}$$
$$+\left(p^{m_i}+3\right)\left(\frac{p^{m_i p^{k-1}}-1}{(p^{m_i}-1)^2}-\frac{p^{k-1}}{p^{m_i}-1}\right)$$
$$+2(p-2)p^{k-1}\left(\frac{p^{m_i p^{k-1}}-1}{p^{m_i}-1}\right)+p^{k-1}.$$

*Especially*, $N_{(p^2,m_i;k)}=1+2p+(2p-3)p^{m_i}$ *when* $k=1$.

**Lemma 3.4** ([7, Corollary 4.4]) *Let* $p\neq 2$, $\alpha=p-1$ *and* $\beta=p-2$. *Then all distinct cyclic codes* $\mathcal{L}_i$ *over the GR* $R_i$ *of length* $p^k$ *and their annihilating ideals* $\mathrm{Ann}(\mathcal{L}_i)=\{\alpha\in R_i[z]/\langle z^{p^k}-1\rangle \mid \alpha\beta=0,\ \forall\beta\in\mathcal{L}_i\}$ *are given by the following*:

| Cases | $\mathcal{L}_i$ | $\mathrm{Ann}(\mathcal{L}_i)$ |
|---|---|---|
| (1) | $\langle 0\rangle$ | $\langle 1\rangle$ |
| (2) | $\langle 1\rangle$ | $\langle 0\rangle$ |
| (3) | $\langle p\rangle$ | $\langle p\rangle$ |
| (4) | $\langle p(z-1)^s\rangle$ $(1\le s\le p^k-1)$ | $\langle p,\ (z-1)^{p^k-s}\rangle$ |
| (5) | $\langle (z-1)^s\rangle$ $(1\le s\le p^{k-1})$ | $\langle (z-1)^{p^k-s}+p(z-1)^{p^{k-1}-s}(-w(z))\rangle$ |
| (6) | $\langle (z-1)^s\rangle$ $(p^{k-1}+1\le s\le p^k-1)$ | $\langle (z-1)^{\alpha p^{k-1}}+p(-w(z)),\ p(z-1)^{p^k-s}\rangle$ |
| (7) | $\langle (z-1)^s+p(z-1)^{s-\alpha p^{k-1}}(-w(z))\rangle$ $(\alpha p^{k-1}\le s\le p^k-1)$ | $\langle (z-1)^{p^k-s}\rangle$ |
| (8) | $\langle (z-1)^s+p(z-1)^{s-\alpha p^{k-1}}(-w(z)$ $+(z-1)^{\nu}\widetilde{h}(z))\rangle$ $(\alpha p^{k-1}\le s\le p^{k-1}+\nu,\ \nu\ge 1)$ | $\langle (z-1)^{p^k-s}+p(z-1)^{p^{k-1}+\nu-s}(-\widetilde{h}(z))\rangle$ |
| (9) | $\langle (z-1)^s+p(z-1)^{s-\alpha p^{k-1}}(-w(z)$ $+(z-1)^{\nu}\widetilde{h}(z))\rangle$ $(p^{k-1}+\nu\le s\le p^k-1,$ $s>\alpha p^{k-1},\ \nu\ge 1)$ | $\langle (z-1)^{\alpha p^{k-1}-\nu}+p(-\widetilde{h}(z)),$ $p(z-1)^{p^k-s}\rangle$ |
| (10) | $\langle (z-1)^{\alpha p^{k-1}}+p(-w(z)$ $+(z-1)^{\nu}\widetilde{h}(z))\rangle$ $p^{k-1}+\nu<\alpha p^{k-1},\ \nu\ge 1)$ | $\langle (z-1)^{\alpha p^{k-1}-\nu}+p(-\widetilde{h}(z))\rangle$ |
| (11) | $\langle (z-1)^s+p(z-1)^{s-\alpha p^{k-1}}h(z)\rangle$ $(\alpha p^{k-1}<s<p^k-1,\ h_0\neq 0,\ 1)$ | $\langle (z-1)^{\alpha p^{k-1}}+p(1-h(z)),$ $p(z-1)^{p^k-s}\rangle$ |
| (12) | $\langle (z-1)^{\alpha p^{k-1}}+ph(z)\rangle$ $(h_0\neq 0,\ 1)$ | $\langle (z-1)^{\alpha p^{k-1}}+p(1-h(z))\rangle$ |
| (13) | $\langle (z-1)^s+p(z-1)^t h(z)\rangle$ $(p^k+t-s\neq p^{k-1},\ s\le p^{k-1},$ $h(z)\neq 0)$ | $\langle (z-1)^{p^k-s}+p(z-1)^{p^{k-1}-s}(-w(z)$ $+(z-1)^{\alpha p^{k-1}+t-s}(-h(z)))\rangle$ |

| Cases | $\mathcal{L}_i$ | $\mathrm{Ann}(\mathcal{L}_i)$ |
|---|---|---|
| (14) | $\langle (z-1)^s + p(z-1)^t h(z)\rangle$ $(p^k + t - s \neq p^{k-1},$ $p^{k-1} < s \leq \alpha p^{k-1} + t,$ $t > 0,\ h(z) \neq 0)$ | $\langle (z-1)^{\alpha p^{k-1}} + p(-w(z)$ $+ (z-1)^{\alpha p^{k-1}+t-s}(-h(z))),$ $p(z-1)^{p^k - s}\rangle$ |
| (15) | $\langle (z-1)^s + ph(z)\rangle$ $(p^{k-1} < s < \alpha p^{k-1},\ h(z) \neq 0)$ | $\langle p(-w(z) + (z-1)^{\alpha p^{k-1}-s}(-h(z)))$ $+ (z-1)^{\alpha p^{k-1}}\rangle$ |
| (16) | $\langle (z-1)^s + p(z-1)^t h(z)\rangle$ $(p^k + t - s \neq p^{k-1},\ s > \alpha p^{k-1} + t,$ $h(z) \neq 0,\ t > 0)$ | $\langle p(-h(z) + (z-1)^{s-t-\alpha p^{k-1}})$ $+ (z-1)^{s-t},\ p(z-1)^{p^k - s}\rangle$ |
| (17) | $\langle (z-1)^s + ph(z)\rangle$ $(s > \alpha p^{k-1},\ h(z) \neq 0)$ | $\langle (z-1)^s + p(-h(z) + (z-1)^{s-\alpha p^{k-1}})\rangle$ |
| (18) | $\langle (z-1)^s,\ p(z-1)^l\rangle$ $(1 \leq s \leq p^k - 1,$ $0 \leq l \leq \min\{s,\ p^{k-1}\})$ | $\langle (z-1)^{p^k - 1} + p(z-1)^{p^{k-1}-l}(-w(z)),$ $p(z-1)^{p^k - s}\rangle$ |
| (19) | $\langle p(z-1)^{s-\alpha p^{k-1}}(-w(z))$ $+(z-1)^s,\ p(z-1)^l\rangle$ $(\alpha p^{k-1} \leq s \leq p^k - 1,$ $s - \alpha p^{k-1} < l < s)$ | $\langle (z-1)^{p^k - l},\ p(z-1)^{p^k - s}\rangle$ |
| (20) | $\langle p(z-1)^{s-\alpha p^{k-1}}(-w(z) + \pi_i^{\nu}\widetilde{h}(z))$ $+ (z-1)^s,\ p(z-1)^l\rangle$ $(\alpha p^{k-1} < s \leq p^k - 1,\ \nu \geq 1,$ $s - \alpha p^{k-1} < l < \min\{s,\ p^{k-1} + \mu\})$ | $\langle (z-1)^{p^k - l} + p(z-1)^{p^{k-1}+\nu-l}(-\widetilde{h}(z)),$ $p(z-1)^{p^k - s}\rangle$ |
| (21) | $\langle p(-w(z) + (z-1)^{\nu}\widetilde{h}(z))$ $+(z-1)^{\alpha p^{k-1}},\ p(z-1)^l\rangle$ $(0 < l < \min\{\alpha p^{k-1},\ p^{k-1} + \nu\},$ $\nu \geq 1)$ | $\langle (z-1)^{p^k - l} + p(z-1)^{p^{k-1}+\nu-l}(-\widetilde{h}(z))\rangle$ |
| (22) | $\langle (z-1)^s + p(z-1)^{s-\alpha p^{k-1}}h(z),$ $p(z-1)^l\rangle$ $(\alpha p^{k-1} < s \leq p^k - 1,\ h_0 \neq 0,\ 1,$ $s - \alpha p^{k-1} < l < p^{k-1})$ | $\langle (z-1)^{p^k - l} + p(z-1)^{p^{k-1}-l}(1 - h(z)),$ $p(z-1)^{p^k - s}\rangle$ |
| (23) | $\langle (z-1)^{\alpha p^{k-1}} + ph(z),\ p(z-1)^l\rangle$ $(h_0 \neq 0,\ 1,\ 0 < l < p^{k-1})$ | $\langle (z-1)^{p^k - l} + p(z-1)^{p^{k-1}-l}(1 - h(z))\rangle$ |
| (24) | $\langle (z-1)^s + p(z-1)^t h(z),\ p(z-1)^l\rangle$ $(p^k + t - s \neq p^{k-1},\ 1 \leq s \leq \alpha p^{k-1} + t,$ $h(z) \neq 0,\ 0 < t < l < \min\{s,\ p^{k-1}\})$ | $\langle (z-1)^{p^k - l} + p(z-1)^{p^{k-1}-l}(-w(z)$ $+ (z-1)^{\alpha p^{k-1}+t-s}(-h(z))),$ $p(z-1)^{p^k - s}\rangle$ |
| (25) | $\langle (z-1)^s + ph(z),\ p(z-1)^l\rangle$ $(1 \leq s < \alpha p^{k-1},\ h(z) \neq 0,$ $0 < l < \min\{s,\ p^{k-1}\})$ | $\langle (z-1)^{p^k - l} + p(z-1)^{p^{k-1}-l}(-w(z)$ $+ (z-1)^{\alpha p^{k-1}+t-s}(-h(z)))\rangle$ |
| (26) | $\langle (z-1)^s + p(z-1)^t h(z),\ p(z-1)^l\rangle$ $(p^k + t - s \neq p^{k-1},\ h(z) \neq 0,\ t > 0$ $s > \alpha p^{k-1},\ 0 < t < l < p^k + t - s)$ | $\langle (z-1)^{p^k - l} + p(z-1)^{p^k+t-s-l}(-h(z)$ $+ (z-1)^{s-t-\alpha p^{k-1}}),\ p(z-1)^{p^k - s}\rangle$ |
| (27) | $\langle (z-1)^s + ph(z),\ p(z-1)^l\rangle$ $(s > \alpha p^{k-1},\ h(z) \neq 0,\ 0 < l < p^k - s)$ | $\langle (z-1)^{p^k - l} + p(z-1)^{p^k+t-s-l}(-h(z)$ $+ (z-1)^{s-\alpha p^{k-1}})\rangle$ |

Then by Theorem 3.1, Lemmas 3.2 and 3.3 we deduce the following corollary.

**Corollary 3.5** *Using the notations of Lemma 3.3, the number of all cyclic codes over* $\mathbb{Z}_{p^2}$ *of length* $p^k n$ *is equal to* $\prod_{i=1}^{r} N_{(p^2,m_i;k)}$.

*Example 3.6* We calculate the number of cyclic codes over $\mathbb{Z}_9$ of length 33. In this case, we have $p = 3,\ k = 1$ and $n = 11$.

Since $\{0, 1, 3, 9, 5, 4\}$ and $\{2, 6, 7, 10, 8\}$ are all distinct 3-cyclotomic cosets modulo 11, we have $y^{11} - 1 = f_1(y)f_2(y)f_3(y)$, where $f_1(y),\ f_2(y),\ f_3(y)$ are monic basic irreducible polynomials in $\mathbb{Z}_9[y]$ satisfying $m_1 = \deg(f_1(y)) = 1$ and $m_i = \deg(f_1(y)) = 5$ for $i = 2,\ 3$. By Corollary 3.5 and Lemma 3.3, the number of cyclic codes over $\mathbb{Z}_9$ of length 33 is equal to

$$\prod_{i=1}^{3} N_{(3^2,m_i;1)} = \prod_{i=1}^{3} \left(1 + 2p + (2p-3)p^{m_i}\right) = 16 \cdot 736^2 = 8,667,136.$$

For any ideal $C_i$ of the ring $R_i[x]/\langle x^{p^k} - \zeta_i\rangle$, the *annihilating ideal* of $C_i$ is defined as $\mathrm{Ann}(C_i) = \{\alpha \in R_i[x]/\langle x^{p^k} - \zeta_i\rangle \mid \alpha\beta = 0,\ \forall \beta \in C_i\}$. In the rest of this paper, we denote $w(z) = \sum_{j=0}^{p-2} \left[\frac{(-1)^{j+1}}{j+1}\right]_1 (z-1)^{jp^{k-1}}$, where $[a]_1$ denotes $a \pmod p$ (cf. [7]), and

$$\pi_i = \zeta_i^e x - 1 \in R_i[x]/\left\langle x^{p^k} - \zeta_i\right\rangle, \quad \text{where} \quad R_i = \mathbb{Z}_{p^2}[\zeta_i].$$

Now, by Lemmas 3.2 and 3.3, we can list all distinct $\zeta_i$-constacyclic codes over the GR $R_i$ of length $p^k$ by the following theorem.

**Theorem 3.7** *Let* $p \neq 2$, $\alpha = p-1$ *and* $\beta = p-2$. *Then all distinct* $\zeta_i$*-constacyclic codes* $C_i$ *over the GR* $R_i$ *of length* $p^k$ *and their annihilating ideals are given by the following*:

| Cases | $C_i$ | $\mathrm{Ann}(C_i)$ |
|---|---|---|
| (1) | $\langle 0\rangle$ | $\langle 1\rangle$ |
| (2) | $\langle 1\rangle$ | $\langle 0\rangle$ |
| (3) | $\langle p\rangle$ | $\langle p\rangle$ |
| (4) | $\langle p\pi_i^s\rangle\ (1 \le s \le p^k - 1)$ | $\langle p,\ \pi_i^{p^k-s}\rangle$ |
| (5) | $\langle \pi_i^s\rangle\ (1 \le s \le p^{k-1})$ | $\langle \pi_i^{p^k-s} + p\pi_i^{p^{k-1}-s}(-w(\zeta_i^e x))\rangle$ |
| (6) | $\langle \pi_i^s\rangle\ (p^{k-1}+1 \le s \le p^k - 1)$ | $\langle \pi_i^{\alpha p^{k-1}} + p(-w(\zeta_i^e x)),\ p\pi_i^{p^k-s}\rangle$ |
| (7) | $\langle \pi_i^s + p\pi_i^{s-\alpha p^{k-1}}(-w(\zeta_i^e x))\rangle$ $(\alpha p^{k-1} \le s \le p^k - 1)$ | $\langle \pi_i^{p^k-s}\rangle$ |
| (8) | $\langle \pi_i^s + p\pi_i^{s-\alpha p^{k-1}}(-w(\zeta_i^e x) + \pi_i^{\nu}\widetilde{h}(\zeta_i^e x))\rangle$ $(\alpha p^{k-1} \le s \le p^{k-1} + \nu,\ \nu \ge 1)$ | $\langle \pi_i^{p^k-s} + p\pi_i^{p^{k-1}+\nu-s}(-\widetilde{h}(\zeta_i^e x))\rangle$ |

| Cases | $C_i$ | $\mathrm{Ann}(C_i)$ |
|---|---|---|
| (9) | $\langle \pi_i^s + p\pi_i^{s-\alpha p^{k-1}}(-w(\zeta_i^e x) + \pi_i^{\nu}\widetilde{h}(\zeta_i^e x))\rangle$ $(p^{k-1} + \nu \le s \le p^k - 1,$ $s > \alpha p^{k-1},\ \nu \ge 1)$ | $\langle \pi_i^{\alpha p^{k-1}-\nu} + p(-\widetilde{h}(\zeta_i^e x)),\ p\pi_i^{p^k-s}\rangle$ |
| (10) | $\langle \pi_i^{\alpha p^{k-1}} + p(-w(\zeta_i^e x) + \pi_i^{\nu}\widetilde{h}(\zeta_i^e x))\rangle$ $p^{k-1} + \nu < \alpha p^{k-1},\ \nu \ge 1)$ | $\langle \pi_i^{\alpha p^{k-1}-\nu} + p(-\widetilde{h}(\zeta_i^e x))\rangle$ |
| (11) | $\langle \pi_i^s + p\pi_i^{s-\alpha p^{k-1}} h(\zeta_i^e x)\rangle$ $(\alpha p^{k-1} < s < p^k - 1,\ h_0 \ne 0, 1)$ | $\langle \pi_i^{\alpha p^{k-1}} + p(1 - h(\zeta_i^e x)),\ p\pi_i^{p^k-s}\rangle$ |
| (12) | $\langle \pi_i^{\alpha p^{k-1}} + ph(\zeta_i^e x)\rangle\ (h_0 \ne 0,\ 1)$ | $\langle \pi_i^{\alpha p^{k-1}} + p(1 - h(\zeta_i^e x))\rangle$ |
| (13) | $\langle \pi_i^s + p\pi_i^t h(\zeta_i^e x)\rangle$ $(p^k + t - s \ne p^{k-1},\ s \le p^{k-1},\ h(x) \ne 0)$ | $\langle \pi_i^{p^k-s} + p\pi_i^{p^{k-1}-s}(-w(\zeta_i^e x)$ $+ \pi_i^{\alpha p^{k-1}+t-s}(-h(\zeta_i^e x)))\rangle$ |
| (14) | $\langle \pi_i^s + p\pi_i^t h(\zeta_i^e x)\rangle$ $(p^k + t - s \ne p^{k-1},\ p^{k-1} < s \le \alpha p^{k-1} + t,$ $t > 0,\ h(x) \ne 0)$ | $\langle \pi_i^{\alpha p^{k-1}} + p(-w(\zeta_i^e x)$ $+ \pi_i^{\alpha p^{k-1}+t-s}(-h(\zeta_i^e x))),\ p\pi_i^{p^k-s}\rangle$ |
| (15) | $\langle \pi_i^s + ph(\zeta_i^e x)\rangle$ $(p^{k-1} < s < \alpha p^{k-1},\ h(x) \ne 0)$ | $\langle p(-w(\zeta_i^e x) + \pi_i^{\alpha p^{k-1}-s}(-h(\zeta_i^e x)))$ $+ \pi_i^{\alpha p^{k-1}}\rangle$ |
| (16) | $\langle \pi_i^s + p\pi_i^t h(\zeta_i^e x)\rangle$ $(p^k + t - s \ne p^{k-1},\ s > \alpha p^{k-1} + t,$ $h(x) \ne 0,\ t > 0)$ | $\langle \pi_i^{s-t} + p(-h(\zeta_i^e x) + \pi_i^{s-t-\alpha p^{k-1}}),$ $p\pi_i^{p^k-s}\rangle$ |
| (17) | $\langle \pi_i^s + ph(\zeta_i^e x)\rangle$ $(s > \alpha p^{k-1},\ h(x) \ne 0)$ | $\langle \pi_i^s + p(-h(\zeta_i^e x) + \pi_i^{s-\alpha p^{k-1}})\rangle$ |
| (18) | $\langle \pi_i^s,\ p\pi_i^l\rangle$ $(1 \le s \le p^k - 1,$ $0 \le l \le \min\{s,\ p^{k-1}\})$ | $\langle \pi_i^{p^k-1} + p\pi_i^{p^{k-1}-l}(-w(\zeta_i^e x)),$ $p\pi_i^{p^k-s}\rangle$ |
| (19) | $\langle \pi_i^s + p\pi_i^{s-\alpha p^{k-1}}(-w(\zeta_i^e x)),\ p\pi_i^l\rangle$ $(\alpha p^{k-1} \le s \le p^k - 1,\ s - \alpha p^{k-1} < l < s)$ | $\langle \pi_i^{p^k-l},\ p\pi_i^{p^k-s}\rangle$ |
| (20) | $\langle \pi_i^s + p\pi_i^{s-\alpha p^{k-1}}(-w(\zeta_i^e x) + \pi_i^{\nu}\widetilde{h}(\zeta_i^e x)),$ $p\pi_i^l\rangle$ $(\alpha p^{k-1} < s \le p^k - 1,\ \nu \ge 1,$ $s - \alpha p^{k-1} < l < \min\{s,\ p^{k-1} + \mu\})$ | $\langle \pi_i^{p^k-l} + p\pi_i^{p^{k-1}+\nu-l}(-\widetilde{h}(\zeta_i^e x)),$ $p\pi_i^{p^k-s}\rangle$ |
| (21) | $\langle \pi_i^{\alpha p^{k-1}} + p(-w(\zeta_i^e x) + \pi_i^{\nu}\widetilde{h}(\zeta_i^e x)),\ p\pi_i^l\rangle$ $(0 < l < \min\{\alpha p^{k-1},\ p^{k-1} + \nu\},\ \nu \ge 1)$ | $\langle \pi_i^{p^k-l} + p\pi_i^{p^{k-1}+\nu-l}(-\widetilde{h}(\zeta_i^e x))\rangle$ |
| (22) | $\langle \pi_i^s + p\pi_i^{s-\alpha p^{k-1}} h(\zeta_i^e x),\ p\pi_i^l\rangle$ $(\alpha p^{k-1} < s \le p^k - 1,\ h_0 \ne 0,\ 1,$ $s - \alpha p^{k-1} < l < p^{k-1})$ | $\langle \pi_i^{p^k-l} + p\pi_i^{p^{k-1}-l}(1 - h(\zeta_i^e x)),$ $p\pi_i^{p^k-s}\rangle$ |
| (23) | $\langle \pi_i^{\alpha p^{k-1}} + ph(\zeta_i^e x),\ p\pi_i^l\rangle$ $(h_0 \ne 0,\ 1,\ 0 < l < p^{k-1})$ | $\langle \pi_i^{p^k-l} + p\pi_i^{p^{k-1}-l}(1 - h(\zeta_i^e x))\rangle$ |
| (24) | $\langle \pi_i^s + p\pi_i^t h(\zeta_i^e x),\ p\pi_i^l\rangle$ $(p^k + t - s \ne p^{k-1},\ 1 \le s \le \alpha p^{k-1} + t,$ $h(x) \ne 0,\ 0 < t < l < \min\{s,\ p^{k-1}\})$ | $\langle \pi_i^{p^k-l} + p\pi_i^{p^{k-1}-l}(-w(\zeta_i^e x)$ $+ \pi_i^{\alpha p^{k-1}+t-s}(-h(\zeta_i^e x))),\ p\pi_i^{p^k-s}\rangle$ |

| Cases | $C_i$ | $\mathrm{Ann}(C_i)$ |
|---|---|---|
| (25) | $\langle \pi_i^s + ph(\zeta_i^e x),\ p\pi_i^l \rangle$ $(1 \leq s < \alpha p^{k-1},\ h(x) \neq 0,$ $0 < l < \min\{s,\ p^{k-1}\})$ | $\langle \pi_i^{p^k-l} + p\pi_i^{p^{k-1}-l}(-w(\zeta_i^e x)$ $+\pi_i^{\alpha p^{k-1}+t-s}(-h(\zeta_i^e x))) \rangle$ |
| (26) | $\langle \pi_i^s + p\pi_i^t h(\zeta_i^e x),\ p\pi_i^l \rangle$ $(p^k + t - s \neq p^{k-1},\ h(x) \neq 0,\ t > 0$ $s > \alpha p^{k-1},\ 0 < t < l < p^k + t - s)$ | $\langle \pi_i^{p^k-l} + p\pi_i^{p^k+t-s-l}(-h(\zeta_i^e x)$ $+\pi_i^{s-t-\alpha p^{k-1}}),\ p\pi_i^{p^k-s} \rangle$ |
| (27) | $\langle \pi_i^s + ph(\zeta_i^e x),\ p\pi_i^l \rangle$ $(s > \alpha p^{k-1},\ h(x) \neq 0,\ 0 < l < p^k - s)$ | $\langle \pi_i^{p^k-l} + p\pi_i^{p^k+t-s-l}(-h(\zeta_i^e x)$ $+\pi_i^{s-\alpha p^{k-1}}) \rangle$ |

Finally, by Theorems 3.1 and 3.7 we deduce the following corollary.

**Corollary 3.8** *Every cyclic code $\mathcal{C}$ over $\mathbb{Z}_{p^2}$ of length $p^k n$ can be constructed by the following two steps*:

(i) *For each $i = 1, \ldots, r$, choose a $\zeta_i$-constacyclic code $C_i$ over $R_i$ of length $p^k$ listed in Theorem 3.7.*

(ii) *Set $\mathcal{C} = \oplus_{i=1}^r \mathcal{C}_i$ with $\mathcal{C}_i = \mathcal{A}_i \Box_{\varphi_i} C_i$.*

*The number of codewords in $\mathcal{C}$ is equal to $|\mathcal{C}| = \prod_{i=1}^r |C_i|$ and the minimal Hamming distance of $\mathcal{C}$ satisfies $d_{\min}(\mathcal{C}) \leq \min\{d_{\min}(\mathcal{A}_i) d_{\min}(C_i) \mid i = 1, \ldots, r\}$, where $d_{\min}(\mathcal{A}_i)$ is the minimal $\mathbb{Z}_{p^2}$-Hamming weight of $\mathcal{A}_i$ and $d_{\min}(C_i)$ is the minimal $R_i$-Hamming weight of $C_i$. Moreover, a generator matrix of $\mathcal{C}$ is given by*

$$G_{\mathcal{C}} = \begin{pmatrix} G_{\mathcal{A}_1 \Box_{\varphi_1} C_1} \\ \cdots \\ G_{\mathcal{A}_r \Box_{\varphi_r} C_r} \end{pmatrix}.$$

Using the notations of Corollary 3.8(ii), $\mathcal{C} = \oplus_{i=1}^r \mathcal{C}_i$ with $\mathcal{C}_i = \mathcal{A}_i \Box_{\varphi_i} C_i$ is called the *canonical form decomposition* of the cyclic code $\mathcal{C}$ over $\mathbb{Z}_{p^2}$.

## 4 Dual codes of cyclic codes over $\mathbb{Z}_{p^2}$ of length $p^k n$

In this section, we give the dual code of each cyclic code over $\mathbb{Z}_{p^2}$ of length $N$ and investigate the self-duality of these codes.

As usual, we will identify $a = (a_0, a_1, \ldots, a_{N-1}) \in \mathbb{Z}_{p^2}^N$ with $a(x) = \sum_{j=0}^{N-1} a_j x^j \in \mathbb{Z}_{p^2}[x]/\langle x^N - 1 \rangle$. In this paper, we define

$$\mu(a(x)) = a\left(x^{-1}\right) = a_0 + \sum_{j=1}^{N-1} a_j x^{N-j}, \quad \forall a(x) \in \mathbb{Z}_{p^2}[x]/\left\langle x^N - 1 \right\rangle.$$

Then $\mu$ is a ring automorphism of $\mathbb{Z}_{p^2}[x]/\langle x^N - 1 \rangle$ satisfying $\mu^{-1} = \mu$ and $\mu(c) = c$ for all $c \in \mathbb{Z}_{p^2}$. The following lemma is well known.

**Lemma 4.1** *Let* $a, b \in \mathbb{Z}_{p^2}^N$. *Then* $[a, b] = 0$ *if* $a(x)\mu(b(x)) = 0$ *in the ring* $\mathbb{Z}_{p^2}[x]/\langle x^N - 1\rangle$.

Using the notations of Sect. 3, we have $\mathbb{Z}_{p^2}[x]/\langle x^N - 1\rangle = \mathcal{A}[x]/\langle x^{p^k} - y\rangle$ under the substitution $y = x^{p^k}$, where $\mathcal{A} = \mathbb{Z}_{p^2}[y]/\langle y^n - 1\rangle$. Hence

$$\mu(y) = \left(x^{-1}\right)^{p^k} = y^{-1} \quad \text{in} \quad \mathcal{A}[x]/\left\langle x^{p^k} - y\right\rangle.$$

Therefore, the restriction of $\mu$ to $\mathcal{A}$ is given by

$$\mu(f(y)) = f\left(y^{-1}\right) \quad (\forall f(y) \in \mathcal{A}),$$

which is a ring automorphism of $\mathcal{A}$. For notations simplicity, we still denote this restriction by $\mu$. From this and by Notation 2.1, we deduce

$$\mu\left(\varepsilon_i(y)\right) = a_i\left(y^{-1}\right)F_i\left(y^{-1}\right) = 1 - b_i\left(y^{-1}\right)f_i\left(y^{-1}\right) \text{ in } \mathcal{A}. \tag{3}$$

Let $f(y) = \sum_{j=0}^m c_j y^j$ be a polynomial in $\mathbb{Z}_{p^2}[y]$ of degree $m \geq 1$. Recall that the *reciprocal polynomial* of $f(y)$ is defined by $\widetilde{f}(y) = y^m f\left(\frac{1}{y}\right) = \sum_{j=0}^m c_j y^{m-j}$. Especially, $f(y)$ is said to be *self-reciprocal* if $\widetilde{f}(y) = \delta f(y)$ for some invertible element $\delta$ in $\mathbb{Z}_{p^2}$, i.e., $\delta \in \mathbb{Z}_{p^2}^\times$. Then by Eq. (1) in Sect. 2, we have

$$y^n - 1 = -\widetilde{f_1}(y), \widetilde{f_2}(y), \ldots, \widetilde{f_r}(y).$$

Since $f_1(y), f_2(y), \ldots, f_r(y)$ are pairwise coprime monic basic polynomials in $\mathbb{Z}_{p^2}[y]$, for each $1 \leq i \leq r$ there is a unique integer $i'$, $1 \leq i' \leq r$, such that $\widetilde{f_i}(y) = \delta_i f_{i'}(y)$ where $\delta_i \in \mathbb{Z}_{p^2}^\times$. Then by (3) and $y^n = 1$ in $\mathcal{A}$, we have

$$\begin{aligned}
\mu\left(\varepsilon_i(y)\right) &= 1 - y^{n-\deg(b_i(y))-m_i}\left(y^{\deg(b_i(y))}b_i\left(y^{-1}\right)\right)\left(y^{m_i}f_i\left(y^{-1}\right)\right) \\
&= 1 - y^{n-\deg(b_i(y))-m_i}\widetilde{b_i}(y)\widetilde{f_i}(y) \\
&= 1 - h_i(y)f_{i'}(y),
\end{aligned}$$

where $h_i(y) = \delta_i y^{n-\deg(b_i(y))-m_i}\widetilde{b_i}(y) \in \mathcal{A}$. Similarly, by (3) it follows that $\mu(\varepsilon_i(y)) = g_i(y)F_{i'}(y)$ for some $g_i(y) \in \mathcal{A}$. Then from these and by Eq. (2) we deduce that $\mu(\varepsilon_i(y)) = \varepsilon_{i'}(y)$.

As stated above, we see that for each $1 \leq i \leq r$ there is a unique integer $i'$, $1 \leq i' \leq r$, such that $\mu(\varepsilon_i(y)) = \varepsilon_{i'}(y)$. We still use $\mu$ to denote this map $i \mapsto i'$; i.e., $\mu(\varepsilon_i(y)) = \varepsilon_{\mu(i)}(y)$. Whether $\mu$ denotes the automorphism of $\mathcal{A}$ or this map on the set $\{1, \ldots, r\}$ is determined by context. The next lemma shows the compatibility of the two uses of $\mu$.

**Lemma 4.2** *With the notations above, the following hold.*

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

(ii) *After a rearrangement of* $\varepsilon_1(y), \ldots, \varepsilon_r(y)$ *there are integers* $\lambda$, $\rho$ *such that* $\mu(i) = i$ *for all* $i = 1, \ldots, \lambda$ *and* $\mu(\lambda + j) = \lambda + \rho + j$ *for all* $j = 1, \ldots, \rho$, *where* $\lambda \geq 1$, $\rho \geq 0$ *and* $\lambda + 2\rho = r$.

(iii) *For each integer* $i$, $1 \leq i \leq r$, *there is a unique invertible element* $\delta_i$ *of* $\mathbb{Z}_{p^2}$ *such that* $\widetilde{f_i}(y) = \delta_i f_{\mu(i)}(y)$.

(iv) *For any integer* $i$, $1 \leq i \leq r$, $\mu(\varepsilon_i(y)) = \varepsilon_{\mu(i)}(y)$ *in the ring* $\mathcal{A}$, *and* $\mu(\mathcal{A}_i) = \mathcal{A}_{\mu(i)}$. *Then* $\mu$ *induces a ring isomorphism from* $\mathcal{A}_i$ *onto* $\mathcal{A}_{\mu(i)}$.

*Proof* (i)–(iii) follow from the definition of the map $\mu$, and (iv) follows from that $\mathcal{A}_i = \varepsilon_i(y)\mathcal{A}$ immediately. □

**Lemma 4.3** *Using the notations above, the following hold for any* $1 \leq i \leq r$.

(i) $\mu$ *induces a ring isomorphism* $\varphi_i^{-1}\mu\varphi_i$ *from* $R_i$ *onto* $R_{\mu(i)}$. *We still denote this isomorphism by* $\mu$ *for notations simplicity. Then the following diagram commutes*

$$\begin{array}{ccc} R_i = \mathbb{Z}_{p^2}[y]/\langle f_i(y)\rangle & \xrightarrow{\mu} & R_{\mu(i)} = \mathbb{Z}_{p^2}[y]/\left\langle f_{\mu(i)}(y)\right\rangle \\ \varphi_i \downarrow & & \downarrow \varphi_i \\ \mathcal{A}_i & \xrightarrow{\mu} & \mathcal{A}_{\mu(i)}. \end{array}$$

*Specifically,* $\mu(a(y)) = a(y^{-1}) \in R_{\mu(i)}$ *for any* $a(y) \in R_i$.

(ii) *Using the notations in* (i), $\mu(\zeta_i) = \zeta_{\mu(i)}^{-1}$ *and* $\mu$ *induces a ring isomorphism from* $R_i[x]/\langle x^{p^k} - \zeta_i\rangle$ *onto* $R_{\mu(i)}[x]/\langle x^{p^k} - \zeta_{\mu(i)}\rangle$ *given by*

$$\alpha(x) = \sum_{j=0}^{p^k-1} \alpha_j x^j \mapsto \widehat{\alpha}\left(x^{-1}\right) := \mu(\alpha_0) + \zeta_{\mu(i)}^{-1} \sum_{j=1}^{p^k-1} \mu\left(\alpha_j\right) x^{p^k-j},$$

*where* $\widehat{\alpha}(x) = \sum_{j=0}^{p^k-1} \mu(\alpha_j)x^j$, $\forall \alpha_0, \alpha_1, \ldots, \alpha_{p^k-1} \in R_i$.

*Proof* (i) It follows from Lemma 2.2(iii) and Lemma 4.2(iii) and (iv).

(ii) From $\zeta_i = y + \langle f_i(y)\rangle \in R_i$ and $\zeta_{\mu(i)} = y + \langle f_{\mu(i)}(y)\rangle \in R_{\mu(i)}$, by (i) we deduce that $\mu(\zeta_i) = \zeta_{\mu(i)}^{-1} \in R_{\mu(i)}$. Since $x$ and $\zeta_{\mu(i)}$ are invertible elements of $R_{\mu(i)}[x]/\langle x^{p^k} - \zeta_{\mu(i)}\rangle$, from $(x^{-1})^{p^k} - \zeta_{\mu(i)}^{-1} = -x^{-p^k}\zeta_{\mu(i)}^{-1}(x^{p^k} - \zeta_{\mu(i)})$ we deduce that $\mu$ induces a ring isomorphism from $R_i[x]/\langle x^{p^k} - \zeta_i\rangle$ onto $R_{\mu(i)}[x]/\langle x^{p^k} - \zeta_{\mu(i)}\rangle$ given by $\alpha(x) = \sum_{j=0}^{p^k-1} \alpha_j x^j \mapsto \mu(\alpha(x)) = \widehat{\alpha}(x^{-1}) = \sum_{j=0}^{p^k-1} \mu(\alpha_j)x^{-j}$, $\forall \alpha_0, \ldots, \alpha_{2^k-1} \in R_i$. Finally, by $x^{p^k} = \zeta_{\mu(i)}$ in $R_{\mu(i)}[x]/\langle x^{p^k} - \zeta_{\mu(i)}\rangle$ it follows that $\widehat{\alpha}(x^{-1}) = \mu(\alpha_0) + \zeta_{\mu(i)}^{-1} \sum_{j=1}^{p^k-1} \mu(\alpha_j)x^{p^k-j}$ as required. □

**Corollary 4.4** *For each integer* $i$, $1 \leq i \leq r$, *denote* $\pi_i = \zeta_i^e x - 1 \in R_i[x]/\langle x^{p^k} - \zeta_i\rangle$, *where* $R_i = \mathbb{Z}_{p^2}[\zeta_i]$. *Then* $\mu(\pi_i^l) = (-1)^l \zeta_{\mu(i)}^{-el} x^{-l} \pi_{\mu(i)}^l \in R_{\mu(i)}[x]/\langle x^{p^k} - \zeta_{\mu(i)}\rangle$, *for any integer* $l$, $1 \leq l \leq p^k - 1$.

*Proof* By the proof of Lemma 4.3(ii), we have $\mu(\pi_i^l) = (\mu(\zeta_i^e x - 1))^l = ((\zeta_{\mu(i)}^{-1})^e x^{-1} - 1)^l = (-1)^l \zeta_{\mu(i)}^{-el} x^{-l} (\zeta_{\mu(i)}^e x - 1)^l = (-1)^l \zeta_{\mu(i)}^{-el} x^{-l} \pi_{\mu(i)}^l$. □

**Lemma 4.5** *Let* $a(x) = \sum_{i=1}^r a_i(x)$, $b(x) = \sum_{i=1}^r b_i(x) \in \mathcal{A}[x]/\langle x^{p^k} - y\rangle$, *with* $a_i(x), b_i(x) \in \mathcal{A}_i[x]/\langle x^{p^k} - y\rangle$. *Then* $a(x)\mu(b(x)) = \sum_{i=1}^r a_i(x)\mu(b_{\mu(i)}(x))$.

*Proof* By Lemma 4.2 we have $\mu(b_{\mu(i)}(x)) \in \mu(\mathcal{A}_{\mu(i)}[x]/\langle x^{p^k} - y\rangle)$ and $\mu(\mathcal{A}_{\mu(i)}[x]/\langle x^{p^k} - y\rangle) = \mathcal{A}_i[x]/\langle x^{p^k} - y\rangle$. Hence $a_i(x)\mu(b_{\mu(i)}(x)) \in \mathcal{A}_i[x]/\langle x^{p^k} - y\rangle$ for all $i$. If $j \neq \mu(i)$, then $i \neq \mu(j)$, which implies $a_i(x)\mu(b_j(x)) \in (\mathcal{A}_i[x]/\langle x^{p^k} - y\rangle)(\mathcal{A}_{\mu(j)}[x]/\langle x^{p^k} - y\rangle) = \{0\}$ by Lemma 2.2(ii). Therefore, $a(x)\mu(b(x)) = \sum_{i=1}^r \sum_{j=1}^r a_i(x)\mu(b_j(x)) = \sum_{i=1}^r a_i(x)\mu(b_{\mu(i)}(x))$. □

Now, we can determine the dual code of each cyclic code over $\mathbb{Z}_{p^2}$.

**Theorem 4.6** *Let* $\mathcal{C}$ *be a cyclic code over* $\mathbb{Z}_{p^2}$ *of length* $N$ *with concatenated structure* $\mathcal{C} = \oplus_{i=1}^r (\mathcal{A}_i \Box_{\varphi_i} C_i)$, *where* $C_i$ *is an ideal of the ring* $R_i[x]/\langle x^{p^k} - \zeta_i\rangle$ *for all* $i = 1, \ldots, r$. *Using the notations of Theorem 3.7 and Lemma 4.3*(ii), *the dual code* $\mathcal{C}^\perp$ *is given by*

$$\mathcal{C}^\perp = \oplus_{i=1}^r \left(\mathcal{A}_{\mu(i)} \Box_{\varphi_{\mu(i)}} D_{\mu(i)}\right),$$

*where* $D_{\mu(i)}$ *is an ideal of the ring* $R_{\mu(i)}[x]/\langle x^{p^k} - \zeta_{\mu(i)}\rangle$ *given by one of the following cases* $(1 \leq i \leq r)$:

| Cases | $C_i$ | $D_{\mu(i)}$ |
|---|---|---|
| (1) | $\langle 0\rangle$ | $\langle 1\rangle$ |
| (2) | $\langle 1\rangle$ | $\langle 0\rangle$ |
| (3) | $\langle p\rangle$ | $\langle p\rangle$ |
| (4) | $\langle p\pi_i^s\rangle$ $(1 \leq s \leq p^k - 1)$ | $\langle p, \pi_{\mu(i)}^{p^k-s}\rangle$ |
| (5) | $\langle \pi_i^s\rangle$ $(1 \leq s \leq p^{k-1})$ | $\langle \pi_{\mu(i)}^{p^k-s} + p\pi_{\mu(i)}^{p^{k-1}-s}(-\widehat{w}(\zeta_{\mu(i)}^{-e}x^{-1}))\omega\rangle$ <br> $\omega = (-1)^{p^{k-1}-p^k}\zeta_{\mu(i)}^{e(p^k-p^{k-1})}x^{p^k-p^{k-1}}$ |
| (6) | $\langle \pi_i^s\rangle$ $(p^{k-1}+1 \leq s \leq p^k - 1)$ | $\langle \pi_{\mu(i)}^{\alpha p^{k-1}} + p(-\widehat{w}(\zeta_{\mu(i)}^{-e}x^{-1}))\omega,\ p\pi_{\mu(i)}^{p^k-s}\rangle$ <br> $\omega = (-1)^{-\alpha p^{k-1}}\zeta_{\mu(i)}^{e\alpha p^{k-1}}x^{\alpha p^{k-1}}$ |
| (7) | $\langle \pi_i^s + p\pi_i^{s-\alpha p^{k-1}}(-w(\zeta_i^e x))\rangle$ <br> $(\alpha p^{k-1} \leq s \leq p^k - 1)$ | $\langle \pi_{\mu(i)}^{p^k-s}\rangle$ |
| (8) | $\langle \pi_i^s + p\pi_i^{s-\alpha p^{k-1}}(-w(\zeta_i^e x) + \pi_i^\nu \widetilde{h}(\zeta_i^e x))\rangle$ <br> $(\alpha p^{k-1} \leq s \leq p^{k-1} + \nu,\ \nu \geq 1)$ | $\langle \pi_{\mu(i)}^{p^k-s} + p\pi_{\mu(i)}^{p^{k-1}+\nu-s}(-\widehat{\widetilde{h}}(\zeta_{\mu(i)}^{-e}x^{-1}))\omega\rangle$ <br> $\omega = (-1)^{p^{k-1}+\nu-p^k}\zeta_{\mu(i)}^{e(p^k-p^{k-1}-\nu)}$ <br> $\cdot x^{p^k-p^{k-1}-\nu}$ |

| Cases | $C_i$ | $D_{\mu(i)}$ |
|---|---|---|
| (9) | $\langle \pi_i^s + p\pi_i^{s-\alpha p^{k-1}}(-w(\zeta_i^e x)+\pi_i^{\nu}\widetilde{h}(\zeta_i^e x))\rangle$<br>$(p^{k-1}+\nu \le s \le p^k-1,$<br>$s > \alpha p^{k-1},\ \nu \ge 1)$ | $\langle \pi_{\mu(i)}^{\alpha p^{k-1}-\nu} + p(-\widehat{\widetilde{h}}(\zeta_{\mu(i)}^{-e}x^{-1}))\omega,\ p\pi_{\mu(i)}^{p^k-s}\rangle$<br>$\omega = (-1)^{\nu-\alpha p^{k-1}}\zeta_{\mu(i)}^{e(\alpha p^{k-1}-\nu)}x^{\alpha p^{k-1}-\nu}$ |
| (10) | $\langle \pi_i^{\alpha p^{k-1}} + p(-w(\zeta_i^e x)+\pi_i^{\nu}\widetilde{h}(\zeta_i^e x))\rangle$<br>$p^{k-1}+\nu < \alpha p^{k-1},\ \nu \ge 1)$ | $\langle \pi_{\mu(i)}^{\alpha p^{k-1}-\nu} + p(-\widehat{\widetilde{h}}(\zeta_{\mu(i)}^{-e}x^{-1}))\omega\rangle$<br>$\omega = (-1)^{\nu-\alpha p^{k-1}}\zeta_{\mu(i)}^{e(\alpha p^{k-1}-\nu)}x^{\alpha p^{k-1}-\nu}$ |
| (11) | $\langle \pi_i^s + p\pi_i^{s-\alpha p^{k-1}}h(\zeta_i^e x)\rangle$<br>$(\alpha p^{k-1} < s < p^k-1,\ h_0 \ne 0,\ 1)$ | $\langle \pi_{\mu(i)}^{\alpha p^{k-1}} + p(1-\widehat{h}(\zeta_{\mu(i)}^{-e}x^{-1}))\omega,\ p\pi_{\mu(i)}^{p^k-s}\rangle$<br>$\omega = (-1)^{-\alpha p^{k-1}}\zeta_{\mu(i)}^{e\alpha p^{k-1}}x^{\alpha p^{k-1}}$ |
| (12) | $\langle \pi_i^{\alpha p^{k-1}} + ph(\zeta_i^e x)\rangle\ (h_0 \ne 0,\ 1)$ | $\langle \pi_{\mu(i)}^{\alpha p^{k-1}} + p(1-\widehat{h}(\zeta_{\mu(i)}^{-e}x^{-1}))\omega\rangle$<br>$\omega = (-1)^{-\alpha p^{k-1}}\zeta_{\mu(i)}^{e\alpha p^{k-1}}x^{\alpha p^{k-1}}$ |
| (13) | $\langle \pi_i^s + p\pi_i^t h(\zeta_i^e x)\rangle$<br>$(p^k+t-s \ne p^{k-1},\ s \le p^{k-1},$<br>$h(x) \ne 0)$ | $\langle \pi_{\mu(i)}^{p^k-s} + p\pi_{\mu(i)}^{p^{k-1}-s}(-\widehat{w}(\zeta_{\mu(i)}^{-e}x^{-1})$<br>$+\pi_{\mu(i)}^{\alpha p^{k-1}+t-s}(-\widehat{h}(\zeta_{\mu(i)}^{-e}x^{-1}))\omega_1)\omega_2\rangle$<br>$\omega_1 = (-1)^{\alpha p^{k-1}+t-s}\zeta_{\mu(i)}^{e(s-\alpha p^{k-1}-t)}$<br>$\cdot x^{s-\alpha p^{k-1}-t}$<br>$\omega_2 = (-1)^{p^{p-1}-p^k}\zeta_{\mu(i)}^{e(p^k-p^{k-1})}x^{p^k-p^{k-1}}$ |
| (14) | $\langle \pi_i^s + p\pi_i^t h(\zeta_i^e x)\rangle$<br>$(p^k+t-s \ne p^{k-1},$<br>$p^{k-1} < s \le \alpha p^{k-1}+t,$<br>$t > 0,\ h(x) \ne 0)$ | $\langle \pi_{\mu(i)}^{\alpha p^{k-1}} + p(-\widehat{w}(\zeta_{\mu(i)}^{-e}x^{-1})$<br>$+\pi_{\mu(i)}^{\alpha p^{k-1}+t-s}(-\widehat{h}(\zeta_{\mu(i)}^{-e}x^{-1}))\omega_1)\omega_2,\ p\pi_{\mu(i)}^{p^k-s}\rangle$<br>$\omega_1 = (-1)^{\alpha p^{k-1}+t-s}\zeta_{\mu(i)}^{e(s-\alpha p^{k-1}-t)}$<br>$\cdot x^{s-\alpha p^{k-1}-t}$<br>$\omega_2 = (-1)^{-\alpha p^{k-1}}\zeta_{\mu(i)}^{e\alpha p^{k-1}}x^{\alpha p^{k-1}}$ |
| (15) | $\langle \pi_i^s + ph(\zeta_i^e x)\rangle$<br>$(p^{k-1} < s < \alpha p^{k-1},\ h(x) \ne 0)$ | $\langle \pi_{\mu(i)}^{\alpha p^{k-1}} + p(-\widehat{w}(\zeta_{\mu(i)}^{-e}x^{-1})$<br>$+\pi_{\mu(i)}^{\alpha p^{k-1}-s}(-\widehat{h}(\zeta_{\mu(i)}^{-e}x^{-1}))\omega_1)\omega_2\rangle$<br>$\omega_1 = (-1)^{\alpha p^{k-1}-s}\zeta_{\mu(i)}^{e(s-\alpha p^{k-1})}x^{s-\alpha p^{k-1}}$<br>$\omega_2 = (-1)^{-\alpha p^{k-1}}\zeta_{\mu(i)}^{e\alpha p^{k-1}}x^{\alpha p^{k-1}}$ |
| (16) | $\langle \pi_i^s + p\pi_i^t h(\zeta_i^e x)\rangle$<br>$(p^k+t-s \ne p^{k-1},$<br>$s > \alpha p^{k-1}+t,$<br>$h(x) \ne 0,\ t > 0)$ | $\langle p(-\widehat{h}(\zeta_{\mu(i)}^{-e}x^{-1}) + \pi_{\mu(i)}^{s-t-\alpha p^{k-1}}\omega_1)\omega_2$<br>$+\pi_{\mu(i)}^{s-t},\ p\pi_{\mu(i)}^{p^k-s}\rangle$<br>$\omega_1 = (-1)^{s-t-\alpha p^{k-1}}\zeta_{\mu(i)}^{e(\alpha p^{k-1}+t-s)}$<br>$\cdot x^{\alpha p^{k-1}+t-s}$<br>$\omega_2 = (-1)^{t-s}\zeta_{\mu(i)}^{e(s-t)}x^{s-t}$ |
| (17) | $\langle \pi_i^s + ph(\zeta_i^e x)\rangle$<br>$(s > \alpha p^{k-1},\ h(x) \ne 0)$ | $\langle p(-\widehat{h}(\zeta_{\mu(i)}^{-e}x^{-1}) + \pi_{\mu(i)}^{s-\alpha p^{k-1}}\omega_1)\omega_2$<br>$+\pi_{\mu(i)}^{s}\rangle$<br>$\omega_1 = (-1)^{s-\alpha p^{k-1}}\zeta_{\mu(i)}^{e(\alpha p^{k-1}-s)}x^{\alpha p^{k-1}-s}$<br>$\omega_2 = (-1)^{-s}\zeta_{\mu(i)}^{es}x^{s}$ |

| Cases | $C_i$ | $D_{\mu(i)}$ |
|---|---|---|
| (18) | $\langle \pi_i^s,\ p\pi_i^l \rangle$ $(1 \le s \le p^k - 1,$ $0 \le l \le \min\{s,\ p^{k-1}\})$ | $\langle \pi_{\mu(i)}^{p^k-1} + p\pi_{\mu(i)}^{p^{k-1}-l}(-\widehat{w}(\zeta_{\mu(i)}^{-e}x^{-1})),$ $p\pi_{\mu(i)}^{p^k-s} \rangle$ $\omega = (-1)^{p^{p-1}-p^k-l+1}\zeta_{\mu(i)}^{e(p^k-p^{k-1}+l-1)}$ $\cdot x^{p^k-p^{k-1}+l-1}$ |
| (19) | $\langle \pi_i^s + p\pi_i^{s-\alpha p^{k-1}}(-w(\zeta_i^e x)),\ p\pi_i^l \rangle$ $(\alpha p^{k-1} \le s \le p^k - 1,$ $s - \alpha p^{k-1} < l < s)$ | $\langle \pi_{\mu(i)}^{p^k-l},\ p\pi_{\mu(i)}^{p^k-s} \rangle$ |
| (20) | $\langle p\pi_i^{s-\alpha p^{k-1}}(-w(\zeta_i^e x) + \pi_i^\nu \widetilde{h}(\zeta_i^e x))$ $+\pi_i^s,\ p\pi_i^l \rangle$ $(\alpha p^{k-1} < s \le p^k - 1,\ \nu \ge 1,$ $s - \alpha p^{k-1} < l < \min\{s,\ p^{k-1} + \mu\})$ | $\langle p\pi_{\mu(i)}^{p^{k-1}+\nu-l}(-\widehat{\widetilde{h}}(\zeta_{\mu(i)}^{-e}x^{-1}))\omega$ $+\pi_{\mu(i)}^{p^k-l},\ p\pi_{\mu(i)}^{p^k-s} \rangle$ $\omega = (-1)^{p^{k-1}+\nu-p^k}\zeta_{\mu(i)}^{-e(p^k-p^{k-1}-\nu)}$ $\cdot x^{p^k-p^{k-1}-\nu}$ |
| (21) | $\langle \pi_i^{\alpha p^{k-1}} + p(-w(\zeta_i^e x) + \pi_i^\nu \widetilde{h}(\zeta_i^e x)),$ $p\pi_i^l \rangle$ $(0 < l < \min\{\alpha p^{k-1},\ p^{k-1} + \nu\},$ $\nu \ge 1)$ | $\langle \pi_{\mu(i)}^{p^k-l} + p\pi_{\mu(i)}^{p^{k-1}+\nu-l}(-\widehat{\widetilde{h}}(\zeta_{\mu(i)}^{-e}x^{-1}))\omega \rangle$ $\omega = (-1)^{p^{k-1}+\nu-p^k}\zeta_{\mu(i)}^{-e(p^k-p^{k-1}-\nu)}$ $\cdot x^{p^k-p^{k-1}-\nu}$ |
| (22) | $\langle \pi_i^s + p\pi_i^{s-\alpha p^{k-1}}h(\zeta_i^e x),\ p\pi_i^l \rangle$ $(\alpha p^{k-1} < s \le p^k - 1,\ h_0 \ne 0,\ 1,$ $s - \alpha p^{k-1} < l < p^{k-1})$ | $\langle \pi_{\mu(i)}^{p^k-l} + p\pi_{\mu(i)}^{p^{k-1}-l}(1 - \widehat{h}(\zeta_{\mu(i)}^{-e}x^{-1}))\omega,$ $p\pi_{\mu(i)}^{p^k-s} \rangle$ $\omega = (-1)^{p^{k-1}-p^k}\zeta_{\mu(i)}^{-e(p^k-p^{k-1})}x^{p^k-p^{k-1}}$ |
| (23) | $\langle \pi_i^{\alpha p^{k-1}} + ph(x),\ p\pi_i^l \rangle$ $(h_0 \ne 0,\ 1,\ 0 < l < p^{k-1})$ | $\langle \pi_{\mu(i)}^{p^k-l} + p\pi_{\mu(i)}^{p^{k-1}-l}(1 - \widehat{h}(\zeta_{\mu(i)}^{-e}x^{-1}))\omega \rangle$ $\omega = (-1)^{p^{k-1}-p^k}\zeta_{\mu(i)}^{-e(p^k-p^{k-1})}x^{p^k-p^{k-1}}$ |
| (24) | $\langle \pi_i^s + p\pi_i^t h(\zeta_i^e x),\ p\pi_i^l \rangle$ $(p^k + t - s \ne p^{k-1},\ 1 \le s \le \alpha p^{k-1} + t,$ $h(x) \ne 0,\ 0 < t < l < \min\{s,\ p^{k-1}\})$ | $\langle \pi_{\mu(i)}^{p^k-l} + p\pi_{\mu(i)}^{p^{k-1}-l}(-\widehat{w}(\zeta_{\mu(i)}^{-e}x^{-1})$ $+\pi_{\mu(i)}^{\alpha p^{k-1}+t-s}(-\widehat{h}(\zeta_{\mu(i)}^{-e}x^{-1}))\omega_1)\omega_2,$ $p\pi_{\mu(i)}^{p^k-s} \rangle$ $\omega_1 = (-1)^{\alpha p^{k-1}+t-s}\zeta_{\mu(i)}^{-e(\alpha p^{k-1}+t-s)}$ $\cdot x^{s-t-\alpha p^{k-1}}$ $\omega_2(-1)^{p^{k-1}-p^k}\zeta_{\mu(i)}^{-e(p^k-p^{k-1})}x^{p^k-p^{k-1}}$ |
| (25) | $\langle \pi_i^s + ph(\zeta_i^e x),\ p\pi_i^l \rangle$ $(1 \le s < \alpha p^{k-1},\ h(x) \ne 0,$ $0 < l < \min\{s,\ p^{k-1}\})$ | $\langle \pi_{\mu(i)}^{p^k-l} + p\pi_{\mu(i)}^{p^{k-1}-l}(-\widehat{w}(\zeta_{\mu(i)}^{-e}x^{-1})$ $+\pi_{\mu(i)}^{\alpha p^{k-1}+t-s}(-\widehat{h}(\zeta_{\mu(i)}^{-e}x^{-1}))\omega_1)\omega_2 \rangle$ $\omega_1 = (-1)^{\alpha p^{k-1}+t-s}\zeta_{\mu(i)}^{-e(\alpha p^{k-1}+t-s)}$ $\cdot x^{s-t-\alpha p^{k-1}}$ $\omega_2(-1)^{p^{k-1}-p^k}\zeta_{\mu(i)}^{-e(p^k-p^{k-1})}x^{p^k-p^{k-1}}$ |
| (26) | $\langle \pi_i^s + p\pi_i^t h(\zeta_i^e x),\ p\pi_i^l \rangle$ $(p^k + t - s \ne p^{k-1},\ h(x) \ne 0,\ t > 0$ | $\langle \pi_{\mu(i)}^{p^k-l} + p\pi_{\mu(i)}^{p^k+t-s-l}(-\widehat{h}(\zeta_{\mu(i)}^{-e}x^{-1})$ $+\pi_{\mu(i)}^{s-t-\alpha p^{k-1}}\omega_1)\omega_2,\ p\pi_{\mu(i)}^{p^k-s} \rangle$ |

| Cases | $C_i$ | $D_{\mu(i)}$ |
|---|---|---|
| | $s > \alpha p^{k-1},\ 0 < t < l < p^k + t - s)$ | $\omega_1 = (-1)^{s-t-\alpha p^{k-1}} \zeta_{\mu(i)}^{-e(s-t-\alpha p^{k-1})} \cdot x^{\alpha p^{k-1}+t-s}$ <br> $\omega_2 = (-1)^{t-s} \zeta_{\mu(i)}^{e(s-t)} x^{s-t}$ |
| (27) | $\langle \pi_i^s + ph(\zeta_i^e x),\ p\pi_i^l \rangle$ <br> $(s > \alpha p^{k-1},\ h(x) \neq 0,\ 0 < l < p^k - s)$ | $\langle \pi_{\mu(i)}^{p^k-l} + p\pi_{\mu(i)}^{p^k+t-s-l}(-\widehat{h}(\zeta_{\mu(i)}^{-e} x^{-1})$ <br> $+\pi_{\mu(i)}^{s-\alpha p^{k-1}} \omega_1)\omega_2 \rangle$ <br> $\omega_1 = (-1)^{s-\alpha p^{k-1}} \zeta_{\mu(i)}^{e(\alpha p^{k-1}-s)} x^{\alpha p^{k-1}-s}$ <br> $\omega_2 = (-1)^{t-s} \zeta_{\mu(i)}^{e(s-t)} x^{s-t}$ |

*Proof* For any integer $i,\ 1 \le i \le r$, let $D_{\mu(i)} = \mu(\mathrm{Ann}(C_i))$. Then $D_{\mu(i)}$ is an ideal of the ring $R_{\mu(i)}[x]/\langle x^{p^k} - \zeta_{\mu(i)} \rangle$. Set $\mathcal{D} = \oplus_{i=1}^r (\mathcal{A}_{\mu(i)} \square_{\varphi_{\mu(i)}} D_{\mu(i)})$. Then $\mathcal{D}$ is an ideal of $\mathcal{A}[x]/\langle x^{p^k} - y \rangle$ and satisfies

$$\begin{aligned} \mathcal{C} \cdot \mu(\mathcal{D}) &= \sum_{i=1}^r \left(\mathcal{A}_i \square_{\varphi_i} C_i\right) \cdot \mu\left(\mathcal{A}_{\mu(i)} \square_{\varphi_{\mu(i)}} D_{\mu(i)}\right) \\ &= \sum_{i=1}^r \left(\mathcal{A}_i \square_{\varphi_i} C_i\right) \cdot \left(\mathcal{A}_i \square_{\varphi_i} \mathrm{Ann}\,(C_i)\right) \\ &= \sum_{i=1}^r \varepsilon_i(y)\,(C_i \cdot \mathrm{Ann}\,(C_i)) \\ &= \{0\}, \end{aligned}$$

by Lemma 4.5. From this and by Lemma 4.1 we deduce $\mathcal{D} \subseteq \mathcal{C}^{\perp}$.

On the other hand, by [5, Theorem 3.5] and Lemma 3.2 we see that $|C_i||D_{\mu(i)}| = |C_i||\mathrm{Ann}(C_i)| = p^{2p^k m_i}$ for all $i = 1, \ldots, r$, which then implies

$$\begin{aligned} |\mathcal{C}||\mathcal{D}| &= \prod_{i=1}^r \left|\mathcal{A}_i \square_{\varphi_i} C_i\right| \left|\mathcal{A}_{\mu(i)} \square_{\varphi_{\mu(i)}} D_{\mu(i)}\right| = \prod_{i=1}^r |C_i| \left|D_{\mu(i)}\right| \\ &= p^{2p^k \sum_{i=1}^r m_i} = p^{2p^k n} = \left|\mathbb{Z}_{p^2}[x]/\left\langle x^{p^k n} - 1\right\rangle\right|. \end{aligned}$$

As stated above, we conclude that $\mathcal{C}^{\perp} = \mathcal{D}$ since $\mathbb{Z}_{p^2}$ is a finite chain ring. Finally, the conclusions follow from Theorem 3.7 and Corollary 4.4 immediately. □

Finally, by Theorem 4.6 and [7, Lemma 4.5] we deduce the following corollary for cyclic self-dual codes over $\mathbb{Z}_{p^2}$.

**Corollary 4.7** *Using the notations in Theorem 4.6 and Lemma 4.2*(ii), *let $\mathcal{C}$ be a cyclic code over $\mathbb{Z}_{p^2}$ of length $N$ with $\mathcal{C} = \oplus_{i=1}^r (\mathcal{A}_i \square_{\varphi_i} C_i)$, where $C_i$ is an ideal of $R_i[x]/\langle x^{p^k} - \zeta_i \rangle$. Then $\mathcal{C}$ is self-dual if and only if for each integer $i,\ 1 \le i \le r$, $C_i$ satisfies one of the following conditions*:

(i) *If* $1 \le i \le \lambda$, $C_i$ *is given by one of the following six cases*:

(i-1) $C_i = \langle p \rangle$.

(i-2) $C_i = \langle \pi_i^{\alpha p^{k-1}} + ph(\zeta_i^e x)\rangle$, *where* $h(z)$ *satisfies* $h_0 \neq 0, 1$ *and* $h(\zeta_i^e x) - (1 - \widehat{h}(\zeta_i^{-e} x^{-1}))(-1)^{-\alpha p^{k-1}} \zeta_i^{e\alpha p^{k-1}} x^{\alpha p^{k-1}} = 0$.

(i-3) $C_i = \langle \pi_i^s + ph(\zeta_i^e x)\rangle$, *where* $s > \alpha p^{k-1}$, $h(z) \neq 0$ *and* $h(\zeta_i^e x) - (\pi_i^{s-\alpha p^{k-1}} \omega_1 - \widehat{h}(\zeta_i^{-e} x^{-1}))\omega_2 = 0$ *with* $\omega_1 = (-1)^{s-\alpha p^{k-1}} \zeta_i^{e(\alpha p^{k-1}-s)} x^{\alpha p^{k-1}-s}$ *and* $\omega_2 = (-1)^{-s} \zeta_i^{es} x^s$.

(i-4) $C_i = \langle \pi_i^s + p\pi_i^{p^k - s}\rangle$, *where* $2s \ge \alpha p^{k-1} + p^k$.

(i-5) $C_i = \langle \pi_i^s + p\pi_i^{s-\alpha p^{k-1}} h(\zeta_i^e x),\ p\pi_i^{p^k-s}\rangle$, *where* $s \ge \alpha p^{k-1} + p^k$, $h_0 \neq 0, 1$ *and* $h(\zeta_i^e x) - (1 - \widehat{h}(\zeta_i^{-e} x^{-1}))\omega = 0$ *with* $\omega = (-1)^{p^{k-1}-p^k} \zeta_i^{-e(p^k - p^{k-1})} x^{p^k - p^{k-1}}$.

(i-6) $C_i = \langle \pi_i^s + p\pi_i^t h(\zeta_i^e x),\ p\pi_i^{p^k-s}\rangle$, *where* $0 < t < p^k - s$, $s > \alpha p^{k-1} + t$, $h(\zeta_i^e x) - (\pi_i^{s-t-\alpha p^{k-1}} \omega_1 - \widehat{h}(\zeta_i^{-e} x^{-1}))(-1)^{t-s} \zeta_i^{e(s-t)} x^{s-t} = 0$ *with* $\omega_1 = (-1)^{s-t-\alpha p^{k-1}} \zeta_i^{-e(s-t-\alpha p^{k-1})} x^{\alpha p^{k-1}+t-s}$.

(ii) *If* $i = \lambda + j$ *where* $1 \le j \le \rho$, *then* $\mu(i) = i + \rho$, $C_{\mu(i)} = D_{\mu(i)}$ *and* $(C_i, D_{\mu(i)})$ *is given by Theorem 4.6.*

## 5 Cyclic self-dual codes over $\mathbb{Z}_9$ of length 33

In this section, we consider to present all cyclic self-dual codes over $\mathbb{Z}_9$ of length 33. In this case, we have $N = 33 = 3^k n$ where $k = 1$ and $n = 11$.

It is known that $y^{11} - 1 = f_1(y) f_2(y) f_3(y)$, where $f_1(y) = y - 1$, $f_2(y) = y^5 + 3y^4 + 8y^3 + y^2 + 2y + 8$ and $f_3(y) = y^5 + 7y^4 + 8y^3 + y^2 + 6y + 8$ are pairwise coprime monic basic irreducible polynomials in $\mathbb{Z}_9[y]$. Obviously, $\widetilde{f}_1(y) = \delta_1 f_1(y)$ and $\widetilde{f}_2(y) = \delta_2 f_3(y)$ where $\delta_1 = \delta_2 = -1$, which implies that $\mu(1) = 1$ and $\mu(2) = 3$. Hence $m_1 = 1$, $m_2 = m_3 = 5$, $r = 3$ and $\lambda = \rho = 1$.

Using the notations in Sect. 2, for each integer $i$, $1 \le i \le 3$, we denote $F_i(y) = \frac{y^{11}-1}{f_i(y)}$, and find polynomials $a_i(y), b_i(y) \in \mathbb{Z}_9[y]$ satisfying $a_i(y)F_i(y) + b_i(y) f_i(y) = 1$. Then set $\varepsilon_i(y) \equiv a_i(y) F_i(y) \pmod{y^{11} - 1}$. Precisely, we have

$$\varepsilon_1(y) = 5y^{10} + 5y^9 + 5y^8 + 5y^7 + 5y^6 + 5y^5 + 5y^4 + 5y^3 + 5y^2 + 5y + 5;$$
$$\varepsilon_2(y) = 3y^{10} + y^9 + 3y^8 + 3y^7 + 3y^6 + y^5 + y^4 + y^3 + 3y^2 + y + 7;$$
$$\varepsilon_3(y) = y^{10} + 3y^9 + y^8 + y^7 + y^6 + 3y^5 + 3y^4 + 3y^3 + y^2 + 3y + 7.$$

Let $\mathcal{A} = \mathbb{Z}_9[y]/\langle y^{11} - 1\rangle$ and $\mathcal{A}_i = \mathcal{A}\varepsilon_i(y)$. Then $\mathcal{A}_i$ is a cyclic code over $\mathbb{Z}_9$ of length 11 with parity check polynomial $f_i(y)$ for $i = 1, 2, 3$. Therefore,

◇ $\mathcal{A}_1$ is a free $\mathbb{Z}_9$-submodule of $\mathbb{Z}_9^{11}$ with $\mathrm{rank}_{\mathbb{Z}_9}(\mathcal{A}_1) = 1$.
◇ $\mathcal{A}_i$ is a free $\mathbb{Z}_9$-submodule of $\mathbb{Z}_9^{11}$ with $\mathrm{rank}_{\mathbb{Z}_9}(\mathcal{A}_i) = 5$ for $i = 2, 3$.

Precisely, a generator matrix $G_{\mathcal{A}_i}$ of the cyclic code $\mathcal{A}_i$ over $\mathbb{Z}_9$ is given by: $G_{\mathcal{A}_1} = (5, 5, 5, 5, 5, 5, 5, 5, 5, 5, 5)$,

$$G_{\mathcal{A}_2}=\begin{pmatrix}7&1&3&1&1&1&3&3&3&1&3\\3&7&1&3&1&1&1&3&3&3&1\\1&3&7&1&3&1&1&1&3&3&3\\3&1&3&7&1&3&1&1&1&3&3\\3&3&1&3&7&1&3&1&1&1&3\end{pmatrix}\quad\text{and}$$

$$G_{\mathcal{A}_3}=\begin{pmatrix}7&3&1&3&3&3&1&1&1&3&1\\1&7&3&1&3&3&3&1&1&1&3\\3&1&7&3&1&3&3&3&1&1&1\\1&3&1&7&3&1&3&3&3&1&1\\1&1&3&1&7&3&1&3&3&3&1\end{pmatrix},$$

respectively. Hence $\mathcal{A}_1=\{(a,a,a,a,a,a,a,a,a,a,a)\mid a\in\mathbb{Z}_9\}$ with $d_{\min}(\mathcal{A}_1)=11$, and $\mathcal{A}_i=\{wG_{\mathcal{A}_i}\mid w\in\mathbb{Z}_9^5\}$ with $d_{\min}(\mathcal{A}_i)=6$ for $i=2,3$.

Denote $\zeta_i=y+\langle f_i(y)\rangle\in R_i$ where $R_i=\mathbb{Z}_9[y]/\langle f_i(y)\rangle$ for $i=1,2,3$. Obviously, $3^k\cdot 7\equiv -1 \pmod{11}$, which implies $(\zeta_i^7)^3=\zeta_i^{-1}$ by $\zeta_i^{11}=1$, for all $i=1,2,3$. Using the notations in Sect. 3, we have $e=7$. Therefore,

$\diamondsuit$ $\pi_1=\zeta_1^7x-1=x-1\in R_1[x]/\langle x^3-1\rangle$ where $R_1=\mathbb{Z}_9[y]/\langle f_1(y)\rangle=\mathbb{Z}_9$.
$\diamondsuit$ $\pi_2=\zeta_2^7x-1=(2y^4+2y^3+6y^2+4y+1)x-1\in R_2[x]/\langle x^3-y\rangle$ where $R_2=\mathbb{Z}_9[y]/\langle f_2(y)\rangle$, since $y^7\equiv 2y^4+2y^3+6y^2+4y+1 \pmod{f_2(y)}$.
$\diamondsuit$ $\pi_3=\zeta_3^7x-1=(2y^4+6y^3+2y^2+8y+5)x-1\in R_3[x]/\langle x^3-y\rangle$ where $R_3=\mathbb{Z}_9[y]/\langle f_3(y)\rangle$, since $y^7\equiv 2y^4+6y^3+2y^2+8y+5 \pmod{f_3(y)}$.

Moreover, by $\zeta_3^{11}=1$, $x^{33}=1$ and $x^3=\zeta_3=y$ in $R_3[x]/\langle x^3-\zeta_3\rangle$ we have $\zeta_3^{-7}x^{-1}=\zeta_3^4x^{32}=y^4y^{10}x^2=y^3x^2$ and $\zeta_3^{14}x^2=y^3x^2$.

Now, by Corollary 4.7 we conclude that all distinct cyclic self-dual codes over $\mathbb{Z}_9$ of length 33 are given by

$$\mathcal{C}=\left(\mathcal{A}_1\Box_{\varphi_1}C_1\right)\oplus\left(\mathcal{A}_2\Box_{\varphi_2}C_2\right)\oplus\left(\mathcal{A}_3\Box_{\varphi_3}C_3\right),$$

where $\varphi_i\colon R_i\to\mathcal{A}_i$ is given by the following

$\diamond$ $\varphi_1(a)=a\varepsilon_1(y)$ for all $a\in R_1$;
$\diamond$ $\varphi_i(a(y))=a(y)\varepsilon_i(y)$ for all $a(y)\in R_i$, $i=2,3$,

and $C_i$ is a $\zeta_i$-constacyclic code over $R_i$ of length 3, i.e., an ideal of the ring $R_i[x]/\langle x^3-y\rangle$, satisfying the following conditions:

• $C_1$ is an ideal of $\mathbb{Z}_9/\langle x^3-1\rangle$ given by one of the following two cases:

$$\langle 3\rangle;\ \left\langle (x-1)^2+6,\ 3(x-1)\right\rangle.$$

• $(C_2, C_3)$ is given by one of the following 736 cases:

| Cases | $C_2$ | $C_3$ |
|---|---|---|
| (1) | $\langle 0\rangle$ | $\langle 1\rangle$ |
| (2) | $\langle 1\rangle$ | $\langle 0\rangle$ |
| (3) | $\langle 3\rangle$ | $\langle 3\rangle$ |
| (4) | $\langle 3\pi_2\rangle$ | $\langle \pi_3^2,\ 3\rangle$ |
| (5) | $\langle 3\pi_2^2\rangle$ | $\langle \pi_3, 3\rangle$ |
| (6) | $\langle \pi_2+3h\rangle$ $(h\in\mathcal{T}_2)$ | $\langle \pi_3^2+3(1+\pi_3(\widehat{h}-1)y^3x^2)y^3x^2\rangle$ |
| (7) | $\langle \pi_2^2+3(1+\pi_2 h)\rangle$ $(h\in\mathcal{T}_2)$ | $\langle \pi_3+3(\widehat{h}-1)y^3x^2\rangle$ |
| (8) | $\langle \pi_2,\ 3\rangle$ | $\langle 3\pi_3^2\rangle$ |
| (9) | $\langle \pi_2^2,\ 3\rangle$ | $\langle 3\pi_3\rangle$ |
| (10) | $\langle \pi_2^2+3h,\ 3\pi_2\rangle$ $(h\in\mathcal{T}_2)$ | $\langle \pi_3^2+3(1-\widehat{h})y^3x^2,\ 3\pi_3\rangle$ |

in which $\mathcal{T}_2=\{\sum_{j=0}^4 t_jy^j \mid t_j\in\{0,\ 1,\ 2\},\ 0\le j\le 4\}$ and $\hat{h}=t_0+t_1y^{10}+t_2y^9+t_3y^8+t_4y^7$ (mod $f_3(y)$) for any $h=\sum_{j=0}^4 t_jy^j\in\mathcal{T}_2$. Hence the number of cyclic self-dual codes over $\mathbb{Z}_9$ of length 33 is equal to $2\times 736=1472$.

Finally, we consider how to give an encode for each self-dual code listed above. For $i=2,\ 3$, we have $R_i[x]/\langle x^3-y\rangle=\{b_0(y)+b_1(y)x+b_2(y)x^2 \mid b_0(y),\ b_1(y),\ b_2(y)\in R_i\}$. If $\beta(x)=b_0(y)+b_1(y)x+b_2(y)x^2\in R_i[x]/\langle x^3-y\rangle$, the ideal $\langle\beta(x)\rangle$ of $R_i[x]/\langle x^3-y\rangle$ is a $y$-constacyclic code over $R_i$ of length 3 having an $R_i$-generator matrix given by $\begin{pmatrix} b_0(y) & b_1(y) & b_2(y)\\ yb_2(y) & b_0(y) & b_1(y)\\ yb_1(y) & yb_2(y) & b_0(y)\end{pmatrix}$.

For example, we choose $\mathcal{C}=(\mathcal{A}_1\Box_{\varphi_1}C_1)\oplus(\mathcal{A}_2\Box_{\varphi_2}C_2)\oplus(\mathcal{A}_3\Box_{\varphi_3}C_3)$, where $C_1=\langle (x-1)^2+6,\ 3(x-1)\rangle$, $C_2=\langle\pi_2+3h\rangle$ and $C_3=\langle\pi_3^2+3(1+\pi_3(\widehat{h}-1)y^3x^2)y^3x^2\rangle$ with $h=1+2y^2$.

$\diamond$ Since the companion matrix of $f_1(y)=y-1$ is $M_{f_1}=(1)$ and $C_1=\langle 7+7x+x^2\rangle\oplus\langle 6+3x\rangle$, a generator matrix of the cyclic code $C_1$ over $R_1$ is $G_{C_1}=\begin{pmatrix}P\\ Q\end{pmatrix}$ where $P=\begin{pmatrix}7&7&1\\1&7&7\\7&1&7\end{pmatrix}$ and $Q=\begin{pmatrix}6&3&0\\0&6&3\\3&0&6\end{pmatrix}$. Then by Theorem 2.5, a generator matrix of $\mathcal{A}_1\Box_{\varphi_1}C_1$ is given by

$$G_{\mathcal{A}_1\Box_{\varphi_1}C_1}=\begin{pmatrix}7G_{\mathcal{A}_1} & 7G_{\mathcal{A}_1} & G_{\mathcal{A}_1}\\ G_{\mathcal{A}_1} & 7G_{\mathcal{A}_1} & 7G_{\mathcal{A}_1}\\ 7G_{\mathcal{A}_1} & G_{\mathcal{A}_1} & 7G_{\mathcal{A}_1}\\ 6G_{\mathcal{A}_1} & 3G_{\mathcal{A}_1} & 0\\ 0 & 6G_{\mathcal{A}_1} & 3G_{\mathcal{A}_1}\\ 3G_{\mathcal{A}_1} & 0 & 6G_{\mathcal{A}_1}\end{pmatrix}.$$

$\diamond$ Since the companion matrix of $f_2(y)$ is $M_{f_2}=\begin{pmatrix}0 & I_4\\ 1 & V_2\end{pmatrix}$, where $V_2=(7,\ 8,\ 1,\ 6)$, and $C_2=\langle(2+6y^2)+(1+4y+6y^2+2y^3+2y^4)x\rangle$, a generator matrix of the $y$-constacyclic code $C_2$ over $R_2$ is $G_{C_2} = \begin{pmatrix} \alpha_2 & \beta_2 & 0 \\ 0 & \alpha_2 & \beta_2 \\ y\beta_2 & 0 & \alpha_2 \end{pmatrix}$, where $\alpha_2 = 2+6y^2,\ \beta_2 = 1+4y+6y^2+2y^3+2y^4$ and $y\beta_2 = 2+6y+2y^2+8y^3+5y^4$. Using the notations of Theorem 2.5, we have $A_{\alpha_2} = 2I_5+6M_{f_2}^2,\ A_{\beta_2} = I_5+4M_{f_2}+6M_{f_2}^2+2M_{f_2}^3+2M_{f_2}^4$ and $A_{y\beta_2} = 2I_5+6M_{f_2}+2M_{f_2}^2+8M_{f_2}^3+5M_{f_2}^4$. Specifically, we obtain

$$A_{\alpha_2} = \begin{pmatrix} 2&0&6&0&0\\ 0&2&0&6&0\\ 0&0&2&0&6\\ 6&6&3&8&0\\ 0&6&6&3&8 \end{pmatrix},\quad A_{\beta_2} = \begin{pmatrix} 1&4&6&2&2\\ 2&6&2&8&5\\ 5&1&1&7&2\\ 2&1&8&3&1\\ 1&0&0&0&0 \end{pmatrix},\quad A_{y\beta_2} = \begin{pmatrix} 2&6&2&8&5\\ 5&1&1&7&2\\ 2&1&8&3&1\\ 1&0&0&0&0\\ 0&1&0&0&0 \end{pmatrix}.$$

Then by Theorem 2.5, a generator matrix of $\mathcal{A}_2\Box_{\varphi_2}C_2$ is given by

$$G_{\mathcal{A}_2\Box_{\varphi_2}C_2} = \begin{pmatrix} A_{\alpha_2}G_{\mathcal{A}_2} & A_{\beta_2}G_{\mathcal{A}_2} & 0 \\ 0 & A_{\alpha_2}G_{\mathcal{A}_2} & A_{\beta_2}G_{\mathcal{A}_2} \\ A_{y\beta_2}G_{\mathcal{A}_2} & 0 & A_{\alpha_2}G_{\mathcal{A}_2} \end{pmatrix}.$$

$\diamond$ Since the companion matrix of $f_3(y)$ is $M_{f_3} = \begin{pmatrix} 0 & I_4 \\ 1 & V_3 \end{pmatrix}$, where $V_3 = (3,\ 8,\ 1,\ 2)$, and $C_3 = \langle 1+(2+2y+2y^2+2y^4)x+(6y+4y^3)x^2 \rangle$, a generator matrix of the $y$-constacyclic code $C_3$ over $R_3$ is $G_{C_3} = \begin{pmatrix} \alpha_3 & \beta_3 & \gamma_3 \\ y\gamma_3 & \alpha_3 & \beta_3 \\ y\beta_3 & y\gamma_3 & \alpha_3 \end{pmatrix}$, where $\alpha_3 = 1,\ \beta_3 = 2+2y+2y^2+2y^4,\ \gamma_3 = 6y+4y^3,\ y\beta_3 = 2+8y+4y^3+4y^4$ and $y\gamma_3 = 6y^2+4y^4$. Using the notations of Theorem 2.5, we have $A_{\alpha_3} = I_5,\ A_{\beta_3} = 2I_5+2M_{f_3}+2M_{f_3}^2+2M_{f_3}^4,\ A_{\gamma_3} = 6M_{f_3}+4M_{f_3}^3,\ A_{y\beta_3} = 2I_5+8M_{f_3}+4M_{f_3}^3+4M_{f_3}^4$ and $A_{y\gamma_3} = 6M_{f_3}^2+4M_{f_3}^4$. Specifically, we obtain

$$A_{\beta_3} = \begin{pmatrix} 2&2&2&0&2\\ 2&8&0&4&4\\ 4&5&4&4&3\\ 3&4&2&7&1\\ 1&6&3&3&0 \end{pmatrix},\quad A_{\gamma_3} = \begin{pmatrix} 0&6&0&4&0\\ 0&0&6&0&4\\ 4&3&5&1&8\\ 8&1&4&4&8\\ 8&5&2&3&2 \end{pmatrix},\quad A_{y\beta_3} = \begin{pmatrix} 2&8&0&4&4\\ 4&5&5&4&3\\ 3&4&2&7&1\\ 1&6&3&3&0\\ 0&1&6&3&3 \end{pmatrix},$$

$$A_{y\gamma_3} = \begin{pmatrix} 0&0&6&0&4\\ 4&3&5&1&8\\ 8&1&4&4&8\\ 8&5&2&3&2\\ 2&5&3&4&7 \end{pmatrix}.$$

Then by Theorem 2.5 a generator matrix of $\mathcal{A}_3\Box_{\varphi_3}C_3$ is given by

$$G_{\mathcal{A}_3\Box_{\varphi_3}C_3} = \begin{pmatrix} G_{\mathcal{A}_3} & A_{\beta_3}G_{\mathcal{A}_3} & A_{\gamma_3}G_{\mathcal{A}_3} \\ A_{y\gamma_3}G_{\mathcal{A}_3} & G_{\mathcal{A}_3} & A_{\beta_3}G_{\mathcal{A}_3} \\ A_{y\beta_3}G_{\mathcal{A}_3} & A_{y\gamma_3}G_{\mathcal{A}_3} & G_{\mathcal{A}_3} \end{pmatrix}.$$

Now, by Corollary 3.8 a generator matrix of the self-dual cyclic code $\mathcal{C}$ over $\mathbb{Z}_9$ of length 33 is given by $G_{\mathcal{C}} = \begin{pmatrix} G_{\mathcal{A}_1\Box_{\varphi_1}C_1} \\ G_{\mathcal{A}_2\Box_{\varphi_2}C_2} \\ G_{\mathcal{A}_3\Box_{\varphi_3}C_3} \end{pmatrix}$. Hence $\mathcal{C} = \{uG_{\mathcal{C}} \mid u \in \mathbb{Z}_9^{36}\}$.

## 6 Conclusions

We present a canonical form decomposition for every cyclic code over $\mathbb{Z}_{p^2}$ of length $p^k n$ ($k \geq 1$ and $\gcd(p, n) = 1$), where each subcode is concatenated by a basic irreducible cyclic code over $\mathbb{Z}_{p^2}$ of length $n$ as the inner code and a constacyclic code over a Galois extension ring of $\mathbb{Z}_{p^2}$ of length $p^k$ as the outer code. By determining their outer codes, we present a precise description for cyclic codes over $\mathbb{Z}_{p^2}$ when $p \neq 2$, give precisely dual codes and investigate self-duality for cyclic codes over $\mathbb{Z}_{p^2}$. These codes enjoy a rich algebraic structure compared to arbitrary linear codes (which makes the search process much simpler). Obtaining some bounds for minimal distance such as BCH-like of a cyclic code over the ring $\mathbb{Z}_{p^2}$ by just looking at the concatenated structure 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. This research is supported in part by the National Natural Science Foundation of China (Grant Nos. 11471255, 61171082).

## References

1. Abualrub, T., Oehmke, R.: On the generators of $\mathbb{Z}_4$ cyclic codes of length $2^e$. IEEE IT **49**(9), 2126–2133 (2003)
2. Blackford, T.: Cyclic codes over $\mathbb{Z}_4$ of oddly even length. Discrete Appl. Math. **128**, 27–46 (2003)
3. Calderbank, A.R., Sloane, N.J.A.: Modular and $p$-adic cyclic codes. Des. Codes Cryptogr. **6**, 21–35 (1995)
4. Dougherty, S.T., Ling, S.: Cyclic codes over $\mathbb{Z}_4$ of even length. Des. Codes Cryptogr. **39**, 127–153 (2006)
5. Kiah, H.M., Leung, K.H., Ling, S.: Cyclic codes over GR$(p^2, m)$ of length $p^k$. Finite Fields Appl. **14**, 834–846 (2008)
6. Pless, V.S., Qian, Z.: Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$. IEEE IT **42**(5), 1594–1600 (1996)
7. Sobhani, R., Esmaeili, M.: Cyclic and negacyclic codes over the Galois ring GR$(p^2, m)$. Discrete Appl. Math. **157**, 2892–2903 (2009)