Bull. Korean Math. Soc. **0** (0), No. 0, pp. 1–0
https://doi.org/10.4134/BKMS.b180148
pISSN: 1015-8634 / eISSN: 2234-3016

REPEATED-ROOT CONSTACYCLIC CODES OF LENGTH $2p^s$ OVER GALOIS RINGS

Chakkrid Klin-eam and Wateekorn Sriwirach

Abstract. In this paper, we consider the structure of γ-constacyclic codes of length $2p^s$ over the Galois ring $\mathrm{GR}(p^a, m)$ for any unit γ of the form $\xi_0 + p\xi_1 + p^2 z$, where $z \in \mathrm{GR}(p^a, m)$ and ξ_0, ξ_1 are nonzero elements of the set $\mathcal{T}(p, m)$. Here $\mathcal{T}(p, m)$ denotes a complete set of representatives of the cosets $\frac{\mathrm{GR}(p^a,m)}{p\mathrm{GR}(p^a,m)} = \mathbb{F}_{p^m}$ in $\mathrm{GR}(p^a, m)$. When γ is not a square, the rings $\mathcal{R}_p(a, m, \gamma) = \frac{\mathrm{GR}(p^a,m)[x]}{\langle x^{2p^s} - \gamma\rangle}$ is a chain ring with maximal ideal $\langle x^2 - \delta\rangle$, where $\delta^{p^s} = \xi_0$, and the number of codewords of γ-constacyclic code are provided. Furthermore, the self-orthogonal and self-dual γ-constacyclic codes of length $2p^s$ over $\mathrm{GR}(p^a, m)$ are also established. Finally, we determine the Rosenbloom-Tsfasman (RT) distances and weight distributions of all such codes.

1. Introduction

Let R be a finite commutative ring with identity. A linear code of length n over the ring R is an R-submodule of R^n. A code C of length n over a ring R is called *cyclic* if $(c_0, c_1, \ldots, c_{n-1}) \in C$ implies that $(c_{n-1}, c_0, \ldots, c_{n-2}) \in C$. In general, let γ be a unit element in R, a code C of length n over R is called γ*-constacyclic* if $(c_0, c_1, \ldots, c_{n-1}) \in C$ implies that $(\gamma c_{n-1}, c_0, \ldots, c_{n-2}) \in C$. When $\gamma = 1$, 1-constacyclic codes are cyclic codes, and when $\gamma = -1$, they are called *negacyclic codes*. Furthermore, γ-constacyclic codes of length n are in correspondence with ideals in the polynomial ring $\frac{R[x]}{\langle x^n - \gamma\rangle}$. The case when the code length n is divisible by the characteristic p of the underlying ring yields the so-called *repeated-root codes*. The structure of repeated-root constacyclic codes have been discussed in [3, 6, 21, 26, 27].

Moreover, constacyclic codes are an important class of cyclic codes in the theory of error-correcting codes. They can be efficiently encoded using shift

Received February 16, 2018; Revised May 30, 2018; Accepted July 12, 2018.
2010 *Mathematics Subject Classification.* Primary 94B15, 94B05; Secondary 11T71.
Key words and phrases. constacyclic codes, repeated-root codes, Galois rings, Rosenbloom-Tsfasman distance.

Research Center for Academic Excellence in Mathematics, Naresuan University, Phitsanulok 65000, Thailand.

registers, which explains their preferred role in engineering. Constacyclic codes over finite fields were initiated by Berlekamp in the early 1960s [2]. After the realization in the 1990's [5,14,20] that many important yet seemingly non-linear binary codes such as Kerdock and Preparata codes are actually closely related to linear codes over the ring of integers modulo four via the Gray map, codes over $\mathbb{Z}_4$ in particular, and codes over finite rings in general, have received a great deal of attention. Constacyclic codes over finite rings were introduced by Wolfmann in [28], where was proved that the binary image of a linear negacyclic code over $\mathbb{Z}_4$ is a binary cyclic code. The structure of constacyclic codes over some finite commutative rings have been discussed in [4, 9, 11, 12, 23]

The Galois ring of characteristic p^a and dimension m, denoted by $\mathrm{GR}(p^a, m)$, is the Galois extension of degree m of the ring $\mathbb{Z}_{p^a}$ for some prime number p and positive integer a. In 2003, Abualrub and Ochmke [1] considered cyclic codes of length 2^s over $\mathbb{Z}_4$. The structure of negacyclic codes of length 2^s over $\mathbb{Z}_{2^m}$ was obtained since 2004 by Dinh and López-Permouth [11]. In 2005, Dinh [8] studied negacyclic codes of length 2^s over the Galois ring $\mathrm{GR}(2^a, m)$. The ring $\frac{\mathrm{GR}(2^a,m)[x]}{\langle x^{2^s}+1\rangle}$ is indeed a chain ring, and the negacyclic codes of length 2^s over $\mathrm{GR}(2^a, m)$ are precisely the ideals generated by $(x+1)^i$ of this chain ring for $i = 0, 1, \ldots, a2^s$. In 2017, Dinh et al. [10] determined the structure of γ-constacyclic codes of length 2^s over $\mathrm{GR}(2^a, m)$ for any unit γ of the form $4z - 1$, where $z \in \mathrm{GR}(2^a, m)$. Furthermore, the Hamming, homogeneous, and Rosenbloom-Tsfasman distances, and Rosenbloom-Tsfasman weight distribution of all such constacyclic codes were computed. Recently, Liu and Maouche [17] studied more general cases and investigated all cases where $\frac{\mathrm{GR}(p^a,m)[x]}{\langle x^{p^s}-\gamma\rangle}$ is a chain ring. Moreover, the structure of $\mathcal{R}_p(a, m, \gamma) = \frac{\mathrm{GR}(p^a,m)[x]}{\langle x^{2p^s}+\gamma\rangle}$ is used to establish the Hamming and homogeneous distances of γ-constacyclic codes.

The purpose of this paper is to study the algebraic structure of all γ-constacyclic codes of length $2p^s$ over $\mathrm{GR}(p^a, m)$ for any unit of the form $\gamma = \xi_0 + p\xi_1 + p^2 z$, where z is an arbitrary element of $\mathrm{GR}(p^a, m)$ and ξ_0, ξ_1 are nonzero elements of the set $\mathcal{T}(p, m)$, which $\mathcal{T}(p, m)$ denotes a complete set of representatives of the cosets $\frac{\mathrm{GR}(p^a,m)}{p\mathrm{GR}(p^a,m)} = \mathbb{F}_{p^m}$ in $\mathrm{GR}(p^a, m)$, and we called the unit of this form is a unit of Type (1). We show that the ring $\mathcal{R}_p(a, m, \gamma)$ is a chain ring if and only if γ is a unit of Type (1). Moreover, we also derive the duals of all such γ-constacyclic codes as well as necessary and sufficient conditions for the existence of self-orthogonal and self-dual γ-constacyclic codes. Using this structure, we obtain the number of codewords, the Rosenbloom-Tsfasman distances and weight distributions of all γ-constacyclic codes.

This paper is organized as follows. We discuss some preliminaries in Section 2. In Section 3, we study γ-constacyclic codes of length $2p^s$ over the ring $\mathrm{GR}(p^a, m)$, where γ is a unit of Type (1) of $\mathrm{GR}(p^a, m)$. In the case, γ is a square, i.e., $\gamma = \alpha^2$ for some $\alpha \in \mathrm{GR}(p^a, m)$. By Chinese Remainder Theorem, the ambient ring $\frac{\mathrm{GR}(p^a,m)[x]}{\langle x^{2p^s}-\gamma\rangle}$ can be decomposed as $\frac{\mathrm{GR}(p^a,m)[x]}{\langle x^{p^s}+\alpha\rangle}$ and

$\frac{\mathrm{GR}(p^a,m)[x]}{\langle x^{p^s}-\alpha\rangle}$. In the main case, when γ is not a square in $\mathrm{GR}(p^a, m)$, we consider the algebraic structure of all Type (1) γ-constacyclic code of length $2p^s$ over $\mathrm{GR}(p^a, m)$. Furthermore, we can show that the ring $\mathcal{R}_p(a, m, \gamma)$ is a chain ring with maximal ideal $\langle x^2 - \delta\rangle$, where $\delta^{p^s} = \xi_0$, and the number of codewords of γ-constacyclic code are provided. This structure is applied to establish the Rosenbloom-Tsfasman distances and weight distributions of all such codes in Section 4.

2. Preliminaries

An ideal I of a ring R is called *principal* if it is generated by a single element. A ring R is a *principal ideal ring* if its ideals are principal. R is called a *local ring* if R has a unique maximal right (left) ideal. Furthermore, a ring R is called a *chain ring* if the set of all right (left) ideals of R is linearly ordered under set-theoretic inclusion. The following equivalent conditions are known for the class of finite commutative rings (see [11, Proposition 2.1])

Proposition 2.1 ([11])**.** *If R is a finite commutative ring with identity, then the following conditions are equivalent*:

(i) *R is a local ring and the maximal ideal M of R is principal,*
(ii) *R is a local principal ideal ring,*
(iii) *R is a chain ring.*

Let θ be a fixed generator of the maximal ideal M of a finite commutative chain ring R, then θ is a nilpotent and we denote its nilpotency index by t. The ideals of R form a chain:

$$R = \langle\theta^0\rangle \supsetneq \langle\theta^1\rangle \supsetneq \cdots \supsetneq \langle\theta^{t-1}\rangle \supsetneq \langle\theta^t\rangle = \langle 0\rangle.$$

Let $\bar{R} = \frac{R}{M}$. By $^-\colon R[x] \to \bar{R}[x]$, we denote the natural ring homomorphism that maps $r \mapsto r + M$ and the variable x to x. The following is a well-known fact about finite commutative chain rings (see [19]).

Proposition 2.2. *Let R be a finite commutative chain ring, with maximal ideal $M = \langle\theta\rangle$, and let t be the nilpotency of θ. Then*

(i) *For some prime p and positive integers k, l $(k \geq l)$, $|R| = p^k$, $|\bar{R}| = p^l$, the characteristic of R and $\bar{R}$ are powers of p,*
(ii) *For $i = 0, 1, \ldots, t$, $|\langle\theta^i\rangle| = |\bar{R}|^{t-i}$. In particular, $|R| = |\bar{R}|^t$, i.e., $k = lt$.*

Each codeword $c = (c_0, c_1, \ldots, c_{n-1})$ is identified with its polynomial representation $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$, and the code C is in turn identified with the set of all polynomial representations of its codewords. Then in the ring $\frac{R[x]}{\langle x^n-\gamma\rangle}$, $xc(x)$ corresponds to a γ-constacyclic shift of $c(x)$. From that, the following fact is well known and straightforward:

Proposition 2.3 ([15, 18])**.** *A linear code C of length n is γ-constacyclic over R if and only if C is an ideal of the quotient ring $\frac{R[x]}{\langle x^n-\gamma\rangle}$.*

Given n-tuples $x = (x_0, x_1, \dots, x_{n-1}), y = (y_0, y_1, \dots, y_{n-1}) \in R^n$, their inner product is defined as usual

$$x \cdot y = x_0y_0 + x_1y_1 + \cdots + x_{n-1}y_{n-1},$$

evaluated in R. Two n-tuples x, y are called *orthogonal* if $x \cdot y = 0$. For a linear code C over R, its dual code $C^\perp$ is the set of n-tuples over R that are orthogonal to all codewords of C, i.e.,

$$C^\perp = \{x \mid x \cdot y = 0, \forall y \in C\}.$$

A code C is called *self-orthogonal* if $C \subseteq C^\perp$, and it is called *self-dual* if $C = C^\perp$. The following proposition can be found in [22].

Proposition 2.4. *Let p be a prime and R be a finite chain ring of size p^α. The number of codewords in any linear code C of length n over R is p^k for some integer $k \in \{0, 1, \dots, \alpha n\}$. Moreover, the dual code $C^\perp$ has p^l codewords, where $k + l = \alpha n$, i.e., $|C| \cdot |C^\perp| = |R|^n$.*

Note that the dual of cyclic code is a cyclic code, and the dual of a negacyclic code is a negacyclic code. In general, we have the following implication of dual of a γ-constacyclic code.

Proposition 2.5. *The dual of a γ-constacyclic code is γ^{-1}-constacyclic code.*

A polynomial in $\mathbb{Z}_{p^a}[x]$ is called a *basic irreducible polynomial* if its reduction modulo p is irreducible in $\mathbb{Z}_p[x]$. The *Galois ring of characteristic p^a and dimension m*, denoted by $GR(p^a, m)$, is the Galois extension of degree m of the ring $\mathbb{Z}_{p^a}$. Equivalently,

$$\mathrm{GR}(p^a, m) = \frac{\mathbb{Z}_{p^a}[u]}{\langle h(u) \rangle},$$

where $h(u)$ is a monic basic irreducible polynomial of degree m in $\mathbb{Z}_{p^a}[u]$. Note that if $a = 1$, then $\mathrm{GR}(p, m) = \mathbb{F}_{p^m}$, and if $m = 1$, then $\mathrm{GR}(p^a, 1) = \mathbb{Z}_{p^a}$. We have some properties of Galois rings as the following proposition.

Proposition 2.6 ([17]). *Let $\mathrm{GR}(p^a, m) = \frac{\mathbb{Z}_{p^a}[u]}{\langle h(u) \rangle}$ be a Galois ring. Then the following hold*:

(i) *Each ideal of $\mathrm{GR}(p^a, m)$ is of the form $\langle p^k \rangle = p^k\mathrm{GR}(p^a, m)$ for $0 \leq k \leq a$. In particular, $\mathrm{GR}(p^a, m)$ is a chain ring with maximal ideal $\langle p \rangle = p\mathrm{GR}(p^a, m)$ and residue field $\mathbb{F}_{p^m}$.*
(ii) *For $0 \leq i \leq a$, $|p^i\mathrm{GR}(p^a, m)| = p^{m(a-i)}$.*
(iii) *Each element of $\mathrm{GR}(p^a, m)$ can be represented as vp^k, where v is a unit and $0 \leq k \leq a$. In this representation k is unique and v is unique modulo p^{a-k}.*
(iv) *$h(u)$ has a root ξ in $\mathrm{GR}(p^a, m)$, which is also a primitive $(p^m - 1)$th root of unity. The set*

$$\mathcal{T}(p, m) = \{0, 1, \xi, \xi^2, \dots, \xi^{p^m-2}\}.$$

is a complete set of representatives of the cosets $\frac{\mathrm{GR}(p^a,m)}{p\mathrm{GR}(p^a,m)} = \mathbb{F}_{p^m}$ *in* $\mathrm{GR}(p^a, m)$*. Each element* $\gamma \in \mathrm{GR}(p^a, m)$ *can be written uniquely as*

$$\gamma = \xi_0 + p\xi_1 + \cdots + p^{a-1}\xi_{a-1}$$

with $\xi_i \in \mathcal{T}(p, m)$*,* $0 \le i \le a-1$*.*

(v) *For* $0 \le i < j \le p^m - 2$*, all* $\xi^i - \xi^j$ *are units of* $\mathrm{GR}(p^a, m)$*.*

In this paper, we will say that an element $\gamma \in \mathrm{GR}(p^a, m)$ is of *Type* (0) if it has the form

$$\gamma = \xi_0 + p^2\xi_2 + \cdots + p^{a-1}\xi_{a-1} = \xi_0 + p^2 z,$$

where ξ_0 is nonzero elements of the set $\mathcal{T}(p, m)$ and $z \in \mathrm{GR}(p^a, m)$. Moreover, γ is said to be of *Type* (1) if it is of the form

$$\gamma = \xi_0 + p\xi_1 + p^2\xi_2 + \cdots + p^{a-1}\xi_{a-1} = \xi_0 + p\xi_1 + p^2 z,$$

where ξ_0, ξ_1 are nonzero elements of the set $\mathcal{T}(p, m)$ and $z \in \mathrm{GR}(p^a, m)$. We can see that the elements of Type (0) and Type (1) are invertible in $\mathrm{GR}(p^a, m)$. Moreover, the sets of Type (0) and Type (1) form a partition of the set of all units of $\mathrm{GR}(p^a, m)$ when $a \ge 2$. We call a γ*-constacyclic code is of Type* (0) (resp. *Type* (1)) if the units γ is of Type (0) (resp. Type (1)).

The unit of γ is determined in the following lemma.

Lemma 2.7 ([17])**.** *Let* $\gamma_1 = \xi_{00} + p\xi_{01} + p^2 z_1$ *and* $\gamma_2 = \xi_{10} + p\xi_{11} + p^2 z_2$ *be two units of Type* (1)*. Let* $\gamma_3 = 1 + p^2 z_3$ *and* $\gamma_4 = 1 + p^2 z_4$ *be two units of Type* (0)*. Let* $a_0 \ge 2$ *be the smallest integer such that* $2^{a_0} \ge a$*, i.e.,* $p^2 a_0 = 0$ *in* $\mathrm{GR}(p^a, m)$*. Then*

- $\gamma_1\gamma_3$ *is of Type* (1)*, i.e., the product of a unit of Type* (1) *and a unit of Type* (0) *is a unit of Type* (1)*.*
- $\gamma_3\gamma_4$ *is of Type* (0)*, i.e., the product of two units of Type* (0) *is a unit of Type* (0)*.*
- $\gamma_1^{-1} = \xi_{00}^{-1}(1 - p(\xi_{00}^{-1}\xi_{01} + p\xi_{00}^{-1}z_1))\Pi_{j=1}^{a_0-1}[1 + p^{2^j}(\xi_{00}^{-1}\xi_{01} + p\xi_{00}^{-1}z_1)^{2^j}]$ *is of Type* (1)*, i.e., the inverse of a unit of Type* (1) *is a unit of Type* (1)*.*
- $\gamma_3^{-1} = (1 - p^2 z_3)\Pi_{j=1}^{a_0-1}[1 + (p^2 z_3)^{2j}]$ *is of Type* (0)*, i.e., the inverse of a unit of Type* (0) *is a unit of Type* (0)*.*

3. $(\xi_0 + p\xi_1 + p^2 z)$-constacyclic codes of length $2p^s$ over $\mathrm{GR}(p^a, m)$

In this section, we consider γ-constacyclic codes of length $2p^s$ over $\mathrm{GR}(p^a, m)$, where γ is of Type (1), i.e., γ is of the form $\xi_0 + p\xi_1 + p^2 z$, where ξ_0, ξ_1 are nonzero elements of the set $\mathcal{T}(p, m)$ and $z \in \mathrm{GR}(p^a, m)$. By Proposition 2.3, γ-constacyclic codes of length $2p^s$ over $\mathrm{GR}(p^a, m)$ are exactly the ideals of the ambient ring

$$\mathcal{R}_p(a, m, \gamma) = \frac{\mathrm{GR}(p^a, m)[x]}{\langle x^{2p^s} - \gamma \rangle}.$$

Now, if the unit γ is a square in $\mathrm{GR}(p^a,m)$, i.e., there exists a unit $\alpha \in \mathrm{GR}(p^a,m)$ such that $\gamma = \alpha^2$. Then we have

$$x^{2p^s} - \gamma = x^{2p^s} - \alpha^2 = (x^{p^s} + \alpha)(x^{p^s} - \alpha).$$

By Chinese Remainder Theorem, we get that

$$\mathcal{R}_p(a,m,\gamma) = \frac{\mathrm{GR}(p^a,m)[x]}{\langle x^{2p^s} - \gamma\rangle} \cong \frac{\mathrm{GR}(p^a,m)[x]}{\langle x^{p^s} + \alpha\rangle} \oplus \frac{\mathrm{GR}(p^a,m)[x]}{\langle x^{p^s} - \alpha\rangle}.$$

It implies that ideals of $\mathcal{R}_p(a,m,\gamma)$ are of the form $A \oplus B$, where A and B are ideals of $\frac{\mathrm{GR}(p^a,m)[x]}{\langle x^{p^s}+\alpha\rangle}$ and $\frac{\mathrm{GR}(p^a,m)[x]}{\langle x^{p^s}-\alpha\rangle}$, respectively, i.e., they are $-\alpha$ and α-constacyclic codes of length p^s over $\mathrm{GR}(p^a,m)$. This means that any γ-constacyclic code of length $2p^s$ over $\mathrm{GR}(p^a,m)$, i.e., an ideal C of the ring $\mathcal{R}_p(a,m,\gamma)$, is represented as a direct sum of $C_{-\alpha}$ and C_α:

$$C = C_{-\alpha} \oplus C_\alpha,$$

where $C_{-\alpha}$ and C_α are ideals of $\frac{\mathrm{GR}(p^a,m)[x]}{\langle x^{p^s}+\alpha\rangle}$ and $\frac{\mathrm{GR}(p^a,m)[x]}{\langle x^{p^s}-\alpha\rangle}$, respectively. Hence we can determine the classification, detailed structure, and number of codewords of $-\alpha$ and α-constacyclic codes length p^s were investigated in [17]. Thus, when γ is a square in $\mathrm{GR}(p^a,m)$, we can obtain γ-constacyclic codes C of length $2p^s$ over $\mathrm{GR}(p^a,m)$ from that of the direct summands $C_{-\alpha}$ and C_α (see [17]). Now, we have the dual code $C^\perp$ of C including a direct sum of the dual codes of the direct summands $C_{-\alpha}^\perp$ and $C_\alpha^\perp$.

Theorem 3.1. *Let the unit $\gamma = \alpha^2 \in \mathrm{GR}(p^a,m)$, and $C = C_{-\alpha} \oplus C_\alpha$ be a γ-constacyclic code of length $2p^s$ over $\mathrm{GR}(p^a,m)$, where $C_{-\alpha}$ and C_α are ideals of $\frac{\mathrm{GR}(p^a,m)[x]}{\langle x^{p^s}+\alpha\rangle}$ and $\frac{\mathrm{GR}(p^a,m)[x]}{\langle x^{p^s}-\alpha\rangle}$, respectively. Then*

$$C^\perp = C_{-\alpha}^\perp \oplus C_\alpha^\perp.$$

In particular, C is a self-dual constacyclic code of length $2p^s$ over $\mathrm{GR}(p^a,m)$ if and only if $C_{-\alpha}$ and C_α are self-dual $-\alpha$ and α-constacyclic codes of length p^s over $\mathrm{GR}(p^a,m)$, respectively.

Proof. We have $C_{-\alpha}^\perp \oplus C_\alpha^\perp \subseteq C^\perp$. Now, we consider

$$\begin{aligned} |C_{-\alpha}^\perp \oplus C_\alpha^\perp| = |C_{-\alpha}^\perp| \cdot |C_\alpha^\perp| &= \frac{|\mathrm{GR}(p^a,m)|^{p^s}}{|C_{-\alpha}|} \cdot \frac{|\mathrm{GR}(p^a,m)|^{p^s}}{|C_\alpha|} \\ &= \frac{|\mathrm{GR}(p^a,m)|^{2p^s}}{|C_{-\alpha}| \cdot |C_\alpha|} \\ &= \frac{|\mathrm{GR}(p^a,m)|^{2p^s}}{|C|} = |C^\perp|. \end{aligned}$$

Hence, $C^\perp = C_{-\alpha}^\perp \oplus C_\alpha^\perp$. □

Next, we will consider on the main case when γ is not square in $\mathrm{GR}(p^a,m)$ and we note that $\mathcal{R}_2(a,m,\gamma) = \frac{\mathrm{GR}(2^a,m)[x]}{\langle x^{2^{s+1}}-\gamma\rangle}$. We have the following.

Proposition 3.2. *Let b and γ be two units of $GR(p^a, m)$. For any positive integer n, there exist polynomials $\alpha_n(x), \beta_n(x), \theta_n(x) \in \mathbb{Z}[x]$, such that*

- *If $p = 2$, then $(x^2 + b)^{2^n} = x^{2^{n+1}} + b^{2^n} + 2\alpha_n(x) = x^{2^{n+1}} + b^{2^n} + 2((bx^2)^{2^{n-1}} + 2\beta_n(x))$. Moreover, $\alpha_n(x)$ is invertible in $\mathcal{R}_2(a, m, \gamma)$.*
- *If p is odd, then $(x^2 + b)^{p^n} = x^{2p^n} + b^{p^n} + p(x^2 + b)\theta_n(x)$.*

Proof. We will prove this by induction on n.

Case 1: If $p = 2$ and $n = 1$, then

$$(x^2 + b)^2 = x^4 + b^2 + 2bx^2,$$

where $\alpha_1(x) = bx^2$, and $\beta_1(x) = 0$. We can see that $\alpha_1(x) = bx^2$ is a unit in $\mathcal{R}_2(a, m, \gamma)$. So, $(x^2 + b)^2 = x^{2^2} + b^2 + 2\alpha_1(x)$. Hence, the assertion is true for $n = 1$. Assume that the assertion is true for any integer up to $n - 1$, we want to prove that it is true for n. We consider

$$\begin{aligned}(x^2 + b)^{2^n} &= ((x^2 + b)^{2^{n-1}})^2 \\ &= (x^{2^n} + b^{2^{n-1}} + 2\alpha_{n-1}(x))^2 \\ &= (x^{2^n} + b^{2^{n-1}})^2 + 2(x^{2^n} + b^{2^{n-1}})(2\alpha_{n-1}(x)) + (2\alpha_{n-1}(x))^2 \\ &= x^{2^{n+1}} + 2b^{2^{n-1}}x^{2^n} + b^{2^n} + 4x^{2^n}\alpha_{n-1}(x) + 4b^{2^{n-1}}\alpha_{n-1}(x) + 4\alpha_{n-1}^2(x) \\ &= x^{2^{n+1}} + b^{2^n} + 2\alpha_n(x),\end{aligned}$$

where $\alpha_n(x) = (bx^2)^{2^{n-1}} + 2\beta_n(x)$ and $\beta_n(x) = \alpha_{n-1}^2(x) + b^{2^{n-1}}\alpha_{n-1}(x) + x^{2^n}\alpha_{n-1}(x)$. Since x and b are invertible in $\mathcal{R}_2(a, m, \gamma)$, $\alpha_n(x)$ is also invertible in $\mathcal{R}_2(a, m, \gamma)$. As 2 is nilpotent in $\mathcal{R}_2(a, m, \gamma)$, the proof is completed for $p = 2$.

Case 2: If p is odd. Then, for any positive integer k,

$$\begin{aligned}&(x^{2p^{k-1}} + b^{p^{k-1}})^p \\ &= x^{2p^k} + b^{p^k} + \sum_{i=1}^{p-1}\binom{p}{i}(b^{p^{k-1}})^i(x^{2p^{k-1}})^{p-i} \\ &= x^{2p^k} + b^{p^k} + \sum_{i=1}^{\frac{p-1}{2}}\left(\binom{p}{i}(x^{2p^{k-1}})^{p-i}(b^{p^{k-1}})^i + \binom{p}{p-i}(x^{2p^{k-1}})^i(b^{p^{k-1}})^{p-i}\right) \\ &= x^{2p^k} + b^{p^k} + \sum_{i=1}^{\frac{p-1}{2}}\binom{p}{i}b^{ip^{k-1}}x^{2ip^{k-1}}\left(x^{2p^{k-1}(p-2i)} + b^{p^{k-1}(p-2i)}\right).\end{aligned}$$

We can see that $p^{k-1}(p-2i)$ is odd, then there exist polynomials $\beta'_i(x) \in \mathbb{Z}[x]$, $0 \le i \le \frac{p-1}{2}$, such that $x^{2p^{k-1}(p-2i)} + b^{p^{k-1}(p-2i)} = (x^2 + b)\beta'_i(x)$. Thus

$$(x^{2p^{k-1}} + b^{p^{k-1}})^p = x^{2p^k} + b^{p^k} + \sum_{i=1}^{\frac{p-1}{2}}\binom{p}{i}b^{ip^{k-1}}x^{2ip^{k-1}}(x^2 + b)\beta'_i(x)$$

$$= x^{2p^k} + b^{p^k} + p(x^2+b)\sum_{i=1}^{\frac{p-1}{2}} \frac{\binom{p}{i}}{p} b^{ip^{k-1}} x^{2ip^{k-1}} \beta_i'(x).$$

Hence

$$(x^{2p^{k-1}} + b^{p^{k-1}})^p = x^{2p^k} + b^{p^k} + p(x^2+b)\beta_k'(x), \tag{1}$$

where

$$\beta_k'(x) = \sum_{i=1}^{\frac{p-1}{2}} \frac{\binom{p}{i}}{p} b^{ip^{k-1}} x^{2ip^{k-1}} (x^2+b)\beta_i'(x).$$

Plugging in $k = 1$ yields that the assertion is true for $n = 1$. Assume the assertion is true for any integer up to $n-1$, we want to prove that it is true for n, we consider

$$\begin{aligned}(x^2+b)^{p^n} &= ((x^2+b)^{p^{n-1}})^p = (x^{2p^{n-1}} + b^{p^{n-1}} + p(x^2+b)\alpha_{n-1}(x))^p \\ &= (x^{2p^{n-1}} + b^{p^{n-1}})^p + \sum_{i=1}^{p}\binom{p}{i}(x^{2p^{n-1}} + b^{p^{n-1}})^{p-i}(p(x^2+b)\alpha_{n-1}(x))^i \\ &= (x^{2p^{n-1}} + b^{p^{n-1}})^p + p(x^2+b)t(x),\end{aligned}$$

where

$$t(x) = \sum_{i=1}^{p}\binom{p}{i}(x^{2p^{n-1}} + b^{p^{n-1}})^{p-i}\frac{(p(x^2+b)\alpha_{n-1}(x))^i}{p(x^2+b)}.$$

By using Equation (1) and inductive hypothesis, we get

$$(x^2+b)^{p^n} = x^{2p^n} + b^{p^n} + p(x^2+b)\beta_n'(x) + p(x^2+b)t(x) = x^{2p^n} + b^{p^n} + p(x^2+b)\theta_n(x),$$

where $\theta_n(x) = \beta_n'(x) + t(x)$. The proof is completed for p is odd. □

We note that the ring $\mathcal{R}_p(a,m,\gamma)$ is a local ring, and hence in $\mathcal{R}_p(a,m,\gamma)$ the sum of two noninvertible elements is noninvertible, and the sum of a non-invertible element and an invertible element is invertible.

Lemma 3.3. *Let $\gamma = \xi_0 + p\xi_1 + p^2 z$ be a unit of Type (1) of $\mathrm{GR}(p^a,m)$, where ξ_0, ξ_1 are nonzero elements of $\mathcal{T}(p,m)$ and $z \in \mathrm{GR}(p^a,m)$. Then there exists an invertible element δ in $\mathcal{T}(p,m)$ such that $\langle (x^2-\delta)^{p^s}\rangle = \langle p\rangle$ in $\mathcal{R}_p(a,m,\gamma)$ and the element $x^2-\delta$ is nilpotent with nilpotency ap^s.*

Proof. We have that $\mathcal{T}(p,m)\backslash\{0\} \cong \mathbb{F}_{p^m}^*$, and $\mathcal{T}(p,m)\backslash\{0\}$ is generated by ξ. Note that $\gcd(p^s, |\mathbb{F}_{p^m}^*|) = \gcd(p^s, p^m-1) = 1$. This implies that ξ^{p^s} is also a generator of $\mathcal{T}(p,m)\backslash\{0\}$. Then, there exists integer i, $0 \le i \le p^m-1$ such that $\xi^{ip^s} = \xi_0$. Let $\delta = \xi^i$, that is $\delta^{p^s} = \xi_0$.

Case 1: If $p = 2$, by Proposition 3.2 we have

$$\begin{aligned}(x^2-\delta)^{2^s} &= x^{2^{s+1}} + (-\delta)^{2^s} + 2\alpha_s(x) \\ &= \gamma + \delta^{2^s} + 2[(-\delta x^2)^{2^{s-1}} + 2\beta_s(x)]\end{aligned}$$

$$= \xi_0 + 2\xi_1 + 4z + \xi_0 + 2[(\delta x^2)^{2^{s-1}} + 2\beta_s(x)]$$
$$= 2[(\delta x^2)^{s-1} + \xi_0 + \xi_1 + 2(\beta_s(x) + z)].$$

Firstly, we will show that $(\delta x^2)^{2^{s-1}} + \xi_0$ is noninvertible. Suppose that $(\delta x^2)^{2^{s-1}} + \xi_0$ is invertible in $\mathcal{R}_2(a, m, \gamma)$, then

$$(\delta x^2)^{2^{s-1}} - \xi_0 = [(\delta x^2)^{2^{s-1}} + \xi_0] - 2\xi_0,$$

is invertible in $\mathcal{R}_2(a, m, \gamma)$, which implies that $((\delta x^2)^{2^{s-1}} - \xi_0)((\delta x^2)^{2^{s-1}} + \xi_0) = (\delta x^2)^{2^s} - \xi_0^2$ is also invertible in $\mathcal{R}_2(a, m, \gamma)$. This is a contradiction because

$$(\delta x^2)^{2^s} - \xi_0^2 = \delta^{2^s} x^{2^{s+1}} - \xi_0^2 = \xi_0(\xi_0 + 2\xi_1 + 4z) - \xi_0^2 = 2\xi_0\xi_1 + 4\xi_0 z = 2(\xi_0\xi_1 + 2\xi_0 z).$$

Therefore, $(\delta x^2)^{2^{s-1}} - \xi_0$ is noninvertible in $\mathcal{R}_2(a, m, \gamma)$. We can see that $2(\beta_n(x) + z)$ is noninvertible in $\mathcal{R}_2(a, m, \gamma)$, which implies that $\xi_1 + ((\delta x^2)^{2^{s-1}} + \xi_0) + 2(\beta_n(x) + z)$ is invertible. Hence, $\langle (x^2 - \delta)^{2^s} \rangle = \langle 2 \rangle$, and $x^2 - \delta$ has nilpotency $a2^s$.

Case 2: If p is odd, by using Proposition 3.2, again,

$$\begin{aligned}(x^2 - \delta)^{p^s} &= x^{2p^s} + (-\delta)^{p^s} + p(x^2 - \delta)\alpha_s(x)\\ &= \gamma - \delta^{p^s} + p(x^2 - \delta)\alpha_s(x)\\ &= (\xi_0 + p\xi_1 + p^2 z) - \xi_0 + p(x^2 - \delta)\alpha_s(x)\\ &= p(\xi_1 + pz + (x^2 - \delta)\alpha_s(x)).\end{aligned}$$

Since p is nilpotent in $\mathrm{GR}(p^a, m)$, $x^2 - \delta$ is also nilpotent. We get that $pz + (x^2 - \delta)\alpha_s(x)$ is a noninvertible element in $\mathcal{R}_p(a, m, \gamma)$. It implies that $\xi_1 + pz + (x^2 - \delta)\alpha_s(x)$ is invertible. Hence, $\langle (x^2 - \delta)^{p^s} \rangle = \langle p \rangle$, and $x^2 - \delta$ has nilpotency ap^s. □

Proposition 3.4. *Let $\gamma = \xi_0 + p\xi_1 + p^2 z$ be a unit of Type (1) of $\mathrm{GR}(p^a, m)$, where ξ_0, ξ_1 are nonzero elements of $\mathcal{T}(p, m)$ and $z \in \mathrm{GR}(p^a, m)$. Then γ is not a square if and only if ξ_0 is not square.*

Proof. Suppose that γ is not a square. We will prove by contradiction, we assume $\xi_0 = \xi_0'^2$, where $\xi_0' \in \mathcal{T}(p, m)$. Consider

$$\begin{aligned}(\xi_0' + p\xi_1' + p^2 z')^2 &= \xi_0'^2 + p(2\xi_0'\xi_1') + p^2(2\xi_0' z' + \xi_1'^2) + p^3(2\xi_1' z') + p^4 z'^2\\ &= \xi_0'^2 + p(2\xi_0'\xi_1') + p^2\left(2\xi_0' z' + \xi_1'^2 + p(2\xi_1' z') + p^2 z'^2\right).\end{aligned}$$

Since $\xi_0'^{-1}$ exists, we can see that $\xi_0 + p\xi_1 + p^2 z = (\xi_0' + p\xi_1' + p^2 z')^2$, where $\xi_1' = 2^{-1}\xi_0'^{-1}\xi_1$ and $z' = (z - 2\xi_1'^2\xi_1)(2\xi_0' + 2p\xi_1' + p^2 z')^{-1}$, which is a contradiction. Hence ξ_0 is not a square. Conversely, proof by contrapositive, assume that γ is a square. Then, there exists $\gamma' = \xi_0' + p\xi_1' + p^2 z' \in \mathrm{GR}(p^a, m)$ such that

$$\begin{aligned}\gamma = \gamma'^2 &= (\xi_0' + p\xi_1' + p^2 z')^2\\ &= \xi_0'^2 + p(2\xi_0'\xi_1') + p^2(2\xi_0' z' + \xi_1'^2) + p^3(2\xi_1' z') + p^4 z'^2\\ &= \xi_0'^2 + p(2\xi_0'\xi_1') + p^2\left(2\xi_0' z' + \xi_1'^2 + p(2\xi_1' z') + p^2 z'^2\right),\end{aligned}$$

where $\xi_0', \xi_1' \in \mathcal{T}(p,m)$ and $z' \in \mathrm{GR}(p^a,m)$. Thus $\xi_0 + p\xi_1 + p^2 z = \xi_0'^2 + p(2\xi_0'\xi_1') + p^2\left(2\xi_0' z' + \xi_1'^2 + p(2\xi_1' z') + p^2 z'^2\right)$. Comparing coefficients, we have $\xi_0 = \xi_0'^2$. Therefore ξ_0 is a square. $\square$

Proposition 3.5. *Any nonzero linear polynomial $cx + d \in \mathrm{GR}(p^a,m)[x]$ is invertible in $\mathcal{R}_p(a,m,\gamma)$.*

Proof. In $\mathcal{R}_p(a,m,\gamma)$, we have

$$(x+d)^{p^s}(x-d)^{p^s} = (x^2-d^2)^{p^s} = x^{2p^s} - d^{2p^s} = (\xi_0 - d^{2p^s}) + p\xi_1 + p^2 z.$$

Since γ is not a square in $\mathrm{GR}(p^a,m)$, ξ_0 is also not square in $\mathcal{T}(p,m)$. It follows that $\xi_0 - d^{2p^s} + p\xi_1 + p^2 z$ is invertible in $\mathcal{R}_p(a,m,\gamma)$. Thus

$$(x+d)^{-1} = (x+d)^{p^s-1}(x-d)^{p^s}(\xi_0 - d^{2p^s} + p\xi_1 + p^2 z)^{-1}.$$

Therefore, for any $c \neq 0$ in $\mathrm{GR}(p^a,m)$,

$$\begin{aligned}(cx+d)^{-1} &= c^{-1}(x + c^{-1}d)^{-1}\\ &= (x+c^{-1}d)^{p^s-1}(x-c^{-1}d)^{p^s}(\xi_0 - c^{-2p^s}d^{2p^s} + p\xi_1 + p^2 z)^{-1}.\end{aligned}$$

The proof is complete. $\square$

Theorem 3.6. *Let $\gamma = \xi_0 + p\xi_1 + p^2 z$ be a unit of Type (1) of $\mathrm{GR}(p^a,m)$, where ξ_0, ξ_1 are nonzero elements of $\mathcal{T}(p,m)$ and $z \in \mathrm{GR}(p^a,m)$. Then the ring $\mathcal{R}_p(a,m,\gamma)$ is a chain ring with maximal ideal $\langle x^2 - \delta\rangle$, where $\delta^{p^s} = \xi_0$. The γ-constacyclic codes of length $2p^s$ over $\mathrm{GR}(p^a,m)$ are precisely the ideals $\langle (x^2-\delta)^i\rangle$ of the ring $\mathcal{R}_p(a,m,\gamma)$, where $0 \le i \le ap^s$. Each γ-constacyclic code $\langle (x^2-\delta)^i\rangle$ has exactly $p^{2m(ap^s-i)}$ codewords.*

Proof. Let $f(x) \in \mathcal{R}_p(a,m,\gamma)$, then $f(x)$ can be expressed as

$$\begin{aligned}f(x) &= (c_0x + d_0) + (c_1x+d_1)(x^2-\delta) + (c_2x+d_2)(x^2-\delta)^2 + \cdots\\ &\quad + (c_{p^s-1}x + d_{p^s-1})(x^2-\delta)^{p^s-1},\end{aligned}$$

where $c_i, d_i \in \mathrm{GR}(p^a,m)$, $0 \le i \le p^s - 1$. Thus, $f(x)$ is noninvertible if and only if $c_0, d_0 \in p\mathrm{GR}(p^a,m)$. By Lemma 3.3, we have $p \in \langle (x^2-\delta)^{p^s}\rangle \subseteq \langle x^2-\delta\rangle$. We can see that $\langle x^2-\delta\rangle$ is the set of all noninvertible elements of $\mathcal{R}_p(a,m,\gamma)$, which implies that $\mathcal{R}_p(a,m,\gamma)$ is a chain ring with maximal ideal $\langle x^2-\delta\rangle$. Moreover, by Lemma 3.3 again, the nilpotency of $x^2-\delta$ is ap^s, so the ideals of $\mathcal{R}_p(a,m,\gamma)$ are $\langle (x^2-\delta)^i\rangle$, $0 \le i \le ap^s$. The rest of the theorem follows readily from the fact that γ-constacyclic codes of length $2p^s$ over $\mathrm{GR}(p^a,m)$ are ideals of the chain ring $\mathcal{R}_p(a,m,\gamma)$, where γ is a unit of Type (1) of $\mathrm{GR}(p^a,m)$. $\square$

Proposition 3.7. *Let $\gamma = \xi_0 + p\xi_1 + p^2 z \in \mathrm{GR}(p^a,m)$ be a unit of Type (1) of $\mathrm{GR}(p^a,m)$, where ξ_0, ξ_1 are nonzero elements of $\mathcal{T}(p,m)$ and $z \in \mathrm{GR}(p^a,m)$. Let $C = \langle (x^2-\delta)^i\rangle \subseteq \mathcal{R}_p(a,m,\gamma)$ be a γ-constacyclic code of length $2p^s$ over $\mathrm{GR}(p^a,m)$, for some $i \in \{0,1,\ldots,ap^s\}$, where $\delta^{p^s} = \xi_0$. The dual of C is a γ^{-1}-constacyclic code of length $2p^s$ over $\mathrm{GR}(p^a,m)$, and $C^{\perp} = \langle (x^2-\delta^{-1})^{ap^s-i}\rangle \subseteq \mathcal{R}_p(a,m,\gamma^{-1})$ which contains precisely p^{2mi} codewords.*

Proof. By Proposition 2.5, $C^\perp$ is a γ^{-1}-constacyclic code of length $2p^s$ over $\mathrm{GR}(p^a, m)$. By Lemma 2.7, $\gamma^{-1} = \xi_0^{-1} + p\xi' + p^2 z'$ is also a unit of Type (1). Then, Theorem 3.6 is applicable for $C^\perp$ and $\mathcal{R}_p(a, m, \gamma^{-1})$. We can see that $(\delta^{-1})^{p^s} = \xi_0^{-1}$. Thus, $C^\perp$ is an ideal of the form $\langle (x^2 - \delta^{-1})^j \rangle \subseteq \mathcal{R}_p(a, m, \gamma^{-1})$, where $0 \le j \le ap^s$. On the other hand, by Proposition 2.4,

$$|C| \cdot |C^\perp| = |\mathrm{GR}(p^a, m)|^{2p^s} = p^{2amp^s},$$

it implies that

$$|C^\perp| = \frac{p^{2amp^s}}{|C|} = \frac{p^{2amp^s}}{p^{2m(ap^s - i)}} = p^{2mi}.$$

Hence, $C^\perp$ must be the ideal $\langle (x^2 - \delta^{-1})^{ap^s - i} \rangle$ of $\mathcal{R}_p(a, m, \gamma^{-1})$. □

By Proposition 2.5, the dual of a γ-constacyclic code is a γ^{-1}-constacyclic code. So when $\gamma = \gamma^{-1}$, there are situations that require a code to be constacyclic according to two different units. For example, in order for a γ-constacyclic code C to be self-dual ($C = C^\perp$), or self-orthogonal ($C \subseteq C^\perp$), it is necessary for C to be γ- and γ^{-1}-constacyclic. Motivated by this, for any code C is a linear code of length n over a finite ring R such that C is both α- and β-constacyclic code for distinct units α, β of R. Then C is called a *multi-constacyclic code*, or more specifically, an $[\alpha, \beta]$-multi-constacyclic code.

It is known that a code C of length n over a finite field $\mathbb{F}$ is a multi-constacyclic code if and only if $C = \{0\}$ or $C = \mathbb{F}^n$. Over a finite ring R, we have some non-trivial multi-constacyclic codes, as follows.

Proposition 3.8. *Let $\gamma_1 = \xi_0 + p\xi_1 + p^2 z_1$, $\gamma_2 = \xi_0 + p\xi_1' + p^2 z_2$ be two distinct units of Type (1) of $\mathrm{GR}(p^a, m)$, where ξ_0, ξ_1, ξ_1' are nonzero elements of $\mathcal{T}(p, m)$ and $z_1, z_2 \in \mathrm{GR}(p^a, m)$. Let $C = \langle (x^2 - \delta)^i \rangle \subseteq \mathcal{R}_p(a, m, \gamma_1)$ be a γ_1-constacyclic code of length $2p^s$ over $\mathrm{GR}(p^a, m)$. Then C is also a γ_2-constacyclic code, i.e., C is a $[\gamma_1, \gamma_2]$-multi-constacyclic code.*

Proof. By the division algorithm, there exist nonnegative integers j, t such that $i = tp^s + j, 0 \le j < p^s$. Using Lemma 3.3, then we have

$$C = \langle (x^2 - \delta)^i \rangle = \langle (x^2 - \delta)^{tp^s} (x^2 - \delta)^j \rangle = \langle p^t (x^2 - \delta)^j \rangle.$$

Let c be an arbitrary codeword of C, then c has the form $c = p^t(c_0, c_1, \dots, c_{2p^s - 1})$. Since C is a γ_1-constacyclic code, we have

$$\begin{aligned}
&p^t(\gamma_1 c_{2p^s-1}, c_0, \dots, c_{2p^s-2}) \\
&= p^t((\xi_0 + p\xi_1 + p^2 z_1) c_{2p^s-1}, c_0, \dots, c_{2p^s-2}) \\
&= p^t(\xi_0 c_{2p^s-1}, c_0, \dots, c_{2p^s-2}) + p^{t+1}((\xi_1 + p z_1) c_{2p^s-1}, 0, \dots, 0) \in C.
\end{aligned}$$

On the other hand,

$$p^{t+1} \in \langle p^{t+1} \rangle = \langle (x^2 - \delta)^{tp^s + j} \rangle = C.$$

This implies that $(p^{t+1}, 0, \dots, 0) \in C$. Since C is a linear code and $p^{t+1}(\xi_1 + pz_1)c_{2p^s-1}, p^{t+1}(\xi_1' + pz_2) \in \mathrm{GR}(p^a, m)$, we have

$$p^{t+1}((\xi_1 + pz_1)c_{2p^s-1}, 0, \dots, 0) \text{ and } p^{t+1}((\xi_1' + pz_2)c_{2p^s-1}, 0, \dots, 0) \in C,$$

which yields that

$$\begin{aligned} &p^t(\gamma_2 c_{2p^s-1}, c_0, \dots, c_{2p^s-2}) \\ =\ &p^t(\xi_0 c_{2p^s-1}, c_0, \dots, c_{2p^s-2}) + p^{t+1}((\xi_1' + pz_2)c_{2p^s-1}, 0, \dots, 0) \in C. \end{aligned}$$

Thus, C is also a γ_2-constacyclic code. □

Corollary 3.9. *Let $\gamma_1 = \xi_0 + p\xi_1 + p^2 z_1$ and $\gamma_2 = \xi_0 + p\xi_1' + p^2 z_2$ be two units of Type (1) of $\mathrm{GR}(p^a, m)$, where ξ_0, ξ_1, ξ_1' are nonzero elements of $\mathcal{T}(p, m)$ and $z_1, z_2 \in \mathrm{GR}(p^a, m)$. Let $C = \langle (x^2 - \delta)^i \rangle \subseteq \mathcal{R}_p(a, m, \gamma_1)$ be a γ_1-constacyclic code of length $2p^s$ over $\mathrm{GR}(p^a, m)$. Then C is also the ideal $\langle (x^2 - \delta)^i \rangle$ of the ring $\mathcal{R}_p(a, m, \gamma_2)$, i.e., let $c(x) \in \mathrm{GR}(p^a, m)[x]$ be a polynomial of degree less than $2p^s$, then there exists a polynomial $g(x) \in \mathrm{GR}(p^a, m)[x]$ such that $c(x) \equiv g(x)(x^2 - \delta)^i \pmod{x^{2p^s} - \gamma_1}$ if and only if there exists a polynomial $g'(x) \in \mathrm{GR}(p^a, m)$ such that $c(x) \equiv g'(x)(x^2 - \delta)^i \pmod{x^{2p^s} - \gamma_2}$*

Proof. By Proposition 3.8, C is also a γ_2-constacyclic code which contains $p^{2m(ap^s - i)}$ codewords. By Proposition 2.3, C is an ideal of the ring $\mathcal{R}_p(a, m, \gamma_2)$, because γ_2 is of Type (1) and $\delta^{p^s} = \xi_0$. Thus, Theorem 3.6 is applicable for C and $\mathcal{R}_p(a, m, \gamma_2)$. Hence, C is the ideal $\langle (x^2 - \delta)^i \rangle$ of the ring $\mathcal{R}_p(a, m, \gamma_2)$. □

Remark 3.10. Corollary 3.9 gives us very important information about γ-constacyclic codes over $\mathrm{GR}(p^a, m)$, where γ is a unit of Type (1). This corollary shows that the γ-constacyclic codes depend on ξ_0 only, which means that there exist just $p^m - 1$ different codes of length $2p^s$ over $\mathrm{GR}(p^a, m)$ of Type (1).

Theorem 3.11. *Let $\gamma = \xi_0 + p\xi_1 + p^2 z$ be a unit of Type (1) of $\mathrm{GR}(p^a, m)$, where ξ_0, ξ_1 are nonzero elements of $\mathcal{T}(p, m)$ and $z \in \mathrm{GR}(p^a, m)$. Let $\delta^{p^s} = \xi_0$, and let $C = \langle (x^2 - \delta)^i \rangle$ be a γ-constacyclic code of length $2p^s$ over $\mathrm{GR}(p^a, m)$. Then the following statements hold.*

- *If $\xi_0 = \xi_0^{-1}$, then C is a γ-constacyclic self-orthogonal code of length $2p^s$ over $\mathrm{GR}(p^a, m)$ if and only if $\lceil \frac{ap^s}{2} \rceil \le i \le ap^s$.*
- *If $\xi_0 \neq \xi_0^{-1}$, then C is a γ-constacyclic self-orthogonal code of length $2p^s$ over $\mathrm{GR}(p^a, m)$ if and only if $\lceil \frac{a}{2} \rceil p^s \le i \le ap^s$.*

Proof. By Proposition 3.7, the dual of C is

$$C^\perp = \langle (x^2 - \delta^{-1})^{ap^s - i} \rangle \subseteq \mathcal{R}_p(a, m, \gamma^{-1}).$$

If C is self-orthogonal, then $|C| < |C^\perp|$. It follows that $2i \ge ap^s$.

Case 1: If $\xi_0 = \xi_0^{-1}$, by Proposition 3.8, $C^\perp$ is also a γ-constayclic code. We can see that $\delta^{p^s} = \xi_0 = \xi_0^{-1} = (\delta^{-1})^{p^s}$ and by Corollary 3.9, we get that $C^\perp = \langle (x^2 - \delta)^{ap^s - i} \rangle \subseteq \mathcal{R}_p(a, m, \gamma)$. Hence, C is self-orthogonal if and only if $\langle (x^2 - \delta)^i \rangle \subseteq \langle (x^2 - \delta)^{ap^s - i} \rangle$ if and only if $\lceil \frac{ap^s}{2} \rceil \le i \le ap^s$.

Case 2: If $\xi_0 \neq \xi_0^{-1}$, by Proposition 2.6 and Lemma 2.7, $\xi_0 - \xi_0^{-1}$ is invertible in $\mathrm{GR}(p^a, m)$ and $\gamma^{-1} = \xi_0^{-1} + p\xi_1' + p^2 z'$. Now we consider the polynomial $x^2 - \delta$ in $\mathcal{R}_p(a, m, \gamma^{-1})$.

Case 2.1. If $p = 2$, by Proposition 3.2, we have

$$\begin{aligned}(x^2-\delta)^{2^s} &= x^{2^{s+1}} + \delta^{2^s} + 2\alpha_s(x)\\ &= \gamma^{-1} + \xi_0 + 2\alpha_s(x)\\ &= \xi_0^{-1} + 2\xi_1' + 4z' + \xi_0 + 2\alpha_s(x)\\ &= \xi_0 + \xi_0^{-1} + 2(\xi_1^{-1} + 2z' + \alpha_s(x)).\end{aligned}$$

Case 2.2. If p is odd, using Proposition 3.2 again, we get that

$$\begin{aligned}(x^2-\delta)^{p^s} &= x^{2p^s} + (-\delta)^{2p^s} + p(x^2-\delta)\beta_s(x)\\ &= \gamma^{-1} - \xi_0 + p(x^2-\delta)\beta_s(x)\\ &= \xi_0^{-1} - \xi_0 + p(\xi_1' + pz' + (x^2-\delta)\beta_s(x)).\end{aligned}$$

This implies that $(x^2-\delta)^{p^s}$ is invertible in $\mathcal{R}_p(a, m, \gamma^{-1})$. Hence, $x^2-\delta$ is also invertible in $\mathcal{R}_p(a, m, \gamma^{-1})$. By the division algorithm, there exist nonnegative integers t and j such that $i = tp^s + j$, $0 \leq i < p^s$ and by Lemma 3.3, we have

$$C = \langle (x^2-\delta)^i \rangle = \langle p^t (x^2-\delta)^j \rangle$$

and

$$C^\perp = \langle (x^2-\delta^{-1})^{ap^s - i} \rangle = \langle p^{a-t-1}(x^2-\delta^{-1})^{p^s-j} \rangle.$$

If $j = 0$, then $C = C^\perp$ if and only if $t \geq \lceil \frac{a}{2} \rceil$ if and only if $i \geq p^s \lceil \frac{a}{2} \rceil$.

Next, we assume that $j \neq 0$.

If $t < a - t - 1$, then $|C| > |C^\perp|$, and hence, in this case C is not self-orthogonal.

If $t = a - t - 1$ and suppose that $C \subseteq C^\perp$ then $p^t(x^2-\delta)^j \in C^\perp$, which implies that $p^t \in C^\perp$, because $x^2 - \delta$ is invertible in $\mathcal{R}_p(a, m, \gamma^{-1})$. Then $j = 0$ and so C is not self-orthogonal in this case either.

If $t \geq a - t$, then

$$p^t \in \langle p^{a-t} \rangle = \langle (x^2-\delta^{-1})^{p^s(a-t)} \rangle \subseteq \langle p^{a-t-1}(x^2-\delta^{-1})^{p^s-j} \rangle = C^\perp.$$

Therefore, C is self-orthogonal if and only if $t \geq a-t$ if and only if $i \geq p^s \lceil \frac{a}{2} \rceil$. □

Corollary 3.12. *Let $\gamma = \xi_0 + p\xi_1 + p^2 z$ be a unit of Type (1) of $\mathrm{GR}(p^a, m)$, where ξ_0, ξ_1 are nonzero elements of $\mathcal{T}(p, m)$ and $z \in \mathrm{GR}(p^a, m)$. Then the following statements hold.*

- *If $\xi_0 = \xi_0^{-1}$, then there exists a self-dual γ-constacyclic code of length $2p^s$ over $\mathrm{GR}(p^a, m)$ if and only if ap is even. In this case, $\langle (x^2-\delta)^{\frac{ap^s}{2}} \rangle$ is the unique self-dual γ-constacyclic code of length $2p^s$ over $\mathrm{GR}(p^a, m)$.*
- *If $\xi_0 \neq \xi_0^{-1}$, then there exists a self-dual γ-constacyclic code of length $2p^s$ over $\mathrm{GR}(p^a, m)$ if and only if a is even. In this case, $p^{\frac{a}{2}}$ is the unique self-dual γ-constacyclic code of length $2p^s$ over $\mathrm{GR}(p^a, m)$.*

Proof. Let C be a γ-constacyclic code of length $2p^s$ over $\mathrm{GR}(p^a, m)$, then $C = \langle (x^2 - \delta)^i \rangle$ and $C^{\perp} = \langle (x^2 - \delta^{-1})^{ap^s - i} \rangle$, where $0 \leq i \leq ap^s$. Note that $C = C^{\perp}$ if and only if $|C| = |C^{\perp}|$ and $C \subseteq C^{\perp}$. If $|C| = |C^{\perp}|$, then $i = ap^s - i$. The rest of the proof follows from Theorem 3.11.

If $\xi_0 \neq \xi_0^{-1}$ and a is an odd number or $\xi_0 = \xi_0^{-1}$ and ap is odd, by Theorem 3.11, if C is self-orthogonal, then $ap^s - i < i$. Hence, self-dual γ-constacyclic codes do not exist in this case. □

4. Rosenbloom-Tsfasman distance

In 1997, Rosenbloom and Tsfasman [25] introduced a new distance in coding theory, which was later named after them as the Rosenbloom-Tsfasman (RT) distance. Well-known bounds for distances such as the Singleton bound, the Plotkin bound, the Hamming bound, and the Gilbert-Varshamov bound were derived for the RT distance. Since then, there are many other studies focusing on codes with respect to this RT metric (see, for example, [7, 13, 16, 24]).

For any finite commutative ring R, the *Rosenbloom-Tsfasman weight* (RT weight) (see [25]) of an n-tuple $c = (c_0, c_1, \dots, c_{n-1}) \in R^n$ is defined as follows:

$$\mathrm{wt}_{\mathrm{RT}}(c) = \begin{cases} 1 + \max\{j | c_j \neq 0\} & \text{if } \ c \neq 0, \\ 0 & \text{if } \ c = 0. \end{cases}$$

The RT distance of any two n-tuple c, c' of R^n is defined as:

$$d_{\mathrm{RT}}(c, c') = \mathrm{wt}_{\mathrm{RT}}(c - c').$$

Let C be a code of length n over R. Then

$$d_{\mathrm{RT}}(C) = \min\{d_{RT}(c, c') \mid c, c' \in C \text{ and } c \neq c'\}$$

is a called the *RT distance* of C.

In this section we consider the RT distances of all γ-constacyclic codes of length $2p^s$ over the ring $\mathrm{GR}(p^a, m)$ for any unit γ of Type (1) of $\mathrm{GR}(p^a, m)$ such that γ is not a square, and p is an odd prime. We start with the definition of the RT weight as the following.

Proposition 4.1. *Let $c = (c_0, c_1, \dots, c_{n-1}) \in \mathrm{GR}(p^a, m)^n$ be a word of length n over $\mathrm{GR}(p^a, m)$, and $c(x)$ be its polynomial presentation. Then*

$$\mathrm{wt}_{\mathrm{RT}}(x) = \begin{cases} 1 + \deg(c(x)) & \textit{if } \ c \neq 0, \\ 0 & \textit{if } \ c = 0. \end{cases}$$

Theorem 4.2. *Let γ be a unit of Type (1) of $\mathrm{GR}(p^a, m)$ such that γ is not a square. Assume that C is a γ-constacyclic code of length $2p^s$ over $\mathrm{GR}(p^a, m)$, i.e., $C = \langle (x^2 - \delta)^i \rangle \subseteq \mathcal{R}_p(a, m, \gamma)$ for some $i \in \{0, 1, \dots, ap^s\}$. Then the RT* *distance* $d_{\mathrm{RT}}(C)$ *is completely determined as follows.*

$$d_{\mathrm{RT}}(x) = \begin{cases} 0 & \textit{if} \;\; ap^s, \\ 1 & \textit{if} \;\; 0 \le i \le (a-1)p^s, \\ 2i - 2(a-1)p^s + 1 & \textit{if} \;\; (a-1)p^s \le i \le ap^s - 1. \end{cases}$$

Proof. **Case 1**: If $i = ap^s$, the code C is the zero code, and the result follows trivially.

Case 2: If $0 \le i \le (a-1)p^s$, by Lemma 3.3 and Theorem 3.6, then

$$\langle (x^2-\delta)^i \rangle \supseteq \langle (x^2-\delta)^{(a-1)p^s} \rangle = \langle p^{a-1} \rangle,$$

which implies that the RT distance of the code $\langle (x^2-\delta)^i \rangle$ is 1.

Case 3: If $(a-1)p^s \le i \le ap^s - 1$, then

$$\langle (x^2-\delta)^i \rangle = \langle (x^2-\delta)^{(a-1)p^s} (x^2-\delta)^{i-(a-1)p^s} \rangle = \langle p^{a-1} (x^2-\delta)^{i-(a-1)p^s} \rangle.$$

We get that $\langle p^{a-1}(x^2-\delta)^{i-(a-1)p^s} \rangle$ has the generator polynomial $p^{a-1}(x^2 - \delta)^{i-(a-1)p^s}$ is of smallest degree, which is $2i - 2(a-1)p^s$. By Proposition 4.1, its RT distance is $2i-2(a-1)p^s+1$. Suppose that $f(x)$ is a nonzero polynomial in $\langle p^{a-1}(x^2-\delta)^{i-(a-1)p^s} \rangle$ of degree $0 \le k \le 2i - 2(a-1)p^s$, then $f(x)$ can be expressed as

$$f(x) = \sum_{j=0}^{k} (c_j x + d_j)(x^2-\delta)^j,$$

where $c_j, d_j \in \mathrm{GR}(p^a, m)$. Let l $(0 \le l \le k)$ be the smallest index such that $c_l x + d_l \neq 0$, then

$$f(x) = (x^2-\delta)^l \sum_{j=l}^{k} (c_j x + d_j)(x^2-\delta)^{j-l} = (x^2-\delta)^l (c_l x + d_l)[1 + (x^2-\delta) g(x)],$$

where $g(x) \in \mathcal{R}_p(a, m, \gamma)$ and

$$g(x) = \begin{cases} 0 & \text{if} \;\; l = k, \\ (c_l x - d_l)^{-1} \sum\limits_{j=l+1}^{k} (c_j x + d_j)(x^2-\delta)^{j-l-l} & \text{if} \;\; 0 \le l < k. \end{cases}$$

In $\mathcal{R}_p(a, m, \gamma)$, we have $x^2 - \delta$ is nilpotent, there is an odd integer t such that $(x^2-\delta)^t = 0$, we get

$$\begin{aligned} 1 &= 1 + [(x^2-\delta)g(x)]^t \\ &= [1 + (x^2-\delta)g(x)][1 - (x^2-\delta)g(x) + (x^2-\delta)^2 g(x)^2 - \cdots \\ &\quad + (x^2-\delta)^{t-1} g(x)^{t-1}]. \end{aligned}$$

Thus, $1 + (x^2-\delta)g(x)$ is invertible in $\mathcal{R}_p(a, m, \gamma)$. Hence, $f(x) = (x^2-\delta)^l h(x)$ for some unit $h(x)$ of $\mathcal{R}_p(a, m, \gamma)$. It implies that $f(x) \in \langle (x^2-\delta)^l \rangle$, but $f(x) \notin (x^2-\delta)^{l+1}$, and in particular, $f(x) \notin C$. Thus, we have any nonzero polynomial of degree less than $2i-2(a-1)p^s$ is not in C, i.e., the smallest degree of nonzero polynomials in C is $2i-2(a-1)p^s$ as desired. □

Proposition 4.3. *For $(a-1)p^s+1 \le i \le ap^s-1$, the RT weight distribution of Type (1) γ-constacyclic code $\langle (x^2-\delta)^i\rangle \subseteq \mathcal{R}_p(a,m,\gamma)$ is as follows.*

$$\mathcal{A}_j = \begin{cases} 1 & \text{if } j=0, \\ 0 & \text{if } 1 \le j \le 2i-2(a-1)p^s, \\ (p^m-1)p^{mk} & \text{if } j = 2i-2(a-1)p^s+1+k \text{ for } 0 \le k \le 2ap^s-2i-1, \end{cases}$$

where $\mathcal{A}_j$ is the number of codewords of RT weight j of $\langle (x^2-\delta)^i\rangle$.

Proof. From the proof of Theorem 4.2, when $(a-1)p^s+1 \le i \le ap^s-1$, $\langle (x^2-\delta)^i\rangle = \langle p^{a-1}(x^2-\delta)^{i-(a-1)p^s}\rangle$, and so $\mathcal{A}_j = 0$ for $1 \le j \le 2i-2(a-1)p^s$. When $2i-2(a-1)p^s+1 \le j \le 2p^s$, say, $j = 2i-2(a-1)p^s+1+k$, for $0 \le k \le 2ap^s-2i-1$, then $\mathcal{A}_j$ is the number of distinct polynomials of degree k in $\mathcal{T}(p,m)[x]$. □

When $i = p^s t$, $0 \le t \le a-1$, by Lemma 3.3, the ideals $\langle (x^2-\delta)^i\rangle = \langle p^t\rangle \subseteq \mathcal{R}_p(a,m,\gamma)$. Thus, we get their weight distributions as follows.

Proposition 4.4. *For $i = p^s t$, $0 \le t \le a-1$, the RT weight distribution of Type (1) γ-constacyclic code $\langle (x^2-\delta)^i\rangle \subseteq \mathcal{R}_p(a,m,\gamma)$ is as follows.*

$$\mathcal{A}_j = \begin{cases} 1 & \text{if } \ j=0, \\ (p^{m(a-t)}-1)p^{m(a-t)(j-1)} & \text{if } \ 1 \le j \le 2p^s, \end{cases}$$

where $\mathcal{A}_j$ is the number of codewords of RT weight j of $\langle (x^2-\delta)^i\rangle$.

Proposition 4.5. *Let $1 \le b \le a-1$. For $(b-1)p^s+1 \le i \le bp^s-1$, the RT weight distribution of Type (1) γ-constacyclic code $\langle (x^2-\delta)^i\rangle \subseteq \mathcal{R}_p(a,m,\gamma)$ is as follows.*

$$\mathcal{A}_j = \begin{cases} 1 \\ \text{if } \ j=0, \\ (p^{m(a-b)}-1)p^{m(a-b)(j-1)} \\ \text{if } \ 1 \le j \le 2i-2(b-1)p^s, \\ (p^{2m(a-b)p^s})(p^m-1)p^{mk} + (p^{m(a-b)}-1)p^{m(a-b)(j-1)} \\ \text{if } \ j = 2i-2(b-1)p^s+1+k, \ \text{for } 0 \le k \le 2bp^s-2i-1, \end{cases}$$

where $\mathcal{A}_j$ is the number of codewords of RT weight j of $\langle (x^2-\delta)^i\rangle$.

Proof. Since $(b-1)p^s+1 \le i \le (b-1)p^s+p^s-1$, it means that $1 \le i-(b-1)p^s \le p^s-1$, so by Lemma 3.3,

$$\langle p^{b-1}(x^2-\delta)\rangle \supseteq \langle (x^2-\delta)^i\rangle = \langle p^{b-1}(x^2-\delta)^{i-p^s(b-1)}\rangle \supseteq \langle p^{b-1}(x^2-\delta)^{p^s-1}\rangle \supsetneq \langle p^b\rangle.$$

Let $\mathcal{B}_j$ be the number of codewords of RT weight j of $\langle (x^2-\delta)^i \rangle$, which are not in $\langle p^b \rangle$ and $\mathcal{B}'_j$ be the number of codewords of RT weight j of $\langle p^b \rangle$. Then, for all j, $\mathcal{A}_j = \mathcal{B}_j + \mathcal{B}'_j$. Similar to Proposition 4.3, we have

$$\mathcal{B}_j = \begin{cases} 0 & \text{if } \ j = 0, \\ 0 & \text{if } \ 1 \le j \le 2i - 2(b-1)p^s, \\ p^{2m(a-b)p^s}(p^m - 1)p^{mk} & \text{if } \ j = 2i - 2(b-1)p^s + 1 + k, \\ & \quad \text{for } 0 \le k \le 2bp^s - 2i - 1. \end{cases}$$

By Proposition 4.4, we can see that

$$B'_j = \begin{cases} 1 & \text{if } \ j = 0, \\ (p^{m(a-b)} - 1)p^{(a-b)(j-1)} & \text{if } \ 1 \le j \le 2p^s. \end{cases}$$

Hence

$$A_j = \begin{cases} 1 \\ \text{if } \ j = 0, \\ (p^{m(a-b)} - 1)p^{m(a-b)(j-1)} \\ \text{if } \ 1 \le j \le 2i - 2(b-1)p^s, \\ (p^{2m(a-b)p^s})(p^m - 1)p^{mk} + (p^{m(a-b)} - 1)p^{m(a-b)(j-1)} \\ \text{if } \ j = 2i - 2(b-1)p^s + 1 + k, \text{ for } \ 0 \le k \le 2bp^s - 2i - 1. \end{cases}$$

The proof is complete. □

Remark 4.6. Propositions 4.3, 4.4 and 4.5 give us the RT weight distributions for all Type (1) γ-constacyclic code $C_i = \langle (x^2-\delta)^i \rangle \subseteq \mathcal{R}_p(a, m, \gamma)$ of length $2p^s$ over $\mathrm{GR}(p^a, m)$. By Theorem 3.6, $|C_i| = p^{2m(ap^s - i)}$. As $|C_i| = \sum_{j=0}^{2p^s} A_j$, these RT weight distributions can be used to verify the size $|C_i|$ of such codes.

- If $(a-1)p^s + 1 \le i \le ap^s - 1$, then

$$\begin{aligned} |C_i| &= \sum_{j=0}^{2p^s} A_j \\ &= 1 + \sum_{k=0}^{2ap^s-2i-1} (p^m - 1)p^{mk} \\ &= 1 + (p^m - 1) \sum_{k=0}^{2ap^s-2i-1} (p^m)^k \\ &= 1 + (p^m - 1)\frac{p^{m(2ap^s-2i)} - 1}{p^m - 1} \\ &= p^{2m(ap^s - i)}. \end{aligned}$$

- If $i = p^s t$, $0 \leq t \leq a-1$, then

$$\begin{aligned}|C_i| &= \sum_{j=0}^{2p^s} A_j \\ &= 1 + \sum_{j=1}^{2p^s} (p^{m(a-t)} - 1) p^{m(a-t)(j-1)} \\ &= 1 + (p^{m(a-t)} - 1) \sum_{j=0}^{2p^s - 1} p^{m(a-t)j} \\ &= 1 + (p^{m(a-t)} - 1) \frac{p^{m(a-t)2p^s} - 1}{p^{m(a-t)} - 1} \\ &= p^{2m(a-t)p^s} \\ &= p^{2m(ap^s - i)}.\end{aligned}$$

- If $(b-1)p^s + 1 \leq i \leq bp^s - 1$, where $1 \leq b \leq a-1$, then

$$\begin{aligned}|C_i| &= \sum_{j=0}^{2p^s} A_j \\ &= 1 + \sum_{j=1}^{2p^s - 2(b-1)p^s} (p^{m(a-b)} - 1) p^{m(a-b)(j-1)} \\ &\quad + \sum_{k=0}^{2p^s - 2i - 1} p^{2m(a-b)p^s} (p^m - 1) p^{mk} \\ &\quad + \sum_{j=2i-2(b-1)p^s+1}^{2p^s} (p^{m(a-b)} - 1) p^{m(a-b)(j-1)} \\ &= 1 + (p^{m(a-b)} - 1) \sum_{j=0}^{2p^s - 1} p^{m(a-b)j} + p^{2m(a-b)p^s} (p^m - 1) \sum_{k=0}^{2bp^s - 2i - 1} p^{mk} \\ &= 1 + (p^{m(a-b)} - 1) \frac{p^{m(a-b)2p^s} - 1}{p^{m(a-b)} - 1} + p^{2m(a-b)p^s} (p^m - 1) \frac{p^{m(2bp^s - 2i)} - 1}{p^m - 1} \\ &= 1 + (p^{m(a-b)bp^s} - 1) + p^{2m(a-b)p^s} (p^{m(2bp^s - 2i)} - 1) \\ &= p^{2m(ap^s - i)}.\end{aligned}$$

5. Conclusion

Let $\mathrm{GR}(p^a, m)$ be the Galois extension of degree m of the ring $\mathbb{Z}_{p^a}$. Let γ be a unit of Type (1) of $\mathrm{GR}(p^a, m)$, i.e., it is of the form $\xi_0 + p\xi_1 + p^2 z$, where ξ_0, ξ_1 are nonzero elements of the set $\mathcal{T}(p, m)$ and $z \in \mathrm{GR}(p^a, m)$. We obtain Type (1) γ-constacyclic codes of length $2p^s$ over $\mathrm{GR}(p^a, m)$, when γ is a square, i.e., $\gamma = \alpha^2$ for some $\alpha \in \mathrm{GR}(p^a, m)$. Then, we get that an ideal C of $\frac{\mathrm{GR}(p^a,m)[x]}{\langle x^{2p^s}-\gamma\rangle}$, is represented as a direct sum of $C_{-\alpha}$ and C_α, where $C_{-\alpha}$ and C_α are ideals of $\frac{\mathrm{GR}(p^a,m)[x]}{\langle x^{p^s}+\alpha\rangle}$ and $\frac{\mathrm{GR}(p^a,m)[x]}{\langle x^{p^s}-\alpha\rangle}$, respectively, that is, they are $-\alpha$ and α-constacyclic codes of length p^s over $\mathrm{GR}(p^a, m)$, respectively. In the remaining case, when γ is not a square in $\mathrm{GR}(p^a, m)$, we can show that the ring $\frac{\mathrm{GR}(p^a,m)[x]}{\langle x^{2p^s}-\gamma\rangle}$ is a chain ring with maximal ideal $\langle x^2 - \delta\rangle$, where $\delta^{p^s} = \xi_0$. Furthermore, γ-constacyclic codes of length $2p^s$ over $\mathrm{GR}(p^a, m)$ are precisely the ideals $\langle (x^2 - \delta)^i\rangle$ of the ring $\frac{\mathrm{GR}(p^a,m)[x]}{\langle x^{2p^s}-\gamma\rangle}$, where $0 \le i \le ap^s$, and the number of codewords of all Type (1) γ-constacyclic code are provided. We also derive the duals of all such γ-constacyclic codes as well as necessary and sufficient conditions for the existence of selforthogonal and self-dual γ-constacyclic codes. Finally, we use the algebraic structure above to established the Rosenbloom-Tsfasman (RT) distances and weight distributions of all such codes.

Acknowledgement. The authors would like to thank Naresuan University and Science Achievement Scholarship of Thailand, which provides supporting for research. We are also thank the referees for careful reading and the useful comments and suggestions.

References

[1] T. Abualrub and R. Oehmke, *On the generators of $\mathbb{Z}_4$ cyclic codes of length 2^e*, IEEE Trans. Inform. Theory **49** (2003), no. 9, 2126–2133.

[2] E. R. Berlekamp, *Negacyclic codes for the Lee metric*, in Combinatorial Mathematics and its Applications (Proc. Conf., Univ. North Carolina, Chapel Hill, N.C., 1967), 298–316, Univ. North Carolina Press, Chapel Hill, NC, 1969.

[3] S. D. Berman, *Semisimple cyclic and Abelian codes. II*, Cybernetics **3** (1967), no. 3, 17–23 (1970).

[4] T. Blackford, *Negacyclic codes over Z_4 of even length*, IEEE Trans. Inform. Theory **49** (2003), no. 6, 1417–1424.

[5] A. R. Calderbank, A. R. Hammons, P.V. Kumar, N. J. A. Sloane, and P. Solé, *A linear construction for certain Kerdock and Preparata codes*, Bull. Amer. Math. Soc. (N.S.) **29** (1993), no. 2, 218–222.

[6] G. Castagnoli, J. L. Massey, P. A. Schoeller, and N. von Seemann, *On repeated-root cyclic codes*, IEEE Trans. Inform. Theory **37** (1991), no. 2, 337–342.

[7] B. Chen, L. Lin, and H. Liu, *Matrix product codes with Rosenbloom-Tsfasman metric*, Acta Math. Sci. Ser. B (Engl. Ed.) **33** (2013), no. 3, 687–700.

[8] H. Q. Dinh, *Negacyclic codes of length 2^s over Galois rings*, IEEE Trans. Inform. Theory **51** (2005), no. 12, 4252–4262.

[9] ______, *Constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$*, J. Algebra **324** (2010), no. 5, 940–950.

[10] H. Q. Dinh, H. Liu, X. Liu, and S. Sriboonchitta, *On structure and distances of some classes of repeated-root constacyclic codes over Galois rings*, Finite Fields Appl. **43** (2017), 86–105.

[11] H. Q. Dinh and S. R. López-Permouth, *Cyclic and negacyclic codes over finite chain rings*, IEEE Trans. Inform. Theory **50** (2004), no. 8, 1728–1744.

[12] S. T. Dougherty and S. Ling, *Cyclic codes over $\mathbb{Z}_4$ of even length*, Des. Codes Cryptogr. **39** (2006), no. 2, 127–153.
[13] S. T. Dougherty and M. M. Skriganov, *MacWilliams duality and the Rosenbloom-Tsfasman metric*, Mosc. Math. J. **2** (2002), no. 1, 81–97, 199.
[14] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, *The $\mathbf{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Inform. Theory **40** (1994), no. 2, 301–319.
[15] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, Cambridge, 2003.
[16] K. Lee, *The automorphism group of a linear space with the Rosenbloom-Tsfasman metric*, European J. Combin. **24** (2003), no. 6, 607–612.
[17] H. Liu and Y. Maouche, *Some repeated-root constacyclic codes over Galois rings*, IEEE Trans. Inform. Theory **63** (2017), no. 10, 6247–6255.
[18] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1998.
[19] B. R. McDonald, *Finite Rings with Identity*, Marcel Dekker, Inc., New York, 1974.
[20] A. A. Nechaev, *Kerdock code in a cyclic form*, Discrete Math. Appl. **1** (1991), no. 4, 365–384; translated from Diskret. Mat. **1** (1989), no. 4, 123–139.
[21] C.-S. Nedeloaia, *Weight distributions of cyclic self-dual codes*, IEEE Trans. Inform. Theory **49** (2003), no. 6, 1582–1591.
[22] V. Pless and W. C. Huffman, *Handbook of Coding Theory*, Elsevier, Amsterdam, 1998.
[23] A. Sălăgean, *Repeated-root cyclic and negacyclic codes over a finite chain ring*, Discrete Appl. Math. **154** (2006), no. 2, 413–419.
[24] M. M. Skriganov, *On linear codes with large weights simultaneously for the Rosenbloom-Tsfasman and Hamming metrics*, J. Complexity **23** (2007), no. 4-6, 926–936.
[25] M. Yu. Rozenblyum and M. A. Tsfasman, *Codes for the m-metric*, Probl. Inf. Transm. **33** (1997), no. 1, 45–52; translated from Problemy Peredachi Informatsii **33** (1997), no. 1, 55–63.
[26] L. Tang, C. B. Soh, and E. Gunawan, *A note on the q-ary image of a q^m-ary repeated-root cyclic code*, IEEE Trans. Inform. Theory **43** (1997), no. 2, 732–737.
[27] J. H. van Lint, *Repeated-root cyclic codes*, IEEE Trans. Inform. Theory **37** (1991), no. 2, 343–345.
[28] J. Wolfmann, *Negacyclic and cyclic codes over Z_4*, IEEE Trans. Inform. Theory **45** (1999), no. 7, 2527–2532.

Chakkrid Klin-eam
Department of Mathematics
Faculty of Science
Naresuan University
Phitsanulok 65000, Thailand
Email address: chakkridk@nu.ac.th

Wateekorn Sriwirach
Department of Mathematics
Faculty of Science
Naresuan University
Phitsanulok 65000, Thailand
Email address: wateekorns@hotmail.com