mathematics

MDPI

Article

Structure and Enumeration of Constacyclic Codes over Cube-Zero Local Rings of Order q^5

Sami H. Saif * and Shayea Aldossari

Mathematics Department, King Saud University, P.O. Box 2455, Riyadh 11451, Saudi Arabia; shaaldossari@ksu.edu.sa
* Correspondence: ssaif1@ksu.edu.sa

Abstract

We investigate λ-constacyclic codes of length n over finite commutative local rings R of characteristic p and order q^5, where $q = p^m$ is an odd prime power, whose Jacobson radical $\mathcal{N}$ satisfies $\mathcal{N}^3 = 0 \neq \mathcal{N}^2$, under the coprimality condition $\gcd(n, p) = 1$. In this setting, exactly two radical types occur, namely $(3, 1)$ and $(2, 2)$, determined by the dimensions of $\mathcal{N}/\mathcal{N}^2$ and $\mathcal{N}^2$. For each type, we provide an explicit classification of the underlying rings and analyze the induced radical filtration of the ambient algebra $A_\lambda = R[X]/\langle X^n - \lambda \rangle$. We prove that every λ-constacyclic code is uniquely determined by its residual component in $A_\lambda/\mathrm{J}(A_\lambda)$ together with two torsion components arising from the radical chain $\mathrm{J}(A_\lambda) \supset \mathrm{J}(A_\lambda)^2 \supset 0$. This residual–torsion decomposition yields explicit generating sets; in particular, every λ-constacyclic code admits a generating set consisting of at most five elements. Furthermore, we derive exact enumeration formulas for all λ-constacyclic codes. In the type $(2, 2)$ case, the enumeration is governed by linear-algebraic constraints over the Chinese Remainder Theorem residue fields and, in the anisotropic class, depends on quadratic character values determined by the extension degrees. In the type $(3, 1)$ case, the enumeration is controlled by the dimension of the radical of the induced symmetric bilinear form on the top radical layer, equivalently by the rank class of the associated canonical matrix.

Keywords: local commutative finite ring; Frobenius rings; codes over rings; constacyclic codes; isomorphism classes

MSC: 13H99; 94B15; 94B60

1. Introduction

Linear codes over finite rings extend classical coding theory beyond the finite-field setting and provide a natural framework for investigating algebraic phenomena arising from nontrivial radicals and non-chain ideal structures. In contrast to the field case, the behavior of cyclic and constacyclic codes over rings is strongly influenced by the internal structure of the ambient algebra, particularly the Jacobson radical and its associated filtration; see [1–4] for general background on finite local rings. While constacyclic codes over finite *chain rings* are now well understood, we refer to [5–8] for representative results; the corresponding theory over *non-chain* local rings remains substantially more intricate due to the interaction of multiple radical layers and a significantly richer lattice of ideals (see [9,10] for related work in this direction).

Check for updates

Academic Editor: Irina Cristea

Received: 2 March 2026
Revised: 5 April 2026
Accepted: 7 April 2026
Published: 9 April 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

Algebraically, a λ-constacyclic code of length n over a finite ring R is an ideal of the quotient algebra

$$A_\lambda = R[X]/\langle X^n - \lambda \rangle, \qquad \lambda \in R^\times. \tag{1}$$

Its structure depends simultaneously on the multiplicative structure of R, the radical filtration of R, and the factorization of $X^n - \bar{\lambda}$ over the residue field $R/\mathcal{N}$, where $\mathcal{N}$.

A complete structural and enumerative description of constacyclic codes over local Frobenius non-chain rings of order p^4 with nilpotency index three was obtained in [11]. The present work extends this line of research to Frobenius and non-Frobenius rings of order $q^5 = p^{5m}$, where $m \geq 1$. The cases of smaller cardinality are more rigid: for orders q^2, q^3, and q^4, the possible local structures under comparable nilpotency assumptions are much more limited, whereas the order q^5 case is the first one in which the two distinct radical types, $(3,1)$ and $(2,2)$, occur simultaneously. Thus, this is the first setting in which the classification and enumeration problems split into two genuinely different algebraic types, leading to new structural and enumerative phenomena that do not arise in smaller orders. Related investigations of constacyclic and other classes of codes over local rings are found in [9,12].

Throughout the paper, R denotes a finite commutative local ring of order $|R| = q^5$, where $q = p^m$ with p odd, whose Jacobson radical $\mathcal{N}$ satisfies

$$\mathcal{N}^3 = 0 \neq \mathcal{N}^2. \tag{2}$$

This cube-zero condition yields exactly two possible radical types,

$$\left(\dim_{\mathbb{F}_q}(\mathcal{N}/\mathcal{N}^2),\ \dim_{\mathbb{F}_q}(\mathcal{N}^2)\right) \in \{(3,1),(2,2)\},$$

which induce fundamentally different multiplicative structures on the top radical layer and consequently distinct constacyclic code architectures.

Our first main contribution is a complete classification of all such rings in terms of matrix-based invariants. For type $(3,1)$, multiplication on $\mathcal{N}/\mathcal{N}^2 \cong \mathbb{F}_q^3$ is encoded by a nonzero symmetric matrix $A \in \mathrm{Sym}_3(\mathbb{F}_q)$, considered up to projective congruence

$$A \sim \theta\, U^T A U, \qquad U \in \mathrm{GL}_3(\mathbb{F}_q),\ \theta \in \mathbb{F}_q^\times,$$

yielding four canonical isomorphism classes in odd characteristic. For type $(2,2)$, multiplication corresponds to a two-dimensional subspace $L \subseteq \mathrm{Sym}_2(\mathbb{F}_q)$ modulo congruence. The associated determinant locus

$$\Sigma(L) = \{(\alpha:\beta) \in \mathbb{P}^1(\mathbb{F}_q) : \det(\alpha A + \beta B) = 0\}$$

serves as a complete invariant distinguishing the canonical classes. Thus, the classification naturally connects the structure theory of finite local rings with projective geometry and the theory of matrix pencils.

Under the coprimality condition $\gcd(n,p) = 1$, the polynomial $X^n - \bar{\lambda}$ is separable over $\mathbb{F}_q$, and the Chinese Remainder Theorem decomposes A_λ into local components. Using the induced radical filtration,

$$A_\lambda \supset \mathrm{J}(A_\lambda) \supset \mathrm{J}(A_\lambda)^2 \supset 0,$$

we prove that every λ-constacyclic code admits a *residual–torsion decomposition*. Each code is uniquely determined by its residual component together with two torsion layers, leading

to explicit generator descriptions. In particular, every code over R can be generated by at most five polynomials.

The enumeration problem then reduces to local counting over the residue fields

$$K_i = \mathbb{F}_q[X]/\langle f_i(X)\rangle,$$

arising from the factorization $X^n - \bar{\lambda} = \prod_{i=1}^{t} f_i(X)$. For radical type $(2,2)$, the counting is governed by linear-algebraic data attached to the canonical class of R, whereas for type $(3,1)$ it depends on quadratic invariants determined by the rank structure of the associated bilinear form. Consequently, even for fixed length and factor degrees, the total number of constacyclic codes depends on the isomorphism class of the underlying ring.

The significance of this work is twofold. First, it shows that relatively small cube-zero local rings already exhibit a rich interplay between ring structure, matrix congruence theory, and coding theory. Second, the matrix-based realization developed here demonstrates that constacyclic codes over non-chain and non-Frobenius rings can be studied via geometric and tensorial invariants arising from bilinear forms and projective spaces. This perspective provides a unified structural framework and opens the way to the systematic investigation of codes over matrix-defined local algebras and higher-nilpotency settings.

This paper is organized as follows. Section 3 classifies finite commutative local rings of order q^5 satisfying $\mathcal{N}^3 = 0 \neq \mathcal{N}^2$. In particular, Sections 3.1 and 3.2 treat the two radical types $(3,1)$ and $(2,2)$ separately and determine their canonical classes. Section 4 studies the ambient ring A_λ and develops the structural theory of λ-constacyclic codes via the residual–torsion decomposition, including the corresponding generator description. Section 5 derives the explicit enumeration formulas by combining the structural results with the CRT decomposition. Sections 5.1 and 5.2 deal with the enumeration for the types $(3,1)$ and $(2,2)$, respectively, and they conclude with illustrative examples for the various ring classes.

2. Preliminaries

Throughout the paper, let p be an odd prime and let $q = p^m$ with $m \geq 1$. Denote by $\mathbb{F}_q$ the finite field with q elements. All rings are assumed to be finite, commutative, and unital of characteristic p. For a finite ring R, we write $\mathcal{N}$ for its Jacobson radical. We restrict attention to commutative local rings R with residue field

$$R/\mathcal{N} \cong \mathbb{F}_q,$$

and for $r \in R$, we denote its residue class in $\mathbb{F}_q$ by $\bar{r}$.

We consider finite commutative local rings R of cardinality $|R| = q^5$ whose Jacobson radical satisfies

$$\mathcal{N}^3 = 0 \qquad \text{and} \qquad \mathcal{N}^2 \neq 0. \tag{3}$$

Thus, R admits a cube-zero radical filtration

$$R \supset \mathcal{N} \supset \mathcal{N}^2 \supset 0, \tag{4}$$

with exactly two nonzero radical layers. Since $R/\mathcal{N} \cong \mathbb{F}_q$, we have $\dim_{\mathbb{F}_q}(R/\mathcal{N}) = 1$, and hence,

$$\dim_{\mathbb{F}_q} R = 5 \quad \text{and} \quad \dim_{\mathbb{F}_q} \mathcal{N} = 4.$$

From the short exact sequence

$$0 \longrightarrow \mathcal{N}^2 \longrightarrow \mathcal{N} \longrightarrow \mathcal{N}/\mathcal{N}^2 \longrightarrow 0 \tag{5}$$

it follows that

$$\dim_{\mathbb{F}_q}(\mathcal{N}/\mathcal{N}^2) + \dim_{\mathbb{F}_q}(\mathcal{N}^2) = 4. \tag{6}$$

Because $\mathcal{N}^2 \neq 0$ and $\mathcal{N} \neq \mathcal{N}^2$, both summands are positive. Therefore,

$$\left(\dim_{\mathbb{F}_q}(\mathcal{N}/\mathcal{N}^2),\ \dim_{\mathbb{F}_q}(\mathcal{N}^2)\right) \in \{(3,1),(2,2)\}. \tag{7}$$

These two possibilities exhaust all finite commutative local rings of order q^5 satisfying (3).

A useful consequence of $\mathcal{N}^3 = 0$ that will be employed repeatedly is

$$\mathcal{N}^2\mathcal{N} = 0,$$

so every element of $\mathcal{N}^2$ annihilates $\mathcal{N}$. For further background in this ring-theoretic setting, we refer to [13,14].

Let $\lambda \in R^\times$ and let $n \geq 1$ satisfy $\gcd(n,p) = 1$. A *λ-constacyclic code of length n over R* is an ideal of the ambient algebra

$$A_\lambda = R[X]/\langle X^n - \lambda\rangle. \tag{8}$$

The coprimality condition ensures that $X^n - \bar{\lambda}$ is square-free in $\mathbb{F}_q[X]$. Hence, its factorization into distinct monic irreducible polynomials admits Hensel lifts to $R[X]$. Consequently, the Chinese Remainder Theorem yields a decomposition of A_λ into a finite direct product of local components, and the structure of λ-constacyclic codes reduces to the description of ideals in these components. Background on codes over finite rings may be found in [10,15].

Since R satisfies $\mathcal{N}^3 = 0 \neq \mathcal{N}^2$, the induced radical filtration of A_λ has the form

$$A_\lambda \supset \mathrm{J}(A_\lambda) \supset \mathrm{J}(A_\lambda)^2 \supset 0, \tag{9}$$

and this filtration interacts naturally with the semisimple quotient

$$A_\lambda/\mathrm{J}(A_\lambda) \cong \mathbb{F}_q[X]/\langle X^n - \bar{\lambda}\rangle. \tag{10}$$

This structure provides the algebraic framework for the residual–torsion description and the enumeration of λ-constacyclic codes developed in the subsequent sections.

Finally, Gaussian binomial coefficients arise in the enumeration of constacyclic codes. For integers $0 \leq t \leq d$ and prime power q, the q-binomial coefficient is defined by

$$\binom{d}{t}_q = \frac{(q^d-1)(q^d-q)\cdots(q^d-q^{t-1})}{(q^t-1)(q^t-q)\cdots(q^t-q^{t-1})}, \tag{11}$$

and counts the t-dimensional $\mathbb{F}_q$-subspaces of an d-dimensional vector space over $\mathbb{F}_q$, (see [16]). These coefficients will be used to enumerate subspaces that parameterize the constacyclic codes of the component rings introduced below.

Throughout the paper, $\langle\cdot\rangle$ denotes the ideal generated by the indicated elements.

3. Structural Classification of Local Rings of Order q^5 with $\mathcal{N}^3 = 0$

In this section, we determine the precise structure of finite commutative local rings R of order q^5 whose Jacobson radical $\mathcal{N}$ satisfies $\mathcal{N}^3 = 0 \neq \mathcal{N}^2$. Using the notation and framework introduced in Section 2, we showed that the radical filtration

$$R \supset \mathcal{N} \supset \mathcal{N}^2 \supset 0$$

forces exactly two possible graded dimension types for R, namely

$$\left(\dim_{\mathbb{F}_q}(\mathcal{N}/\mathcal{N}^2), \dim_{\mathbb{F}_q}(\mathcal{N}^2)\right) \in \{(3,1),(2,2)\}.$$

These two cases lead to distinct algebraic configurations, which we analyze separately and classify explicitly via canonical matrix representations.

Lemma 1. *Let R be a ring and let $I \subseteq R$ be a nilpotent ideal, and suppose I is nilpotent with $I^t = 0$. The, n an element $\omega \in R$ is a unit if and only if its image in R/I is a unit. In particular, if $R/I \cong \mathbb{F}_q$, then*

$$R^\times = \mathbb{F}_q^\times + I.$$

Moreover, if $a \in R$ maps to $\bar{a} \in (R/I)^\times$ and $u \in I$, then

$$(a+u)^{-1} = a^{-1} \sum_{k=0}^{t-1} (-a^{-1}u)^k.$$

Proof. Let $\pi : R \to R/I$ denote the canonical projection. If $\omega \in R^\times$, then clearly $\pi(\omega) \in (R/I)^\times$.

Conversely, suppose that $\pi(\omega)$ is a unit in R/I. Then, there exists $\omega_1 \in R$ such that $\pi(\omega\omega_1) = 1$, and hence

$$\omega\omega_1 = 1 + v \quad \text{for some } v \in I.$$

Since I is nilpotent, we have $v^t = 0$. Therefore,

$$(1+v)\left(\sum_{k=0}^{t-1}(-v)^k\right) = 1,$$

so $1+v$ is a unit with inverse $\sum_{k=0}^{t-1}(-v)^k$. Consequently,

$$\omega \cdot \left(\omega_1 \sum_{k=0}^{t-1}(-v)^k\right) = 1,$$

which shows that ω is a unit in R.

For the explicit formula, write $\omega = a + u$ with a mapping to a unit in R/I and $u \in I$. Then

$$a + u = a(1 + a^{-1}u),$$

where $a^{-1}u \in I$. Applying the previous argument to $1 + a^{-1}u$ yields

$$(1 + a^{-1}u)^{-1} = \sum_{k=0}^{t-1}(-a^{-1}u)^k,$$

and multiplying by a^{-1} gives the desired expression. □

3.1. Characterization for the Type $(3,1)$

Throughout this subsection, let R be a finite commutative local ring with maximal ideal $\mathcal{N}$ and residue field $R/\mathcal{N} \cong \mathbb{F}_q$, satisfying

$$|R| = q^5, \qquad \mathcal{N}^3 = 0 \neq \mathcal{N}^2, \qquad \dim_{\mathbb{F}_q}(\mathcal{N}/\mathcal{N}^2) = 3, \qquad \dim_{\mathbb{F}_q}(\mathcal{N}^2) = 1.$$

Choose elements $x, y, z \in \mathcal{N} \setminus \mathcal{N}^2$ whose images form an $\mathbb{F}_q$-basis of $\mathcal{N}/\mathcal{N}^2$, and choose $0 \neq w \in \mathcal{N}^2$ so that $\mathcal{N}^2 = \mathbb{F}_q w$. Then, as ideals of R, we have

$$\mathcal{N} = \langle x, y, z, w \rangle, \qquad \mathcal{N}^2 = \langle z, w \rangle.$$

Since $\mathcal{N}^3 = 0$, we have $\mathcal{N}^2\mathcal{N} = 0$, and in particular

$$w^2 = wx = wy = wz = 0. \tag{12}$$

Moreover, the products of x, y, z lie in $\mathcal{N}^2 = \mathbb{F}_q w$, so there exist unique scalars $a_{ij} \in \mathbb{F}_q$ such that, with $(x_1, x_2, x_3) = (x, y, z)$,

$$x_i x_j = a_{ij} w, \qquad 1 \le i, j \le 3. \tag{13}$$

Commutativity of R implies $a_{ij} = a_{ji}$, so the matrix $A = (a_{ij})$ belongs to $\mathrm{Sym}_3(\mathbb{F}_q)$.

Lemma 2. *With the above choice of generators, we have $A \neq 0$.*

Proof. Suppose, for contradiction, that $A = 0$. Then $x_i x_j = 0$ for all i, j. Together with $w\mathcal{N} = 0$ from (12), this implies that every product of two elements of $\mathcal{N}$ is zero, and hence $\mathcal{N}^2 = 0$, contradicting the assumption that $\mathcal{N}^2 \neq 0$. □

We now classify rings of type $(3, 1)$ up to projective congruence of the associated symmetric matrix A.

Theorem 1. *Let $A = (a_{ij}) \in \mathrm{Sym}_3(\mathbb{F}_q)$ be nonzero. Define the $\mathbb{F}_q$-vector space*

$$R(A) = \mathbb{F}_q + x\mathbb{F}_q + y\mathbb{F}_q + z\mathbb{F}_q + w\mathbb{F}_q,$$

with multiplication determined by $\mathbb{F}_q$-bilinearity, 1 as the identity, commutativity, and the relations (12) and (13). Then,

(i) $R(A)$ is a finite commutative local ring of order q^5 with maximal ideal $\mathcal{N} = \langle x, y, z, w \rangle$ satisfying

$$\mathcal{N}^2 = \mathbb{F}_q w, \quad \mathcal{N}^3 = 0 \neq \mathcal{N}^2, \quad \dim_{\mathbb{F}_q}(\mathcal{N}/\mathcal{N}^2) = 3.$$

(ii) Conversely, every commutative local ring R of type $(3, 1)$ is isomorphic to $R(A)$ for some nonzero $A \in \mathrm{Sym}_3(\mathbb{F}_q)$.

(iii) For nonzero $A, A' \in \mathrm{Sym}_3(\mathbb{F}_q)$,

$$R(A) \cong R(A') \iff A' = \theta\, U^T A U \text{ for some } U \in \mathrm{GL}_3(\mathbb{F}_q),\ \theta \in \mathbb{F}_q^\times.$$

Proof. We prove the claims in several steps.

Step 1: Well-defined ring structure. Multiplication is specified on the basis $\{1, x, y, z, w\}$ and extended $\mathbb{F}_q$-bilinearly, so it is well-defined and distributive. Commutativity is imposed by definition.

To check associativity, consider basis elements:

(i) If one factor is 1, associativity holds trivially.
(ii) If one factor is w, then any product involving w is 0 by (12), so associativity holds.
(iii) If all three factors are in $\{x, y, z\}$, then the product of any two lies in $\mathbb{F}_q w$ by (13), and multiplying by the third gives 0 by (12). Both parenthesizations vanish, so associativity holds.

Step 2: As an $\mathbb{F}_q$-vector space, $\dim_{\mathbb{F}_q} R(A) = 5$, so $|R(A)| = q^5$. Let $\mathcal{N} = \langle x, y, z, w \rangle$. Then $R(A)/\mathcal{N} \cong \mathbb{F}_q$, so $\mathcal{N}$ is maximal. Since $\mathcal{N}^3 = 0$, Lemma 1 implies that elements of the

form $a+u$ with $a \in \mathbb{F}_q^\times$ and $u \in \mathcal{N}$ are units, while elements in $\mathcal{N}$ are not. Hence, $R(A)$ is local with maximal ideal $\mathcal{N}$.

Step 3: Through (13) and (12), products of elements of $\mathcal{N}$ lie in $\mathbb{F}_q w$, so $\mathcal{N}^2 \subseteq \mathbb{F}_q w$. Since $A \neq 0$, some $x_i x_j = a_{ij} w \neq 0$, implying $w \in \mathcal{N}^2$. Therefore, $\mathcal{N}^2 = \mathbb{F}_q w \neq 0$, and clearly $\mathcal{N}^3 = (\mathbb{F}_q w)\mathcal{N} = 0$. By construction, $\dim_{\mathbb{F}_q}(\mathcal{N}/\mathcal{N}^2) = 3$.

Step 4: Let R be any type $(3,1)$ ring. Choose generators x, y, z, w as above. Relations (12) and (13) hold, and the corresponding $A \in \mathrm{Sym}_3(\mathbb{F}_q)$ is nonzero (Lemma 2). Define $\psi : R(A) \to R$ by sending the basis $\{1, x, y, z, w\}$ of $R(A)$ to these elements of R. This $\mathbb{F}_q$-linear bijection preserves multiplication and is hence an isomorphism.

Step 5: Let $\varphi : R(A) \to R(A')$ be a ring isomorphism. Then, $\varphi(\mathcal{N}) = \mathcal{N}'$ and $\varphi(\mathcal{N}^2) = \mathcal{N}'^2$. Since $\mathcal{N}^2 = \mathbb{F}_q w$ and $\mathcal{N}'^2 = \mathbb{F}_q w'$, there exists $\theta \in \mathbb{F}_q^\times$ such that

$$\varphi(w) = \theta\, w'. \tag{14}$$

The induced map on $\mathcal{N}/\mathcal{N}^2$ is an $\mathbb{F}_q$-linear isomorphism, represented by some $U \in \mathrm{GL}_3(\mathbb{F}_q)$ in the bases $\{\bar{x}, \bar{y}, \bar{z}\}$ and $\{\overline{x'}, \overline{y'}, \overline{z'}\}$. Equivalently, lifting to $\mathcal{N}'$, we may write

$$\begin{pmatrix} \varphi(x) \\ \varphi(y) \\ \varphi(z) \end{pmatrix} = U \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} + \begin{pmatrix} r_1 \\ r_2 \\ r_3 \end{pmatrix} w' \qquad \text{for some } r_1, r_2, r_3 \in \mathbb{F}_q. \tag{15}$$

Because $\mathcal{N}'^2 \mathcal{N}' = 0$, the w'-parts do not affect products of two elements from $\mathcal{N}'$. Applying φ to $x_i x_j = a_{ij} w$ yields

$$\varphi(x_i)\varphi(x_j) = \varphi(x_i x_j) = a_{ij}\, \varphi(w) = \theta a_{ij}\, w'$$

by (14). On the other hand, using (15) and bilinearity gives

$$\varphi(x_i)\varphi(x_j) = \Big(\sum_k u_{ki} x'_k + r_i w'\Big)\Big(\sum_\ell u_{\ell j} x'_\ell + r_j w'\Big) = \Big(\sum_k u_{ki} x'_k\Big)\Big(\sum_\ell u_{\ell j} x'_\ell\Big),$$

since all terms containing w' vanish (because $w'\mathcal{N}' = 0$). Thus,

$$\varphi(x_i)\varphi(x_j) = \sum_{k,\ell} u_{ki} u_{\ell j}\, x'_k x'_\ell = \sum_{k,\ell} u_{ki} u_{\ell j}\, a'_{k\ell}\, w' = (U^T A' U)_{ij}\, w'.$$

Comparing coefficients of w' gives $U^T A' U = \theta A$, and equivalently, $A' = \theta\, (U^{-1})^T A (U^{-1})$. Setting $V = U^{-1} \in \mathrm{GL}_3(\mathbb{F}_q)$ yields $A' = \theta\, V^T A V$, as claimed.

Step 6: Conversely, suppose $A' = \theta\, U^T A U$ with $U \in \mathrm{GL}_3(\mathbb{F}_q)$ and $\theta \in \mathbb{F}_q^\times$. Define $\varphi : R(A) \to R(A')$ by $\varphi(1) = 1$,

$$\begin{pmatrix} \varphi(x) \\ \varphi(y) \\ \varphi(z) \end{pmatrix} = U \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix}, \qquad \varphi(w) = \theta\, w'.$$

Then, φ is an $\mathbb{F}_q$-linear bijection. Moreover,

$$\varphi(x_i)\varphi(x_j) = \sum_{k,\ell} u_{ki} u_{\ell j} x'_k x'_\ell = \sum_{k,\ell} u_{ki} u_{\ell j} a'_{k\ell} w' = (U^T A' U)_{ij} w' = \theta a_{ij} w' = a_{ij} \varphi(w) = \varphi(x_i x_j),$$

and products involving w map to 0 because $w\mathcal{N} = 0$ and $w'\mathcal{N}' = 0$. Hence, φ preserves multiplication on generators, and thus on all of $R(A)$. Therefore, φ is a ring isomorphism. □

The following theorem determines explicit projective normal forms for type $(3,1)$ over $\mathbb{F}_q$.

Theorem 2. *Assume* $\mathrm{char}(\mathbb{F}_q) \neq 2$ *and fix a nonsquare* $\vartheta \in \mathbb{F}_q^\times$. *Let* R *be a finite local ring with* $|R| = q^5$ *and* $\mathcal{N}^3 = 0 \neq \mathcal{N}^2$, *of radical type* $(3,1)$. *Then,* R *is isomorphic to exactly one of the following four rings:*

$$A_{(3,1)}^{(1)} = \mathrm{diag}(1,0,0) \iff R_{(3,1)}^{(1)} = \frac{\mathbb{F}_q[x,y,z,w]}{\left\langle \begin{array}{llll} x^2-w, & y^2, & z^2, & \\ xy, & xz, & yz, & \\ w^2, & wx, & wy, & wz \end{array} \right\rangle};$$

$$A_{(3,1)}^{(2)} = \mathrm{diag}(1,1,0) \iff R_{(3,1)}^{(2)} = \frac{\mathbb{F}_q[x,y,z,w]}{\left\langle \begin{array}{llll} x^2-w, & y^2-w, & z^2, & \\ xy, & xz, & yz, & \\ w^2, & wx, & wy, & wz \end{array} \right\rangle};$$

$$A_{(3,1)}^{(3)} = \mathrm{diag}(1,\vartheta,0) \iff R_{(3,1)}^{(3)} = \frac{\mathbb{F}_q[x,y,z,w]}{\left\langle \begin{array}{llll} x^2-w, & y^2-\vartheta w, & z^2, & \\ xy, & xz, & yz, & \\ w^2, & wx, & wy, & wz \end{array} \right\rangle};$$

$$A_{(3,1)}^{(4)} = \mathrm{diag}(1,1,1) \iff R_{(3,1)}^{(4)} = \frac{\mathbb{F}_q[x,y,z,w]}{\left\langle \begin{array}{llll} x^2-w, & y^2-w, & z^2-w, & \\ xy, & xz, & yz, & \\ w^2, & wx, & wy, & wz \end{array} \right\rangle}.$$

These four rings are pairwise non-isomorphic.

Proof. According to Theorem 1, the isomorphism classes of type $(3,1)$ rings are in bijection with projective congruence classes of nonzero matrices $A \in \mathrm{Sym}_3(\mathbb{F}_q)$, where

$$A \sim A' \iff A' = \theta\, U^T A U \quad \text{for some } U \in \mathrm{GL}_3(\mathbb{F}_q),\ \theta \in \mathbb{F}_q^\times.$$

Assume $\mathrm{char}(\mathbb{F}_q) \neq 2$. Over a finite field of odd characteristic, every symmetric matrix is congruent to a diagonal matrix (see, for instance, [17]). Hence, every nonzero $A \in \mathrm{Sym}_3(\mathbb{F}_q)$ is congruent to

$$\mathrm{diag}(\alpha_1, \alpha_2, \alpha_3), \qquad \alpha_i \in \mathbb{F}_q,$$

with $\alpha_i \neq 0$ for $1 \leq i \leq r = \mathrm{rank}(A)$ and $\alpha_i = 0$ for $i > r$.

Rank 1. If $r = 1$, then A is congruent to $\mathrm{diag}(1,0,0)$. Projective scaling does not produce new classes, so there is a single projective class in rank 1.

Rank 2. If $r = 2$, then A is congruent to $\mathrm{diag}(1,\delta,0)$ with $\delta \in \mathbb{F}_q^\times$. Under ordinary congruence, two such forms are equivalent if and only if δ differs by a square in $\mathbb{F}_q^\times$. Projective scaling multiplies both diagonal entries by θ, which does not alter the square-class of δ. Hence, there are exactly two projective classes in rank 2, represented by

$$\mathrm{diag}(1,1,0) \quad \text{and} \quad \mathrm{diag}(1,\vartheta,0),$$

where ϑ is a fixed nonsquare in $\mathbb{F}_q^\times$.

Rank 3. If $r = 3$, then A is nondegenerate. Over $\mathbb{F}_q$ with q odd, nondegenerate quadratic forms in dimension 3 have two ordinary congruence classes distinguished by $\det(A) \in \mathbb{F}_q^\times/(\mathbb{F}_q^\times)^2$. Under projective scaling $A \mapsto \theta A$, one has

$$\det(\theta A) = \theta^3 \det(A).$$

Since 3 is odd, multiplication by θ^3 ranges over both square and nonsquare classes as θ varies over $\mathbb{F}_q^\times$. Thus, the two ordinary congruence classes become equivalent under projective congruence. Consequently, there is a single projective class in rank 3, represented by $\mathrm{diag}(1,1,1)$.

Collecting all cases, the projective congruence classes of nonzero matrices in $\mathrm{Sym}_3(\mathbb{F}_q)$ are exactly

$$\mathrm{diag}(1,0,0), \quad \mathrm{diag}(1,1,0), \quad \mathrm{diag}(1,\vartheta,0), \quad \mathrm{diag}(1,1,1).$$

Substituting each diagonal representative into the defining relations $x_i x_j = a_{ij} w$ and using $w\mathcal{N} = 0$ produces the four corresponding ring presentations. Since the rank and, in the rank 2 case, the square-class invariant are preserved under projective congruence, these four classes are distinct. Hence, the associated rings are pairwise non-isomorphic. □

Remark 1. *When* $\mathrm{char}(\mathbb{F}_q) \neq 2$*, projective congruence may collapse distinct ordinary congruence classes. In particular, in odd dimension (*3 *here), the two ordinary congruence classes of nondegenerate symmetric forms (distinguished by* $\det(A)$ *modulo squares) become projectively congruent because scaling by a nonsquare changes the determinant square-class by a factor of* θ^3*. For later sections, the invariant formulation in Theorem 1 is typically sufficient; explicit representatives are only needed for tabulation.*

3.2. Characterization for the Type $(2,2)$

In this subsection, we assume $\dim_{\mathbb{F}_q}(\mathcal{N}/\mathcal{N}^2) = 2, \dim_{\mathbb{F}_q}(\mathcal{N}^2) = 2$. Choose elements

$$x, y \in \mathcal{N} \setminus \mathcal{N}^2, \qquad z, w \in \mathcal{N}^2, \tag{16}$$

such that $\bar{x}, \bar{y}$ form an $\mathbb{F}_q$-basis of $\mathcal{N}/\mathcal{N}^2$ and z, w form an $\mathbb{F}_q$-basis of $\mathcal{N}^2$. Then,

$$\mathcal{N} = \langle x, y, z, w \rangle, \qquad \mathcal{N}^2 = \langle z, w \rangle. \tag{17}$$

With the above choice of generators, we have

$$z^2 = w^2 = zw = zx = zy = wx = wy = 0, \tag{18}$$

and there exist unique $a_{ij}, b_{ij} \in \mathbb{F}_q$ such that

$$x^2 = a_{11} z + b_{11} w, \qquad y^2 = a_{22} z + b_{22} w, \qquad xy = a_{12} z + b_{12} w. \tag{19}$$

Defining

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{12} & a_{22} \end{pmatrix}, \qquad B = \begin{pmatrix} b_{11} & b_{12} \\ b_{12} & b_{22} \end{pmatrix}. \tag{20}$$

Changing the basis of $\mathcal{N}/\mathcal{N}^2$ by $U \in \mathrm{GL}_2(\mathbb{F}_q)$ replaces (A, B) by $(U^T A U, U^T B U)$, while changing the basis of $\mathcal{N}^2$ replaces (A, B) by another ordered basis of the same two-dimensional subspace

$$L = \langle A, B \rangle \subseteq \mathrm{Sym}_2(\mathbb{F}_q). \tag{21}$$

Next, we show that the isomorphism class of R is determined by the $\mathrm{GL}_2(\mathbb{F}_q)$-orbit of the two-dimensional subspace L.

Lemma 3. *The matrices $A, B \in \mathrm{Sym}_2(\mathbb{F}_q)$ are linearly independent over $\mathbb{F}_q$.*

Proof. The annihilation relations (18) follow from $\mathcal{N}^2\mathcal{N} = 0$. Since $x, y \in \mathcal{N}$, we have $x^2, y^2, xy \in \mathcal{N}^2$, so they have unique expansions in the basis $\{z, w\}$, giving (19). Commutativity implies $xy = yx$, so A and B are symmetric.

Finally, $\mathcal{N}^2$ is spanned by products of elements of $\mathcal{N}$. Because any product involving a factor from $\mathcal{N}^2$ is zero, $\mathcal{N}^2$ is spanned by x^2, y^2, xy. Since $\dim_{\mathbb{F}_q} \mathcal{N}^2 = 2$, these products do not all lie in a one-dimensional $\mathbb{F}_q$-subspace of $\mathcal{N}^2$. Equivalently, their coordinate vectors in the basis (z, w) span $\mathbb{F}_q^2$, which forces A and B to be linearly independent. □

Lemma 4. *Let $L \subseteq \mathrm{Sym}_2(\mathbb{F}_q)$ be a 2-dimensional $\mathbb{F}_q$-subspace. Then L contains a matrix of nonzero determinant.*

Proof. Assume every nonzero $M \in L$ is singular. Choose $0 \neq M \in L$. Then $\mathrm{rank}(M) = 1$, so there exists $U \in \mathrm{GL}_2(\mathbb{F}_q)$ with $U^T M U = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$. Replacing L by $U^T L U$ preserves the hypothesis, so assume $M = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) \in L$. Choose $N = \left(\begin{smallmatrix} a & b \\ b & c \end{smallmatrix}\right) \in L$ linearly independent from M. Every element of L has the form

$$\alpha M + \beta N = \begin{pmatrix} \alpha + \beta a & \beta b \\ \beta b & \beta c \end{pmatrix}.$$

Its determinant equals $\alpha\beta c + \beta^2(ac - b^2)$ and must vanish for all $(\alpha, \beta) \neq (0, 0)$. Fix $\beta \neq 0$; then, this determinant is an affine linear function of α, and hence, its α-coefficient must be zero, forcing $c = 0$. Then $ac - b^2 = 0$ gives $b = 0$; hence, $N = \mathrm{diag}(a, 0) = aM$, contradicting the choice of N. □

The next lemma investigates the change of generators and the induced action on (A, B).

Lemma 5. *Maintain the type $(2, 2)$ assumptions and notation of Lemma 3. Let (x', y') be another pair in $\mathcal{N} \setminus \mathcal{N}^2$ whose images form a basis of $\mathcal{N}/\mathcal{N}^2$, and let (z', w') be another basis of $\mathcal{N}^2$. Then there exist $U \in \mathrm{GL}_2(\mathbb{F}_q)$ and $T \in \mathrm{GL}_2(\mathbb{F}_q)$ such that*

$$\begin{pmatrix} x' \\ y' \end{pmatrix} \equiv U \begin{pmatrix} x \\ y \end{pmatrix} \pmod{\mathcal{N}^2}, \qquad \begin{pmatrix} z' \\ w' \end{pmatrix} = T \begin{pmatrix} z \\ w \end{pmatrix}.$$

Writing $T^{-1} = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$, the matrix pair (A, B) associated with $(x, y; z, w)$ transforms to the pair (A', B') associated with $(x', y'; z', w')$ via

$$(A', B') = \left(U^T A U,\ U^T B U\right) \cdot T^{-1} = \left(\alpha\, U^T A U + \beta\, U^T B U,\ \gamma\, U^T A U + \delta\, U^T B U\right). \tag{22}$$

Equivalently, the $\mathbb{F}_q$-subspace $L = \langle A, B \rangle \subseteq \mathrm{Sym}_2(\mathbb{F}_q)$ is well-defined up to congruence $L \mapsto U^T L U$, and the ordered basis (A, B) of L is well-defined up to a $\mathrm{GL}_2(\mathbb{F}_q)$-change of basis.

Proof. Since $\bar{x}, \bar{y}$ and $\overline{x'}, \overline{y'}$ are bases of the two-dimensional $\mathbb{F}_q$-space $\mathcal{N}/\mathcal{N}^2$, there exists $U = (u_{ij}) \in \mathrm{GL}_2(\mathbb{F}_q)$ such that $\left(\begin{smallmatrix} \bar{x}' \\ \bar{y}' \end{smallmatrix}\right) = U\left(\begin{smallmatrix} \bar{x} \\ \bar{y} \end{smallmatrix}\right)$, i.e., $\left(\begin{smallmatrix} x' \\ y' \end{smallmatrix}\right) \equiv U\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) \pmod{\mathcal{N}^2}$. Likewise, since (z, w) and (z', w') are bases of $\mathcal{N}^2$, there exists $T \in \mathrm{GL}_2(\mathbb{F}_q)$ with $\left(\begin{smallmatrix} z' \\ w' \end{smallmatrix}\right) = T\left(\begin{smallmatrix} z \\ w \end{smallmatrix}\right)$. Lift the congruence to write

$$x' = u_{11}x + u_{12}y + u_1, \qquad y' = u_{21}x + u_{22}y + u_2, \qquad u_1, u_2 \in \mathcal{N}^2.$$

Using $\mathcal{N}^2\mathcal{N} = 0$, every cross-term involving u_1 or u_2 vanishes in products with x or y. Hence

$$(x')^2 = (u_{11}x + u_{12}y)^2, \qquad (y')^2 = (u_{21}x + u_{22}y)^2, \qquad x'y' = (u_{11}x + u_{12}y)(u_{21}x + u_{22}y).$$

Expanding these products and using (19) shows that, relative to the old basis (z, w) of $\mathcal{N}^2$, the pair (A, B) transforms to $(U^T AU, U^T BU)$.

Finally, rewriting the same products in the new basis (z', w') amounts to applying T^{-1} to the coordinate column, which is precisely (22). The last sentence is a restatement: U acts by congruence on L, while T changes the ordered basis of L. □

We are now ready to give the classification of type $(2, 2)$ rings of order q^5.

Theorem 3. *Assume* $\mathrm{char}(\mathbb{F}_q) \neq 2$ *and fix a non-square* $\vartheta \in \mathbb{F}_q^\times$. *Let*

$$\Sigma(L) = \{(\alpha : \beta) \in \mathbb{P}^1(\mathbb{F}_q) : \det(\alpha A + \beta B) = 0\}.$$

Then, $|\Sigma(L)| \in \{2, 1, 0\}$ *and* R *is isomorphic to exactly one of the following three rings:*

$$(A^{(1)}_{(2,2)}, B^{(1)}_{(2,2)}) = \left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\right) \Longleftrightarrow R^{(1)}_{(2,2)} = \frac{\mathbb{F}_q[x, y, z, w]}{\left\langle \begin{array}{llll} x^2 - z, & y^2 - w, & xy, & \\ z^2, & w^2, & zw, & \\ zx, & zy, & wx, & wy \end{array} \right\rangle};$$

$$(A^{(2)}_{(2,2)}, B^{(2)}_{(2,2)}) = \left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\right) \Longleftrightarrow R^{(2)}_{(2,2)} = \frac{\mathbb{F}_q[x, y, z, w]}{\left\langle \begin{array}{llll} x^2 - w, & y^2, & xy - z, & \\ z^2, & w^2, & zw, & \\ zx, & zy, & wx, & wy \end{array} \right\rangle};$$

$$(A^{(3)}_{(2,2)}, B^{(3)}_{(2,2)}) = \left(\begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right) \Longleftrightarrow R^{(3)}_{(2,2)} = \frac{\mathbb{F}_q[x, y, z, w]}{\left\langle \begin{array}{llll} x^2 - z, & y^2 - \vartheta z, & xy - w, & \\ z^2, & w^2, & zw, & \\ zx, & zy, & wx, & wy \end{array} \right\rangle}.$$

Moreover,

$$|\Sigma(L)| = 2 \Longleftrightarrow R \cong R^{(1)}_{(2,2)}, \qquad |\Sigma(L)| = 1 \Longleftrightarrow R \cong R^{(2)}_{(2,2)}, \qquad |\Sigma(L)| = 0 \Longleftrightarrow R \cong R^{(3)}_{(2,2)}.$$

These three rings are pairwise non-isomorphic.

Proof. We proceed carefully, making each reduction explicit.

Step 1: Lemma 3 provides generators x, y, z, w and an associated linearly independent pair $(A, B) \in \mathrm{Sym}_2(\mathbb{F}_q)^2$ encoding the products x^2, y^2, xy.
Step 2: Through Lemma 5, changing the chosen generators in $\mathcal{N}/\mathcal{N}^2$ and $\mathcal{N}^2$ transforms (A, B) by (22). Equivalently, the isomorphism class of R is determined by the congruence class of the 2-dimensional subspace $L = \langle A, B\rangle \subseteq \mathrm{Sym}_2(\mathbb{F}_q)$ under $L \mapsto U^T LU$ with $U \in \mathrm{GL}_2(\mathbb{F}_q)$.
Step 3: Fix an ordered basis (A, B) of L and consider

$$\Delta(\alpha, \beta) = \det(\alpha A + \beta B) \in \mathbb{F}_q[\alpha, \beta],$$

a homogeneous quadratic polynomial. If we replace (A, B) by another ordered basis of L, then (α, β) undergoes an invertible linear change of variables, so the projective zero set

$$\Sigma(L) = \{(\alpha : \beta) \in \mathbb{P}^1(\mathbb{F}_q) : \Delta(\alpha, \beta) = 0\}$$

depends only on L. If we replace L by $U^T L U$, then

$$\det(\alpha(U^T A U) + \beta(U^T B U)) = \det(U)^2 \det(\alpha A + \beta B),$$

so $\Sigma(L)$ is unchanged. Hence, $\Sigma(L)$ is an isomorphism invariant of R.

We now show that Δ is not identically zero. By Lemma 4, the 2-dimensional subspace L contains an invertible matrix, so for some (α, β) we have $\det(\alpha A + \beta B) \neq 0$. Therefore, Δ is nonzero, and the conic $\Delta(\alpha, \beta) = 0$ in $\mathbb{P}^1(\mathbb{F}_q)$ has either two distinct points, one double point, or no $\mathbb{F}_q$-point. Consequently,

$$|\Sigma(L)| \in \{2, 1, 0\}.$$

Step 4: Assume $\Sigma(L)$ has two distinct points. Then there exist two linearly independent singular matrices $M_1, M_2 \in L$, spanning two distinct singular directions. Over $\mathbb{F}_q$ with $\mathrm{char}(\mathbb{F}_q) \neq 2$, any nonzero singular symmetric 2×2 matrix has rank 1 and hence a one-dimensional kernel in $V = \mathbb{F}_q^2$. Distinct projective singular directions correspond to non-proportional rank-1 matrices, and their kernels are distinct lines in V.

Choose a basis of V so that $\ker(M_1) = \langle e_1 \rangle$ and $\ker(M_2) = \langle e_2 \rangle$. In that basis, M_1 and M_2 become diagonal rank-1 matrices. Using the freedom to change the basis of $\mathcal{N}^2$ (equivalently, the ordered basis of L), we may scale so that

$$M_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \qquad M_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

Hence, after admissible changes, L is congruent to

$$\left\langle \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle,$$

which is exactly $(A^{(1)}_{(2,2)}, B^{(1)}_{(2,2)})$. The relations (18) and (19) become $x^2 = z$, $y^2 = w$, $xy = 0$, yielding $R \cong R^{(1)}_{(2,2)}$.

Step 5: Assume $\Sigma(L)$ is a single projective point. Then, up to scalar, there is a unique nonzero singular matrix $N \in L$. Since $\mathrm{char}(\mathbb{F}_q) \neq 2$, N has rank 1, choose a basis of V such that

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

Choose $C \in L$ linearly independent from N. Then C must be invertible; otherwise, C would provide a second singular direction and hence $|\Sigma(L)| \geq 2$.

Write

$$C = \begin{pmatrix} a & b \\ b & c \end{pmatrix}, \qquad \det(C) = ac - b^2 \neq 0.$$

If $b = 0$, then C is diagonal and $L = \langle \mathrm{diag}(1, 0), \mathrm{diag}(a, c) \rangle$ contains the independent singular matrices $\mathrm{diag}(1, 0)$ and $\mathrm{diag}(0, 1)$ (since $c \neq 0$), contradicting $|\Sigma(L)| = 1$. Thus $b \neq 0$.

Conjugating by $D = \mathrm{diag}(b^{-1}, 1)$ keeps N fixed and normalizes the off-diagonal entry to 1, so we may assume $b = 1$. Next, replace C by $C - aN$, which corresponds to changing the ordered basis of L (equivalently, changing the basis of $\mathcal{N}^2$). This yields

$$C = \begin{pmatrix} 0 & 1 \\ 1 & c \end{pmatrix}.$$

Now replace the ordered basis of L by (C, N). Then

$$L \sim \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \right\rangle,$$

which is $(A^{(2)}_{(2,2)}, B^{(2)}_{(2,2)})$. The relations become $xy = z$, $x^2 = w$, $y^2 = 0$, so $R \cong R^{(2)}_{(2,2)}$.

Step 6: Assume $\Sigma(L) = \varnothing$. Then every nonzero matrix in L is invertible. Choose an invertible $A \in L$ and complete it to an ordered basis (A, B) of L. Since $\mathrm{char}(\mathbb{F}_q) \neq 2$, there exists $U \in \mathrm{GL}_2(\mathbb{F}_q)$ such that $U^T A U = \mathrm{diag}(1, d)$ for some $d \in \mathbb{F}_q^\times$. Replacing L by $U^T L U$, we may assume

$$A = \mathrm{diag}(1, d), \qquad B = \begin{pmatrix} a & b \\ b & c \end{pmatrix}.$$

The condition $\Sigma(L) = \varnothing$ forces $b \neq 0$, for if $b = 0$, then B is diagonal and one can choose $(\alpha : \beta)$ so that $\alpha A + \beta B$ is singular, giving a point of $\Sigma(L)$.

Now conjugate by the diagonal matrix $P = \mathrm{diag}(1, b^{-1})$. This preserves the diagonal form of A and normalizes the off-diagonal entry of B to 1. Next, replace the ordered basis (A, B) by $(A,\ B - aA)$, which does not change L and kills the $(1,1)$-entry of B. Thus, we may assume

$$A = \mathrm{diag}(1, d), \qquad B = \begin{pmatrix} 0 & 1 \\ 1 & c \end{pmatrix}.$$

Finally, apply the shear $Q = \begin{pmatrix} 1 & -\frac{c}{2} \\ 0 & 1 \end{pmatrix}$ to obtain

$$Q^T B Q = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = H, \qquad A_1 = Q^T A Q = \begin{pmatrix} 1 & u \\ u & v \end{pmatrix}$$

for some $u, v \in \mathbb{F}_q$. Since A is invertible, so is A_1, hence $v \neq 0$. Because we are free to change the ordered basis of the 2-dimensional space $L = \langle A_1, H \rangle$, we may replace (A_1, H) by $(A_1 - uH,\ H)$. Set

$$A_2 = A_1 - uH = \begin{pmatrix} 1 & 0 \\ 0 & v \end{pmatrix} = \mathrm{diag}(1, v).$$

Thus,

$$L = \langle A_2, H \rangle = \left\langle \mathrm{diag}(1, v),\ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle.$$

For $(\alpha : \beta) \in \mathbb{P}^1(\mathbb{F}_q)$ we have

$$\det(\alpha A_2 + \beta H) = \det \begin{pmatrix} \alpha & \beta \\ \beta & \alpha v \end{pmatrix} = \alpha^2 v - \beta^2.$$

The condition $\Sigma(L) = \varnothing$ is equivalent to $\alpha^2 v - \beta^2 \neq 0$ for all $(\alpha : \beta) \in \mathbb{P}^1(\mathbb{F}_q)$, which holds if and only if v is a nonsquare in $\mathbb{F}_q^\times$. Therefore, L is congruent to the span of

$$A_{(2,2)}^{(3)} = \mathrm{diag}(1, \vartheta), \qquad B_{(2,2)}^{(3)} = H = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

where $\vartheta \in \mathbb{F}_q^\times$ is the fixed nonsquare. This yields the canonical anisotropic ring $R_{(2,2)}^{(3)}$ with relations $x^2 = z$, $y^2 = \vartheta z$, $xy = w$ (and $w\mathcal{N} = 0$ as before).

Step 7: The values $|\Sigma(L)| \in \{2, 1, 0\}$ are mutually exclusive, and $\Sigma(L)$ is an isomorphism invariant; hence, the three canonical rings are pairwise non-isomorphic. Conversely, every commutative type $(2, 2)$ ring yields a 2-dimensional subspace $L \subseteq \mathrm{Sym}_2(\mathbb{F}_q)$ with an invertible element by Lemma 4, so exactly one of the three cases occurs, and the above reductions show that R is isomorphic to the corresponding canonical representative.

□

Remark 2. *The matrix-pair framework of Lemma 3 and the basis-change description in Lemma 5 are valid in all characteristics. However, when* $\mathrm{char}(\mathbb{F}_q) = 2$*, the classification of symmetric bilinear forms differs. For this reason, the explicit canonical lists in both Theorem 2 and Theorem 3 are stated only for* $\mathrm{char}(\mathbb{F}_q) \neq 2$*.*

Remark 3. *The classification in this section (see Table 1) is governed by natural invariants arising from the induced multiplication on* $\mathcal{N}/\mathcal{N}^2$*. For type* $(3, 1)$ *rings, multiplication on* $V = \mathcal{N}/\mathcal{N}^2$ *is encoded by a nonzero symmetric matrix* $A \in \mathrm{Sym}_3(\mathbb{F}_q)$ *via* $x_i x_j = a_{ij} w$*, and the isomorphism class depends only on the projective congruence class of* A*, namely* $A \sim \theta U^T A U$ *with* $U \in \mathrm{GL}_3(\mathbb{F}_q)$ *and* $\theta \in \mathbb{F}_q^\times$*. In odd characteristic, this projective class is determined by the rank of* A*, and in rank* 2 *by the square class of the determinant of the nondegenerate* 2×2 *part. For type* $(2, 2)$ *rings, multiplication induces a symmetric bilinear map* $\mu : V \times V \to W$*, where* $V = \mathcal{N}/\mathcal{N}^2$ *and* $W = \mathcal{N}^2$*; equivalently, there is a two-dimensional subspace* $L \subseteq \mathrm{Sym}_2(\mathbb{F}_q)$ *up to congruence. In odd characteristic, the projective zero set*

$$\Sigma(L) = \{(\alpha : \beta) \in \mathbb{P}^1(\mathbb{F}_q) : \det(\alpha A + \beta B) = 0\} \tag{23}$$

is a complete invariant for the type $(2, 2)$ *classification described in Theorem 3 (in the odd-characteristic setting assumed there).*

Table 1. Summary of local rings of order q^5 with $\mathcal{N}^3 = 0 \neq \mathcal{N}^2$ for odd q.

Radical Type	Classification Invariant	Canonical Representatives (Odd q)	Cardinality
$(3, 1)$	projective congruence class of $A \in \mathrm{Sym}_3(\mathbb{F}_q) \setminus \{0\}$	$\mathrm{diag}(1,0,0)$; $\mathrm{diag}(1,1,0)$; $\mathrm{diag}(1,\vartheta,0)$; $\mathrm{diag}(1,1,1)$	4
$(2, 2)$	congruence class of $L = \langle A, B\rangle \subseteq \mathrm{Sym}_2(\mathbb{F}_q)$; invariant $\Sigma(L)$	$\lvert\Sigma(L)\rvert = 2$: $(A_{(2,2)}^{(1)}, B_{(2,2)}^{(1)})$ $\lvert\Sigma(L)\rvert = 1$: $(A_{(2,2)}^{(2)}, B_{(2,2)}^{(2)})$ $\lvert\Sigma(L)\rvert = 0$: $(A_{(2,2)}^{(3)}, B_{(2,2)}^{(3)})$	3

4. Constacyclic Codes over Local Rings of Order q^5 with $\mathcal{N}^3 = 0$

In this section, we analyze the ring

$$A_\lambda = R[X]/\langle X^n - \lambda\rangle, \qquad \lambda \in R^\times, \tag{24}$$

under the standing hypotheses, $\gcd(n,p) = 1$ and $(\rho_1,\rho_2) \in \{(3,1),(2,2)\}$, where $\rho_1 = \dim_{\mathbb{F}_q}(\mathcal{N}/\mathcal{N}^2)$ and $\rho_2 = \dim_{\mathbb{F}_q}(\mathcal{N}^2)$. Our goal is to describe λ-constacyclic codes, i.e., ideals of A_λ, via the radical filtration of A_λ and to obtain a residual–torsion decomposition that will later permit explicit enumeration. Set $\bar{\lambda}$ for the image of λ in $\mathbb{F}_q$, and

$$S = \mathbb{F}_q[X]/\langle X^n - \bar{\lambda}\rangle. \tag{25}$$

Since the derivative of $X^n - \bar{\lambda}$ is $nX^{n-1} \neq 0$ in $\mathbb{F}_q[X]$, the polynomial $X^n - \bar{\lambda}$ is square-free. Hence

$$S \cong \prod_{i=1}^{t} \mathbb{F}_{q^{d_i}} \tag{26}$$

is a finite semisimple $\mathbb{F}_q$-algebra.

Proposition 1. *The ring A_λ is local, and*

(i) $\mathrm{J}(A_\lambda) = \mathcal{M} = \mathcal{N}A_\lambda$.
(ii) $\mathcal{M}^2 = \mathcal{N}^2A_\lambda$ *and* $\mathcal{M}^3 = 0 \neq \mathcal{M}^2$.
(iii) $A_\lambda/\mathcal{M} \cong (R/\mathcal{N})[X]/\langle X^n - \bar{\lambda}\rangle \cong S$.
(iv) One has $\dim_{\mathbb{F}_q}(R) = 1 + \rho_1 + \rho_2$ *and hence*

$$\dim_{\mathbb{F}_q}(A_\lambda) = (1+\rho_1+\rho_2)n, \quad \dim_{\mathbb{F}_q}(\mathcal{M}/\mathcal{M}^2) = \rho_1 n, \quad \dim_{\mathbb{F}_q}(\mathcal{M}^2) = \rho_2 n.$$

In particular, $\dim_{\mathbb{F}_q}(A_\lambda) = 5n$.

Proof. Consider the natural surjection

$$\pi : A_\lambda \longrightarrow \frac{R[X]}{\langle X^n - \lambda,\ \mathcal{N}R[X]\rangle} \cong \mathbb{F}_q[X]/\langle X^n - \bar{\lambda}\rangle = S, \tag{27}$$

whose kernel is $\ker(\pi) = \mathcal{N}A_\lambda$.

(i) Since S is a finite product of fields, $\mathrm{J}(S) = 0$. Hence $\pi(\mathrm{J}(A_\lambda)) \subseteq \mathrm{J}(S) = 0$, so $\mathrm{J}(A_\lambda) \subseteq \ker(\pi) = \mathcal{N}A_\lambda$. Conversely, $\mathcal{N}A_\lambda$ is nilpotent because $(\mathcal{N}A_\lambda)^3 = \mathcal{N}^3A_\lambda = 0$, so every element of $\mathcal{N}A_\lambda$ lies in the Jacobson radical. Therefore, $\mathrm{J}(A_\lambda) = \mathcal{N}A_\lambda = \mathcal{M}$. This means that A_λ is local.
(ii) Since A_λ is commutative, $(\mathcal{N}A_\lambda)^k = \mathcal{N}^kA_\lambda$ for $k \geq 1$, hence $\mathcal{M}^2 = \mathcal{N}^2A_\lambda$ and $\mathcal{M}^3 = \mathcal{N}^3A_\lambda = 0$. Moreover, $\mathcal{M}^2 \neq 0$ because $\mathcal{N}^2 \neq 0$.
(iii) This is exactly the isomorphism induced by π.
(iv) As an R-module, A_λ is free of rank n with basis $\{1, X, \ldots, X^{n-1}\}$; hence $\dim_{\mathbb{F}_q}(A_\lambda) = n\dim_{\mathbb{F}_q}(R)$. Also, $\mathcal{M} = \mathcal{N}A_\lambda$ and $\mathcal{M}^2 = \mathcal{N}^2A_\lambda$ satisfy $\dim_{\mathbb{F}_q}(\mathcal{M}) = n\dim_{\mathbb{F}_q}(\mathcal{N})$ and $\dim_{\mathbb{F}_q}(\mathcal{M}^2) = n\dim_{\mathbb{F}_q}(\mathcal{N}^2)$. Thus,

$$\dim_{\mathbb{F}_q}(\mathcal{M}/\mathcal{M}^2) = n\big(\dim_{\mathbb{F}_q}(\mathcal{N}) - \dim_{\mathbb{F}_q}(\mathcal{N}^2)\big) = \rho_1 n, \qquad \dim_{\mathbb{F}_q}(\mathcal{M}^2) = \rho_2 n.$$

Finally, $\dim_{\mathbb{F}_q}(R) = 1 + \rho_1 + \rho_2$ follows from the filtration $0 \subset \mathcal{N}^2 \subset \mathcal{N} \subset R$ and $R/\mathcal{N} \cong \mathbb{F}_q$.

□

We now relate A_λ to the factorization of $X^n - \bar{\lambda}$ over $\mathbb{F}_q$. Since $\gcd(n,p) = 1$, the polynomial $X^n - \bar{\lambda}$ is square-free and hence factors into distinct monic irreducibles

$$X^n - \bar{\lambda} = f_1(X)\cdots f_t(X) \qquad \text{in } \mathbb{F}_q[X]. \tag{28}$$

Lemma 6. *Let R be a finite local ring with maximal ideal $\mathcal{N}$ and residue field $\mathbb{F}_q$. Let $F(X) \in R[X]$ and write $\bar{F}(X)$ for its reduction modulo $\mathcal{N}$. Suppose $\bar{F} = \bar{f}_1 \cdots \bar{f}_t$ with $\bar{f}_i$ monic and pairwise coprime in $\mathbb{F}_q[X]$. Then there exist monic polynomials $F_1, \ldots, F_t \in R[X]$ with $F_i \bmod \mathcal{N} = \bar{f}_i$ such that $F = F_1 \cdots F_t$ in $R[X]$, and the ideals $\langle F_i \rangle$ are pairwise comaximal in $R[X]$.*

Proof. Since the $\bar{f}_i$ are pairwise coprime in $\mathbb{F}_q[X] = (R/\mathcal{N})[X]$, there exist $\bar{a}_i, \bar{b}_i \in \mathbb{F}_q[X]$ with $\bar{a}_i \bar{f}_i + \bar{b}_i(\bar{F}/\bar{f}_i) = 1$. Lifting $\bar{a}_i, \bar{b}_i$ to $a_i, b_i \in R[X]$ gives $a_i f_i + b_i(F/f_i) \equiv 1 \pmod{\mathcal{N}R[X]}$, and since $\mathcal{N}$ is nilpotent, one can iteratively correct the lifts to obtain exact factorizations and comaximality. This is the standard coprime factorization lifting (Hensel lifting) over a local ring with a nilpotent maximal ideal; see, e.g., McDonald [2], Ch. IX. □

Apply Lemma 6 to $F(X) = X^n - \lambda$ and (28). Let $F_i(X) \in R[X]$ be monic Hensel lifts of $f_i(X)$ such that

$$X^n - \lambda = F_1(X) \cdots F_t(X) \qquad \text{in } R[X].$$

Theorem 4. *With the notation as above, the ideals $\langle F_i(X) \rangle$ are pairwise comaximal in $R[X]$, and there is a ring isomorphism:*

$$A_\lambda \cong \prod_{i=1}^{t} R[X]/\langle F_i(X) \rangle. \tag{29}$$

Under this isomorphism, λ-constacyclic codes correspond bijectively to products of ideals in the factors. Moreover,

$$S \cong \prod_{i=1}^{t} \mathbb{F}_q[X]/\langle f_i(X) \rangle \cong \prod_{i=1}^{t} \mathbb{F}_{q^{\deg f_i}}, \tag{30}$$

so S is a finite principal ideal ring (indeed, a finite product of fields).

Proof. According to Lemma 6, the ideals $\langle F_i \rangle$ are pairwise comaximal and $X^n - \lambda = \prod_i F_i$. Hence

$$\langle X^n - \lambda \rangle = \bigcap_{i=1}^{t} \langle F_i \rangle,$$

and the Chinese remainder theorem yields

$$R[X]/\langle X^n - \lambda \rangle \cong \prod_{i=1}^{t} R[X]/\langle F_i \rangle,$$

which is (29). Ideals in a finite product are products of ideals in the components. Reducing modulo $\mathcal{N}$ sends F_i to f_i and commutes with finite products. Using Proposition 1(iii) (namely, $A_\lambda/\mathcal{M} \cong S$ with $\mathcal{M} = \mathcal{N}A_\lambda$), we obtain (30). The last isomorphism follows since each $\mathbb{F}_q[X]/\langle f_i \rangle$ is a finite field of size $q^{\deg f_i}$. □

The quotient map $A_\lambda \to S = A_\lambda/\mathcal{M}$ induces S-module structures on the radical layers $\mathcal{M}/\mathcal{M}^2$ and $\mathcal{M}^2$: for $s = \bar{a} \in S$ and $x \in \mathcal{M}$, set $s \cdot (x + \mathcal{M}^2) = ax + \mathcal{M}^2$, and for $y \in \mathcal{M}^2$, set $s \cdot y = ay$. These actions are well-defined since $(a - a')\mathcal{M} \subseteq \mathcal{M}^2$ whenever $a \equiv a' \pmod{\mathcal{M}}$, and $(a - a')\mathcal{M}^2 \subseteq \mathcal{M}^3 = 0$.

Remark 4. *The ring S is canonically an $\mathbb{F}_q$-algebra via the composition $\mathbb{F}_q \hookrightarrow R \twoheadrightarrow A_\lambda \twoheadrightarrow S$. Hence, the tensor products $(\mathcal{N}/\mathcal{N}^2) \otimes_{\mathbb{F}_q} S$ and $\mathcal{N}^2 \otimes_{\mathbb{F}_q} S$ are well-defined and carry natural S-module structures.*

Proposition 2. *There are canonical S-module isomorphisms*

$$\mathcal{M}/\mathcal{M}^2 \;\cong\; (\mathcal{N}/\mathcal{N}^2) \otimes_{\mathbb{F}_q} S, \qquad \mathcal{M}^2 \;\cong\; \mathcal{N}^2 \otimes_{\mathbb{F}_q} S.$$

In particular, $\mathcal{M}/\mathcal{M}^2 \cong S^{\rho_1}$ and $\mathcal{M}^2 \cong S^{\rho_2}$ as S-modules. Moreover, multiplication in A_λ induces an S-bilinear map

$$\mu : \; (\mathcal{M}/\mathcal{M}^2) \times (\mathcal{M}/\mathcal{M}^2) \to \mathcal{M}^2$$

which corresponds, under the above identifications, to the scalar extension to S of the $\mathbb{F}_q$-bilinear product map $(\mathcal{N}/\mathcal{N}^2) \times (\mathcal{N}/\mathcal{N}^2) \to \mathcal{N}^2$.

Proof. Define

$$\Psi : (\mathcal{N}/\mathcal{N}^2) \otimes_{\mathbb{F}_q} S \to \mathcal{M}/\mathcal{M}^2, \qquad (\bar{v}) \otimes \bar{f} \mapsto \overline{vf},$$

where $v \in \mathcal{N}$ and $f \in A_\lambda$ are lifts and bars denote quotient classes. If v is replaced by $v + v_2$ with $v_2 \in \mathcal{N}^2$, then $v_2 f \in \mathcal{N}^2 A_\lambda = \mathcal{M}^2$. If f is replaced by $f + h$ with $h \in \mathcal{M} = \mathcal{N}A_\lambda$, then $vh \in \mathcal{N}\mathcal{N}A_\lambda = \mathcal{N}^2 A_\lambda = \mathcal{M}^2$. Hence, Ψ is well-defined. It is S-linear by construction.

Surjectivity: any class in $\mathcal{M}/\mathcal{M}^2$ has a representative in $\mathcal{M} = \mathcal{N}A_\lambda$, so it is a sum of terms vf with $v \in \mathcal{N}$, $f \in A_\lambda$, and hence lies in the image. Injectivity follows by comparing $\mathbb{F}_q$-dimensions:

$$\dim_{\mathbb{F}_q}\big((\mathcal{N}/\mathcal{N}^2) \otimes_{\mathbb{F}_q} S\big) = \rho_1 \dim_{\mathbb{F}_q}(S) = \rho_1 n = \dim_{\mathbb{F}_q}(\mathcal{M}/\mathcal{M}^2),$$

using Proposition 1(iv). Thus, Ψ is an isomorphism. The proof for $\mathcal{M}^2 \cong \mathcal{N}^2 \otimes_{\mathbb{F}_q} S$ is identical.

Finally, since $\mathcal{M}^3 = 0$, multiplication satisfies $\mathcal{M} \cdot \mathcal{M} \subseteq \mathcal{M}^2$, and changing either factor by an element of $\mathcal{M}^2$ changes the product by an element of $\mathcal{M}^3 = 0$. Therefore, multiplication induces a well-defined S-bilinear map $\mu : (\mathcal{M}/\mathcal{M}^2) \times (\mathcal{M}/\mathcal{M}^2) \to \mathcal{M}^2$, which is precisely the scalar extension of the $\mathbb{F}_q$-bilinear product on $\mathcal{N}/\mathcal{N}^2$ with values in $\mathcal{N}^2$. □

Remark 5. *With $|R| = q^5$, we have $(\rho_1, \rho_2) \in \{(3,1),(2,2)\}$. Consequently,*

$$\mathcal{M}/\mathcal{M}^2 \cong S^3,\ \mathcal{M}^2 \cong S \quad \text{or} \quad \mathcal{M}/\mathcal{M}^2 \cong S^2,\ \mathcal{M}^2 \cong S^2,$$

corresponding to the two radical types classified in Section 3.

Let $C \subseteq A_\lambda$ be a λ-constacyclic code, i.e., an ideal. The interaction of C with the filtration $A_\lambda \supset \mathcal{M} \supset \mathcal{M}^2 \supset 0$ is recorded by residual and torsion layers.

Definition 1. *For an ideal $C \subseteq A_\lambda$, define*

$$C_0 = \frac{C + \mathcal{M}}{\mathcal{M}} \subseteq S, \qquad C^{(1)} = C \cap \mathcal{M}, \qquad C^{(2)} = C \cap \mathcal{M}^2, \tag{31}$$

and

$$C_1 = \frac{C^{(1)} + \mathcal{M}^2}{\mathcal{M}^2} \subseteq \mathcal{M}/\mathcal{M}^2, \qquad C_2 = C^{(2)} \subseteq \mathcal{M}^2. \tag{32}$$

We call C_0 the residual code and C_1, C_2 the first and second torsion codes.

Lemma 7. *Each C_i is an S-submodule of its ambient space. In particular, C_0 is an ideal of S and hence an $\bar{\lambda}$-constacyclic code over $\mathbb{F}_q$. Moreover, under the natural maps induced by the filtration,*

$$C_2 \subseteq C^{(2)} \subseteq C^{(1)} \subseteq C, \qquad \frac{C^{(1)}}{C^{(2)}} \cong C_1, \qquad \frac{C}{C^{(1)}} \cong C_0. \tag{33}$$

Proof. The S-module structures on $\mathcal{M}/\mathcal{M}^2$ and $\mathcal{M}^2$ are described above. Since $C^{(1)} = C \cap \mathcal{M}$ is an ideal of A_λ, the submodule $C^{(1)} + \mathcal{M}^2 \subseteq \mathcal{M}$ is stable under multiplication by A_λ; hence, its image $C_1 = (C^{(1)} + \mathcal{M}^2)/\mathcal{M}^2$ is stable under the induced S-action. Thus, C_1 is an S-submodule. Similarly, $C_2 = C \cap \mathcal{M}^2$ is an ideal contained in $\mathcal{M}^2$ and hence stable under the S-action.

Finally, $C_0 = (C + \mathcal{M})/\mathcal{M}$ is an ideal of S. The quotient identifications follow from the isomorphism theorems:

$$\frac{C}{C \cap \mathcal{M}} \cong \frac{C + \mathcal{M}}{\mathcal{M}} = C_0, \qquad \frac{C^{(1)}}{C^{(1)} \cap \mathcal{M}^2} \cong \frac{C^{(1)} + \mathcal{M}^2}{\mathcal{M}^2} = C_1,$$

and $C^{(1)} \cap \mathcal{M}^2 = C \cap \mathcal{M}^2 = C^{(2)} = C_2$. □

Theorem 5. *Let $C \subseteq A_\lambda$ be a λ-constacyclic code and set $C^{(1)} = C \cap \mathcal{M}$ and $C^{(2)} = C \cap \mathcal{M}^2$. Then there are natural short exact sequences of S-modules*

$$0 \longrightarrow C^{(1)}/C^{(2)} \longrightarrow C/C^{(2)} \longrightarrow C_0 \longrightarrow 0, \tag{34}$$

$$0 \longrightarrow C_2 \longrightarrow C^{(1)} \longrightarrow C_1 \longrightarrow 0, \tag{35}$$

and one has the canonical identification $C^{(1)}/C^{(2)} \cong C_1$ as S-modules.

Proof. Consider the natural surjection

$$\phi : C \longrightarrow (C + \mathcal{M})/\mathcal{M} = C_0, \qquad c \longmapsto c + \mathcal{M}.$$

Its kernel is $C \cap \mathcal{M} = C^{(1)}$, so ϕ induces a surjection $\bar{\phi} : C/C^{(2)} \twoheadrightarrow C_0$ with kernel $C^{(1)}/C^{(2)}$, giving (34). For (35), restrict the quotient map $\mathcal{M} \to \mathcal{M}/\mathcal{M}^2$ to $C^{(1)}$: its image is C_1 and its kernel is $C^{(1)} \cap \mathcal{M}^2 = C^{(2)} = C_2$, yielding (35). The induced map $C^{(1)}/C^{(2)} \to C_1$ is an S-module isomorphism by construction. □

Since S is a finite product of fields, it is a semisimple Artinian ring (hence a principal ideal ring). In particular, every S-submodule of a free module S^t is generated by at most t elements: indeed, $S^t \cong \prod_j K_j^t$, and submodules correspond componentwise to vector subspaces.

Theorem 6. *Let $C \subseteq A_\lambda$ be a λ-constacyclic code and let C_0, C_1, C_2 be as shown in Definition 1. Assume $|R| = q^5$. Then there exist polynomials*

$$G_0(X) \in R[X], \qquad G_1^{(1)}(X), \ldots, G_1^{(r)}(X) \in R[X], \qquad G_2^{(1)}(X), \ldots, G_2^{(s)}(X) \in R[X],$$

with $r \leq \rho_1$ and $s \leq \rho_2$ such that:

(i) $G_0(X) \bmod \mathcal{N} = g_0(X)$, *where $g_0(X) \in \mathbb{F}_q[X]$ generates the ideal $C_0 \subseteq S$;*

(ii) *The images of $G_1^{(j)}(X)$ in $\mathcal{M}/\mathcal{M}^2$ generate C_1 as an S-module;*

(iii) *The images of $G_2^{(\ell)}(X)$ in $\mathcal{M}^2$ generate C_2 as an S-module;*

and

$$C = \left\langle\, G_0(X),\ G_1^{(1)}(X), \ldots, G_1^{(r)}(X),\ G_2^{(1)}(X), \ldots, G_2^{(s)}(X) \,\right\rangle_{A_\lambda}.$$

In particular, every λ-constacyclic code over R is generated by at most $1+\rho_1+\rho_2=5$ polynomials.

Proof. By Proposition 2, $\mathcal{M}/\mathcal{M}^2 \cong S^{\rho_1}$ and $\mathcal{M}^2 \cong S^{\rho_2}$. Since S is semisimple (a finite product of fields), any S-submodule of S^t is generated by at most t elements. Hence, C_1 is generated by at most ρ_1 elements and C_2 by at most ρ_2 elements as S-modules. Since C_0 is an ideal of the principal ideal ring S, choose $g_0 \in S$ such that $C_0 = \langle g_0 \rangle$. Choose $G_0(X) \in R[X]$ lifting g_0 modulo $\mathcal{N}$. Choose S-generators $\bar{u}_1, \ldots, \bar{u}_r$ of C_1 with $r \le \rho_1$, and choose lifts $u_j \in C \cap \mathcal{M}$ representing $\bar{u}_j$ modulo $\mathcal{M}^2$. Let $G_1^{(j)}(X) \in R[X]$ represent u_j in A_λ. Similarly, choose S-generators $v_1, \ldots, v_s$ of $C_2 \subseteq \mathcal{M}^2$ with $s \le \rho_2$, and choose representatives $G_2^{(\ell)}(X) \in R[X]$ of v_ℓ in A_λ. Let $I \le A_\lambda$ be the ideal generated by these polynomials. Clearly, $I \subseteq C$. We show that $C \subseteq I$.

Step 1. For $c \in C$, its image in $S = A_\lambda/\mathcal{M}$ lies in $C_0 = \langle g_0 \rangle$, so $c + \mathcal{M} = s_0 g_0$ for some $s_0 \in S$. Lift s_0 to $a_0 \in A_\lambda$. Then $c - a_0 G_0 \in C \cap \mathcal{M} = C^{(1)}$.
Step 2. Put $c_1 = c - a_0 G_0 \in C^{(1)}$. Its image in $\mathcal{M}/\mathcal{M}^2$ lies in C_1, so $c_1 + \mathcal{M}^2 = \sum_{j=1}^{r} s_j \bar{u}_j$ for some $s_j \in S$. Lift s_j to $a_j \in A_\lambda$. Then

$$c_1 - \sum_{j=1}^{r} a_j G_1^{(j)} \in \mathcal{M}^2.$$

Set $c_2 = c_1 - \sum_j a_j G_1^{(j)} \in C \cap \mathcal{M}^2 = C_2$.
Step 3. Since $v_1, \ldots, v_s$ generate C_2 as an S-module, write $c_2 = \sum_{\ell=1}^{s} t_\ell v_\ell$ with $t_\ell \in S$. Lift t_ℓ to $b_\ell \in A_\lambda$. Because the S-action on $\mathcal{M}^2$ is induced from A_λ, the element $\sum_\ell b_\ell G_2^{(\ell)}$ represents $\sum_\ell t_\ell v_\ell = c_2$ in $\mathcal{M}^2$ (the choice of lifts is immaterial since $(b_\ell - b'_\ell)\mathcal{M}^2 \subseteq \mathcal{M}^3 = 0$). Thus $c_2 \in I$.
Step 4. Combining the steps yields $c \in I$. Hence, $C \subseteq I$, and therefore, $C = I$. The generator bound $1 + r + s \le 1 + \rho_1 + \rho_2 = 5$ follows.
□

Remark 6. *Since $\mathcal{M}/\mathcal{M}^2 \cong S^{\rho_1}$ and $\mathcal{M}^2 \cong S^{\rho_2}$, the torsion layers C_1 and C_2 require at most ρ_1 and ρ_2 generators as S-modules, respectively. Therefore, if C_1 and C_2 are generated by r and s elements, then $\tau(C) \le 1 + r + s \le 1 + \rho_1 + \rho_2 = 5$, where $\tau(C)$ denotes the minimal number of generators of C as an A_λ-module. Hence, the bound in Theorem 6 is global but not always sharp. In particular, C is principal if $C_1 = C_2 = 0$, and the number of generators decreases whenever one of the torsion layers is trivial or cyclic. Also, in type $(3,1)$ one has $s \le 1$, while in type $(2,2)$ both torsion layers may be nontrivial.*

Remark 7. *Assume that R is Frobenius. Then $A_\lambda = R[X]/\langle X^n - \lambda \rangle$ is Frobenius as a finite R-algebra, and its Frobenius functional induces a nondegenerate associative bilinear form $\langle \cdot, \cdot \rangle : A_\lambda \times A_\lambda \to R$. Passing to quotients yields perfect pairings on the successive radical layers, compatible with the filtration $A_\lambda \supset \mathcal{M} \supset \mathcal{M}^2 \supset 0$. In particular, the induced pairing on $A_\lambda/\mathcal{M} \cong S$ recovers the classical duality for $\bar{\lambda}$-constacyclic codes over $\mathbb{F}_q$. Moreover, the induced pairings on $\mathcal{M}/\mathcal{M}^2$ and on $\mathcal{M}^2$ are perfect S-bilinear pairings (via the action of $S = A_\lambda/\mathcal{M}$), so the dual code $C^\perp$ can be described layer by layer: its residual and torsion layers are the annihilators of C_0, C_1, C_2 under the corresponding pairings (Table 2). This observation will be used in later duality results.*

Under the standing hypotheses, write

$$X^n - \bar{\lambda} = \prod_{i=1}^{t} f_i(X), \qquad X^n - \lambda = \prod_{i=1}^{t} F_i(X),$$

with f_i distinct monic irreducible over $\mathbb{F}_q$ and F_i their Hensel lifts. Set

$$A_i = R[X]/\langle F_i(X)\rangle, \qquad K_i = \mathbb{F}_q[X]/\langle f_i(X)\rangle, \qquad Q_i = |K_i|.$$

Let

$$\mathfrak{m}_i = \mathrm{J}(A_i), \qquad V_i = \mathfrak{m}_i/\mathfrak{m}_i^2, \qquad W_i = \mathfrak{m}_i^2.$$

Then $V_i \cong K_i^{\rho_1}$ and $W_i \cong K_i^{\rho_2}$. For a λ-constacyclic code $C_i \subseteq A_i$, define

$$r_i = \dim_{K_i}(C_{1,i}), \qquad s_i = \dim_{K_i}(C_{2,i}),$$

where $C_{1,i} \leq V_i$ and $C_{2,i} \leq W_i$ are the first and second torsion layers of C_i. Furthermore, define

$$U_0 = \{\, i : \, C_i \subseteq \mathfrak{m}_i \,\}, \qquad U_1 = \{\, i : \, C_i = A_i \,\}. \tag{36}$$

Theorem 7. *Let $C \subseteq A_\lambda$ be a λ-constacyclic code. Then $\{1, \ldots, t\} = U_0 \cup U_1$. Moreover,*

(i) For each $i \in U_0$, fix reduced row echelon matrices over K_i representing the subspaces

$$C_{1,i} \leq V_i, \qquad C_{2,i} \leq W_i.$$

Choose lifts

$$G_{i,1}^{(1)}(X), \ldots, G_{i,1}^{(r_i)}(X), \qquad G_{i,2}^{(1)}(X), \ldots, G_{i,2}^{(s_i)}(X)$$

whose images generate $C_{1,i}$ and $C_{2,i}$, respectively. Let $e_i(X)$ be the CRT idempotent corresponding to A_i and set

$$F_{U_0}(X) = \prod_{i \in U_0} F_i(X).$$

Then

$$\begin{aligned} C = \Big\langle & F_{U_0}(X),\ \{\, e_i(X) G_{i,1}^{(j)}(X) : i \in U_0,\ 1 \leq j \leq r_i \,\}, \\ & \{\, e_i(X) G_{i,2}^{(\ell)}(X) : i \in U_0,\ 1 \leq \ell \leq s_i \,\} \Big\rangle. \end{aligned} \tag{37}$$

In particular, each local component C_i is generated by at most $\rho_1 + \rho_2 \leq 4$ elements, and hence, every λ-constacyclic code over R is generated by at most five polynomials globally.

(ii) For $i \in U_1$, one has $|C_i| = |A_i| = q^{5d_i}$. For $i \in U_0$, one has

$$|C_i| = Q_i^{r_i + s_i} = q^{d_i(r_i + s_i)}.$$

Consequently,

$$|C| = \prod_{i \in U_1} q^{5d_i} \cdot \prod_{i \in U_0} q^{d_i(r_i + s_i)}. \tag{38}$$

Proof. Because $X^n - \bar{\lambda} = \prod_{i=1}^t f_i(X)$ is square-free, the f_i are pairwise coprime in $\mathbb{F}_q[X]$. By Hensel lifting, the monic lifts F_i are pairwise comaximal in $R[X]$ and satisfy $X^n - \lambda = \prod_i F_i$. Hence

$$\langle X^n - \lambda \rangle = \bigcap_{i=1}^t \langle F_i \rangle,$$

and the Chinese remainder theorem yields

$$A_\lambda = R[X]/\langle X^n - \lambda \rangle \cong \prod_{i=1}^t A_i. \tag{39}$$

Thus, constacyclic codes of a finite direct product are exactly products of constacyclic codes in the components. For uniquely determined ideals $C_i \leq A_i$, we have

$$C \cong \prod_{i=1}^{t} C_i. \tag{40}$$

Let $e_i \in A_\lambda$ denote the corresponding CRT idempotents, so $1 = \sum_i e_i$, $e_i e_j = 0$ for $i \neq j$, and $e_i A_\lambda \cong A_i$.

Step 1. Define

$$U_1 = \{\, i : \, C_i = A_i \,\}, \qquad U_0 = \{1, \ldots, t\} \setminus U_1 = \{\, i : \, C_i \subseteq \mathrm{J}(A_i) \,\}.$$

For $i \in U_0$, the residual layer of C_i in $A_i/\mathrm{J}(A_i) \cong K_i$ is 0, whereas for $i \in U_1$ it is K_i. Hence the residual code

$$C_0 = \frac{C + \mathrm{J}(A_\lambda)}{\mathrm{J}(A_\lambda)} \leq S \cong \prod_{i=1}^{t} K_i$$

is exactly $\prod_{i \in U_1} K_i \times \prod_{i \in U_0} 0$, so C_0 is the principal ideal of S generated by the CRT idempotent $\sum_{i \in U_1} \bar{e}_i$. Equivalently, C_0 is generated by the product of the complementary factors, namely

$$g_0(X) = \prod_{i \in U_0} f_i(X) \in S.$$

Let $F_{U_0}(X) = \prod_{i \in U_0} F_i(X)$; then $F_{U_0} \bmod \mathcal{N} = g_0$ in S.

Step 2. Fix $i \in U_0$. Apply the residual–torsion framework inside A_i: with $\mathfrak{m}_i = \mathrm{J}(A_i)$, the code C_i has residual layer 0 and torsion layers

$$(C_i)_1 \leq V_i, \qquad (C_i)_2 \leq W_i,$$

which are K_i-subspaces of $V_i \cong K_i^{\rho_1}$ and $W_i \cong K_i^{\rho_2}$. Choose K_i-generators of these subspaces and lift them to polynomials

$$G_{i,1}^{(1)}(X), \ldots, G_{i,1}^{(r_i)}(X) \in R[X], \qquad G_{i,2}^{(1)}(X), \ldots, G_{i,2}^{(s_i)}(X) \in R[X],$$

so that their images generate $(C_i)_1$ in V_i and $(C_i)_2$ in W_i. Then, Theorem 6 (applied to the local ring A_i) yields

$$C_i = \langle G_{i,1}^{(1)}, \ldots, G_{i,1}^{(r_i)}, \, G_{i,2}^{(1)}, \ldots, G_{i,2}^{(s_i)} \rangle_{A_i}, \tag{41}$$

since the residual layer is 0. For $i \in U_1$, we have $C_i = A_i$, and hence, no generators are needed beyond 1.

Step 3. Under the isomorphism (39), the element $e_i \in A_\lambda$ projects to 1 in the ith factor and to 0 in all others. Therefore, the ideals

$$e_i C \subseteq A_\lambda \quad \text{correspond exactly to} \quad 0 \times \cdots \times 0 \times C_i \times 0 \times \cdots \times 0.$$

Hence, $C = \sum_{i=1}^{t} e_i C$ and, using (41) for $i \in U_0$ and $C_i = A_i$ for $i \in U_1$, we obtain (37).

Step 4. For each i, the additive group of A_i has size $|A_i| = |R|^{d_i} = q^{5d_i}$ since A_i is free of rank d_i over R. If $i \in U_1$, then $|C_i| = |A_i| = q^{5d_i}$. If $i \in U_0$, the residual layer of C_i is 0, and the successive quotients in the filtration

$$0 \subseteq C_i \cap \mathfrak{m}_i^2 \subseteq C_i \cap \mathfrak{m}_i \subseteq C_i \subseteq \mathfrak{m}_i$$

identify as

$$\frac{C_i}{C_i \cap \mathfrak{m}_i} \cong 0, \qquad \frac{C_i \cap \mathfrak{m}_i}{C_i \cap \mathfrak{m}_i^2} \cong (C_i)_1, \qquad C_i \cap \mathfrak{m}_i^2 = (C_i)_2.$$

Thus $|C_i| = |(C_i)_1| \cdot |(C_i)_2|$. Since $(C_i)_1$ and $(C_i)_2$ are K_i-vector spaces of dimensions r_i and s_i, we have $|(C_i)_1| = Q_i^{r_i}$ and $|(C_i)_2| = Q_i^{s_i}$, hence

$$|C_i| = Q_i^{r_i+s_i} = q^{d_i(r_i+s_i)}.$$

Finally, $|C| = \prod_i |C_i|$ because $C \cong \prod_i C_i$ as an additive group under the CRT, giving (38). □

Table 2. Structural layers of $A_\lambda = R[X]/\langle X^n - \lambda\rangle$ with $|R| = q^5$, $\mathcal{N}^3 = 0 \neq \mathcal{N}^2$, and $\gcd(n, p) = 1$.

Object	Description	$\mathbb{F}_q$-Dimension
$\mathcal{M} = \mathrm{J}(A_\lambda)$	$\mathcal{N}A_\lambda$	$n \dim_{\mathbb{F}_q}(\mathcal{N}) = n(\rho_1 + \rho_2)$
$\mathcal{M}^2$	$\mathcal{N}^2 A_\lambda$	$\rho_2 n$
$A_\lambda/\mathcal{M}$	$S = \mathbb{F}_q[X]/\langle X^n - \bar{\lambda}\rangle$	n
$\mathcal{M}/\mathcal{M}^2$	$(\mathcal{N}/\mathcal{N}^2) \otimes_{\mathbb{F}_q} S \cong S^{\rho_1}$	$\rho_1 n$
C_0	Residual layer $(C + \mathcal{M})/\mathcal{M} \leq S$	$\dim_{\mathbb{F}_q}(C/C^{(1)})$
C_1	First torsion layer $(C^{(1)} + \mathcal{M}^2)/\mathcal{M}^2 \leq S^{\rho_1}$	$\dim_{\mathbb{F}_q}(C^{(1)}/C^{(2)})$
C_2	Second torsion layer $C \cap \mathcal{M}^2 \leq S^{\rho_2}$	$\dim_{\mathbb{F}_q}(C^{(2)})$
Generator bound	$C = \langle G_0, G_1^{(1)}, \ldots, G_1^{(r)}, G_2^{(1)}, \ldots, G_2^{(s)}\rangle$, with $r \leq \rho_1$ and $s \leq \rho_2$	$\leq$5 generators

5. Enumeration of λ-Constacyclic Codes

This section determines the exact number

$$N_\lambda(R, n) = \big|\{\lambda\text{–constacyclic codes of length } n \text{ over } R\}\big|.$$

By the structural results established earlier, every such code is an ideal of

$$A_\lambda = R[X]/\langle X^n - \lambda\rangle,$$

and the enumeration problem reduces to counting the ideals of A_λ. Assume $\gcd(n, p) = 1$. Then $X^n - \bar{\lambda}$ is square-free in $\mathbb{F}_q[X]$, so

$$X^n - \bar{\lambda} = \prod_{i=1}^{t} f_i(X), \qquad \deg f_i = d_i,$$

with distinct monic irreducible factors. Let $F_i(X)$ denote the corresponding Hensel lifts. By Theorem 4,

$$A_\lambda \cong \prod_{i=1}^{t} A_i, \qquad A_i = R[X]/\langle F_i(X)\rangle,$$

and every λ-constacyclic code decomposes uniquely as

$$C \cong \prod_{i=1}^{t} C_i, \qquad C_i \leq A_i.$$

Consequently,

$$N_\lambda(R, n) = \prod_{i=1}^{t} N(A_i), \tag{42}$$

where $N(A_i)$ denotes the number of constacyclic codes over the local ring A_i.

The remainder of this section is devoted to computing $N(A_i)$. The answer depends only on the residue field size

$$Q_i = q^{d_i}$$

and on the canonical class of R. For each radical type, $(3,1)$ and $(2,2)$, we determine the local ideal counts explicitly. Substituting these into (42) yields closed formulas for $N_\lambda(R,n)$.

Lemma 8. *For each i, reduction modulo $\mathcal{N}$ induces an isomorphism*

$$A_i/\mathcal{N}A_i \;\cong\; (R/\mathcal{N})[X]/\langle \overline{F_i}(X)\rangle \;=\; \mathbb{F}_q[X]/\langle f_i(X)\rangle \;=\; K_i.$$

Moreover,

$$\mathrm{J}(A_i) = \mathfrak{m}_i = \mathcal{N}A_i, \qquad \mathfrak{m}_i^2 = \mathcal{N}^2A_i, \qquad \mathfrak{m}_i^3 = 0,$$

and $\mathfrak{m}_i/\mathfrak{m}_i^2$ and $\mathfrak{m}_i^2$ are naturally K_i-vector spaces with

$$\dim_{K_i}(\mathfrak{m}_i/\mathfrak{m}_i^2) = \rho_1, \qquad \dim_{K_i}(\mathfrak{m}_i^2) = \rho_2.$$

Proof. Reducing the defining relation modulo $\mathcal{N}$ gives

$$A_i/\mathcal{N}A_i \cong (R/\mathcal{N})[X]/\langle \overline{F_i}(X)\rangle = \mathbb{F}_q[X]/\langle f_i(X)\rangle = K_i,$$

so $\mathcal{N}A_i$ is a maximal ideal of A_i. Since $\mathcal{N}^3 = 0$, we have $(\mathcal{N}A_i)^3 = \mathcal{N}^3A_i = 0$, so $\mathcal{N}A_i$ is nilpotent and hence contained in $\mathrm{J}(A_i)$. Conversely, $\mathrm{J}(A_i)$ maps to $\mathrm{J}(K_i) = 0$, which implies $\mathrm{J}(A_i) \subseteq \mathcal{N}A_i$. Thus, $\mathrm{J}(A_i) = \mathfrak{m}_i = \mathcal{N}A_i$. Commutativity yields $\mathfrak{m}_i^k = (\mathcal{N}A_i)^k = \mathcal{N}^kA_i$ for $k \geq 1$, and hence $\mathfrak{m}_i^2 = \mathcal{N}^2A_i$ and $\mathfrak{m}_i^3 = 0$. Since $A_i/\mathfrak{m}_i \cong K_i$, the A_i-module structures on $\mathfrak{m}_i/\mathfrak{m}_i^2$ and $\mathfrak{m}_i^2$ factor through K_i, so these are K_i-vector spaces.

Finally, A_i is free of rank d_i over R (since F_i is monic of degree d_i). Hence, $\dim_{\mathbb{F}_q}(\mathcal{N}^jA_i) = d_i \dim_{\mathbb{F}_q}(\mathcal{N}^j)$ for $j = 1,2$. As $[K_i : \mathbb{F}_q] = d_i$, this implies the stated K_i-dimensions. □

Remark 8. *Each local factor A_i has the same radical type (ρ_1,ρ_2) as R, now viewed over K_i.*

Fix i and abbreviate

$$A = A_i, \qquad \mathfrak{m} = \mathrm{J}(A), \qquad K = A/\mathfrak{m} \cong K_i, \qquad Q = |K| = Q_i.$$

Set

$$V = \mathfrak{m}/\mathfrak{m}^2, \qquad W = \mathfrak{m}^2.$$

Through Lemma 8, $V \cong K^{\rho_1}$ and $W \cong K^{\rho_2}$ as K-vector spaces, and multiplication in A induces a well-defined K-bilinear map:

$$\mu : V \times V \to W, \qquad \mu(\bar{x},\bar{y}) = xy \;(\mathrm{mod}\; \mathfrak{m}^3 = 0). \tag{43}$$

Lemma 9. *The ideals I of A satisfying $\mathfrak{m}^2 \subseteq I \subseteq \mathfrak{m}$ are in bijection with K-subspaces $U \leq V$ via $U \leftrightarrow \pi^{-1}(U)$, where $\pi : \mathfrak{m} \twoheadrightarrow V$ is the quotient map. Consequently,*

$$\left|\{I \leq A :\; \mathfrak{m}^2 \subseteq I \subseteq \mathfrak{m}\}\right| = G_{\rho_1}(Q) = \sum_{k=0}^{\rho_1} \binom{\rho_1}{k}_Q.$$

After choosing a K-basis of $V \cong K^{\rho_1}$, the k-dimensional subspaces $U \leq V$ are parametrized by $k \times \rho_1$ matrices over K in reduced row echelon (RRE) form.

Proof. Because $\mathfrak{m}(\mathfrak{m}/\mathfrak{m}^2) = 0$, the action of A on $V = \mathfrak{m}/\mathfrak{m}^2$ factors through $A/\mathfrak{m} \cong K$. Hence, A-submodules of V are precisely K-subspaces. The correspondence theorem for π gives the desired bijection with ideals I satisfying $\mathfrak{m}^2 \subseteq I \subseteq \mathfrak{m}$. Counting such subspaces, through (11), yields the Gaussian number $G_{\rho_1}(Q)$, and the RRE parametrization is standard. □

Lemma 10. *The ideals J of A with $J \subseteq \mathfrak{m}^2$ are precisely the K-subspaces of $W = \mathfrak{m}^2$. Consequently,*

$$\left|\{J \leq A : J \subseteq \mathfrak{m}^2\}\right| = G_{\rho_2}(Q) = \sum_{k=0}^{\rho_2} \binom{\rho_2}{k}_Q.$$

Proof. Since $\mathfrak{m}\mathfrak{m}^2 = \mathfrak{m}^3 = 0$, the action of A on $\mathfrak{m}^2$ factors through $A/\mathfrak{m} \cong K$. Hence, A-submodules of $\mathfrak{m}^2$ are precisely the K-subspaces of W. □

Remark 9. *Lemmas 9 and 10 account for all ideals containing $\mathfrak{m}^2$ and all ideals contained in $\mathfrak{m}^2$. The remaining ideals are those $I \subseteq \mathfrak{m}$ with $I \cap \mathfrak{m}^2 = 0$; these are governed by the multiplication constraints imposed by μ in (43).*

5.1. Type $(3,1)$

Assume that R has radical type $(3,1)$, i.e., $\rho_1 = 3$ and $\rho_2 = 1$, and assume $\mathrm{char}(\mathbb{F}_q) \neq 2$. Fix a local CRT factor

$$A = A_i, \qquad \mathfrak{m} = \mathrm{J}(A), \qquad K = A/\mathfrak{m} \cong K_i, \qquad Q = |K|.$$

Then

$$\mathfrak{m}^2 = \langle w \rangle_K \cong K, \qquad V = \mathfrak{m}/\mathfrak{m}^2 \cong K^3.$$

Multiplication in A induces a symmetric K-bilinear form

$$b_s : V \times V \to K, \qquad uv = b_s(u,v)\, w,$$

belonging to one of the four canonical projective congruence classes represented by

$$A^{(1)}_{(3,1)} = \mathrm{diag}(1,0,0), \quad A^{(2)}_{(3,1)} = \mathrm{diag}(1,1,0), \quad A^{(3)}_{(3,1)} = \mathrm{diag}(1,\vartheta,0), \quad A^{(4)}_{(3,1)} = \mathrm{diag}(1,1,1),$$

where $\vartheta \in \mathbb{F}_q^{\times}$ is a fixed nonsquare.

Let

$$\mathrm{Rad}(b_s) = \{\, u \in V : b_s(u,v) = 0 \text{ for all } v \in V \,\}$$

denote the radical of the bilinear form.

Proposition 3. *Every proper ideal $I \subsetneq A$ satisfies exactly one of the following:*

(i) *$w \in I$. Then $\mathfrak{m}^2 \subseteq I \subseteq \mathfrak{m}$, and I is uniquely determined by the K-subspace $U = \pi(I) \leq V$ via $I = \pi^{-1}(U)$.*

(ii) *$w \notin I$. Then $I \subseteq \mathfrak{m}$ and $I \cap \mathfrak{m}^2 = 0$. Writing $U = \pi(I) \leq V$, one has $U \subseteq \mathrm{Rad}(b_s)$. Conversely, fix a K-linear section $s : V \to \mathfrak{m}$ of π (so $\pi \circ s = \mathrm{id}_V$). For every K-subspace $U \leq \mathrm{Rad}(b_s)$ and every K-linear map $\varphi : U \to K$, the subset*

$$I(U,\varphi) = \{\, s(u) + \varphi(u)w : u \in U \,\}$$

is an ideal of A with $\pi(I(U,\varphi)) = U$ and $I(U,\varphi) \cap \mathfrak{m}^2 = 0$. Moreover, for fixed U, the ideals $I(U,\varphi)$ are pairwise distinct, and there are exactly $Q^{\dim U}$ of them.

Proof. If $w \in I$, then $\mathfrak{m}^2 = \langle w \rangle_K \subseteq I \subseteq \mathfrak{m}$, and the correspondence theorem yields $I = \pi^{-1}(U)$ uniquely. Assume $w \notin I$. Since $\mathfrak{m}^2 = \langle w \rangle_K$ is the unique minimal nonzero ideal, one has $I \cap \mathfrak{m}^2 = 0$. Let $U = \pi(I) \leq V$. For any $x \in \mathfrak{m}$ and $y \in I$, we have $xy \in \mathfrak{m}^2$ and $xy \in I$, hence $xy \in I \cap \mathfrak{m}^2 = 0$. Thus, $b_s(\pi(x), u) = 0$ for all $u \in U$ and all $x \in \mathfrak{m}$, so $U \subseteq \mathrm{Rad}(b_s)$. Conversely, let $U \leq \mathrm{Rad}(b_s)$ and $\varphi : U \to K$ be K-linear. The set $I(U, \varphi)$ is a K-subspace of $\mathfrak{m}$, and $\pi(I(U, \varphi)) = U$ by construction. Also, $I(U, \varphi) \cap \mathfrak{m}^2 = 0$ since π restricts to an isomorphism $I(U, \varphi) \xrightarrow{\sim} U$. To see that it is an ideal, note that $A = K \oplus \mathfrak{m}$ as K-vector spaces, so it suffices to check stability under multiplication by $\mathfrak{m}$. For $x \in \mathfrak{m}$ and $u \in U$,

$$x\big(s(u) + \varphi(u)w\big) = xs(u) \in \mathfrak{m}^2 = \langle w \rangle_K,$$

and the coefficient of w equals $b_s(\pi(x), u) = 0$ because $u \in \mathrm{Rad}(b_s)$. Hence, $x\big(s(u) + \varphi(u)w\big) = 0 \in I(U, \varphi)$, so $\mathfrak{m} I(U, \varphi) = 0$ and $I(U, \varphi)$ is an ideal. Finally, if $\varphi \neq \psi$, choose $u \in U$ with $\varphi(u) \neq \psi(u)$; then, $s(u) + \varphi(u)w \neq s(u) + \psi(u)w$, so $I(U, \varphi) \neq I(U, \psi)$. Since $\mathrm{Hom}_K(U, K)$ has size $Q^{\dim U}$, the stated count follows. □

Theorem 8. *Let A be as above and let $r_s = \dim_K \mathrm{Rad}(b_s)$. Then the number of ideals of A equals*

$$N(A) = 1 + G_3(Q) + H_s(Q),$$

where

$$G_3(Q) = \sum_{k=0}^{3} \binom{3}{k}_Q = 2Q^2 + 2Q + 4, \qquad H_s(Q) = \sum_{k=0}^{r_s} \binom{r_s}{k}_Q Q^k.$$

For the four canonical classes, one has

$$\begin{aligned}
s = 1\ (\mathrm{rank}\,1): &\quad r_1 = 2, \quad N(A) = 4Q^2 + 3Q + 6,\\
s = 2\ (\mathrm{rank}\,2): &\quad r_2 = 1, \quad N(A) = 2Q^2 + 3Q + 6,\\
s = 3\ (\mathrm{rank}\,2): &\quad r_3 = 1, \quad N(A) = 2Q^2 + 3Q + 6,\\
s = 4\ (\mathrm{rank}\,3): &\quad r_4 = 0, \quad N(A) = 2Q^2 + 2Q + 6.
\end{aligned}$$

Consequently,

$$N_\lambda(R, n) = \prod_{i=1}^{t} N(A_i).$$

Proof. The ideals split into (i) those containing w, counted by $G_3(Q)$ (together with A itself); (ii) those not containing w, counted by pairs (U, φ) with $U \leq \mathrm{Rad}(b_s)$ and $\varphi \in \mathrm{Hom}_K(U, K)$. Hence,

$$N(A) = 1 + G_3(Q) + \sum_{U \leq \mathrm{Rad}(b_s)} |\mathrm{Hom}_K(U, K)| = 1 + G_3(Q) + \sum_{k=0}^{r_s} \binom{r_s}{k}_Q Q^k.$$

The explicit evaluations follow from $G_3(Q) = 2Q^2 + 2Q + 4$ and $r_s \in \{2, 1, 1, 0\}$ for the four classes. □

Example 1. *Let R be a finite commutative local ring with residue field $R/\mathcal{N} \cong \mathbb{F}_3$,*

$$|R| = 3^5, \qquad \mathcal{N}^3 = 0 \neq \mathcal{N}^2,$$

and radical type $(3, 1)$, i.e.,

$$\dim_{\mathbb{F}_3}(\mathcal{N}/\mathcal{N}^2) = 3, \qquad \dim_{\mathbb{F}_3}(\mathcal{N}^2) = 1.$$

Set

$$A = R[X]/\langle X^4 - 1\rangle, \qquad \mathcal{M} = \mathrm{J}(A) = \mathcal{N}A.$$

Since $\gcd(4,3) = 1$, *the polynomial* $X^4 - 1$ *is separable over* $\mathbb{F}_3$.

Step 1: Factorization over $\mathbb{F}_3$ *and CRT. Over* $\mathbb{F}_3$ *we have*

$$X^4 - 1 = (X^2 - 1)(X^2 + 1) = (X - 1)(X + 1)(X^2 + 1),$$

and $X^2 + 1$ *is irreducible over* $\mathbb{F}_3$ *since* $-1 \equiv 2$ *is a nonsquare in* $\mathbb{F}_3$. *Thus,*

$$X^4 - 1 = \prod_{j=1}^{3} f_j(X), \qquad (f_1, f_2, f_3) = (X - 1,\ X + 1,\ X^2 + 1), \qquad (d_1, d_2, d_3) = (1, 1, 2).$$

Let

$$K_j = \mathbb{F}_3[X]/\langle f_j(X)\rangle, \qquad Q_j = |K_j| = 3^{d_j}.$$

Then,

$$K_1 \cong K_2 \cong \mathbb{F}_3, \qquad K_3 \cong \mathbb{F}_9, \qquad (Q_1, Q_2, Q_3) = (3, 3, 9).$$

Let F_j *be monic Hensel lifts of* f_j *to* $R[X]$ *and set*

$$A^{(j)} = R[X]/\langle F_j(X)\rangle.$$

By the Chinese remainder theorem,

$$A \cong \prod_{j=1}^{3} A^{(j)}, \qquad N_1(R, 4) = \prod_{j=1}^{3} N\big(A^{(j)}\big).$$

Step 2: Local counts for the four canonical classes. In type $(3,1)$ *(with* $\mathrm{char}(\mathbb{F}_3) \neq 2$*), the number of ideals of each local factor* $A^{(j)}$ *depends only on the canonical class index* $s \in \{1,2,3,4\}$ *of the induced bilinear form on* $\mathrm{J}(A^{(j)})/\mathrm{J}(A^{(j)})^2 \cong K_j^3$. *By Theorem 8, for* $Q = |K_j|$ *one has*

$$N(A^{(j)}) = \begin{cases} 4Q^2 + 3Q + 6, & s = 1\ \big(\mathrm{diag}(1,0,0)\big), \\ 2Q^2 + 3Q + 6, & s = 2\ \big(\mathrm{diag}(1,1,0)\big), \\ 2Q^2 + 3Q + 6, & s = 3\ \big(\mathrm{diag}(1,\vartheta,0)\big), \\ 2Q^2 + 2Q + 6, & s = 4\ \big(\mathrm{diag}(1,1,1)\big). \end{cases}$$

In particular, no quadratic character conditions occur in the ideal counts for type $(3,1)$.

(i) *Class* $R^{(1)}_{(3,1)}$ *(rank* 1*:* $\mathrm{diag}(1,0,0)$*). For* $(Q_1, Q_2, Q_3) = (3,3,9)$*:*

$$N(A^{(1)}) = 4 \cdot 3^2 + 3 \cdot 3 + 6 = 51, \quad N(A^{(2)}) = 51, \quad N(A^{(3)}) = 4 \cdot 9^2 + 3 \cdot 9 + 6 = 357.$$

Hence

$$N_1\big(R^{(1)}_{(3,1)}, 4\big) = 51^2 \cdot 357.$$

(ii) *Class* $R^{(2)}_{(3,1)}$ *(rank* 2*:* $\mathrm{diag}(1,1,0)$*).*

$$N(A^{(1)}) = 2 \cdot 3^2 + 3 \cdot 3 + 6 = 33, \quad N(A^{(2)}) = 33, \quad N(A^{(3)}) = 2 \cdot 9^2 + 3 \cdot 9 + 6 = 195.$$

Hence

$$N_1\big(R^{(2)}_{(3,1)}, 4\big) = 33^2 \cdot 195.$$

(iii) *Class* $R^{(3)}_{(3,1)}$ *(rank* 2*:* $\mathrm{diag}(1,\vartheta,0)$*). This class has the same rank as (ii), hence the same local ideal counts:*

$$N(A^{(1)}) = 33, \quad N(A^{(2)}) = 33, \quad N(A^{(3)}) = 195,$$

so

$$N_1\big(R^{(3)}_{(3,1)}, 4\big) = 33^2 \cdot 195.$$

(iv) *Class* $R^{(4)}_{(3,1)}$ *(rank* 3*:* $\mathrm{diag}(1,1,1)$*).*

$$N(A^{(1)}) = 2\cdot 3^2 + 2\cdot 3 + 6 = 30, \quad N(A^{(2)}) = 30, \quad N(A^{(3)}) = 2\cdot 9^2 + 2\cdot 9 + 6 = 186.$$

Hence

$$N_1\big(R^{(4)}_{(3,1)}, 4\big) = 30^2 \cdot 186.$$

This example illustrates that, for fixed $(q,n,\lambda) = (3,4,1)$ *and CRT degrees* $(1,1,2)$*, the total number of* λ*-constacyclic codes varies substantially with the canonical type* $(3,1)$ *class, i.e., the rank class s of the induced bilinear form.*

5.2. Type $(2,2)$

Assume that R has radical type $(2,2)$, i.e.,

$$\rho_1 = \dim_{\mathbb{F}_q}(\mathcal{N}/\mathcal{N}^2) = 2, \qquad \rho_2 = \dim_{\mathbb{F}_q}(\mathcal{N}^2) = 2,$$

and assume throughout that $\mathrm{char}(\mathbb{F}_q) \neq 2$. In odd characteristic, Theorem 3 yields three canonical isomorphism classes, $R^{(1)}_{(2,2)}, R^{(2)}_{(2,2)}, R^{(3)}_{(2,2)}$, distinguished by the invariant $|\Sigma(L)| \in \{2,1,0\}$.

Theorem 9. *Assume that* $\mathrm{char}(\mathbb{F}_q) \neq 2$ *and let* R *be a commutative type* $(2,2)$ *ring of order* q^5*. Fix an index* i *and set* $K = K_i$ *and* $Q = |K|$*. Let* A_i *be the i-th local CRT factor. Then,* A_i *is a commutative type* $(2,2)$ *local ring over* K*, and the number of ideals of* A_i *depends only on the canonical class of* R *(equivalently, on* $|\Sigma(L)|$*) as follows:*

$$N(A_i) = \begin{cases} 4Q+6, & R \cong R^{(1)}_{(2,2)} \ \ (|\Sigma(L)| = 2), \\ 3Q+6, & R \cong R^{(2)}_{(2,2)} \ \ (|\Sigma(L)| = 1), \\ 4Q+6, & R \cong R^{(3)}_{(2,2)} \ \ (|\Sigma(L)| = 0 \text{ and } \chi_K(\vartheta) = 1), \\ 2Q+6, & R \cong R^{(3)}_{(2,2)} \ \ (|\Sigma(L)| = 0 \text{ and } \chi_K(\vartheta) = -1), \end{cases}$$

where $\vartheta \in \mathbb{F}_q^\times$ *is the fixed nonsquare parameter appearing in the canonical presentation of* $R^{(3)}_{(2,2)}$ *in Theorem 3, and* χ_K *denotes the quadratic character of* $K^\times$ *(extended by* $\chi_K(0) = 0$*). Consequently,*

$$N_\lambda(R,n) = \prod_{i=1}^{t} N(A_i).$$

Proof. Fix i and set $K = K_i$, $Q = |K|$. By Lemma 8, A_i has residue field K and radical type $(2,2)$ over K. Equivalently, after scalar extension, one may identify A_i with a type $(2,2)$ local K-algebra $\widetilde{R}$ having maximal ideal $\mathfrak{m} = \mathrm{J}(\widetilde{R})$ satisfying

$$\mathfrak{m}^3 = 0, \qquad \mathfrak{m}\mathfrak{m}^2 = 0, \qquad V = \mathfrak{m}/\mathfrak{m}^2 \cong K^2, \qquad W = \mathfrak{m}^2 \cong K^2.$$

Multiplication induces a symmetric K-bilinear map:

$$\mu : V \times V \to W, \qquad \mu(\bar{x}, \bar{y}) = xy \ (\mathrm{mod}\ \mathfrak{m}^3 = 0).$$

Choose a K-linear section $s : V \to \mathfrak{m}$ so that $\mathfrak{m} = s(V) \oplus W$ as K-vector spaces and $s(u)s(v) = \mu(u, v) \in W$ for all $u, v \in V$.

Step 1. Let $I \subseteq \widetilde{R}$ be a proper ideal. Then $I \subseteq \mathfrak{m}$. Define

$$U = \pi(I) \leq V, \qquad U_2 = I \cap W \leq W,$$

where $\pi : \mathfrak{m} \twoheadrightarrow V$ is the quotient map. Fix a pair (U, U_2). Any K-subspace $I \leq \mathfrak{m}$ with $\pi(I) = U$ and $I \cap W = U_2$ is the graph of a K-linear map $\varphi : U \to W/U_2$. Hence, the number of such subspaces is

$$|\mathrm{Hom}_K(U, W/U_2)| = Q^{\dim U \cdot (2 - \dim U_2)}. \tag{44}$$

Step 2. Since $W\mathfrak{m} = 0$ and $\mathfrak{m} = s(V) \oplus W$, for $u \in U$ and $v \in V$ one has

$$\mathfrak{m} \cdot (s(u) + W) = s(V) \cdot s(u) = \mu(V, u) \subseteq W.$$

Therefore, the condition $\mathfrak{m}I \subseteq I$ is equivalent to

$$\mu(U, V) \subseteq U_2, \tag{45}$$

which depends only on the pair (U, U_2).

Step 3. Combining Steps 1 and 2, the number of proper ideals of $\widetilde{R}$ equals

$$\left|\{I \leq \widetilde{R} : \ I \subseteq \mathfrak{m}\}\right| = \sum_{\substack{U \leq V,\ U_2 \leq W \\ \mu(U,V) \subseteq U_2}} Q^{\dim U \cdot (2 - \dim U_2)}. \tag{46}$$

Finally,

$$N(A_i) = N(\widetilde{R}) = 1 + \left|\{I \leq \widetilde{R} : \ I \subseteq \mathfrak{m}\}\right|.$$

Case $R^{(1)}_{(2,2)}$ ($|\Sigma(L)| = 2$). Choose bases $V = \langle x, y \rangle_K$ and $W = \langle z, w \rangle_K$ such that $x^2 = z$, $y^2 = w$, and $xy = 0$. Equivalently, $\mu((a, b), (c, d)) = ac\, z + bd\, w$. Then, $\mu(U, V) = 0$ if and only if $U = 0$; $\mu(U, V)$ is one-dimensional if and only if U is one of the two coordinate lines; and otherwise, $\mu(U, V) = W$. Evaluating (46),

(i) $\dim U = 0$: contribution $G_2(Q) = Q + 3$.
(ii) $\dim U = 1$: the two special lines contribute $2(Q + 1)$; the remaining $Q - 1$ lines contribute $(Q - 1) \cdot 1$. The total contribution is $3Q + 1$.
(iii) $\dim U = 2$: $U = V$, and only $U_2 = W$ is admissible, contributing 1.

Hence, $|\{I \subseteq \mathfrak{m}\}| = (Q + 3) + (3Q + 1) + 1 = 4Q + 5$, so $N(A_i) = 4Q + 6$.

Case $R^{(2)}_{(2,2)}$ ($|\Sigma(L)| = 1$). Choose bases such that $x^2 = w$, $y^2 = 0$, and $xy = z$, i.e., $\mu((a, b), (c, d)) = (ad + bc)\, z + ac\, w$. Then $\mu(\langle y \rangle, V) = \langle z \rangle$, and $\mu(U, V) = W$ for every line $U \neq \langle y \rangle$. Evaluating (46) gives $|\{I \subseteq \mathfrak{m}\}| = (Q + 3) + (2Q + 1) + 1 = 3Q + 5$, hence $N(A_i) = 3Q + 6$.

Case $R^{(3)}_{(2,2)}$ ($|\Sigma(L)| = 0$). Choose bases such that $x^2 = z$, $y^2 = \vartheta z$, and $xy = w$, i.e., $\mu((a, b), (c, d)) = (ac + \vartheta bd)\, z + (ad + bc)\, w$. For a line $U = \langle (a, b) \rangle \leq V$, one has $\dim \mu(U, V) = 1$ if and only if there exists $(c, d) \neq 0$ with $\mu((a, b), (c, d)) = 0$, equivalently

$$a^2 - \vartheta b^2 = 0. \tag{47}$$

Thus, if $\chi_K(\vartheta) = -1$, then (47) has no nontrivial solution and every line satisfies $\mu(U, V) = W$; if $\chi_K(\vartheta) = 1$, then there are exactly two solution lines and all other lines satisfy $\mu(U, V) = W$. Evaluating (46) yields

$$N(A_i) = \begin{cases} 2Q + 6, & \chi_K(\vartheta) = -1, \\ 4Q + 6, & \chi_K(\vartheta) = 1. \end{cases}$$

The global product formula follows from Equation (42).

□

Remark 10. *Let $\vartheta \in \mathbb{F}_q^\times$ be a fixed nonsquare and let $K = \mathbb{F}_{q^d}$. Then, $\chi_K(\vartheta) = (-1)^d$. Equivalently, ϑ is a square in K if and only if d is even.*

In all cases,

$$N_\lambda(R, n) = \prod_{i=1}^{t} N(A_i), \qquad Q_i = q^{d_i}.$$

Example 2. *Let R be a finite local ring with*

$$|R| = 5^5, \qquad \mathcal{N}^3 = 0 \neq \mathcal{N}^2,$$

and radical type $(2, 2)$:

$$\dim_{\mathbb{F}_5}(\mathcal{N}/\mathcal{N}^2) = 2, \qquad \dim_{\mathbb{F}_5}(\mathcal{N}^2) = 2.$$

Set

$$A = R[X]/\langle X^6 + 1\rangle.$$

Since $\gcd(6, 5) = 1$, the polynomial $X^6 + 1$ is separable over $\mathbb{F}_5$.

Step 1: Factorization over $\mathbb{F}_5$ and CRT degrees. In $\mathbb{F}_5[X]$, we have

$$X^6 + 1 = (X^2 + 1)(X^4 - X^2 + 1).$$

Because $-1 \equiv 4$ is a square in $\mathbb{F}_5$, one has

$$X^2 + 1 = (X - 2)(X + 2).$$

Moreover,

$$X^4 - X^2 + 1 = (X^2 + 2X - 1)(X^2 - 2X - 1),$$

and each quadratic factor is irreducible over $\mathbb{F}_5$ (its discriminant equals $4 - 4(-1) = 8 \equiv 3$, which is a nonsquare in $\mathbb{F}_5$). Thus,

$$X^6 + 1 = \prod_{j=1}^{4} f_j(X), \qquad (f_1, f_2, f_3, f_4) = (X - 2,\ X + 2,\ X^2 + 2X - 1,\ X^2 - 2X - 1),$$

with degrees

$$(d_1, d_2, d_3, d_4) = (1, 1, 2, 2).$$

Let

$$K_j = \mathbb{F}_5[X]/\langle f_j(X)\rangle, \qquad Q_j = |K_j| = 5^{d_j}.$$

Then

$$K_1 \cong K_2 \cong \mathbb{F}_5, \qquad K_3 \cong K_4 \cong \mathbb{F}_{25}, \qquad (Q_1, Q_2, Q_3, Q_4) = (5, 5, 25, 25).$$

Let F_j be monic Hensel lifts of f_j to $R[X]$ and set

$$A^{(j)} = R[X]/\langle F_j(X)\rangle.$$

By the Chinese remainder theorem,

$$A \cong \prod_{j=1}^{4} A^{(j)}, \qquad N_{-1}(R,6) = \prod_{j=1}^{4} N\big(A^{(j)}\big).$$

Step 2: Quadratic character values over K_j. Let χ_{K_j} denote the quadratic character on $K_j^\times$ (extended by $\chi_{K_j}(0) = 0$). Fix a nonsquare $\vartheta \in \mathbb{F}_5^\times$ (so $\vartheta \in \{2,3\}$), as in the canonical presentation of $R_{(2,2)}^{(3)}$ in Theorem 3. For $K_1 \cong K_2 \cong \mathbb{F}_5$, we have $\chi_{\mathbb{F}_5}(\vartheta) = -1$ by the definition of ϑ. For $K_3 \cong K_4 \cong \mathbb{F}_{25}$ (a degree-2 extension), every element of $\mathbb{F}_5^\times$ becomes a square in $\mathbb{F}_{25}^\times$, hence

$$\chi_{\mathbb{F}_{25}}(a) = 1 \quad \textit{for all } a \in \mathbb{F}_5^\times, \qquad \textit{in particular} \qquad \chi_{\mathbb{F}_{25}}(\vartheta) = 1.$$

Step 3: Local ideal counts. By Theorem 9, the number of ideals of a local factor $A^{(j)}$ depends on the canonical class of R (equivalently, on $|\Sigma(L)|$) and on $Q_j = |K_j|$.

(i) If $R \cong R_{(2,2)}^{(1)}$ (so $|\Sigma(L)| = 2$), then

$$N\big(A^{(j)}\big) = 4Q_j + 6.$$

Hence,

$$N\big(A^{(1)}\big) = N\big(A^{(2)}\big) = 4 \cdot 5 + 6 = 26, \qquad N\big(A^{(3)}\big) = N\big(A^{(4)}\big) = 4 \cdot 25 + 6 = 106.$$

(ii) If $R \cong R_{(2,2)}^{(2)}$ (so $|\Sigma(L)| = 1$), then

$$N\big(A^{(j)}\big) = 3Q_j + 6.$$

Hence,

$$N\big(A^{(1)}\big) = N\big(A^{(2)}\big) = 3 \cdot 5 + 6 = 21, \qquad N\big(A^{(3)}\big) = N\big(A^{(4)}\big) = 3 \cdot 25 + 6 = 81.$$

(iii) If $R \cong R_{(2,2)}^{(3)}$ (so $|\Sigma(L)| = 0$), then

$$N\big(A^{(j)}\big) = \begin{cases} 4Q_j + 6, & \chi_{K_j}(\vartheta) = 1, \\ 2Q_j + 6, & \chi_{K_j}(\vartheta) = -1. \end{cases}$$

Using $\chi_{K_1}(\vartheta) = \chi_{K_2}(\vartheta) = -1$ and $\chi_{K_3}(\vartheta) = \chi_{K_4}(\vartheta) = 1$, we obtain

$$N\big(A^{(1)}\big) = N\big(A^{(2)}\big) = 2 \cdot 5 + 6 = 16, \qquad N\big(A^{(3)}\big) = N\big(A^{(4)}\big) = 4 \cdot 25 + 6 = 106.$$

Step 4: Global enumeration. Combining the local counts yields

$$N_{-1}(R,6) = \begin{cases} 26^2 \cdot 106^2, & R \cong R_{(2,2)}^{(1)} \ (|\Sigma(L)| = 2), \\ 21^2 \cdot 81^2, & R \cong R_{(2,2)}^{(2)} \ (|\Sigma(L)| = 1), \\ 16^2 \cdot 106^2, & R \cong R_{(2,2)}^{(3)} \ (|\Sigma(L)| = 0). \end{cases}$$

This example shows that for fixed $(q, n, \lambda) = (5, 6, -1)$, the CRT degrees are $(1, 1, 2, 2)$ and the total number of negacyclic codes depends on the canonical class of the underlying type $(2, 2)$ ring. In particular, in the anisotropic class $R^{(3)}_{(2,2)}$, the local counts split according to whether the CRT residue field degree is odd or even, via the quadratic character values $\chi_{K_j}(\vartheta)$.

6. Conclusions

In this work, we obtained a structural and enumerative description of λ-constacyclic codes of length n over finite commutative local rings R of order q^5 with $\mathcal{N}^3 = 0 \neq \mathcal{N}^2$, under the standing assumption $\gcd(n, p) = 1$. Exactly two radical types occur, namely $(3, 1)$ and $(2, 2)$, both fitting into a unified residual–torsion framework arising from the radical filtration of

$$A_\lambda = R[X]/\langle X^n - \lambda \rangle. \tag{48}$$

Every λ-constacyclic code is realized as an ideal of A_λ, encoded by a residual component over the semisimple algebra $S = A_\lambda/\mathrm{J}(A_\lambda)$ together with two torsion layers inside $\mathrm{J}(A_\lambda)$. This layered description provides explicit generating sets and reduces global enumeration to local computations over finite extensions of $\mathbb{F}_q$ via the Chinese remainder decomposition $A_\lambda \cong \prod_{i=1}^{t} A_i$.

For radical type $(2, 2)$, the local ideal counts depend only on the field sizes $Q_i = q^{d_i}$ and the determinant-locus invariant $|\Sigma(L)|$, with an additional quadratic-character split in the anisotropic class. For type $(3, 1)$, the counts are governed by the induced symmetric bilinear form on $\mathrm{J}(A_i)/\mathrm{J}(A_i)^2$; equivalently, they are governed by the rank class of a canonical matrix representing multiplication on the top radical layer (or, equivalently, by $r_s = \dim_{K_i} \mathrm{Rad}(b_s)$). Combining the local formulas yields the closed product expression

$$N_\lambda(R, n) = \prod_{i=1}^{t} N(A_i), \tag{49}$$

explicitly in terms of the factor degrees d_i and the canonical isomorphism class of R.

For convenience, we summarize the local counts $N(A_i)$ in Table 3, where $Q = Q_i = q^{d_i}$ and $K_i = \mathbb{F}_q[X]/\langle f_i(X) \rangle$.

Table 3. Local ideal counts $N(A_i)$ for the CRT factors A_i.

Type of R	Canonical Class	Local Count $N(A_i)$
$(3, 1)$	$R^{(1)}_{(3,1)}$: $\mathrm{diag}(1, 0, 0)$	$4Q^2 + 3Q + 6$
	$R^{(2)}_{(3,1)}$: $\mathrm{diag}(1, 1, 0)$	$2Q^2 + 3Q + 6$
	$R^{(3)}_{(3,1)}$: $\mathrm{diag}(1, \vartheta, 0)$	$2Q^2 + 3Q + 6$
	$R^{(4)}_{(3,1)}$: $\mathrm{diag}(1, 1, 1)$	$2Q^2 + 2Q + 6$
$(2, 2)$	$R^{(1)}_{(2,2)}$ $(\lvert\Sigma(L)\rvert = 2)$	$4Q + 6$
	$R^{(2)}_{(2,2)}$ $(\lvert\Sigma(L)\rvert = 1)$	$3Q + 6$
	$R^{(3)}_{(2,2)}$ $(\lvert\Sigma(L)\rvert = 0)$	$\begin{cases} 4Q + 6, & \chi_{K_i}(\vartheta) = 1, \\ 2Q + 6, & \chi_{K_i}(\vartheta) = -1 \end{cases}$

The methods developed here provide a unified framework for constacyclic codes over cube-zero local rings of order q^5 and suggest several natural extensions. These include analogous classifications for larger orders (e.g., q^6) and for higher nilpotency

indices ($\mathcal{N}^\ell = 0$ with $\ell > 3$), where additional radical layers and multilinear structures are expected to play a decisive role.

Author Contributions: Conceptualization, S.H.S.; methodology, S.H.S.; software, S.H.S. and S.A.; validation, S.H.S.; formal analysis, S.H.S.; investigation, S.H.S.; data curation, S.A.; writing—original draft, S.H.S.; writing—review and editing, S.H.S. and S.A.; visualization, S.A.; funding acquisition, S.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the Ongoing Research Funding program, (ORF-2026-839), King Saud University, Riyadh, Saudi Arabia.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Raghavendran, R. Finite associative rings. *Compos. Math.* **1969**, *21*, 195–229.
2. McDonald, B.R. *Finite Rings with Identity*; Marcel Dekker: New York, NY, USA, 1974.
3. Whelan, E.A. A note on finite local rings. *Rocky Mt. J. Math.* **1992**, *22*, 757–759. [CrossRef]
4. Corbas, B.; Williams, G.D. Rings of order p^5, Part II: Local rings. *J. Algebra* **2000**, *231*, 691–704. [CrossRef]
5. Kanwar, P.; López-Permouth, S.R. Cyclic codes over the integers modulo p^m. *Finite Fields Their Appl.* **1997**, *3*, 334–352. [CrossRef]
6. Dinh, H.Q.; López-Permouth, S.R. Cyclic and negacyclic codes over finite chain rings. *IEEE Trans. Inf. Theory* **2004**, *50*, 1728–1744. [CrossRef]
7. Kim, B.; Lee, Y. Classification of self-dual cyclic codes over the chain ring $\mathbb{Z}_p[u]/\langle u^3\rangle$. *Des. Codes Cryptogr.* **2020**, *88*, 2247–2273. .. [CrossRef]
8. Bonnecaze, A.; Udaya, P. Cyclic codes and self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$. *IEEE Trans. Inf. Theory* **1999**, *45*, 1250–1255. [CrossRef]
9. Saif, S.H. Constructions and enumerations of self-dual and LCD double circulant codes over a local ring. *Mathematics* **2025**, *13*, 3527. [CrossRef]
10. Choi, H.S.; Kim, B. Various structures of cyclic codes over the non-Frobenius ring $\mathbb{F}_p[u,v]/\langle u^2, v^2, uv, vu\rangle$. *Adv. Math. Commun.* **2024**, *18*, 304–327. . [CrossRef]
11. Castillo-Guillén, C.A.; Rentería-Márquez, C.; Tapia-Recillas, H. Constacyclic codes over finite local Frobenius non-chain rings with nilpotency index 3. *Finite Fields Their Appl.* **2017**, *43*, 1–21. [CrossRef]
12. Li, S.; Shi, M.; Liu, H. Several constructions of optimal LCD codes over small finite fields. *Cryptogr. Commun.* **2024**, *16*, 779–800. [CrossRef]
13. Alabiad, S.; Alhomaidhi, A.A. Frobenius local rings of length 5 and index of nilpotency 3. *Mathematics* **2025**, *13*, 781. [CrossRef]
14. Wood, J. Duality for modules over finite rings and applications to coding theory. *Am. J. Math.* **1999**, *121*, 555–575. [CrossRef]
15. Shi, M.; Huang, D.; Sok, L.; Solé, P. Double circulant self-dual and LCD codes over Galois rings. *Adv. Math. Commun.* **2019**, *13*, 171–183. [CrossRef]
16. Nijenhuis, A.; Solow, A.E.; Wilf, H.S. Bijective methods in the theory of finite vector spaces. *J. Comb. Theory Ser. A* **1984**, *37*, 80–84. [CrossRef]
17. Saif, S.H.; Alkhamees, Y. Enumeration of Frobenius local rings of order p^{6r} via bilinear forms. *Symmetry* **2026**, *18*, 285. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.