

\$ sciendo Vol. 28(2),2020, 67–91

Constacyclic codes over finite local Frobenius non-chain rings of length 5 and nilpotency index 4

C. A. Castillo-Guillén and C. Rentería-Márquez

Abstract

The family of finite local Frobenius non-chain rings of length 5 and nilpotency index 4 is determined, as a by-product all finite local Frobenius non-chain rings with p^5 elements (p a prime) and nilpotency index 4 are given. And the number and structure of γ -constacyclic codes over those rings, of length relatively prime to the characteristic of the residue field of the ring, are determined.

1 Introduction

After the work of R. Hammons et al. (see [7]) the study of linear codes over finite rings has been a research topic of considerable interest. Some results on the description of structural properties of linear codes, particularly cyclic codes, over finite fields, finite chain rings and some finite local Frobenius nonchain rings, are available in the literature ([1], [2], [4], [5], [6], [8]). The γ constacyclic codes over the finite ring A are codes invariant under the mapping $\sigma_{\gamma} : \mathbf{A}^n \longrightarrow \mathbf{A}^n$ given by $\sigma_{\gamma}(a_0, a_1, \ldots, a_{n-1}) = (\gamma a_{n-1}, a_0, \ldots, a_{n-2})$, where γ is a unit of A, and are a generalization of cyclic codes. Finite Frobenius rings represent an interesting family of rings in Coding theory due to the fact that MacWilliams identities on the weight enumerator polynomial of a linear

Key Words: Chain rings, Commutative finite local rings, Constacyclic codes, Frobenius local rings.

²⁰¹⁰ Mathematics Subject Classification: Primary 94B15 ; Secondary 13H99. Received: 11.10.2019. Revised: 19.10.2019.

Accepted: 13.11.2019.

code and the relations $(C^{\perp})^{\perp} = C$ and $|C||C^{\perp}| = |A|^n$ are satisfied (see [11]), where C is a linear code of length n over A.

If p is a prime number, it is well-known that up to isomorphism there is only one local commutative ring with p elements, namely the Galois field GF(p). The local commutative rings with p^2 elements are: \mathbb{Z}_{p^2} , $\mathrm{GF}(p)[X]/\langle X^2 \rangle$ and $GF(p^2)$. If p is odd, the local commutative Frobenius rings with p^3 elements are: $\operatorname{GF}(p^3)$, \mathbb{Z}_{p^3} , $\operatorname{GF}(p)[X]/\langle X^3 \rangle$, $\mathbb{Z}_{p^2}[X]/\langle X^2 - p, pX \rangle$, $\operatorname{GF}(p)[X, Y]/\langle X, Y \rangle^2$, $\mathbb{Z}_{p^2}[X]/\langle X^2, pX \rangle$ and $\mathbb{Z}_{p^2}[X]/\langle X^2 - \zeta p, pX \rangle$, where $\overline{\zeta}$ is a primitive element of $\operatorname{GF}(p)$. If p = 2, the local commutative Frobenius rings with $2^3 = 8$ elements are: $GF(2^3)$, \mathbb{Z}_{2^3} , $GF(2)[X]/\langle X^3 \rangle$, $\mathbb{Z}_{2^2}[X]/\langle X^2 - 2, 2X \rangle$, $GF(2)[X, Y]/\langle X, Y \rangle^2$ and $\mathbb{Z}_{2^2}[X]/\langle X^2, 2X \rangle$, (see [10]).

If p is odd, the local commutative Frobenius non-chain rings with p^4 elements are:

- (1) $\mathbb{Z}_{p^3}[X]/\langle X^2 \zeta p^2, pX \rangle$, $\overline{\zeta}$ is a primitive element of GF(p),
- (2) $\mathbb{Z}_{p^3}[\mathbf{X}]/\langle \mathbf{X}^2 p^2, p\mathbf{X} \rangle$,

(3) $\mathbb{Z}_{p^2}[X]/\langle X^2 \rangle$, (4) $\mathbb{Z}_{p^2}[X,Y]/\langle X^2 - Y^2, Y^2 - p, XY, Y^3, pX, pY \rangle$, (5) $\mathbb{Z}_{p^2}[X,Y]/\langle X^2 - \zeta Y^2, Y^2 - p, XY, Y^3, pX, pY \rangle$, $\overline{\zeta}$ is a primitive element of $\mathrm{GF}(p)$.

(6) $GF(p)[X,Y]/\langle X^2 - Y^2, XY, Y^3 \rangle$, (7) $GF(p)[X,Y]/\langle X^2 - \zeta Y^2, XY, Y^3 \rangle$, ζ is a primitive element of GF(p).

And the local commutative Frobenius non-chain rings with 2^4 elements are: (1) $\mathbb{Z}_8[X]/\langle X^2-4, 2X\rangle$,

- (2) $\mathbb{Z}_4[\mathbf{X}]/\langle \mathbf{X}^2 \rangle$,
- (3) $\mathbb{Z}_4[X,Y]/\langle X^2 Y^2, Y^2 2, XY, Y^3, 2X, 2Y \rangle$,
- (4) $\mathbb{Z}_4[X,Y]/\langle X^2, Y^2, XY 2, 2X, 2Y \rangle$, (5) $\mathbb{Z}_4[X]/\langle X^2 2X \rangle$,
- (6) $GF(2)[X, Y]/\langle X^2, Y^2 \rangle$,
- (7) $GF(2)[X,Y]/\langle X^2 Y^2, XY, Y^3 \rangle$, (see [2], [9]).

Now it would be interesting to determine the family of finite local Frobenius non-chain rings with p^5 elements. A local Frobenius non-chain rings with p^5 elements has length 5 and the maximal ideal of a finite local Frobenius non-chain ring of length 5 has nilpotency index 3 or 4, (see Section 4).

The purpose of this paper is twofold. First, to determine the family of finite local Frobenius non-chain rings of length 5 and nilpotency index 4, as a by-product all local Frobenius non-chain rings with p^5 elements and nilpotency index 4, p a prime, are given. Second, determine the number and structure of γ -constacyclic codes whose alphabets are finite local Frobenius non-chain rings of length 5 and nilpotency index 4, when the length of the code is relatively prime to the characteristic of the residue field of the ring.

The paper is organized as follows: in Section 2 basic facts on finite local rings and modules over these rings are recalled. In Section 3 some isomorphisms between particular finite local rings are given. In Section 4 the family of finite local Frobenius non-chain rings of length 5 and nilpotency index 4 is determined and the finite local Frobenius non-chain rings with p^5 elements and nilpontency index 4, p a prime, are given. In Section 5 the number and structure of γ -constacyclic codes over finite local Frobenius non-chain rings of length 5 and nilpotency index 4 are determined, when the length of the code is relatively prime to the characteristic of the residue field of the ring. In the last section some conclusions are given.

2 Preliminaries

Throughout this work all rings are assumed to be finite, commutative with unit element and all modules are finitely generated. As usual, $GF(p^d)$ is the Galois field with p^d elements, p a prime, and $GF(p^d)^*$ denotes the non zero elements of $GF(p^d)$. For details about this section we refer the reader to [10].

Let A be a ring, I an ideal of A and M an A-module. Two elements $a, b \in A$ are called *coprime* if $\langle a \rangle + \langle b \rangle = A$. The submodule IM is called the *expansion* of I to M. The *annihilator ideal* of M in A is defined as $ann_A(M) := \{a \in A : am = 0, \forall m \in M\}$. $\mathcal{L}(A)$ is the set of ideals of A. The *length* of M, denoted by $\ell_A(M)$, is the length of a composition series for M. If the ring A has the unique maximal ideal \mathfrak{m} , then it is called *local*, $k = A/\mathfrak{m}$ its *residue* field and it will be denoted by the triple $(A, \mathfrak{m}, GF(q))$. If $(A, \mathfrak{m}, GF(q))$ is a finite local ring, then $|\mathsf{M}| = |\mathsf{GF}(q)|^{\ell_A(M)}$. There is an integer $t \geq 1$ such that $\mathfrak{m}^t = \langle 0 \rangle$ and $\mathfrak{m}^{t-1} \neq \langle 0 \rangle$, called the *nilpotency index* of \mathfrak{m} , and $t \leq \ell_A(A)$, (see [2]). A subset G of M generates M if and only if its image \overline{G} in M/ \mathfrak{m} M generates M/ \mathfrak{m} M as a GF(q)-vector space. A set of generators for M obtained from lifting a basis of the GF(q)-vector space M/ \mathfrak{m} M is called a *minimal* A-generating set for the A-module M, (see [10], Theorem V.5). Note that $v_A(M) = \dim_{\mathrm{GF}(q)}(M/\mathfrak{m}M) = \ell_A(M/\mathfrak{m}M)$.

Let $(A, \mathfrak{m}, GF(q))$ be a finite local ring and $\bar{}: A[T] \to GF(q)[T]$ the natural ring homomorphism that maps $a \mapsto a + \mathfrak{m}$ and the variable T to T. The polynomial $f \in A[T]$ is called *basic irreducible* if \bar{f} is irreducible in GF(q)[T]. Hensel's Lemma (see [10], Theorem XIII.4) guarantees that factorization as a product of pairwise coprime polynomials in GF(q)[T] lifts to such a factorization over A. Hence if γ is a unit of A and (n, q) = 1 there exists a unique family of monic basic irreducible pairwise coprime polynomials $f_1, \ldots, f_r \in A[T]$ such that $T^n - \gamma = f_1 \cdots f_r$. If g_1, \ldots, g_k are basic irreducible polynomials such that $T^n - \gamma$ is an associate of $g_1 \cdots g_k$, then r = k and, after renumbering, f_i is an associate of g_i , $1 \le i \le r$. And if $g_1, \ldots, g_k \in A[T]$ are monic polynomials such that $T^n - \gamma = g_1 \cdots g_k$, then g_1, \ldots, g_k are pairwise coprime, $r \ge k$ and there is a partition of $\{1, 2, \ldots, r\}$, U_1, \ldots, U_k such that $g_i = \prod_{u \in U_i} f_u$, (see [3]).

A finite ring A is called a *chain ring* if the lattice of its ideals is a chain under set-theoretic inclusion. The ring A is a finite chain ring if and only if A is local and its maximal ideal is principal if and only if A is local and $\ell_A(A) = t$, where t is the nilpotency index of the maximal ideal of A, (see [4]). A finite local ring $(A, \mathfrak{m}, GF(q))$ is *Frobenius* if $\operatorname{ann}_A(\mathfrak{m})$ is the unique minimal ideal, (see [11]).

Let $(A, \mathfrak{m}, GF(q))$ be a finite local ring, t the nilpotency index of $\mathfrak{m}, f \in A[T]$ be a basic irreducible polynomial and $s = \deg(\overline{f})$. There is a monic polynomial g in A[T] and a unit v in A[T] such that $\overline{f} = \overline{g}$ and g = vf (see [10], Theorem XIII.6). Let $B = A[T]/\langle f \rangle = A[T]/\langle g \rangle = \{a_0 + a_1T + \cdots + a_{s-1}T^{s-1} : a_i \in A\}$. This ring is called the separable extension of A determined by f and has the following properties (see [2], [3] and [10]): (a) B is local with maximal ideal $\mathfrak{m}B$ and residue field $GF(q^s)$; (b) if $\mathbb{T} \subset A$ is a set of representatives of GF(q) the set $\mathbb{T}_s := \{a_0 + a_1T + \cdots + a_{s-1}T^{s-1} : a_i \in \mathbb{T}\} \subset B$ is a set of representatives of $GF(q^s)$; (c) if I is an ideal of A, then $\ell_A(I) = \ell_B(IB)$; (d) $(\operatorname{ann}_A(I))B = \operatorname{ann}_B(IB)$; (e) if $\{\alpha_1, \ldots, \alpha_l\}$ is a minimal A-generating set for I, then it is also a minimal B-generating set for IB and $v_A(I) = v_B(IB)$; (f) The nilpotency index of $\mathfrak{m}B$ is t; (g) A is a chain ring if and only if B is a chain ring; (h) A is a Frobenius ring if and only if B is a Frobenius ring, the unique minimal ideal of B is $\operatorname{ann}_B(\mathfrak{m}B) = \operatorname{ann}_A(\mathfrak{m})B = \mathfrak{m}^{t-1}B$; (i) If I is an ideal of A, then $\operatorname{ann}_A(\operatorname{ann}_A(I)) = I$ and $\ell_A(\operatorname{ann}_A(I)) + \ell_A(I) = \ell_A(A)$.

A $(k \times n)$ matrix over the field GF(q) is said to be in reduced row echelon form, (rre)-form, if in each row i = 1, ..., k, the first nonzero entry is equal to 1, the index of the column in which the 1 occurs, called a *pivotal column*, strictly increases with i, and the k pivotal columns are, in order, the columns of the $(k \times k)$ identity matrix.

The following result describes the submodules between M and $\mathfrak{m}M$, where M is a module over the local ring $(A, \mathfrak{m}, GF(q))$, (see [2]).

Lemma 2.1. Let $(A, \mathfrak{m}, GF(q))$ be a finite local ring, $\mathbb{T} \subset A$ a set of representatives of GF(q), M an A-module and $\{\alpha_1, \ldots, \alpha_l\}$ be a minimal A-generating set for M. Then the A-submodules of M between M and $\mathfrak{m}M$ of length $k + \ell_A(\mathfrak{m}M)$, where $0 < k < l = \dim_{GF(q)}(M/\mathfrak{m}M)$, are in one to one correspondence with the $(k \times l)$ matrices over GF(q) in (rre)-form. The matrix $H = (\bar{a}_{ij})$ corresponds to the submodule $\langle \sum_{i=1}^n a_{1i}\alpha_i, \ldots, \sum_{i=1}^n a_{ki}\alpha_i \rangle + \mathfrak{m}M$.

The following result is a consequence of the previous result, when $v_A(M) = \ell_A(M) - \ell_A(\mathfrak{m}M) = 2$. Recall that (0, 1) and $(1, \lambda)$, where $\lambda \in GF(q)$, are all the 1×2 matrices in (rre)-form over GF(q).

Corollary 2.2. Let $(A, \mathfrak{m}, GF(q))$ be a finite local ring, $\mathbb{T} \subset A$ a set of representatives of GF(q), M an A-module with $v_A(M) = 2$ and $\{\alpha_1, \alpha_2\}$ a minimal A-generating set for M. Then the A-submodules of M between M and $\mathfrak{m}M$ of length $1 + \ell_A(\mathfrak{m}M)$ are:

 $\langle \alpha_2 \rangle + \mathfrak{m}M, \langle \alpha_1 + \lambda_1 \alpha_2 \rangle + \mathfrak{m}M, \langle \alpha_1 + \lambda_2 \alpha_2 \rangle + \mathfrak{m}M, \dots, \langle \alpha_1 + \lambda_q \alpha_2 \rangle + \mathfrak{m}M, \lambda_i \in \mathbb{T}.$

3 Some isomorphism between local rings

We present results on particular finite local rings and results on finite fields which we will use later. Some of them may be found in the literature but we include them all here for completeness.

The following result is a well-know fact on finite local rings, (see [10], Theorem XVII.1).

Theorem 3.1 (Structure Theorem for Finite Local Rings). Let (A, \mathfrak{m}, k) be a finite local ring of characteristic p^k , $\{\alpha_1, \ldots, \alpha_l\}$ a minimal A-generating set of \mathfrak{m} and $d = [k : \mathbb{F}_p]$. Then a subring S of A exists such that

- (a) S ≃ GR(p^k, d), S is unique and is the largest Galois ring extension of Z_{p^k} in A.
- (b) A is a homomorphic image of $S[X_1, \ldots, X_l]$, i.e., $A = S[\alpha_1, \ldots, \alpha_l]$.

For the next result see [2].

Lemma 3.2. Let I be an ideal of the ring $GR(p^k, d)[X_1, \ldots, X_l]$ such that for all $i \in \{1, \ldots, l\}$, $X_i^{k_i} \in I$, for some $k_i \in \mathbb{N}$. Then the ring

$$\operatorname{GR}(p^k, d)[X_1, \ldots, X_l]/I$$

is local with maximal ideal $\langle p, X_1, \ldots, X_l \rangle / I$ and residue field $GF(p^d)$.

For the next result recall that any ideal of the ring $GR(p^k, d)[X_1, \ldots, X_l]$ is finitely generated.

Corollary 3.3. Let $(A, \mathfrak{m}, \operatorname{GF}(p^d))$ and $(A_1, \mathfrak{m}_1, \operatorname{GF}(p_1^{d_1}))$ be finite local rings, char $(A) = p^k$ and $v_A(\mathfrak{m}) = l$. By Theorem 3.1, let $\psi : \operatorname{GR}(p^k, d)[X_1, \ldots, X_l] \to A$ an epimorphism and ker $(\psi) = \langle g_1, \ldots, g_r \rangle$. Then $A \cong A_1$ if and only if $|A| = |A_1|, p = p_1, d = d_1, \operatorname{char}(A_1) = \operatorname{char}(A), v_{A_1}(\mathfrak{m}_1) = v_A(\mathfrak{m})$ and a minimal A_1 -generating set for \mathfrak{m}_1 exists, $\{\alpha_1, \ldots, \alpha_l\}$, such that $g_1(\alpha_1, \ldots, \alpha_l) = \ldots = g_r(\alpha_1, \ldots, \alpha_l) = 0$ in A_1 . Proof: \Rightarrow) We have $|\mathbf{A}| = |\mathbf{A}_1|$, $p = p_1$, $d = d_1$, $\operatorname{char}(\mathbf{A}_1) = \operatorname{char}(\mathbf{A})$, $\mathbf{v}_{\mathbf{A}_1}(\mathbf{m}_1) = \mathbf{v}_{\mathbf{A}}(\mathbf{m})$ and we may assume that the Galois ring $\operatorname{GR}(p^k, d) \subset \mathbf{A}_1$. If $\varphi : \mathbf{A} \to \mathbf{A}_1$ is an isomorphism, then $\{\varphi\psi(\mathbf{X}_1), \ldots, \varphi\psi(\mathbf{X}_l)\}$ is a minimal \mathbf{A}_1 -generating set for \mathbf{m}_1 and $\mathbf{g}_i(\varphi\psi(\mathbf{X}_1), \ldots, \varphi\psi(\mathbf{X}_l)) = \varphi\psi(\mathbf{g}_i) = \varphi(0) = 0$, $i \in \{1, \ldots, r\}$. Conversely: by Theorem 3.1, let the epimorphism $\psi_1 : \operatorname{GR}(p^k, d)[\mathbf{X}_1, \ldots, \mathbf{X}_l] \to \mathbf{A}_1$ given by $\mathbf{X}_i \mapsto \alpha_i$, then $\operatorname{ker}(\psi) \subseteq \operatorname{ker}(\psi_1)$ and there is an epimorphism from $\mathbf{A} \cong \operatorname{GR}(p^k, d)[\mathbf{X}_1, \ldots, \mathbf{X}_l]/\operatorname{ker}(\psi)$ to $\operatorname{GR}(p^k, d)[\mathbf{X}_1, \ldots, \mathbf{X}_l]/\operatorname{ker}(\psi_1) \cong \mathbf{A}_1$. The assertion follows from the relation $|\mathbf{A}| = |\mathbf{A}_1|$.

Lemma 3.4. Let $\mathbb{F} = GF(p^d)$ be a finite field.

- (1) If $u, v \in \mathbb{F}$ are such that $\sqrt{u} \notin \mathbb{F}$ and $\sqrt{v} \notin \mathbb{F}$, then $\sqrt{uv} \in \mathbb{F}$.
- (2) Let $\rho, \eta, \sigma \in \mathbb{F}$ with $\rho \neq 0$ and $\rho\sigma \neq \eta$. The solutions of the system of equations $BB_1 = \rho B^2 \dots (a), AA_1 - \rho A^2 - \sigma B^3 = 0 \dots (b), B_1^2 = \rho BB_1 \dots (c), A_1^2 - \rho AA_1 - \eta B^3 = 0 \dots (d), AB_1 - A_1 B \neq 0 \dots (e)$ are: If $p = 2, A = \frac{\sigma \sqrt{B^3}}{\sqrt{\rho\sigma + \eta}}, A_1 = \frac{\eta \sqrt{B^3}}{\sqrt{\rho\sigma + \eta}}, B_1 = \rho B, B \in \mathbb{F}^*$. If p is odd and $\sigma = 0$, then $\eta \neq 0, A = 0, B = \eta, A_1 = \pm \eta^2, B_1 = \rho \eta$. If p is odd and $\sigma \neq 0, A = \pm \frac{\eta - \rho \sigma}{\sigma^2} a^3, B = \frac{\eta - \rho \sigma}{\sigma^2} a^2, A_1 = \pm \frac{(\eta - \rho \sigma)\eta}{\sigma^3} a^3, B_1 = \frac{(\eta - \rho \sigma)\rho}{\sigma^2} a^2, a \in \mathbb{F}^*$.
- (3) Let $u, v \in \mathbb{F}$ with $u \neq 0$. Some solution of the system of equations $AA_1 = vB_1^3 \dots (a), BB_1 = 0 \dots (b), B^2 = 0 \dots (c), A^2 = uB_1^3 \dots (d), AB_1 A_1B \neq 0 \dots (e)$ are $A = \pm \frac{a^3}{u}, B = 0, A_1 = \pm \frac{va^3}{u^2}, B_1 = \frac{a^2}{u}$, where $a \in \mathbb{F}^*$.

Lemma 3.5. Let $\mathbb{F} = GF(p^d)$ be the finite field $u, u_1, v, r, r_1, s, s_1 \in \mathbb{F}$ with $uu_1 \neq 0, r$ and s not both zero and r_1 and s_1 not both zero. Let $u_1AA_1 + B_1C + BC_1 - vB_1^3 = 0...(a), u_1A^2 + 2BC - uB_1^3 = 0...(b), BB_1 = 0...(c), B^2 = 0...(d), u_1rA_1^2 + 2rB_1C_1 + sB_1^3 = s_1...(e), rB_1^2 = r_1...(f), AB_1 - A_1B \neq 0...(g).$

(1) If $r \neq 0$ (if and only if $r_1 \neq 0$) the system of equations has solution if and only if $\frac{r_1}{r} \in \mathbb{F}^2$ and $\sqrt{\frac{r_1}{r}} \frac{u}{u_1} \in \mathbb{F}^2$,

(a) If
$$p = 2$$
 some solutions are $A = \sqrt{\frac{r_1}{r}} \sqrt{\sqrt{\frac{r_1}{r}} \frac{u}{u_1}}$, $B = 0$, $C = \frac{vr_1}{r} + \frac{r_1}{r} \sqrt{\frac{us}{r}} + \sqrt{\frac{s_1u}{r}} \sqrt{\frac{r_1}{r}}$, $A_1 = \sqrt{\sqrt{\frac{r}{r_1}} \frac{s_1}{ru_1}} \frac{r_1}{r} + \sqrt{\frac{s_1}{ru_1}}$, $B_1 = \sqrt{\frac{r_1}{r}}$, $C_1 \in \mathbb{F}$.

(b) If $p \neq 2$ some solutions are $A = \sqrt{\frac{r_1}{r}} \sqrt{\sqrt{\frac{r_1}{r}} \frac{u}{u_1}}$, B = 0, $C \in \mathbb{F}$, $A_1 = -\sqrt{\sqrt{\frac{r_1}{r_1} \frac{u}{u}} \frac{C}{u_1}} + \sqrt{\sqrt{\frac{r_1}{r_1} \frac{u}{u}} \frac{vr_1}{u_1r}}$, $B_1 = \sqrt{\frac{r_1}{r}}$, $C_1 = \frac{s_1}{2r} \sqrt{\frac{r}{r_1}} - \frac{C^2r}{2ur_1} - \frac{v^2r_1}{2ur} + \frac{Cv}{u} - \frac{sr_1}{2r^2}$.

(2) If r = 0 (and then $s \neq 0$ and $s_1 \neq 0$) the system of equations has solution if and only if $\frac{s_1}{s} \in \mathbb{F}^3$ and $\frac{s_1u}{su_1} \in \mathbb{F}^2$.

(a) Some solutions are $A = \sqrt{\frac{s_1 u}{s u_1}}$, B = 0, $C \in \mathbb{F}$, $A_1 = -\frac{C}{u_1} \sqrt[3]{\frac{s_1}{s}} \sqrt{\frac{s u_1}{s_1 u}} + \frac{v}{u_1} \sqrt{\frac{s_1 u_1}{s u}}$, $B_1 = \sqrt[3]{\frac{s_1}{s}}$, $C_1 \in \mathbb{F}$.

Lemma 3.6. Let $\mathbb{F} = GF(p^d)$ be the finite field, $u, r, s, \eta, \sigma, \rho, f, g$ with $u\rho \neq 0$, $\rho\sigma \neq \eta, r$ and s not both zero and f and g not both zero. Let $fB_1^2 = r...(a)$, $fuA_1^2 + 2fB_1C_1 + gB_1^3 = s...(b)$, $BB_1 - \rho B^2 = 0...(c)$, $BC_1 + B_1C + uAA_1 - u\rho A^2 - 2\rho BC - \sigma B^3 = 0...(d)$, $B_1^2 - \rho BB_1 = 0...(e)$, $uA_1^2 + 2B_1C_1 - \rho BC_1 - \rho B_1C - u\rho AA_1 - \eta B^3 = 0...(f)$, $AB_1 - A_1B \neq 0...(g)$.

(1) If $r \neq 0$ (if and only if $f \neq 0$) the system of equations has solution if and only if $\frac{r}{f} \in \mathbb{F}^2$ and $\frac{\eta - \sigma \rho}{u\rho} \sqrt{\frac{r}{f}} \in \mathbb{F}^2$.

(a) If
$$p = 2$$
 the solutions are:

$$A = \frac{1}{f\rho}\sqrt{\frac{gr}{u}\sqrt{\frac{r}{f}}} + \frac{1}{\rho}\sqrt{\frac{s}{fu}} + \frac{1}{\rho^2}\sqrt{\frac{r}{f}}\sqrt{\frac{\eta-\sigma\rho}{u\rho}\sqrt{\frac{r}{f}}}, \quad B = \frac{1}{\rho}\sqrt{\frac{r}{f}}, \quad C \in \mathbb{F},$$

$$A_1 = \frac{1}{f}\sqrt{\frac{gr}{u}\sqrt{\frac{r}{f}}} + \sqrt{\frac{s}{fu}}, \quad B_1 = \sqrt{\frac{r}{f}}, \quad C_1 = \rho C + \frac{r\eta}{f\rho^3} + \frac{r}{f^2\rho}\sqrt{\frac{fg(\eta-\sigma\rho)}{\rho}} + \frac{1}{\rho}\sqrt{\frac{s(\eta-\sigma\rho)}{f\rho}\sqrt{\frac{r}{f}}}.$$

(b) If p is odd, the solutions are:

$$\mathbf{A} \in \mathbb{F}, \ \mathbf{B} = \frac{1}{\rho} \sqrt{\frac{r}{f}}, \ \mathbf{C} = -\frac{\mathbf{A}^2 u\rho}{2} \sqrt{\frac{f}{r}} - \frac{r}{2f^2 \rho^4} [f(\eta + \sigma\rho) + g\rho^3] + \frac{s}{2f\rho} \sqrt{\frac{f}{r}},$$

$$\mathbf{A}_1 = \rho \mathbf{A} \pm \frac{1}{\rho} \sqrt{\frac{r}{f}} \sqrt{\frac{\eta - \sigma\rho}{u\rho}} \sqrt{\frac{r}{f}}, \ \mathbf{B}_1 = \sqrt{\frac{r}{f}}, \ \mathbf{C}_1 = -\frac{u\rho^2 \mathbf{A}^2}{2} \sqrt{\frac{f}{r}} - \frac{r(\eta - \sigma\rho)}{2f\rho^3} \mp$$

$$\mathbf{A} u \sqrt{\frac{\eta - \sigma\rho}{u\rho}} \sqrt{\frac{r}{f}} - \frac{gr}{2f^2} + \frac{s}{2f} \sqrt{\frac{f}{r}}.$$

(2) If r = 0 (if and only if f = 0) then $s \neq 0$ and $g \neq 0$ and the system of equations has solution if and only if $\frac{s}{g} \in \mathbb{F}^3$ and $\frac{(\eta - \sigma \rho)s}{ug\rho} \in \mathbb{F}^2$. The solutions are:

A
$$\in \mathbb{F}$$
, B $= \frac{1}{\rho} \sqrt[3]{\frac{s}{g}}$, C $\in \mathbb{F}$, A₁ $= \rho A \pm \frac{1}{\rho} \sqrt{\frac{(\eta - \sigma \rho)s}{ug\rho}}$, B₁ $= \sqrt[3]{\frac{s}{g}}$, C₁ $= \rho C \mp Au \sqrt[3]{\frac{g}{s}} \sqrt{\frac{(\eta - \sigma \rho)s}{ug\rho}} + \frac{\sigma}{\rho^2} \sqrt[3]{\frac{s^2}{g^2}}$.

For the rest of this paper, for α in the ring $\operatorname{GR}(p^k, d)$, the class $\alpha + \langle p \rangle$ is denoted by $\overline{\alpha}$.

Recall the following: (1) 3 $/p^d - 1$ if and only if $GF(p^d)^3 = GF(p^d)$, (2) $3|p^d - 1|^2 = GF(p^d)$, (2) $3|p^d - 1|^2 = GF(p^d)$

if and only if $\operatorname{GF}(p^d)^3 \subset \operatorname{GF}(p^d)$ and in the last case the set of representatives for the group $\operatorname{GF}(p^d)^*/[\operatorname{GF}(p^d)^*]^3$ is $\{\operatorname{GF}(p^d)^{*3}, \zeta \operatorname{GF}(p^d)^{*3}, \zeta^2 \operatorname{GF}(p^d)^{*3}\}$, where ζ is a primitive element of $\operatorname{GF}(p^d)$.

Lemma 3.7. Let $\mathbb{T} = \{0, 1, \ldots, \zeta^{p^d-2}\}$ be the Teichmüller set of the Galois ring $\operatorname{GR}(p^2, d)$, $u, v, r, s, \eta, \sigma, \rho, f, g \in \mathbb{T}$, with $u\rho \neq 0$, $\overline{\rho\sigma} \neq \overline{\eta}$, r and s not both zero and f and g not both zero. Let $A_{(u,v,r,s)}$ given by $\operatorname{GR}(p^2, d)[X,Y]/\langle rY^2 + sY^3 - p, X^2 - uY^3, XY - vY^3, X^4, X^3Y, X^2Y^2, XY^3, Y^4\rangle$ and $B_{(\eta,\sigma,\rho,f,g)}$ given by $\operatorname{GR}(p^2, d)[X,Y]/\langle fY^2 + gY^3 - p, XY - \rho X^2 - \sigma X^3, Y^2 - \rho XY - \eta X^3, X^4, X^3Y, X^2Y^2, XY^3, Y^4\rangle$. Then the rings $A_{(u,v,r,s)}$ and $B_{(\eta,\sigma,\rho,f,g)}$ are isomorphic to one of the following rings:

(a) If
$$r \neq 0$$
 and $p = 2$.
(1) $A_{(1,0,1,0)} = GR(2^2, d)[X, Y]/\langle Y^2 - 2, X^2 - Y^3, XY \rangle$.

- (b) If $r \neq 0$ and p is odd.
 - $\begin{array}{l} (1) \ \mathbf{A}_{(1,0,1,0)} = \mathrm{GR}(p^2,d)[\mathbf{X},\mathbf{Y}]/\langle\mathbf{Y}^2 p,\mathbf{X}^2 \mathbf{Y}^3,\mathbf{XY}\rangle; \\ (2) \ \mathbf{A}_{(1,0,\zeta,0)} = \mathrm{GR}(p^2,d)[\mathbf{X},\mathbf{Y}]/\langle\zeta\mathbf{Y}^2 p,\mathbf{X}^2 \mathbf{Y}^3,\mathbf{XY}\rangle; \\ (3) \ \mathbf{A}_{(\zeta,0,1,0)} = \mathrm{GR}(p^2,d)[\mathbf{X},\mathbf{Y}]/\langle\mathbf{Y}^2 p,\mathbf{X}^2 \zeta\mathbf{Y}^3,\mathbf{XY}\rangle; \\ (4) \ \mathbf{A}_{(\zeta,0,\zeta,0)} = \mathrm{GR}(p^2,d)[\mathbf{X},\mathbf{Y}]/\langle\zeta\mathbf{Y}^2 p,\mathbf{X}^2 \zeta\mathbf{Y}^3,\mathbf{XY}\rangle. \end{array}$
- $\begin{array}{ll} (c) & If \ r=0, \ p=2 \ and \ 3|2^d-1. \\ (1) \ \mathbf{A}_{(1,0,0,1)} = \mathrm{GR}(2^2,d)[\mathbf{X},\mathbf{Y}]/\langle\mathbf{Y}^3-2,\mathbf{X}^2-\mathbf{Y}^3,\mathbf{X}\mathbf{Y}\rangle; \\ (2) \ \mathbf{A}_{(1,0,0,\zeta)} = \mathrm{GR}(2^2,d)[\mathbf{X},\mathbf{Y}]/\langle\zeta\mathbf{Y}^3-2,\mathbf{X}^2-\mathbf{Y}^3,\mathbf{X}\mathbf{Y}\rangle; \\ (3) \ \mathbf{A}_{(1,0,0,\zeta^2)} = \mathrm{GR}(2^2,d)[\mathbf{X},\mathbf{Y}]/\langle\zeta^2\mathbf{Y}^3-2,\mathbf{X}^2-\mathbf{Y}^3,\mathbf{X}\mathbf{Y}\rangle. \end{array}$
- $\begin{array}{ll} (d) \ \ I\!f \ r=0, \ p=2 \ \ and \ 3 \ \ /\!\!\!/ 2^d-1. \\ (1) \ \ \mathbf{A}_{(1,0,0,1)}=\mathrm{GR}(2^2,d)[\mathbf{X},\mathbf{Y}]/\langle \mathbf{Y}^3-2,\mathbf{X}^2-\mathbf{Y}^3,\mathbf{X}\mathbf{Y}\rangle. \end{array}$
- $\begin{array}{ll} (e) & If \ r=0, \ p \ is \ odd \ and \ 3|p^d-1. \\ (1) \ \mathbf{A}_{(1,0,0,1)} = \mathrm{GR}(p^2,d)[\mathbf{X},\mathbf{Y}]/\langle\mathbf{Y}^3-p,\mathbf{X}^2-\mathbf{Y}^3,\mathbf{XY}\rangle; \\ (2) \ \mathbf{A}_{(1,0,0,\zeta)} = \mathrm{GR}(p^2,d)[\mathbf{X},\mathbf{Y}]/\langle\zeta\mathbf{Y}^3-p,\mathbf{X}^2-\mathbf{Y}^3,\mathbf{XY}\rangle; \\ (3) \ \mathbf{A}_{(1,0,0,\zeta^2)} = \mathrm{GR}(p^2,d)[\mathbf{X},\mathbf{Y}]/\langle\zeta^2\mathbf{Y}^3-p,\mathbf{X}^2-\mathbf{Y}^3,\mathbf{XY}\rangle; \\ (4) \ \mathbf{A}_{(\zeta,0,0,1)} = \mathrm{GR}(p^2,d)[\mathbf{X},\mathbf{Y}]/\langle\mathbf{Y}^3-p,\mathbf{X}^2-\zeta\mathbf{Y}^3,\mathbf{XY}\rangle; \\ (5) \ \mathbf{A}_{(\zeta,0,0,\zeta)} = \mathrm{GR}(p^2,d)[\mathbf{X},\mathbf{Y}]/\langle\zeta\mathbf{Y}^3-p,\mathbf{X}^2-\zeta\mathbf{Y}^3,\mathbf{XY}\rangle; \\ (6) \ \mathbf{A}_{(\zeta,0,0,\zeta^2)} = \mathrm{GR}(p^2,d)[\mathbf{X},\mathbf{Y}]/\langle\zeta^2\mathbf{Y}^3-p,\mathbf{X}^2-\zeta\mathbf{Y}^3,\mathbf{XY}\rangle. \end{array}$
- (f) If r = 0, p is odd and $3 \not| p^d 1$. (1) $A_{(1,0,0,1)} = GR(p^2, d)[X, Y]/\langle Y^3 - p, X^2 - Y^3, XY \rangle$; (2) $A_{(\zeta,0,0,1)} = GR(p^2, d)[X, Y]/\langle Y^3 - p, X^2 - \zeta Y^3, XY \rangle$.

Proof: We have $A_{(u,v,r,s)} = GR(p^2, d)[X, Y]/\langle rY^2 + sY^3 - p, X^2 - uY^3, XY - vY^3, Y^4 \rangle$, $B_{(\eta,\sigma,\rho,f,g)} = GR(p^2, d)[X, Y]/\langle fY^2 + gY^3 - p, XY - \rho X^2 - \sigma X^3, Y^2 - \rho XY - \eta X^3, X^4 \rangle$ and, by Lemma 3.2, the rings $A_{(u,v,r,s)}$ and $B_{(\eta,\sigma,\rho,f,g)}$ are

local with maximal ideal $\langle \mathbf{x}, \mathbf{y} \rangle$ and residue field $GF(p^d)$. First we consider the ring $A_{(u,v,r,s)}$. In the ring $A_{(u,v,r,s)}$ the relations $p = ry^2 + sy^3$, $py = ry^3$, $p\mathbf{x} = r\mathbf{x}\mathbf{y}^2 + s\mathbf{x}\mathbf{y}^3 = 0$ are satisfied, then every element of the ring $A_{(u,v,r,s)}$ can be uniquely written as $a_0 + a\mathbf{x} + b\mathbf{y} + c\mathbf{y}^2 + d\mathbf{y}^3$, where $a_0, a, b, c, d \in \mathbb{T}$, the elements of its maximal ideal are $a\mathbf{x} + b\mathbf{y} + c\mathbf{y}^2 + d\mathbf{y}^3$, where $a, b, c, d \in \mathbb{T}$.

Observe that for $u, v, r, s, u_1, r_1, s_1 \in \mathbb{T}$ such that $uu_1 \neq 0, r$ and s not both zero and r_1 and s_1 not both zero, by Corollary 3.3, $A_{(u,v,r,s)} \cong A_{(u_1,0,r_1,s_1)}$ if and only if there exist $a, a_1, b, b_1, c, c_1 \in \mathbb{T}$ such that $\{\alpha = ax + by + cy^2, \beta = a_1x + b_1y + c_1y^2\}$ is a minimal $A_{(u_1,0,r_1,s_1)}$ -generating set for the maximal ideal of $A_{(u_1,0,r_1,s_1)}$, hence $\overline{ab_1} - \overline{a_1b} \neq 0$, and these elements must satisfy the relations satisfied by x and y in $A_{(u,v,r,s)}$, i.e., $\alpha\beta - v\beta^3 = 0, \alpha^2 - u\beta^3 = 0, r\beta^2 + s\beta^3 = p$. From these relations and the expression for α and β we have: $(u_1aa_1 + b_1c + bc_1 - vb_1^3)y^3 + bb_1y^2 = 0, (u_1a^2 + 2bc - ub_1^3)y^3 + b^2y^2 = 0$ and $(u_1ra_1^2 + 2rb_1c_1 + sb_1^3)y^3 + rb_1^2y^2 = s_1y^3 + r_1y^2$. These last relations hold if and only if $a, a_1, b, b_1, c, c_1 \in \mathbb{T}$ exist such that $\overline{u_1}\overline{aa_1} + \overline{b_1}\overline{c} + \overline{bc_1} - \overline{vb_1}^3 = 0, \overline{u_1}\overline{a^2} + 2\overline{bc} - \overline{ub_1}^3 = 0, \overline{bb_1} = 0, \overline{b^2} = 0, \overline{u_1}\overline{ra_1}^2 + 2\overline{rb_1}\overline{c_1} + \overline{sb_1}^3 = \overline{s_1}, \overline{rb_1}^2 = \overline{r_1}, \overline{ab_1} - \overline{a_1}\overline{b} \neq 0$ if and only if $a, a_1, b, b_1, c, c_1 \in \mathbb{T}$ exist such that $\overline{a}, \overline{a_1}, \overline{b}, \overline{b_1}, \overline{c}, \overline{c_1}$ are solutions of the system of equations of Lemma 3.5.

From the above argument it is easy to see that an isomorphism between $A_{(u,v,r,s)}$ and $A_{(u_1,0,r_1,s_1)}$ is given by $\mathbf{x} \mapsto a\mathbf{x}+b\mathbf{y}+c\mathbf{y}^2$ and $\mathbf{y} \mapsto a_1\mathbf{x}+b_1\mathbf{y}+c_1\mathbf{y}^2$, where $a, a_1, b, b_1, c, c_1 \in \mathbb{T}$ are such that $\overline{a}, \overline{a}_1, \overline{b}, \overline{b}_1, \overline{c}, \overline{c}_1$ are solutions of the equations of Lemma 3.5.

Now for the case $B_{(\eta,\sigma,\rho,f,g)} \cong A_{(u,0,r,s)}$, we use Lemma 3.6 and the same arguments as above. That is, if we affirm $B_{(\eta,\sigma,\rho,f,g)} \cong A_{(u,0,r,s)}$, then there is a minimal generating set $\{\alpha = ax + by + cy^2 + dy^3, \beta = a_1x + b_1y + c_1y^2 + d_1y^3\}$ of the maximal ideal of $A_{(u,0,r,s)}$, where $a, a_1, b, b_1, c, c_1, d, d_1 \in \mathbb{T}$ satisfy $\overline{fb}_1^2 = \overline{r}$, $\overline{fua}_1^2 + 2\overline{fb}_1\overline{c}_1 + \overline{gb}_1^3 = \overline{s}, \overline{bb}_1 - \overline{\rho}\overline{b}^2 = 0, \overline{bc}_1 + \overline{b}_1\overline{c} + \overline{uaa}_1 - \overline{\rho}\overline{ua}^2 - 2\overline{\rho}\overline{b}\overline{c} - \overline{\sigma}\overline{b}^3 = 0$, $\overline{b}_1^2 - \overline{\rho}\overline{bb}_1 = 0, \overline{ua}_1^2 + 2\overline{b}_1\overline{c}_1 - \overline{\rho}\overline{b}\overline{c}_1 - \overline{\rho}\overline{b}_1\overline{c} - \overline{\rho}\overline{uaa}_1 - \overline{\eta}\overline{b}^3 = 0$ and $\overline{ab}_1 - \overline{a}_1\overline{b} \neq 0$. And the assertion follows.

Lemma 3.8. Let $u, v, \eta, \sigma, \rho \in GF(p^d)$ with $u\rho \neq 0$, $\rho\sigma \neq \eta$. Let $A_{(u,v)} = GF(p^d)[X, Y]/\langle X^2 - uY^3, XY - vY^3, X^4, X^3Y, X^2Y^2, XY^3, Y^4 \rangle$ and $B_{(\eta,\sigma,\rho)} = GF(p^d)[X, Y]/\langle XY - \rho X^2 - \sigma X^3, Y^2 - \rho XY - \eta X^3, X^4, X^3Y, X^2Y^2, XY^3, Y^4 \rangle$. Then the rings $A_{(u,v)}$ and $B_{(\eta,\sigma,\rho)}$ are isomorphic to the ring:

$$A_{(1,0)} = GF(p^d)[X,Y]/\langle X^2 - Y^3, XY \rangle.$$

Proof: The same arguments as in Lemma 3.7, and using (2) and (3) of Lemma 3.4, can be followed.

Lemma 3.9. Let $\mathbb{T} = \{0, 1, \dots, \zeta^{p^d-2}\}$ be the Teichmüller set of the Galois ring $\operatorname{GR}(p^4, d)$ and $u, v, \eta, \sigma, \rho \in \mathbb{T}$ with $u\rho \neq 0$ and $\overline{\rho\sigma} \neq \overline{\eta}$. Let $A_{(u,v)}$

given by $\operatorname{GR}(p^4, d)[X, Y]/\langle X-p, Y^2-uX^3, XY-vX^3, X^4, X^3Y, X^2Y^2, XY^3, Y^4\rangle$ and $B_{(\eta,\rho,\sigma)}$ given by $GR(p^4,d)[X,Y]/\langle X-p,XY-\rho X^2-\sigma X^3,Y^2-\rho XY-\eta X^3,X^4,X^3Y,X^2Y^2,XY^3,Y^4\rangle$. Then the rings $A_{(u,v)}$ and $B_{(\eta,\rho,\sigma)}$ are isomorphic to one of the following rings:

- (a) If p = 2(1) $A_{(1,0)} = GR(2^4, d)[X]/\langle X^2 - 2^3, 2X \rangle.$
- (b) If p is odd (1) $A_{(1,0)} = GR(p^4, d)[X]/\langle X^2 - p^3, pX \rangle;$ (2) $A_{(\zeta,0)} = GR(p^4, d)[X]/\langle X^2 - \zeta p^3, pX \rangle.$

Proof: The same arguments as in Lemma 3.7 can be followed. And observe that $A_{(\zeta,0)} \cong A_{(1,0)}$ if and only if $\overline{\zeta} \in GF(p^d)^2$ if and only if p = 2.

Lemma 3.10. Let $\mathbb{T} = \{0, 1, \dots, \zeta^{p^d-2}\}$ be the Teichmüller set of the Galois $ring \ \mathrm{GR}(p^3,d), \ u,v \in \mathbb{T} \ with \ u \neq 0 \ and \ \mathbf{A}_{(u,v)} = \mathrm{GR}(p^3,d)[\mathbf{X},\mathbf{Y}]/\langle \mathbf{X}-p,\mathbf{X}^2-p,\mathbf{X}$ $uY^3, XY - vY^3, X^4, X^3Y, X^2Y^2, XY^3, Y^4\rangle$. Then the ring $A_{(u,v)}$ is isomorphic to one of the following rings:

(a) $3 \not p^d - 1$ (1) $A_{(1 \ 0)} = GR(p^3, d)[X]/\langle p^2 - X^3, pX \rangle.$ (b) $3|p^d - 1$ $\begin{array}{l} \text{(1)} & \mathbf{A}_{(1,0)} = \mathrm{GR}(p^3,d)[\mathbf{X}]/\langle p^2 - \mathbf{X}^3,p\mathbf{X} \rangle \\ \text{(2)} & \mathbf{A}_{(\zeta,0)} = \mathrm{GR}(p^3,d)[\mathbf{X}]/\langle p^2 - \zeta \mathbf{X}^3,p\mathbf{X} \rangle \\ \text{(3)} & \mathbf{A}_{(\zeta^2,0)} = \mathrm{GR}(p^3,d)[\mathbf{X}]/\langle p^2 - \zeta^2 \mathbf{X}^3,p\mathbf{X} \rangle. \end{array}$

Proof: The same arguments as in Lemma 3.7 can be followed. And observe that: $A_{(1,0)} \cong A_{(\zeta,0)}$ if and only if $\overline{\zeta} \in GF(p^d)^3$, $A_{(1,0)} \cong A_{(\zeta^2,0)}$ if and only if $\overline{\zeta}^2 \in \mathrm{GF}(p^d)^3, \, \mathcal{A}_{(\zeta,0)} \cong \mathcal{A}_{(\zeta^2,0)} \text{ if and only if } \overline{\zeta} \in \mathrm{GF}(p^d)^3.$

4 Finite local Frobenius non-chain rings of length 5 and nilpotency index 4

In the following we focus on describing the family of finite local Frobenius non-chain rings of length 5 and nilpotency index 4. As a corollary the finite local Frobenius non-chain rings with 32 elements and nilpotency index 4 are given.

Let \mathfrak{F}_t be the family of finite local Frobenius non-chain rings with nilpotency index t, \mathfrak{L}_l be the family of finite local Frobenius non-chain rings of length l and $\mathfrak{F}_l^t = \mathfrak{F}_t \cap \mathfrak{L}_l$. Observe the following: a) local Frobenius rings with nilpotency index 2 are chain rings because $\operatorname{ann}_{A}(\mathfrak{m}) = \mathfrak{m}$ is a simple ideal and \mathfrak{m} is principal; (b) local rings with nilpotency index 1 are fields; (c) $\mathfrak{L}_{5} = \mathfrak{F}_{5}^{3} \cup \mathfrak{F}_{5}^{4}$ because the previous observations and the relation $t < \ell_{A}(A)$, where A is a local non chain ring and t is the nilpotency index of its maximal ideal.

The following results on local Frobenius rings will be used later on. Recall that if $(A, \mathfrak{m}, \operatorname{GF}(p^d))$ is a local Frobenius ring, I is an ideal of A and t is its nilpotency index, then the relations $(a) \ \ell_A(A) = \ell_A(I) + \ell_A(\operatorname{ann}(I)), (b) \operatorname{ann}_A(\operatorname{ann}_A(I)) = I$ and $(c) \operatorname{ann}_A(\mathfrak{m}) = \mathfrak{m}^{t-1}$ are satisfied.

Lemma 4.1. Let $(A, \mathfrak{m}, GF(q))$ be a finite local Frobenius non-chain ring, t the nilpontency index of \mathfrak{m} and I an ideal of A. Then

- (1) $\ell_{\rm A}(\mathfrak{m}^2) \le \ell_{\rm A}({\rm A}) 3.$
- (2) If $\ell_A(I) = \ell_A(A) 2$, then $\mathfrak{m}^2 \subset I \subset \mathfrak{m}$.
- (3) If $\ell_{A}(I) = 2$, then $\mathfrak{m}^{t-1} \subset I \subset \operatorname{ann}(\mathfrak{m}^{2})$.
- (4) If $\ell_A(I) = \ell_A(\operatorname{ann}_A(\mathfrak{m}^2))$ and $v_A(I) = \ell_A(I) 1$, then $I = \operatorname{ann}_A(\mathfrak{m}^2)$.
- (5) Let $i \in \{2, ..., t-1\}$, then $\mathfrak{m}^{i-1} \operatorname{ann}_{A}(\mathfrak{m}^{i}) = \operatorname{ann}_{A}(\mathfrak{m}) = \mathfrak{m}^{t-1}$.
- (6) $v_A(ann_A(\mathfrak{m}^2)) = v_A(\mathfrak{m}).$

Proof: (1) The assertion follows from the relation: $v_A(\mathfrak{m}) = \ell_A(\mathfrak{m}/\mathfrak{m}^2) = \ell_A(\mathfrak{m}) - \ell_A(\mathfrak{m}^2) = \ell_A(A) - 1 - \ell_A(\mathfrak{m}^2) \ge 2.$ (2) By Nakayama's Lemma $I + \mathfrak{m}^2 \subset \mathfrak{m}$, then: $\ell_A(A) - 2 = \ell_A(I) \leq \ell_A(I + \mathfrak{m}^2) < \ell_A(\mathfrak{m}) = \ell_A(A) - 1, \ \ell_A(I) = \ell_A(I + \mathfrak{m}^2) \text{ and } \ell_A(I) = \ell_A(I + \mathfrak{m}^2)$ $\mathfrak{m}^2 \subset I = I + \mathfrak{m}^2.$ (3) Since $\ell_A(\operatorname{ann}_A(I)) = \ell_A(A) - \ell_A(I) = \ell_A(A) - 2$, then: $\mathfrak{m}^2 \subset \operatorname{ann}_A(I) \subset \mathfrak{m}$, and $\mathfrak{m}^{t-1} = \operatorname{ann}_A(\mathfrak{m}) \subset I \subset \operatorname{ann}_A(\mathfrak{m}^2)$. (4) Since $v_A(I) = \ell_A(I) - 1 = \ell_A(I) - \ell_A(\mathfrak{m}I)$, then: $\ell_{A}(\mathfrak{m}I) = 1, \mathfrak{m}I = \mathfrak{m}^{t-1}, \mathfrak{m}^{2}I = \langle 0 \rangle \text{ and } I \subseteq \operatorname{ann}_{A}(\mathfrak{m}^{2}).$ The assertion follows from the relation $\ell_A(I) = \ell_A(\operatorname{ann}_A(\mathfrak{m}^2))$. (5) The relation \mathfrak{m}^{i-1} ann_A(\mathfrak{m}^i) = $\langle 0 \rangle$ implies $\mathfrak{m}^{i-1} \subseteq \operatorname{ann}_A(\operatorname{ann}_A(\mathfrak{m}^i)) = \mathfrak{m}^i$, which is not possible. Then $\mathfrak{m}^{i-1}ann_{\mathcal{A}}(\mathfrak{m}^{i}) \neq \langle 0 \rangle$, $\mathfrak{m}[\mathfrak{m}^{i-1}ann_{\mathcal{A}}(\mathfrak{m}^{i})] = \langle 0 \rangle$, $\mathfrak{m}^{i-1}\operatorname{ann}_{A}(\mathfrak{m}^{i}) \subseteq \operatorname{ann}_{A}(\mathfrak{m}) \text{ and } \mathfrak{m}^{i-1}\operatorname{ann}_{A}(\mathfrak{m}^{i}) = \operatorname{ann}_{A}(\mathfrak{m}) = \mathfrak{m}^{t-1}.$ (6) From (5), $\mathfrak{m}_{A}(\mathfrak{m}^2) = \mathfrak{m}^{t-1}$, then: $\mathbf{v}_{\mathbf{A}}(\operatorname{ann}_{\mathbf{A}}(\mathfrak{m}^2)) = \ell_{\mathbf{A}}(\operatorname{ann}_{\mathbf{A}}(\mathfrak{m}^2)/\mathfrak{m}^{t-1}) = \ell_{\mathbf{A}}(\operatorname{ann}_{\mathbf{A}}(\mathfrak{m}^2)) - 1 = \ell_{\mathbf{A}}(\mathbf{A}) - \ell_{\mathbf{A}}(\mathfrak{m}^2) - \ell_{\mathbf{A}}(\mathfrak{m}^2)$ $1 = \ell_{\mathrm{A}}(\mathfrak{m}) - \ell_{\mathrm{A}}(\mathfrak{m}^2) = \mathrm{v}_{\mathrm{A}}(\mathfrak{m}).$

Lemma 4.2. Let $(A, \mathfrak{m}, GF(q))$ be a finite local Frobenius ring, $t \ge 4$ the nilpotency index of $\mathfrak{m}, \mathbb{T} \subset A$ a set of representatives of $GF(q), \{\alpha_1, \ldots, \alpha_l\}$ a minimal A-generating set for \mathfrak{m} , I an ideal of A and $B = A/\mathfrak{m}^{t-1}$. We have the following:

(1) B is a local ring

- (a) The maximal ideal of B is $\mathfrak{m}/\mathfrak{m}^{t-1}$,
- (b) The residue field of B is isomorphic to GF(q).
- (c) $\mathbb{T}_1 = \{\beta + \mathfrak{m}^{t-1} : \beta \in \mathbb{T}\} \subset \mathcal{B} \text{ is a set of representatives for } GF(q),$
- (d) If $I \neq 0$, then $\ell_B(I/\mathfrak{m}^{t-1}) = \ell_A(I) 1$, in particular $\ell_B(B) = \ell_A(A) 1$.
- (e) $\{\alpha_1 + \mathfrak{m}^{t-1}, \ldots, \alpha_l + \mathfrak{m}^{t-1}\}$ is a B-generating set for $\mathfrak{m}/\mathfrak{m}^{t-1}$.
- (2) $\ell_{\mathrm{B}}(\mathrm{ann}_{\mathrm{B}}(\mathfrak{m}/\mathfrak{m}^{t-1})) < \ell_{\mathrm{A}}(\mathrm{A}) 2.$
- (3) If A is not a chain ring, then B is not a Frobenius ring.

Proof: (1a) follows from the Correspondence Theorem.

- (1b) follows from the relation $[A/\mathfrak{m}^{t-1}]/[\mathfrak{m}/\mathfrak{m}^{t-1}] \cong A/\mathfrak{m}$.
- (1c) and (1d) are easy.
- (1e) the assertion follows from the relation

$$v_{\mathrm{B}}(\mathfrak{m}/\mathfrak{m}^{t-1}) = \ell_{\mathrm{B}}([\mathfrak{m}/\mathfrak{m}^{t-1}]/[\mathfrak{m}^2/\mathfrak{m}^{t-1}]) = \ell_{\mathrm{A}}(\mathfrak{m}/\mathfrak{m}^2) = v_{\mathrm{A}}(\mathfrak{m}).$$

(2) We have $\operatorname{ann}_{B}(\mathfrak{m}/\mathfrak{m}^{t-1}) = (\mathfrak{m}^{t-1}:\mathfrak{m})/\mathfrak{m}^{t-1}$, where $(\mathfrak{m}^{t-1}:\mathfrak{m}) = \{\alpha \in A : \alpha\mathfrak{m} \subseteq \mathfrak{m}^{t-1}\}$. The relation $(\mathfrak{m}^{t-1}:\mathfrak{m}) = \mathfrak{m}$ implies $\mathfrak{m}^{2} \subseteq \mathfrak{m}^{t-1}$, which is not possible, by Nakayama's Lemma, then $(\mathfrak{m}^{t-1}:\mathfrak{m}) \subset \mathfrak{m}$ and

$$\ell_{\mathrm{B}}(\mathrm{ann}_{\mathrm{B}}(\mathfrak{m}/\mathfrak{m}^{t-1})) < \ell_{\mathrm{A}}(\mathfrak{m}) - 1 = \ell_{\mathrm{A}}(\mathrm{A}) - 2.$$

(3) By (5) and (6) of Lemma 4.1, $\operatorname{mann}_{A}(\mathfrak{m}^{2}) = \mathfrak{m}^{t-1}$ and $l = v_{A}(\operatorname{ann}_{A}(\mathfrak{m}^{2})) = v_{A}(\mathfrak{m}) \geq 2$. By Lemma 2.1, the ideals between $\operatorname{ann}_{A}(\mathfrak{m}^{2})$ and $\operatorname{mann}_{A}(\mathfrak{m}^{2}) = \mathfrak{m}^{t-1}$ of length $1 + \ell_{A}(\mathfrak{m}^{t-1}) = 2$ are in one to one correspondence with the, $\frac{q^{l}-1}{q-1}$, $(1 \times l)$ matrices over GF(q) in (rre)-form. Since ideals of A of length 2 are in one to one correspondence with minimal ideals of B, then B has $\frac{q^{l}-1}{q-1}$ minimal ideals and is not a Frobenius ring.

Lemma 4.3. Let $(A, \mathfrak{m}, GF(q)) \in \mathfrak{F}_5^4$. Then:

- (1) $v_A(ann_A(\mathfrak{m}^2)) = v_A(\mathfrak{m}) = 2,$
- (2) $v_A(\mathfrak{m}^2) = 1$,
- (3) $\ell_{\rm A}(\mathfrak{m}^2) = 2$,
- (4) $\ell_{\mathrm{A}}(\mathrm{ann}_{\mathrm{A}}(\mathfrak{m}^2)) = 3,$

Proof: The first equality in (1) follows from Lemma 4.1(6). (4) follows from (3) and the relation $\ell_A(I) + \ell_A(\operatorname{ann}(I)) = \ell_A(A)$. Since $5 = \ell_A(A) = \ell_A(A/\mathfrak{m}) + \ell_A(\mathfrak{m}/\mathfrak{m}^2) + \ell_A(\mathfrak{m}^2/\mathfrak{m}^3) + \ell_A(\mathfrak{m}^3) = 2 + v_A(\mathfrak{m}) + v_A(\mathfrak{m}^2)$ and $v_A(\mathfrak{m}) \ge 2$, then $v_A(\mathfrak{m}) = 2$, $v_A(\mathfrak{m}^2) = 1$ and $\ell_A(\mathfrak{m}^2) = 2$.

The following result is central in proving the main result of this section. Observe that if $(A, \mathfrak{m}, GF(q))$ is a finite local ring, $\mathbb{T} \subset A$ a set of representatives of GF(q) and $x, y \in \mathfrak{m}$ with $\operatorname{ann}_B(x) = \operatorname{ann}_B(y)$. Then $x^2 = 0$ if and only if $x \in \operatorname{ann}_B(x) = \operatorname{ann}_B(y)$ if and only if xy = 0 if and only if $y \in \operatorname{ann}_B(x) = \operatorname{ann}_B(y)$ if and only if $y^2 = 0$. And if $\langle x \rangle = \langle y \rangle$ is a minimal ideal of A. By Nakayama's Lemma $\mathfrak{m}y = \langle 0 \rangle$ and there are $a \in \mathbb{T} \setminus \{0\}$ and $m \in \mathfrak{m}$ such that x = (a + m)y = ay.

Lemma 4.4. Let $(A, \mathfrak{m}, GF(q)) \in \mathfrak{F}_5^4$, $\mathbb{T} \subset A$ a set of representatives of GF(q)and $x \in \mathfrak{m} \setminus \mathfrak{m}^2$. Then $y \in \mathfrak{m} \setminus \mathfrak{m}^2$ exists such that $\{x, y\}$ is a minimal Agenerating set of \mathfrak{m} , $x^4 = x^3y = x^2y^2 = xy^3 = y^4 = 0$ and one of the following three relations is satisfied:

- (a) $x^3 = 0$, $y^3 \neq 0$, $x^2 = uy^3$, $xy = vy^3$, where $u, v \in \mathbb{T}$, $u \neq 0$, and $\mathfrak{m}^2 = \langle y^2 \rangle$.
- (b) $y^3 = 0$, $x^3 \neq 0$, $y^2 = ux^3$, $xy = vx^3$, where $u, v \in \mathbb{T}$, $u \neq 0$, and $\mathfrak{m}^2 = \langle x^2 \rangle$.
- (c) $xy = \rho x^2 + \sigma x^3$ and $y^2 = \rho xy + \eta x^3$, where $\eta, \sigma, \rho \in \mathbb{T}$ are such that $\rho \neq 0$ and $\bar{\rho}\bar{\sigma} \neq \bar{\eta}$ in GF(q), $\mathfrak{m}^2 = \langle x^2 \rangle = \langle xy \rangle = \langle y^2 \rangle$ and $\mathfrak{m}^3 = \langle x^3 \rangle$.

Proof: Since $v_A(\mathfrak{m}) = 2$ and \mathfrak{m} has nilpotency index 4, then $y \notin \mathfrak{m} \setminus \mathfrak{m}^2$ exists such that $\{x, y\}$ is a minimal A-generating set for \mathfrak{m} and $x^4 = x^3y = x^2y^2 = xy^3 = y^4 = 0$.

Let $B = A/\mathfrak{m}^3$, x_1 and y_1 be the elements in the ring B corresponding to x and y modulo \mathfrak{m}^3 . By Lemma 4.2, B is local ring with maximal ideal $\mathfrak{m}_1 = \mathfrak{m}/\mathfrak{m}^3$, residue field GF(q), $\ell_B(B) = 4$, $\{x_1, y_1\}$ is a minimal B-generating set for \mathfrak{m}_1 , $\mathbb{T}_1 = \{\beta + \mathfrak{m}^3 \in B : \beta \in \mathbb{T}\}$ is a set of representatives for GF(q), $1 < \ell_B(\operatorname{ann}_B(\mathfrak{m}_1)) < 3$ and $\ell_B(\operatorname{ann}_B(\mathfrak{m}_1)) = 2$. By Lemma 4.3(2), $\ell_B(\mathfrak{m}_1^2) = \ell_B((\mathfrak{m}/\mathfrak{m}^3)^2) = \ell_B(\mathfrak{m}^2/\mathfrak{m}^3) = \ell_A(\mathfrak{m}^2/\mathfrak{m}^3) = v_A(\mathfrak{m}^2) = 1$, hence \mathfrak{m}_1^2 is a simple ideal of B and is generated by any of its nonzero elements.

On the other hand, since $\operatorname{ann}_{B}(\mathfrak{m}_{1}) = \operatorname{ann}_{B}(x_{1}) \cap \operatorname{ann}_{B}(y_{1})$, $\ell_{B}(\operatorname{ann}_{B}(\mathfrak{m}_{1})) = 2$, $\ell_{B}(\mathfrak{m}_{1}) = 3$, then $\ell_{B}(\operatorname{ann}_{B}(x_{1})) \in \{2,3\}$, $\ell_{B}(\operatorname{ann}_{B}(y_{1})) \in \{2,3\}$, $\operatorname{ann}_{B}(x_{1}) \in \{\mathfrak{m}_{1}, \operatorname{ann}_{B}(\mathfrak{m}_{1})\}$ and $\operatorname{ann}_{B}(y_{1}) \in \{\mathfrak{m}_{1}, \operatorname{ann}_{B}(\mathfrak{m}_{1})\}$. Thus the only possibilities are the following:

(a) $\operatorname{ann}_{B}(x_{1}) = \mathfrak{m}_{1}$ and $\operatorname{ann}_{B}(y_{1}) = \operatorname{ann}_{B}(\mathfrak{m}_{1}),$

(b) $\operatorname{ann}_{\mathrm{B}}(\mathbf{x}_1) = \operatorname{ann}_{\mathrm{B}}(\mathfrak{m}_1)$ and $\operatorname{ann}_{\mathrm{B}}(\mathbf{y}_1) = \mathfrak{m}_1$.

(c) $\operatorname{ann}_{B}(\mathbf{x}_{1}) = \operatorname{ann}_{B}(\mathfrak{m}_{1})$ and $\operatorname{ann}_{B}(\mathbf{y}_{1}) = \operatorname{ann}_{B}(\mathfrak{m}_{1}),$

(d) $\operatorname{ann}_{B}(x_{1}) = \mathfrak{m}_{1}$ and $\operatorname{ann}_{B}(y_{1}) = \mathfrak{m}_{1}$.

Each one of these cases will be treated. Observe that the case (b) is similar to (a). Case (d) is impossible because $\operatorname{ann}_{B}(\mathfrak{m}_{1}) = \operatorname{ann}_{B}(x_{1}) \cap \operatorname{ann}_{B}(y_{1}) = \mathfrak{m}_{1}$ is impossible.

CASE (a) $\operatorname{ann}_{B}(x_{1}) = \mathfrak{m}_{1}$ and $\operatorname{ann}_{B}(y_{1}) = \operatorname{ann}_{B}(\mathfrak{m}_{1})$.

We have $x_1^2 = x_1y_1 = 0$, hence $y_1^2 \neq 0$, $x^2 \in \mathfrak{m}^3$, $xy \in \mathfrak{m}^3$ and $y^2 \notin \mathfrak{m}^3$. Since the nilpotency index is 4 and $v_A(\mathfrak{m}^2) = 1$, $x^3 = x^2y = xy^2 = 0$, $y^3 \neq 0$, $\mathfrak{m}^2 = \langle y^2 \rangle$, $\mathfrak{m}^3 = \langle y^3 \rangle$. Observe the relations $x^2 = xy = 0$ imply $x \in \operatorname{ann}_A(\mathfrak{m}) = \mathfrak{m}^3$ which are not possible. If $x^2 = 0$, then $xy \neq 0$, $\mathfrak{m}^3 = \langle y^3 \rangle = \langle xy \rangle$, $y^3 = \tau xy$, where $\tau \in \mathbb{T} \setminus \{0\}$, $y^2 - \tau x \in \operatorname{ann}_A(\mathfrak{m}) = \mathfrak{m}^3$ and $x \in \mathfrak{m}^2$, a contradiction, hence $x^2 \neq 0$, $\mathfrak{m}^3 = \langle y^3 \rangle = \langle x^2 \rangle$, $x^2 = uy^3$, $xy = vy^3$, where $u, v \in \mathbb{T}$ and $u \neq 0$.

CASE (c) $\operatorname{ann}_{B}(x_{1}) = \operatorname{ann}_{B}(\mathfrak{m}_{1})$ and $\operatorname{ann}_{B}(y_{1}) = \operatorname{ann}_{B}(\mathfrak{m}_{1})$.

We have $x_1^2 \neq 0$, $x_1y_1 \neq 0$, $y_1^2 \neq 0$, then $\mathfrak{m}_1^2 = \langle x_1^2 \rangle = \langle y_1^2 \rangle = \langle x_1y_1 \rangle$, $x_1y_1 = \rho x_1^2$, where $\rho \in \mathbb{T}_1 \setminus \{0\}$, $x_1(y_1 - \rho x_1) = 0$, $y_1 - \rho x_1 \in \operatorname{ann}_B(x_1) = \operatorname{ann}_B(y_1)$ and $y_1^2 - \rho x_1y_1 = 0$. These relations are equivalent to $xy - \rho x^2 \in \mathfrak{m}^3$, $y^2 - \rho xy \in \mathfrak{m}^3$, $x^2 \notin \mathfrak{m}^3$, $y^2 \notin \mathfrak{m}^3$ and $xy \notin \mathfrak{m}^3$, where $\rho \in \mathbb{T} \setminus \{0\}$. Hence $\mathfrak{m}^2 = \langle x^2 \rangle = \langle xy \rangle = \langle y^2 \rangle$, by Lemma 4.3(2). Since the nilpotency index of \mathfrak{m} is 4, $x^2y = \rho x^3$, $xy^2 = \rho x^2y = \rho^2 x^3$, $y^3 = \rho xy^2 = \rho^3 x^3$, $\mathfrak{m}^3 = \langle x^3 \rangle$, $xy = \rho x^2 + \sigma x^3$ and $y^2 = \rho xy + \eta x^3$, where $\sigma, \eta \in \mathbb{T}$.

Finally, if $\bar{\rho}\bar{\sigma} = \bar{\eta}$ in GF(q), then $\eta x^3 = \rho \sigma x^3 = \sigma x^2 y$, $x(y - \rho x - \sigma x^2) = 0$ and $y(y - \rho x - \sigma x^2) = y^2 - \rho xy - \sigma x^2 y = y^2 - \rho xy - \eta x^3 = 0$, consequently $y - \rho x - \sigma x^2 \in \operatorname{ann}_A(\mathfrak{m}) = \mathfrak{m}^3 \subset \mathfrak{m}^2$, a contradiction.

Corollary 4.5. Let $(A, \mathfrak{m}, GF(p^d)) \in \mathfrak{L}_5^4$.

- (1) If $p \in \mathfrak{m}^2$, then char(A) $\in \{p, p^2\}$.
- (2) If p ∉ m², there is x ∈ m \ m² such that {p, x} is a minimal A-generating set for m and:
 - (i) If $\{p, x\}$ satisfies the relation of Lemma 4.4(1), then char(A) = p^3 .
 - (ii) If $\{p, x\}$ satisfies the relation of Lemma 4.4(2), then char(A) = p^4 .
 - (iii) If $\{p, x\}$ satisfies the relation of Lemma 4.4(3), then char(A) = p^4 .

Proof: (1) If $p \in \mathfrak{m}^2$, then $p^2 \in \mathfrak{m}^4 = \langle 0 \rangle$ and the assertion follows. (2) By Lemma 4.4, we have the following three cases:

- (i) $p^3 = 0$, $x^3 \neq 0$, $p^2 = ux^3$, $px = vx^3$, where $u, v \in \mathbb{T}$, $u \neq 0$. Then $p^2 \neq 0$ and char(A) = p^3 .
- (ii) $\mathbf{x}^3 = 0$, $p^3 \neq 0$, $\mathbf{x}^2 = up^3$, $p\mathbf{x} = vp^3$, where $u, v \in \mathbb{T}$, $u \neq 0$. Then $char(\mathbf{A}) = p^4$.

(iii) $p\mathbf{x} = \rho p^2 + \sigma p^3$, $\mathbf{x}^2 = \rho p\mathbf{x} + \eta p^3$, $\mathfrak{m}^3 = \langle p^3 \rangle \neq \langle 0 \rangle$, where $\eta, \sigma, \rho \in \mathbb{T}$ are such that $\rho \neq 0$ and $\bar{\rho}\bar{\sigma} \neq \bar{\eta}$ in GF(q). Then char(A) = p^4 .

The cases in Corollary 4.5 will be treated in the following propositions.

Proposition 4.6. Let $(A, \mathfrak{m}, GF(p^d)) \in \mathcal{L}_5^4$ be such that $char(A) = p^2$ and $p \in \mathfrak{m}^2$. Then:

- (i) When $\langle p \rangle = \mathfrak{m}^2$.
 - (1) If p = 2 the ring A is isomorphic to $GR(2^2, d)[X, Y]/\langle Y^2 2, X^2 Y^3, XY \rangle$.
 - (2) If p is odd the ring A is isomorphic to $GR(p^2, d)[X, Y]/\langle Y^2 - p, X^2 - Y^3, XY \rangle \text{ or}$ $GR(p^2, d)[X, Y]/\langle \zeta Y^2 - p, X^2 - Y^3, XY \rangle \text{ or}$ $GR(p^2, d)[X, Y]/\langle Y^2 - p, X^2 - \zeta Y^3, XY \rangle \text{ or}$ $GR(p^2, d)[X, Y]/\langle \zeta Y^2 - p, X^2 - \zeta Y^3, XY \rangle.$

(*ii*) When $\langle p \rangle = \mathfrak{m}^3$.

- (1) If p = 2 and $3|2^d 1$ the ring A is isomorphic to $GR(2^2, d)[X, Y]/\langle Y^3 - 2, X^2 - Y^3, XY \rangle$ or $GR(2^2, d)[X, Y]/\langle \zeta Y^3 - 2, X^2 - Y^3, XY \rangle$ or $GR(2^2, d)[X, Y]/\langle \zeta^2 Y^3 - 2, X^2 - Y^3, XY \rangle$.
- (2) If p = 2 and $3 \not| 2^d 1$ the ring A is isomorphic to $GR(2^2, d)[X, Y]/\langle Y^3 2, X^2 Y^3, XY \rangle.$
- (3) If p is odd and $3|p^d 1$ the ring A is isomorphic to $GR(p^2, d)[X, Y]/\langle Y^3 - p, X^2 - Y^3, XY \rangle$ or $GR(p^2, d)[X, Y]/\langle \zeta Y^3 - p, X^2 - Y^3, XY \rangle$ or $GR(p^2, d)[X, Y]/\langle \zeta^2 Y^3 - p, X^2 - Y^3, XY \rangle$ or $GR(p^2, d)[X, Y]/\langle Y^3 - p, X^2 - \zeta Y^3, XY \rangle$ or $GR(p^2, d)[X, Y]/\langle \zeta^2 Y^3 - p, X^2 - \zeta Y^3, XY \rangle$ or $GR(p^2, d)[X, Y]/\langle \zeta^2 Y^3 - p, X^2 - \zeta Y^3, XY \rangle$.
- (4) If p is odd and $3 \not| p^d 1$ the ring A is isomorphic to $\operatorname{GR}(p^2, d)[X, Y]/\langle Y^3 p, X^2 Y^3, XY \rangle$ or $\operatorname{GR}(p^2, d)[X, Y]/\langle Y^3 p, X^2 \zeta Y^3, XY \rangle$.

 $\mathbb{T} = \{0, 1, \dots, \zeta^{p^d-2}\}$ is the Teichmüller set of the Galois ring $\operatorname{GR}(p^2, d)$.

In these cases $\mathfrak{m} = \langle x, y \rangle$, $\mathfrak{m}^2 = \langle y^2 \rangle$ and $\operatorname{ann}_A(\mathfrak{m}^2) = \langle x, y^2 \rangle$.

Proof: By Theorem 3.1 we may assume that the Galois ring $\operatorname{GR}(p^2, d) \subset A$ and let $\mathbb{T} = \{0, 1, \ldots, \zeta^{p^d-2}\}$ the Teichmüller set of this Galois ring. Let $\{\mathbf{x}, \mathbf{y}\}$ be a minimal A-generating set for the maximal ideal \mathfrak{m} satisfying statements (i), (ii) or (iii) of Lemma 4.4. Cases (i) and (ii) are similar. By (i) and (iii) of Lemma 4.4, $\mathfrak{m}^2 = \langle \mathbf{y}^2 \rangle$ and $\mathfrak{m}^3 = \langle \mathbf{y}^3 \rangle$, then $p \in \langle \mathbf{y}^2 \rangle$ implies $p = \omega_1 \mathbf{y}^2 + \omega_2 \mathbf{y}^3$, where $\omega_1, \omega_2 \in \mathbb{T}$ not both zero. Observe that $\omega_1 \neq 0$ if and only if $\langle p \rangle = \mathfrak{m}^2$ and $\omega_1 = 0$ if and only if $\langle p \rangle = \mathfrak{m}^3$. Again by Theorem 3.1, in case (i) there is an epimorphism from $A_{(u,r,s)} := \operatorname{GR}(p^2, d)[X, Y]/\langle rY^2 + sY^3 - p, X^2 - uY^3, XY, X^4, X^3Y, X^2Y^2, XY^3, Y^4 \rangle$ onto A, and in the case (iii) from $B_{(\eta,\sigma,\rho,f,g)} := \operatorname{GR}(p^2, d)[X, Y]/\langle fY^2 + gY^3 - p, XY - \rho X^2 - \sigma X^3, Y^2 - \rho XY - \eta X^3, X^4, X^3Y, X^2Y^2, XY^3, Y^4 \rangle$ onto A, where $r, s, f, g, u, \eta, \sigma, \rho \in \mathbb{T}$ with $u\rho \neq 0$ and $\rho\sigma \neq \eta$, r and s not both zero and f and g not both zero. By the proof of Lemma 3.7, $|A_{(u,r,s)}| = |B_{(\eta,\sigma,\rho,f,g)}| = p^{5s} = |A|$ then the epimorphism mentioned above is an isomorphism and from the same Lemma the assertion follows.

Proposition 4.7. Let $(A, \mathfrak{m}, GF(p^d)) \in \mathcal{L}_5^4$ be such that char(A) = p. Then A is isomorphic to

$$GF(p^d)[X,Y]/\langle X^2 - Y^3, XY \rangle$$

In this case $\mathfrak{m} = \langle x, y \rangle$, $\mathfrak{m}^2 = \langle y^2 \rangle$ and $\operatorname{ann}_A(\mathfrak{m}^2) = \langle x, y^2 \rangle$.

Proof: Use the same arguments as in Proposition 4.6 and Lemma 3.8.

Proposition 4.8. Let $(A, \mathfrak{m}, GF(p^d)) \in \mathcal{L}_5^4$ be such that $char(A) = p^4$ and $p \notin \mathfrak{m}^2$. Then:

- (1) If p = 2 the ring A is isomorphic to $GR(2^4, d)[X]/\langle X^2 2^3, 2X \rangle$.
- (2) If p is odd the ring A is isomorphic to $GR(p^{4},d)[X]/\langle X^{2} - p^{3}, pX \rangle \text{ or }$ $GR(p^{4},d)[X]/\langle X^{2} - \zeta p^{3}, pX \rangle,$ $\{0,1,\ldots,\zeta^{p^{d}-2}\} \text{ is the Teichmüller set of the Galois ring } GR(p^{4},d).$

In these cases $\mathfrak{m} = \langle p, \mathbf{x} \rangle$, $\mathfrak{m}^2 = \langle p^2 \rangle$ and $\operatorname{ann}_A(\mathfrak{m}^2) = \langle p^2, \mathbf{x} \rangle$.

Proof: Use the same arguments as in Proposition 4.6 and Lemma 3.9.

Proposition 4.9. Let $(A, \mathfrak{m}, GF(p^d)) \in \mathcal{L}_5^4$ be such that $char(A) = p^3$ and $p \notin \mathfrak{m}^2$. Then:

(1) If $3 \not| p^d - 1$ the ring A is isomorphic to $\operatorname{GR}(p^3, d)[X]/\langle p^2 - X^3, pX \rangle.$

(2) If $3|p^d - 1$ the ring A is isomorphic to $GR(p^3, d)[X]/\langle p^2 - X^3, pX \rangle$ or $GR(p^3, d)[X]/\langle p^2 - \zeta X^3, pX \rangle$ or $GR(p^3, d)[X]/\langle p^2 - \zeta^2 X^3, pX \rangle$, $\{0, 1, \dots, \zeta^{p^d-2}\}$ is the Teichmüller set of the Galois ring $GR(p^3, d)$.

In these cases $\mathfrak{m} = \langle p, \mathbf{x} \rangle$, $\mathfrak{m}^2 = \langle \mathbf{x}^2 \rangle$ and $\operatorname{ann}_A(\mathfrak{m}^2) = \langle p, \mathbf{x}^2 \rangle$.

Proof: Use the same arguments as in Proposition 4.6 and Lemma 3.10.

In the following theorem we summarize the previously proven claims as the main result of this section.

Theorem 4.10. Let $(A, \mathfrak{m}, GF(p^d))$ be a finite local Frobenius non-chain ring of length 5 and nilpotency index 4. Then A is isomorphic to one of the following rings:

- (a) If p = 2: $GR(2^2, d)[X, Y]/\langle Y^2 - 2, X^2 - Y^3, XY \rangle$. If p is odd: $GR(p^2, d)[X, Y]/\langle Y^2 - p, X^2 - Y^3, XY \rangle$ or $GR(p^2, d)[X, Y]/\langle Y^2 - p, X^2 - \zeta Y^3, XY \rangle$ or $GR(p^2, d)[X, Y]/\langle Y^2 - p, X^2 - \zeta Y^3, XY \rangle$. In this case: $char(A) = p^2, \mathfrak{m} = \langle x, y \rangle, \mathfrak{m}^2 = \langle y^2 \rangle = \langle p \rangle$ and $ann_A(\mathfrak{m}^2) = \langle x, y^2 \rangle$. (b) If p = 2 and $3|2^d - 1$ $GR(2^2, d)[X, Y]/\langle Y^3 - 2, X^2 - Y^3, XY \rangle$ or $GR(2^2, d)[X, Y]/\langle \zeta^2 Y^3 - 2, X^2 - Y^3, XY \rangle$ or $GR(2^2, d)[X, Y]/\langle \zeta^2 Y^3 - 2, X^2 - Y^3, XY \rangle$. If p = 2 and $3/2^d - 1$ $GR(2^2, d)[X, Y]/\langle \zeta^2 Y^3 - 2, X^2 - Y^3, XY \rangle$. If p = 2 and $3/2^d - 1$ $GR(2^2, d)[X, Y]/\langle Y^3 - 2, X^2 - Y^3, XY \rangle$. If p is odd and $3|p^d - 1$
 - $\begin{array}{l} \text{GR}(p^2,d)[\text{X},\text{Y}]/\langle \text{Y}^3 p, \text{X}^2 \text{Y}^3, \text{XY} \rangle \ or \\ \text{GR}(p^2,d)[\text{X},\text{Y}]/\langle \zeta \text{Y}^3 p, \text{X}^2 \text{Y}^3, \text{XY} \rangle \ or \\ \text{GR}(p^2,d)[\text{X},\text{Y}]/\langle \zeta^2 \text{Y}^3 p, \text{X}^2 \text{Y}^3, \text{XY} \rangle \ or \\ \text{GR}(p^2,d)[\text{X},\text{Y}]/\langle \zeta^2 \text{Y}^3 p, \text{X}^2 \zeta \text{Y}^3, \text{XY} \rangle \ or \\ \text{GR}(p^2,d)[\text{X},\text{Y}]/\langle \zeta \text{Y}^3 p, \text{X}^2 \zeta \text{Y}^3, \text{XY} \rangle \ or \\ \text{GR}(p^2,d)[\text{X},\text{Y}]/\langle \zeta^2 \text{Y}^3 p, \text{X}^2 \zeta \text{Y}^3, \text{XY} \rangle \ or \\ \text{GR}(p^2,d)[\text{X},\text{Y}]/\langle \zeta^2 \text{Y}^3 p, \text{X}^2 \zeta \text{Y}^3, \text{XY} \rangle. \\ \text{If } p \ is \ odd \ and \ 3 \ / p^d 1 \\ \text{GR}(p^2,d)[\text{X},\text{Y}]/\langle \text{Y}^3 p, \text{X}^2 \text{Y}^3, \text{XY} \rangle \ or \\ \text{GR}(p^2,d)[\text{X},\text{Y}]/\langle \text{Y}^3 p, \text{X}^2 \text{Y}^3, \text{XY} \rangle. \end{array}$

In this case: $\operatorname{char}(A) = p^2, \mathfrak{m} = \langle x, y \rangle, \mathfrak{m}^2 = \langle y^2 \rangle, \mathfrak{m}^3 = \langle p \rangle \text{ and } \operatorname{ann}_A(\mathfrak{m}^2) = \langle x, y^2 \rangle.$

- $\begin{array}{ll} (c) & \mathrm{GF}(p^d)[\mathrm{X},\mathrm{Y}]/\langle\mathrm{X}^2-\mathrm{Y}^3,\mathrm{XY}\rangle.\\ & In \ this \ case:\\ & \mathrm{char}(\mathrm{A})=p, \mathfrak{m}=\langle\mathrm{x},\mathrm{y}\rangle, \mathfrak{m}^2=\langle\mathrm{y}^2\rangle \ and \ \mathrm{ann}_\mathrm{A}(\mathfrak{m}^2)=\langle\mathrm{x},\mathrm{y}^2\rangle. \end{array}$
- (d) If p = 2 $\operatorname{GR}(2^4, d)[X]/\langle X^2 - 2^3, 2X \rangle$. If p is odd $\operatorname{GR}(p^4, d)[X]/\langle X^2 - p^3, pX \rangle$ or $\operatorname{GR}(p^4, d)[X]/\langle X^2 - \zeta p^3, pX \rangle$, $\{0, 1, \dots, \zeta^{p^d-2}\}$ is the Teichmüller set of the Galois ring $\operatorname{GR}(p^4, d)$. In this case: $\operatorname{char}(A) = p^4, p \notin \mathfrak{m}^2, \mathfrak{m} = \langle p, \mathbf{x} \rangle, \mathfrak{m}^2 = \langle p^2 \rangle$ and $\operatorname{ann}_A(\mathfrak{m}^2) = \langle p^2, \mathbf{x} \rangle$.
- $\begin{array}{ll} (e) & If \ 3 \ /\!\!/ p^d 1 \\ & \operatorname{GR}(p^3,d)[\mathrm{X}]/\langle p^2 \mathrm{X}^3,p\mathrm{X}\rangle. \\ & If \ 3|p^d 1 \\ & \operatorname{GR}(p^3,d)[\mathrm{X}]/\langle p^2 \mathrm{X}^3,p\mathrm{X}\rangle \ or \\ & \operatorname{GR}(p^3,d)[\mathrm{X}]/\langle p^2 \zeta \mathrm{X}^3,p\mathrm{X}\rangle \ or \\ & \operatorname{GR}(p^3,d)[\mathrm{X}]/\langle p^2 \zeta^2 \mathrm{X}^3,p\mathrm{X}\rangle, \\ & \{0,1,\ldots,\zeta^{p^d-2}\} \ is \ the \ Teichm{\ddot{u}}ller \ set \ of \ the \ Galois \ ring \ \operatorname{GR}(p^3,d). \\ & In \ this \ case: \\ & \operatorname{char}(\mathrm{A}) = p^3, p \not\in \mathfrak{m}^2, \mathfrak{m} = \langle p, \mathrm{x}\rangle, \mathfrak{m}^2 = \langle \mathrm{x}^2 \rangle \ and \ \operatorname{ann}_{\mathrm{A}}(\mathfrak{m}^2) = \langle p, \mathrm{x}^2 \rangle. \end{array}$

Let $(A, \mathfrak{m}, GF(2^d)) \in \mathcal{L}_5^4$ be such that A has 2^5 elements. Since $|A| = 2^5 = (2^{5d})$ and $3 \not| 2^5 - 1$, then d = 1 and we have the following;

Corollary 4.11. Let $(A, \mathfrak{m}, GF(p^d))$ be a finite local Frobenius non-chain ring with nilpotency index 4 and $2^5 = 32$ elements. Then A is isomorphic to one of the following rings:

- (a) $\mathbb{Z}_{2^2}[X,Y]/\langle Y^2-2,X^2-Y^3,XY\rangle$. In this case, char(A) = 2^2 , $2 \in \mathfrak{m}^2$, $\langle 2 \rangle = \mathfrak{m}^2$.
- $\begin{array}{ll} (b) \ \mathbb{Z}_{2^2}[\mathrm{X},\mathrm{Y}]/\langle\mathrm{Y}^3-2,\mathrm{X}^2-\mathrm{Y}^3,\mathrm{X}\mathrm{Y}\rangle\\ In \ this \ case, \ \mathrm{char}(\mathrm{A})=2^2, \ 2\in\mathfrak{m}^2, \ \langle 2\rangle=\mathfrak{m}^3. \end{array}$
- $\begin{array}{ll} (c) \ \ {\rm GF}(2)[{\rm X},{\rm Y}]/\langle {\rm X}^2-{\rm Y}^3,{\rm XY}\rangle \\ In \ this \ case, \ {\rm char}({\rm A})=2. \end{array}$
- (d) $\mathbb{Z}_{2^4}[X]/\langle X^2 2^3, 2X \rangle$. In this case, char(A) = 2^4 , $2 \notin \mathfrak{m}^2$.

(e) $\mathbb{Z}_{2^3}[X]/\langle 2^2 - X^3, 2X \rangle$. In this case, char(A) = 2^3 , $2 \notin \mathfrak{m}^2$.

5 Constacyclic codes over finite local rings in \mathfrak{F}_5^4

Let $(A, \mathfrak{m}, \operatorname{GF}(q))$ be a finite local ring and γ a unit of A. Assume that the integer n > 1 is not divisible by p, so that by Hensel's Lemma, $\operatorname{T}^n - \gamma$ is the product of basic irreducible pairwise coprime polynomials in A[T]. Recall that a linear code of length n over A is γ -constacyclic if it is invariant under the permutation $(a_0, a_1, \ldots, a_{n-1}) \mapsto (\gamma a_{n-1}, a_0, \ldots, a_{n-2})$. As usual, γ -constacyclic codes of length n over A can be identified as ideals in the quotient ring A[T]/ $\langle \operatorname{T}^n - \gamma \rangle$ via the isomorphism from Aⁿ to A[T]/ $\langle \operatorname{T}^n - \gamma \rangle$ defined by $(a_0, \ldots, a_{n-1}) \mapsto a_0 + a_1 \mathrm{T} + \ldots + a_{n-1} \mathrm{T}^{n-1}$, (the polynomial representation of Aⁿ).

Recall that \mathfrak{F}_4^5 is the family of finite local Frobenius non-chain rings of length 5 and nilpotency index 4. In this Section the structure and the number of constacyclic codes over rings in \mathfrak{F}_4^5 of length relatively prime to the characteristic of the residue field of the ring are determined.

The following result is on the structure of γ -constacyclic codes given in [2].

Lemma 5.1. Let $(A, \mathfrak{m}, GF(q))$ be a finite local ring, $l = \ell_A(A)$, γ a unit of Aand n an integer relatively prime to q. Let $T^n - \gamma = f_1 \cdots f_r$ be a representation of $T^n - \gamma$ as a product of basic irreducible pairwise coprime polynomials in $A[T], A_i = A[T]/\langle f_i \rangle$ and $s_i = \deg(\overline{f_i})$. Then

- (1) $A[T]/\langle T^n \gamma \rangle \cong \bigoplus_{i=1}^r A_i.$
- (2) Any ideal I of $A[T]/\langle T^n \gamma \rangle$ is a direct sum of ideals of A_i and there is a partition of $[1, \ldots, r]$, U_0, U_1, \ldots, U_l , such that:

$$I = \bigoplus_{u \in U_1} I_u \oplus \bigoplus_{u \in U_2} I_u \oplus \ldots \oplus \bigoplus_{u \in U_{l-2}} I_u \oplus \bigoplus_{u \in U_{l-1}} I_u \oplus \bigoplus_{u \in U_l} I_u$$

where $U_i = \{u : \ell_{A_u}(I_u) = i\}.$

(3) Let I and U_0, U_1, \ldots, U_l be as above, then:

$$|\mathbf{I}| = q^{\sum_{u \in \mathbf{U}_1} s_u + 2\sum_{u \in \mathbf{U}_2} s_u + \ldots + (l-1)\sum_{u \in \mathbf{U}_{l-1}} s_u + l\sum_{u \in \mathbf{U}_l} s_u}.$$

(4) The number of γ -constacyclic codes of length n over A is:

$$|\mathcal{L}(\mathbf{A}_1)| \cdots |\mathcal{L}(\mathbf{A}_r)|.$$

For the remainder of this paper the following notation will be used. Let $(A, \mathfrak{m}, GF(q)) \in \mathfrak{F}_5^4$, $f \in A[T]$ a basic irreducible polynomial, $s = \deg(\bar{f})$ and $(B = A[T]/\langle f \rangle, \mathfrak{m}B, GF(q^s))$ the separable extension of A determined by f.

- (a) For $\mathbb{T} \subset A$, a set of representatives of GF(q), without loss of generality it can be assume that \mathbb{T} is the Teichmüller set of the Galois ring GR(char(A), d).
- (b) $\mathbb{T}_s = \{a_0 + a_1 \mathbf{T} + \dots + a_{s-1} \mathbf{T}^{s-1} : a_i \in \mathbb{T}\} \subset \mathbf{B}$ the set of representatives of $\mathbf{B}/\mathfrak{m}\mathbf{B} = \mathbf{GF}(q^s)$.
- (c) For $a \in GF(q^s)$, $a(\mathbb{T}_s)$ will denote the only representative of a in \mathbb{T}_s . For $h = a_0 + a_1 T + \ldots + a_l T^l \in GF(q^s)[T]$ the polynomial $a_0(\mathbb{T}_s) + a_1(\mathbb{T}_s)T + \ldots + a_l(\mathbb{T}_s)T^l$ in B[T] will denoted by $h_{\mathbb{T}_s}$.
- (d) A fixed minimal A-generating set $\{\alpha_1, \alpha_2\}$ of the maximal ideal \mathfrak{m} will be considered.

If the ring A is one of the rings in case (a), (b) and (c) of Theorem 4.10, $\alpha_1 = x$ and $\alpha_2 = y$.

If the ring A is one of the rings in case (d) of Theorem 4.10, $\alpha_1 = x$ and $\alpha_2 = p$.

If the ring A is one of the rings in case (e) of Theorem 4.10, $\alpha_1 = p$ and $\alpha_2 = x$.

When we take a minimal A-generating set for \mathfrak{m} we understand that $\{\alpha_1, \alpha_2\}$ is that ordered minimal A-generating set for \mathfrak{m} .

Observe that, in all cases, $\alpha_1 \alpha_2 = 0$, $\mathfrak{m} = \langle \alpha_1, \alpha_2 \rangle$, $\mathfrak{m}^2 = \langle \alpha_2^2 \rangle$, and $\operatorname{ann}_A(\mathfrak{m}^2) = \langle \alpha_1, \alpha_2^2 \rangle$.

For our purposes the following result on the ideals of a ring in the family \mathfrak{F}_5^4 will be useful.

Lemma 5.2. Let $(A, \mathfrak{m}, GF(q)) \in \mathfrak{F}_5^4$, \mathbb{T} and \mathbb{T}_s as above, $\tilde{\alpha} = \{\alpha_1, \alpha_2\}$ the minimal A-generating set for $\mathfrak{m}, f \in A[T]$ a monic basic irreducible polynomial of degree s and $B = A[T]/\langle f \rangle$, then:

The ideals of length 2 of B are between m³B and ann_A(m²)B and these ideals are:

 $\langle \alpha_2^2 \rangle, \langle \alpha_1 + \lambda_1 \alpha_2^2 \rangle, \langle \alpha_1 + \lambda_2 \alpha_2^2 \rangle, \dots, \langle \alpha_1 + \lambda_{q^s} \alpha_2^2 \rangle \quad \lambda_i \in \mathbb{T}_s.$

(2) The ideals of length 3 of B are between $\mathfrak{m}^2 B$ and $\mathfrak{m} B$ and these ideals are:

 $\langle \alpha_1, \alpha_2^2 \rangle, \langle \alpha_2 \rangle, \langle \alpha_1 + \lambda_2 \alpha_2 \rangle, \langle \alpha_1 + \lambda_3 \alpha_2 \rangle, \dots, \langle \alpha_1 + \lambda_{q^s} \alpha_2 \rangle \quad \lambda_i \in \mathbb{T}_s \setminus \{0\}$

In particular, the number of ideals of B is $2q^s + 6$, $\mathfrak{m}B$ and $\operatorname{ann}_A(\mathfrak{m}^2)B$ are the only two non principal ideals of B.

Proof: First recall the following facts: (a) $(B, \mathfrak{m}B, GF(q^s)) \in \mathfrak{F}_5^4$ and $\mathfrak{m}^3 B$ is the unique minimal ideal of B, (b) $\mathfrak{m}ann_A(\mathfrak{m}^2) = \mathfrak{m}^3$ and $[ann_A(\mathfrak{m}^2)]B = ann_B(\mathfrak{m}^2 B) = \langle \alpha_1, \alpha_2^2 \rangle$, (c) a minimal A-generating set for an ideal of A is a minimal B-generating set for its expansion to B, (d) $v_A(ann_A(\mathfrak{m}^2)) = v_B(ann_A(\mathfrak{m}^2)B) = v_A(\mathfrak{m}) = v_B(\mathfrak{m}B) = 2$, (e) $\mathfrak{m}^2 B = \langle \alpha_2^2 \rangle$ and $v_A(\mathfrak{m}^2) = v_B(\mathfrak{m}^2 B) = 1$

(1) $\{\alpha_1, \alpha_2^2\}$ is a minimal A-generating set for $\operatorname{ann}_A(\mathfrak{m}^2)$. By Lemma 4.1(3), the ideals of length 2 are between $\operatorname{mann}_A(\mathfrak{m}^2)B = \mathfrak{m}^3 B$ and $\operatorname{ann}(\mathfrak{m}^2)B$. The assertion follows from Corollary 2.2.

(2) By Lemma 4.1(2), the ideals of length 3 are between $\mathfrak{m}^2 B$ and $\mathfrak{m} B$. By Corollary 2.2, the ideals between $\mathfrak{m}^2 B$ and $\mathfrak{m} B$ are $\langle \alpha_2 \rangle + \mathfrak{m}^2 B$, $\operatorname{ann}_B(\mathfrak{m}^2 B) = \langle \alpha_1 \rangle + \mathfrak{m}^2 B, \langle \alpha_1 + \lambda_2 \alpha_2 \rangle + \mathfrak{m}^2 B, \langle \alpha_1 + \lambda_3 \alpha_2 \rangle + \mathfrak{m}^2 B, \ldots, \langle \alpha_1 + \lambda_{q^s} \alpha_2 \rangle + \mathfrak{m}^2 B,$ where $\lambda_i \in \mathbb{T}_s \setminus \{0\}$. Now let I be an ideal of B of length 3, since $v_B(\mathfrak{m}^2 B) = 1$, then $v_B(I) \leq 2$, and if $v_B(I) = 2$, then $I = \operatorname{ann}_B(\mathfrak{m}^2 B) = \langle \alpha_1, \alpha_2^2 \rangle$, by Lemma 4.1(4). The assertion follows.

Corollary 5.3. Let $(A, \mathfrak{m}, GF(q)) \in \mathfrak{F}_5^4$, γ a unit of A and (n, q) = 1. Let f_1, \ldots, f_r the unique monic basic irreducible pairwise coprime polynomials such that $T^n - \gamma = f_1 \cdots f_r$ and $s_i = \deg(\overline{f_i})$. Then the number of γ -constacyclic codes of length n over A is:

$$[2q^{s_1}+6][2q^{s_2}+6]\cdots[2q^{s_r}+6]$$

Proof: The assertion follows from Lemma 5.1(4) and Lemma 5.2.

Observation 1. With the notation as in Lemma 5.2.

- (1) The ideals of A of length 2 are in one to one correspondence with the set $\{(0,1), (1,\lambda) : \lambda_i \in \mathbb{T}_s\}$, that is: $(0,1) \mapsto \langle \alpha_2^2 \rangle, (1,\lambda_i) \mapsto \langle \alpha_1 + \lambda_i \alpha_2^2 \rangle \qquad \lambda_i \in \mathbb{T}_s.$
- (2) The ideals of A of length 3 are in one to one correspondence with the set $\{(0,1), (1,\lambda) : \lambda_i \in \mathbb{T}_s\}$, that is: $(0,1) \mapsto \langle \alpha_2 \rangle, (1,0) \mapsto \langle \alpha_1, \alpha_2^2 \rangle, (1,\lambda_i) \mapsto \langle \alpha_1 + \lambda_i \alpha_2 \rangle \qquad \lambda_i \in \mathbb{T}_s \setminus \{0\}.$
- (3) We write $\tilde{\alpha}$ for $\{\alpha_1, \alpha_2\}$ and $\tilde{\beta}$ for $\{\alpha_1, \alpha_2^2\}$; $(0, 1)^{\mathrm{B}}_{\tilde{\alpha}}$ for the ideal of B generated by α_2 ; $(1, 0)^{\mathrm{B}}_{\tilde{\alpha}}$ for the ideal of B generated by α_1 and α_2^2 ; $(1, \lambda_i)^{\mathrm{B}}_{\tilde{\beta}}$ for the ideal of B generated by $\alpha_1 + \lambda_i \alpha_2$, where $\lambda_i \in \mathbb{T}_s \setminus \{0\}$; $(0, 1)^{\mathrm{B}}_{\tilde{\beta}}$ for the ideal of B generated by α_2^2 ; $(1, \lambda_i)^{\mathrm{B}}_{\tilde{\beta}}$ for the ideal of B generated by $\alpha_1 + \lambda_i \alpha_2^2$, where $\lambda_i \in \mathbb{T}_s$.

For the remainder of the manuscript the following notation will be used. Given $(A, \mathfrak{m}, GF(q))$ a finite local ring, γ a unit of A. If g(T) is a factor of $T^n - \gamma$, let $\hat{g}(T) = \frac{T^n - \gamma}{g(T)}$. We will just write $a_0 + a_1T + \ldots + a_{n-1}T^{n-1}$ for the corresponding class of $a_0 + a_1 T + \ldots + a_{n-1} T^{n-1} + \langle T^n - \gamma \rangle$ in the ring $A[T]/\langle T^n - \gamma \rangle$.

The main result of this section, on the structure of γ -constacyclic codes over a ring of the family \mathfrak{F}_5^4 can now be established.

Theorem 5.4. Let $(A, \mathfrak{m}, GF(q)) \in \mathfrak{F}_5^4$, γ be a unit of A, $\tilde{\alpha} = \{\alpha_1, \alpha_2\}$ a minimal A-generating set for \mathfrak{m} , \mathbb{T} and \mathbb{T}_s as above, C a γ -constacyclic code of length n over A, f_1, \ldots, f_r the unique monic basic irreducible pairwise coprime polynomials such that $T^n - \gamma = f_1 \cdots f_r$ and $s_i = \deg(\overline{f_i})$. Then there exists unique monic polynomials F_0, F_1, F_4, F_5 , unique subsets U_2, U_3 of $[1, \ldots, r]$, and for each $i \in \{2, 3\}$ and each $u \in U_i$, a unique $\vec{v}_u \in \{(0, 1), (1, \lambda) : \lambda \in \mathbb{T}_{\deg(f_u)}\}$, such that:

- (1) $\mathbf{T}^n \gamma = \mathbf{F}_0 \mathbf{F}_1 \mathbf{F}_4 \mathbf{F}_5 \prod_{u \in \mathbf{U}_1} \mathbf{f}_u \prod_{u \in \mathbf{U}_2} \mathbf{f}_u$,
- $(2) \ \mathcal{C} = \langle \mathfrak{m}^3 \widehat{\mathcal{F}_1}, \mathfrak{m} \widehat{\mathcal{F}_4}, \widehat{\mathcal{F}_5}, (\vec{\mathbf{v}}_u)_{\tilde{\beta}} \widehat{\mathbf{f}}_u, (\vec{\mathbf{v}}_w)_{\tilde{\alpha}} \widehat{\mathbf{f}}_w : u \in \mathcal{U}_2, w \in \mathcal{U}_3 \rangle.$
- (3) $|\mathbf{C}| = q^{5\deg(\mathbf{F}_5) + 4\deg(\mathbf{F}_4) + \deg(\mathbf{F}_1) + 2\sum_{u \in \mathbf{U}_2} \deg(\mathbf{f}_u) + 3\sum_{\nu \in \mathbf{U}_3} \deg(\mathbf{f}_\nu)}$

Proof: Let $A_i = A[T]/\langle f_i \rangle$. From Lemma 5.1(2) and since $\mathfrak{m}^3 A_i$ is the minimal ideal of A_i and $\mathfrak{m} A_i$ is the maximal ideal of A_i , there is a partition of $[1, \ldots, r], V_0, V_1, \ldots, V_5$, such that C has the form:

$$\bigoplus_{v \in V_1} \mathfrak{m}^3 \mathrm{A}_v \oplus \bigoplus_{v \in V_2} \mathrm{I}_v \oplus \bigoplus_{v \in V_3} \mathrm{I}_v \oplus \bigoplus_{v \in V_4} \mathfrak{m} \mathrm{A}_v \oplus \bigoplus_{v \in V_5} \mathrm{A}_v$$

where $V_i = \{v : \ell_{A_v}(I_v) = i\}.$

Let $u \in V_2$, by Lemma 5.2(1), I_u is of the form $(\vec{v}_u)_{\tilde{\beta}}$ and it is identified in $A[T]/\langle T^n - \gamma \rangle$ with $(\vec{v}_u)_{\tilde{\beta}} \hat{f}_u$, where $\vec{v}_u \in \{(0,1), (1,\lambda) : \lambda \in \mathbb{T}_{\deg(f_u)}\}$. Let $w \in V_3$, by Lemma 5.2(2), I_w of the form $(\vec{v}_w)_{\tilde{\alpha}}$, and it is identified in $A[T]/\langle T^n - \gamma \rangle$ with $(\vec{v}_w)_{\tilde{\alpha}} \hat{f}_v$, where $\vec{v}_w \in \{(0,1), (1,\lambda) : \lambda \in \mathbb{T}_{\deg(f_w)}\}$. Let $F_i = \prod_{v \in V_i} f_v$, for $i \in \{0, 1, 4, 5\}$. Since $\bigoplus_{v \in V_i} A_v$ is identified in $A[T]/\langle T^n - \gamma \rangle$ with \hat{F}_i , the assertions (1) and (2) follow, the last assertion follows from Lemma 5.1(3). The uniqueness is trivial.

The following examples are given illustrating the previous results.

Example 1. Let $A = GF(2)[X, Y]/\langle X^2 - Y^3, XY \rangle$, be the ring of Proposition 4.7, and γ be a unit of A. $\{x, y\}$ is a minimal A-generating set for \mathfrak{m} , $\mathbb{T} = GF(2) \subset A$ is a set of representatives for its residue field. By Hensel's Lemma, $T^{15} - \gamma = f_1 f_2 f_3 f_4 f_5$, where $\deg(f_1) = 1$, $\deg(f_2) = 2$, $\deg(f_3) = \deg(f_4) = \deg(f_5) = 4$. Then $A[T]/\langle T^{15} - \gamma \rangle \cong A \oplus A[T]/\langle f_2 \rangle \oplus A[T]/\langle f_3 \rangle \oplus A[T]/\langle f_4 \rangle \oplus A[T]/\langle f_5 \rangle$, $\mathbb{T}_2 = \{a_1 + a_2 T : a_i \in GF(2)\}$ is a set of representatives for the

residue field of the ring $A[T]/\langle f_2 \rangle$, $\mathbb{T}_4 = \{a_1 + a_2T + a_3T^2 + a_4T^3 : a_i \in GF(2)\}$ is a set of representatives for the residue field of the rings $A[T]/\langle f_i \rangle$, $i \in \{3, 4, 5\}$.

The number of γ -constacyclic codes of length 15 over A is $[2(2)^4 + 6][2(2)^4 + 6][2(2)^2 + 6][2(2)^2 + 6][2(2) + 6] = 7682080$, and

(a) If $U_2 = \{2\}$, $U_3 = \{3\}$, $F_0 = f_1f_4$, $F_1 = f_5$, $F_4 = F_5 = 1$, $\vec{v}_2 = (1, a_0 + a_1T)$ and $\vec{v}_3 = (0, 1)$, the corresponding code is:

$$\mathcal{C} = \langle \mathfrak{m}^3 \widehat{\mathcal{F}}_1, \mathfrak{m} \widehat{\mathcal{F}}_4, \widehat{\mathcal{F}}_5, (\vec{\mathbf{v}}_u)_{\tilde{\beta}} \widehat{\mathbf{f}}_u, (\vec{\mathbf{v}}_w)_{\tilde{\alpha}} \widehat{\mathbf{f}}_w : u \in \mathcal{U}_2, w \in \mathcal{U}_3 \rangle =$$

$$\langle \mathfrak{m}^3 \hat{\mathbf{f}}_5, [\mathbf{x} + (a_0 + a_1 \mathbf{T})\mathbf{y}^2] \hat{\mathbf{f}}_2, \hat{\mathbf{y}} \hat{\mathbf{f}}_3 \rangle =$$

 $\langle \mathbf{y}^3 \mathbf{f}_1 \mathbf{f}_2 \mathbf{f}_3 \mathbf{f}_4, \mathbf{f}_1 \mathbf{f}_2 \mathbf{f}_3 \mathbf{f}_4, [\mathbf{x} + (a_0 + a_1 \mathbf{T} + a_2 \mathbf{T}^2 + a_3 \mathbf{T}^3) \mathbf{y}^2] \mathbf{f}_1 \mathbf{f}_3 \mathbf{f}_4 \mathbf{f}_5, \mathbf{y} \mathbf{f}_1 \mathbf{f}_2 \mathbf{f}_4 \mathbf{f}_5 \rangle.$

(b) If $U_2 = \{4\}$, $U_3 = \emptyset$, $F_0 = 1$, $F_1 = f_2$, $F_4 = f_1f_3$, $F_5 = f_5$, $\vec{v}_4 = (1, a_0 + a_1T + a_2T^2 + a_3T^3)$, the corresponding code is:

 $\mathbf{C} = \langle \mathfrak{m}^{3} \widehat{\mathbf{F}_{1}}, \mathfrak{m} \widehat{\mathbf{F}_{4}}, \widehat{\mathbf{F}_{5}}, (\vec{\mathbf{v}}_{u})_{\tilde{\beta}} \widehat{\mathbf{f}}_{u}, (\vec{\mathbf{v}}_{w})_{\tilde{\alpha}} \widehat{\mathbf{f}}_{w} : u \in \mathbf{U}_{2}, w \in \mathbf{U}_{3} \rangle = \\ \langle \mathfrak{m}^{3} \widehat{\mathbf{f}_{2}}, \mathfrak{m} \widehat{\mathbf{f}_{1}}, \widehat{\mathbf{f}_{5}}, [\mathbf{x} + (a_{0} + a_{1}\mathbf{T} + a_{2}\mathbf{T}^{2} + a_{3}\mathbf{T}^{3})\mathbf{v}^{2}] \widehat{\mathbf{f}}_{4} \rangle =$

 $\langle y^{3}f_{1}f_{3}f_{4}f_{5}, xf_{2}f_{4}f_{5}, yf_{2}f_{4}f_{5}, f_{1}f_{2}f_{3}f_{4}, [x+(a_{0}+a_{1}T+a_{2}T^{2}+a_{3}T^{3})y^{2}]f_{1}f_{2}f_{3}f_{5}\rangle.$

Example 2. Let $A = GR(2^2, d)[X, Y]/\langle Y^2 - 2, X^2 - Y^3, XY \rangle$, be the ring of Proposition 4.6, and γ be a unit of $A \{x, y\}$ is a minimal A-generating set for $\mathfrak{m}, \mathbb{T} = \{0, 1\} \subset A$ is a set of representatives for its residue field. By Hensel's Lemma, $T^7 - \gamma = f_1 f_2 f_3$, where $\deg(f_1) = 1$, $\deg(f_2) = \deg(f_3) = 3$. Then $A[T]/\langle T^7 - \gamma \rangle \cong A \oplus A[T]/\langle f_2 \rangle \oplus A[T]/\langle f_3 \rangle, \mathbb{T}_3 = \{a_1 + a_2 T + a_3 T^2 : a_i \in GF(2)\}$ is a set of representatives for the residue field of the rings $A[T]/\langle f_i \rangle, i \in \{2, 3\}$. The number of γ -constacyclic codes of length 7 over A is $[2(2) + 6][2(2)^3 + 6][2(2)^3 + 6] = 4840$, and

(a) If $U_2 = \{1,2\}$, $U_3 = \{3\}$, $F_0 = F_1 = F_4 = F_5 = 1$, $\vec{v}_1 = (1,0)$, $\vec{v}_2 = (1, a_0 + a_1 T + a_2 T^2)$ and $\vec{v}_3 = (1, b_0 + b_1 T + b_2 T^2)$, the corresponding code is:

$$\begin{split} \mathbf{C} &= \langle \mathfrak{m}^3 \widehat{\mathbf{F}_1}, \mathfrak{m} \widehat{\mathbf{F}_4}, \widehat{\mathbf{F}_5}, (\vec{\mathbf{v}}_u)_{\tilde{\beta}} \widehat{\mathbf{f}}_u, (\vec{\mathbf{v}}_w)_{\tilde{\alpha}} \widehat{\mathbf{f}}_w : u \in \mathbf{U}_2, w \in \mathbf{U}_3 \rangle = \\ &\qquad \langle \mathfrak{m}^3 \widehat{\mathbf{f}_5}, [\mathbf{x} + (a_0 + a_1 \mathbf{T}) \mathbf{y}^2] \widehat{\mathbf{f}}_2, \mathbf{y} \widehat{\mathbf{f}}_3 \rangle = \\ &\qquad \langle \mathbf{y}^3 \mathbf{f}_1 \mathbf{f}_2 \mathbf{f}_3 \mathbf{f}_4, \mathbf{f}_1 \mathbf{f}_2 \mathbf{f}_3 \mathbf{f}_4, [\mathbf{x} + (a_0 + a_1 \mathbf{T} + a_2 \mathbf{T}^2 + a_3 \mathbf{T}^3) \mathbf{y}^2] \mathbf{f}_1 \mathbf{f}_3 \mathbf{f}_4 \mathbf{f}_5, \mathbf{y} \mathbf{f}_1 \mathbf{f}_2 \mathbf{f}_4 \mathbf{f}_5 \rangle. \end{split}$$

$$\begin{array}{ll} (b) \ \ If \ \mathbf{U}_2 \ = \ \{4\}, \ \mathbf{U}_3 \ = \ \emptyset, \ \mathbf{F}_0 \ = \ 1, \ \mathbf{F}_1 \ = \ \mathbf{f}_2, \ \mathbf{F}_4 \ = \ \mathbf{f}_1\mathbf{f}_3, \ \mathbf{F}_5 \ = \ \mathbf{f}_5, \ \vec{\mathbf{v}}_4 \ = \\ (1, a_0 + a_1\mathbf{T} + a_2\mathbf{T}^2 + a_3\mathbf{T}^3), \ the \ corresponding \ code \ is: \\ \\ \mathbf{C} \ = \ \langle \mathfrak{m}^3\widehat{\mathbf{F}_1}, \mathfrak{m}\widehat{\mathbf{F}_4}, \widehat{\mathbf{F}_5}, (\vec{\mathbf{v}}_u)_{\hat{\beta}}\widehat{\mathbf{f}}_u, (\vec{\mathbf{v}}_w)_{\hat{\alpha}}\widehat{\mathbf{f}}_w \ : u \in \mathbf{U}_2, w \in \mathbf{U}_3 \rangle = \\ \\ & \quad \langle \mathfrak{m}^3\widehat{\mathbf{f}_2}, \mathfrak{m}\widehat{\mathbf{f}_1\mathbf{f}_3}, \widehat{\mathbf{f}_5}, [\mathbf{x} + (a_0 + a_1\mathbf{T} + a_2\mathbf{T}^2 + a_3\mathbf{T}^3)\mathbf{y}^2]\widehat{\mathbf{f}}_4 \rangle = \\ \\ & \quad \langle \mathbf{y}^3\mathbf{f}_1\mathbf{f}_3\mathbf{f}_4\mathbf{f}_5, \mathbf{x}\mathbf{f}_2\mathbf{f}_4\mathbf{f}_5, \mathbf{y}\mathbf{f}_2\mathbf{f}_4\mathbf{f}_5, \mathbf{f}_1\mathbf{f}_2\mathbf{f}_3\mathbf{f}_4, [\mathbf{x} + (a_0 + a_1\mathbf{T} + a_2\mathbf{T}^2 + a_3\mathbf{T}^3)\mathbf{y}^2]\mathbf{f}_1\mathbf{f}_2\mathbf{f}_3\mathbf{f}_5 \rangle. \end{array}$$

6 Conclusion

In this paper the family of finite local Frobenius non-chain rings of length 5 and nilpotency index 4 is determined. Furthermore, the number and structure of γ -constacyclic over finite local Frobenius non-chain rings of length 5 and nilpotency index 4, of length relatively prime to the characteristic of the residue field of the ring, are determined. Examples are included illustrating the main results.

References

- [1] Y. Cao, Yonglin Cao, Negacyclic codes over the local ring $\mathbb{Z}_4[v]/\langle v^2 + 2v \rangle$ of oddly even length and their Gray images, Finite Fields Appl. 52 (2018) 67-93.
- [2] C. A. Castillo-Guillén, C. Rentería-Márquez, H. Tapia-Recillas, Constacyclic Codes over Finite local Frobenius Non-Chain Rings with nilpotency index 3, Finite Fields Appl. 43 (2017) 1-21.
- [3] C. A. Castillo-Guillén, C. Rentería-Márquez, H. Tapia-Recillas, Duals of constacyclic codes over finite local Frobenius non-chain rings of length 4, Discrete Math. 341 (2018) 919-933.
- [4] H. Q. Dinh, S. R. López-Permouth, Cyclic and Negacyclic Codes Over Finite Chain Rings, IEEE Trans. Inf. Theory 50 (2004) 1728-1744.
- [5] H. Q. Dinh, A. K. Singh, P. Kumar, S. Sriboonchitta, On the structure of cyclic codes over the ring Z_{2^s}[u]/⟨u^k⟩, Discrete Math. 341 (2018) 2243-2275.
- [6] S. T. Dougherty, S. Karadeniz, B. Yildiz, *Cyclic codes over* R_k, Des. Codes and Cryptogr., vol. **63**, (113-126), (2012).

- [7] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, P. Solé, The Z₄-linearity of Kerdock, Preparata, Goethals, and related codes, IEEE Trans. Inf. Theory 40 (1994) 301-319.
- [8] S. Karadeniz and B. Yildiz, *Cyclic codes over* $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, Des. Codes and Cryptogr., vol. **58**, (221-234), (2011).
- [9] E. Martínez-Moro and S. Szabo, On Codes over Local Frobenius Non-Chain Rings of Order 16, Contemporary Mathematics, vol. 684, (227-241), (2015).
- [10] B. R. McDonald, Finite Rings with Identity, Marcel Dekker, New York, 1974.
- [11] J. Wood, Duality for Modules Over Finite Rings and Applications to Coding Theory, Am. J. Math. 121 (1999) 555-575.

C. A. Castillo-Guillén,
Department of Mathematics,
Universidades para el Bienestar Benito Juárez García,
Tláhuac Ave 6391, 13360 Ciudad de México, México.
Email: carlos_53@hotmail.com
C. Rentería-Márquez,
Department of Mathematics,
Escuela Superior de Física y Matemáticas, Instituto Politécnico Nacional,
Instituto Politécnico Nacional Ave s/n, 07300, Ciudad de México, México

CONSTACYCLIC CODES OVER FINITE LOCAL FROBENIUS NON-CHAIN RINGS OF LENGTH 5 AND NILPOTENCY INDEX 4

92