International Journal of Pure and Applied Mathematics
Volume 80 No. 2 2012, 181-190
ISSN: 1311-8080 (printed version)
url: http://www.ijpam.eu

ijpam.eu

ON THE CYCLICITY OF THE GRAY IMAGE OF A CLASS OF LINEAR CYCLIC CODES OVER A FINITE CHAIN RING

C.A. López-Andrade[1] §, H. Tapia-Recillas[2]

[1]Facultad de Ciencias Físico Matemáticas
Benemérita Universidad Autónoma de Puebla
18 Sur y Av. San Claudio Col. San Manuel
Puebla, Pue., 72570, MÉXICO

[1,2]Departamento de Matemáticas
Universidad Autónoma Metropolitana-Iztapalapa
Col. Vicentina, Del. Iztapalapa
México, D.F., 09340, MÉXICO

Abstract: Results on the linear cyclicity of the Gray image of a class of linear cyclic codes over a finite chain ring $\mathcal{R}$ of nilpotency index 2 are presented. For this purpose, following [1], the generator polynomial of an $\mathcal{R}$-linear cyclic code of length n relatively prime to the characteristic of the residual field of $\mathcal{R}$ is given.

AMS Subject Classification: 94B15, 94B05, 13E10
Key Words: finite chain rings, linear cyclic codes, gray map

1. Introduction

Since the Kerdock and Preparata codes were found to be the Gray image of $\mathbb{Z}_4$-linear codes, the study of codes over finite rings has increased (see [3]). First codes over the ring $\mathbb{Z}_{p^n}$ of integers modulo p^n where p is a prime and $n > 1$ an integer, and the corresponding Gray image were treated (see [5],

Received: May 6, 2012

§Correspondence author

[10]). Then codes over some finite rings, including Galois rings, and recently over general finite chain rings, were studied (see [6], [7]). Since finite chain rings generally do not have a rich structure the description of codes over these rings and, particularly, the Gray image of these codes is not a trivial question to answer. However in an attempt to give an answer to this question, in this note the Gray image of a class of linear cyclic codes defined over a finite chain ring of characteristic p and nilpotency index 2 is determined. The manuscript is divided as follows. In Section 2 basic definitions and facts on finite chain rings and the Gray map on these rings are recalled. In Section 3 a polynomial formulation of the Gray map is presented as well as technical results which are used in Section 4 where the main results of this manuscript are given.

2. About Finite Chain Rings

In this section basic definitions and properties of finite chain rings are recalled. For further details we refer the reader to [8] (see also [1], [9]).

We recall that a *finite chain ring* is an associative, commutative, finite ring with identity whose ideals are ordered by inclusion. This class of rings has the following properties (see [1], Proposition 2.1):

Proposition 1. *For a finite commutative ring $\mathcal{R}$ the following conditions are equivalent:*

i) *$\mathcal{R}$ is a local ring and the maximal ideal $\mathcal{M}$ of $\mathcal{R}$ is principal,*

ii) *$\mathcal{R}$ is a local principal ideal ring,*

iii) *$\mathcal{R}$ is a chain ring.*

Let $(\mathcal{R}, \mathcal{M})$ be a finite chain ring and let π be a fixed generator for the maximal ideal $\mathcal{M}$. Then π is a nilpotent element and let $t+1$ be its nilpotency index. The finite chain of ideals of $\mathcal{R}$ is:

$$\mathcal{R} = \langle \pi^0 \rangle \supset \langle \pi^1 \rangle \supset \cdots \langle \pi^{t-1} \rangle \supset \langle \pi^{t+1} \rangle = \langle 0 \rangle.$$

Let $\mathbb{F} = \mathcal{R}/\mathcal{M}$ be the residue field of $\mathcal{R}$ which is isomorphic to a finite field $I\!F_{p^m}$ with p^m elements and let $\mu : \mathcal{R} \longrightarrow \mathbb{F}$, $\mu(a) = \overline{a} = a + \mathcal{M}$ be the canonical residue homomorphism.

Let $\mathcal{T} \subseteq \mathcal{R}$ be a set of representatives for the equivalence classes of $\mathcal{R}$ modulo $\mathcal{M}$. Equivalently, $\mathcal{T}$ can be defined as the maximal subset of $\mathcal{R}$ with

the property that $\mu(r_1) \neq \mu(r_2)$ implies $r_1 \neq r_2$, for all $r_1, r_2 \in \mathcal{R}$. This set is called the *Teichmüller* set of representatives of $\mathcal{R}$.

Lemma 2. *(see [9]) Let $\mathcal{R}$ be a finite chain ring with nilpotency index $t+1$ and let $\mathcal{T} \subset R$ be a Teichmüller set of representatives of $\mathcal{R}$. Then,*

i) Any element $a \in \mathcal{R}$ has a unique representation: $a = \rho_0(a) + \rho_1(a)\pi + \cdots + \rho_t(a)\pi^t$ where $\rho_j(a) \in \mathcal{T}$.

ii) $|\mathcal{T}| = |\mathbb{F}|$.

iii) $|\pi^i\mathcal{R}| = |\mathbb{F}|^{t-i+1}$ for $0 \leq i \leq t+1$. In particular, $|\mathcal{R}| = |I\!F|^{t+1}$, i.e., $|\mathcal{R}| = p^{(t+1)m}$.

Examples of finite chain rings include the following:

i) Galois rings $GR(p^n, m)$ where p is a prime and $n, m \geq 1$ are integers. If $m = 1$, $GR(p^n, 1) = \mathbb{Z}_{p^n}$, the ring of integers modulo p^n, and if $n = 1$, $GR(p, m) = \mathbb{F}_{p^m}$, the finite field with p^m elements (see [8]).

ii) Residue class rings $I\!F_p[\xi]/\langle w(\xi)^k \rangle$, where $w(\xi)$ is an irreducible polynomial over $I\!F_p$ of degree $m \geq 1$ and $k \geq 1$ is an integer (see [11]).

2.1. The Gray Map on a Finite Chain Ring

From now on $\mathcal{R}$ will denote a finite commutative chain ring of nilpotency index $t+1 = 2$, i.e., $t = 1$. Let π be a fixed generator of the maximal ideal $\mathcal{M}$ of $\mathcal{R}$, $I\!F$ the residue field of $\mathcal{R}$, which is isomorphic to $I\!F_q$ where $q = p^m$ for some prime p and an integer $m \geq 1$, and let $\mathcal{T}$ be a Teichmüller set of representatives of the ring $\mathcal{R}$.

We recall that if $X = (x_0, ..., x_{n-1})$ and $Y = (y_0, ..., y_{m-1})$ are elements of $\mathcal{R}^n$, $n > 1$ an integer, their Kronecker product is defined as:

$$X \otimes Y = (x_0Y, x_1Y, ..., x_{n-1}Y).$$

Let $I\!F = \{0, \omega^0, ..., \omega^{q-2}\}$ be the residue field of the finite chain ring $\mathcal{R}$, where ω is a primitive element, let $\mathbf{C_0} = (0, \omega^0, ..., \omega^{q-2})$ be the vector whose entries are all the elements of $I\!F$ and let $\mathbf{C_1} = (1, 1, ..., 1)$ be the all-one vector of length q. Let a be any element of $\mathcal{R}$ with π-adic representation $a = \rho_0(a) + \rho_1(a)\pi$ where $\rho_0(a), \rho_1(a) \in \mathcal{T}$ and let $r_j(a) = \mu(\rho_j(a)) \in I\!F$.

Let $A = (a_0, ..., a_{n-1}) \in \mathcal{R}^n$ which can be written as $A = \rho_0(A) + \rho_1(A)\pi$ where $\rho_j(A) = (\rho_j(a_0), ..., \rho_j(a_{n-1}))$, $j = 0, 1$ and $\rho_j(a_i) \in \mathcal{T}$ so that $r_j(A) = (r_j(a_0), ..., r_j(a_{n-1}))$ for $j = 0, 1$.

The Gray map on $\mathcal{R}^n$ is defined (permutation equivalente) as (cf. [2]):

$$\Phi : \mathcal{R}^n \longrightarrow I\!F^{nq},\ \Phi(\mathbf{A}) = \mathbf{C_0} \otimes r_0(\mathbf{A}) + \mathbf{C_1} \otimes r_1(\mathbf{A}), \tag{1}$$

where $\mathbf{A} = (a_0, ..., a_{n-1}) \in \mathcal{R}^n$ and " $\otimes$ " is the Kronecker product (expanded from right to left).

Let

$$b_j(a_k) = \begin{cases} r_1(a_k), & \text{for } j = k \text{ and } k \in \{0, ..., n-1\}, \\ \omega^{s-1} r_0(a_k) + r_1(a_k), & \text{for } j = sn + k,\ s \in \{1, ..., q-1\}, \\ & k \in \{0, , 1, ..., n-1\}. \end{cases}$$

From the definition of the Gray map it is easy see that

$$\Phi(A) = (\ldots, b_j(a_k), \ldots) \in I\!F^{qn}.$$

The *homogeneous* weight on the ring $\mathcal{R}$ is defined as (cf. [2], [4]):

$$wt_h(\gamma) = \begin{cases} q-1, & \text{if } \gamma \in \mathcal{R} \setminus \langle \pi \rangle \\ q, & \text{if} \gamma \in \langle \pi \rangle \setminus \{0\} \\ 0, & \text{otherwise} \end{cases}$$

with $q = p^m$ as above. This weight is extended to $\mathcal{R}^n$ as:

$$wt_h(A) = wt_h(a_0) + \cdots + wt_h(a_{n-1}),$$

where $A = (a_0, a_1, ..., a_{n-1}) \in \mathcal{R}^n$.

Let d_h be the *homogeneous* distance on $\mathcal{R}^n$ determined by the homogeneous weight. One of the main properties of the Gray map is the following (see [2]):

Theorem 3. *With the notation as introduced above, the Gray map is an injective isometry from $(\mathcal{R}^n, d_h)$ into $(\mathbb{F}^{nq}, d_H)$ where d_H is the Hamming distance on $\mathbb{F}^{nq}$.*

3. The Polynomial Representation of the Gray Map

Let $\mathcal{S}$ be a finite commutative ring, $\mathcal{A}_{\mathcal{S}}(t) = \mathcal{S}[\xi]/\langle \xi^t - 1 \rangle$ and let

$$\mathcal{P}^t_{\mathcal{S}} : \mathcal{S}^t \longrightarrow \mathcal{A}_{\mathcal{S}}(t),$$

$$(a_0, a_1, ..., a_{t-1}) \quad \longrightarrow \quad a_0 + a_1\xi + \cdots + a_{t-1}\xi^{t-1} + \langle \xi^t - 1 \rangle$$

be the polynomial representation of $\mathcal{S}^t$ into the ring $\mathcal{A}_{\mathcal{S}}(t)$. By taking representatives of the elements of $\mathcal{A}_{\mathcal{S}}(t)$, we just write

$$\mathcal{P}^t_{\mathcal{S}}(a_0, a_1, ..., a_{t-1}) = \ a_0 + a_1\xi + \cdots + a_{t-1}\xi^{t-1}.$$

Definition 4. With the notation as introduced above, the polynomial representation of the Gray Φ is the mapping $\Phi_{\mathcal{P}} : \mathcal{A}_{\mathcal{R}}(n) \longrightarrow \mathcal{A}_{I\!F}(qn)$ defined as

$$\Phi_{\mathcal{P}} = \mathcal{P}^{qn}_{I\!F} \circ \Phi \circ (\mathcal{P}^n_{\mathcal{R}})^{-1}.$$

If $A(\xi)$ is the polynomial representation in $\mathcal{A}_{\mathcal{R}}(n)$ of $A \in \mathcal{R}^n$ then $\Phi_{\mathcal{P}}(A(\xi))$ is the polynomial representation of $\Phi(A)$ in $\mathcal{A}_{I\!F}(qn)$.

The polynomial representation of $\Phi(A)$ in $\mathcal{A}_{I\!F}(qn)$ can be written as:

$$\Phi_{\mathcal{P}}(A(\xi)) = \sum_{s=0}^{q-1} \sum_{k=0}^{n-1} b_{sn+k}(a_k)\xi^{sn+k}, \tag{2}$$

where $b_j(a_k)$ is as defined above.

For $s \in \{0, 1, \ldots, q-1\}$ let $f_s(\xi) = \sum_{k=0}^{n-1} b_{sn+k}(a_k)\xi^k$, then relation (2) can be expressed as

$$\Phi_{\mathcal{P}}(A(\xi)) = \sum_{s=0}^{q-1} f_s(\xi)\xi^{sn}.$$

The following identities are easy to prove and will be useful later.

Lemma 5. *Let $q = p^m$, $I\!F_q$ be the finite field with q elements and ω a primitive element of $I\!F_q$. Then on $I\!F_q[\xi]$ the following relations hold:*

i) $1 + \xi^n + \xi^{2n} + \cdots + \xi^{(p^m-1)n} = (\xi^{p^m n} - 1)/(\xi^n - 1) = (\xi^n - 1)^{p^m - 1}$.

ii) $\xi^n + \omega\xi^{2n} + \ldots + \omega^{p^m-2}\xi^{(p^m-1)n} = \omega^{p^m-2}\xi^n \prod_{i=0}^{p^m-2}(\xi^n - \omega^i)$.

Let $A(\xi) = a_0 + a_1\xi + \cdots + a_{n-1}\xi^{n-1} \in \mathcal{A}_{\mathcal{R}}(n)$ be the polynomial representation of $A = (a_0, \ldots, a_{n-1}) \in \mathcal{R}^n$. If $a_i = \rho_0(a_i) + \pi\rho_1(a_i)$, where $\rho_0(a_i)$, $\rho_1(a_i) \in \mathcal{T}$ for each $i \in \{0, 1, \ldots, n-1\}$, then

$$A(\xi) = \rho_0(A)(\xi) + \pi\rho_1(A)(\xi),$$

where $\rho_0(A)(\xi)$ and $\rho_1(A)(\xi)$ are, respectively, the polynomial representations in $\mathcal{A}_{\mathcal{R}}(n)$ of

$$\rho_0(A) \quad = \quad (\rho_0(a_0), \rho_0(a_1), \ldots, \rho_0(a_{n-1})),$$

$$\rho_1(A) \;=\; (\rho_1(a_0), \rho_1(a_1), \ldots, \rho_1(a_{n-1})).$$

The following expression for the polynomial representation of the Gray map will be useful for our purposes.

Proposition 6. *If* $A(\xi) = \rho_0(A)(\xi) + \pi\rho_1(A)(\xi)$, *then*

$$\Phi_{\mathcal{P}}(A(\xi)) = r_0(A)(\xi)\omega^{p^m-2}\xi^n \prod_{i=0}^{p^m-2} (\xi^n - \omega^i) + r_1(A)(\xi)(\xi^n - 1)^{p^m-1}, \qquad (3)$$

where $r_0(A)(\xi), r_1(A)(\xi) \in \mathcal{A}_{\mathbb{F}}(n)$ *are the polynomial representations of* $r_0(A) = (r_0(a_0), r_0(a_1), \ldots, r_0(a_{n-1}))$ *and* $r_1(A) = (r_1(a_0), r_1(a_1), \ldots, r_1(a_{n-1}))$ *respectively. Furthermore,* $r_0(A)(\xi)$ *and* $r_1(A)(\xi)$ *are the* μ*-reductions of* $\rho_0(A)(\xi)$ *and* $\rho_1(A)(\xi)$ *respectively.*

Proof. The first summand of relation (3) follows from collecting the first terms of the expression of the coefficients $b_{sn+k}(a_k)$ in relation (2) and from part ii) of Lemma 5. The second summand appearing in (3) is obtained by collecting the remaining terms of the expression for $\Phi_{\mathcal{P}}(A(\xi))$ given in (2). □

Observation. The result of Proposition 6 generalizes Proposition 12 *c*) of [12].

Lemma 7. *Let* $H = (h_0, h_1, \ldots, h_{n-1})$ *be any element of* $\mathcal{R}^n$, $H(\xi)$ *in* $\mathcal{A}_{\mathcal{R}}(n)$ *its corresponding polynomial representation, and let* $h(\xi)$ *in* $\mathcal{A}_{\mathbb{F}}(n)$ *be the* μ*-reduction of* $H(\xi)$. *If* $\Phi_{\mathcal{P}}(\pi H(\xi)) \in \mathcal{A}_{\mathbb{F}}(qn)$ *is the polynomial representation of* $\Phi(\pi H)$ *then,*

$$\Phi_{\mathcal{P}}(\pi H(\xi)) = h(\xi)(\xi^n - 1)^{p^m-1}.$$

Proof. Let $H = (h_0, h_1, \ldots, h_{n-1}) \in \mathcal{R}^n$ with $h_i = \rho_0(h_i) + \pi\rho_1(h_i) \in \mathcal{R}$, $\rho_0(h_i), \rho_1(h_i) \in \mathcal{T}$. Then

$$\begin{aligned} \pi H &= (\pi h_0, \ldots, \pi h_{n-1}) \\ &= (\pi(\rho_0(h_0) + \pi\rho_1(h_0)), \ldots, \pi(\rho_0(h_{n-1}) + \pi\rho_1(h_{n-1}))) \\ &= (0 + \pi\rho_0(h_0), \ldots, 0 + \pi\rho_0(h_{n-1})). \end{aligned}$$

Applying Proposition 6 to πH we have:

$$\Phi_{\mathcal{P}}(\pi H)(\xi) \;=\; \left[\sum_{i=0}^{n-1} r_1(\pi h_i)\xi^i\right] \left[(\xi^n - 1)^{p^m-1}\right]$$

$$= \left[\sum_{i=0}^{n-1} r_0(h_i)\xi^i\right]\left[(\xi^n-1)^{p^m-1}\right] = h(\xi)(\xi^n-1)^{p^m-1}$$

where $h(\xi) := \mu(H(\xi)) = \sum_{i=0}^{n-1} r_0(h_i)\xi^i$, and the claim follows. □

4. Gray Image of a Class of Linear Cyclic Codes over $\mathcal{R}$

Let $\mathcal{R}$ be a ring as described above. We recall that a subset $\mathcal{C} \subseteq \mathcal{R}^n$ is an $\mathcal{R}$-linear code of length n if $\mathcal{C}$ is an $\mathcal{R}$-submodule of $\mathcal{R}^n$, and $\mathcal{C}$ is cyclic if whenever $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$ then $(c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}$. Via the polynomial representation mapping, an element $c = (c_0, c_1, \ldots \ldots, c_{n-1}) \in \mathcal{R}^n$ is identified with the polynomial $c_0 + c_1\xi + \cdots + c_{n-1}\xi^{n-1}$ in $\mathcal{R}[\xi]/\langle\xi^n - 1\rangle$. It is well known that a code $\mathcal{C}$ of length n over $\mathcal{R}$ is cyclic if and only if its image under the polynomial representation mapping is an ideal of $\mathcal{R}[\xi]/\langle\xi^n - 1\rangle$. If the length n of the code is relatively prime to the characteristic of the residue field $\mathbb{F}$ of the ring $\mathcal{R}$, a characterization of linear cyclic codes of length n can be found in [1]. Along the same line of ideas we have the following result.

Theorem 8. *With the notation as above, let $n \geq 1$ be an integer relatively prime to the characteristic p of the residue field $\mathbb{F}$ and let $\mathcal{C}$ be a $\mathcal{R}$-linear cyclic code of length n. Then there exists a unique family of pairwise coprime monic polynomials $A(\xi), B(\xi), C(\xi) \in \mathcal{R}[\xi]$ such that $A(\xi)B(\xi)C(\xi) = \xi^n - 1$ and $\mathcal{C} = \langle A(\xi)[B(\xi) + \pi]\rangle$ in $\mathcal{R}[\xi]/\langle\xi^n - 1\rangle$.*

Proof. Let I be a nontrivial ideal of $\mathcal{A}(n) = \mathcal{R}[\xi]/\langle\xi^n - 1\rangle$. From [1, Theorem 3.4], there exists a unique family of pairwise coprime monic polynomials $A(\xi), B(\xi), C(\xi) \in \mathcal{R}[\xi]$ with $A(\xi)B(\xi)C(\xi) = \xi^n - 1$ in $\mathcal{R}[\xi]$ such that $I = \langle\hat{C}(\xi), \pi\hat{B}(\xi)\rangle$ where $\hat{B}(\xi) = A(\xi)C(\xi)$ and $\hat{C}(\xi) = A(\xi)B(\xi)$. Moreover, from [1, Theorem 3.6] it follows that, $I = \langle\hat{C}(\xi) + \pi\hat{B}(\xi)\rangle$. Let $J = \langle G(\xi)\rangle$ where $G(\xi) = A(\xi)[B(\xi) + \pi]$. The claim of the Theorem would be proved if it can be shown that $I = J$. First we see that $I \supseteq J$. Since $C(\xi)$ and $B(\xi)$ are coprime there exists $U(\xi), V(\xi) \in \mathcal{R}[\xi]$ such that $U(\xi)C(\xi) + V(\xi)B(\xi) = 1$. By reducing modulo $\xi^n - 1$ a similar relation for $U(s)$ and $V(s)$ in $\mathcal{A}(n)$ is obtained. Then,

$$\pi U(\xi)A(\xi)C(\xi) + \pi V(\xi)A(\xi)B(\xi) = \pi A(\xi) \text{ in } \mathcal{A}(n). \tag{4}$$

Using relation (4) it is easy to see that

$$G(\xi) = [\pi V(\xi) + 1]\hat{C}(\xi) + \pi U(\xi)\ \hat{B}(\xi),$$

from which it follows that $G(\xi) \in I$ proving that $J \subseteq I$.

On the other hand, since $A(\xi)B(\xi)C(\xi) = \xi^n - 1$ in $\mathcal{R}[\xi]$ we have $C(\xi)G(\xi) = A(\xi)B(\xi)C(\xi) + \pi A(\xi)C(\xi)$ in $\mathcal{R}[\xi]$ and hence in $\mathcal{A}(n)$:

$$C(\xi)G(\xi) = \pi A(\xi)C(\xi) = \pi \hat{B}(\xi). \tag{5}$$

Also, in $\mathcal{A}(n)$ the following relation holds:

$$\pi G(\xi) = \pi A(\xi)[B(\xi) + \pi] = \pi A(\xi)B(\xi) = \pi \hat{C}(\xi). \tag{6}$$

Thus, from relations (5) and (6) it follows that $\pi\hat{B}(\xi)$ and $\pi\hat{C}(\xi)$ belong to J. Furthermore, since

$$\pi U(\xi)A(\xi)C(\xi) + \pi V(\xi)A(\xi)B(\xi) = \pi A(\xi), \tag{7}$$

i.e., $\pi U(\xi)\hat{B}(\xi) + \pi V(\xi)\hat{C}(\xi) = \pi A(\xi)$, then $\pi A(\xi) \in J$. Since $A(\xi)B(\xi) = G(\xi) - \pi A(\xi)$, then $A(\xi)B(\xi) = \hat{C}(\xi) \in J$. Therefore, $\hat{C}(\xi) + \pi\hat{B}(\xi) \in J$ showing that $I \subseteq J$. Hence $I = J$ proving that I is generated by $G(\xi)$. □

If the generator polynomial $G(\xi)$ of the $\mathcal{R}$-linear cyclic code $\mathcal{C}$ is as in the previous Theorem, the following cases can be considered:

i) If $C(\xi) = 1$ then $G(\xi) = \pi A(\xi)$.

ii) If $A(\xi) = 1$ then $G(\xi) = B(\xi) + \pi$.

As it was pointed out in the Introduction, describing the Gray image of codes over a finite chain ring is in general a non-trivial question to answer, even for the case where the ring has nilpotency index 2. As an attempt to provide a solution to this question, in the following lines the Gray image of the linear cyclic code whose generating polynomial is as in *i*) of the above mentioned cases will be described. Case *ii*) as well as other cases require further investigation.

Theorem 9. *With the notation as above let $n > 1$ be an integer relatively prime to the characteristic of the residue field $\mathbb{F}_q$ of $\mathcal{R}$ and let $\mathcal{C}$ be a $\mathcal{R}$-linear cyclic code of length n. If $G(\xi) = \pi A(\xi)$ and $\mathcal{C} = \langle G(\xi)\rangle$ then $\Phi_{\mathcal{P}}(G(\xi)) = a(\xi)(\xi^n - 1)^{p^m - 1}$ where $a(\xi) = \mu(A(\xi))$ and $\Phi_{\mathcal{P}}(G(\xi))$ divides $\xi^{np^m} - 1$. Moreover, the Gray image, $\Phi(\mathcal{C})$, of $\mathcal{C}$ is a linear cyclic code over $\mathbb{F}_q$ of length qn.*

Proof. Applying Lemma 7 to the generator polynomial $G(\xi)$ of the code $\mathcal{C}$, it follows that,

$$\Phi_{\mathcal{P}}(G(\xi)) = a(\xi)(\xi^n - 1)^{p^m - 1}.$$

Furthermore, since $A(\xi)$ divides $\xi^n - 1$ in $\mathcal{R}[\xi]$ then $a(\xi)$ divides $(\xi^n - 1)$ in $\mathbb{F}_q[\xi]$ and, therefore, $\xi^n - 1 = a(\xi)q(\xi)$ for some $q(\xi) \in \mathbb{F}_q[\xi]$. As $\xi^{p^m n} - 1 = (\xi^n - 1)(\xi^n - 1)^{p^m - 1} = a(\xi))q(\xi)(\xi^n - 1)^{p^m - 1}$, i.e., $\xi^{p^m n} - 1 = \Phi_{\mathcal{P}}(G(\xi))q(\xi)$, it follows that $\Phi_{\mathcal{P}}(G(\xi))$ divides $\xi^{p^m n} - 1$ in $\mathbb{F}_q[\xi]$. In consequence, the polynomial $\Phi_{\mathcal{P}}(G(\xi))$ generates a $\mathbb{F}_q$-linear cyclic code of length np^m.

Furthermore,

$$\Phi_{\mathcal{P}}(UG(\xi)) \in \langle \Phi_{\mathcal{P}}(G(\xi)) \rangle$$

for each $U(\xi) \in \mathcal{R}[\xi]/(\xi^n - 1)$.

Let $U(\xi) \in \mathcal{R}[\xi]/(\xi^n - 1)$. Then $U(\xi)G(\xi) = \pi U(\xi)A(\xi) = \pi H(\xi)$ where $H(\xi) = U(\xi)A(\xi)$. Again, from Lemma 7 applied to the polynomial $\hat{U}(\xi)\hat{G}(\xi)$ we have,

$$\Phi_{\mathcal{P}}(UG(\xi)) = \Phi_P(\pi H)(\xi) = h(\xi)(\xi^n - 1)^{p^m - 1} =$$
$$u(\xi)a(\xi)(\xi^n - 1)^{p^m - 1} = u(\xi)\Phi_{\mathcal{P}}(G(\xi)),$$

i.e., $\Phi_{\mathcal{P}}(UG(\xi)) = u(\xi)\Phi_{\mathcal{P}}(G(\xi))$. Therefore,

$$\Phi_{\mathcal{P}}(UG(\xi)) \in \langle \Phi_P(G(\xi)) \rangle.$$

and in consequence,

$$\Phi_P(\langle G(\xi) \rangle) \subseteq \langle \Phi_{\mathcal{P}}(G(\xi)) \rangle.$$

Let $deg(A(\xi)) = r$. Then since $C(\xi) = 1$, $deg(B(\xi)) = n - r$ and $|\mathcal{C}| = |\mathbb{F}|^{2deg(C(\xi))+1deg(B(\xi))} = (p^m)^{n-r}$ (cf. [1]). On the other hand,

$$\begin{aligned} |\langle \Phi_{\mathcal{P}}(G(\xi)) \rangle| &= (p^m)^{p^m n - deg(\Phi_P(G_(\xi))} = (p^m)^{p^m n - (n(p^m - 1) + r)} \\ &= (p^m)^{n-r}, \end{aligned}$$

and we conclude that $\Phi(\mathcal{C})$ is a $[qn, n - r]$-linear cyclic code over $\mathbb{F}_q$, proving the claim of the Theorem. □

References

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

[2] M. Greferath, S.E. Schmidt, Gray isometries for finite chain rings and a nonlinear ternary $(36, 3^{12}, 15)$ Code, *IEEE Trans. Inform. Theory*, **45** (1999), 2522-2524.

[3] A.R. Hammons Jr., P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, P. Solé, The $\mathbb{Z}_4$-linearity of kerdock, preparata, goethals, and related codes, *IEEE Trans. Inform. Theory*, **40** (1994), 301-319.

[4] T. Honold, A.A. Nechaev, Weighted modules and representations of codes, *Problems Inform. Transmission*, **35**, No. 3 (1999), 205-223.

[5] S. Ling, J.T. Blackford, $\mathbb{Z}_{p^{k+1}}$-linear codes, *IEEE Trans. Inform. Theory*, **48**, No. 9 (2002), 2592–2605.

[6] C.A. López-Andrade, H. Tapia-Recillas, On the quasi-cyclicity of the gray map image of a class of codes over Galois rings, In: *ICMCTA '08: Proceedings of the 2nd International Castle Meeting on Coding Theory and Applications*, LNCS **5228**, Springer-Verlag (2008), 107-116.

[7] C.A. López-Andrade, H. Tapia-Recillas, On the linearity and quasi-cyclicity of the gray image of codes over a galois ring, In: *Groups, Algebras and Applications*, Contemporary Mathematics, **537**, AMS (2011), 255-268.

[8] B.R. McDonald, *Finite Rings with Identity*, Pure and Applied Mathematics, **28**, Marcel Dekker, New York (1974).

[9] G. Norton, A. Salagean-Mandache, On the structure of linear cyclic codes over finite chain rings, *AAECC*, **10**, No. 6 (2000), 489-506.

[10] H. Tapia-Recillas, G. Vega, On the $\mathbb{Z}_{2^k}$-linear and quaternary codes, *SIAM Journal on Discrete Mathematics*, **17**, No. 1 (2003), 103-113.

[11] P. Udaya, M.U. Siddiqi, Optimal large linear complexity frequency Hopping patterns derived from polynomial residue class rings, *IEEE Trans. Inform. Theory*, **44** (1998), 1492–1503.

[12] J. Wolfmann, Binary images of cyclic codes over $\mathbb{Z}_4$, *IEEE, Trans. Inform. Theory*, **47** (2001), 1773-1779.