Journal of Algebra and Related Topics
Vol. 6, No 2, (2018), pp 63-78

BASIS OF A MULTICYCLIC CODE AS AN IDEAL IN $\mathbb{F}_q[X_1, \ldots, X_s]/\langle X_1^{\rho_1} - 1, \ldots, X_s^{\rho_s} - 1\rangle$

R. M. LALASOA, R. ANDRIAMIFIDISOA*, AND T. J. RABEHERIMANANA

Abstract. First, we apply the method presented by Zahra Sepasdar in the two-dimensional case to construct a basis of a three dimensional cyclic code. We then generalize this construction to a general s-dimensional cyclic code.

1. Introduction

Multicyclic codes are cyclic codes of dimension s, or s-D cyclic codes, where $s \geqslant 2$ is an integer. Two-dimensional cyclic codes have been intensively studied ([2, 3, 7, 8, 9, 10, 11]). There are much less results about general s-D cyclic codes, where $s \geqslant 3$. Because of their rich mathematical structure, as in [6], involving Algebraic Geometry or in [5, 9, 10, 11], using group algebra and Galois Theory or ideals in a polynomial quotient ring, multicyclic codes are of great importance.

A fundamental problem in coding theory is the construction of a generator matrix, which allows to find parameters of the code and to encode messages. The representation of a 2-D cyclic code as an ideal in a polynomial quotient ring makes the construction of a generator matrix possible, since it can be deducted from a basis of the ideal ([9, 10, 11]).

MSC(2010): primary: 13F20, 16D25; Secondary: 94B60
Keywords: quotient ring, ideal, ideal basis, multicyclic code, polynomial division algorithm (by many divisors).
Received: 1 August 2018, Accepted: 3 December 2018.
∗ Corresponding author .

Sepasdar, in [9, 11] presented a method which allowed to construct an ideal basis of a 2-D cyclic code, which is represented as an ideal in a two-variables polynomial quotient ring. Her method is based on an "elimination principle", and the fact that the coefficients of two-variate polynomials in the ideals are also polynomials in one variable, which belongs to principal ideals, and therefore, already have a "generator polynomial". From these generator polynomials, one then can construct a basis of the code, as a vector space.

In the present paper, we apply Sepasdar's method first to the 3-D case and then to the general s-D case ($s \geqslant 2$). It is organized as follows :

In Section 2, we give a brief description of multicyclic codes, as ideals in a polynomial quotient ring. Then we describe the structure of these polynomial quotient rings. Finally, we describe an auxiliary polynomial quotient ring which will allow us to apply Sepasdar's method to higher-dimensional cases

In Section 3, we first describe 2-D cyclic codes while applying what we saw in Section 2 to the 2-D case. We also present Sepasdar's result.

In Section 4, we state and prove our main Theorem 4.1. This give the construction of a basis of a 3-D code, as an ideal in a three-variables polynomial quotient ring. We prove it by using Sepasdar's method with ideals in two variables, a modification of the method and more calculation to the 3-D case.

In the last Section 5, we state and prove Theorem 5.1, which is the generalization of Theorem 4.1 to the s-D case, by induction.

2. Multicyclic codes

Throughout this paper, $\mathbb{F}_q$ denotes the Galois Field with q elements (where q is a power of a prime number). Let $s \geqslant 2$ be an integer, $X_1, \ldots, X_s$ distinct letters (or variables) and $\rho_1, \ldots, \rho_s \geqslant 1$ integers. Let $\mathbb{F}_q[X_1, \ldots, X_s]$ the ring of the polynomials in the variables $X_1, \ldots, X_s$ with coefficients in $\mathbb{F}_q$. An element of this ring is of the form

$$d(X_1, \ldots, X_s) = \sum_{(\alpha_1, \ldots, \alpha_s) \in \mathbb{N}^s} d_{\alpha_1, \ldots, \alpha_s} X_1^{\alpha_1} \cdots X_s^{\alpha_s} \tag{2.1}$$

where $d_{\alpha_1,\ldots,\alpha_s} \in \mathbb{F}_q$, the sum being finite.

A *multicyclic code*, or more precisely, an *s-dimensional cyclic code* (s-D multicyclic code), is an ideal I in the quotient ring (and also an $\mathbb{F}$-*algebra*)

$$R = \mathbb{F}_q[X_1, \ldots, X_s]/\langle X_1^{\rho_1} - 1, \ldots, X_s^{\rho_s} - 1\rangle. \tag{2.2}$$

For $\sigma = 1, \ldots, s$, let x_σ be the residue class of X_σ modulo the ideal $\langle X_1^{\rho_1} - 1, \ldots, X_s^{\rho_s} - 1\rangle$:

$$x_\sigma = X_\sigma + \langle X_1^{\rho_1} - 1, \ldots, X_s^{\rho_s} - 1\rangle. \tag{2.3}$$

We then have

$$x_\sigma^{\rho_\sigma} = 1. \tag{2.4}$$

We will need some supplementary notations :

• Let $\mathbb{Z}/\rho_\sigma\mathbb{Z} = \{0, 1, \ldots, \rho_\sigma - 1\}$ be the set of the residue classes of the integers modulo ρ_σ. for $\sigma = 1, \ldots, s$. Now, construct the abelian groups

$$\begin{aligned} \mathcal{G}_s &= \mathbb{Z}/\rho_1\mathbb{Z} \times \ldots \times \mathbb{Z}/\rho_s\mathbb{Z}, \\ \mathcal{G}_{s-1} &= \mathbb{Z}/\rho_1\mathbb{Z} \times \ldots \times \mathbb{Z}/\rho_{s-1}\mathbb{Z}. \end{aligned} \tag{2.5}$$

• Let $\mathbb{F}_q[x_1, \ldots, x_s]$ be the set of polynomials in the variables $x_1, \ldots, x_s$. Using (2.4), we have

$$\begin{aligned} \mathbb{F}_q[x_1, \ldots, x_s] =\{ &\sum_{(\alpha_1,\ldots,\alpha_s)\in\mathcal{G}_s} r_{\alpha_1,\ldots,\alpha_s} x_1^{\alpha_1} \cdots x_s^{\alpha_s} \mid r_{\alpha_1,\ldots,\alpha_s} \in \mathbb{F}_q \\ &\text{for } (\alpha_1, \ldots, \alpha_s) \in \mathcal{G}_s\}. \end{aligned} \tag{2.6}$$

• In the same manner, we define

$$\begin{aligned} \mathbb{F}_q[x_1, \ldots, x_{s-1}] =\{ &\sum_{(\alpha_1,\ldots,\alpha_{s-1})\in\mathcal{G}_{s-1}} r_{\alpha_1,\ldots,\alpha_{s-1}} x_1^{\alpha_1} \cdots x_{s-1}^{\alpha_{s-1}} \mid r_{\alpha_1,\ldots,\alpha_{s-1}} \in \mathbb{F}_q \\ &\text{for } (\alpha_1, \ldots, \alpha_{s-1}) \in \mathcal{G}_{s-1}\}. \end{aligned} \tag{2.7}$$

Note that the set $\mathbb{F}_q[x_1, \ldots, x_s]$ (resp. $\mathbb{F}_q[x_1, \ldots, X_{s-1}]$) is finite and has cardinality $q^{\rho_1\cdots\rho_s}$ (resp. $q^{\rho_1\cdots\rho_{s-1}}$) since it can be identified with the set of mappings from $\mathcal{G}_s$ (resp. $\mathcal{G}_{s-1}$) to $\mathbb{F}_q$.
• Let S be the quotient ring

$$S = \mathbb{F}_q[X_1, \ldots, X_{s-1}]/\langle X_1^{\rho_1} - 1, \ldots, X_{s-1}^{\rho_{s-1}} - 1\rangle. \tag{2.8}$$

The following proposition gives another representation of the ring R :

Proposition 2.1. *With the preceding notations, the rings* $R = \mathbb{F}_q[X_1, \dots, X_s]/\langle X_1^{\rho_1} - 1, \dots, X_s^{\rho_s} - 1\rangle$ *and* $\mathbb{F}_q[x_1, \dots, x_s]$ *are isomorphic.*

Proof. Let φ_s be the ring homomorphism defined by

$$\begin{aligned} \varphi_s : \mathbb{F}_q[X_1, \dots, X_s] &\longrightarrow \mathbb{F}_q[x_1, \dots, x_s] \\ X_i &\longmapsto x_i \end{aligned} \tag{2.9}$$

for $i = 1, \dots, s$. Let $d(X_1, \dots, X_s) \in \mathbb{F}_q[X_1, \dots, X_r]$ as in (2.1). Using (2.4), we then have

$$\varphi_s(d(X_1, \dots, X_s)) = \sum_{(\alpha_1,\dots,\alpha_s)\in\mathbb{N}^s} d_{\alpha_1,\dots,\alpha_s} x_1^{\alpha_1 \mod \rho_1} \cdots x_s^{\alpha_s \mod \rho_s}$$

where "$\alpha_\sigma \mod \rho_\sigma$" designs the remainder of α_σ by the euclidean division of α_σ by ρ_σ, Moreover, φ_s is surjective and its kernel is the ideal $\langle X_1^{\rho_1} - 1, \dots, X_s^{\rho_s} - 1\rangle$. Therefore, by the first isomorphism theorem for rings ([4]), there is an isomorphism $\bar{\varphi}$ which makes the following diagram commutative :

$$\begin{tikzcd} \mathbb{F}_q[X_1, \dots, X_s] \arrow[r, "\varphi_s"] \arrow[d, "\pi_s"'] & \mathbb{F}_q[x_1, \dots, x_s] \\ \mathbb{F}_q[X_1, \dots, X_s]/\langle X_1^{\rho_1} - 1, \dots, X_s^{\rho_s} - 1\rangle \arrow[ur, dashed, "\bar{\varphi}_s"] & \end{tikzcd}$$

where π_s is the canonical surjection. This proves the proposition.

□

The following proposition gives another representation of the ring S:

Proposition 2.2. *With the preceding notations the rings* $S = \mathbb{F}_q[X_1, \dots, X_{s-1}]/\langle X_1^{\rho_1} - 1, \dots, X_{s-1}^{\rho_{s-1}} - 1\rangle$ *and* $\mathbb{F}_q[x_1, \dots, x_{s-1}]$ *are isomorphic.*

Proof. We define the homomorphism ψ_s by

$$\begin{aligned} \psi_s : \mathbb{F}_q[X_1, \dots, X_{s-1}] &\longrightarrow \mathbb{F}_q[y_1, \dots, y_{s-1}] \\ X_i &\longmapsto y_i = X_i + \langle X_1^{\rho_1} - 1, \dots, X_{s-1}^{\rho_{s-1}} - 1\rangle \end{aligned} \tag{2.10}$$

(It is not the same as φ_{s-1} defined by (2.9). Here, y_i is the residue class of X_i modulo the ideal $\langle X_1^{\rho_1} - 1, \dots, X_{s-1}^{\rho_{s-1}} - 1\rangle$). Using the same arguments as for the mapping φ_s in (2.9), there exists an isomorphism

$\bar{\psi}_s$ which makes the following diagram commutative :

$$\begin{tikzcd}
\mathbb{F}_q[X_1,\dots,X_{s-1}] \arrow[r, "\psi_s"] \arrow[d, "\pi_{s-1}"'] & \mathbb{F}_q[y_1,\dots,y_{s-1}] \\
\mathbb{F}_q[X_1,\dots,X_{s-1}]/\langle X_1^{\rho_1}-1,\dots,X_{s-1}^{\rho_{s-1}}-1\rangle, \arrow[ur, dashed, "\bar{\psi}_s"] &
\end{tikzcd} \tag{2.11}$$

where π_{s-1} is the canonical projection. Now define the homomorphism θ by

$$\begin{aligned} \theta : \mathbb{F}_q[y_1,\dots,y_{s-1}] &\longrightarrow \mathbb{F}_q[x_1,\dots,x_{s-1}] \\ y_i &\longmapsto x_i. \end{aligned} \tag{2.12}$$

for $i = 1,\dots,s$. The mapping θ is obviously surjective and since its domain and codomain have the same cardinality (see the remark next to (2.7)), it follows that it is bijective, hence a ring isomorphism. Going back to the commutative diagram (2.11), we have that the mapping $\theta \circ \bar{\psi}_s$ is an isomorphism between S and $\mathbb{F}_q[x_1,\dots,x_s]$. □

From the propositions 2.1 and 2.2, we then can make the following identifications:

$$R = \mathbb{F}_q[X_1,\dots,X_s]/\langle X_1^{\rho_1}-1,\dots,X_s^{\rho_s}-1\rangle = \mathbb{F}[x_1,\dots,x_s]$$

and

$$S = \mathbb{F}_q[X_1,\dots,X_{s-1}]/\langle X_1^{\rho_1}-1,\dots,X_{s-1}^{\rho_{s-1}}-1\rangle = \mathbb{F}[x_1,\dots,x_{s-1}]. \tag{2.13}$$

We directly deduce the following corollary :

Corollary 2.3. *Using the notations in* (2.13), *we have*

$$R = \mathbb{F}_q[x_1,\dots,x_{s-1}][x_s] = S[x_s]. \tag{2.14}$$

Remark 2.4. For $d(X_1,\dots,X_s) \in \mathbb{F}_q[X_1,\dots,X_s]$, by the *division algorithm* ([1, 5]) of $d(X_1,\dots,X_s)$ by $X_\sigma^{\rho_\sigma}-1$, for $\sigma = 1,\dots s$, we can write

$$d(X_1,\dots,X_s) = \sum_{\sigma=1}^{s} q_\sigma(X_1,\dots,X_s)(X_\sigma^{\rho_\sigma}-1) + r(X_1,\dots,X_s), \tag{2.15}$$

with $q_\sigma, r \in \mathbb{F}_q[X_1,\dots,X_s]$ and r being of the form

$$r(X_1,\dots,X_s) = \sum_{(\alpha_1,\dots,\alpha_s)} r_{\alpha_1,\dots,\alpha_s} X_1^{\alpha_1}\cdots X_s^{\alpha_s} \tag{2.16}$$

where $\alpha_\sigma \leqslant \rho_\sigma - 1$ for $\sigma = 1,\dots s$. Therefore, a representative of the residue class of $d(X_1,\dots,X_s)$ modulo the ideal $\langle X_1^{\rho_1}-1,\dots,X_s^{\rho_s}-1\rangle$ is $r(X_1,\dots,X_s)$. Using this, we can find the result of Proposition 2.1 :

the class of $d(X_1, \dots, X_s)$ is the same of that of $r(X_1, \dots, X_s)$, which is

$$r(x_1, \dots, x_s) = \sum_{(\alpha_1,\dots,\alpha_s)\in\mathcal{G}_s} r_{\alpha_1,\dots,\alpha_s} x_1^{\alpha_1} \cdots x_s^{\alpha_s},$$

and immediately deduce that

$$R = \{ \sum_{(\alpha_1,\dots,\alpha_s)\in\mathcal{G}_s} r_{\alpha_1,\dots,\alpha_s} x_1^{\alpha_1} \cdots x_s^{\alpha_s} \mid r_{\alpha_1,\dots,\alpha_s} \in \mathbb{F}_q \} = \mathbb{F}_q[x_1, \dots, x_s].$$

Similar considerations also allow to show that $S = \mathbb{F}_q[x_1, \dots, x_{s-1}]$.

Using Corollary 2.14, an element $f(x_1, \dots, x_s) \in R$ can be uniquely written under the form

$$f(x_1, \dots, x_s) = \sum_{i=0}^{\rho_s - 1} f_i(x_1, \dots, x_{s-1}) x_s^i, \tag{2.17}$$

where $f_i(x_1, \dots, x_{s-1}) \in S$ for $i = 0, \dots, \rho_s - 1$.

3. Two dimensional cyclic codes

Let $l, n \geqslant 1$ be integers, X, Y two letters or variables, $\mathbb{F}_q[X, Y]$ the ring of polynomials in X, Y with coefficients in $\mathbb{F}_q$ and R the quotient ring

$$R = \mathbb{F}_q[X, Y]/\langle X^l - 1, Y^m - 1\rangle.$$

and S the quotient ring

$$S = \mathbb{F}_q[X]/\langle X^l - 1\rangle.$$

According to (2.3), let

$$x = X + \langle X^l - 1, Y^m - 1\rangle$$
$$y = Y + \langle X^l - 1, Y^m - 1\rangle$$

the residue classes of X and Y modulo the ideal $\langle X^l - 1, Y^m - 1\rangle$. A two dimensional (2-D) *cyclic code* is an Ideal I in R. Using (2.13), we can write

$$R = \mathbb{F}_q[x, y] = \{ \sum_{(\alpha,\beta)\in\mathcal{G}_2} d_{\alpha,\beta} x^\alpha y^\beta \mid d_{\alpha,\beta} \in \mathbb{F}_q \},$$

where $\mathcal{G}_2 = \mathbb{Z}/l\,\mathbb{Z} \times \mathbb{Z}/m\,\mathbb{Z}$ and

$$S = \mathbb{F}_q[x] = \{ \sum_{\alpha\in\mathbb{Z}/l\,\mathbb{Z}} c_\alpha x^\alpha \mid c_\alpha \in \mathbb{F}_q \}.$$

Here is Sepasdar's result :

Result 3.1 (Sepasdar, [9, 11])**.** *An ideal in $\mathbb{F}_q[X, Y]/\langle X^l - 1, Y^m - 1\rangle$, i.e. a two-dimensional cyclic code has a finite basis.*

If I is an ideal in $R = \mathbb{F}_q[X,Y]/\langle X^l - 1, Y^m - 1\rangle$, this result states that there exist elements $\mathfrak{p}_1(x,y), \ldots, \mathfrak{p}_k(x,y) \in R$ (where $k \geqslant 1$ is an integer) such that an element $c(x,y) \in I$ may be written as

$$c(x,y) = \sum_{i=1}^{k} u_i(x,y)\mathfrak{p}_i(x,y)$$

with $u_i(x,y) \in R$ for $i = 1, \ldots, k$.

4. Ideal basis of a three-dimensional cyclic code

Now, applying what we saw in Section 2 for $s = 3$, A 3-D cyclic code is then an Ideal I in $R = \mathbb{F}_q[X^l, Y^m, Z^n]/\langle X^l - 1, Y^m - 1, Z^n - 1\rangle$. By (2.8),

$$S = \mathbb{F}_q[X,Y]/(X^l - 1, Y^m - 1).$$

According to (2.3), let

$$\begin{aligned} x &= X + \langle X^l - 1, Y^m - 1, Z^n - 1\rangle, \\ y &= Y + \langle X^l - 1, Y^m - 1, Z^n - 1\rangle, \\ z &= Z + \langle X^l - 1, Y^m - 1, Z^n - 1\rangle \end{aligned}$$

the residue classes X, Y and Z modulo the ideal $\langle X^l - 1, Y^m - 1, Z^n - 1\rangle$. Using (2.13), we can write

$$\begin{aligned} R = \mathbb{F}_q[x,y,z] &= \{ \sum_{(\alpha,\beta,\gamma)\in\mathcal{G}_3} d_{\alpha,\beta,\gamma} x^\alpha y^\beta z^\gamma \mid d_{\alpha,\beta,\gamma} \in \mathbb{F}_q \}, \\ S = \mathbb{F}[x,y] &= \{ \sum_{(\alpha,\beta)\in\mathcal{G}_2} c_{\alpha,\beta} x^\alpha y^\beta \mid c_{\alpha,\beta} \in \mathbb{F}_q \}, \end{aligned}$$

where $\mathcal{G}_3 = \mathbb{Z}/l\,\mathbb{Z} \times \mathbb{Z}/m\,\mathbb{Z} \times \mathbb{Z}/n\,\mathbb{Z}$ and $\mathcal{G}_2 = \mathbb{Z}/l\,\mathbb{Z} \times \mathbb{Z}/m\,\mathbb{Z}$. By (2.17), an element $f(x,y,z) \in R$ can be uniquely written under the form

$$f(x,y,z) = \sum_{i=0}^{n-1} f_i(x,y) z^i \tag{4.1}$$

where $f_i(x,y) \in S$ for $i = 0, \ldots, n-1$.
Using the equality $z^n = 1$, we have

$$\begin{aligned} zf(x,y,z) &= f_{n-1}(x,y) + f_0(x,y)z + \cdots + f_{n-2}(x,y)z^{n-1}, \\ z^2 f(x,y,z) &= f_{n-2}(x,y) + f_{n-1}(x,y)z + \cdots + f_{n-3}(x,y)z^{n-1}, \\ &\vdots \\ z^{n-1} f(x,y,z) &= f_1(x,y) + f_2(x,y)z + \cdots f_0(x,y)z^{n-1}. \end{aligned} \tag{4.2}$$

The main task in this section is to prove our main theorem:

Theorem 4.1. *Using the preceding notations, let I be an ideal of $R = \mathbb{F}_q[X^l, Y^m, Z^n]/\langle X^l - 1, Y^m - 1, Z^n - 1\rangle$. For $j = 0, \ldots, n-1$, let I_j be the following set*

$$I_j = \{g_j(x,y) \in S \mid \exists g(x,y,z) \in I \text{ with } g(x,y,z) = \sum_{i=j}^{n-1} g_i(x,y)z^i \text{ where } g_i \in S \text{ for } i = j, \ldots, n-1\}. \tag{4.3}$$

Then the following hold:
(1) *The I_j's are ideals of S, generated by elements $p_1^{(j)}, \ldots, p_{r_j}^{(j)} \in S$, i.e.*

$$I_j = \langle p_1^{(j)}, p_2^{(j)}, \ldots, p_{r_j}^{(j)}\rangle = \{\sum_{\mu=1}^{r_j} p_\mu^{(j)}(x,y)q_\mu(x,y) \mid q_\mu \in S\}.$$

(2) *There exist elements $\mathfrak{p}_1^{(j)}(x,y,z), \ldots, \mathfrak{p}_{r_{n-1}}^{(j)}(x,y,z) \in I$, such that*

$$\mathfrak{p}_\mu^{(j)}(x,y,z) = \sum_{i=j}^{n-1} p_{i\mu}^{(j)}(x,y)z^i, \tag{4.4}$$

for $j = 0, \ldots, n-1, i = j, \ldots, n-1$, where $p_{i\mu}^{(j)}(x,y) \in S$, with $p_{j\mu}^{(j)}(x,y) = p_\mu^{(j)}(x,y)$ for $\mu = 1, \ldots, r_i$.
(3) *The elements $\mathfrak{p}_1^{(j)}, \ldots, \mathfrak{p}_{r_j}^{(j)}$, $j = 1, \ldots, n-1$ generate I, i.e.*

$$I = \langle \mathfrak{p}_1^{(0)}, \ldots, \mathfrak{p}_{r_1}^{(0)}, \mathfrak{p}_1^{(1)}, \ldots, \mathfrak{p}_{r_1}^{(1)}, \ldots, \mathfrak{p}_1^{(j)}, \ldots, \mathfrak{p}_{r_j}^{(j)}, \ldots, \mathfrak{p}_1^{(n-1)}, \ldots, \mathfrak{p}_{r_{n-1}}^{(n-1)}\rangle.$$

Proof. We see that that all the I_j's are non-empty since they contains the zero polynomial.

(1) Fix an element $j \in \{0, \ldots, n-1\}$. If $g_0(x,y) \in I_j$, there exists $g(x,y,z) \in I$ such that

$$g(x,y,z) = \sum_{i=j}^{n-1} g_j(x,y)z^i.$$

First, we have $xg_0(x,y), yg_0(x,y) \in I_j$ since I is an ideal of R and

$$xg(x,y,z) = \sum_{i=j}^{n-1} xg_i(x,y)z^i, yg(x,y,z) = \sum_{i=j}^{n-1} yg_i(x,y)z^i$$

are elements of I. Second, for $g(x,y,z)$ and $g'(x,y,z) \in I$, we have $g(x,y,z) + g'(x,y,z) \in I$ since I is an ideal. Thus, with obvious notations, $g_0(x,y) + g_0'(x,y) \in I_j$, for $g_0(x,y)$ and $g_0'(x,y) \in I_j$ and, I_j is indeed an ideal of $S = \mathbb{F}_q[X,Y]/(X^l - 1, Y^m - 1)$. By Result 3.1, it has a basis $\{p_1^{(j)}, p_2^{(j)}, \dots, p_{r_j}^{(j)}\}$ (where $r_j \in \mathbb{N}^*$), as stated in the theorem.

The ideal I_0 will be of special interest:

$$I_0 = \{g_0(x,y) \in S \mid \exists g(x,y,z) \in I \text{ with } g(x,y,z) = \sum_{i=0}^{n-1} g_i(x,y) z^i \text{ where } g_i \in S \text{ for } i = 0, \dots, n-1\}. \tag{4.5}$$

By (4.2), it follows that

$$z^i f(x,y,z) \in I_0, \tag{4.6}$$

which yields that $f_i(x,y) \in I_0$ for $i = 0, \dots, n-1$.

(2) The assertion results from the fact that $p_\mu^{(j)}(x,y)$ is an element of S for $j = 0, \dots, n-1$ and $\mu = 1, \dots, r_i$ and the definition of I_j in (5.2).

By (4.2) and (4.6), where we replace f by $\mathfrak{p}^{(j)}$, we have, by appropriate choices of k, $z^k \mathfrak{p}_\mu^{(j)}(x,y,z) \in I$, which implies that $p_{i\mu}^{(j)} \in I_0$ for $i = 0, \dots, n-1$. This latter being generated by $p_1^{(0)}, \dots, \dots, p_{r_0}^{(0)}$, there exist $t_{i\mu\nu}^{(j)}(x,y) \in S$ such that

$$p_{i\mu}^{(j)}(x,y) = \sum_{\nu=1}^{r_0} p_\nu^{(0)}(x,y) t_{i\mu\nu}^{(j)}(x,y) \tag{4.7}$$

for $j = 0, \dots, n-1$ and $\mu = 1, \dots, r_i$. Using (5.3) and (4.7), we then have

$$\mathfrak{p}_\mu^{(j)}(x,y,z) = \sum_{i=j}^{n-1} \sum_{\nu=1}^{r_0} p_\nu^{(0)}(x,y) t_{i\mu\nu}^{(j)}(x,y) z^i. \tag{4.8}$$

Now, consider an element $f(x,y,z) \in I$ of the form (4.1). Since $f_0(x,y) \in I_0$, there exist $q_\mu^{(0)}(x,y) \in S$, $\mu = 1, \dots, r_0$ such that

$$f_0(x,y) = \sum_{\mu=1}^{r_0} p_\mu^{(0)}(x,y) q_\mu^{(0)}(x,y). \tag{4.9}$$

Using (4.7) for $j = 0$ and the fact that $p_{0\mu}^{(0)}(x,y) = p_\mu^{(0)}(x,y)$, from (2), Theorem 4.1, it follows that

$$f_0(x,y) = \sum_{\mu=1}^{r_0} \sum_{\nu=1}^{r_0} p_\nu^{(0)}(x,y) t_{0\mu\nu}^{(0)}(x,y) q_\mu^{(0)}(x,y). \tag{4.10}$$

Put

$$h_1(x,y,z) = f(x,y,z) - \sum_{\mu=1}^{r_0} \mathfrak{p}_\mu^{(0)}(x,y,z) q_\mu^{(0)}(x,y). \tag{4.11}$$

We have

$$\begin{aligned}
h_1(x,y,z) &= \sum_{i=0}^{n-1} f_i(x,y)z^i - \sum_{i=0}^{n-1}\sum_{\mu=1}^{r_0}\sum_{\nu=1}^{r_0} p_\nu^{(0)}(x,y) t_{i\mu\nu}^{(0)}(x,y) q_\mu^{(0)}(x,y) z^i \\
&\quad \text{(by (4.8) for } j=0\text{)}, \\
&= (f_0(x,y) + \sum_{i=1}^{n-1} f_i(x,y)z^i) - \sum_{i=1}^{n-1}\sum_{\mu=0}^{r_0}\sum_{\nu=1}^{r_0} (p_\nu^{(0)}(x,y) t_{i\mu\nu}^{(0)}(x,y) q_\mu^{(0)}(x,y) z^i, \\
&= (f_0(x,y) - \sum_{\mu=1}^{r_0}\sum_{\nu=1}^{r_0} p_\nu^{(0)}(x,y) t_{0\mu\nu}^{(0)}(x,y) q_\mu^{(0)}(x,y)) + \sum_{i=1}^{n-1} f_i(x,y)z^i \\
&\quad - \sum_{i=1}^{n-1}(\sum_{\mu=1}^{r_0}\sum_{\nu=1}^{r_0} p_{i\mu}^{(0)}(x,y) t_{i\mu\nu}^{(0)}(x,y) q_\mu^{(0)}(x,y)) z^i, \\
&= \sum_{i=1}^{n-1} f_i(x,y)z^i - \sum_{i=1}^{n-1}(\sum_{\mu=1}^{r_0} p_\mu^{(0)}(x,y) q_\mu^{(0)}(x,y)) z^i \\
&\quad \text{(by (4.10) and (4.7) for } j=0\text{)}.
\end{aligned} \tag{4.12}$$

Since f and $\mathfrak{p}_\mu^{(0)}$ are elements of I which is an ideal of R, the polynomial h_1 is also an element of I. We remark that

$$h_1(x,y,z) = \sum_{i=1}^{n-1} h_i^{(1)}(x,y) z^i$$

where $h_i^{(1)} \in S$ for $i = 1, \dots, n-1$. In other words, $h_1^{(1)}(x,y) \in I_1$. Therefore, there exists $q_\mu^{(1)} \in S$, $\mu = 1, \dots, r_1$ such that

$$h_1^{(1)}(x,y) = \sum_{\mu=1}^{r_1} p_\mu^{(1)}(x,y) q_\mu^{(1)}(x,y).$$

Using (4.7), for $j = 1$, and the fact that $p_{1\mu}^{(1)}(x,y) = p_\mu^{(1)}(x,y)$, from (2), Theorem 4.1, it follows that

$$h_1^{(1)}(x,y) = \sum_{\mu=1}^{r_1}\sum_{\nu=1}^{r_0} p_\nu^{(0)}(x,y) t_{i\mu\nu}^{(1)}(x,y) q_\mu^{(1)}(x,y). \tag{4.13}$$

Put

$$h_2(x,y,z) = h_1(x,y,z) - \sum_{\mu=1}^{r_1} \mathfrak{p}_\mu^{(1)}(x,y,z) q_{1\mu}^{(1)}(x,y). \tag{4.14}$$

We have

$$\begin{aligned}
h_2(x,y,z) &= \sum_{i=1}^{n-1} h_1(x,y,z)z^i - \sum_{\mu=1}^{r_1}\sum_{\nu=1}^{r_0}\sum_{i=1}^{n-1} p_\nu^{(0)}(x,y)t_{i\mu\nu}^{(1)}(x,y)q_{1\mu}^{(1)}(x,y)z^i \\
&\quad \text{(by (4.8) for } j=1), \\
&= (h_1^{(1)}(x,y)z + \sum_{i=2}^{n-1} h_i^1(x,y)z^i - \sum_{\mu=1}^{r_1}\sum_{\nu=1}^{r_0}(p_\nu^{(0)}(x,y)t_{1\mu\nu}^{(1)}(x,y)q_{1\mu}^{(1)}(x,y))z \\
&\quad - \sum_{i=1}^{n-1}(\sum_{\mu=1}^{r_1}\sum_{\nu=1}^{r_0} p_\nu^{(0)}(x,y)t_{i\mu\nu}^{(1)}(x,y)q_{1\mu}^{(1)}(x,y))z^i \\
&= \sum_{i=2}^{n-1} h_i^{(1)}(x,y)z^i - \sum_{i=1}^{n-1}\sum_{\mu=1}^{r_1}\sum_{\nu=1}^{r_0} p_\nu^{(0)}(x,y)t_{i\mu\nu}^{(1)}(x,y)q_\mu^{(1)}(x,y)z^i \\
&= \sum_{i=2}^{n-1} h_i^1(x,y)z^i - \sum_{i=1}^{n-1}\sum_{\mu=1}^{r_1} p_{i\mu}^{(0)}(x,y)q_{1\mu}^{(1)}(x,y))z^i \\
&\quad \text{(by (4.13) and (4.7) for } j=1).
\end{aligned} \tag{4.15}$$

(3) Since $h_1(x,y,z)$ and $\mathfrak{p}_\mu^{(1)}(x,y,z)$ are elements of I which is an ideal of R, the polynomial $h_2(x,y,z)$ is also in I and can be written in the form

$$h_2(x,y,z) = \sum_{i=2}^{n-1} h_i^{(2)}(x,y)z^i$$

where $h_i^{(2)}(x,y) \in S$. In other words, $h_2(x,y,z) \in I_2$. Therefore there exist $q_\mu^{(2)}(x,y) \in S, \mu = 1,\ldots,r_2$ such that

$$h_2^{(2)}(x,y) = \sum_{\mu=1}^{r_2} p_\mu^{(2)}(x,y)q_\mu^{(2)}(x,y). \tag{4.16}$$

Using (4.7), for $j=2$, and the fact that $p_{2\mu}^{(2)}(x,y) = p_\mu^{(2)}(x,y)$, from (2), Theorem 4.1, it follows that

$$h_2^{(2)}(x,y) = \sum_{\mu=1}^{r_2}\sum_{\nu=1}^{r_0} p_\nu^{(0)}(x,y)t_{i\mu\nu}^{(2)}(x,y)q_\mu^{(2)}(x,y). \tag{4.17}$$

Put

$$h_3(x,y,z) = h_2(x,y,z) - \sum_{\mu=1}^{r_2} \mathfrak{p}_\mu^{(2)}(x,y,z) q_\mu^{(2)}(x,y). \tag{4.18}$$

We then have

$$\begin{aligned}
&= \sum_{i=2}^{n-1} h_i^{(2)}(x,y,z)z^i - \sum_{\mu=1}^{r_2}\sum_{i=2}^{n-1}\sum_{\nu=1}^{r_0} p_\nu^{(0)}(x,y)t_{i\mu\nu}^{(2)}(x,y)q_\mu^{(2)}(x,y)z^i \\
&\text{(by (4.8) for } j=2\text{)}, \\
&= (h_2^{(2)}(x,y)y)z^2 + \sum_{i=3}^{n-1} h_i^2(x,y)z^i - \sum_{\mu=1}^{r_2}\sum_{\nu=1}^{r_0}(p_\nu^{(0)}(x,y)t_{2\mu\nu}^{(2)}q_\mu^{(2)}(x,y))z^2 \\
&- \sum_{\mu=1}^{r_2}(\sum_{i=3}^{n-1}\sum_{\nu=1}^{r_0} p_\nu^{(0)}(x,y)t_{i\mu\nu}^{(2)}(x,y)q_{1\mu}^{(2)}(x,y))z^i \\
&= \sum_{i=3}^{n-1} h_i^{(2)}(x,y)z^i - \sum_{i=3}^{n-1}\sum_{\mu=1}^{r_2}\sum_{\nu=1}^{r_0} p_\nu^{(0)}(x,y)t_{i\mu\nu}^{(2)}(x,y)q_\mu^{(2)}(x,y)z^i \\
&= \sum_{i=3}^{n-1} h_i^{(2)}(x,y)z^i - \sum_{i=3}^{n-1}\sum_{\mu=1}^{r_2} p_{i\mu}^{(2)}(x,y)q_\mu^{(2)}(x,y)z^i \\
&\text{(by (4.17) and (4.7) for } j=2\text{)}.
\end{aligned} \tag{4.19}$$

Since $h_2(x,y,z)$ and $\mathfrak{p}_\mu^{(2)}(x,y,z)$ are elements of I which is an ideal of R, the polynomial $h_3(x,y,z)$ is also in I and can be written in the form

$$h_3(x,y,z) = \sum_{i=3}^{n-1} h_i^{(3)}(x,y)z^i, \tag{4.20}$$

with $h_i^{(3)}(x,y) \in S$.

Applying the preceding methods, we get polynomials

$$\begin{aligned}
&h_4(x,y,z), \ldots, h_{n-2}(x,y,z), \\
&q_\mu^{(3)}(x,y,z)_{1\leqslant\mu\leqslant r_3}, \ldots, q_\mu^{(n-2)}(x,y,z)_{1\leqslant\mu\leqslant r_{n-2}}
\end{aligned}$$

of S. Finally, put

$$h_{n-1}(x,y,z) = h_{n-2}(x,y,z) - \sum_{\mu=1}^{r_{n-1}} \mathfrak{p}_\mu^{(n-2)}(x,y,z)q_\mu^{(n-2)}(x,y). \tag{4.21}$$

Then $h_{n-1}(x,y,z)$ is a polynomial of I of the form $h_{n-1}^{n-1}(x,y)z^{n-1}$. In other words, $h_{n-1}^{(n-1)}(x,y) \in I_{n-1}$. Therefore, there exist $q_\mu^{(n-1)}(x,y) \in S$, $\mu = 1,\ldots,r_{n-1}$ such that

$$h_{n-1}^{(n-1)}(x,y) = \sum_{\mu=1}^{r_{n-1}} p_\mu^{(n-1)}(x,y) q_\mu^{(n-1)}(x,y), \tag{4.22}$$

which yields

$$\begin{aligned} h_{n-1}(x,y,z) &= (\sum_{\mu=0}^{r_{n-1}} p_\mu^{(n-1)}(x,y) q_\mu^{(n-1)}(x,y)) z^{n-1} \\ &= \sum_{\mu=0}^{r_{n-1}} \mathfrak{p}_\mu^{(n-1)}(x,y,z) q_\mu^{(n-1)}(x,y). \end{aligned}$$

For an arbitrary element $f(x,y,z) \in I$ we then have shown the following equalities :

$$\begin{aligned} h_1(x,y,z) &= f(x,y,z) - \sum_{\mu=1}^{r_0} \mathfrak{p}_\mu^{(0)}(x,y,z) q_\mu^{(0)}(x,y), \\ h_2(x,y,z) &= h_1(x,y,z) - \sum_{\mu=1}^{r_1} \mathfrak{p}_\mu^{(1)}(x,y,z) q_\mu^{(1)}(x,y), \\ h_3(x,y,z) &= h_2(x,y,z) - \sum_{\mu=1}^{r_1} \mathfrak{p}_\mu^{(2)}(x,y,z) q_\mu^{(2)}(x,y), \\ &\cdots \\ h_{n-1}(x,y,z) &= h_{n-2}(x,y,z) - \sum_{\mu=1}^{r_{n-2}} \mathfrak{p}_\mu^{(n-2)}(x,y,z) q_\mu^{(n-2)}(x,y), \\ &= \sum_{\mu=1}^{r_{n-1}} \mathfrak{p}_\mu^{(n-1)}(x,y,z) q_\mu^{(n-1)}(x,y) \end{aligned}$$

and finally have

$$
\begin{aligned}
f(x,y,z) &= \sum_{\mu=1}^{r_0} \mathfrak{p}_\mu^{(0)}(x,y,z) q_\mu^{(0)}(x,y) + h_1(x,y),\\
&= \sum_{\mu=1}^{r_0} \mathfrak{p}_\mu^{(0)}(x,y,z) q_\mu^{(0)}(x,y) + \sum_{\mu=1}^{r_1} \mathfrak{p}_\mu^{(1)}(x,y,z) q_\mu^{(1)}(x,y) + h_2(x,y),\\
&= \cdots,\\
&= \sum_{\mu=1}^{r_0} \mathfrak{p}_\mu^{(0)}(x,y,z) q_\mu^{(0)}(x,y) + \cdots + \sum_{\mu=1}^{r_{n-1}} \mathfrak{p}_\mu^{(n-1)}(x,y,z) q_\mu^{(n-1)}(x,y),
\end{aligned}
$$

and conclude that

$$
I = \langle \mathfrak{p}_1^{(0)}, \ldots, \mathfrak{p}_{r_1}^{(0)}, \mathfrak{p}_1^{(1)}, \ldots, \mathfrak{p}_{r_1}^{(1)}, \ldots, \mathfrak{p}_1^{(i)}, \ldots, \mathfrak{p}_{r_i}^{(i)}, \ldots, \mathfrak{p}_1^{(n-1)}, \ldots, \mathfrak{p}_{r_{n-1}}^{(n-1)} \rangle.
$$

□

5. Basis for an s-dimensional cyclic code

Now, we generalize Theorem 4.1 for general s-D multicyclic codes ($s \geqslant 2$). Let

$$
R = \mathbb{F}_q[X_1, \ldots, X_s]/\langle X_1^{\rho_1} - 1, \ldots, X_s^{\rho_s} - 1 \rangle,
$$

as in (2.2) and S the quotient ring

$$
S = \mathbb{F}_q[X_1, \ldots, X_{s-1}]/\langle X_1^{\rho_1} - 1, \ldots, X_{s-1}^{\rho_{s-1}} - 1 \rangle.
$$

In section 2, by (2.13) and (2.14), we know that if x_i denotes the residue class of X_i modulo the ideal $\langle X_1^{\rho_1} - 1, \ldots, X_s^{\rho_s} - 1 \rangle$, then

$$
S = \mathbb{F}_q[x_1, \ldots, x_{s-1}], R = \mathbb{F}_q[x_1, \ldots, x_s] = S[x_s]. \tag{5.1}
$$

Theorem 5.1. *Let I be an ideal of the quotient ring $R = \mathbb{F}_q[X_1, \ldots, X_s]/\langle X_1^{\rho_1} - 1, \ldots, X_s^{\rho_s} - 1 \rangle$. For $j = 0, \ldots, \rho_s - 1$, let I_j be the following set*

$$
\begin{aligned}
I_j = \{ g_j(x_1, \ldots, x_{s-1}) \in S \mid & \exists g(x_1, \ldots, x_s) \in I \text{ with} \\
& g(x_1, \ldots, x_s) = \sum_{i=j}^{\rho_s - 1} g_i(x_1, \ldots, x_{s-1}) x_s^i \\
& \text{where } g_i \in S \text{ for } i = j, \ldots, \rho_s - 1 \}.
\end{aligned} \tag{5.2}
$$

Then the following hold:
(1) *The I_j's are ideals of S, generated by elements $p_1^{(j)}, \dots, p_{r_j}^{(j)} \in S$, i.e.*

$$I_j = \langle p_1^{(j)}, p_2^{(j)}, \dots, p_{r_j}^{(j)} \rangle = \{\sum_{\mu=1}^{r_j} p_\mu^{(j)}(x_1, \dots, x_{s-1}) q_\mu(x_1, \dots, x_{s-1}) \mid q_\mu \in S\}.$$

(2) *There exist elements $\mathfrak{p}_1^{(j)}(x_1, \dots, x_s), \dots, \mathfrak{p}_{r_{\rho_s-1}}^{(j)}(x_1, \dots, x_s) \in I$, such that*

$$\mathfrak{p}_\mu^{(j)}(x_1, \dots, x_s) = \sum_{i=j}^{\rho_s-1} p_{i\mu}^{(j)}(x_1, \dots, x_{s-1}) x_s^i, \tag{5.3}$$

for $j = 0, \dots, n-1, i = j, \dots, \rho_s - 1$, where $p_{i\mu}^{(j)}(x_1, \dots, x_{s-1}) \in S$, with $p_{j\mu}^{(j)}(x_1, \dots, x_{s-1}) = p_\mu^{(j)}(x_1, \dots, x_{s-1})$ for $\mu = 1, \dots, r_i$.
(3) *The elements $\mathfrak{p}_1^{(j)}, \dots, \mathfrak{p}_{r_j}^{(j)}$, $j = 1, \dots, \rho_s - 1$ generate I, i.e.*

$$I = \langle \mathfrak{p}_1^{(0)}, \dots, \mathfrak{p}_{r_1}^{(0)}, \mathfrak{p}_1^{(1)}, \dots, \mathfrak{p}_{r_1}^{(1)}, \dots, \mathfrak{p}_1^{(j)}, \dots, \mathfrak{p}_{r_j}^{(j)}, \dots, \mathfrak{p}_1^{(\rho_s-1)}, \dots, \mathfrak{p}_{r_{\rho_s-1}}^{(\rho_s-1)} \rangle.$$

Proof. We prove by induction on s: the case $s = 2$ was treated by Sepasdar and the case $s = 3$ in Section 4. Now, suppose the theorem is true for $s - 1$, where $s \geqslant 4$. Let I be an s-dimensional ideal in the quotient ring $R = \mathbb{F}_q[X_1, \dots, X_s]/\langle X_1^{\rho_1} - 1, \dots, X_s^{\rho_s} - 1\rangle$. By (5.1), we have $R \cong S[x_s]$. Using the representation $S = \mathbb{F}_q[X_1, \dots, X_{s-1}]/\langle X_1^{\rho_1} - 1, \dots, X_{s-1}^{\rho_{s-1}} - 1\rangle$, by the induction hypothesis, each of the I_j's as in the theorem have a basis $\{p_\mu^{(j)}(x_1, \dots, x_{s-1})\}$, since they are ideals of S. As we have done in Section 4, there are also polynomials $\mathfrak{p}_\mu^{(j)}(x_1, \dots, x_s)$ whose set is a basis of I. Thus, the result is true for s and, therefore, by induction, for all $s \in \mathbb{N}^*$. □

Acknowledgments

The authors would like to thank the referee for careful reading.

References

1. D. Cox D, J. Little, D. O'Shea, *Ideals, Varieties and Algorithms*, Springer, Second Edition, 1997.
2. T. Ikai, H. Kosako, Y. Kojima, *Two-dimensional cyclic Codes*, Electronics and Communications in Japan, **57-A** (1975), 27-35.
3. H. Imai, *A theory of two-dimensional cyclic Codes*, Information and Control, **34** (1977), 1-21.
4. N. Jacobson, *Basic Algebra II (2nd ed.)*, Dover, New York, 2009.

5. R. M. Lalasoa, R. Andriamifidisoa and T. J. Rabeherimanana, *Multicyclic codes and algebraic dynamical Systems*, British Journal of Mathematics & Computer Science, (2) **21** (2017), 1-22.
6. K. Saints and C. Heegard, *Algebraic-geometric codes and multidimensional cyclic Codes : A unified Theory and Algorithms for decoding using Groebner Bases*, IEEE Trans. IT, (6) **41** (1995), 1733-1751 .
7. S. Sakata, *Decoding binary 2-D cyclic codes by the 2-D BerlekampMassey algorithm*, IEEE Trans. Inf. Theory IT, (4) **37** (1991), 12001203.
8. S. Sakata, *S. On determining the independent Point Set for doubly periodic Arrays and encoding two-dimensional cyclic Codes and their Duals*, IEEE Trans. Inf. Theory IT, (5) **27** (1981), 556565.
9. Z. Sepasdar, *Some notes on the characterization of two dimensional skew cyclic Codes*, J. Algebra Relat. Topics, (2) **4** (2016), 1-8.
10. Z. Sepasdar, *Characterizations of some two-dimensional cyclic Codes correspond to the Ideals of* $\mathbb{F}_q[x, y]/\langle x^s - 1, y^{2k} - 1\rangle$, Finite Fields Appl., **41** (2016), 97112.
11. Z. Sepasdar, *Generator Matrix for two-dimensional cyclic Codes of arbitrary Length*, arXiv:1704.08070v1, [math.AC], 26 Apr 2017.

Rufine Marius Lalasoa
Department of Mathematics and Computer Science, University of Antananarivo, p.O.Box 906, 101 Antananarivo, Madagascar.
Email: larissamarius.lm@gmail.com

Ramamonjy Andriamifidisoa
Department of Mathematics, University of Antananarivo, p.O.Box 906, 101 Antananarivo, Madagascar,
And
Higher Polytechnics Institute of Madagascar (ISPM), Ambatomaro Antsobolo, 101 Antananarivo, Madagascar.
Email: ramamonjy.andriamifidisoa@univ-antananarivo.mg

Toussaint Joseph Rabeherimanana
Department of Mathematics, University of Antananarivo, p.O.Box 906, 101 Antananarivo, Madagascar.
Email: rabeherimanana.toussaint@yahoo.fr