Journal of Algebra and Related Topics
Vol. 7, No 2, (2019), pp 63-83

FINDING A GENERATOR MATRIX OF A MULTIDIMENSIONAL CYCLIC CODE

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

ABSTRACT. We generalize Sepasdar's method for finding a generator matrix of two-dimensional cyclic codes to find a generating subset and a linearly independent subset of a general multicyclic code. From these sets, a basis of the code as a vector subspace can be deduced or constructed. A generator matrix can be then deduced from this basis.

1. INTRODUCTION

Sepasdar, in [4] presented a method to find a generator matrix of two dimensional skew cyclic Codes. Then, Sepasdar and Khashyarmanesh, in [5] gave a method to find a generator matrix of some class of two-dimensional cyclic codes. Finally, Sepasdar, in [6], found a method to construct a generator matrix for general two-dimensional cyclic codes. In this paper, we will generalize this Sepasdar's method for a general multicyclic code. Our method uses an ideal basis of the code whose construction was presented by Lalasoa et al. in [3].

In section 2 of this paper, we recall the notations used in [3] and the mathematical tools we will need, including two orderings : the partial ordering "$\leqslant_+$" and the well ordering "$\leqslant_{\text{lex}}$". This latter allows to define degrees of polynomials in the quotient ring with a special property,

MSC(2010): primary: 13F20, 16D25; Secondary: 94B60
Keywords: quotient ring, lexicographic order, ideal basis, multicyclic code, generator matrix
Received: 4 April 2019.
* Corresponding author .

given by Proposition 3.5.

In section 3, we present our results. Proposition 3.1 gives an idea of how a basis of the multicyclic code, considered as a vector space will look like. It also provides a generating set for the code. Corollary 3.2 gives a simple condition for this set to be a basis. The main result is Theorem 3.4, which allows the construction of an independent subset of the code. If this set is too small to be a generating set, we must add elements from the generating set found by Proposition 3.1. Once a basis is found, one can then construct a generator matrix by forming the matrix whose rows are the coefficients of the polynomials of the basis.

In the last section 4, we give examples for the 2-D and 3-D case..

In Appendix A, we state the method for constructing the examples of multicyclic codes and in Appendix B we present algorithms for finding ideal bases for these codes. Computations were done using the SageMath mathematical software system.

2. Notations and Preliminaries

We briefly recall the notations which are used in [3]. Let R be the quotient ring

$$R = \mathbb{F}_q[X_1, \ldots, X_s]/\langle X_1^{\rho_1} - 1, \ldots, X_s^{\rho_s} - 1\rangle = \mathbb{F}_q[x_1, \ldots, x_s] \tag{2.1}$$

where $\mathbb{F}_q$ is the finite field with q elements and x_i the residue class of X_i modulo the ideal $\langle X_1^{\rho_1} - 1, \ldots, X_s^{\rho_s} - 1\rangle$. We have

$$x_i^{\rho_i} = 1, \tag{2.2}$$

so that

$$x_i^m = x_i^{m \mod \rho_i} \quad \text{for} \quad m \in \mathbb{N} \quad \text{and} \quad i = 1, \ldots, s, \tag{2.3}$$

where $m \mod \rho_i$ is the remainder of m by the euclidean division of m by ρ_i.

The additive product group $\mathcal{G}_s$ is defined by

$$\mathcal{G}_s = \mathbb{Z}/\rho_1\mathbb{Z} \times \ldots \times \mathbb{Z}/\rho_s\mathbb{Z}, \tag{2.4}$$

with

$$\mathbb{Z}/\rho_i\mathbb{Z} = \{0, 1, \ldots, \rho_i - 1\}.$$

An element of $\mathbb{F}_q[x_1, \ldots, x_s]$ is of the form

$$f(x_1, \ldots, x_s) = \sum_{(\alpha_1, \ldots, \alpha_s) \in \mathcal{G}_s} f_{(\alpha_1, \ldots, \alpha_s)} x_1^{\alpha_1} \cdots x_s^{\alpha_s}. \tag{2.5}$$

For sake of simplicity, we denote $(\alpha_1, \ldots, \alpha_s) \in \mathcal{G}_s$ or, more generally, $(\alpha_1, \ldots, \alpha_s) \in \mathbb{N}^s$ by α. Then (2.5) can then be written as a

$$f(x) = \sum_{\alpha \in \mathcal{G}_s} f_\alpha x^\alpha, \tag{2.6}$$

where

$$x^\alpha = x_1^{\alpha_1} \cdots x_s^{\alpha_s}, \tag{2.7}$$

and we may omit the set $\mathcal{G}_s$. For $\alpha \in \mathbb{N}^s$, we also adopt the notation

$$\alpha \mod \rho = (\alpha_1 \mod \rho_1, \ldots, \alpha_s \mod \rho_s) \in \mathcal{G}_s,$$

where $\rho = (\rho_1, \ldots, \rho_s)$. Equations (2.2) and (2.3) are then "generalized" to the following:

$$x^\rho = 1 \quad \text{and} \quad x^\alpha = x^{\alpha \mod \rho}. \tag{2.8}$$

The set $\mathbb{N}^s$, and therefore also he product group $\mathcal{G}_s$ is provided with two orders : a partial ordering $\leqslant_+$ defined by

$$\alpha \leqslant_+ \beta \iff \alpha_i \leqslant \beta_i \quad \text{for} \quad i = 1, \ldots, s,$$

and a *well ordering* $\leqslant_{\text{lex}}$ (the "lexicographical ordering'), defined by

$$\alpha <_{\text{lex}} \beta \iff \text{for the first index } i \text{ such that } \alpha_i \neq \beta_i \text{, one has } \alpha_i < \beta_i.$$

Put $n = \rho_1 \cdots \rho_s$. We then may write $\mathcal{G}_s = \{\alpha^{(1)}, \ldots, \alpha^{(i)}, \ldots, \alpha^{(n)}\}$ with

$$\alpha^{(1)} <_{\text{lex}} \cdots \alpha^{(i)} <_{\text{lex}} \cdots <_{\text{lex}} \alpha^{(n)} \tag{2.9}$$

and the polynomial $f(x)$ in (2.6) can be written as

$$f(x) = f_{\alpha^{(1)}} x^{\alpha^{(1)}} + \cdots + f_{\alpha^{(i)}} x^{\alpha^{(1)}} + \cdots + f_{\alpha^{(\rho_s)}} x^{\alpha^{(n)}}. \tag{2.10}$$

If $f(x)$ is non-zero, we may define its *degree,* denoted $\deg f(x)$ or simply $\deg f$ as

$$\deg f = \max_{\leqslant_{\text{lex}}} \{\alpha^{(i)} \mid f_{\alpha^{(i)}} \neq 0\}. \tag{2.11}$$

(Note that it is the usual definition of the degree of a multivariate polynomial). However, due to equations (2.8), for two polynomials f and g of $\mathbb{F}_q[x_1, \ldots, x_s]$, the equality $\deg(fg) = \deg f + \deg g$ does not necessarily hold. The following proposition gives a sufficient condition for this property.

Proposition 2.1. *If f and g are non-zero elements of $\mathbb{F}_q[x_1, \ldots, x_s]$ such that $\deg f + \deg g <_+ \rho$, then $\deg(fg) = \deg f + \deg g$.*

Proof. Write $f(x_1,\dots,x_s)=\sum_\alpha f_\alpha x^\alpha$ and $g(x_1,\dots,x_s)=\sum_\beta g_\beta x^\beta$. Then, using the second equation of (2.8), we have

$$\begin{aligned} f(x_1,\dots,x_s)g(x_1,\dots,x_s) &= \sum_\alpha\sum_\beta f_\alpha g_\beta x^{(\alpha+\beta) \mod \rho} \\ &= \sum_\alpha\sum_\beta f_\alpha g_\beta x^{(\alpha+\beta)} \end{aligned}$$

since $\alpha+\beta \leqslant_+ \deg f + \deg g <_+ \rho = (\rho_1,\dots,\rho_s)$ for all α and β. Thus

$$\deg(fg) = \max_{\leqslant_{\text{lex}}}(\alpha+\beta) = \deg f + \deg g.$$

□

All the previous results are also true for the quotient ring

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

with $s-1$ variables, where x_i is the residue class of x_i modulo the ideal $\langle X_1^{\rho_1}-1,\dots,X_{s-1}^{\rho_{s-1}}-1\rangle$. Note that we have used the same notation x_i, because the residue class of x_i modulo the ideal $\langle X_1^{\rho_1}-1,\dots,X_{s-1}^{\rho_{s-1}}-1\rangle$ may be identified with its class modulo the ideal $\langle X_1^{\rho_1}-1,\dots,X_s^{\rho_s}-1\rangle$, (cf. Proposition 2.2, [3]).

A *multicyclic code* is an ideal of R (equation (2.1)).

Let I be a non-zero ideal of R and

$$\mathfrak{B} = \{\mathfrak{p}_1^{(0)},\dots,\mathfrak{p}_{r_1}^{(0)},\mathfrak{p}_1^{(1)},\dots,\mathfrak{p}_{r_1}^{(1)},\dots,\mathfrak{p}_1^{(i)},\dots,\mathfrak{p}_{r_i}^{(i)},\dots,\mathfrak{p}_1^{(\rho_s-1)},\dots,\mathfrak{p}_{r_{\rho_s-1}}^{(\rho_s-1)}\} \tag{2.12}$$

the basis of I, found by Lalasoa et al. by the method in [3], with $p_k \in I_k$. Then an element $f(x_1,\dots,x_s)\in R$ may be written as a finite sum

$$f(x_1,\dots,x_s) = \sum_{i=0}^{r_{\rho_s-1}}\sum_{j=1}^{r_j} q_j^{(i)}(x_1,\dots,x_{s-1})\mathfrak{p}_j^{(i)}(x_1,\dots,x_s). \tag{2.13}$$

Note that in (2.13), the coefficients of the polynomials in $\mathfrak{B}$ are polynomials in S.

3. Results

Our aim in this section is to construct a basis of I, as an $\mathbb{F}_q$-vector subspace of R (an $\mathbb{F}_q$-basis), from the ideal basis $\mathfrak{B}$ of I, in (2.12).

Proposition 3.1. *The set*

$$B' = \{x_1^{\alpha_1}\cdots x_{s-1}^{\alpha_{s-1}}\mathfrak{p} \mid (\alpha_1,\dots,\alpha_{s-1}) \leqslant_+ (\rho_1-1,\dots,\rho_{s-1}-1) \text{ and } \mathfrak{p}\in\mathfrak{B}\}$$

is a generating set of I, as an $\mathbb{F}_q$-vector space.

Proof. It suffices to use (2.13) and write

$$q_j^{(i)}(x_1,\dots,x_{s-1}) = \sum_{(\alpha_1,\dots,\alpha_{s-1})\leqslant_+(\rho_1-1,\dots,\rho_{s-1}-1)} q^{(i)}_{j\alpha_1,\dots,\alpha_{s-1}} x_1^{\alpha_1}\cdots x_{s-1}^{\alpha_{s-1}},$$

where $q^{(i)}_{j\alpha_1,\dots,\alpha_{s-1}}\in\mathbb{F}_q$, the sum being finite. Then the polynomial f is written as a linear combination of elements of B', with coefficients in $\mathbb{F}_q$. □

Corollary 3.2. *With the notations in Proposition 3.1, if* $|B'| = \dim I = \log_q|I|$, *then B' is an $\mathbb{F}_q$-basis of I, when I is considered as an $\mathbb{F}_q$-subspace of R.*

Proof. The ring R is isomorphic to a subspace of $\mathbb{F}_q^n$, by the mapping

$$R \longleftrightarrow \mathbb{F}_q^n$$
$$f(x) = \sum_{\alpha\in\mathcal{G}_s} f_\alpha x^\alpha \longleftrightarrow (f_\alpha)_{\alpha\in\mathcal{G}_s},$$

where $n=\prod_{i=1}^s \rho_i$. Thus, I may be identified with a subspace of $\mathbb{F}_q^n$, and it is known that in this case, $\dim I = \log_{\mathrm{q}}|I|$. Since the set B' is an $\mathbb{F}_q$-generating set, it follows that it is an $\mathbb{F}_q$-basis of I, when its cardinality equals to $\dim I$.

□

The set B' in 3.1 may be too large to be an $\mathbb{F}_q$- basis of I. In other words, the elements of B' may be linearly dependent. If this is the case, an $\mathbb{F}_q$ - basis B of I should be then extracted from B'.

We will find linearly independent elements of B' and check whether they form an $\mathbb{F}_q$ -base of I.

According to the notations in (2.12), we choose polynomials

$$\mathfrak{p}_0(x_1,\dots,x_s),\dots,\mathfrak{p}_{\rho_s-1}(x_1,\dots,x_s), \tag{3.1}$$

where $\mathfrak{p}_k\in\{\mathfrak{p}_1^{(k)},\dots,\mathfrak{p}^{(k)}_{r_{\rho_s-1}}\}$. Let $p_k(x_1,\dots,x_{s-1})\in S$ be the coefficient of $\mathfrak{p}_k$ with respect to x_s^k and

$$a_k = \deg p_k, \tag{3.2}$$

where the degree is defined as in (2.11), but, now, in the quotient ring S. We have

$$\mathfrak{p}_k(x_1, \ldots, x_s) = \sum_{h=k}^{\rho_{s-1}} p_h^h(x_1, \ldots, x_{s-1}) x_s^h, \tag{3.3}$$

with $p_h^h \in S$ and

$$p_k^k = p_k. \tag{3.4}$$

Proposition 3.3. *Let $l_0(x_1, \ldots, x_{s-1}), \ldots, l_{\rho_{s-1}}(x_1, \ldots, x_{s-1})$ be polynomials in $\mathbb{F}_q[x_1, \ldots, x_{s-1}]$ such that $\deg(l_k) <_+ [(\rho_1, \ldots, \rho_{s-1}) - (a_k)]$. Then*

$$\sum_{k=0}^{\rho_{s-1}} l_k(x_1, \ldots, x_{s-1}) \mathfrak{p}_k(x_1, \ldots, x_{s-1}) = 0 \Longrightarrow l_k(x_1, \ldots, x_{s-1}) = 0$$

$$\textit{for } k = 0 \ldots, \rho_{s-1}.$$

Proof. Let $l_0(x_1, \ldots, x_{s-1}), \ldots, l_{\rho_{s-1}}(x_1, \ldots, x_{s-1})$ be polynomials in $\mathbb{F}_q[x_1, \ldots, x_{s-1}]$ which verify the hypothesis of the proposition, such that

$$\sum_{k=0}^{\rho_{s-1}} l_k(x_1, \ldots, x_{s-1}) \mathfrak{p}_k(x_1, \ldots, x_s) = 0.$$

Then

$$l_0(x_1, \ldots, x_{s-1}) p_0(x_1, \ldots, x_{s-1}) = 0.$$

Suppose that $l_0 \neq 0$. By taking the degrees, we have, by Proposition 3.5,

$$\deg(l_0 p_0) = \deg(l_0) + \deg(p_0) > 0. \tag{3.5}$$

But this is impossible for a non-zero polynomial. It follows that $l_0 = 0$ and using (3.3), the same reasoning can be applied step by step to show that l_i for $i = 1, \ldots, \rho_{s-1}$. ☐

Theorem 3.4. *With the previous notations, let B be the set*

$$\begin{aligned} B = &\{x_1^{i_1^0} \ldots x_{s-1}^{i_{s-1}^0} \mathfrak{p}_0(x_1, \ldots, x_s) \mid (i_1^0, \ldots, i_{s-1}^0) <_+ (\rho_1, \ldots, \rho_{s-1}) - a_0\} \\ &\cup \{x_1^{i_1^1} \ldots x_{s-1}^{i_{s-1}^1} \mathfrak{p}_1(x_1, \ldots, x_s) \mid (i_1^1, \ldots, i_{s-1}^1) <_+ (\rho_1, \ldots, \rho_{s-1}) - a_1\} \\ &\quad \ldots \\ &\cup \{x_1^{i_1^{r_{n-1}}} \ldots x_{s-1}^{i_{s-1}^{r_{n-1}}} \mathfrak{p}_{\rho_s - 1}(x_1, \ldots, x_s) \mid \\ &\qquad\qquad (i_1^{r_{n-1}}, \ldots, i_{s-1}^{r_{n-1}}) <_+ (\rho_1, \ldots, \rho_{s-1}) - a_{\rho_s - 1}\}. \end{aligned}$$

Then

(1) *The elements of B are $\mathbb{F}_q$-linearly independent.*

(2) *If $|B| = \log_q |I|$, then B is an $\mathbb{F}_q$-basis of I.*

Proof. (1) We construct the finite sequence of numbers

$N_k = |\{x_1^{i_1^k} \dots x_{s-1}^{i_{s-1}^k} \mathfrak{p}_k(x_1, \dots, x_s) \mid (i_1^k, \dots, i_{s-1}^k) <_+ (\rho_1, \dots, \rho_{s-1}) - a_k|.$

for $k = 0, \dots, \rho_s - 1$. Now, let $(\alpha_j^k)_{1 \leqslant j \leqslant N_k}$ be sequences of elements of $\mathbb{F}_q$ such that

$$\sum_{k=0}^{\rho_s - 1} \sum_{j=1}^{N_k} \alpha_j^k x_1^{i_1^k} \dots x_{s-1}^{i_{s-1}^k} \mathfrak{p}_k(x_1, \dots, x_s) = 0 \tag{3.6}$$

(this is a linear combination of elements of B which equals to zero). By taking

$$l_k(x_1, \dots, x_{s-1}) = \sum_{j=1}^{N_k} \alpha_j^k x_1^{i_1^k} \dots x_{s-1}^{i_{s-1}^k}$$

for $k = 0, \dots, \rho_s - 1$, equation (3.6) becomes

$$\sum_{k=0}^{\rho_s - 1} l_k(x_1, \dots, x_{s-1}) \mathfrak{p}_k(x_1, \dots, x_s) = 0.$$

By Proposition 3.3, we have $l_k(x_1, \dots, x_{s-1}) = 0$ for $k = 0, \dots, \rho_{s-1}$, i.e. $\alpha_j^k = 0$ for $j = 1, \dots, N_k$.
(2) The proof is similar to that of Corollary 3.2 where B' is replaced by B, which is an $\mathbb{F}_q$-linearly independent of I. □

From its construction, it is clear that the independent set B is a subset of the generating set B'. If B is too small to be an $\mathbb{F}_q$-basis for the code, we can add elements from B' in order to get a basis.

For an $\mathbb{F}_q$-basis $B = \{g_1(x), \dots, g_l(x)\}$ of I, where, according to (2.10)

$$g_\lambda(x) = g_{\lambda\alpha^{(1)}} x^{\alpha^{(1)}} + \dots + g_{\lambda\alpha^{(i)}} x^{\alpha^{(1)}} + \dots + g_{\lambda\alpha^{(\rho_s)}} x^{\alpha^{(n)}} \text{ for } \lambda = 1, \dots, l. \tag{3.7}$$

A generator matrix for I, as a multicyclic code is then

$$G = \begin{pmatrix} g_{1\alpha^{(1)}} & \dots & g_{1\alpha^{(\nu)}} & \dots & g_{1\alpha^{(n)}} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ g_{\lambda\alpha^{(1)}} & \dots & g_{\lambda\alpha^{(\nu)}} & \dots & g_{\lambda\alpha^{(n)}} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ g_{l\alpha^{(1)}} & \dots & g_{l\alpha^{(\nu)}} & \dots & g_{l\alpha^{(n)}} \end{pmatrix} \in \mathbb{F}_q^{l,n}, \tag{3.8}$$

where $\mathbb{F}_q^{l,n}$ is the set of matrices with l rows and n columns and entries in $\mathbb{F}_q$. In other words, G is the matrix whose rows are the coefficients of the elements of B.

4. Examples

In this section, we refer to Appendix A for the construction of the codes and to Appendix B for the construction of an ideal basis of the code.

Example 4.1 (2-D case)**.** We consider the following 2-D cyclic code:

$$\begin{aligned} I =&\{0, -x-1, -x+y, x+1, x-y, -y-1, y+1, -x-y+1,\\ &x+y-1, -xy+1, xy-1, -xy-y, xy+y, -xy-x, xy+x,\\ &-xy+y-1, xy-y+1, -xy+x-1, xy-x+1, -xy+x+y,\\ &xy-x-y, -xy-x-y-1, -xy-x+y+1, -xy+x-y+1,\\ &xy-x+y-1, xy+x-y-1, xy+x+y+1\}. \end{aligned}$$

It is an ideal of the quotient ring

$$\mathbb{F}_3[X,Y]/\langle X^2-1, Y^2-1\rangle = \mathbb{F}_3[x,y],$$

The code has $|I| = 27$ elements. Thus $\dim I = \log_3 |I| = \log_3 27 = 3$. An ideal basis of I, found in Appendix B is

$$\mathfrak{B} = \{\mathfrak{p}_0(x,y), \mathfrak{p}_1(x,y)\} = \{1+y, y+xy\}.$$

We will construct the $\mathbb{F}_3$-generating set B', as in Proposition 3.1. Since $s = 2$ and $(\rho_1, \rho_2) = (2,2)$, we have

$$\Delta = \{i \in \mathbb{N} \mid i \leqslant \rho_1 - 1\} = \{0,1\}$$

and

$$\begin{aligned} B' &= \{x^i\mathfrak{p}_0, x^i\mathfrak{p}_1 \mid i \in \Delta\} = \{x^i\mathfrak{p}_0, x^i\mathfrak{p}_1 \mid i \in \{0,1\}\}\\ &= \{\mathfrak{p}_0, x\mathfrak{p}_0, \mathfrak{p}_1, x\mathfrak{p}_1\}\\ &= \{y+1, x+xy, y+xy, y+xy\}. \end{aligned}$$

Since $|B'| = 4 > \dim I$, the set B' is not linearly independent (we must remove one element) and therefore is not an $\mathbb{F}_3$-basis. We see that the two last elements of B' are equal. Thus the set

$$B" = \{1+y, x+xy, y+xy\}$$

is also a generating set of I. Since $|B"| = 3 = \dim I$, it is also an $\mathbb{F}_3$-basis of I.

Now, we are going to construct the independent B found using Theorem 3.4. Using the notations in (3.3) and (3.4) and the data in Appendix B, we have:

$$\begin{aligned} p_0^0(x) &= 1 = p_0(x) \in J_0,\\ p_1^1(x) &= x+1 = p_1(x) \in J_1, \end{aligned}$$

so that $a_0 = \deg p_0 = 0$ and $a_1 = \deg p_1 = 1$. The order $\leqslant_+$ is the usual order $\leqslant$ on $\mathbb{N}$. Using Theorem 3.4, we have

$$\begin{aligned} B &= \{x^i \mathfrak{p}_0 \mid i < 2-0\} \bigcup \{x^i \mathfrak{p}_1 \mid i < 2-1\} \\ &= \{\mathfrak{p}_0(x,y), x\mathfrak{p}_0(x,y), \mathfrak{p}_1(x,y)\} = \{1+y, x+xy, y+xy\}. \end{aligned}$$

Since $|B| = \dim I = 3$, it follows that the set B is indeed an $\mathbb{F}_3$- basis of I. Moreover, we see that $B = B$".

We will write the elements of B as vectors, by taking the coefficients. The set of exponents of the elements of R is

$$\mathcal{G}_2 = \{00, 01, 10, 11\} = \mathbb{Z}/2\,\mathbb{Z} \times \mathbb{Z}/2\,\mathbb{Z}$$

as in (2.4). According to (2.9), we have

$$00 <_{\text{lex}} 01 <_{\text{lex}} 10 <_{\text{lex}} 11,$$

and using (2.10), we can make the identification

$$a + by + cx + dxy \equiv \begin{pmatrix} a, & b, & c, & d \end{pmatrix}.$$

between polynomials in R and the vectors of $\mathbb{F}_3^4$. We then can write

$$B = \{(1,1,0,0), (0,0,1,1), (0,1,0,1)\} \subset \mathbb{F}_3^4\,.$$

Writing as in (3.8), a generator matrix of the 2-D code I is

$$G = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} \in \mathbb{F}_3^{3,4}\,.$$

Example 4.2 (3-D case)**.** We have constructed the following 3-D cyclic code

$$\begin{aligned}J =&\{0, -z+2, xz+z+2, -xyz-x+2, -xy-x+z+1,\\ &xyz+xy-x+1, xyz+xy-x-z, xyz+xy+yz+2,\\ &-xz+yz+x-y+2, xy-yz+y+z+1, xyz+xz+x-y-z,\\ &xyz+xy+xz-x+z, -xyz+xy-xz-yz+z,\\ &xyz-xy+yz+x-y+1, -xyz+xy-yz-x+y+z,\\ &-xyz+xy-xz+x+y-z, xyz+xy+xz+yz+z+1,\\ &xyz-xy-xz+yz-y+1, -xyz+xz-yz+x+y-z+2,\\ &xyz-xy-xz-x-y-z+2, -xyz-xy-xz-yz+x-z+1,\\ &xyz-xy+xz+yz+x-z+2, xyz-xy+xz+yz+x-y+z,\\ &-xyz-xy-xz-yz-x+y-z+1,\\ &-xyz-xy-xz-yz+x-y+z+2,\\ &-xyz+xy+xz+yz-x-y-z+1,\\ &xyz-xy+xz+yz-x+y-z+2, ...\}.\end{aligned}$$

It is an ideal of the quotient ring

$$\mathbb{F}_3[X, Y, Z]/\langle X^2-1, Y^2-1, Z^2-1\rangle = \mathbb{F}_3[x, y, z],$$

The code J has 2187 elements, so that $\dim J = \log_3 |J| = \log_3 2178 = 7$.

And ideal basis of J, found in Appendix B is

$$\mathfrak{B} = \{\mathfrak{p}_0^{(0)}, \mathfrak{p}_1^{(0)}, \mathfrak{p}_0^{(1)}, \mathfrak{p}_1^{(1)}\} = \{1+z+y+yz, -z+y, z+yz, yz-xyz\}.$$

Since $|\mathfrak{B}| = 4 < \dim I$, it is not a generating set of I. We are going to construct the generating set B', according to Proposition 3.1. Since $s = 3$ and $(\rho_1, \rho_2, \rho_3) = (2, 2, 2)$, we have

$$\begin{aligned}\Delta &= \{(i, j) \in \mathbb{N}^2 \mid (i, j) \leqslant_+ (\rho_1-1, \rho_2-1) = (1, 1)\}\\ &= \{(0, 0), (1, 0), (0, 1), (1, 1)\},\end{aligned}$$

so that

$$\begin{aligned}B' &= \{x^iy^j\mathfrak{p}_0^{(0)}, x^iy^j\mathfrak{p}_1^{(0)}, x^iy^j\mathfrak{p}_0^{(1)}, x^iy^j\mathfrak{p}_1^{(1)} \mid (i, j) \in \Delta\}\\ &= \{xyz-yz, yz+y+z+1, xyz+xy+xz+x, xy-xz, -xyz+x,\\ &\quad xz-z, -yz+1, -xyz+yz, -xz+z, y-z\}\end{aligned}$$

Since $|B'| = 10 > \dim I$, it follows from Corollary that B' is not an $\mathbb{F}_3$-linearly independent set and therefore not an $\mathbb{F}_3$-basis of J (too large).

We are going to construct the $\mathbb{F}_3$-linearly independent set B as in Theorem 3.4. According to the notations in Appendix B, (3.1) and (3.4), we choose a polynomial $\mathfrak{p}_k \in \mathfrak{B}$ with $p_k \in J_k$ for $k = 0, 1$, where p_k is the coefficient of z^k as a polynomial in whose coefficients are polynomials in x and y. We may take

$$\begin{aligned}
\mathfrak{p}_1(x,y,z) &= \mathfrak{p}_0^{(0)}(x,y,z) = 1 + y + z + yz, \\
p_0(x,y) &= 1 + y,\ a_0 = \deg p_0 = (0,1) \\
\mathfrak{p}_2(z,y,z) &= \mathfrak{p}_1^{(1)}(x,y,z) = yz - xyz \\
p_1(x,y) &= y - xy,\ \deg p_1 = (1,1).
\end{aligned}$$

We get

$$\begin{aligned}
B &= \{x^i y^j \mathfrak{p}_0 \mid (i,j) <_+ (\rho_1,\rho_2) - \deg a_0\} \\
&\quad \bigcup \{x^i y^j \mathfrak{p}_1 \mid (i,j) <_+ (\rho_1,\rho_2) - \deg a_1\ \} \\
&= \{x^i y^j \mathfrak{p}_0 \mid (i,j) <_+ (2,2) - (0,1)\} \bigcup \{x^i y^j \mathfrak{p}_1 \mid (i,j) <_+ (2,2) - (1,1)\ \} \\
&= \{x^i y^j \mathfrak{p}_0 \mid (i,j) \in \{(0,0),(1,0)\}\} \bigcup \{x^i y^j \mathfrak{p}_1 \mid (i,j) \in \{(0,0),(1,0),(1,0),(1,1\}\ \} \\
&= \{\mathfrak{p}_o, x\mathfrak{p}_0, \mathfrak{p}_1, x\mathfrak{p}_1, y\mathfrak{p}_1, xy\mathfrak{p}_1\} \\
&= \{-yz + xyz, x + xz + xy + xyz, 1 + z + y + yz, z - xz\}
\end{aligned}$$

Since $|B| = 4 < \dim J = 7$, the set B fails to be a basis for J (too small). Since $B \subset B'$, we will add three elements from $B' \setminus B$ to B in order to obtain an $\mathbb{F}_3$-basis. We have

$$B' \setminus B = \{y - z, yz + z, -yz + 1, xy - xz, xyz + xz, -xyz + x\}.$$

We will write the elements of B and $B' \setminus B$ as vectors, by taking the coefficients. The set of exponents of the elements of R is

$$\mathcal{G}_3 = \{000, 001, 010, 011, 100, 101, 110, 111\}$$

as in (2.4). According to (2.9), we have

$$\begin{aligned}
&000 <_{\text{lex}} 001 <_{\text{lex}} 010 <_{\text{lex}} 011 <_{\text{lex}} 100 <_{\text{lex}} 101 <_{\text{lex}} 110 \\
&<_{\text{lex}} 111,
\end{aligned} \tag{4.1}$$

and using (2.10), we can make the identification

$$a+bz+cy+dyz+ex+fxz+gxy+hxyz \equiv \begin{pmatrix} a, & b, & c, & d, & e, & f, & g, & h \end{pmatrix}.$$

between polynomials in R and the vectors of $\mathbb{F}_3^8$. We then can write

$$\begin{aligned}
B =&\{(0,0,0,-1,0,0,0,1),(0,0,0,0,1,1,1,1),(1,1,1,1,0,0,0,0), \\
&(0,1,0,0,0,-1,0,0)\},
\end{aligned}$$

and may identify it with the matrix

$$V = \begin{pmatrix} 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 \end{pmatrix} \in \mathbb{F}_3^{4,8},$$

whose rows are the elements of B. We do the same with the elements of $B' \setminus B$ and get a matrix $V' \in \mathbb{F}_3^{6,8}$. We then can add three rows of V' to V in order to obtain a matrix with seven $\mathbb{F}_3$-linearly independent rows. We find the following vectors

$$\begin{aligned} &\begin{pmatrix} 0, & -1, & 1, & 0, & 0, & 0, & 0, & 0 \end{pmatrix} \equiv z - y, \\ &\begin{pmatrix} 0, & 1, & 0, & 1, & 0, & 0, & 0, & 0 \end{pmatrix} \equiv z + yz, \\ &\begin{pmatrix} 1, & 0, & 0, & -1, & 0, & 0, & 0, & 0 \end{pmatrix} \equiv 1 - yz. \end{aligned}$$

Finally, an $\mathbb{F}_3$-basis of J is the set

$$\begin{aligned} B\text{''} =& \{z - y, z + yz, 1 - yz\} \cup B \\ =& \{z - y, z + yz, 1 - yz, -yz + xyz, x + xz + xy + xyz, \\ & 1 + z + y + yz, z - xz\}. \end{aligned}$$

This correspond to the matrix

$$G = \begin{pmatrix} 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 \end{pmatrix} \in \mathbb{F}_3^{7,8},$$

which is a generator matrix of J.

Appendix A: Construction of multicyclic codes

Here we summarize the construction of multicyclic codes in [2].

In the general case, an r-*dimensional multicyclic code* (or r-D multicyclic code) is an ideal of the quotient ring

$$R = \mathbb{F}_q[X_1, \ldots, X_r]/\langle X_1^{n_1} - 1, \ldots, X_r^{n_r} - 1\rangle.$$

In [2], we considered the important case where q is of the form $q = p^m$ with $m \geqslant 1$ an integer and p a prime integer which does not divide any of the $n_1, \dots, n_r$.

We recall the main result about the characterization of these codes :

Theorem (Ideals in $\mathbb{F}_q[x]$, [2, 1]). A set $\boldsymbol{I}$ is an ideal of $\mathbb{F}_q[x]$ if and only if these exists a subset Z of S such that

$$\boldsymbol{I} = \{a(x) \in \mathbb{F}_q[x] \mid a(\underline{\xi}^{h(i)}) = 0 \ \forall i \in Z\}.$$

Proof. See [2]. □

The above theorem means that the ideal I is the set of the polynomials of $\mathbb{F}[x]$ which vanish on the elements $\underline{\xi}^{(h(i)} \in \mathbb{F}_{q^t}^r$ for $i \in Z$. The notations are explained bellow :

The set S is equal to $\{1, \dots, s\}$, where s is the number of orbits by the operation of the Galois group

$$\Gamma = \mathrm{GAL}(\mathbb{F}_{q^t}, \mathbb{F}_q) = \{\sigma^\nu \mid \nu = 0, \dots, t-1,\ \sigma^\nu : \mathbb{F}_{q^t} \longrightarrow \mathbb{F}_{q^t},\ \omega \longmapsto \omega^{q^\nu}\}$$

on the abelian group $\mathcal{G}_+ = \prod_{\rho=1}^{r} \mathbb{Z}/n_\rho\mathbb{Z}$.

One construct the integer t as the follows : one takes $\varepsilon = \mathrm{ppcm}(n_1, \dots, n_r)$, and

$$t = \min\{k \in \mathbb{N} \ \mid \ q^k \equiv 1 \pmod{\varepsilon}\}.$$

There exist in $\mathbb{F}_{q^t}$ an element of order ε and for $\rho = 1, \dots, r$, the element $\xi_\rho = \alpha^{\frac{\varepsilon}{n_\rho}}$ de $\mathbb{F}_{q^t}$ is a n_ρ-th primitive root of unity, i.e. $\xi^{n_\rho} = 1$ and each n_ρ-th root of unity in $\mathbb{F}_{q^t}$ is a power of ξ_ρ.

Next, we explain other notations used in the above theorem:

(1) Let ξ_ρ be a primitive n_ρ-th root of unity in $\mathbb{F}_{q^t}$ for $\rho = 1, \dots, r$. Let $\underline{\xi}$ the vector defined by

$$\underline{\xi} = (\xi_1, \dots, \xi_\rho, \dots, \xi_r) \in \mathbb{F}_{q^t}^r \quad \text{and} \quad \xi = \xi_1 \cdots \xi_\rho \cdots \xi_r \in \mathbb{F}_{q^t},$$

and for $h = (h_1, \dots, h_r) \in \prod_{\rho=1}^{r} \mathbb{Z}/n_\rho\mathbb{Z}$,

$$\underline{\xi}^h = (\xi_1^{h_1}, \dots, \xi_\rho^{h_\rho}, \dots, \xi_r^{h_r}) \in \mathbb{F}_{q^t}^r \quad \text{et} \quad \xi^h = \xi_1^{h_1} \cdots \xi_\rho^{h_\rho} \cdots \xi_r^{h_r} \in \mathbb{F}_{q^t}. \tag{4.2}$$

(2) for $c(x) = \sum_{g \in \mathcal{G}_+} c_g x^g \in \mathbb{F}_q[x]$ and $h = (h_1, \dots, h_r)$ in $\mathcal{G}_+$, the element $c(\underline{\xi}^h)$ is defined by

$$c(\underline{\xi}^h) = \sum_{g \in \mathcal{G}_+} c_g \xi^{hg} = \sum_{g \in \mathcal{G}_+} c_g \xi_1^{h_1 g_1} \cdots \xi_r^{h_r g_r} \in \mathbb{F}_{q^t}.$$

A method for constructing a multicyclic code

Input: An integer $r \geqslant 1$, integers $n_1, \dots, n_r \geqslant 1$ and a prime integer p which does not divide any of $n_1, \dots, n_r$.
Output: An r-D multicyclic code $\mathcal{C}$ of $\mathbb{F}_q[x]$, of length $n = n_1 \cdots n_r$.

Step 1: Construction of the base field and the group $\mathcal{G}_+$:
- $\mathbb{F}_p = \mathbb{Z}/p\,\mathbb{Z}$,
- $\mathcal{G}_+ = \prod_{\rho=1}^{r} \mathbb{Z}/n_\rho\,\mathbb{Z}$.

Step 2: Construction of the first extension of the base field:
- choose an integer $m \geqslant 1$ and take $q = p^m$,
- construct the field $\mathbb{F}_q$, extension of $\mathbb{F}_p$.

Step 3: Construction of the second extension of the base field:
- $\varepsilon = \mathrm{ppcm}(n_1, \dots, n_r)$,
- find $t = \min\{k \in \mathbb{N} \mid q^k \equiv 1 \pmod{\varepsilon}\}$,
- construct the field $\mathbb{F}_{q^t} = \mathbb{F}_{p^{mt}}$, extension of $\mathbb{F}_q$.

Step 4: Construction of the primitive n_ρ-th roots of unity, $\rho = 1, \dots, r$:
- choose an element α of order ε in $\mathbb{F}_{q^t}^*$: $\alpha = a^{\frac{q^t-1}{\varepsilon}}$ where a is a generator of the cyclic group $(\mathbb{F}_{q^t}^*, \times)$.
- take $\xi_\rho = \alpha^{\frac{\varepsilon}{n_\rho}}$ for $\rho = 1, \dots, r$.

Step 5: Construction of the Galois group:
$\Gamma = \mathrm{GAL}(\mathbb{F}_{q^t}, \mathbb{F}_q) = \{\sigma^\nu \mid \sigma^\nu : \mathbb{F}_{q^t} \longrightarrow \mathbb{F}_{q^t} \;,\; \omega \longmapsto \omega^{q^\nu}, \quad \nu = 0, \dots, t-1\}$.

Step 6:
- for each $g \in \mathcal{G}_+$, find the orbit of g:

$$\Gamma.g = \{g q^\nu \mid \nu = 0, \dots, t-1\}.$$

- find all the orbits : $\mathcal{O}_1, \dots, \mathcal{O}_s$,
- take $S = \{1, \dots, s\}$.

Step 7: Choice of the zeros of the code:
- choose a subset Z of S,
- for $i \in Z$, choose a representative $h(i)$ of $\mathcal{O}_i$,
- the zeroes of the code are $\{h(i) \mid i \in Z\}$.

Step 8: Construction of the code:
- $\mathcal{C} = \{c(x) \in \mathbb{F}_q[x] \mid c(\xi^{h(i)}) = 0 \text{ for } \ i \in Z\}$.

The code I in Example 4.1 is constructed with the following parameters: $r = 2, n_1 = n_2 = 2, p = 3, m = 1$. The length of the code is $n = n_1 n_2 = 4$. Since $t = 1$, we have $q = 3$. The primitive roots of unity are $\xi_1 = \xi_2 = 2$ and $\xi = (2, 2) \in \mathbb{F}_3^2$. The the of the orbits is

$$\{\mathcal{O}_1, \mathcal{O}_2, \mathcal{O}_3, \mathcal{O}_4\} = \{\{(0,1)\}, \{(1,0)\}, \{(0,0)\}, \{(1,1)\}\} \subset (\mathbb{Z}/3\,\mathbb{Z})^2,$$

so that $s = 4$ and $S = \{1, 2, 3, 4\}$. We take $Z = \{4\}$, which correspond to $\mathcal{O}_4 = \{(1,1)\}$. The code is then the ideal whose elements are the polynomials of $\mathbb{F}_3[x, y]$ which vanish on the set

$$O_Z = \{\xi^{(1,1)}\} = \{(\xi_1^1, \xi_2^1)\} = \{(2,2)\} \subset (\mathbb{Z}/3\,\mathbb{Z})^2.$$

The code J in Example 4.2 is constructed with the following parameters: $r = 3, n_1 = n_2 = n_3 = 2, p = 3, m = 1$. The length is $n = n_1 n_2 n_3 = 8$. Since $t = 1$, we have $q = 3$. The primitive roots of unity are $\xi_1 = \xi_2 = \xi_3 = 2$ and $\xi = (2, 2, 2) \in \mathbb{F}_3^3$. The set of the orbits is

$$\begin{aligned}
&\{\mathcal{O}_1, \mathcal{O}_2, \mathcal{O}_3, \mathcal{O}_4, \mathcal{O}_5, \mathcal{O}_6, \mathcal{O}_7, \mathcal{O}_8\} \\
&= \{\{(1,0,1)\}, \{(1,1,0)\}, \{(1,1,1)\}, \{(0,1,0)\}, \\
&\quad \{(0,1,1)\}, \{(0,0,1)\}, \{(0,0,0)\}, \{(1,0,0)\}\} \subset (\mathbb{Z}/3\,\mathbb{Z})^3,
\end{aligned}$$

so that $s = 8$ and $S = \{1, 2, 3, 4, 5, 6, 7, 8\}$. We take $Z = \{5\}$, which correspond to $\mathcal{O}_5 = \{(0,1,1)\}$. The code is then the ideal whose elements are the polynomials of $\mathbb{F}_3[x, y, z]$ which vanish on the set

$$O_Z = \{\xi^{(0,1,1)}\} = \{(\xi_1^0, \xi_2^1, \xi_3^1)\} = \{(1,2,2)\} \subset (\mathbb{Z}/3\,\mathbb{Z})^3.$$

Appendix B: Algorithms for constructing an ideal basis of a multicylic code

In this section, we present algorithms which are derived from Sepasdar's method ([6, 3]) for finding a basis of an ideal in the two-dimensional case and its extension to the three-dimensional case. The case of a more variable can be deduced from these algorithms.

First algorithm: case of an ideal in two variables
Input : two integers $m, n \geqslant 1$, an integer q which is the power of a prime number, a non-zero ideal I of $\mathbb{F}_q[x, y]$.
Output : a basis B of the ideal I.

Step 1. For $i = 0, \dots, n-1$, find the ideals I_i and the subsets H_i, of $\mathbb{F}_q[x]$ defined by

$$I_0 = H_0 = \{\text{constant terms of the elements of } I \text{ as polynomials in } y\}$$

and for $i = 1, ..., n-1$,

$$H_i = \{\text{elements of } I \text{ whose coefficient of } y^j, j = 0, \dots, i-1 \text{ are zero}\}$$

$$(= \{\text{elements of } H_{i-1} \text{ whose coefficient of } y^{i-1} \text{ is zero}\}),$$

$$I_i = \{\text{coefficients of } y^i \text{ of the elements of } H_i\}.$$

Step 2. For $i = 0, \dots, n-1$, find a generator $p_i(x)$ of I_i in $\mathbb{F}_q[x]$.
Step 3. Find an element $P_0(x, y) \in I$ whose constant term, as a polynomial in y is $p_0(x)$.
Step 4. Find an element $P_i(x, y) \in I$ whose coefficients of y^j, $j = 0, \dots, i-1$ are zeros, the coefficient of y^i being $p_i(x)$.
Step 5. A basis of I is

$$B = \{P_i(x, y) \mid i = 0, \dots, n-1\}.$$

For the code in Example 4.1, we apply this first algorithm.

$$\begin{aligned}
I_0 = H_0 = \{&g_0(x) \in \mathbb{F}_3[x, y] \mid \exists g(x, y) \in I \text{ such that } \\
&g(x, y) = g_0(x) + g_1(x)y \text{ where } g_1(x) \in \mathbb{F}_3[x]\} \\
= \{&-1, 0, 1, x, y, xy, -x, -y, -xy, -x-1, -x+1, -x-y, -x+y, \\
&x-1, x+1, x-y, x+y, -y-1, -y+1, y-1, y+1, -x-y-1, \\
&-x-y+1, -x+y-1, -x+y+1, x-y-1, x-y+1, x+y-1, \\
&x+y+1, -xy-1, -xy+1, xy-1, xy+1, -xy-y, -xy+y, \\
&xy-y, xy+y, -xy-x, -xy+x, xy-x, xy+x, -xy-y-1, \\
&-xy-y+1, -xy+y-1, -xy+y+1, xy-y-1, xy-y+1, \\
&xy+y-1, xy+y+1, -xy-x-1, -xy-x+1, -xy+x-1, \\
&-xy+x+1, xy-x-1, xy-x+1, xy+x-1, xy+x+1, \\
&-xy-x-y, -xy-x+y, -xy+x-y, -xy+x+y, xy-x-y, \\
&xy-x+y, xy+x-y, xy+x+y, -xy-x-y-1, -xy-x-y+1, \\
&-xy-x+y-1, -xy-x+y+1, -xy+x-y-1, -xy+x-y+1, \\
&-xy+x+y-1, -xy+x+y+1, xy-x-y-1, xy-x-y+1, \\
&xy-x+y-1, xy-x+y+1, xy+x-y-1, xy+x-y+1, \\
&xy+x+y-1, xy+x+y+1\}.
\end{aligned}$$

A generator of I_0 is $p_0^0(x) = 1$.

$$\begin{aligned} H_1 &= \{\text{element of } I \text{ whose constant constant term, as a} \\ &\qquad\qquad\qquad\qquad \text{polynomial in } y \text{ is zero}\} \\ &= \{0, -xy - y, xy + y\}, \\ I_1 &= \{\text{coefficients of } y \text{ of the elements of } H_1\ \} \\ &= \{0, -x - 1, x + 1\}. \end{aligned}$$

A generator of I_1 is $p_1^1(x) = x + 1$. Thus, we can take

$\mathfrak{p}_0(x, y) = 1 + y$ (polynomial of I whose constant term is 1)
$\mathfrak{p}_1(x, y) = (x + 1)y = y + xy$ (polynomial of H_1 whose coefficient of y is $x + 1$).

An ideal basis of I is then given by

$$B\ = \{\mathfrak{p}_0(x, y), \mathfrak{p}_1(x, y)\} = \{1 + y, y + xy\}.$$

Second algorithm: case of an ideal in three variables
Input : three integers l, m and $n \geqslant 1$, an integer q which is the power of a prime number, a non zero ideal I of $\mathbb{F}_q[x, y, z]$.
Ouput : a basis B of the ideal I.
Step 1. For $i = 0, \ldots, n - 1$, find the ideals I_i and the subsets H_i of $\mathbb{F}_q[x, y]$ defined by

$$\begin{aligned} I_0 = H_0 &= \{\text{constant terms of the elements of } I \text{ as} \\ &\qquad \text{polynomials in } z\} \end{aligned}$$

and for $i = 1, ..., n - 1$,

$$\begin{aligned} H_i &= \{\text{elements of } I \text{ whose coefficients of } z^j, j = 0, \ldots, i - 1 \\ &\qquad\qquad\qquad\qquad\qquad\qquad \text{are zero}\} \\ I_i &= \{\text{coefficients of } z^i \text{ of the elements of } H_i\}. \end{aligned}$$

Step 2. For $i = 0, \ldots, n-1$, find a basis $B_i = \{p_{i0}(x, y), \ldots, p_{ir_i}(x, y)\}$ of I_i in $\mathbb{F}_q[x, y]$ by the algorithm for the two variables case.
Step 3. For each element $p_{0\rho}(x, y)$ of B_0, find an element $P_{0\rho}(x, y, z) \in I$ whose constant term, as a polynomial in z is $p_{0\rho}(x, y)$.
Step 4. For each element $p_{i\rho}(x, y)$ of B_i, $i = 1, \ldots, n - 1$, find an element $P_{i\rho}(x, y, z) \in I$ whose coefficient of z^j, $j = 0, \ldots, i - 1$ are zeros, the coefficient of z^i being $p_{i\rho}(x, y)$.
Step 5. A basis of I is

$$B = \{P_{i\rho}(x, y, z) \mid i = 0, \ldots, n - 1, \rho = 0, \ldots, r_i\}.$$

For the code J in Example 4.2, we first use the second algorithm.

$$\begin{aligned}
J_0 = H_0 = \{&g_0(x,y) \in \mathbb{F}_3[x,y] \mid \exists g(x,y,z) \in J \text{ such that} \\
&\qquad g(x,y,z) = g_0(x,y) + g_1(x,y)z \text{ where } g_1(x,y) \in \mathbb{F}_3\, x, y\} \\
= \{&-1, 0, 1, x, y, xy, -x, -y, -xy, -x-1, -x+1, -x-y, -x+y, \\
&x-1, x+1, x-y, x+y, -y-1, -y+1, y-1, y+1, -x-y-1, \\
&-x-y+1, -x+y-1, -x+y+1, x-y-1, x-y+1, x+y-1, \\
&x+y+1, -xy-1, -xy+1, xy-1, xy+1, -xy-y, -xy+y, \\
&xy-y, xy+y, -xy-x, -xy+x, xy-x, xy+x, -xy-y-1, \\
&-xy-y+1, -xy+y-1, -xy+y+1, xy-y-1, xy-y+1, \\
&xy+y-1, xy+y+1, -xy-x-1, -xy-x+1, -xy+x-1, \\
&-xy+x+1, xy-x-1, xy-x+1, xy+x-1, xy+x+1, \\
&-xy-x-y, -xy-x+y, -xy+x-y, -xy+x+y, xy-x-y, \\
&xy-x+y, xy+x-y, xy+x+y, -xy-x-y-1, -xy-x-y+1, \\
&-xy-x+y-1, -xy-x+y+1, -xy+x-y-1, -xy+x-y+1, \\
&-xy+x+y-1, -xy+x+y+1, xy-x-y-1, xy-x-y+1, \\
&xy-x+y-1, xy-x+y+1, xy+x-y-1, xy+x-y+1, \\
&xy+x+y-1, xy+x+y+1\}.
\end{aligned}$$

Then, since J_0 is an ideal with two variables, we use the first algorithm to find a basis. Take

$$\begin{aligned}
J_{00} = H_{00} = \{&g_{00}(x) \in \mathbb{F}_3[x] \mid \exists g(x,y) \in J_0 \text{ such that} \\
&\qquad g(x,y) = g_{00}(x) + g_{01}(x)y \text{ where } g_{01}(x) \in \mathbb{F}_3[x]\} \\
= \{&0, 1, -1, x, x+1, x-1, -x, -x+1, -x-1\}.
\end{aligned}$$

We have $J_{00} = \langle 1 \rangle$. By taking $p^0_{00}(x) = 1$, there exists $p_{00}(x,y) \in J_0$ such that $p_{00}(x,y) = 1 + g_{01}(x)y$ where $g_{01}(x) \in S_1$. We can take $g_{01}(x) = 1$, so that

$$p_{00}(x,y) = 1 + y.$$

Now, we are going to find the set H_{01} of the elements of J_0 whose constant terms, as polynomials in y are zero. We find

$$H_{01} = \{0, y, xy, -y, -xy, -xy-y, -xy+y, xy-y, xy+y\}.$$

Now, we consider

$$\begin{aligned}
J_{01} &= \{g_{01}(x) \in \mathbb{F}_3[x] \mid \exists g(x,y) \in H_{01} \text{ such that } g(x,y) = g_{01}(x)y\} \\
&= \text{the set of the coefficients of } y \text{ of the elements of } H_0 \\
&= \{0, 1, -1, x, x+1, x-1, -x, -x+1, -x-1\}.
\end{aligned}$$

We have $J_{01} = \langle 1 \rangle$. By taking $p_{01}^1(x) = 1$, there exists $p_{01}(x,y) \in J_0$ such that $p_{01}(x,y) = g_{01}(x,y)y$. We can take $p_{01}(x,y) = y$. A basis of J_0 is then

$$B_0 = \{p_{00}(x,y), p_{01}(x,y)\} = \{y, 1+y\}.$$

Next, we construct

$$\begin{aligned}
H_1 = \{&\text{elements of } J \text{ whose constant terms, as} \\
&\qquad\qquad\qquad\qquad\text{polynomial in } z \text{ are zero}\} \\
= \{&0, -xz+z, xz-z, -yz-z, yz+z, -xz-yz, xz+yz, -xyz-z, \\
&xyz+z, -xyz+yz, xyz-yz, -xyz-xz, xyz+xz, -xz+yz-z, \\
&xz-yz+z, -xyz-yz+z, xyz+yz-z, -xyz+xz+z, \\
&xyz-xz-z, -xyz+xz-yz, xyz-xz+yz, -xyz-xz-yz-z, \\
&-xyz-xz+yz+z, -xyz+xz+yz-z, xyz-xz-yz+z, \\
&xyz+xz-yz-z, xyz+xz+yz+z\}.
\end{aligned}$$

We then have

$$\begin{aligned}
J_1 &= \{g_1(x,y) \in \mathbb{F}_3[x,y] \mid \exists g(x,y,z) \in H_1 \text{ such that } g(x,y,z) = g_1(x,y)z\} \\
&= \{0, -x+1, -x-y, x-1, x+y, -y-1, y+1, -x+y-1, \\
&\quad x-y+1, -xy-1, xy+1, -xy+y, xy-y, -xy-x, xy+x \\
&\quad xy-y+1, xy+y-1, -xy+x+1, xy-x-1, -xy+x-y, \\
&\quad xy-x+y, -xy-x-y-1, -xy-x+y+1, -xy+x+y-1, \\
&\quad xy-x-y+1, xy+x-y-1, xy+x+y+1\}.
\end{aligned}$$

We use the first algorithm to find a basis of J_1: we construct

$$\begin{aligned}
J_{10} = H_{10} &= \{g_{10}(x) \in \mathbb{F}_3[x] \mid \exists g(x,y) \in J_1 \text{ such that} \\
&\qquad g(x,y) = g_{10}(x) + g_{11}(x)y \text{ where } g_{11}(x) \in \mathbb{F}_3[x]\} \\
&= \{0, 1, -1, x, x+1, x-1, -x, -x+1, -x-1\}.
\end{aligned}$$

We have $J_{10} = \langle 1 \rangle$. If we take $p_{10}^0(x) = 1$, there exists $p_{10}(x,y) \in J_1$ such that $p_{10}(x,y) = 1 + g_{11}(x)y$. We can take $p_{10}(x,y) = 1+y$. Now, consider

$$\begin{aligned}
H_{11} = \{&\text{elements of } J_1 \text{ whose constant terms,} \\
&\qquad\qquad\qquad\text{as polynomials in } y \text{ are zero}\} \\
= \{&0, -xy+y, xy-y\}
\end{aligned}$$

and

$$\begin{aligned}
J_{11} &= \{g_{11}(x) \in \mathbb{F}_3[x] \mid \exists g(x,y) \in H_{11} \text{ and } g(x,y) = g_{11}(x)y\} \\
&= \{0, x-1, -x+1\}.
\end{aligned}$$

We have $J_{11} = \langle 1-x\rangle$. Taking $p_{11}^1(x) = 1-x$, there exists a polynomial $p_{11}(x,y) \in J_1$ such that $p_{11}(x,y) = (1-x)y$. A basis of J_1 is

$$B_1 = \{p_{10}(x,y), p_{11}(x,y)\} = \{1+y, y-xy\}.$$

According to the notations in [5, 3] and in (2.12), an ideal basis of J is then given by

$$\mathfrak{B} = \{\mathfrak{p}_0^{(0)}(x,y,z), \mathfrak{p}_1^{(0)}(x,y,z), \mathfrak{p}_0^{(1)}(x,y,z), \mathfrak{p}_1^{(1)}(x,y,z)\}$$

where

$\mathfrak{p}_0^{(0)}(x,y,z) \in J$, whose constant term is $p_{00}(x,y) = 1+y \in J_0$, as a polynomial in z,

$\mathfrak{p}_1^{(0)}(x,y,z) \in J$, whose constant term is $p_{01}(x,y) = y \in J_0$, as a polynomial in z,

$\mathfrak{p}_0^{(1)}(x,y,z) \in J$, whose constant term is zero, as a polynomial in z, the coefficient of z being $p_{10}(x,y) = 1+y \in J_1$,

$\mathfrak{p}_1^{(1)}(x,y,z) \in J$, whose constant term is zero as a polynomial in z, the coefficient of z being $p_{11}(x,y) = (1-x)y \in J_1$.

We can take

$$\begin{aligned}
\mathfrak{p}_0^{(0)}(x,y,z) &= 1+y+z+yz,\\
\mathfrak{p}_1^{(0)}(x,y,z) &= y-z,\\
\mathfrak{p}_0^{(1)}(x,y,z) &= z+yz,\\
\mathfrak{p}_1^{(1)}(x,y,z) &= yz-xyz,
\end{aligned}$$

and finally,

$$\mathfrak{B} = \{1+y+z+yz, -z+y, z+yz, yz-xyz\}.$$

Acknowledgments

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

References

1. C. Heegard and K. Saints, *Algebraic-Geometry Codes and Multidimensional Cyclic Codes: A Unified Theory and Algorithms for Decoding using Gröbner Bases*. IEEE Trans. Inf. Theory, **41** (1995), 1733–1751.

2. 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.
3. R. M. Lalasoa, R. Andriamfidisoa and T. J. Rabeherimanana, *Basis of a multicyclic code as an Ideal in* $\mathbb{F}[X_1, \ldots, X_s]/\langle X_1^{\rho_1} - 1, \ldots, X_s^{\rho_s} - 1\rangle$, J. Algebra Relat. Topics, (2) **6** (2018), 63–78.
4. Z. Sepasdar, *Some Notes on the Characterization of two dimensional skew cyclic Codes*, J. Algebra Relat. Topics, (2) **4** (2016), 1-8.
5. Z. Sepasdar, K. Khashyarmanesh, *Characterizations of some two-dimensional cyclic Codes correspond to the Ideals of* $\mathbb{F}[x, y]/\langle x^s - 1, y^{2k} - 1\rangle$, Finite Fields Appl. **41** (2016), 97-112.
6. Z. Sepasdar, *Generator Matrix for two-dimensional cyclic Codes of arbitrary Length*, arXiv:1704.08070v1, [math.AC], 26 Apr 2017.

R. 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: `andriamifidisoa.ramamonjy@univ-antananarivo.mg`

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

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