British Journal of Mathematics & Computer Science
21(2): 1-22, 2017, Article no.BJMCS.31510
ISSN: 2231-0851

SCIENCEDOMAIN *international*
www.sciencedomain.org

Multicyclic Codes and Algebraic Dynamical Systems

R. M. Lalasoa[1], R. Andriamifidisoa[2*] and T. J. Rabeherimanana[1]

[1] *Department of Mathematics and Computer Science, Faculty of Sciences, University of Antananarivo, BOP 906, 101 Antananarivo, Madagascar.*
[2] *Higher Polytechnics Institute of Madagascar (ISPM), Ambatomaro, Antsobolo, 101 Antananarivo, Madagascar.*

Authors' contributions

This work was carried out in collaboration between all authors. Author RML worked on proofs and examples, did computer computations, managed literature search and finished the manuscript. Author RA designed the study, wrote the first draft and the protocol, and managed literature search. Author TJR analyzed and verified the results. All authors read and approved the final manuscript.

Article Information

DOI: 10.9734/BJMCS/2017/31510
Editor(s):
(1) Dragos-Patru Covei, Department of Applied Mathematics, The Bucharest University of Economic Studies, Piata Romana, Romania.
Reviewers:
(1) Adegoke Solomon Osifodunrin, Houston Community College, Northline Campus, USA.
(2) Samuel Asante Gyamerah, Pan African University Institute of Science Technology and Innovation, Kenya.
(3) Danjuma Samaila, Adamawa State University, Mubi, Nigeria.
Complete Peer review History: http://www.sciencedomain.org/review-history/18302

Received: 9th January 2017
Accepted: 5th March 2017
Published: 22nd March 2017

Original Research Article

Abstract

We present the structures within group algebras constructed from commutative groups and finite fields. Then we define and construct multicyclic codes in these group algebras. At the end, in the frame of the decoding process, we give a characterization of the locator ideal to the multidimensional case. All of this is done using algebraic dynamical systems, which explains the underlying mathematical objects.

Keywords: Galois group; group algebra; categories and functors; algebraic dynamical system; multicyclic code.

2010 Mathematics Subject Classification: 11S20, 20C20, 94B15.

*Corresponding author: E-mail: ramamonjy.andriamifidisoa@univ-antananarivo.mg;

1 Introduction

Two dimensional (2D) cyclic codes are important because they are used in daily technical applications such as video encoding. Higher dimensional cyclic codes (*multicyclic codes*) are also important, not only for they allow the use of rich mathematics structures, but also because they are generalize *algebraic-geometry codes*, which form an important class of codes ([1, 2]).

Until now, the use of algebraic dynamical systems in the decoding process of *block codes* over finite fields has been mainly introduced by two authors : Kuijper and Andriamifidisoa. In [3], Kuijper introduced algebraic dynamical systems with the decoding of RS and BCH codes. She proved that the construction of a *minimal a state-space system* from the syndrome vector of a received word solves the problem of finding the error vector. Andriamifidisoa, in [4] also used the construction of an algebraic dynamical systems with the decoding process, but within the context of algebraic-geometry codes.

In this article, one of our goal is to use concepts from algebraic dynamical systems for the decoding process the multicyclic codes. Instead of constructing an algebraic dynamical system from the syndrome of the received word, we start from the fact that the error vector and its Fourier transform already belongs to an algebraic dynamical system and therefore we can use tools from algebraic dynamical systems.

Generally, multicyclic codes are defined as linear codes which are invariant under *multicyclic shifts* or, equivalently, ideals in the quotient-ring $\mathbb{F}_q[X_1, \ldots, X_r]/\langle X_1^{n_1} - 1, \ldots, X_r^{n_r} - 1\rangle$ and these ideals are the subsets having zeros from a certain subset ([1, 2, 5, 6]). The residue class $\overline{X}_\rho$ of X_ρ with respect to the ideal $\langle X_1^{n_1} - 1, \ldots, X_r^{n_r} - 1\rangle$ of $\mathbb{F}_q[X_1, \ldots, X_r]$ verifies $\overline{X}_\rho^{n_\rho} = 1$. Therefore, it may be viewed as an element of a certain group algebra. This leads to the introduction a group algebra instead of the quotient ring and allows the use of rich mathematics structures: the characterization the of ideals in this group algebras is an interesting and powerful tool for the study of multicyclic codes. Moreover, this way of constructing multicyclic codes is very suitable for computing with computer algebra systems.

This article is organized as follows:

In section 2, we introduce some theoretical background including results from Finite Fields Theory, Algebraic Dynamical Systems Theory, group algebras, Fourier and Wedderburn transforms with proofs.

In section 3, we present the problems and the methods which will be used to solve these problems.

In section 4, we present the results. We prove some properties of the group algebra, mainly Theorem 4.1, using notion from algebraic dynamical systems. This theorem is new. Next, we prove the injectivity of the Fourier transform, a well known result, stated in Proposition 2.14, using materials from the previous sections and from algebraic geometry. We then prove the Theorem 4.6, which characterizes the ideals in the group algebra $\mathbb{F}_q[x]$ and permits the definition and the construction of multicyclic codes. This result is usually stated without proof (for example in [1, 2]) as a characterization of multicyclic codes. We give a proof of this theory, within our framework. At the end, in Theorem 4.18, we give a characterization of the locator ideal. This theorem is new.

2 Preliminaries

2.1 Results from finite fields theory

Here, we prove directly some results from finite (or Galois) fields. The interested reader may consult [7, 8, 9].

Lemma 2.1. *Let $\mathbb{F}_Q$ be the finite field with Q elements (where Q is a power of a prime number). Let $d \in \mathbb{N}^*$ be a divisor of $Q-1$. Then there exists a unique element of order d in the multiplicative group $(\mathbb{F}_Q^*, \times)$.*

Proof. It is known that $(\mathbb{F}_Q^*, \times)$ is a cyclic group having $Q-1$ elements, so that there exists an element ω of order $Q-1$ in $\mathbb{F}_Q^*$. Let $k \in \mathbb{N}^*$ such that $Q-1 = dk$. Set $a = \omega^{\frac{Q-1}{d}}$. Then

$$a^d = (\omega^{\frac{Q-1}{d}})^d = w^{Q-1} = 1,$$

so that the order d' of a is less than or equal to d. Now, suppose that $d' < d$. Since $a^{d'} = 1$, i.e.

$$1 = (\omega^{\frac{Q-1}{d}})^{d'} = \omega^{d'k},$$

it is then necessary that the order $Q-1$ of ω verifies $Q-1 \leqslant d'k$. But we then have $Q-1 = dk \leqslant d'k$ which is impossible because $d > d'$. Hence, the order of a is exactly d.
Now, suppose that b is another element in $\mathbb{F}_Q^*$ of order d. There exits an integer h such that $0 \leqslant h \leqslant Q-2$ and $b = \omega^h$. Then $1 = b^d = \omega^{hd}$. Since ω is of order dk, we have $dk \mid hd$, so that there exists $l \in \mathbb{N}^*$ such that $hd = dkl$. We get $h = kl$, but this gives

$$b^d = \omega^{hd} = \omega^{dkl} = \omega^l = 1.$$

Therefore, the order dk of ω verifies $dk = Q-1 \leqslant l \leqslant h \leqslant Q-2$, which is impossible. Thus, a is the only element of order d. □

Corollary 2.2. *Let $n_1, \ldots, n_r \geqslant 1$ be integers, p a prime number such that p does not divide n_ρ for $\rho = 1, \ldots, r$, $q = p^m$ where $m \geqslant 1$ is an integer,*

$$\varepsilon = \operatorname{lcm}(n_1, \ldots, n_r)$$

and

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

Let α be a generator of the cyclic group $(\mathbb{F}_{q^t}^*, \times)$. Then, for $\rho = 1, \ldots, r$, the element $\xi_\rho = \alpha^{\frac{q^t-1}{n_\rho}}$ is an n_ρ-th primitive root of unity in $\mathbb{F}_{q^t}$.

Proof. Since ε and p are coprime, by Euler's theorem ([10]), , we have

$$p^{\varphi(\varepsilon)} \equiv 1 \ (\text{mod } \varepsilon),$$

where φ is the Euler's *totient function.* We also have $p^{m\varphi(\varepsilon)} \equiv 1 \equiv q^{\varphi(\varepsilon)}$, so that the set of integers $k \in \mathbb{N}^*$ which verify $q^k \equiv 1$ (mod ε) is not empty. This ensures the existence of t.

By Lemma 2.1 with $Q = q^t$ and $d = n_\rho$ for $\rho = 1, \ldots r$, the elements ξ_ρ's are of order n_ρ in $\mathbb{F}_{q^t}$, i.e. n_ρ- roots of unity.

If $\zeta \in \mathbb{F}_{q^t}$ is another n_ρ-th root of unity which is different from ξ_ρ, i.e. $\zeta^{n_\rho} = 1$, we can write

$$\zeta = \alpha^{\frac{q^t-1}{m}} \tag{2.1}$$

where m is the order of ζ. By Lemma 2.1, we have $m \neq n_\rho$. By the definition of the order, there exists $l \in \mathbb{N}^*$ such that $n_\rho = ml$, so that equation (2.1) then yields

$$\zeta = \alpha^{\frac{q^t-1}{n_\rho}l} = \xi_\rho^l.$$

We have shown that any root of unity is a power of ξ_ρ, i.e. ξ_ρ is indeed a primitive n_ρ-th root of unity. □

Remark 2.3. Note that Lemma 2.1 and Corollary 2.2 depend on the use of a generator of the cyclic group $(\mathbb{F}_Q^*, \times)$. In [9], there is an algorithm for finding a generator of $\mathbb{F}_Q^*$ when a factorization of $Q-1$ is known.

Notations. From now on, we fix integers $r, m, n_1, \dots, n_r \geqslant 1$ with $r \leqslant n_1 \cdots n_r$, a prime number p which does not divide any of the n_ρ's, $q = p^m$ and $\varepsilon = \operatorname{lcm}(n_1, \dots, n_r)$. The Galois field with q elements is denoted by $\mathbb{F}_q$. We will make use of the integer t defined by Corollary 2.2 and the elements ξ_ρ's.

Examples 2.4. (1) Case $r = 1$. Set $n_1 = n = 5, p = 2, q = p^2 = 4$. Then $\varepsilon = 5$ and

$$t = \min\{k \in \mathbb{N}^* \mid 4^k \equiv 1 \ (\mathrm{mod}\ 5)\} = 2,$$

so we have $\mathbb{F}_{q^t} = \mathbb{F}_{16}$, the Galois field with 16 elements. We know that

$$\mathbb{F}_{16} = \mathbb{F}_2[Z]/\langle Z^4 + Z + 1\rangle = \{aZ^3 + bZ^2 + cZ + 1 \mid a, b, c, d \in \mathbb{F}_2 = \{0, 1\}\},$$

and $\alpha = Z$ is a generator of $\mathbb{F}_{16}^*$, i.e of order 15. Then $\xi = \alpha^{\frac{15}{5}} = \alpha^3$ is a primitive 5th root of unity in $\mathbb{F}_{16}^*$.
(2) Case $r = 2$. Set $n_1 = 3, n_2 = 7, p = 2, q = p^2 = 4$. Then $\varepsilon = \operatorname{lcm}(3, 7) = 21$ and

$$t = \min\{k \in \mathbb{N}^* \mid 4^k \equiv 1 \ (\mathrm{mod}\ 21)\} = 3.$$

We then have $\mathbb{F}_{q^t} = \mathbb{F}_{64}$. Let α be a generator of $\mathbb{F}_{64}^*$, i.e. of order 63. Then $\xi_1 = \alpha^{\frac{63}{3}} = \alpha^{21}$ is a primitive 3rd root of unity in $\mathbb{F}_{16}^*$ and $\xi_2 = \alpha^{\frac{63}{7}} = \alpha^9$ a primitive 7th root of unity.
(3) Case $r = 3$. Set $n_1 = 3, n_2 = 5, n_3 = 7$ and $p = 2, q = p^2 = 4$. Then $\varepsilon = \operatorname{lcm}(3, 5, 7) = 105$ and

$$t = \min\{k \in \mathbb{N}^* \mid 4^k \equiv 1 \ (\mathrm{mod}\ 105)\} = 6.$$

Then $\mathbb{F}_{q^t} = \mathbb{F}_{4096}$. If α is a generator of $\mathbb{F}_{4096}^*$, i.e. an element of order 4095, then

$$\begin{aligned} \xi_1 &= \alpha^{\frac{4095}{3}} = \alpha^{1365}, \\ \xi_2 &= \alpha^{\frac{4095}{5}} = \alpha^{819}, \\ \xi_3 &= \alpha^{\frac{4095}{17}} = \alpha^{585} \end{aligned}$$

are respectively a 3rd, 5th and a 7th root of unity in $\mathbb{F}_{4096}$.

Notations. Throughout this document, we will use the following notations

$$\underline{\xi} = (\xi_1, \dots, \xi_\rho, \dots, \xi_r) \in \mathbb{F}_{q^t}^r \quad \text{and} \quad \xi = \xi_1 \cdots \xi_\rho \cdots \xi_r \in \mathbb{F}_{q^t}, \tag{2.2}$$

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

$$\underline{\xi}^h = (\xi_1^{h_1}, \dots, \xi_\rho^{h_\rho}, \dots, \xi_r^{h_r}) \in \mathbb{F}_{q^t}^r \quad \text{and} \quad \xi^h = \xi_1^{h_1} \cdots \xi_\rho^{h_\rho} \cdots \xi_r^{h_r} \in \mathbb{F}_{q^t}\,. \tag{2.3}$$

We will denote the Galois group $\mathrm{Gal}(\mathbb{F}_{q^t}, \mathbb{F}_q)$ by Γ :

$$\Gamma = \mathrm{Gal}(\mathbb{F}_{q^t}, \mathbb{F}_q) = \{\sigma^\nu \mid \nu = 0, \dots, t-1,\ \sigma^\nu : \mathbb{F}_{q^t} \longrightarrow \mathbb{F}_{q^t},\ \omega \longmapsto \omega^{q^\nu}\}. \tag{2.4}$$

It is the set automorphisms of $\mathbb{F}_{q^t}$ who fix all of the elements of $\mathbb{F}_q$ ([7]).

The abelian group $(\prod_{\rho=1}^r \mathbb{Z}/n_\rho\mathbb{Z}, +)$ will be denoted by $\mathcal{G}_+$. An element of $\mathcal{G}_+$ is then of the form $(g_1, \dots, g_\rho, \dots, g_r)$ with $g_\rho \in \mathbb{Z}/n_\rho\mathbb{Z}$ for $\rho = 1, \dots, r$.

Proposition 2.5 ([1, 11])**.** *The Galois group* Γ *operates on* $\mathcal{G}_+$.

Proof. Consider the following mapping :

$$\begin{aligned} \Gamma \times \prod_{\rho=1}^{r} \mathbb{Z}/n_\rho\mathbb{Z} &\longrightarrow \prod_{\rho=1}^{r} \mathbb{Z}/n_\rho\mathbb{Z} \\ (\sigma^\nu, g) &\longmapsto \sigma^\nu \cdot g = gq^\nu = (g_1q^\nu, \ldots, g_rq^\nu). \end{aligned} \tag{2.5}$$

For elements $\sigma^\mu, \sigma^\nu \in \Gamma$ and $g = (g_1, \ldots, g_r) \in \prod_{\rho=1}^{r} \mathbb{Z}/n_\rho\mathbb{Z}$, we have

$$\begin{aligned} \sigma^\mu \cdot (\sigma^\nu \cdot g) = \sigma^\mu \cdot (g_1q^\nu, \ldots, g_rq^\nu) &= ((g_1q^\nu)q^\mu, \ldots, (g_rq^\nu)q^\mu) \\ &= (g_1(q^\nu q^\mu), \ldots, g_r(q^\nu q^\mu)) \\ &= (g_1(q^{\nu+\mu}), \ldots, g_r(q^{\nu+\mu}) \\ &= \sigma^{\nu+\mu} \cdot g \\ &= (\sigma^\mu \circ \sigma^\nu) \cdot g. \end{aligned}$$

Moreover,

$$\mathrm{Id}_{\mathbb{F}_q^t} \cdot g = \sigma^0 \cdot q = g \cdot 1 = g,$$

so that equation (2.5) indeed defines an operation of Γ on $\mathcal{G}_+$.

The *orbits* are the sets $(\Gamma \cdot g)_{g \in \prod_{\rho=1}^{r} \mathbb{Z}/n_\rho\mathbb{Z}}$ with

$$\Gamma \cdot g = \{gq^\nu |\ \nu = 0, \ldots, t-1\}.$$

Let s be the number of the orbits and $S = \{1, \ldots, s\}$. We denote the orbits by $\mathcal{O}_1, \ldots, \mathcal{O}_i \ldots, \mathcal{O}_s$ and $|\mathcal{O}_i| = o_i$. We have the following properties :

$$\bigcup_{i=1}^{s} \mathcal{O}_i = \mathcal{G}_+, \quad \mathcal{O}_i \bigcap_{i \neq j} \mathcal{O}_j = \emptyset \quad \text{and} \quad \sum_{i \in S} o_i = |\,\mathcal{G}_+\,| = n. \tag{2.6}$$

For $i \in S$, let $h(i)$ be a representative of $\mathcal{O}_i$, i.e. $h(i) \in \mathcal{G}_+$ and

$$\mathcal{O}_i = \Gamma \cdot h(i) = \{h(i)q^\nu \mid \nu = 0, \ldots, t-1\}. \tag{2.7}$$

Proposition 2.6. *With the preceding notations, one has*

$$\mathcal{O}_i = \{h(i)q^\nu \mid \nu = 0, \ldots, o_i - 1\}. \tag{2.8}$$

Proof. Consider the *stabilizer* of $h(i)$:

$$\mathrm{Stab}(h(i)) = \{\sigma^\nu \in \Gamma \mid \sigma^\nu \cdot h(i) = h(i)\},$$

where the equality in the second set is with respect to the set $\mathcal{G}_+$. Let

$$\mu = \min\{\nu \mid \sigma^\nu \in \mathrm{Stab}(h(i))\}.$$

For $j > 1$, we have

$$\sigma^{\mu+j} \cdot h(i) = \sigma^j \cdot h(i),$$

so that

$$\mathcal{O}_i = \{\sigma^\nu \cdot h(i) \mid \nu = 0, \ldots, \mu - 1\}.$$

Hence $|\mathcal{O}_i| = \mu = o_i$. □

Examples 2.7. Take $p = q = r = 2, n_1 = n_2 = 3$. Then $\varepsilon = \mathrm{lcm}(3,3) = 3$ and

$$t = \min\{\ k \in \mathbb{N}^* \ \mid 2^k \equiv 1 \mod 3\ \} = 2.$$

Thus $\mathbb{F}_{q^t} = \mathbb{F}_4 = \mathbb{F}_2[Z]/\langle Z^4 + Z + 1\rangle = \{0, 1, Z, Z + 1\}$ and $\alpha = Z$ is a generator of $\mathbb{F}_4^*$, which is also a primitive 3rd root of unity. We can take $\xi_1 = \xi_2 = \alpha$. The Galois group Γ is

$$\begin{aligned}\Gamma = \mathrm{Gal}(\mathbb{F}_4, \mathbb{F}_2) &= \{\sigma^\nu : \mathbb{F}_4 \longrightarrow \mathbb{F}_4\ ,\ \omega \longmapsto \omega^{2^\nu}\ \nu = 0, 1\},\\ &= \{\mathrm{Id}_{\mathbb{F}_4}, \sigma\},\ \text{where } \sigma(\omega) = \omega^2 \text{ for } \omega \in \mathbb{F}_4,\end{aligned}$$

and

$$\mathcal{G}_+ = \mathbb{Z}/3\,\mathbb{Z} \times \mathbb{Z}/3\,\mathbb{Z} = \{(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2), (2, 0), (2, 1), (2, 2)\}.$$

For $(g_1, g_2) \in \mathcal{G}_+$, we have by equation (2.7)

$$\Gamma \cdot (g_1, g_2) = \{(g_1, g_2), (2g_1, 2g_2)\} \subset \mathbb{Z}/3\,\mathbb{Z} \times \mathbb{Z}/3\,\mathbb{Z}$$

so that

$$\begin{aligned}\Gamma \cdot (0, 0) &= \{(0, 0)\},\\ \Gamma \cdot (0, 1) &= \{(0, 1), (0, 2)\},\\ \Gamma \cdot (0, 2) &= \{(0, 2), (0, 1)\},\\ \Gamma \cdot (1, 0) &= \{(1, 0), (2, 0)\},\\ \Gamma \cdot (1, 1) &= \{(1, 1), (2, 2)\},\\ \Gamma \cdot (1, 2) &= \{(1, 2), (2, 1)\},\\ \Gamma \cdot (2, 0) &= \{(2, 0), (1, 0)\},\\ \Gamma \cdot (2, 1) &= \{(2, 1), (1, 2)\},\\ \Gamma \cdot (2, 2) &= \{(2, 2), (1, 1)\}.\end{aligned}$$

There are five orbits: $S = \{1, 2, 3, 4, 5\}$ and

$$\mathcal{O}_1 = \{(0, 0)\},\ \mathcal{O}_2 = \{(0, 1), (0, 2)\},\ \mathcal{O}_3 = \{(1, 0), (2, 0)\},\ \mathcal{O}_4 = \{(1, 1), (2, 2)\}, \mathcal{O}_5 = \{(1, 2), (2, 1)\}.$$

We may take as representatives of these orbits the following elements of $\mathcal{G}_+$:

$$h(1) = (0, 0),\ h(2) = (0, 1),\ h(3) = (1, 0),\ h(4) = (1, 1),\ h(5) = (1, 2).$$

2.2 Algebraic dynamical systems

In this section, we refer to [4, 12, 13, 14]. For categories and functors, we refer to [15].

Let $X_1, \ldots, X_r$ and $Y_1, \ldots, Y_r$ be distinct letters, which are the *variables*. For sake of simplicity, the letter X (resp. Y) will denote $X_1, \ldots, X_r$ (resp. $Y_1, \ldots, Y_r$). For $\alpha = (\alpha_1, \ldots, \alpha_r) \in \mathbb{N}^r$, we define X^α (resp. Y^α) by

$$X^\alpha = X_1^{\alpha_1} \cdots X_r^{\alpha_r} \text{ (resp. } Y^\alpha = Y_1^{\alpha_1} \cdots Y_r^{\alpha_r}).$$

Let $\mathbf{D} = \mathbb{F}_q[X_1, \ldots, X_r] = \mathbb{F}_q[X]$ be the $\mathbb{F}_q$-vector space of the polynomials with the r variables $X_1, \ldots, X_r$ and coefficients in $\mathbb{F}_q$. An element of $\mathbf{D}$ can be uniquely written as

$$d(X_1, \ldots, X_r) = d(X) = \sum_{\alpha \in \mathbb{N}^r} d_\alpha X^\alpha \quad \text{with} \quad d_\alpha \in \mathbb{F}_q \quad \text{for all } \alpha \in \mathbb{N}^r,$$

where $d_\alpha = 0$ except for a finite number of α's.

Let $\mathbf{A} = \mathbb{F}_q[[Y_1, \ldots, Y_r]] = \mathbb{F}_q[[Y]]$ be $\mathbb{F}_q$-vector space of the formal power series with the variables $Y_1, \ldots, Y_r$ and coefficients in $\mathbb{F}_q$. An element of $\mathbf{A}$ can be uniquely written as

$$W(Y_1, \ldots, Y_r) = W(Y) = \sum_{\alpha \in \mathbb{N}^r} W_\alpha Y^\alpha$$

where $W_\alpha \in \mathbb{F}_q$ for all $\alpha \in \mathbb{N}^r$.

For integers $k, l \geqslant 1$, the set of matrices with k rows and l columns with coefficients in $\mathbf{D}$ is denoted by $\mathbf{D}^{k,l}$. An element $R(X) \in \mathbf{D}^{k,l}$ is of the form

$$R(X) = (R_{ij}(X))_{1 \leqslant i \leqslant k, 1 \leqslant j \leqslant \ l}$$

where $R_{ij}(X) \in \mathbf{D}$ for $i = 1, \ldots, k$ and $j = 1, \ldots, l$. We will mainly use the sets $\mathbf{D}^{r,1}$ and $\mathbf{D}^{1,r}$. The notation $\mathbf{A}^l$ will be for the set of row column for power series in $\mathbf{A}$ with l rows.

Let Vect($\mathbb{F}$) be the category of the vector spaces over $\mathbb{F}_q$. For vector spaces $E, F \in$ Vect($\mathbb{F}$), the set of morphisms from E into F is $\mathbf{Hom}_\mathbb{F}(E, F)$, the set of linear mappings from E to F. We will use the functor

$$\begin{aligned} \mathbf{Hom}_\mathbb{F}(-, \mathbb{F}) : \mathrm{Vect}(\mathbb{F}) &\longrightarrow \mathrm{Vect}(\mathbb{F}) \\ E &\longmapsto \mathbf{Hom}_\mathbb{F}(E, \mathbb{F}) \\ (f : E \longrightarrow F) &\longmapsto \begin{cases} \mathbf{Hom}_\mathbb{F}(f, \mathbb{F}) : \mathbf{Hom}_\mathbb{F}(F, & \mathbb{F}) \longrightarrow \mathbf{Hom}_\mathbb{F}(E, \mathbb{F}) \\ & u \longmapsto u \circ f. \end{cases} \end{aligned} \tag{2.9}$$

The *adjoint* of a linear mapping $u \in \mathbf{Hom}_\mathbb{F}(E, F)$, is the linear mapping $\mathbf{Hom}_\mathbb{F}(u, \mathbb{F}) = u \circ f$.

The external operation of $\mathbf{D}$ on $\mathbf{A}$ is defined by

$$\begin{aligned} \mathbf{D} \times \mathbf{A} &\longrightarrow \mathbf{A} \\ (d(X), W(Y)) &\longmapsto d(X) \circ W(Y) = \sum_{\alpha \in \mathbb{N}^r} (\sum_{\beta \in \mathbb{N}^r} d_\beta W_{\alpha+\beta}) Y^\alpha. \end{aligned} \tag{2.10}$$

This operation provides $\mathbf{A}$ and $\mathbf{A}^h$ for all $h \geqslant 1$ with a $\mathbf{D}$-module structure by the external operation

$$\begin{aligned} \mathbf{D} \times \mathbf{A}^h &\longrightarrow \mathbf{A}^h \\ (d(X), (W(Y))_{j=1,\ldots,h}) &\longmapsto \sum_{j=1}^{h} d(X) \circ W_j(Y). \end{aligned} \tag{2.11}$$

We denote by $\mathbf{Mod}(\mathbf{D})$ the category of the $\mathbf{D}$-modules. For two elements $M, M' \in \mathbf{Mod}(\mathbf{D})$, the set of morphisms from M to M' is $\mathbf{Hom}_\mathbf{D}(M, M')$, the set of the $\mathbf{D}$-linear mappings from M to M'. The category $\mathbf{Modf}(\mathbf{D})$ is the subcategory of $\mathbf{Mod}(\mathbf{D})$ whose elements are the finitely generated $\mathbf{D}$-modules.

In [13], we proved that given $R(X) \in \mathbf{D}^{k,l}$, the mapping

$$\begin{aligned} R(X) : \mathbf{A}^l &\longrightarrow \mathbf{A}^k \\ W(Y) &\longmapsto R(X) \circ W(Y) \end{aligned} \tag{2.12}$$

with

$$R(X)\circ W(Y)=\begin{pmatrix}\sum_{j=1}^{l}R_{1j}(X)\circ W_j(Y)\\ \vdots\\ \sum_{j}^{l}R_{kj}(X)\circ W_j(Y)\end{pmatrix}$$
$$=\begin{pmatrix}\sum_{\rho\in\mathbb{N}^r}(\sum_{j=1}^{l}\sum_{\alpha\in\mathbb{N}^r}R_{1j\alpha}W_{j(\alpha+\rho)})Y^\rho\\ \vdots\\ \sum_{\rho\in\mathbb{N}^r}(\sum_{j=1}^{l}\sum_{\alpha\in\mathbb{N}^r}R_{ij\alpha}W_{j(\alpha+\rho)})Y^\rho\\ \vdots\\ \sum_{\rho\in\mathbb{N}^r}(\sum_{j=1}^{l}\sum_{\alpha\in\mathbb{N}^r}R_{kj\alpha}W_{j(\alpha+\rho)})Y^\rho\end{pmatrix}, \tag{2.13}$$

(where $R_i(X)=(R_{i1}(X),\dots,R_{il}(X))\in\mathbf{D}^{1,l}$ are the rows of $R(X)$, for $i=1,\dots,k$) is the adjoint of the $\mathbb{F}$-linear mapping

$$\begin{aligned}R(X)^T:\mathbf{D}^k&\longrightarrow\mathbf{D}^l\\ c(X)&\longmapsto c(X)\cdot R(X)\end{aligned}$$

(right multiplication by $R(X)$). Moreover, the mapping (2.12) is also a $\mathbf{D}$-linear mapping of $\mathbf{D}$-modules, the sets $\mathbf{D}^k$ and $\mathbf{D}^l$ being $\mathbf{D}$-modules by equation (2.11).

Now, we are ready to define *algebraic dynamical systems.*

Definition 2.8 ([4, 14])**.** An algebraic dynamical system (or simply a *system*) is a $\mathbf{D}$-submodule of $\mathbf{A}^l$ of the form

$$\boldsymbol{\mathcal{B}}=\operatorname{Ker}R(X)=\{W(Y)\in\mathbf{A}^l\mid R(X)\circ W(Y)=0\}$$

where $R(X)\in\mathbf{D}^{k,l}$ and also denotes the $\mathbf{D}$-linear mapping of $\mathbf{D}$-modules defined by equation (2.12).

We denote by $\mathbf{Syst(A)}$ the category of these systems. Let $\mathcal{S}$ be the *covariant* functor

$$\begin{aligned}\boldsymbol{\mathcal{S}}=\mathbf{Hom_D}(-,\mathbf{A}):\mathbf{Modf(D)}&\longrightarrow\mathbf{Syst(A)}\\ M&\longmapsto\mathbf{Hom_D}(M,\mathbf{A})\end{aligned} \tag{2.14}$$

and for $M,N\in\mathbf{Modf(D)}$,

$$(f:M\longrightarrow N)\longmapsto\left\{\begin{aligned}\mathbf{Hom_D}(f,\mathbf{A}):\mathbf{Hom_D}(N,\quad\mathbf{A})&\longrightarrow\mathbf{Hom_D}(M,\mathbf{A})\\ u&\longmapsto u\circ f.\end{aligned}\right.$$

It is a *categorical duality* ([14, 15]). As a consequence, a system $\boldsymbol{\mathcal{B}}\subset\mathbf{A}$ can be written as

$$\boldsymbol{\mathcal{B}}=\mathbf{Hom_D}(M,\mathbf{A}),$$

where $M\in\mathbf{Modf(D)}$, and an element $M\in\mathbf{Modf(D)}$ defines a system which is $\mathbf{Hom_D}(M,\mathbf{A})$. But every $M\in\mathbf{Modf(D)}$ can be uniquely written as a quotient of $\mathbf{D}$-modules $M=\mathbf{D}^k\,/\,\mathbf{D}^{1,k}\,R(X)$ where $R(X)$ is a matrix of $\mathbf{D}^{k,l}$. We then have

$$\begin{aligned}\boldsymbol{\mathcal{B}}=\mathbf{Hom_D}(\mathbf{D}^k\,/\,\mathbf{D}^{1,k}\,R(X),\mathbf{A})&=\operatorname{Ker}R(X)\\ &=\{W(Y)\in\mathbf{A}^l\mid R(X)\circ W(Y)=0\},\end{aligned} \tag{2.15}$$

([4, 14]).

For a subset P (resp Q) of $\mathbf{D}^{1,l}$ (resp. $\mathbf{A}^l$), we define its *orthogonal* by

$$\begin{aligned} P^{\perp} &= \{W(Y) \in \mathbf{A}^l \mid d(X) \circ W(Y) = 0 \text{ for } d(X) \in P\} \subset \mathbf{A}^l \\ (\text{resp. } Q^{\perp} &= \{d(X) \in \mathbf{D}^{1,l} \mid d(X) \circ W(Y) = 0 \text{ for } W(Y) \in \mathbf{A}^l\} \subset \mathbf{D}^{1,l}). \end{aligned} \tag{2.16}$$

2.3 The group algebra $\mathbb{F}_q[x]$

In this section, we mainly refer to [4, 11, 16, 17].

Let $(\mathcal{G}, \cdot)$ be a finite commutative group, which is a direct product of cyclic groups generated by elements x_ρ of order n_ρ for $\rho = 1, \ldots, r$:

$$\mathcal{G} = \prod_{\rho=1}^{r} \langle x_\rho \rangle.$$

An element of $\mathcal{G}$ is of the form $x_1^{g_1} \cdots x_r^{g_r}$, where $(g_1, \ldots, g_r) \in \mathbb{Z}^r$.

An element of $\mathcal{G}$ id of the form $x_1^{g_1} \cdots x_r^{g_r}$, where $(g_1, \ldots, g_r) \in \mathcal{G}_+$. Writing $x = (x_1, \ldots, x_r)$, we have the following groups isomorphism

$$\begin{aligned} \mathcal{G}_+ &\longrightarrow \mathcal{G} \\ g = (g_1, \ldots, g_r) &\longmapsto x^g = x_1^{g_1} \cdots x_r^{g_r}. \end{aligned} \tag{2.17}$$

Definition 2.9 ([4, 11, 17])**.** The group algebra $\mathbb{F}_q[\mathcal{G}_+] = \mathbb{F}_q[\mathcal{G}]$ is the $\mathbb{F}_q$-vector space of formal sums

$$\begin{aligned} \mathbb{F}_q[x] &= \{\sum_{g \in \mathcal{G}} a_g g \mid a_g \in \mathbb{F}_q \quad \text{for} \quad g \in \mathcal{G}\} \\ &= \{a(x) = \sum_{g \in \mathcal{G}_+} a_g x^g \mid a_g \in \mathbb{F}_q \quad \text{for} \quad g \in \mathcal{G}_+\}, \end{aligned} \tag{2.18}$$

with the multiplication, denoted by $*$ and defined by

$$a(x) * a'(x) = \sum_{k \in \mathcal{G}_+} (\sum_{g \in \mathcal{G}_+} a_g a'_{k-g}) x^k. \tag{2.19}$$

As an $\mathbb{F}_q$-vector space, a basis of $\mathbb{F}_q[x]$ is the set $\{x^g \mid g \in \mathcal{G}_+\}$ and with the multiplication (2.19), it becomes an $\mathbb{F}_q[x]$ algebra. We then have the following result:

Proposition 2.10. *The group algebra $\mathbb{F}_q[x]$ is an $\mathbb{F}_q$-vector space of dimension n and also an $\mathbb{F}_q$-algebra.*

We will also need the variables y_ρ and y, defined by

$$y_\rho = x_\rho^{-1} \quad \text{for} \quad \rho = 1, \ldots, r, \quad y = (y_1, \ldots, y_r).$$

This leads to the following identification

$$\mathbb{F}_q[x] = \mathbb{F}_q[y] = \{b(y) = \sum_{g \in \mathcal{G}_+} a_g y^g \mid a_g \in \mathbb{F}_q \quad \text{for} \quad g \in \mathcal{G}_+\}.$$

Notations. Let $c(x) = \sum_{g \in \mathcal{G}_+} c_g x^g \in \mathbb{F}_q[x]$. For $h = (h_1, \ldots, h_r)$ in $\mathcal{G}_+$, we denote by $c(\underline{\xi}^h)$ the element defined by

$$c(\underline{\xi}^h) = \sum_{g \in \mathcal{G}_+} c_g \xi^{hg} = \sum_{g \in \mathcal{G}_+} c_g \xi_1^{h_1 g_1} \cdots \xi_r^{h_r g_r} \in \mathbb{F}_{q^t}. \tag{2.20}$$

We end this section by the following proposition :

Proposition 2.11. *Let $c(x) \in \mathbb{F}_q[x]$ and $i \in S$ such that $c(\underline{\xi}^{(h(i)}) = 0$. Then $c(\underline{\xi}^h) = 0$ for $h \in \mathcal{O}_i$.*

Proof. Under the assumption of the proposition, let $h \in \mathcal{O}_i$. Then there exists en element $\sigma^\nu \in \Gamma$ such that $h = \sigma^\nu \cdot h(i) = h(i)q^\nu$. Now, write $c(x) = \sum_{g \in \mathcal{G}_+} c_g x^g$. Then, using the fact that σ^ν belongs to $\mathrm{Gal}(\mathbb{F}_{q^t}, \mathbb{F}_q)$, we have

$$\begin{aligned}
0 = \sigma^\nu(c(\underline{\xi}^{h(i)})) &= \sigma^\nu(\sum_{g\in\mathcal{G}_+} c_g \xi^{h(i)g}) = \sigma^\nu(\sum_{g\in\mathcal{G}_+} c_g \xi_1^{h(i)_1 g_1} \cdots \xi_r^{h(i)_r g_r})\\
&= \sum_{g\in\mathcal{G}_+} \sigma^\nu(c_g)\sigma^\nu(\xi_1^{h(i)_1 g_1}) \cdots \sigma^\nu(\xi_r^{h(i)_r g_r})\\
&= \sum_{g\in\mathcal{G}_+} c_g \xi_1^{h(i)_1 g_1 q^\nu} \cdots \xi_r^{h(i)_r g_r q^\nu}\\
&= \sum_{g\in\mathcal{G}_+} c_g (\xi^{(h(i)q^\nu})\\
&= \sum_{g\in\mathcal{G}_+} c_g \xi^h\\
&= c(\underline{\xi}^h). \quad \square
\end{aligned}$$

2.4 The discrete fourier transform

In this subsection, we will mainly refer to [4, 11, 16, 17, 18].

Definition 2.12 (Characters, [16, 17])**.** The *characters* are the mapping $(\chi_h)_{h\in\mathcal{G}_+}$ defined by

$$\begin{aligned}
\chi_h &: \mathcal{G} \longrightarrow \mathbb{F}_{q^t}\\
x_1^{g_1} \cdots x_r^{g_r} &\longmapsto \xi_1^{g_1 h_1} \cdots \xi_r^{g_r h_r} = \xi^{gh},
\end{aligned}$$

where $gh = (g_1h_1, \ldots, g_rh_r)$.

Extending all the χ_h on $\mathbb{F}_q[\mathcal{G}]$ by linearity, we have the mappings, again denoted by χ_h for $h \in \mathcal{G}_+$, defined by

$$\begin{aligned}
\chi_h &: \mathbb{F}_q[x] \longrightarrow \mathbb{F}_{q^t}\\
\sum_{g\in\mathcal{G}_+} a_g x^g &\longmapsto a(\underline{\xi}^h) = \sum_{g\in\mathcal{G}_+} a_g \chi_h(x^g) = \sum_{g\in\mathcal{G}_+} a_g \xi_1^{g_1 h_1} \cdots \xi_r^{g_r h_r} = \sum_{g\in\mathcal{G}_+} a_g \xi^{gh}.
\end{aligned} \tag{2.21}$$

Taking all the χ_h for all $h \in \mathcal{G}_+$, we have the *discrete Fourier transform.*

Definition 2.13 ([17])**.** The **discrete Fourier transform (DFT)** is the mapping

$$\begin{aligned}
\mathrm{DFT} = \Phi &: \mathbb{F}_q[x] \longrightarrow \mathbb{F}_{q^t}[y]\\
a(x) = \sum_{g\in\mathcal{G}_+} a_g x^g &\longmapsto \Phi(a(x)) = \sum_{h\in\mathcal{G}_+} (\sum_{g\in\mathcal{G}_+} a_g \xi^{gh}) y^h = \sum_{h\in\mathcal{G}_+} a(\underline{\xi}^h) y^h.
\end{aligned}$$

Proposition 2.14. *The discrete Fourier transform* DFT *is an injective homomorphism of vector spaces.*

We will give a proof of this proposition in section 4.

Corollary 2.15. *Let $a(x) \in \mathbb{F}_q[x]$ such that $a(\underline{\xi}^{h(i)}) = 0$ for $i \in S$. Then $a(x) = 0$.*

Proof. We know by Proposition 2.11 that if $a(\underline{\xi}^{h(i)}) = 0$, then $a(\underline{\xi}^h) = 0$ for $h \in \mathcal{O}_i$. Using the hypothesis, we have $a(\underline{\xi}^h) = 0$ for $h \in \bigcup_{i=1}^s \mathcal{O}_i$, which is equal to $\mathcal{G}_+$. Thus $\Phi(a(x)) = 0$ and using the injectivity of the DFT, we have $a(x) = 0$. □

The DFT is not surjective ([4, 11, 17]).

2.5 The wedderburn transform

Lemma 2.16. *For $i \in S$, the following inequalities holds:*

$$\xi_\rho^{h(i)_\rho q^{o_i}} = \xi_\rho^{h(i)_\rho} \text{ for } \rho = 1, \ldots, r.$$

Proof. Write $h(i) = (h(i)_1, \ldots, h(i)_\rho)$. In the proof of Proposition 2.6, we showed that σ^{o_i} belongs to $\mathrm{Stab}(h(i))$, i.e. $\sigma^{o_i} \cdot h(i) = h(i)q^{o_i} = h(i)$, which means that for $\rho = 1, \ldots, r$, there exists $k_\rho \in \mathbb{Z}$ such that

$$h(i)_\rho q^{o_i} - h(i)_\rho = k_\rho n_\rho.$$

Therefore

$$\xi_\rho^{h(i)_\rho q^{o_i} - h(i)_\rho} = (\xi_\rho)^{k_\rho n_\rho} = (\xi_\rho^{n_\rho})^{k_\rho} = 1,$$

since ξ_ρ is a n_ρ-th root of unity. This gives the result. □

Corollary 2.16 means that for $i \in S$ and $\rho = 1, \ldots r$, the element $\xi_\rho^{h(i)_\rho q^{o_i}}$ belongs to the Galois field $K_i = \mathbb{F}_{q^{o_i}}$. Therefore, for $a(x) \in \mathbb{F}_q[x]$, the element $a(\underline{\xi}^{h(i)})$ also belongs to K_i. This leads to the *Wedderburn transform.*

Definition 2.17 ([4, 11, 17])**.** The *Wedderburn transform* is defined by

$$\begin{aligned} W : \mathbb{F}_q[x] &\longrightarrow \prod_{i \in S} K_i \\ a(x) &\longmapsto (\chi_{(h(i)}(a(x))_{i \in S} = (a(\underline{\xi}^{h(i)}))_{i \in S}. \end{aligned}$$

Theorem 2.18 ([4, 11])**.** *The Wedderburn transform is an isomorphism of the $\mathbb{F}_q$-algebra $(\mathbb{F}_q[x], +, *)$ onto the $\mathbb{F}_q$-algebra $(\prod_{i \in S} K_i, +, \bullet)$, where $\bullet$ is the coordinatewise multiplication.*

Proof. It is clear that W is a homomorphism of $\mathbb{F}_q$- algebras. Now, if $a(x) \in \mathbb{F}_q[x]$ and $a(\underline{\xi}^{h(i)}) = 0$ for $i \in S$, then, by Corollary 2.15, $a(x) = 0$, hence W is injective. But, as vector spaces over $\mathbb{F}_q$, we have $\dim \mathbb{F}_q[x] = n = \sum_{i=1}^{s} o_i = \dim \prod_{i \in S} K_i$, so that W is indeed an isomorphism. □

3 Problems and Methods

Our goal is to define and construct multidimensional code of any cyclic dimension (limited by the capacity of computing only) and to define and characterize the syndrome of the error. The construction must allow the theoretical study of these code and to give computational examples. More precisely, we want to replace the abstract quotient ring $\mathbb{F}_q[X_1, \ldots, X_r]/\langle X_1^{n_1} - 1, \ldots, X_r^{n_1} - 1\rangle$ by another isomorphic object whose structure is more convenient both for theoretical and practical (mainly computational) studies.

For this purpose, starting from the fact that $\overline{X}_\rho^{n_\rho} - 1 = 0$, where $\overline{X}_\rho$ is the residue class of X_ρ modulo the ideal $\langle X_1^{n_1} - 1, \ldots, X_\rho^{n_\rho} - 1\rangle$, and since the quotient ring is generated by $\{\overline{X}_1, \ldots, \overline{X}_r\}$, we replace the quotient ring by a group algebra of the form $\mathbb{F}_q[x_1, \ldots, x_r]$ where the x_ρ's are elements of an abelian group and verify $x_\rho^{n_\rho} = 1$. We use the DFT and the Wedderburn transform to study the structure of the group algebra and its ideals.

Remarking that the variables x_ρ are invertible, we can construct another group algebra, namely $\mathbb{F}_q[y_1, \ldots, y_r]$ and represent the DFT of the elements of $\mathbb{F}_q[x_1, \ldots, x_r]$ as polynomials in the y_ρ's (with coefficients in an extension of $\mathbb{F}_q$). This situation is very similar to that of the theory of algebraic dynamical systems which makes use of the polynomial ring $\mathbf{D} = \mathbb{F}_q[X_1, \ldots, X_r]$ and those of the formal power series $= \mathbb{F}_q[[Y_1, \ldots, Y_r]]$. We then look for relations between these mathematical objets and use notion from algebraical dynamical systems theory, which are the orthogonals to redefine and generalize a notion which are used in the one-dimensional case.

4 Solution of the Problems

4.1 The group algebras $\mathbb{F}_q[x], \mathbb{F}_q[y]$ and dynamical systems

In this subsection, we are going to prove the following theorem :

Theorem 4.1. *The group algebras* $\mathbb{F}_q[x], \mathbb{F}_q[y]$ *are* $\mathbf{D}$*-isomorphic algebraic dynamical systems with the* $\mathbf{D}$*-isomorphisms*

$$\mathbf{Hom_D}(\mathbb{F}_q[x], \mathbf{A}) \cong \mathbb{F}_q[y] \cong S \tag{4.1}$$

and

$$\mathbf{Hom_D}(\mathbb{F}_q[y], \mathbf{A}) \cong \mathbb{F}_q[x] \cong S, \tag{4.2}$$

where $S = \boldsymbol{\mathcal{S}}(M)$ *with* $M = \mathbf{D} \,/\langle X_1^{n_1} - 1, \ldots, X_r^{n_r} - 1\rangle$.

Let $R(X)$ be the matrix defined by

$$R(X) = \begin{pmatrix} X_1^{n_1} \; - \; 1 \\ \vdots \\ X_r^{n_r} \; - \; 1 \end{pmatrix} \in \mathbf{D}^{r,1}\,.$$

Recall that $\mathbf{D} = \mathbb{F}_q[X_1, \ldots, X_r]$, according to our notations in subsection 2.2. The polynomial ideal in $\mathbf{D}$, generated by the rows of the matrix $R(X)$ is

$$\mathbf{D}^{1,r}\, R(X) = \langle X_1^{n_1} - 1, \ldots, X_r^{n_r} - 1\rangle.$$

An element of the $\mathbf{D}$-module

$$M = \mathbf{D} \,/\, \mathbf{D}^{1,r}\, R(X) = \mathbf{D} \,/\langle X_1^{n_1} - 1, \ldots, X_r^{n_r} - 1\rangle \tag{4.3}$$

is of the form $\overline{d(X)}$, where $d(X) \in \mathbf{D}$ and $\overline{d(X)} = d(X) + \mathbf{D}^{1,r}\, R(X)$ the *residue class* of $d(X)$ modulo $\mathbf{D}^{1,r}\, R(X)$.

Fix a total ordering on $\mathbb{N}^r$, for example the *lexicographical order* $\leqslant_{\text{lex}}$. For $d(X) \in \mathbf{D}$, by the division algorithm of $d(X)$ by $X^{n_\rho} \; - \; 1,\ \rho = 1, \ldots r$ ([19]), we can write

$$d(X) = \sum_{\rho=1}^{r} q_\rho(X_\rho)(X_\rho^{n_\rho} \; - \; 1) \; + \; r(X) \tag{4.4}$$

with $q_\rho, r(X) \in \mathbf{D}$ for $\rho = 1, \ldots, r$ such that

$$r(X) = \sum_{g \in \mathcal{G}_+} r_g X^g, \tag{4.5}$$

where none of the monomial in $r(X)$ is divisible by any of the $X_\rho^{n_\rho}$ for $\rho = 1, \ldots r$. We then have $\overline{d(X)} = \overline{r(X)}$ and this gives the $\mathbb{F}$-isomorphism

$$\begin{aligned} M &\longrightarrow \mathbb{F}_q[x] \\ \overline{d(X)} &\longmapsto r(x) = \sum_{g \in \mathcal{G}_+} r_g x^g. \end{aligned} \tag{4.6}$$

By the canonical projection

$$\mathbf{D} \longrightarrow M,$$

and by equation (4.6), we also have an onto linear mapping

$$\begin{aligned} \mathbf{D} &\longrightarrow \mathbb{F}_q[x] \\ d(X) &\longmapsto r(x) = \sum_{g\in\mathcal{G}_+} r_g x^g. \end{aligned} \tag{4.7}$$

Thus we have a one-to-one correspondence between ideals $\boldsymbol{I}$ of $\mathbb{F}_q[x]$ and the ideals $\boldsymbol{J}$ of $\mathbf{D}$ containing $\mathbf{D}^r\, R(X)$. This correspondence comes from the inequality

$$\boldsymbol{I} = \overline{\boldsymbol{J}}$$

where the residue class is with respect to $\mathbf{D}^r\, R(X)$.

The set $\mathbb{F}_q[x]$ is provided with a $\mathbf{D}$-module structure by the external operation

$$\begin{aligned} \mathbf{D}\times\mathbb{F}_q[x] &\longrightarrow \mathbb{F}_q[x] \\ (d(X), a(x)) &\longmapsto r(x) * a(x), \end{aligned} \tag{4.8}$$

so that equation (4.6) becomes a $\mathbf{D}$-isomorphism of $\mathbf{D}$-modules.

Similarly, $\mathbb{F}_q[y]$ becomes a $\mathbf{D}$-module too, by the external operation

$$\begin{aligned} \mathbf{D}\times\mathbb{F}_q[y] &\longrightarrow \mathbb{F}_q[y] \\ (d(X), b(y)) &\longmapsto r(y) * b(y) = \sum_{k\in\mathcal{G}_+} (\sum_{g\in\mathcal{G}_+} r_g b_{g+k}) y^k, \end{aligned} \tag{4.9}$$

so that we have the following $\mathbf{D}$-isomorphim of $\mathbf{D}$-modules, similar to equation (4.6) :

$$\begin{aligned} M &\longrightarrow \mathbb{F}_q[y] \\ \overline{d(X)} &\longmapsto r(y) = \sum_{g\in\mathcal{G}_+} r_g x^g. \end{aligned} \tag{4.10}$$

For the proof of the Proposition 4.1. We need the following lemma:

Lemma 4.2. *One has the* $\mathbf{D}$*-isomorphism*

$$\begin{aligned} \varrho : S = \boldsymbol{\mathcal{S}}(M) &\longrightarrow \mathbb{F}_q[y] \\ \sum_{\alpha\in\mathbb{N}^r} W_\alpha Y^\alpha &\longmapsto \sum_{\alpha\in\mathcal{G}_+} W_\alpha y^\alpha. \end{aligned} \tag{4.11}$$

Proof. Applying the functor $\boldsymbol{\mathcal{S}} = \mathbf{Hom}_{\mathbf{D}}(-, \mathbf{A})$ to the $\mathbf{D}$-module M in equation (4.3), we have, by equation (2.15),

$$\begin{aligned} \boldsymbol{\mathcal{S}}(M) = S &= \{W(Y) \in \mathbf{A} \mid R(X_1, \ldots, X_r) \circ W(Y) = 0\} \\ &= \{W(Y) \in \mathbf{A} \mid (X_\rho^{n_\rho} - 1) \circ W(Y) = 0 \quad \text{for} \quad \rho = 1, \ldots, r\}, \end{aligned}$$

which is the $\mathbf{D}$-submodule of $\mathbf{A}$ consisting of the powers series $W(Y)$ which are $(n_1, \ldots, n_r)$-periodic. Indeed, if $W(Y) = \sum_{\alpha\in\mathbb{N}^r} W_\alpha Y^\alpha$, then, by equation (2.10)

$$\begin{aligned} (X_\rho^{n_\rho} - 1) \circ W(Y) &= \sum_{\alpha\in\mathbb{N}^r} W_{\alpha_1\ldots\alpha_\rho+n_\rho\ldots\alpha_r} Y^\alpha - W(Y) \\ &= \sum_{\alpha\in\mathbb{N}^r} (W_{\alpha_1\ldots\alpha_\rho+n_\rho\ldots\alpha_r} - W_{\alpha_1\ldots\alpha_\rho\ldots\alpha_r}) Y^\alpha. \end{aligned}$$

Therefore, $(X_\rho^{n_\rho} - 1) \circ W(Y) = 0$ yields

$$W_{\alpha_1 \ldots \alpha_\rho + n_\rho \ldots \alpha_r} = W_{\alpha_1 \ldots \alpha_\rho \ldots \alpha_r}$$

for $\rho = 1, \ldots, r$. This means that $W(Y)$ is completely determined by W_α where $\alpha_\rho \in \mathbb{Z}/n_\rho\mathbb{Z}$ for $\rho = 1, \ldots, r$, i.e for $\alpha \in \mathcal{G}_+$. □

We have seen the proof of the following corollary in the proof of Lemma 4.11:

Corollary 4.3. *As a* $\mathbf{D}$*-module (and an algebraic dynamical system),* $\mathbb{F}_q[y]$ *is isomorphic to the* $\mathbf{D}$*-modules of series of* $\mathbf{A} = \mathbb{F}_q[[Y_1, \ldots, Y_r]]$ *which are* $(n_1, \ldots, n_r)$*-periodic.*

Proof of Theorem 4.1. By Lemma 4.2 (and also equation (2.14)), $\mathbb{F}_q[y]$ is an algebraic dynamical system. The same applies to $\mathbb{F}_q[x]$. Applying the exact functor $\boldsymbol{\mathcal{S}}$ to equation (4.6), we have

$$S = \boldsymbol{\mathcal{S}}(M) \cong \boldsymbol{\mathcal{S}}(\mathbb{F}_q[x]) = \mathbf{Hom}_{\mathbf{D}}(\mathbb{F}_q[x], \mathbf{A}),$$

and the isomorphism in Lemma 4.2 gives the isomorphism in equation (4.1). The same method proves the isomorphism in equation (4.2). Since both $\mathbb{F}_q[x]$ and $\mathbb{F}_q[y]$ are isomorphic to S, they are isomorphic. □

Definition 4.4. Let $A \subset \mathbb{F}_q[x]$ and $B \subset \mathbb{F}_q[y]$. The *orthogonals* of these sets are

$$A^\perp = \{b(y) \in \mathbb{F}_q[y] \mid a(x) * b(y) = 0 \ \ \forall\, a(x) \in A\}, \tag{4.12}$$
$$B^\perp = \{a(x) \in \mathbb{F}_q[x] \mid a(x) * b(y) = 0 \ \ \forall\, b(y) \in B\}$$

(compare with equation (2.16)).

The set $A^\perp$ is then a $\mathbf{D}$-submodule of $\mathbb{F}_q[y]$ and the set $B^\perp$ is a $\mathbf{D}$-submodule of $\mathbb{F}_q[x]$.

4.2 Injectivity of the discrete Fourier transform

Proof of Proposition 2.14. We will use the following lemma from algebraic geometry :

Lemma 4.5 ([20])**.** *Let* $\mathbb{K}$ *be a field,* $r \geqslant 2$ *an integer,* $V = \{P_1, \ldots, P_r\}$ *a finite set of points in* $\mathbb{K}^r$*. Then there exists a polynomial* F *of* $\mathbb{K}[X_1, \ldots, X_r]$ *such that*

$$F(P_1) = 1 \ \textit{and} \ F(P_i) = 0 \ \textit{for} \ i \neq 1.$$

Now we get back to the proposition. Let $a(x) \in \mathbb{F}_q[x]$ such that $(\Phi a)(y) = 0 = \sum_h A_h y^h$, i.e $A_h = a(\underline{\xi}^h) = 0$ for all $h \in \mathcal{G}_+$. Since by our assumption (see the notations in subsection 2.1), $r \leqslant n_1 \cdots n_r = |\,\mathcal{G}_+|$, we can choose r distinct points $\xi^{g(0)}, \ldots, \xi^{g(r-1)}$ in $\mathbb{F}_{q^t}^r$. From Lemma 4.5, there exists an element $B(X) = \sum_{h \in \mathbb{N}^r} B_h X^h \in \mathbb{F}_{q^t}[X_1, \ldots, X_r]$ (where the sum is finite) such that,

$$B(\underline{\xi}^{g(\rho)}) = \sum_{h \in \mathbb{N}^r} B_h \xi^{g(\rho) h} = \begin{cases} 0 & \text{if } \rho = 0, \\ 1 & \text{if } \rho \neq 0. \end{cases} \tag{4.13}$$

Since ξ_ρ is a n_ρ-th root of unity for $\rho = 1, \ldots, r$, equation (4.13) suggests that by reducing the exponents h of the variable X in the expression of $B(X)$ and also the indices h of the coefficients in the group $\mathcal{G}_+ = \prod_{\rho=1}^r \mathbb{Z}/n_\rho\mathbb{Z}$, we may suppose that $B(X)$ is of the form $B(X) = \sum_{h \in \mathcal{G}_+} B_h X^h$ or even an element of $\mathbb{F}_q[x]$, i.e. of the form

$$B(x) = \sum_h B_h x^h,$$

where the indices h belong to $\mathcal{G}_+$. Then equation (4.13) can be written as

$$B(\underline{\xi}^{g(\rho)}) = \sum_h B_h \xi^{g(\rho)h} = \begin{cases} 0 & \text{if } \rho = 0, \\ 1 & \text{if } \rho \neq 0. \end{cases}$$

It follows that

$$\begin{aligned} 0 = \sum_h A_h = \sum_h B_h A_h &= \sum_h B_h \big(\sum_\rho a_{g(\rho)} \xi^{g(\rho)h}\big) \\ &= \sum_\rho a_\rho \sum_h B_h \xi^{g(\rho)} = a_{g^{(0)}} B(\underline{\xi}^{g^{(0)}}) = a_{g^{(0)}}. \end{aligned}$$

Since this holds for all $g^{(0)} \in \mathcal{G}_+$, we have $a = 0$. □

4.3 Ideals in $\mathbb{F}_q[x]$

Theorem 4.6 (Ideals in $\mathbb{F}_q[x]$)**.** *A set* $\boldsymbol{I}$ *is an ideal of* $\mathbb{F}_q[x]$ *if and only if there exists a subset* Z *of* S *such that*

$$\boldsymbol{I} = \{a(x) \in \mathbb{F}_q[x] \mid a(\underline{\xi}^{h(i)}) = 0 \;\forall i \in Z\}. \tag{4.14}$$

Proof. It is clear that the set on the right hand side of equation (4.14) is an ideal of $\mathbb{F}_q[x]$. For the converse, we make use of Theorem 2.18 : let $\boldsymbol{I}$ be an ideal of $\mathbb{F}_q[x]$. Then $W(\boldsymbol{I})$ is an ideal of $K = \prod_{i=1}^s K_i$, which is of the form $\prod_{i=1}^s I_i$, where I_i is an ideal of K_i, hence equal to $\{0\}$ or K_i since K_i is a field, for $i = 1, \ldots, s$. Let

$$Z = \{i \in \{1, \ldots, s\} \mid I_i = \{0\}\}.$$

If $Z = \emptyset$, then $W(\boldsymbol{I}) = K$ and $\boldsymbol{I} = \mathbb{F}_q[x]$. If $Z \neq \emptyset$, then

$$W(\boldsymbol{I}) = \prod_{i=1}^s I_i \text{ where and } I_i = \{0\} \text{ whenever } i \in Z \text{ and } I_i = K_i \text{ otherwise.}$$

We will show that

$$\boldsymbol{I} = \{a(x) \in \mathbb{F}_q[x] \mid a(\underline{\xi}^{h(i)}) = 0 \;\forall i \in Z\}. \tag{4.15}$$

Let $a(x) \in \boldsymbol{I}$ and $i \in Z$. Since $a(\underline{\xi}^{(h(i)}) \in I_i$, we have $a(\underline{\xi}^{(h(i)}) = 0$. Thus $\boldsymbol{I}$ is a subset of the set at the right hand of equation (4.15). Conversely, if $a(x) \in \mathbb{F}_q[x]$ is such that $a(\underline{\xi}^{(h(i)}) = 0$ for $i \in Z$, then $a(\underline{\xi}^{(h(i)}) \in I_i = \{0\}$ for $i \in Z$. Thus $W(a(x)) \in \prod_{i=1}^s I_i = W(\boldsymbol{I})$. It follows that $a(x) \in \boldsymbol{I}$, since W is injective. Hence the two sets at the left and at the right hand side of the equality in equation (4.15) are equal. □

Corollary 4.7. *Let* $Z \subset S$. *Let* I_Z *be the ideal of* $\mathbb{F}_q[x]$ *defined by* Z, *i.e. of the form* (4.14). *Then*
(1) $I_\emptyset = \mathbb{F}_q[x]$,
(2) $I_S = \{0\}$,
(3) *if* $\emptyset \neq Z \neq S$, *then* $\{0\} \neq I_Z \neq \mathbb{F}_q[x]$.

Proof. (1) Already seen with the proof of Proposition 4.6.
(2) Let $c(x) \in I$. Then $c(\underline{\xi}^{(h(i)}) = 0$ for $i \in S$. By Corollary 2.15, we have $c(x) = 0$.
(3) If $I_Z = \mathbb{F}_q[x]$, then $a(\underline{\xi}^{h(i)}) = 0$ for $a(x) \in \mathbb{F}_q[x]$ and $i \in Z$, which is, of course false. Thus $I_Z \neq \mathbb{F}_q[x]$. Now, write $W(I_Z) = \prod_{i=1}^s I_i$. Then $W(I_Z) \neq K$, otherwise $I_Z = \mathbb{F}_q[x]$, since W is bijective. Therefore, there exists $i \in S$ such that $I_i = \{0\}$. Let $u = (u_i)_{i \in S}$ such that $u_i = 1$ if

$I_i \neq \{0\}$ and $u_i = 1$ if $I_i = \{0\}$. Then $0 \neq u \in W(I_Z)$ and since W is bijective, we have that $0 \neq W^{-1}(u) \in I_Z$. Hence $\emptyset \neq I_Z$ and this proves all the properties. □

By Corollary 4.7, given a subset Z of S, we can always construct the ideal I_Z and it is non trivial if and only if Z is a non trivial subset of S. In other words, a method to construct an ideal I of $\mathbb{F}_q[x]$ is simply to give a subset Z of S and take $I = I_Z$.

4.4 Multicyclic codes

Usually, a cyclic code is defined as a linear code having the *cyclic shifts* invariance property. Here, we are going to present cyclic codes, using the group algebra $\mathbb{F}_q[x]$ and then find these proprieties.

Definition 4.8. A *multicyclic code* is an ideal of $\mathbb{F}_q[x]$.

Notation. From now on, the letter $\boldsymbol{\mathcal{C}}$ will denote a multicyclic code.

Terminology. The integer r is called the *cyclic dimension* of $\boldsymbol{\mathcal{C}}$ and we say that $\boldsymbol{\mathcal{C}}$ is an r-dimensional (or r-D) cyclic code.

Being an ideal of $\mathbb{F}_q[x]$, $\boldsymbol{\mathcal{C}}$ is linear and has the propriety of *cyclic shifts* invariance property :

$$x^g * c(x) \in \boldsymbol{\mathcal{C}} \quad \text{for} \quad c(x) \in \boldsymbol{\mathcal{C}} \quad \text{and} \quad g \in \mathcal{G}\,.$$

The code $\boldsymbol{\mathcal{C}}$ is then constructed from a subset Z of $\mathbb{F}_q[x]$, as the ideal I_Z. Set

$$\mathcal{O}_Z = \bigcup_{i \in Z} \mathcal{O}_i.$$

By Proposition 2.11, we know that if $c(x) \in \mathbb{F}_q[x], i \in Z$ and $h \in \mathcal{O}_i$, then $c(\underline{\xi}^h) = 0$. It follows that

$$\boldsymbol{\mathcal{C}} = \{c(x) \in \mathbb{F}_q[x] \mid c(\underline{\xi}^h) = 0 \text{ for } h \in \mathcal{O}_Z\}. \tag{4.16}$$

Terminology. We say that Z is the *zero* of the code $\boldsymbol{\mathcal{C}}$. But since all of the elements of $\boldsymbol{\mathcal{C}}$ vanishes at $\underline{\xi}^h$ for $h \in Z$, we may also say that the $\underline{\xi}^h$'s are the *zeroes* of $\boldsymbol{\mathcal{C}}$.

In order to describe the zeroes of a multicyclic code, we need more notions.

Definition 4.9 (Support of a multicyclic code)**.** Let $\boldsymbol{\mathcal{C}}$ a multicyclic of $\mathbb{F}_q[x]$ defined by $Z \subset S$. The *support* of $\boldsymbol{\mathcal{C}}$ is

$$\mathrm{Supp}(\boldsymbol{\mathcal{C}}) = \{\underline{\xi}^h \;\mid\; h \in \mathcal{G}_+\} \subset \;\mathbb{F}_{q^t}^r\,.$$

We see that the zeroes of $\boldsymbol{\mathcal{C}}$ belong to Supp($\boldsymbol{\mathcal{C}}$). It is related to the an *affine variety* in algebraic geometry :

Definition 4.10. (Affine variety) Let S a subset of polynomials in $\mathbb{F}_{q^t}[X_1, \ldots, X_r]$. The *affine variety* defined by S is the set

$$\mathrm{Var}(S) = \{P \in \mathbb{F}_{q^t}^r \;\mid f(P) = 0 \;\text{ for all }\; f \in S\} \subset \mathbb{F}_{q^t}^r\,.$$

Proposition 4.11. *According to the previous notations, if $\boldsymbol{\mathcal{C}}$ is a multicyclic code, then*

$$\mathrm{Supp}(\boldsymbol{\mathcal{C}}) = \mathrm{Var}(\langle X_1^{n_1} \;-\; 1, \ldots, X_r^{n_r}\rangle). \tag{4.17}$$

Proof. We must show that

$$\mathrm{Var}(\langle X_1^{n_1} - 1, \dots, X_r^{n_r} - 1\rangle) = \{\underline{\xi}^h \mid h \in \prod_{\rho=1}^{r} \mathbb{Z}/n_\rho\mathbb{Z}\}. \tag{4.18}$$

If $h = (h_1, \dots, h_r) \in \prod_{\rho=1}^{r} \mathbb{Z}/n_\rho\mathbb{Z}$, then, for $\rho = 1, \dots, r$, we have $(\xi_\rho^{h_\rho})^{n_\rho} = (\xi_\rho^{n_\rho})^{h_\rho} = 1$, so that $\underline{\xi}^h = (\xi_1^{h_1}, \dots, \xi_r^{h_r})$ belongs to the set $\mathrm{Var}(\langle X_1^{n_1} - 1, \dots, X_r^{n_r} - 1\rangle)$. Conversely, suppose that the point $P = (\beta_1, \dots, \beta_r) \in \mathbb{F}_{q^t}^r$ belongs to the set $\mathrm{Var}(\langle X_1^{n_1} - 1, \dots, X_r^{n_r} - 1\rangle)$. Then, for $\rho = 1, \dots, r$, it is necessary that $\beta_\rho^{n_\rho} = 1$ and therefore, β_ρ must be of the form $\xi_\rho^{l_\rho}$ where $l_\rho \in \mathbb{Z}/n_\rho\mathbb{Z}$. It follows that $P = (\xi_1^{l_1}, \dots, \xi_r^{l_r}) \in \{\underline{\xi}^h \mid h \in \prod_{\rho=1}^{r} \mathbb{Z}/n_\rho\mathbb{Z}\}$. □

The following corollary is then immediate :

Corollary 4.12. *Let $\boldsymbol{\mathcal{C}}$ be a multicyclic code. Then* $\{\underline{\xi}^h \mid h \in \mathcal{O}_Z\} \subset \mathrm{Supp}(\boldsymbol{\mathcal{C}})$.

Notations. From now on, $\boldsymbol{\mathcal{C}}$ will denote a multicyclic code of $\mathbb{F}_q[x]$ whose zero is Z. A codeword of $\boldsymbol{\mathcal{C}}$ is of the form $c(x) = \sum_{g\in\mathcal{G}_+} c_g x^g$. By the isomorphism (2.17), we can write

$$c(x) = (c_g)_{g\in\mathcal{G}_+}.$$

Let $\leqslant_{\mathrm{lex}}$ the *lexicographic order* on $\mathcal{G}_+$ defined by

$$g = (g_1, \dots, g_r) \leqslant_{\mathrm{lex}} (h_1, \dots, h_r) \iff g = h \text{ or}$$
$$\text{for the smallest } \rho \text{ such that } g_\rho \neq h_\rho, \text{ one has } g_\rho < h_\rho.$$

Let $n = |\,\mathcal{G}_+\,| = n_1 \cdots n_r$. We can write $c(x)$ as a vector of $\mathbb{F}_q^n$: if we arrange the indexes as

$$g^{(1)} \leqslant_{\mathrm{lex}} \cdots \leqslant_{\mathrm{lex}} g^{(n)},$$

then

$$c(x) = (c_{g^{(1)}}, c_{g^{(2)}}, \dots, c_{g^{(n)}}) \in \mathbb{F}_q^n.$$

Thus the *length* of $\boldsymbol{\mathcal{C}}$ is n.

Examples 4.13. (1) According to the notations in Corollary 2.2, Examples 2.4 and equation (2.4), take $p = q = 3, n_1 = n_2 = 2$. Then $\varepsilon = \mathrm{lcm}(2, 2) = 2$ and

$$\mathcal{G}_+ = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{(0,0), (0,1), (1,0), (1,1)\},$$
$$t = \min\{k \in \mathbb{N}^* \mid 3^k \equiv 1 \pmod 2\} = 1.$$

Therefore we have $\mathbb{F}_{q^t} = \mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z} = \{0, 1, 2\}$. A primitive 2nd root of unity in $\mathbb{F}_3^*$ is $\xi = 2$ and

$$\Gamma = \mathrm{Gal}(\mathbb{F}_3, \mathbb{F}_3) = \{\mathrm{Id}_{\mathbb{F}_3}\}.$$

The orbits are the singletons

$$\mathcal{O}_1 = \{(0,0)\}, \quad \mathcal{O}_2 = \{(0,1)\}, \quad \mathcal{O}_3 = \{(1,0)\}, \quad \mathcal{O}_4 = \{(1,1)\}$$

and $S = \{1, 2, 3, 4\}$. Using equation (4.18),

$$\mathrm{Var}(\langle X_1^2 - 1, X_2^2 - 1\rangle) = \{(2^k, 2^l) \mid (k, l) \in \mathcal{G}_+\} = \{(1,1), (1,2), (2,1), (2,2)\}.$$

The elements of the group algebra $\mathbb{F}_3[x] = \mathbb{F}_3[x_1, x_2]$ are of the form

$$a(x) = \sum_{(g_1,g_2)\in\mathcal{G}_+} a_g x_1^{g_1} x_2^{g_2} \tag{4.19}$$

with $x_1^2 = x_2^2 = 1$. We may write the sum in (4.19) as

$$a(x) = b + cx_2 + dx_1 + ex_1x_2, \tag{4.20}$$

where $b, c, d, e \in \mathbb{F}_3$ and

$$\mathbb{F}_3[x_1, x_2] = \{b + cx_2 + dx_1 + ex_1x_2 \mid b, c, d, e \in \mathbb{F}_3\}$$

(there are 81 elements). Now, let $\boldsymbol{\mathcal{C}}$ be the 2-D cyclic code whose zero is $Z = \{1, 4\}$ This corresponds to the subset $\{(1, 1), (2, 2)\}$ of Supp($\boldsymbol{\mathcal{C}}$). We then have

$$\boldsymbol{\mathcal{C}} = \{c(x) \in \mathbb{F}_3[x_1, x_2] \mid c(1, 1) = 0 \quad \text{and} \quad c(2, 2) = 0\}.$$

Using the algebra software SAGE to find the elements of $\boldsymbol{\mathcal{C}}$, we have

$$\begin{aligned}\boldsymbol{\mathcal{C}} = \{&0, 2x_1 + x_2, x_1 + 2x_2, 2x_1x_2 + 1, 2x_1x_2 + 2x_1 + x_2 + 1, 2x_1x_2 + x_1 + 2x_2 + 1, x_1x_2 + 2,\\ &x_1x_2 + 2x_1 + x_2 + 2, x_1x_2 + x_1 + 2x_2 + 2\}\end{aligned}$$

($\boldsymbol{\mathcal{C}}$ has 9 elements). Since in equation (4.20) we may identify $a(x) = b + cx_2 + dx_1 + ex_1x_2$ with the vector $bcde$ of $\mathbb{F}_3^4$, we may rewrite the code $\boldsymbol{\mathcal{C}}$ as

$$\boldsymbol{\mathcal{C}} = \{0000, 0120, 0210, 1002, 1122, 1212, 2001, 2121, 2211\} \subset \mathbb{F}_3^4\,.$$

Now, we are going to verify that $\boldsymbol{\mathcal{C}}$ is invariant under 2-D cyclic shifts. For example, take the codeword $c(x) = 2x_1 + x_2 = 0120$ and consider all the 2-D cyclic shifts, which are the multiplication by x_1, x_2 and x_1x_2 :

$$\begin{aligned} x_1 * c(x) &= 2x_1^2 + x_1x_2 = 2001\\ x_2 * c(x) &= 2x_1x_2 + x_2^2 = 1002\\ x_1x_2 * c(x) &= 2x_1^2x_2 + x_1x_2^2 = 0210. \end{aligned} \tag{4.21}$$

We see that all of these are elements of $\boldsymbol{\mathcal{C}}$.
(2) Take $p = q = r = 3; n_1 = n_2 = n_3 = 2$. then $\varepsilon = \text{lcm}(2, 2, 2) = 2$ and

$$\begin{aligned}\mathcal{G}_+ &= \mathbb{Z}/2\,\mathbb{Z} \times \mathbb{Z}/2\,\mathbb{Z} \times \mathbb{Z}/2\,\mathbb{Z}\\ &= \{(0, 0, 0), (0, 0, 1), (0, 1, 0), (1, 0, 0), (0, 1, 1), (1, 0, 1), (1, 1, 0), (1, 1, 1\},\\ t &= \min\{k \in \mathbb{N}^* \mid 3^k \equiv 1 \pmod 2\} = 1.\end{aligned}$$

Therefore we also have $\mathbb{F}_{q^t} = \mathbb{F}_3 = \mathbb{Z}/3\,\mathbb{Z} = \{0, 1, 2\}$. As in the previous example, a primitive 2nd root of unity in $\mathbb{F}_3^*$ is $\xi = 2$ and

$$\Gamma = \text{Gal}(\mathbb{F}_3, \mathbb{F}_3) = \{\text{Id}_{\mathbb{F}_3}\}.$$

Our group algebra is

$$\mathbb{F}_3[x, y, z] = \{b + cz + dy + ex + fyz + gxz + hxy + ixyz \mid b, c, d, e, f, g, h, i \in \mathbb{Z}/3\,\mathbb{Z}\}$$

(we have use the variables x, y, z for simplicity, with $x^2 = y^2 = z^2 = 1$). It has $3^8 = 6561$ elements. We have

$$\text{V} = \text{Var}(X^2 - 1, Y^2 - 1, Z^2 - 1) = \{(2^u, 2^v, 2^w) \mid u, v, w \in (\mathbb{Z}/3\,\mathbb{Z})^3\},$$

so it has $3^3 = 81$ elements. To construct a non trivial 3-D cyclic code $\boldsymbol{\mathcal{C}}$ in this case, we must choose a non trivial subset Z of Vsuch that Z is the zero of $\boldsymbol{\mathcal{C}}$. Being an additive subgroup of $\mathbb{F}_3[x, y, z]$, the cardinality of $\boldsymbol{\mathcal{C}}$ must be a divisor of 3^8, therefore of the form 3^l where $1 \leqslant l \leqslant 7$. The goal of this example is only to show that the number of elements of a multicyclic code can grow up quickly.

Remark 4.14. Being invariant under r-D cyclic shifts does not mean also invariant under 1-D cyclic shifts, i.e. by a *circular permutation* of the form $(c_1, c_2, \ldots, c_n) \longmapsto (c_n, c_1, \ldots, c_{n-1})$. For example, as we see in equations (4.21), a 1-D cyclic shift of $c(x) = 0120$ is 0012, which does not belongs to $\boldsymbol{\mathcal{C}}$. In fact, one cannot get 0012 from 0120 when using a 2-D cyclic shift.

Now, we consider the decoding process : a codeword $c(x)$ of the code $\boldsymbol{\mathcal{C}}$ has been sent through a communication cannel. At the reception, the received word is of the form $w(x) = c(x)+e(x) \in \mathbb{F}_q[x]$, where $e(x) \in \mathbb{F}_q[x]$ is the *error* produced by the canal. Of course, $c(x)$ and $e(x)$ are unknown to the receiver, who know $w(x)$ only. The aim of the decoding is to find $e(x)$, since the decoder will be able to find $c(x)$ by the equality $c(x) = w(x) - e(x)$.

The equation $w(x) = c(x) + e(x)$ yields

$$w(\underline{\xi}^h) = c(\underline{\xi}^h) + e(\underline{\xi}^h) \quad \text{for} \quad h \in \mathcal{G}_+,$$

so that

$$w(\underline{\xi}^h) = e(\underline{\xi}^h) \quad \text{for} \quad h \in \mathcal{O}_Z. \tag{4.22}$$

This leads to the definition of *syndromes*:

Definition 4.15 (Syndrome)**.** For a received word $w(x)$, the *syndrome* is the element of $\mathbb{F}_{q^t}[y]$ defined by

$$S(y) = \sum_{h \in \mathcal{O}_Z} w(\underline{\xi}^h) y^h.$$

In principle, no error occurred in the transmission through the communication channel if the received word $w(x)$ is a codeword. In this case, $S(y) = 0$. Otherwise, $w(x)$ is not a codeword and $S(y) \neq 0$. We have proved the following proposition:

Proposition 4.16. *An error occurred in the received word $w(x)$ if and only if $S(y) \neq 0$.*

We need the following definition for our last theorem:

Definition 4.17 (Locator ideal)**.** For a received word $w(x) = c(x) + e(x) \in \mathbb{F}_q[x]$, the *locator ideal* of e is

$$\boldsymbol{L} = \{v(x) \in \mathbb{F}_{q^t}[x] \mid v(\underline{\xi}^k) = 0 \quad \forall\, k \in \mathrm{Supp}(e)\}.$$

Using the discrete Fourier transform Φ of Definition 2.13, we have the following characterization of the locator ideal :

Theorem 4.18. *The locator ideal of the error e is the orthogonal of $E(y) = \Phi(e(x))$.*

Proof. We have

$$E(y)^{\perp} = \{c(x) \in \mathbb{F}_q[x] \mid c(x) \ * \ E(y) = 0\}. \tag{4.23}$$

and

$$\boldsymbol{L} = \{c(x) \in \mathbb{F}_{q^r}[x] \mid c(\underline{\xi}^g) = 0 \ \forall g \in \mathrm{Supp}(e)\}.$$

Since

$$c(x) \ * \ E(y) = \sum_{h \in \mathcal{G}_+} \big(\sum_{g \in \mathcal{G}_+} c_g E_{g+h} \big) x^h \tag{4.24}$$

and for $h \in \mathcal{G}_+$:

$$\begin{aligned} \sum_{g \in \mathcal{G}_+} c_g E_{g+h} &= \sum_g c_g \sum_k e_k \xi^{k(g+h)} = \sum_k e_k \xi^{kh} \sum_g c_g \xi^{kg}. \\ &= \sum_k e_k \xi^{kh} c(\underline{\xi}^k). \end{aligned} \tag{4.25}$$

we get

$$c(x) * E(y) = \sum_h \big(\sum_k e_k \xi^{kh} c(\underline{\xi}^k)\big) x^h.$$

Taking $a(x) = \sum_k e_k c(\underline{\xi}^k) x^k$, it follows that

$$\Phi(a(x)) = \sum_h a(\underline{\xi}^h) y^h = \sum_h \big(\sum_k e_k \xi^{kh} c(\underline{\xi}^k)\big) y^h.$$

Thus

$$c(x) * E(y) = \Phi(a(x))$$

and

$$c(x) * E(y) = 0 \Longleftrightarrow \Phi(a(x)) = 0 \Longleftrightarrow a(x) = 0.$$

since Φ is injective. But

$$a(x) = 0 \Longleftrightarrow c(\underline{\xi}^g) = 0 \quad \forall\, g \in \mathrm{Supp}(e),$$

which gives the result. □

The problem is that we know a part of the coefficients of $\Phi(e(x))$ only. Recall that the coefficients of $\Phi(e(x))(y)$ are $(e(\xi^h))_{h \in \mathcal{G}_+}$. Then, we now the coefficients for $h \in \mathcal{O}_Z$ only, which are the same those of $\Phi(w(x))$. We hope that under appropriate conditions, or further formulations, we could use algorithms such as the Berlekamp-Massey-Sakata ([2, 21]) algorithm to find the missing terms of $\Phi(e(x))$ and then to find $e(x)$ itself.

5 Conclusion

a In section 2, we gave results from finite fields, Galois group actions, algebraic dynamical systems, discrete Fourier transforms and Wedderburn transforms. We gave certain proofs and examples. The group algebra is isomorphic to a product of fields, the proof uses the Wedderburn transform.

b In section 3, we explained our goal, which is the definition and construction of multicyclic codes, using group algebra and algebraic dynamical systems.

In section 4, we presented the main results :

c In subsection 4.1, we showed that the group algebra is an algebraic dynamical system.

d In subsection 4.2, we proved that the discrete Fourier transform is an injective homomorphism of the group algebra into another group algebra whose base field is an extension of those of the first group algebra.

e In subsection 4.3, we proved, using again the Wedderburn transform , that the ideals in these group algebras are defined be subsets called "zeros" and conversely. This allowed the definition multicyclic codes as ideals having zeroes from an algebraic affine variety. Examples of construction of 2-D and 3-D cyclic codes using the SAGE computer algebra system are given.

f Using the discrete Fourier transform and notions from dynamical systems, we obtained a definition and characterization of the locator ideal of a received word, when a codeword was transmitted through a communication channel. The locator ideal is a generalization of the locator polynomial in the one dimensional case to the multidimensional case.

We have seen that Galois groups allow the construction of multicyclic codes and explains why polynomials defining these codes must have zeros from a certain set. This illustrates the utility of the Galois Theory. The use of notions from algebraic dynamical systems explains the construction and properties of error locator polynomials, which are key points to the decoding processes. We hope that the introduction of these different theories will allow us to avoid too many calculations in the beginning, but will serve as starting point for interesting ones later, especially in the decoding process. This will give multicyclic codes and their decoding an elegant aspect.

Possible future works are the search for the multicyclic code parameters such as the number of codewords, minimum distance, generator and check matrices and polynomials, at least under particular cases or hypotheses (on the cyclic dimension, zeroes, etc...). And, as we already mentioned at the end of the article, to look for the conditions in order to make use of the algorithm of Berlekamp-Massey-Sakata.

Competing Interests

Authors have declared that no competing interests exist.

References

[1] Bernal JJ, Guerreiro M, Simón JJ. Ds-bounds for Cyclic Codes: New Bounds for Abelian Codes. ArXiv:1604.02949v1, [cs.IT]; 2016.

[2] Saints K, Heegard C. Algebraic-geometric codes and multidimensional cyclic codes: A unified theory and algorithms for decoding using grobner bases. IEEE Transactions on Information Theory. 1995;41(6).

[3] Kuijper M. Berlekamp-massey algorithm, error-correction, keystream and modeling. Dynamical Systems, Control, Coding, Computer Vision. Springer; 1999.

[4] Andriamifidisoa R. Systèmes Dynamiques Linéaires Discrets et Codes Algébriques. Thèse de Doctorat, Université d'Antananarivo, Madagascar. French; 2002.

[5] Güneri C, Özbudak F. Multidimensional Cyclic Codes and Artin-Schreier type Hypersurfaces over Finite Fields. Finite Fields and Their Applications. 2008;14:44-58.

[6] Güneri C, Özbudak F. A Relation Between Quasi-cyclic Codes and 2-D cyclic Codes. Finite Fields and Their Applications. 2012;18:123-132.

[7] Gallian JA. Contemporary abstract algebra. BROOKS/COLE CENGAGE Learning, Seventh Edition; 2010.

[8] Lidl R, Niederreiter H. Finite fields. Cambridge Univ. Press; 1997.

[9] Mullen GL, Panario D. Handbook of finite fields. CRC Press; 2013

[10] Childs LN. A Concrete Introduction to Higher Algebra. Springer; 1995.

[11] Raschke J. Abelsche codes. Diplomarbeit, Fakültat für Mathematik der Universität Bielefeld, Germany. German; 2001.

[12] Andriamifidisoa R, Andrianjanahary J. Polynomial Operator in the Shifts in Discrete Algebraic Dynamical Systems. British Journal of Mathematics & Computer Science 2015;6(2):119-128. DOI: 10.9734/BJMCS/2015/15028

[13] Andriamifidisoa R. Action of a polynomial matrix on a vector of power series. British Journal of Mathematics and Computer Science. 2016;16(4):1-8. DOI: 10.9734/BJMCS/2016/25791

[14] Oberst U. Multidimensional Constant Linear Systems. Acta Appl. Math. 1990;20:1-175.

[15] Lane SM. Categories for the Working Mathematician. Springer; 1971.

[16] Camion P. Abelian codes. Combinatorial Mathematics Year; 1969-1970

[17] Schiffels G. Transformation de fourier Discrète. Cours à l'Université d'Antananarivo, Madagascar. French; 1996.

[18] Blahut RE. Algebraic Methods for Signal Processing and Communications Coding. Springer; 1992.

[19] Cox D, Little J, O'Shea D. Ideals, Varieties and Algorithms. Springer, Second Edition; 1997.

[20] Fulton W. Algebraic curves, an introduction to algebraic geometry. Addison-Wesley, 3rd Edition; 2008.

[21] Sakata S. Extension of the Berlekamp-Massey Algorithm to N Dimensions. Information and Computation. 1990;84:207-239.

Peer-review history:
The peer review history for this paper can be accessed here (Please copy paste the total link in your browser address bar)
http://sciencedomain.org/review-history/18302