A Gröbner basis approach to m-dimensional skew (consta-) cyclic codes

Willi Geiselmann, Félix Ulmer

A Gröbner basis approach to m-dimensional skew (consta-) cyclic codes

Dedicated to André Leroy on his retirement

Willi Geiselmann[1] and Felix Ulmer [23]

December 12, 2022

Abstract

Algebraic linear codes $J/I \subset \mathbb{F}_q[X_1, \dots X_m]/I$ that are finite dimension quotients of multivariate polynomial rings, have been studied intensively; in particular m-dimensional cyclic codes where the ideal I is $(X_1^{n_1} - 1, \dots, X_m^{n_m} - 1)$. Recently this notion has been extended to two dimensional skew cyclic codes using multivariate skew polynomial rings over fields [12, 16, 18] and even over rings [15]. In this paper we use a Gröbner basis approach in order to generalize algebraic linear codes and m-dimensional cyclic codes to the skew polynomial rings setting. The approach encompass all previous results on m-dimensional (consta-)cyclic codes and allows for many generalizations.

1 Introduction

Definition 1 *A **code** $\mathcal{C}$ of **length** $n \in \mathbb{N}$ over a field $\mathbb{F}$ is a nonempty subset of $\mathbb{F}^n$. The elements of $\mathcal{C}$ are called codewords. The code $\mathcal{C}$ is a **linear code** if it is an $\mathbb{F}$-subspace of $\mathbb{F}^n$. If $\mathbb{F}$ is a finite field $\mathbb{F}_q$, then a linear code of length n and dimension k is a k-dimensional subspace of $\mathbb{F}_q^n$. A **code** $\mathcal{C}$ of length $n \in \mathbb{N}$ over a finite field $\mathbb{F}_q$ is a nonempty subset of $\mathbb{F}_q^n$. The elements of $\mathcal{C}$ are called codewords. The code $\mathcal{C}$ is a **linear code** if it is a k-dimensional $\mathbb{F}_q$-subspace of $\mathbb{F}_q^n$. The **Hamming distance** between two vectors of $\mathbb{F}_q^n$ is defined as the number of coordinates at which the two vectors differ. The **minimal distance** d of a k-dimensional linear code $\mathcal{C} \subset \mathbb{F}_q^n$ is defined to be the minimum Hamming distance between two distinct codewords of $\mathcal{C}$. In this case we say that $\mathcal{C}$ is a code with **parameters** $[n, k, d]_q$.*

[1]KIT, Institut für Theoretische Informatik (ITI), Am Fasanengarten 5, D-76131 Karlsruhe
[2]Univ Rennes, CNRS, IRMAR - UMR 6625, F-35000 Rennes, France.
[3]This work was supported in part by French projects ANR-11-LABX-0020-01 "Centre Henri Lebesgue" and ANR-18-EURE-0004 "Cyberschool"

Definition 2 *An $\mathbb{F}_q$-code of length $n_1 n_2 \cdots n_m$ is an m-**dimensional constacylic code** if for any code word, viewed as a particular m-dimensional matrix of size $n_1 \times n_2 \times \cdots \times n_m$, is invariant under application of a cyclic shift in the dimension i and multiplication of the resulting first entry by $\lambda_i \in \mathbb{F}_q$.*

Example 1 *A length $n_1 n_2$ code over $\mathbb{F}_q$ is a 2-dimensional constacylic code if there is a basis of $\mathbb{F}_q^{n_1 n_2}$ arranged in an $n_1 \times n_2$ array such that for any code word*

$$\begin{pmatrix} a_{0,n_2-1} & a_{1,n_2-1} & \dots & a_{n_1-1,n_2-1} \\ a_{0,n_2-2} & a_{1,n_2-2} & \dots & a_{n_1-1,n_2-2} \\ \vdots & \vdots & \dots & \vdots \\ a_{0,1} & a_{1,1} & \dots & a_{n_1-1,1} \\ a_{0,0} & a_{1,0} & \dots & a_{n_1-1,0} \end{pmatrix}. \tag{1}$$

both

$$\begin{pmatrix} \lambda_1 a_{n_1-1,n_2-1} & a_{0,n_2-1} & \dots & a_{n_1-2,n_2-1} \\ \lambda_1 a_{n_1-1,n_2-2} & a_{0,n_2-2} & \dots & a_{n_2-1,n_2-2} \\ \vdots & \vdots & \dots & \vdots \\ \lambda_1 a_{n_1-1,1} & a_{0,1} & \dots & a_{n_1-2,1} \\ \lambda_1 a_{n_1-1,0} & a_{0,0} & \dots & a_{n_1-2,0} \end{pmatrix}$$

and

$$\begin{pmatrix} a_{0,n_2-2} & a_{1,n_2-2} & \dots & a_{n_1-1,n_2-2} \\ \vdots & \vdots & \dots & \vdots \\ a_{0,1} & a_{1,1} & \dots & a_{n_1-1,1} \\ a_{0,0} & a_{1,0} & \dots & a_{n_1-1,0} \\ \lambda_2 a_{0,n_2-1} & \lambda_2 a_{1,n_2-1} & \dots & \lambda_2 a_{n_1-1,n_2-1} \end{pmatrix}$$

belong to the code for some $\lambda_1, \lambda_2 \in \mathbb{F}_q$. Here the firt shift is to the right and the second shift is upwards for reasons that are connected to the representation of standard monomials and that will soon become apparent.

Let $\mathbb{F}_q$ be a field and $R = \mathbb{F}_q[X_1, \dots X_m]$ the polynomial ring in $n \geq 1$ variables. We refer to [3] for the definition of an admissible ordering $<$ on $\mathbb{N}^m$. A admissible ordering induces an admissible ordering $<$ on the set of monomials $\mathcal{M} = \{X^\alpha = X_1^{\alpha_1} X_2^{\alpha_2} \cdots X_m^{\alpha_m} \,|\, \alpha_i \in \mathbb{N}\}$ in $\mathbb{F}_q[X_1, \dots X_m]$ via $X^\alpha < X^\beta$ if and only if $\alpha < \beta$. For any expression $f = \sum_{\alpha \in \mathbb{N}^m} c_\alpha X^\alpha \in \mathbb{F}_q[X_1, \dots, X_m]$ where only finitely many c_α are nonzero, the monomial $X^\gamma = \max\{X^\alpha | c_\alpha \neq 0\}$ is the ***leading monomial*** of f and c_α is the ***leading coefficient*** of f, denoted respectively by $\mathrm{lm}(f)$ and $\mathrm{lc}(f)$. The monomial $X^\alpha \in \mathcal{M}$ is divisible by X^β if $X^\alpha = \mathrm{lm}(X^\omega X^\beta)$ for some $X^\omega \in \mathcal{M}$ and the least common multiple of X^α and X^β is defined as $\mathrm{lcm}(X^\alpha, X^\beta) = X^\gamma$ where $\gamma_i = \max(\alpha_i, \beta_i)$.

A basis $G = \{g_1, \dots, g_m\}$ of and ideal $I \subset R$ is a ***Gröbner basis*** if and only if $\{\mathrm{LM}(g_1), \dots, \mathrm{LM}(g_m)\}$ generates the ideal $\mathrm{LM}(I) = \{\mathrm{LM}(f) | f \in I\}$ of leading monomials of I. If $G = \{g_1, \dots, g_m\}$ is a Gröbner Basis, then the reduction $\overline{f}^G$ of f by G is unique. The ***standard monomials*** of I are the set of monomials

that do not belong to $\mathrm{LM}(I)$. The quotient R/I is a finite dimensional k-vector space if and only if G contains a polynomial with leading monomial $X_i^{n_i}$ for each $i \in \{1, \ldots, m\}$. In this case the standard monomials form a basis of the k-vector space R/I (see [3]).

Example 2 *If for $I \subset \mathbb{F}_q[X,Y]$ we have $\dim_{\mathbb{F}_q}(\mathbb{F}_q[X,Y])/I) < \infty$, then the standard monomials X^iY^j can always be represented as a **staircase** of $\bullet$ points (i,j) in the upper half plane of the form*

$$\begin{array}{ccccc} \cdot & \cdot & \cdot & \cdot & \cdot \\ \bullet & \bullet & \cdot & \cdot & \cdot \\ \bullet & \bullet & \bullet & \cdot & \cdot \\ \bullet & \bullet & \bullet & \cdot & \cdot \\ \bullet & \bullet & \bullet & \bullet & \cdot \end{array}$$

For two ideals $I \subset J \subset R$ the correspondance of ideals shows that J/I is a submodule of R/I. The ideal $J/I \subset R/I$ is $\mathbb{F}_q$-subspace of R/I. The isomorphism $(R/I)/(J/I) \cong R/J$ shows that the quotient of the vector spaces $(R/I)/(J/I)$ is isomorphic to R/J. The ideal I is a ***zero dimensional*** if the $\mathbb{F}_q$-vector space R/I of finite dimension n. In this case image $\pi(J) = J/I$ under $\pi : R \rightarrow: R/I$ is a linear code of length $n = \dim_{\mathbb{F}_q}(R/I)$ and dimension $k = n - \dim_{\mathbb{F}_q}(R/J)$ (see [4]). Since $I \subset J$, the standard monomials of J (a basis of R/J) are contained in the set of standard monomials of I (a basis of R/I). The above isomorphisms show that standard monomials of R/I which are not standard monomials of R/J form a basis of code $\pi(J)$. We denote $\overline{w}^J$ the reduction of $w \in R$ with a Gröbner basis of J. From ([4], Theorem 3.9) we get that the information position are the standard monomials of I that are not standard monomials of J and that $E(w) = w - \overline{w}^J$ (which is always an element of J) is an encoding of any linear combination $w \in J/I$ of information positions.

Definition 3 *(see [4]) Consider the ring $R = \mathbb{F}_q[X_1, \ldots X_m]$ and two zero-dimensional ideals $I \subset J \subset R$. We call the submodule J/I of R/I a **quotient ideal code** of $\mathbb{F}_q[X_1, \ldots X_m]$. The parameters $[n,k]$ of this code are $n = \dim(R/I)$ and $k = \dim(R/J)$.*

For the basis $G = \{X_1^{n_1} - \lambda_1, \ldots, X_m^{n_m} - \lambda_m\}$ all S-polynomial (see [3])

$$\begin{aligned} S(f_i, f_j) &= X_j^{n_j}(X_1^{n_i} - \lambda_i) - X_i^{n_i}(X_1^{n_j} - \lambda_j) \\ &= X_i^{n_i}\lambda_j - X_j^{n_j}\lambda_i \end{aligned}$$

reduce to $\overline{S(f_i, f_j)}^G = \lambda_i\lambda_j - \lambda_j\lambda_i = 0$ (see [3]). Therefore the basis G is a Gröbner basis of $I \subset \mathbb{F}_q[X_1, \ldots X_m]$ (see [3]).

Example 3 *The $\mathbb{F}_q[X_1, X_2]$-module*

$$J/(X_1^{n_1} - \lambda_1, X_2^{n_2} - \lambda_2) \subset \mathbb{F}_q[X_1, X_2]/(X_1^{n_1} - \lambda_1, X_2^{n_2} - \lambda_2)$$

corresponds to 2*-dimensional constacyclic code. In order to see this we consider the following* $\mathbb{F}_q$*-basis of* $\mathbb{F}_q[X_1, X_2]/(X_1^{n_1} - 1, X_2^{n_2} - 1)$ *:*

$$\begin{array}{cccc} X_2^{n_2-1} & X_1X_2^{n_2-1} & \dots & X_1^{n_1-1}X_2^{n_2-1} \\ \vdots & \vdots & \dots & \vdots \\ X_2 & X_1X_2 & \dots & X_1^{n_1-1}X_2 \\ 1 & X_1 & \dots & X_1^{n_1-1} \end{array} \tag{2}$$

and represent the code word $\sum_{i=0}^{n_1-1}\sum_{j=0}^{n_2-1} a_{i,j}X_1^iX_2^j$ *as in (1). This basis reflects the staircases of the standard monomials of* I *represented by* $\circ$ *and* $\bullet$ *which contains the standard monomials of* J *represented by* $\bullet$*. For example*

$$\begin{array}{lcccc} n_2 = 3 & \cdot & \cdot & \cdot & \cdot \\ & \circ & \circ & \circ & \cdot \\ & \bullet & \bullet & \circ & \cdot \\ & \bullet & \bullet & \bullet & \cdot \\ (0,0) & & & & n_1 = 3 \end{array}$$

By construction the code is an $\mathbb{F}_q[X_1, X_2]$*-module. We now show that is also a* 2*-dimensional constacyclic code. Multiplication by* X_1 *of the first* $n_1 - 1$ *columns results in a shift of of those columns to the right. Since* $X_1a_{n_1-1,j}X_1^{n_1-1}X_2^j = a_{n_1-1,j}X_1^{n_1}X_2^j$ *is reduced to* $\lambda a_{n_1-1,j}X_2^j$ *by the Gröbner basis, we see that multiplication by* X_1 *of the last column results in a shift to the first column and a multiplication by* λ_1*. The action on the rows results from multiplication by* X_2*.*

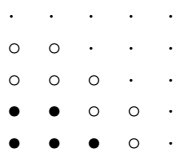
The example shows that all $\mathbb{F}_q[X_1, X_2, \dots, X_m]$-modules of the form $J/I \subset \mathbb{F}_q[X_1, X_2, \dots, X_m]/I$ where $I = (X_1^{n_1} - \lambda_1, \dots, X_m^{n_m} - \lambda_m)$ are ***m-dimensional constacyclic code***. The m-dimensional cyclic code $J/I \subset \mathbb{F}_q[X_1, X_2, \dots, X_m]/I$ where $I = (X_1^{n_1} - 1, \dots, X_m^{n_m} - 1)$ have been extensively studied [10, 9].

For any zero-dimensional ideal $I \subset R$ the ideal $J = (f_1, \cdots, f_s) + I$ determines a quotient ideal code $J/I \subset R/I$, but the parameters $[n, k]$ of the code can only be determined using a Gröbner basis for I and J and therefore cannot be prescribed in the construction of [4], Chapter 9 or [14]). In the next section we will show how to prescribe the parameter $[n, k]$ during the construction of the code.

2 The variety of quotient ideal codes of given length and dimension

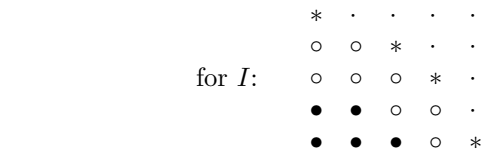
The following Gröbner basis approach allows to compute all finite dimensional ideals $I \subset J \subset \mathbb{F}_q[X_1, \dots X_m]$ with prescribed staircases. In the following we fixe a monomial ordering and two staircases of two finite dimensional ideals $I \subset J$,

such that the staircase of I is contained in the staircase of J. For example

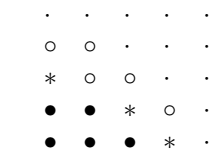


We need to **prescribe the leading monomials**, denoted by $*$ below, of the ideal of leading monomials in both cases:

for I:



and for J:



This gives the following algorithm:

1. (a) Choice of J: For each prescribed leading monomial $X_1^{n_{1,\ell}} \cdots X_m^{n_{m,\ell}}$ of a generator of J we must have an element in the Gröbner basis of J of the form $g_m = X_1^{n_{1,\ell}} \cdots X_m^{n_{m,\ell}} + \sum_i \alpha_{\ell,i} X_1^{n_{1,\alpha_{\ell,i}}} \cdots X_m^{n_{m,\alpha_{\ell,i}}}$ (we put all possible lower monomials with unknown coefficients) for J. Since the leading monomials of the basis $\mathcal{B} = (g_1, \ldots, g_s)$ of J have unitary leading coefficients, we can reduce all S-polynomials $S(g_i, g_j)$ modulo $\mathcal{B}$. This will lead to polynomials in $X_1, \ldots, X_m$ with polynomial coefficients in the unknown $\alpha_{\ell,i}$. Setting them to 0 gives a polynomial system $\mathcal{S}_1$ for the unknown $\alpha_{\ell,i}$ whose solutions are all possible J with this prescribed staircase.

   (b) Choice of I:

      i. We can either fix the generators of I, for example of the form $X_i^{n_i} - 1$ in order to obtain m-dimensional cyclic codes

      ii. or proceed as above: For each prescribed leading monomial

$$X_1^{n_{1,\rho}} \cdots X_m^{n_{m,\rho}}$$

      of a generator of I we must have an element in the Gröbner basis of J of the form a

$$f_\rho = X_1^{n_{1,\rho}} \cdots X_m^{n_{m,\rho}} + \sum \beta_{\rho,i} X_1^{n_{1,\beta_{\rho,i}}} \cdots X_m^{n_{m,\beta_{\rho,i}}}$$

      (we put all possible lower monomials with unknown coefficients) for generators of I. Since the leading monomials of the basis $\mathcal{B}' = (f_1, \ldots, f_t)$ of I has unitary leading coefficients, we can reduce all S-polynomials $S(f_i, f_j)$ modulo $\mathcal{B}'$. This will lead to polynomials in $X_1, \ldots, X_m$ with polynomial coefficients in the unknown $\beta_{\rho,i}$. Setting them to 0 gives a polynomial system $\mathcal{S}_2$ for the unknown $\beta_{\rho,i}$ whose solutions are all possible I with this prescribed staircase.

2. Imposing $I \subset J$: Since the leading monomials of the basis $\mathcal{B} = (g_1, \ldots, g_s)$ of J has unitary leading coefficients, we can reduce all generator polynomials f_i of I in the above basis for I modulo $\mathcal{B}$. Since $f_i \in J$ if and only if the reduction of f_i by a Gröbner basis of J is zero, this will lead to polynomials in $X_1, \ldots, X_m$ with polynomial coefficients in the unknown $\alpha_{\ell,i}$ and $\beta_{\rho,i}$. Putting them to 0 gives a polynomial system $\mathcal{S}_3$ for the unknown $\alpha_{\ell,i}$ and $\beta_{\rho,i}$.

3. The solutions of the polynomial system $\mathcal{S}_1 \cup \mathcal{S}_2 \cup \mathcal{S}_3$ gives all possible ideals $I \subset J \subset \mathbb{F}_q[X_1, \ldots X_m]$ for the prescribed staircases.

Example 4 *Consider* $\mathbb{F}_4 = \mathbb{F}_2[w]/\left(w^2 + w + 1\right)$. *Then* $G = \{X_1^2 + w, X_2^2 + w\}$ *is a Gröbner basis which generates an ideal* $I \subset \mathbb{F}_4[X_1, X_2]$ *whose standard monomials belong to a quadratic staircase of length 2. We now look for an ideal* J *containing* I. *The code* $J/I \subset \mathbb{F}_4[X_1, X_2]/I$ *has dimension* 2 *if and only if* J *has* 2 *standard monomials. There are exactly 2 possible staircases for a* 2*-dimensional cyclic code with parameters* $[4, 2]_4$*:*

$$\begin{array}{ccc} \cdot & \cdot & \cdot \\ \bullet & \circ & \cdot \\ \bullet & \circ & \cdot \end{array} \qquad\qquad \begin{array}{ccc} \cdot & \cdot & \cdot \\ \circ & \circ & \cdot \\ \bullet & \bullet & \cdot \end{array}$$

For the first staircase we found one ideal $J \subset \mathbb{F}_4[X_1, X_2]$ *containing* I*; it defines a* $[4, 2, 2]$*-code. For the second staircase we found four ideals, two of them produce a* $[4, 2, 2]$*-code, both are equivalent to the one already found. The two remaining ideals produce two equivalent* $[4, 2, 3]$*-codes. An example of a* $[4, 2, 3]$*-code is given by* $J = (X_2 + w^2 X_1 + 1,\ X_1^2 + w)$.

Example 5 *Consider* $\mathbb{F}_{27} = \mathbb{F}_3[w]/\left(w^3 - w + 1\right)$. *Then* $G = \{X_1^3 - 1, X_2^3 - 1\}$ *is a Gröbner basis which generates an ideal* $I \subset \mathbb{F}_{27}[X_1, X_2]$ *whose standard monomials belong to a quadratic staircase of length 3. We now look for an ideal* J *containing* I. *The code has dimension* $4 = 9 - 5$ *if and only if* J *has* 5 *standard monomials. There are exactly 3 possible staircases for a* 2*-dimensional cyclic code with parameters* $[9, 5]_{27}$*:*

$$\begin{array}{cccc} \cdot & \cdot & \cdot & \cdot \\ \bullet & \circ & \circ & \cdot \\ \bullet & \bullet & \circ & \cdot \\ \bullet & \bullet & \circ & \cdot \end{array} \qquad \begin{array}{cccc} \cdot & \cdot & \cdot & \cdot \\ \bullet & \circ & \circ & \cdot \\ \bullet & \circ & \circ & \cdot \\ \bullet & \bullet & \bullet & \cdot \end{array} \qquad \begin{array}{cccc} \cdot & \cdot & \cdot & \cdot \\ \circ & \circ & \circ & \cdot \\ \bullet & \bullet & \circ & \cdot \\ \bullet & \bullet & \bullet & \cdot \end{array}$$

where the staircases of I *are represented by* $\bullet$ *and* $\circ$ *and those of* J *by* $\bullet$.

In the following discussion we say that two codes are equivalent if they have the same weight enumerator. For the first staircase we found 1 *ideal*

$$J = \left(X_2^3 + 2,\ X_1 X_2^2 + 2X_2^2 + X_1 X_2 + 2X_2^2 + X_1 + 2,\ X_1^2 + X_1 + 1\right)$$

and the parameters of the code $J/I \subset \mathbb{F}_{27}[X_1, X_2]$ *are* $[9, 4, 3]_{27}$. *For the second staircase we found* 27 *ideals, they give 3 (equivalent)* $[9, 4, 4]$*-codes and 24 (equivalent)* $[9, 4, 5]$*-codes. An example of a* $[9, 4, 5]$*-code is given by*

$$J = \left(X_2^3 + 2,\ X_1 X_2 + 2X_2 + wX_1^2 + w^3 X_1 + w^9,\ X_1^3 + 2\right).$$

The third staircase produced 729 *left ideals; 3 of them produced* $[9,4,3]$*-codes, equivalent to the one already found, 3 of them produced* $[9,4,4]$*-codes, equivalent to the one already found, 219 of them produced* $[9,4,4]$*-codes, and extend the* $[9,4,5]$*-codes to three not equivalent codes. The 504 remailing ideals produced* $[9,4,6]$*-codes, all of them are equivalent. An example of a* $[9,4,6]$*-code is given by*

$$\begin{aligned} J &= \big(X_2^2 + w^2X_1X_2 + w^{25}X_2 + wX_1^2 + w^{17}X_1 + w^6, \\ &\quad X_1^2X_2 + X_1X_2 + X_2 + 2X_1^2 + 2X_1 + 2,\ X_1^3 + 2\big). \end{aligned}$$

Up to equivalence, we have found 6 different codes.

3 Skew *left* quotient ideal code

We first recall some basic fact concerning skew polynomial rings. Let A be a ring with an automorphism θ, then a θ-derivation is a map $\delta : A \to A$ such that for all a and b in A: $\delta(a+b) = \delta(a) + \delta(b)$ and $\delta(ab) = \delta(a)b + \theta(a)\delta(b)$. Starting from A, an automorphism θ of A and a θ-derivation on A, we define a ring structure on the set:

$$R = A[X;\theta,\delta] \,=\, \{a_nX^n + \ldots + a_1X + a_0 \,|\, a_i \in \mathbb{F}_q \text{ and } n \in \mathbb{N}\}.$$

The addition in R is defined to be the usual addition of polynomials and the multiplication is defined by the basic rule $X\,a = \theta(a)\,X + \delta(a)$ $(a \in \mathbb{F}_q)$ and extended to all elements of R by associativity and distributivity. According to [13] R is a ring called Ore ring or skew polynomial ring. The classical commutative polynomial ring corresponds to A commutative, $\theta = \mathrm{id}$ and $\delta : a \mapsto 0$. For a finite field $\mathbb{F}_q$ and an automorphism $\theta \in \mathrm{Aut}(\mathbb{F}_q)$ the univariate skew polynomial ring $\mathbb{F}_q[X;\theta]$ is a left and right euclidean ring (see [13]). By repeating this construction we obtain the ***iterated skew polynomial ring*** in ℓ non commutative variables over A:

$$\mathcal{R}_m \;=\; (\ldots((A[X_1;\theta_1,\delta_1])[X_2;\theta_2,\delta_2])\ldots)[X_m;\theta_m,\delta_m]. \tag{3}$$

where $\mathcal{R}_0 = A$, θ_i is an automorphism of $\mathcal{R}_{i-1}$ and δ_i is a θ_i-derivation of $\mathcal{R}_{i-1}$. The following is a generalization of Definition 3 and Section 5 of [2]:

Definition 4 *Let* $A = \mathbb{F}_q$ *and* $\mathcal{R}_m$ *be definied as in (3). For two zero-dimensional* left *ideals* $\mathcal{I} \subset \mathcal{J} \subset \mathcal{R}_m$ *we call the left submodule* $\mathcal{J}/\mathcal{I}$ *of* $\mathcal{R}_m/\mathcal{I}$ *a* ***skew left quotient ideal code*** *of* $\mathcal{R}_m$*. The parameters* $[n,k]$ *of this code are* $n = \dim(\mathcal{R}_m/\mathcal{I})$ *and* $k = \dim(\mathcal{R}_m/\mathcal{J})$.

In [7, 8] a theory of Gröbner basis is presented for a large class of skew polynomial rings, making the above definition effective for all such rings. As in the commutative case we obtain that the information positions are the standard monomials of the left ideal $\mathcal{I}$ that are not standard monomials of the left ideal $\mathcal{J}$ and that $E(w) = w - \overline{w}^{\mathcal{J}}$ (which is always an element of $\mathcal{J}$) is an encoding

of any linear combination $w \in \mathcal{J}/\mathcal{I}$ of information positions. We can compute the variety of m-dimension skew left quotient ideal codes of a given dimension using the approach of Section 2.

In order to obtain examples of codes we will construct families of skew polynomial rings satisfying the criteria given in [7, 8] for the existence of a Gröbner basis.

As in the commutative case, a monomial ordering induces an ordering $\prec$ on the set of monomials $\mathcal{M} = \{X^\alpha = X_1^{\alpha_1} X_2^{\alpha_2} \cdots X_m^{\alpha_m} \,|\, \alpha_i \in \mathbb{N}\}$ (because of the non commutativity, the variables need to be in this precise order) via $X^\alpha \prec X^\beta$ if and only if $\alpha < \beta$. For any expression $f = \sum_{\alpha \in \mathbb{N}^m} c_\alpha X^\alpha$ where only finitely many constants c_α are nonzero, the monomial $X^\gamma = \max\{X^\alpha | c_\alpha \neq 0\}$ is the ***leading monomial*** of f and c_α is the ***leading coefficient*** of f, denoted respectively by $\mathrm{lm}(f)$ and $\mathrm{lc}(f)$. Then the least common multiple of X^α and X^β is defined as $\mathrm{lcm}(X^\alpha, X^\beta) = X^\gamma$ where $\gamma_i = \max(\alpha_i, \beta_i)$. We will be interested in left ideals I of $\mathcal{R}_m$. From [7, 8] we obtain that Gröbner base of left ideals exist for the following type of rings (sometimes called σ-PBW Extensions):

Definition 5 *Let $\mathcal{R}_m = A[X_1; \theta_1, \delta_1] \cdots [X_m; \theta_m, \delta_m]$ be an iterative skew polynomial ring with $m \in \mathbb{N}$ as defined above. We call the ring $\mathcal{R}_m$* ***left-lex-solvable****, for the lexicographical order $1 \prec X_1 \prec \ldots \prec X_m$, if*

1. *for any $a \in A$ and any $i \in \{1, \ldots, m\}$, $X_i a = b X_i + p_{i,a}$ where $b \in A$ and $p_{i,a} \in \mathcal{R}_{i-1}$;*
2. *for all $j < i$ in $\{1, \ldots, m\}$, $X_i X_j = b X_j X_i + p_{i,j}$ where $b \in A$ and all monomials in $p_{i,j}$ are $\prec X_i X_j$.*

We follow the definition of an ***S-polynomial*** given in ([19], Definition 2.5). If $\mathrm{LM}(f) = X^\alpha$, $\mathrm{LM}(g) = X^\beta$, $X^\gamma = \mathrm{lcm}(X^\alpha, X^\beta)$, $t_f = X^{\gamma - \alpha}$ and $t_g = X^{\gamma - \beta}$, then

$$\mathrm{SPoly}(f, g) = t_f \, f \; - \; c \, t_g \, g, \text{ where } c = \frac{\mathrm{lc}(t_f \, f)}{\mathrm{lc}(t_g \, g)}.$$

A Gröbner basis is now constructed the usual way using the classical Buchberger algorithm.

4 m-dimensional skew cyclic codes with commuting variables

Recently several authors generalized 2-D (consta-)cyclic codes to skew polynomial rings $R[x, y; \rho, \theta]$ whose variables x and y commute [12, 16, 18, 15]. In those papers the authors use a canonical form of an element of an ideal without using the theory of Gröbner basis. In this section we give a unified Gröbner basis approach, a generalization of the approach in [2], that encompass all previous results and allows for many generalizations.

Definition 6 *A code over $\mathbb{F}_q$ of length $n_1 n_2$ is a 2-dimensional skew constacylic code if there is a basis of $\mathbb{F}_q^{n_1 n_2}$, non zero elements λ_1, λ_2 in $\mathbb{F}_q$ and automorphisms θ_1 and θ_2 of $\mathbb{F}_q$ such that for any code word*

$$\begin{pmatrix} a_{0,n_2-1} & a_{1,n_2-1} & \dots & a_{n_1-1,n_2-1} \\ \vdots & \vdots & \dots & \vdots \\ a_{0,1} & a_{1,1} & \dots & a_{n_1-1,1} \\ a_{0,0} & a_{1,0} & \dots & a_{n_1-1,0} \end{pmatrix},$$

both

$$\begin{pmatrix} \lambda_1\theta_1(a_{n_1-1,n_2-1}) & \theta_1(a_{0,n_2-1}) & \dots & \theta_1(a_{n_1-2,n_2-1}) \\ \vdots & \vdots & \dots & \vdots \\ \lambda_1\theta_1(a_{n_1-1,1}) & \theta_1(a_{0,1}) & \dots & \theta_1(a_{n_1-2,1}) \\ \lambda_1\theta_1(a_{n_1-1,0}) & \theta_1(a_{0,0}) & \dots & \theta_1(a_{n_1-2,0}) \end{pmatrix}$$

and

$$\begin{pmatrix} \theta_2(a_{0,n_2-2}) & \theta_2(a_{1,n_2-2}) & \dots & \theta_2(a_{n_1-1,n_2-2}) \\ \vdots & \vdots & \dots & \vdots \\ \theta_2(a_{0,0}) & \theta_2(a_{1,0}) & \dots & \theta_2(a_{n_1-1,0}) \\ \lambda_2\theta_2(a_{0,n_2-1}) & \lambda_2\theta_2(a_{1,n_2-1}) & \dots & \lambda_2\theta_2(a_{n_1-1,n_2-1}) \end{pmatrix}$$

belong to the code. The generalization to m-dimensional skew constacylic code is straigthforward.

Lemma 1 *(cf. [2]) In a finite field $\mathbb{F}_q$ of order q we consider the automorphisms $\theta_i \in \mathrm{Aut}(\mathbb{F}_q)$ where $i \in \{1, \dots, m\}$. There exists a skew polynomial ring*

$$\mathfrak{K}_m^{\theta_1,\dots,\theta_m} = (\cdots((\mathbb{F}_q[X_1;\theta_1])[X_2;\theta_2])\cdots[X_m;\theta_m]) \tag{4}$$

whose elements are the finite sums of the form $\sum a_{i_1,\dots,i_n} X_1^{i_1} X_2^{i_2} \cdots X_m^{i_m}$ where the addition in R is the usual addition of multivariate polynomials and the multiplication is defined by the rules $X_i a = \theta_i(a) X_i$ and $X_i X_j = X_j X_i$ and extended to $\mathfrak{K}_m$ by distributivity.

Proof. We proceed by induction on m. Since the automorphism θ_1 and θ_2 commute in $\mathrm{Aut}(\mathbb{F}_q)$, we can extend θ_2 by $X_1 \mapsto X_1$ to an automorphisms of $\mathbb{F}_q[X_1;\theta_1]$ ([17], Theorem 2.2) and define $\mathfrak{K}_2^{\theta_1,\theta_2} = (\mathbb{F}_q[X_1;\theta_1])[X_2;\theta_2]$. Suppose that $\mathfrak{K}_\ell - 1^{\theta_1,\dots,\theta_\ell - 1}$ has been defined. Using again ([17], Theorem 2.2) we can extend θ_ℓ by $X_1 \mapsto X_1, \dots, X_{\ell-1} \mapsto, X_{\ell-1}$ to an automorphism of $\mathfrak{K}_{\ell-1}^{\theta_1,\dots,\theta_{\ell-1}}$ and therefore define $\mathfrak{K}_\ell^{\theta_1,\dots,\theta_{\ell-1},\theta_\ell}$. The result follows by induction. ∎

The ring $\mathfrak{K}_m^{\theta_1,\dots,\theta_m}$ is left-lex-solvable (definition 5). Therefore, using lex order, we can define a left Gröbner basis for any left ideal.

Theorem 1 *We keep the notation of the previous Lemma 1 to define the ring $\mathfrak{K}_m^{\theta_1,\dots,\theta_m}$ whose variables X_i commute $X_i X_j = X_j X_i$. For $\lambda_1, \lambda_2, \dots, \lambda_m$ in $\mathbb{F}_q$ such that $\theta_i^{n_i}(\lambda_j)\lambda_i = \theta_j^{n_j}(\lambda_i)$ the set $G = \{X_1^{n_1} - \lambda_1, X_2^{n_2} - \lambda_2, \dots, X_m^{n_m} - \lambda_m\}$ is a left Gröbner basis of the left ideal $\mathcal{I}$ that it generates. For any left ideal*

$\mathcal{J}$ containing $\mathcal{I}$ we obtain an m-dimensional constacyclic code $C = \mathcal{J}/\mathcal{I} \subset \mathfrak{K}_m^{\theta_1,\ldots,\theta_m}/\mathcal{I}$ over $\mathbb{F}_q$ of length $n_1 n_2 \cdots n_m$. The encoding $E(w) = w - \overline{w}^{\mathcal{J}} \in \mathcal{J}$ of the standard monomials of $\mathfrak{K}_m^{\theta_1,\ldots,\theta_m}/\mathcal{I}$ which are not standard monomials of $\mathfrak{K}_m^{\theta_1,\ldots,\theta_m}/\mathcal{J}$ form a basis of code C.

PROOF. In the ring $\mathfrak{K}_m^{\theta_1,\ldots,\theta_m}$ the S-polynomial $S(f_i, f_j) = X_j^{n_j} f_i - X_i^{n_i} f_j$ of $f_i = X_i^{n_i} - \lambda_i$ and $f_j = X_j^{n_j} - \lambda_j$ is $\theta_i^{n_i}(\lambda_j) X_i^{n_i} - \theta_j^{n_j}(\lambda_i) X_j^{n_j}$. The reduction of $S(f_i, f_j)$ by the G is obtained by substracting

$$\theta_i^{n_i}(\lambda_j) f_i - \theta_j^{n_j}(\lambda_i) f_j = \theta_i^{n_i}(\lambda_j)\lambda_i - \theta_j^{n_j}(\lambda_i)\lambda_j$$

and is zero according to the assumption in the lemma. This shows that G is a left Gröbner basis of the left ideal $\mathcal{I} \subset \mathfrak{K}_m^{\theta_1,\ldots,\theta_m}$ generated by G.

For the remainder of the proof we assume for simplicity that $m = 2$. We consider the $\mathbb{F}_q$-basis of $\mathfrak{K}_2^{\theta_1,\theta_2}/(X_1^{n_1} - 1, X_2^{n_2} - 1)$ given by :

$$\begin{array}{cccc} X_2^{n_2-1} & X_1 X_2^{n_2-1} & \ldots & X_1^{n_1-1} X_2^{n_2-1} \\ \vdots & \vdots & \ldots & \vdots \\ X_2 & X_1 X_2 & \ldots & X_1^{n_1-1} X_2 \\ 1 & X_1 & \ldots & X_1^{n_1-1} \end{array}$$

and represent the code word $\sum_{i=0}^{n_1-1} \sum_{j=0}^{n_2-1} a_{i,j} X_1^i X_2^j$ as in definition 6. The code $C = \mathcal{J}/\mathcal{I} \subset \mathfrak{K}_2^{\theta_1,\theta_2}/\mathcal{I}$ is a left $\mathfrak{K}_2^{\theta_1,\theta_2}$-module.

Multiplication of $a_{i,j} X_1^i X_2^j$ on the left by X_1 leads to

$$X_1 a_{i,j} X_1^i X_2^j = \theta_1(a_{i,j}) X_1^{i+1} X_2^j$$

and therefore to an application of θ_1 and a right shift for $i < n_1 - 1$. For $X_1 a_{i,j} X_1^{n_1-1} X_2^j = \theta_1(a_{i,j}) X_1^{n_1} X_2^j$ we must reduce the expression using the basis G by substracting $\theta_1(a_{i,j}) X_2^j (X_1^{n_1} - \lambda_1)$ which gives $\theta_1(a_{i,j}) X_2^j$. We obtain the first property of skew constacyclic codes stated in the above definition.

Multiplication of $a_{i,j} X_1^i X_2^j$ on the left by X_2 leads to

$$X_2 a_{i,j} X_1^i X_2^j = \theta_1(a_{i,j}) X_1^i X_2^{j+1}$$

and therefore to an application of θ_2 and a upward shift for $j < n_2 - 1$. For $X_2 a_{i,j} X_1^i X_2^{n_2-1} = \theta_2(a_{i,j}) X_1^i X_2^{n_2}$ we must reduce the expression using the basis G by substracting $\theta_2(a_{i,j}) X_1^i (X_2^{n_2} - \lambda_2)$ which gives $\theta_2(a_{i,j}) X_1^i$. We obtain the second property of skew constacyclic codes stated in the above definition. ∎

Example 6 *Consider $\mathbb{F}_{16} = \mathbb{F}_2[w]/\left(w^4 + w + 1\right)$, the automorphisms $\theta_1(w) = w^2, \theta_2(w) = w^4$. In the skew polynomial ring $\mathfrak{K}_2^{\theta_1,\theta_2}$ we have $X_1 X_2 = X_2 X_1$, $X_1 w = \theta_1(w) X_1 = w^2 X_1$ and $X_2 w = \theta_2(w) X_2 = w^4 X_2$. The previous theorem shows that $G = \{X_1^2 + w^3, X_2^3 + w^{12}\}$ is a left Gröbner basis of the left ideal $\mathcal{I}$ that G generates in $\mathfrak{K}_2^{\theta_1,\theta_2}$. The standard monomials of $\mathcal{I}$ belong to a rectangular 2×3-staircase. our goal is to construct a 2-dim skew constacyclic code $\mathcal{J}/\mathcal{I} \subset$*

$\mathfrak{K}_2^{\theta_1,\theta_2}/\mathcal{I}$ *for the parameters* $[6,3]$. *The left ideal* $\mathcal{J}$ *we are looking for must contain* 3 *standard monomials, which leads to the staircase*

$$\begin{array}{ccc} \cdot & \cdot & \cdot \\ \circ & \circ & \cdot \\ \bullet & \circ & \cdot \\ \bullet & \bullet & \cdot \end{array}$$

We found 12 *left ideals* $\mathcal{J}$. *Six of these left ideals gave a* $[6,3,3]$*-code, the other six an optimal* $[6,3,4]$*-code. One of the optimal codes is given by*

$$\mathcal{J} = \left(X_2^2 + w^{12}X_2 + w^9X_1 + w^5,\ X_1X_2 + w^4X_2 + w^6X_1 + w^7, X_1^2 + w^3\right).$$

The algorithm presented in Section 2, applied to left ideals, allows to compute all m-dimensional skew constacyclic codes of any given length and dimension.

5 m dimensional skew constacyclic codes with non commuting variables

In the following we will introduce relations of the form $X_jX_i = \beta_{i,j}X_iX_j$, in order to be able to use more values of λ_i such that $\{X_1^{n_1} - \lambda_1, \ldots, X_m^{n_m} - \lambda_m\}$ is a Gröbner basis and to use more iterated skew polynomial rings. This will lead to many more codes. The discussion in this section show that many more generalizations of this type are possible.

Definition 7 *A length* n_1n_2 *code over* $\mathbb{F}_q$ *is a* 2***-dimensional scaled skew constacylic code*** *if there exist* λ_1 *and* λ_2 *in* $\mathbb{F}_q \setminus \{0\}$ *such that any code word, viewed as a particular* m*-dimensional matrix of size* n_1n_2*, is invariant under the following two operations*

1. *application of*
   (a) *a cyclic shift in the columns*
   (b) *application of the automorphism* θ_1 *to all entries of the code word*
   (c) *multiplication of* j*-th entry of the resulting first column by*

$$\frac{\theta_2^{n_2-j}(\lambda_1)}{\prod_{\ell=0}^{n_2-j-1}\prod_{k=0}^{n_1-1}\theta_2^{\ell}(\theta_1^k(\beta_{1,2}))}.$$

2. *application of*
   (a) *a cyclic shift in the rows*
   (b) *applying the automorphism* θ_2 *to all entries of the code word*
   (c) *multiply the entries of the* j*-th column by* $\left(\prod_{k=0}^{j-2}\theta_1^k(\beta_{1,2})\right)$.

(d) multiplication of the new bottom row by $\lambda_2 \in \mathbb{F}_q^*$ and the j-th column by $\left(\prod_{k=0}^{j-2} \theta_1^k(\beta_{1,2})\right)$ for some $\beta_{1,2} \in \mathbb{F}_q^*$ and $j \in \{2, \ldots, n_1\}$.

We denote such a code $C_{\theta_1,\theta_2,\beta_{1,2}}$.

An $n_1 n_2$-dimensional code over $\mathbb{F}_q$ is a 2-dimensional skew scaled cyclic code over $\mathbb{F}_q$ if there is a basis of $\mathbb{F}_q^{n_1 n_2}$ and fixed automorphism θ_1 and θ_2 of $\mathbb{F}_q$ such that for any code word

$$\begin{pmatrix} a_{0,n_2-1} & a_{1,n_2-1} & \ldots & a_{n_1-1,n_2-1} \\ \vdots & \vdots & \ldots & \vdots \\ a_{0,1} & a_{1,1} & \ldots & a_{n_1-1,1} \\ a_{0,0} & a_{1,0} & \ldots & a_{n_1-1,0} \end{pmatrix},$$

both (here we shift in the columns to the right)

$$\begin{pmatrix} \frac{\theta_2^{n_2-1}(\lambda_1)}{\prod_{\ell=0}^{(n_2-1)-1} \prod_{k=0}^{n_1-1} \theta_2^\ell(\theta_1^k(\beta_{1,2}))} \theta_1(a_{n_1-1,n_2-1}) & \theta_1(a_{0,n_2-1}) & \ldots & \theta_1(a_{n_1-2,n_2-1}) \\ \vdots & \vdots & \ldots & \vdots \\ \frac{\theta_2(\lambda_1)}{\prod_{k=0}^{n_1-1} \theta_1^k(\beta_{1,2})} \theta_1(a_{n_1-1,1}) & \theta_1(a_{0,1}) & \ldots & \theta_1(a_{n_1-2,1}) \\ \lambda_1 \theta_1(a_{n_1-1,0}) & \theta_1(a_{0,0}) & \ldots & \theta_1(a_{n_1-2,0}) \end{pmatrix}$$

and (here we shift upwards in the rows)

$$\begin{pmatrix} \theta_2(a_{0,n_2-2}) & \beta_{1,2}\theta_2(a_{1,n_2-2}) & \ldots & \left(\prod_{k=0}^{n_1-2} \theta_1^k(\beta_{1,2})\right)\theta_2(a_{n_1-1,n_2-2}) \\ \vdots & \vdots & \ldots & \vdots \\ \theta_2(a_{0,0}) & \beta_{1,2}\theta_2(a_{1,0}) & \ldots & \left(\prod_{k=0}^{n_1-2} \theta_1^k(\beta_{1,2})\right)\theta_2(a_{n_1-1,0}) \\ \lambda_2\theta_2(a_{0,n_2-1}) & \lambda_2^{\theta_1}\beta_{1,2}\theta_2(a_{1,n_2-1}) & \ldots & \lambda_2^{\theta_1^{n_1-1}}\left(\prod_{k=0}^{n_1-2} \theta_1^k(\beta_{1,2})\right)\theta_2(a_{n_1-1,n_2-1}) \end{pmatrix}$$

belong to the code.

Definition 8 *([6], page 1887, relation 2.18) Consider θ_1, θ_2 two automorphisms of $\mathbb{F}_q$ and $\beta_{1,2} \in \mathbb{F}_q^*$ an invertible element. The automorphism θ_2 extends to an automorphism $\tilde{\theta}_2$ of $\mathbb{F}_q[X_1, \theta_1]$ by $\tilde{\theta}_2(X_1) = \beta_{1,2}X_1$. This allows to define an iterated skew polynomial ring $\mathfrak{Q}_2^{\theta_1,\theta_2,\beta_{1,2}} = \mathbb{F}_q[X_1, \theta_1][X_2, \tilde{\theta}_2]$. In $\mathfrak{Q}_2^{\theta_1,\theta_2,\beta_{1,2}}$ we have $X_1 a = \theta_1(a)X_1$, $X_2 a = \theta_2(a)X_2$ and $X_2X_1 = \beta_{1,2}X_1X_2$.*

In $\mathfrak{Q}_2^{\theta_1,\theta_2,\beta_{1,2}}$ we obtain

$$X_2X_1^i = (\underbrace{\beta_{1,2}X_1\beta_{1,2}X_1 \cdots \beta_{1,2}X_1}_{i})X_2 = \left(\prod_{k=0}^{i-1} \theta_1^k(\beta_{1,2})\right)X_1^iX_2 \qquad (5)$$

from which we decuce the following relation $(*)$

$$\begin{aligned} X_2^{n_2}X_1^{n_1} &= X_2^{n_2-1}\left(\prod_{k=0}^{n_1-1}\theta_1^k(\beta_{1,2})\right)X_1^{n_1}X_2 \\ &= \theta_2^{n_2-1}\left(\prod_{k=0}^{n_1-1}\theta_1^k(\beta_{1,2})\right)X_2^{n_2-1}X_1^{n_1}X_2 \\ &= \left(\prod_{k=0}^{n_1-1}\theta_2^{n_2-1}(\theta_1^k(\beta_{1,2}))\right)X_2^{n_2-1}X_1^{n_1}X_2 \\ &= \left(\prod_{\ell=0}^{n_2-1}\prod_{k=0}^{n_1-1}\theta_2^{\ell}(\theta_1^k(\beta_{1,2}))\right)X_1^{n_1}X_2^{n_2} \qquad (*) \end{aligned}$$

Theorem 2 *Consider the skew polynomial ring $\mathfrak{O}_2^{\theta_1,\theta_2,\beta_{1,2}}$ defined above. For any $\lambda_1,\lambda_2,\beta_{1,2}$ in $\mathbb{F}_q^*$ satisfying the relation*

$$\frac{\theta_2^{n_2}(\lambda_1)}{\lambda_1} = \left(\prod_{\ell=0}^{n_2-1}\prod_{k=0}^{n_1-1}\theta_2^{\ell}(\theta_1^k(\beta_{1,2}))\right)\frac{\theta_1^{n_1}(\lambda_2)}{\lambda_2} \qquad (6)$$

the set $G=\{X_1^{n_1}-\lambda_1, X_2^{n_2}-\lambda_2\}$ is a left Gröbner basis of the ideal $\mathcal{I}$ it generates in $\mathfrak{O}_2^{\theta_1,\theta_2,\beta_{1,2}}$. For any left ideal $\mathcal{J}$ of $\mathfrak{O}_2^{\theta_1,\theta_2,\beta_{1,2}}$ that contains $\mathcal{I}$, the code $\mathcal{J}/\mathcal{I}\subset\mathfrak{O}_2^{\theta_1,\theta_2,\beta_{1,2}}/\mathcal{I}$ is a 2-dimensional scaled skew constacylic code $C_{\theta_1,\theta_2,\beta_{1,2}}$ over $\mathbb{F}_q$ of length n_1n_2. The encoding $E(w)=w-\overline{w}^{\mathcal{J}}\in\mathcal{J}$ of the standard monomials of $\mathfrak{O}_2^{\theta_1,\theta_2,\beta_{1,2}}/\mathcal{I}$ which are not standard monomials of $\mathfrak{O}_2^{\theta_1,\theta_2,\beta_{1,2}}/\mathcal{J}$ form a basis of $C_{\theta_1,\theta_2,\beta_{1,2}}$.

Proof. In order to show that G is a Gröbner basis we compute the reduction of the polynomial $\mathrm{SPoly}(X_1^{n_1}-\lambda_1, X_2^{n_2}-\lambda_2)$

$$\begin{aligned} &= X_2^{n_2}(X_1^{n_1}-\lambda_1)-\left(\prod_{\ell=0}^{n_2-1}\prod_{k=0}^{n_1-1}\theta_2^{\ell}(\theta_1^k(\beta_{1,2}))\right)X_1^{n_1}(X_2^{n_2}-\lambda_2) \\ &= \left(\prod_{\ell=0}^{n_2-1}\prod_{k=0}^{n_1-1}\theta_2^{\ell}(\theta_1^k(\beta_{1,2}))\right)X_1^{n_1}X_2^{n_2}-X_2^{n_2}\lambda_1 \\ &\quad -\left(\prod_{\ell=0}^{n_2-1}\prod_{k=0}^{n_1-1}\theta_2^{\ell}\theta_1^k(\beta_{1,2}))\right)X_1^{n_1}X_2^{n_2}+\left(\prod_{\ell=0}^{n_2-1}\prod_{k=0}^{n_1-1}\theta_2^{\ell}\theta_1^k(\beta_{1,2}))\right)X_1^{n_1}\lambda_2 \\ &= -\theta_2^{n_2}(\lambda_1)X_2^{n_2}+\left(\prod_{\ell=0}^{n_2-1}\prod_{k=0}^{n_1-1}\theta_2^{\ell}(\theta_1^k(\beta_{1,2}))\right)\theta_1^{n_1}(\lambda_2)X_1^{n_1} \\ &= \theta_2^{n_2}(\lambda_1)\lambda_2-\left(\prod_{\ell=0}^{n_2-1}\prod_{k=0}^{n_1-1}\theta_2^{\ell}(\theta_1^k(\beta_{1,2}))\right)\theta_1^{n_1}(\lambda_2)\lambda_1 \end{aligned}$$

Therefore, if the relation (6) holds, then $\mathrm{SPoly}(X_1^{n_1}-\lambda_1, X_2^{n_2}-\lambda_2)$ reduces to 0, showing that $(X_1^{n_1}-\lambda_1, X_2^{n_2}-\lambda_2)$ is a Gröbner basis.

For a 2-dimensional skew constacyclic code

$$\mathcal{J}/(X_1^{n_1}-\lambda_1, X_2^{n_2}-\lambda_2) \subset \mathfrak{Q}_2^{\theta_1,\theta_2,\beta_{1,2}}/(X_1^{n_1}-\lambda_1, X_2^{n_2}-\lambda_2)$$

we consider again the $\mathbb{F}_q$-basis (2)

$$\begin{array}{llll} X_2^{n_2-1} & X_1X_2^{n_2-1} & \dots & X_1^{n_1-1}X_2^{n_2-1} \\ \vdots & \vdots & \dots & \vdots \\ X_2 & X_1X_2 & \dots & X_1^{n_1-1}X_2 \\ 1 & X_1 & \dots & X_1^{n_1-1} \end{array}$$

of $\mathfrak{Q}_2^{\theta_1,\theta_2,\beta_{1,2}}/(X_1^{n_1}-\lambda_1, X_2^{n_2}-\lambda_2)$ and represent the code word again in the basis (1). By definition the code is an $\mathfrak{Q}_2^{\theta_1,\theta_2,\beta_{1,2}}$-module. The entry $a_{i,j}$ corresponds to the monomial $a_{i,j}X_1^{i-1}X_2^{j-1}$.
1) **Multiplication on the left by** X_1 results in

$$X_1a_{i,j}X_1^{i-1}X_2^{j-1} = \theta_1(a_{i,j})X_1^{(i+1)-1}X_2^{j-1}$$

and therefore, for $i-1 < n_1-1$ in a cyclic shift and application of θ_1 in the first row, and in a shift and application of θ_1 of the n_1-1 first elements of all other rows. In order to compute the affect on the last entry of the $j+1$-th row, we need to reduce the expression $\theta_1(a_{n-1,j-1})X_1^{n_1}X_2^j$ using the Gröbner basis $(X_1^{n_1}-\lambda_1, X_2^{n_2}-\lambda_2)$. The calculations in relation (*) can be adapted to

$$X_2^jX_1^{n_1} = \left(\prod_{\ell=0}^{j-1}\prod_{k=0}^{n_1-1}\theta_2^\ell(\theta_1^k(\beta_{1,2}))\right)X_1^{n_1}X_2^j$$

Therefore, to reduce the expression $\theta_1(a_{n-1,j-1})X_1^{n_1}X_2^j$, we have to substract

$$\theta_1(a_{n-1,j-1})X_1^{n_1}X_2^j \;-\; \theta_1(a_{n-1,j-1})\left(\prod_{\ell=0}^{j-1}\prod_{k=0}^{n_1-1}\theta_2^\ell(\theta_1^k(\beta_{1,2}))\right)^{-1} X_2^j\,(X_1^{n_1}-\lambda_1)$$

which leads to

$$= \left(\prod_{\ell=0}^{j-1}\prod_{k=0}^{n_1-1}\theta_2^\ell(\theta_1^k(\beta_{1,2}))\right)^{-1}\theta_2^j(\lambda_1)\theta_1(a_{n-1,j-1})X_2^j$$

showing that the first entries of the $j+1$-th row is

$$\frac{\theta_2^j(\lambda_1)}{\prod_{\ell=0}^{j-1}\prod_{k=0}^{n_1-1}\theta_2^\ell(\theta_1^k(\beta_{1,2}))}\theta_1(a_{n-1,j-1}).$$

2) **Multiplication on the left by** X_2 results in

$$\begin{aligned} X_2a_{i,j}X_1^{i-1}X_2^{j-1} &= \theta_2(a_{i,j})X_2X_1^{i-1}X_2^{j-1} \\ &= \theta_2(a_{i,j})\left(\prod_{k=0}^{(i-1)-1}\theta_1^k(\beta_{1,2})\right)X_1^{i-1}X_2^j \end{aligned}$$

When $j = n_2$ we need to reduce the expression using $X_2^{n_2} - \lambda_2$. For that we have to substract to the above $\theta_2(a_{i,n_2-1}) \left(\prod_{k=0}^{i-2} \theta_1^k(\beta_{1,2})\right) X_1^{i-1} (X_2^{n_2} - \lambda_2)$ which leads to

$$\left(\prod_{k=0}^{i-2} \theta_1^k(\beta_{1,2})\right) \theta_1^{i-1}(\lambda_2)\theta_2(a_{i,n_2-1})X_1^{i-1}$$

This shows that C corresponds to the 2-dimensional scaled skew constacylic code $C_{\theta_1,\theta_2,\beta_{1,2}}$ ∎

Example 7 *Consider* $\mathbb{F}_{27} = \mathbb{F}_3[w]/\left(w^3 - w + 1\right)$, *the automorphisms* $\theta_1(w) = w^3, \theta_2(w) = w^3$ *and the element* $\beta_{1,2} = w^6 \in \mathbb{F}_{27}$. *The previous theorem shows that* $G = \{X_1^3 + 1, X_2^3 + 1\}$ *is a Gröbner basis of the ring* $\mathfrak{Q}_2^{\theta_1,\theta_2,\beta_{1,2}}$ *which generates a left ideal* $\mathcal{I}$ *whose standard monomials belong to a quadratic staircase of length 3. We now look for a left ideal* $\mathcal{J}$ *containing* $\mathcal{I}$. *The staircases of* $\mathcal{I}$ *are represented by* • *and* ∘ *and those of* $\mathcal{J}$ *by* •*:*

$$\begin{array}{cccc} \cdot & \cdot & \cdot & \cdot \\ \circ & \circ & \circ & \cdot \\ \bullet & \bullet & \circ & \cdot \\ \bullet & \bullet & \bullet & \cdot \end{array}$$

Using the algorithm of Section 2 we found 1365 *left ideals* $\mathcal{J} \subset \mathfrak{Q}_2^{\theta_1,\theta_2,\beta_{1,2}}$ *containing* $\mathcal{I}$. *An example of such a code is given by:*

$$\mathcal{J} = \big(X_1^3 + 1,\ X_2^2 + w^{16}X_1X_2 + w^{24}X_2 + w^{22}X_1^2 + w^{19}X_1 + w^{25},$$

$$X_1^2X_2 + w^7X_1X_2 + w^{18}X_2 + w^3X_1^2 + w^8X_1 + w\big)$$

This scaled skew consta-cylic code $C_{\theta_1,\theta_2,\beta_{1,2}}$ *is an optimal* $[9, 4, 6]$ *code over* $\mathbb{F}_{27}$.

Note that the leading monomials correspond to three upper corners of the staircase of $\mathcal{J}$. *In order to compute a basis of the corresponding scaled skew consta-cylic code* $C_{\theta_1,\theta_2,\beta_{1,2}}$ *we encode the* 4 *standard monomials* $e_{0,2} = X_2^2, e_{1,2} = X_2^2X_1, e_{2,2} = X_2^2X_1^2, e_{2,1} = X_2X_1^2$ *of* $\mathcal{I}$ *that are not standard monomials of* $\mathcal{J}$ *by computing* $E(e_{i,j}) = e_{i,j} - \overline{e_{i,j}}^{\mathcal{J}} \in \mathcal{J}$. *We obtain the* 4 *code words that generate the code:*

$$\begin{aligned} E(e_{0,2}) &= X_2^2 + w^{16}X_1X_2 + w^{24}X_2 + w^{22}X_1^2 + w^{19}X_1 + w^{25} \\ E(e_{1,2}) &= X_1X_2^2 + w^8X_1X_2 + wX_2 + w^9X_1^2 + w^2X_1 + w^4 \\ E(e_{2,2}) &= X_1^2X_2^2 + w^2X_1X_2 + w^3X_2 + w^{21}X_1^2 + w^{16}X_1 + w^7 \\ E(e_{2,1}) &= X_1^2X_2 + w^7X_1X_2 + w^{18}X_2 + w^3X_1^2 + w^8X_1 + w \end{aligned}$$

which can be represented as matrices using the corresponding basis form (2)

$$M_{0,2} = \begin{pmatrix} 1 & 0 & 0 \\ w^{24} & w^{16} & 0 \\ w^{25} & w^{19} & w^{22} \end{pmatrix},\ M_{1,2} = \begin{pmatrix} 0 & 1 & 0 \\ w & w^8 & 0 \\ w^4 & w^2 & w^9 \end{pmatrix},$$

$$M_{2,2} = \begin{pmatrix} 0 & 0 & 1 \\ w^3 & w^2 & 0 \\ w^7 & w^{16} & w^{21} \end{pmatrix},\ M_{2,1} = \begin{pmatrix} 0 & 0 & 0 \\ w^{18} & w^7 & 1 \\ w & w^8 & w^3 \end{pmatrix}$$

Multiplication of any codeword by X_1 from the left results in a codeword. For $E(e_{0,2})$ we get:

$$X_1E(e_{0,2}) = X_1X_2^2 + w^{22}X_1^2X_2 + w^{20}X_1X_2 + w^{14}X_1^3 + w^5X_1^2 + w^{23}X_1.$$

Reducing with the Gröbner Basis G of $\mathcal{I}$ we obtain

$$\overline{X_1E(e_{0,2})}^G = X_1X_2^2 + w^{22}X_1^2X_2 + w^{20}X_1X_2 + w^5X_1^2 + w^{23}X_1 + w.$$

When we represent this code word as matrices using the corresponding basis (2), we get

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & w^{20} & w^{22} \\ w & w^{23} & w^5 \end{pmatrix}$$

This matrix can also be constructed using the first rule shown after Definition 7.

Multiplication of any codeword by X_2 from the left results in a codeword. For $E(e_{0,2})$ we get:

$$X_2E(e_{0,2}) = X_2^3 + w^2X_1X_2^2 + w^{20}X_2^2 + w^{12}X_1^2X_2 + w^{11}X_1X_2 + w^{23}X_2.$$

Reducing with the Gröbner Basis G of $\mathcal{I}$ we obtain

$$\overline{X_2E(e_{0,2})}^G = w^2X_1X_2^2 + w^{20}X_2^2 + w^{12}X_1^2X_2 + w^{11}X_1X_2 + w^{23}X_2 + 2$$

and in matrix representation

$$\begin{pmatrix} w^{20} & w^2 & 0 \\ w^{23} & w^{11} & w^{12} \\ 2 & 0 & 0 \end{pmatrix}$$

This matrix can also be constructed using the second rule shown after Definition 7.

Example 8 *Consider $\mathbb{F}_{16} = \mathbb{F}_2[w]/\left(w^4 + w + 1\right)$, the automorphisms $\theta_1(w) = w^2, \theta_2(w) = w^4$ and the element $\beta_{1,2} = w \in \mathbb{F}_{16}$. The set*

$$G = \{X_1^2 + w^3, X_2^3 + w^{12}\}$$

is a Gröbner basis of the ring $\mathfrak{Q}_2^{\theta_1,\theta_2,\beta_{1,2}}$ which generates a left ideal $\mathcal{I}$ whose standard monomials belong to a quadratic 2×3-staircase. We now look for a left ideal $\mathcal{J}$ containing $\mathcal{I}$ containing 3 standard monomials. There are two possible staircases :

$$\begin{array}{ccc} \cdot & \cdot & \cdot \\ \bullet & \circ & \cdot \\ \bullet & \circ & \cdot \\ \bullet & \circ & \cdot \end{array} \qquad \textit{and} \qquad \begin{array}{ccc} \cdot & \cdot & \cdot \\ \circ & \circ & \cdot \\ \bullet & \circ & \cdot \\ \bullet & \bullet & \cdot \end{array}$$

For the first staircase, we found 3 *left ideals* $\mathcal{J} \subset \mathfrak{Q}_2^{\theta_1,\theta_2,\beta_{1,2}}$ *containing* $\mathcal{I}$*, using the algorithm of Section 2. Each of these left ideals gave a* $[6,3,2]$*-code, all three codes are equivalent. An example of such a code is given by:*

$$\mathcal{J} = \left(X_2^3 + w^{12},\ X_1 + w\right).$$

For the second staircase, we found 12 *left ideals. Six of these left ideals gave a* $[6,3,3]$*-code, the other six an optimal* $[6,3,4]$*-code. The codes in both sets are equivalent codes. An example of an optimal code is given by:*

$$\mathcal{J} = \left(X_2^2 + w^8 X_2 + w^4 X_1 + 1,\ X_1 X_2 + w^3 X_2 + w^4 X_1 + w^5, X_1^2 + w^3\right).$$

This approach extends to the case of m-variables where we need to consider m automorphism $\theta_1, \ldots, \theta_m$ of $\mathbb{F}_q$ and extend recursively θ_i to an automorphism $\tilde{\theta}_i$ of $\mathbb{F}_q[X_1, \theta_1] \ldots [X_i, \tilde{\theta}_i]$ by $\tilde{\theta}_i(X_j) = \beta_{j,i} X_j$ where $\beta_{j,i} \in \mathbb{F}_q^*$ ([6], page 1887, relation 2.18). In the polynomial ring $\mathbb{F}_q[X_1, \theta_1] \ldots [X_n, \tilde{\theta_n}]$ we have $X_i a = \theta_i(a) X_i$ and $X_i X_j = \beta_{j,i} X_j X_i$ for $j < i$. In this ring we can choose $\binom{m}{2}$ values $\beta_{j,i}$. In order to test if $\{X_1^{n_1} - \lambda_1, \ldots, X_m^{n_m} - \lambda_m\}$ is a Gröbner basis we need to check $\binom{m}{2}$ relations of the form (6), but we can also freely choose the $\binom{m}{2}$ invertible constants $\beta_{i,j}$ $(1 \leq i < j \leq n_j)$.

6 Conclusion

In [8] we showed that a Gröbner basis for left ideals can be defined for various iterated skew polynomials that satisfy the requirements of definition 5, including iterated skew polynomials with derivations or over chain rings. This allows many generalizations.

References

[1] D. Boucher and F. Ulmer, *Self-dual skew codes and factorization of skew polynomials*, Journal of Symbolic Computation, 60, 47–61 (2014)

[2] L. Chaussade, *Codes correcteurs avec les polynômes tordus*, Thèse Université de Rennes 1 (2010)

[3] D.A. Cox, J. Little, D. Shea, *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Springer Undergraduate Texts in Mathematics, 4th Edition (2015)

[4] D.A. Cox, J. Little, D. Shea, *Using Algebraic Geometry*, Graduate Texts in Mathematics 185, Springer science+business media NewYork (1998).

[5] F. Dumas, *An introduction to noncommutative polynomial invariants*, CIMPA course "Homological methods and representations of noncommutative algebras", Argentina, 2006

[6] César Fernando Venegas Ramírez, *Automorphisms for Skew PBW Extensions and Skew Quantum Polynomial Rings*, Communications in Algebra, 43:5, 1877-1897 (2015)

[7] C. Gallego, 0. Lezama, *Gröbner Bases for Ideals of σ-PBW Extensions*, Communications in Algebra 39(1):50-75 (2011)

[8] W. Geiselmann and F. Ulmer, *Skew Reed Muller codes*, Contemporary Mathematics, Volume 727, 107–116 (2019)

[9] C. Güneri, F. Özbudak, *Multidimensional cyclic codes and Artin-Schreier type hypersurfaces over finite fields*, Finite Fields and Their Applications 14 (2008) 44–58

[10] H. Imai, *A Theory of Two-Dimensional Cyclic Codes* , Information and Control, Vol. 34, 1–21 (1977)

[11] E. Martinez-Moro and I.F. Rua, *Multivariable Codes Over Finite Chain Rings: Serial Codes*, SIAM Journal on Discrete Mathematics, 2006, Vol. 20, No. 4 : pp. 947-959

[12] Mostafanasab, H. *2-D skew constacyclic codes over $R[x, y; \rho, \theta]$*, Journal of Algebra and Related Topics Vol. 4, No 2, (2016), pp 49-63

[13] O. Ore, Theory of Non-Commutative Polynomials, *The Annals of Mathematics*, 2nd Ser, Vol. 34, No. 3. pp. 480-508 (1933)

[14] M. Saleemi, *Coding Theory via Gröbner Base*, Phd Technischen Universität Hamburg-Harburg (2012).

[15] A. Sharma and M. Bhaintwal, *A class of 2D skew-cyclic codes over $\mathbb{F}_q+u\mathbb{F}_q$*, AAECC 30, 471–490 (2019)

[16] Z. Sepasdar, Some notes on the characterization of two dimensional skew cyclic codes, *Journal of Algebra and Related Topics*, Vol. 4, No. 3. pp. 1–8 (2016)

[17] M.G. Voskoglou, *Extending derivations and automorphisms to skew polynomial rings*, Publication de l'Institut Mathématique, Nouvelle série, tome 39 (53), pp. 79–82 (1986).

[18] L. Xiuli, L. Hongyan, *2-D skew cyclic codes over $\mathbb{F}_q[x, y; \rho, \theta]$*, Finite Fields Appl. 25, 49–63 (2014)

[19] X. Zhao and Y. Zhang, *A signature-based algorithm for computing Gröbner-Shirshov bases in skew solvable polynomial rings*, Open Mathematics. Volume 13, Issue 1, ISSN (Online) 2391-5455, DOI: 10.1515/math-2015-0028, May 2015