Chapter 1

Finding a Gröbner basis for the ideal of recurrence relations on m-dimensional periodic arrays

Ivelisse M. Rubio

Department of Computer Science, University of Puerto Rico, Box 70377, S.J., PR 00936-8377 iverubio@gmail.com

Moss Sweedler

Department of Mathematics, Cornell University, 310 Malott Hall, Ithaca, NY 14853 3.14159x2.71828@gmail.com

Chris Heegard

Native Intelligence, 17179 La Brisa Ct., Sugarloaf, FL 33042
heegard@nativei.com

1.1 Abstract

Recent developments in applications of multidimensional periodic arrays [9] have drawn new attention to the computation of Gröbner bases for the ideal of linear recurrence relations on the arrays. An m-dimensional infinite array can be represented by a multivariate power series sitting within the ring of multivariate Laurent series. We reinterpret the problem of finding linear recurrence relations on m-dimensional periodic arrays as finding the kernel of a module map involving quotients of Laurent series and present an algorithm to compute a Gröbner basis for this kernel. The algorithm does not assume the knowledge of a generating set for the kernel of this ideal and it is based on linear algebra computations. Finding a generating set is one application of the algorithm.

1.2 Introduction

There are different algorithms to find Gröbner bases for the ideal of linear recurrence relations on multidimensional arrays (or equivalently, multivariate power series). One of the best known is Sakata's algorithm [14,15]. This algorithm is an extension to m-dimensions of the Berlekamp-Massey algorithm and has been used for decoding multidimensional cyclic codes and algebraic geometric codes [12, 13, 16]. Recent developments in applications of multidimensional periodic arrays [9] have drawn new attention to the computation of Gröbner bases for the ideal of linear recurrence relations on the arrays. The approach that we present here can be implemented easily and is suitable for these new applications.

In [7], Faugere et al. presented an efficient algorithm to transform a Gröbner basis of a 0-dimensional ideal with respect to a given monomial order into a Gröbner basis with respect to another monomial order. Shortly after it appeared, Moss Sweedler and Lee Taylor showed in [17] that the ideas in [7] could be expanded and cast as: 1) an initial Gröbner basis allows one to effectively do linear algebra in the finite dimensional vector space quotient; 2) if one can effectively do linear algebra in a finite dimensional vector space quotient module, then one can find a reduced Gröbner basis for the kernel ideal, without having an initial generating set for this kernel.

Let $\mathcal{F}$ be a field and $\mathcal{F}[\mathbf{x}] := \mathcal{F}[x_1, \ldots, x_m]$ be the ring of polynomials in m variables and coefficients in $\mathcal{F}$. The Sweedler-Taylor algorithm in [17] computes reduced Gröbner bases for 0-dimensional ideals $I \subseteq \mathcal{F}[\mathbf{x}]$ and it is based upon considering ascending subspaces of $\mathcal{F}[\mathbf{x}]/I$. The ascending subspaces are spanned by the image of monomials which are ascending in the monomial order. An ascending chain of subspaces of a finite dimensional vector space must stabilize and this forces termination of the algorithm. A description of the Sweedler-Taylor algorithm and a complete proof of its validity was presented in [11]. Like Sakata's algorithm, this algorithm does not assume the knowledge of a basis for the ideal. Other algorithms to compute a basis for $\mathcal{F}[\mathbf{x}]/I$ have been presented in [1–4].

After reinterpreting the definition and basics of linear recurrence relations on multidimensional periodic arrays, we modify the Sweedler-Taylor algorithm to find a Gröbner basis that generates these relations. This analog to the Sweedler-Taylor algorithm computes what we call *lead monomial generating sets* and, under certain conditions, a lead monomial generating set turns out to be a Gröbner basis for the ideal of linear recurrence relations. We will see in Proposition 1.2 that twice the period minus the

dimension of the array is an upper bound for the degree of the polynomials required to form a Gröbner basis for the ideal of linear recurrence relations valid on the array with respect to the graded lexicographic order.

The next example on a one dimensional array illustrates the first steps of the algorithm.

Example 1.1.

Consider the one dimensional array $S = (3, 5, 9, 6, \ldots)$ over $\mathbb{F}_{11}$, the finite field with 11 elements. This sequence is defined by the recurrence $S_0 = 3$, and $S_{i+1} = 2^{i+1} + S_i$, for $i > 0$. One can write this sequence as the power series:

$$S(x) = S_0 + S_1x + S_2x^2 + S_3x^3 + \cdots = 3 + 5x + 9x^2 + 6x^3 + \cdots .$$

A polynomial $C = \sum_{i=0}^{L} C_i x^i \in \mathbb{F}_{11}[x]$ defines a linear recurrence relation at a point S_u of the array S if $L \leq u$ and $\sum_{i=0}^{L} C_i S_{i+u-L} = 0$. We say that the polynomial is valid for the array S if it defines a linear recurrence relation for each $u \geq L$. The set of all linear recurrence relations valid on the array S form an ideal in $\mathbb{F}_{11}[x]$. To find a polynomial valid for the array one needs a polynomial $C_0 + C_1x + C_2x^2 + \cdots + C_Lx^L$ such that

$$C_03 + C_15 + C_29 + \cdots + C_LS_L = 0, \quad C_05 + C_19 + \cdots + C_LS_{L+1} = 0,$$
$$C_09 + C_16 + \cdots + C_LS_{L+2} = 0, \ldots .$$

This would be the same as finding constants $C_0, C_1, \ldots, C_L$ such that, in the following table, when one sums the rows multiplied by their respective constant, and consider the reduction mod 11, one gets a sequence of 0's.

$$\begin{array}{c|cccc} C_0 & 3 & 5 & 9 & 6 \ \cdots \\ C_1 & 5 & 9 & 6 & \cdots \\ C_2 & 9 & 6 & \cdots & \\ \vdots & & \vdots & \cdots & \\ C_k & S_k & S_{k+1} & \cdots & \\ \hline & 0 & 0 & \cdots & \end{array} \tag{1.1}$$

Note that each shift is equivalent to multiplying the power series $S(x)$ by $x^{-1}, x^{-2}, \ldots$ respectively and "mod out" (or ignore) the terms with negative exponents. In Section 1.4.1 we define these shift operations algebraically. In this example, if one consider $C_0 = 2, C_1 = 8, C_2 = 1, C_i = 0$ for $i > 2$, one gets the following operations modulo 11 on the power series $S(x)$:

$$\begin{aligned} 2 \ & \left(3 + 5x + 9x^2 + 6x^3 + \cdots\right) \\ + \ 8x^{-1} \ & \left(3 + 5x + 9x^2 + 6x^3 + \cdots\right) \\ + \ x^{-2} \ & \left(3 + 5x + 9x^2 + 6x^3 + \cdots\right). \end{aligned} \tag{1.2}$$

Ignoring the terms with negative exponents one gets $S'_2x^2 + S'_3x^3 + \cdots$; hence, the polynomial x^2+8x+2 gives a recurrence relation up to S_3. The theory and algorithm in this paper imply that this is actually the minimal polynomial valid for the array S.

For this particular example, since we have the explicit recurrence, $S_{i+1} = 2^{i+1} + S_i$, we may directly verify the relation $x^2 + 8x + 2$:

$$C_0S_i + C_1S_{i+1} + C_2S_{i+2} = 2S_i + 8S_{i+1} + S_{i+2} = 2S_i + 8\left(2^{i+1} + S_i\right) + S_{i+2}$$
$$= 2S_i + 8\left(2^{i+1} + S_i\right) + 2^{i+2} + 2^{i+1} + S_i = 11S_i + 112^{i+1} = 0.$$

Since this holds for the recurrence, it tells us that $x^2 + 8x + 2$ holds not just up to S_3 but for the full array S. What if we did not have the recurrence but had a black-box that gave as much (but only a finite amount) of a sequence requested? How might one determine such an equation, as we did here, finding x^2+8x+2? How might one determine if there even exists such an equation? Suppose you had the black-box and the information that there is an equation of degree less than some specific degree. How might one determine the equation?

Note that one could find the coefficients of C by performing row reduction in (1.1) and finding a linear dependency relation among the rows. Of course, the array is infinite and one might not be able to compute the dependency relations effectively. But the arrays that we will consider are periodic and we will see that it will be enough to compute the dependency relations in a finite subarray.

From (1.2) note that, intuitively, what one is looking is for a polynomial $C(x)$ such that in $C\left(x^{-1}\right)S(x)$ the only non-zero terms have negative exponents.

The method used here is an application of the analog to the Sweedler-Taylor algorithm that will be described in Section 1.5 after we introduce the concept of lead monomial generating sets. In Section 1.4 we present the basics of linear recurrence relations and reformulate the problem in order to use the algorithm to find a Gröbner basis for the ideal of linear recurrence relations on an m-dimensional periodic array.

1.3 Gröbner bases and the Sweedler-Taylor algorithm

The set of polynomials that define the linear recursion relations on an m-dimensional array form an ideal over $\mathcal{F}[\mathbf{x}]$. These ideals have a finite generating set and Gröbner bases are ideal generating sets with "nice properties".

Let $\mathbb{N}_0 := \{0, 1, 2, \ldots\}$ and consider the set of exponents $\alpha = (\alpha_1, \ldots, \alpha_m) \in \mathbb{N}_0^m$. Set $\alpha \leq \beta$ if and only if $\alpha_i \leq \beta_i$ for $i = 1, \ldots, m$. This defines the partial order of divisibility where $\mathbf{x}^\alpha | \mathbf{x}^\beta$ if and only if $\alpha \leq \beta$. We say that a monomial $\mathbf{x}^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_m^{\alpha_m}$ in a set of monomials is minimal with respect to $\leq$ if there is no other monomial $\mathbf{x}^\beta$ in the set with $\beta < \alpha$.

We say that $<_T$ is a **monomial order** if it is a well ordering in $\mathbb{N}_0^m$ such that $<_T$ is a total order, and $\alpha <_T \beta$ implies that $\alpha + \gamma <_T \beta + \gamma$ for $\alpha, \beta, \gamma \in \mathbb{N}_0^m$. Note that divisibility is not a total order and hence is not a monomial order, but it is compatible with any monomial order in the sense that $\mathbf{x}^\alpha | \mathbf{x}^\beta$ implies that $\mathbf{x}^\alpha \leq_T \mathbf{x}^\beta$.

Define $|\alpha| = \sum_{i=1}^m \alpha_i$. Two common examples of monomial orders are the **lexicographical order**, where $\alpha <_{lex} \beta$ if in $\beta - \alpha$ the left most non-zero entry is positive, and the **graded lexicographical order**, where $\alpha <_{grlex} \beta$ if $|\alpha| < |\beta|$ or if $|\alpha| = |\beta|$ and $\alpha <_{lex} \beta$. We will use the following notation:

Let $f = \sum_\alpha a_\alpha \mathbf{x}^\alpha$ be a nonzero polynomial with each $a_\alpha \neq 0$ and $I \subset \mathcal{F}[\mathbf{x}]$. Then,

(1) $LE(f) = leadexp(f)$ is the largest exponent vector α in f with respect to $<_T$.
(2) $LM(f)$ denotes the leading monomial of f and it equals $\mathbf{x}^{LE(f)}$.
(3) $LC(f)$ denotes the coefficient of $LM(f)$. In other words, the so called leading term of f is $LC(f)LM(f)$.
(4) $LE(I) := \{LE(f) \mid 0 \neq f \in I\} \subseteq \mathbb{N}_0^m$. (Note that if $I = \{0\}$, then $LE(I) = \{\}$.)
(5) $LM(I) := \{LM(f) \mid 0 \neq f \in I\} = \{\mathbf{x}^\alpha \mid \alpha \in LE(I)\}$. (If $I = \{0\}$, then $LM(I) = \{\}$.)

Definition 1.1. Let $G = \{g_1, \ldots, g_l\} \subset I$, I an ideal in $\mathcal{F}[\mathbf{x}]$. One says that G is a **Gröbner basis** for I with respect to $<_T$ if $\langle LM(g_1), \ldots, LM(g_l)\rangle = \langle LM\,(I)\rangle$. If $LC(g_i) = 1$ for $i = 1, \ldots, l$ and $LM(g_i)$ does not divide any term of g_j for $i \neq j$, then one says that G is a **reduced Gröbner basis** for I with respect to $<_T$.

It is a standard result that a Gröbner basis for an ideal generates the ideal. Also $G = \{g_1, \ldots, g_l\} \subset I$ is a Gröbner basis for I if and only if for any $p \in I$, $LM(g_i) | LM(p)$ for some $g_i \in G$ (see [6]).

An important concept that will be used to determine a finite subarray $S' \subset S$ that is sufficient to compute a Gröbner basis for the ideal of linear

recurrence relations on S is the concept of a *delta set*. A set $\Delta \subset \mathbb{N}_0^m$ is called a **delta set** if it satisfies 1 in the following lemma:

Lemma 1.1. *Let $\Delta, \Gamma \subset \mathbb{N}_0^m$ be set theoretic complements. The following conditions are equivalent:*

(1) For $\beta \in \Delta, \alpha \in \mathbb{N}_0^m$, if $\alpha \leq \beta$ then $\alpha \in \Delta$.
(2) For $\alpha \in \Gamma, \beta \in \mathbb{N}_0^m$, if $\alpha \leq \beta$ then $\beta \in \Gamma$.

Obviously the set of exponents of all monomials which occur as leading monomials of an ideal I satisfies 2 of Lemma 1.1. Hence, the set of exponents of all monomials that do not occur as leading monomials of an ideal I is a delta set (these monomials are called *standard monomials* in [5]). We will denote *the delta set of the ideal I* as Δ_I. So, $\Delta_I = \mathbb{N}_0^m \backslash LE(I)$. Of course the delta set of an ideal depends on the specific monomial order chosen.

When we talk about the *dimension* of an ideal $I \subset R$ we mean the *Krull dimension* of the ring R/I. $I \subset \mathcal{F}[\mathbf{x}]$ is a 0-dimensional ideal if and only if $\mathcal{F}[\mathbf{x}]/I$ has finite dimension as a $\mathcal{F}$-vector space. The set of monomials which do not occur as leading monomials of elements in I map one to one to a basis of $\mathcal{F}[\mathbf{x}]/I$. Thus, one has that Δ_I corresponds to a basis of $\mathcal{F}[\mathbf{x}]/I$ as a $\mathcal{F}$ vector space and hence its size does not depend on the specific monomial order chosen. So, I is a 0-dimensional ideal if and only if Δ_I is a finite set.

Algorithms for computing Gröbner bases usually assume the knowledge of some basis for the ideal. We will describe an algorithm, due to Moss Sweedler and Lee Taylor [11,17], that computes a reduced Gröbner basis for a 0-dimensional ideal without necessarily knowing a basis for the ideal. This algorithm is based on linear algebra and generalizes a common technique relating to the irreducible polynomial of an element in a field extension, the minimal polynomial of a matrix and more. Namely, suppose that B is a finite degree field extension of $\mathcal{F}$, or B is the $\mathcal{F}$ algebra of $n \times n$ matrices over $\mathcal{F}$, or B is any finite dimensional algebra over $\mathcal{F}$. Suppose that $b \in B$ and consider $1 = b^0, b^1, b^2, \ldots$. Since B is finite dimensional, there is a first t where b^t is linearly dependent upon $1, b^1, b^2, \ldots, b^{t-1}$. Thus there is a linear relation:

$$0 = \lambda_0 + \lambda_1 b + \cdots + \lambda_{t-1} b^{t-1} + \lambda_t b^t,$$

with $\lambda_i \in \mathcal{F}$ and $\lambda_t \neq 0$. This gives the following degree t polynomial in $\mathcal{F}[x]$ which b satisfies:

$$\lambda_0 + \lambda_1 x + \cdots + \lambda_{t-1} x^{t-1} + \lambda_t x^t.$$

By the minimality of t, this is the lowest degree non-zero polynomial satisfied by b.

From a Gröbner basis viewpoint, here is what we have just done. Let $\Pi : \mathcal{F}[x] \to B$ be the map defined by: $f(x) \mapsto f(b)$, for $f(x) \in \mathcal{F}[x]$. This is an $\mathcal{F}$ algebra map and gives B an $\mathcal{F}[x]$-module structure. In the general procedure, we shall assume and use that Π is a module map. Under the *unique* monomial order on $\mathcal{F}[x]$, the ascending list of monomials is: $1, x, x^2, x^3, \ldots$. Consider

$$\Pi(1),\ \Pi(x),\ \Pi(x^2),\ \Pi(x^3),\ \ldots\ =\ 1, b, b^2, b^3, \ldots.$$

Since B is finite dimensional, there is a first t where $\Pi(x^t)$ is linearly dependent upon

$$\Pi(1),\ \Pi(x),\ \Pi(x^2),\ \Pi(x^3),\ \ldots,\ \Pi(x^{t-1}).$$

Thus, there is a linear relation

$$0 = \lambda_0\Pi(1) + \lambda_1\Pi(x) + \cdots + \lambda_{t-1}\Pi(x^{t-1}) + \lambda_t\Pi(x^t)$$

or, equivalently,

$$0 = \Pi\left(\lambda_0 + \lambda_1 x + \cdots + \lambda_{t-1}x^{t-1} + \lambda_t x^t\right),$$

with $\lambda_i \in \mathcal{F}$ and $\lambda_t \neq 0$. This gives the following degree t polynomial in $ker(\Pi)$:

$$\lambda_0 + \lambda_1 x + \cdots + \lambda_{t-1}x^{t-1} + \lambda_t x^t.$$

By the minimality of t, this polynomial is the lowest degree non-zero polynomial in $ker(\Pi)$. Hence it generates the principal ideal $ker(\Pi)$. In the multivariate case which follows, $ker(\Pi)$ is still an ideal, but it no longer is a principal ideal. One must iterate the preceding procedure. In order to actually do what we just described, we must be able to effectively determine linear dependence in B. This could be given by a "linear dependence oracle". The Sweedler-Taylor algorithm is not concerned with how linear dependence is determined. Let us now present the general algorithm.

Let B be an $\mathcal{F}[\mathbf{x}]$-module, and consider an $\mathcal{F}[\mathbf{x}]$-module map $\Pi : \mathcal{F}[\mathbf{x}] \longrightarrow B$, where $dim_{\mathcal{F}}\left(Im(\Pi)\right) = dim_{\mathcal{F}}\left(\mathcal{F}[\mathbf{x}]/ker(\Pi)\right)$ is finite and one can determine linear dependence among the elements of B. Under these conditions, one can compute a reduced Gröbner basis for $I = ker(\Pi)$ with respect to any monomial order using the following algorithm.

Suppose $<_T$ is a monomial order on $\mathcal{F}[\mathbf{x}]$. *Begin counting the monomials in* $\mathcal{F}[\mathbf{x}]$ with respect to $<_T$, forming: $1 = t_{1,0} <_T t_{1,1} <_T t_{1,2} <_T \cdots$. If $M \subset \mathcal{F}[\mathbf{x}]$, *begin counting the monomials in* M *with respect to* $<_T$ means

to form the sequence $(a <_T b <_T c <_T \cdots)$, where a is the smallest monomial in M with respect to $<_T$, b is the smallest monomial of $M\backslash\{a\}$ with respect to $<_T$, c is the smallest monomial of $M\backslash\{a,b\}$, etc. Since the set of monomials is well ordered with respect to a monomial order, there is always such a smallest monomial unless after a finite number of steps the set $M\backslash\{a,b,c,\ldots,e\}$ contains no more monomials. (This includes the possibility that M had no monomials in the first place, in which case the sequence is the empty sequence.) When M has but a finite number of monomials, they are eventually all selected for the sequence and no monomials remain to be selected. At this point the sequence simply stops.

Consider the subspaces $B_{1,i}$ of B, where $B_{1,i}$ is the $\mathcal{F}$ subspace spanned by $t_{1,0}, t_{1,1}, t_{1,2}, \ldots, t_{1,i}$. The spirit of the algorithm is better displayed if we define these sets recursively:

$$B_{1,-1} = \{0\} \subseteq B_{1,0} = \mathcal{F}\,\Pi(t_{1,0}) \subseteq B_{1,1} = B_{1,0} + \mathcal{F}\,\Pi(t_{1,1}) \subseteq$$

$$\cdots \subseteq B_{1,l} = B_{1,l-1} + \mathcal{F}\,\Pi(t_{1,l}) \subseteq \cdots \subseteq Im(\Pi).$$

Since $dim_{\mathcal{F}}(Im(\Pi)) < \infty$, it must happen that some $B_{1,i} = B_{1,i-1}$. This means that there will be a first linearly dependent element, call it $\Pi(t_{1,e_1})$, in $Im(\Pi)$. This is, $\Pi(t_{1,e_1}) \in B_{1,e_1-1}$. Thus,

$$\Pi(t_{1,e_1}) = \sum_{j=0}^{e_1-1} \lambda_{1,j}\Pi(t_{1,j}) \quad \text{or, equivalently,}$$

$$\Pi\left(t_{1,e_1} - \sum_{j=0}^{e_1-1} \lambda_{1,j} t_{1,j}\right) = 0. \tag{1.3}$$

Set $g_1 := t_{1,e_1} - \sum_{j=0}^{e_1-1} \lambda_{1,j} t_{1,j}$ and $G_1 := \{g_1\}$. Then, $G_1 \subset I = ker(\Pi)$ and $LM(g_1) = t_{1,e_1}$. Set $\Delta_{I,1} := \{LE(t_{1,j})\}_{j<e_1}$.

Now begin counting the set of monomials which are greater than t_{1,e_1} and not divisible by t_{1,e_1},
$t_{2,0} <_T t_{2,1} <_T t_{2,2} <_T \cdots$, and define

$$B_{2,-1} = B_{1,e_1-1} \subseteq B_{2,0} = B_{2,-1} + \mathcal{F}\,\Pi(t_{2,0}) \subseteq B_{2,1} = B_{2,0} + \mathcal{F}\,\Pi(t_{2,1}) \cdots .$$

So one has

$$B_{1,-1} \subseteq B_{1,0} \subset B_{1,1} \subset \cdots \subset B_{1,e_1-1} = B_{1,e_1}$$

$$= B_{2,-1} \subseteq B_{2,0} \subseteq B_{2,1} \subseteq \cdots \subseteq Im(B),$$

and again, find the first t_{2,e_2} such that $\Pi(t_{2,e_2}) \in B_{2,e_2-1}$.

$$g_2 := t_{2,e_2} - \sum_{j=0}^{e_2-1} \lambda_{2,j} t_{2,j} - \sum_{i=0}^{e_1-1} \lambda_{1,i} t_{1,i}, \quad \text{and} \quad \Pi(g_2) = 0.$$

Then, $g_2 \in I = ker(\Pi)$, $LM(g_2) = t_{2,e_2}$. Set $\Delta_{I,2} := \Delta_{I,1} \cup \{LE(t_{2,j})\}_{j<e_2}$, and $G_2 := G_1 \cup \{g_2\}$.

The general inductive step is the following. Suppose that $\Delta_{I,n-1}$ and G_{n-1} have been defined. Begin counting the set of monomials greater than $t_{n-1,e_{n-1}}$ and not divisible by

$$t_{1,e_1}, t_{2,e_2}, t_{3,e_3}, \ldots, t_{n-1,e_{n-1}},$$

the lead monomials of the elements in G_{n-1}. Suppose this counting yields:

$$t_{n,0} <_T t_{n,1} <_T t_{n,2} <_T \cdots.$$

Then define the subspaces $B_{n,i}$'s as:

$$B_{n,-1} = B_{n-1,e_{n-1}-1} \subseteq B_{n,0} = B_{n,-1} + \mathcal{F}\,\Pi(t_{n,0}) \subseteq B_{n,1}$$

$$= B_{n,0} + \mathcal{F}\,\Pi(t_{n,1}) \subseteq \cdots \subseteq Im(\Pi).$$

It can happen that there are only a finite number of monomials in the sequence

$$t_{n,0} <_T t_{n,1} <_T \cdots <_T t_{n,p}$$

and that all of them are linearly independent and one runs out of monomials. It can also happen that the sequence is empty, i.e. there are no monomials greater than $t_{n-1,e_{n-1}}$ and not divisible by a lead monomial in G_{n-1}. In these cases, set $\Delta_{I,n} := \Delta_{I,n-1} \cup \{LE(t_{n,j})\}_{i=0}^{p}$, and $G_n := G_{n-1}$. Note that in case the sequence was empty, $\Delta_{I,n} = \Delta_{I,n-1}$. The algorithm now terminates with $G_{n-1} = G_n$ a reduced Gröbner basis for $I = ker(\Pi)$ and $\Delta_{I,n}$ the set of lead exponents of the standard monomials. Set $G := G_n$ and $\Delta_I := \Delta_{I,n}$.

If the algorithm did not terminate, there will be a minimum e_n, where $B_{n,e_n-1} = B_{n,e_n}$, or equivalently,

$$\Pi(t_{n,e_n}) \in B_{n,e_n-1}$$

$$\Pi\left(t_{n,e_n}\right)=\sum_{j=0}^{e_n-1}\lambda_{n,j}\Pi\left(t_{n,j}\right)+\sum_{k=0}^{e_{n-1}-1}\lambda_{n-1,k}\Pi\left(t_{n-1,k}\right)+\cdots+\sum_{i=0}^{e_1-1}\lambda_{1,i}\Pi\left(t_{1,i}\right)$$

$$\Pi\left(t_{n,e_n}-\sum_{j=0}^{e_n-1}\lambda_{n,j}t_{n,j}-\sum_{k=0}^{e_{n-1}-1}\lambda_{n-1,k}t_{n-1,k}-\cdots-\sum_{i=0}^{e_1-1}\lambda_{1,i}t_{1,i}\right)=0.$$

In this case, set

$$g_n:=t_{n,e_n}-\sum_{j=0}^{e_n-1}\lambda_{n,j}t_{n,j}-\sum_{k=0}^{e_{n-1}-1}\lambda_{n-1,k}t_{n-1,k}-\cdots-\sum_{i=0}^{e_1-1}\lambda_{1,i}t_{1,i},$$

$$\Delta_{I,n}:=\Delta_{I,n-1}\cup\left\{LE(t_{n,j})\right\}_{j<e_n},\text{ and }G_n:=G_{n-1}\cup\left\{g_n\right\}.$$

In short, what the algorithm does is to find $\mathbf{x}^\alpha$'s, minimal in terms of divisibility, such that $\Pi\left(\mathbf{x}^\alpha\right)\in Span_{\mathcal{F}}\left\{\Pi\left(\mathbf{x}^\beta\right)\right\}_{\beta<_T\alpha}$, where $Span_{\mathcal{F}}\left(V\right)$ is the $\mathcal{F}$ vector space spanned by the elements in V. The exponents β are exponents of independent monomials, and the Δ_I set is the set of exponents of all the independent monomials.

The above algorithm was presented in [17]. The algorithm together with a complete proof of its validity are included in [11]. The algorithm is summarized as follows:

Algorithm 1.1 (The Sweedler-Taylor Algorithm).

Input: 1) A $\mathcal{F}[\mathbf{x}]$-module B.
2) A $\mathcal{F}[\mathbf{x}]$-module map $\Pi:\mathcal{F}[\mathbf{x}]\longrightarrow B$,
where $dim_{\mathcal{F}}\left(Im(\Pi)\right)<\infty$,
and we can compute linear dependence in B.
3) A monomial order $<_T$ on $\mathcal{F}[\mathbf{x}]$.

Output: 1) A reduced Gröbner basis for $I=ker(\Pi)$ with respect to $<_T$.
2) Δ_I.

1) BEGIN
2) Let A be the set of all monomials in $\mathcal{F}[\mathbf{x}]$, $l:=1$, $G_0=\emptyset$, $\Delta_{I,0}=\emptyset$
3) Order all monomials in A with respect to $<_T$: $t_{l,0}<_T t_{l,1}<_T\cdots$

4) REPEAT
5) $i := -1$
6) REPEAT
7) $i := i + 1$
8) $A := A - \{t_{l,i}\}$
9) UNTIL $\Pi(t_{l,e_l}) = \sum_{h=1}^{l} \sum_{j=0}^{e_h-1} \lambda_{h,j} \Pi(t_{h,j})$ or $A = \emptyset$
10) IF $\Pi(t_{l,e_l}) = \sum_{h=1}^{l} \sum_{j=0}^{e_h-1} \lambda_{h,j} \Pi(t_{h,j})$, THEN
11) $g_l := t_{l,e_l} - \sum_{h=1}^{l} \sum_{j=0}^{e_h-1} \lambda_{h,j} t_{h,j}$
12) $G_l := G_{l-1} \cup \{g_l\}$
13) $\Delta_{I,l} := \Delta_{I,l-1} \cup \{LE(t_{l,j})\}_{j<e_l}$
14) Order the monomials in
$A := A - \{t_{l,e_l} M \mid M \text{ a monomial in } \mathcal{F}[\mathbf{x}]\}$
with respect to $<_T$
15) $l := l + 1$
16) ELSE
17) $\Delta_{I,l} := \Delta_{I,l-1} \cup \{leadexp(t_{l,j})\}_{j \leq i}$
18) UNTIL $A = \emptyset$
19) $G := G_{l-1}$, $\Delta_I := \Delta_{I,l-1}$
20) END

Theorem 1.2. *The above algorithm computes a reduced Gröbner basis* $G = \{g_1, \cdots, g_l\}$ *for* $ker(\Pi)$ *with respect to* $<_T$ *and* Δ_I *is the delta set of* $I = ker(\Pi)$.

1.4 Linear recurrence relations on m-dimensional arrays

Sakata [14] studied the relation between periodic arrays, linear recurrence relations and ideals. He proved that if an array S is m-dimensional periodic, then the ideal of linear recurrence relations valid on S is 0-dimensional, a fact that also follows from the paper of Gianni [8]. This will allow us to use the analog to the Sweedler-Taylor algorithm in Section 1.5 to find a Gröbner basis that generates the ideal of linear recurrences. In this section we present the basics from linear recurrence relations on m-dimensional arrays, and reformulate the problem in terms of Laurent series where the desired Gröbner basis will be the kernel of a module map.

Let $S \subset \mathcal{F}^{\mathbb{N}_0^m}$ be an m-dimensional infinite array. The arrays considered in this paper are m-dimensional periodic and this is key in order to

effectively compute linear dependency in the algorithm that we will present.

Definition 1.2. An m-dimensional array S is said to be **m-dimensional periodic** if there is a m-tuple, that we call the **period vector**, $n = (n_1, \ldots, n_m) \in \mathbb{N}^m$, such that

$$S_{(\alpha_1,\ldots,\alpha_m)} = S_{(\alpha_1+n_1k_1,\ldots,\alpha_m+n_mk_m)}$$

for $k_i \in \mathbb{N}_0$ and all $(\alpha_1, \ldots, \alpha_m) \in \mathbb{N}_0^m$.

Let $C(\mathbf{x}) = \sum_{\alpha \in Supp(C)} C_\alpha \mathbf{x}^\alpha \in \mathcal{F}[\mathbf{x}]$, where $Supp(C) := \{\alpha \mid C_\alpha \text{ is a non-zero coefficient of } C\}$.

Definition 1.3. The polynomial $C(\mathbf{x})$ defines a linear recurrence relation at a point S_u of the array S if $LE(C) \leq u$ and

$$\sum_{\alpha \in Supp(C)} C_\alpha S_{\alpha+u-LE(C)} = 0. \tag{1.4}$$

In this case we say that C **is valid at the point** S_u. Also set C to be valid at S_u, if $LE(C) \not\leq u$.

Definition 1.4. A polynomial C **is valid for the array** S if the equation

$$\sum_{\alpha \in Supp(C)} C_\alpha S_{\alpha+\beta} = 0 \tag{1.5}$$

holds for all $\beta \in \mathbb{N}_0^m$. In this case we also say that S **satisfies the m-dimensional linear recurrence relation given by** C.

Note that C is a valid polynomial for S if and only if C is a valid polynomial at every point S_u such that $LE(C) \leq u$.

Let $Val(S)$ denote the set of all valid polynomials for the array S. The set $Val(S)$ is an ideal in $\mathcal{F}[\mathbf{x}]$ and our goal is to find a Gröbner basis for $Val(S)$. If S is an m-dimensional periodic array with period vector $n = (n_1, \ldots, n_m)$ then it is clear that $Val(S)$ contains the polynomials $x_1^{n_1} - 1, x_2^{n_2} - 1, \ldots, x_m^{n_m} - 1$. So, in this case, $Val(S)$ is a 0-dimensional ideal as it was proved in [8]. From now on, we only consider periodic arrays.

We now reformulate the definition of a valid polynomial in order to have $Val(S) = ker(\Pi)$, the kernel of a map $\Pi : \mathcal{F}[\mathbf{x}] \longrightarrow B$. By choosing Π as a $\mathcal{F}[\mathbf{x}]$-module map, we can then use the analog to the Sweedler-Taylor algorithm to find a Gröbner basis for the ideal of valid polynomials $Val(S)$. The approach that we use is a generalization of Example 1.1 to the multivariate case.

1.4.1 *Reformulation of the problem*

Let us look at Example 1.1 again. The algebraic way to view the power series operations in (1.2) is as follows: view the power series as sitting within the ring of Laurent series $\mathcal{F}\{\{x\}\}$ and multiply by x^{-1}. This is not quite correct because $x^{-1}\left(3+5x+9x^2+6x^3+\cdots\right) = 3x^{-1}+5+9x+6x^2+\cdots$, and there is an "unwanted" $3x^{-1}$ term. Hence, factor out the subspace L^- of Laurent series spanned by $x^{-1}, x^{-2}, x^{-3}, \cdots$. Since $x^{-1}L^- \subseteq L^-$, multiplying by x^{-1} gives an operator on $\mathcal{F}\{\{x\}\}/L^-$. Now, $\mathcal{F}\{\{x\}\}/L^-$ has a complete basis $1, \overline{x}, \overline{x}^2, \ldots$, and the image of $S(x)$ in $\mathcal{F}\{\{x\}\}/L^-$ is:

$$3+5\overline{x}+9\overline{x}^2+6\overline{x}^3+\cdots, \text{ and}$$

$$x^{-1}\left(3+5\overline{x}+9\overline{x}^2+6\overline{x}^3+\cdots\right) \;=\; 5+9\overline{x}+6\overline{x}^2+\cdots,$$

since $3x^{-1} \equiv 0 \; mod \; L^-$. This algebraic treatment immediately generalizes to the multivariate case.

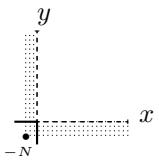
Denote the ring of Laurent series in several variables and coefficients in $\mathcal{F}$ by $\mathcal{F}\{\{\mathbf{x}\}\} = \mathcal{F}\{\{x_1, \ldots, x_m\}\}$. There are several definitions for Laurent series if $m > 1$ [10], the one considered here is not a field and can be defined as $\mathcal{F}\{\{\mathbf{x}\}\} =$

$$\left\{ \sum_{\alpha_1=-k_1}^{\infty} \sum_{\alpha_2=-k_2}^{\infty} \cdots \sum_{\alpha_m=-k_m}^{\infty} a_\alpha \mathbf{x}^\alpha \; | \alpha = (\alpha_1, \alpha_2, \ldots, \alpha_m) \;\; a_\alpha \in \mathcal{F}, k_i \in \mathbb{N} \right\}.$$

Here every $f(\mathbf{x}) \in \mathcal{F}\{\{\mathbf{x}\}\}$ has the property that there is a monomial $\mathbf{x}^\alpha \in \mathcal{F}[\mathbf{x}]$ where $\mathbf{x}^\alpha f(\mathbf{x}) \in \mathcal{F}[[\mathbf{x}]]$. An alternative way of defining $\mathcal{F}\{\{\mathbf{x}\}\}$ is as $\mathcal{F}[[\mathbf{x}]]$ localized at the multiplicative system consisting of the monomials of $\mathcal{F}[x]$. This gives the ring structure on $\mathcal{F}\{\{\mathbf{x}\}\}$.

One can associate the array S to a multivariate power series $S(\mathbf{x})$ by assigning the coefficient S_α to the monomial $\mathbf{x}^\alpha$. S is also a Laurent series with the coefficients of the terms with negative exponents equal to 0. For a polynomial $C(\mathbf{x})$ let $C(\mathbf{x}^{-1})$ denote $C\left(x_1^{-1}, x_2^{-1}, \ldots, x_m^{-1}\right)$. Since C is a polynomial, $C(\mathbf{x}^{-1})$ is a Laurent series in $\mathcal{F}\{\{\mathbf{x}\}\}$, and one can multiply S and $C(\mathbf{x}^{-1})$ as Laurent series. In this setting, we say that a polynomial C is **valid at a point** S_u if $u - LE(C) \not\geq 0$ or if $u - LE(C) \geq 0$, then in the product $C(\mathbf{x}^{-1})S(\mathbf{x})$ the term with exponent $u - LE(C)$ has coefficient 0. Similarly, the equation that defines a valid polynomial (1.5) can be "translated" to multiplication of Laurent series as follows: $\sum_{\alpha \in Supp(C)} C_\alpha S_{\alpha+\beta} = 0$ for all $\beta \in \mathbb{N}_0^m$ is equivalent to say that all the (non-zero) terms of the product $C(\mathbf{x}^{-1})S(\mathbf{x})$ have negative exponents, where we say that $ax_1^{e_1}\cdots x_m^{e_m}$ has negative exponents if at least one of the e_i's is negative. For example, $x_1^{5234}x_2^{-1}x_3^{749}$ has negative exponents!

Consider the 2-dimensional case and look at the product $C(\mathbf{x}^{-1})S(\mathbf{x})$ in the plane. The m-dimensional case is a straightforward generalization of this case. One has that C is a valid polynomial for the array S if the coefficients of the terms of $C(\mathbf{x}^{-1})S(\mathbf{x})$ outside the shaded area are zero:

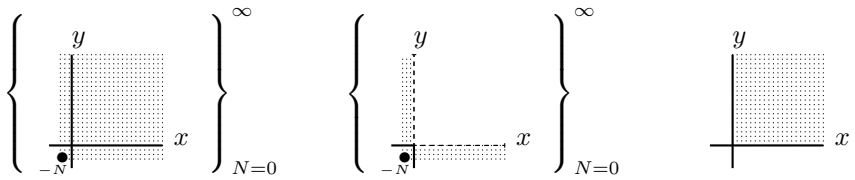


Note that a term ax^iy^j lies in the shaded area if and only if $i < 0$ or $j < 0$. In the figure, N is the exponent of the least common multiple of all the monomials in $C(\mathbf{x})$.

To define $Val(S)$ as the kernel of a map one needs to be able to multiply by polynomials in x^{-1} and y^{-1}. Let $L := \mathcal{F}\{\{x, y\}\}$, and let L^- be the subspace of Laurent series all of whose non-zero terms have negative exponents.

Since L and L^- are $\mathcal{F}[x^{-1}, y^{-1}]$-modules, $L^- \subset L$, one can form the $\mathcal{F}[x^{-1}, y^{-1}]$-module $B := L/L^-$.

In pictures,



L L^- $B = L/L^-$

Note that the natural representation of B is by power series in x and y; i.e. B is isomorphic to $\mathcal{F}[[x, y]]$ as a vector space. The m-dimensional case is similar. From now on consider B to be represented in terms of $\mathcal{F}[[x_1, \ldots, x_m]]$ as a vector space.

Within $\mathcal{F}\{\{x_1, \ldots, x_m\}\}$, the elements $x_1^{-1}, \ldots, x_m^{-1}$ are algebraically independent over $\mathcal{F}$. Let $\mathcal{F}[\mathbf{x}^{-1}] = \mathcal{F}[x_1^{-1}, \ldots, x_m^{-1}]$ denote the subalgebra of $\mathcal{F}\{\{x_1, \ldots, x_m\}\}$ generated by $x_1^{-1}, \ldots, x_m^{-1}$. By the algebraic independence of $x_1^{-1}, \ldots, x_m^{-1}, \mathcal{F}[\mathbf{x}^{-1}]$ is (isomorphic to) the polynomial ring in $x_1^{-1}, \ldots, x_m^{-1}$. Since $\mathcal{F}[\mathbf{x}^{-1}]L^- \subset L^-$, there is a natural multiplicative action of $\mathcal{F}[\mathbf{x}^{-1}]$ on $\mathcal{F}\{\{\mathbf{x}\}\}/L^- = B$. In (1.6), $x_1^{-1} = x^{-1}$ is the "shift left" operator and $x_2^{-1} = y^{-1}$ is the "shift down" operator.

In terms of the representation of B as power series in $x_1, \ldots, x_m$, for $p(\mathbf{x}) \in \mathcal{F}[[\mathbf{x}]]$:

$$\mathbf{x}^{-\alpha} p(\mathbf{x}) = \mathbf{x}^{-\alpha} p(\mathbf{x}) \ + \ L^-,$$

i.e. $\mathbf{x}^{-\alpha} p(\mathbf{x})$ is the coset of $\mathbf{x}^{-\alpha} p(\mathbf{x})$ in L/L^-.

The $\mathcal{F}\left[\mathbf{x}^{-1}\right]$-module action on B is also informally described as: when a polynomial $g(\mathbf{x}^{-1})$ in $\mathbf{x}^{-1}$ acts upon a power series $p(\mathbf{x})$ in $\mathbf{x}$, simply multiply $g(\mathbf{x}^{-1})$ by $p(\mathbf{x})$ as Laurent series and consider all resulting terms with exponents with negative entries to be zero.

Now, consider the coset of the periodic array S, $\overline{S(\mathbf{x})} \in B = L/L^-$. Then $\overline{\mathcal{F}[\mathbf{x}^{-1}]S(\mathbf{x})}$ is the cyclic submodule of L/L^- generated by $\overline{S(\mathbf{x})}$. Note that using our reformulation of the problem, a polynomial C is valid on the array S if and only if $\overline{C(\mathbf{x}^{-1})S(\mathbf{x})} = 0$. That is, all terms with exponents with non-negative coordinates are zero. So, if one defines the map

$$\Pi_S : \mathcal{F}[\mathbf{x}^{-1}] \longrightarrow \overline{\mathcal{F}[\mathbf{x}^{-1}]S(\mathbf{x})} \subseteq B = L/L^-,$$

$$C(\mathbf{x}^{-1}) \longmapsto C(\mathbf{x}^{-1})S(\mathbf{x}) \ + \ L^-,$$

one says that C is valid for the array S if and only if $C(\mathbf{x}^{-1}) \in ker(\Pi_S)$. That is, the set of valid polynomials is the kernel of the map, $Val(S) = ker(\Pi_S)$ (if we identify $C(\mathbf{x})$ with $C(\mathbf{x}^{-1})$).

Now that the 0-dimensional ideal $Val(S)$ is expressed as the kernel of the module map Π_S one may use the Sweedler-Taylor algorithm for computing a Gröbner basis for $ker(\Pi_S)$ and have a Gröbner basis for $Val(S)$. However, $\overline{\mathcal{F}[\mathbf{x}^{-1}]S(\mathbf{x})} \subseteq B$, B is not a finite dimensional $\mathcal{F}$-vector space and one cannot directly compute linear dependence as needed in the Sweedler-Taylor algorithm. But one can use the fact that S is periodic to see that it is enough to just consider a finite subarray of S to obtain $Val(S)$.

Although B is infinite dimensional, there are aspects of local finiteness about it. If $S(\mathbf{x})$ were a polynomial, then $\overline{\mathcal{F}[\mathbf{x}^{-1}]S(\mathbf{x})}$ is finite dimensional. There are also many power series $S(x)$ that are not polynomials but $\overline{\mathcal{F}[\mathbf{x}^{-1}]S(\mathbf{x})}$ is finite dimensional; these are precisely the periodic power series considered in this paper.

The analog to the Sweedler-Taylor algorithm was designed to deal with the situation of B being infinite dimensional. The linear dependency will be computed "modulo" multiples of certain monomials. With this we will be able to compute minimal polynomials that are valid "up to" a certain point in the array, this is, valid in a subarray. Because of the periodicity,

polynomials valid on certain subarray will be valid for the complete array S.

In the next section we will introduce the concept of *being valid up to a point* S_u. Then we define a set B_u such that B/B_u is finite dimensional. Using the B_u's we modify the Sweedler-Taylor algorithm to compute what we call lead monomial generating sets. The modified algorithm will produce a reduced Gröbner basis for $Val(S)$.

1.5 Lead monomial generating sets for the set of recurrence relations valid on subarrays

Let $C\left(\mathbf{x}^{-1}\right) \in \mathcal{F}[\mathbf{x}^{-1}]$. Since $\mathcal{F}[\mathbf{x}^{-1}]$ is a polynomial ring in $x_1^{-1}, \ldots, x_m^{-1}$, one may apply all the theory of Gröbner bases to it. For a monomial order $<_T$ in $\mathcal{F}[\mathbf{x}]$, the monomial order in $\mathcal{F}[\mathbf{x}^{-1}]$ is given by $\mathbf{x}^{-\alpha} <_T \mathbf{x}^{-\beta}$ if and only if $\mathbf{x}^{\alpha} <_T \mathbf{x}^{\beta}$. Then, for $C\left(\mathbf{x}^{-1}\right) = \sum_{\alpha \in Supp(C)} C_\alpha \mathbf{x}^{-\alpha}$, we set $LE(\left(C\left(\mathbf{x}^{-1}\right)\right) = LE\left(C(\mathbf{x})\right)$.

Let $u \in \mathbb{N}_0^m$ be such that $LE(C) \leq u$. Then, $\beta = u - LE(C) \geq 0$. From (1.4) one has that C is valid at S_u if $\sum_{\alpha \in Supp(C)} C_\alpha S_{\beta+\alpha} = 0$. Using the new notation, this is the same as saying that in $\overline{C(\mathbf{x}^{-1})S(\mathbf{x})}$ the term with exponent β has coefficient zero.

Note that if $LE(C) \not\leq u$ then the m-tuple $\beta = u - LE(C)$ has at least one negative entry and when one mods out by L^- the term with exponent β will assuredly be zero. So, for checking the validity of C at a particular entry S_u, one does not have to check whether $LE(C) \leq u$ or not.

We formalize this as:

Definition 1.5. The m-dimensional linear recurrence relation given by the polynomial C **is valid at the point** S_u if in $\overline{C(\mathbf{x}^{-1})S(\mathbf{x})}$ the term with exponent $\beta = u - LE(C)$ has coefficient zero. We say that **C is valid up to** S_u if C is valid at each S_l with $l \leq_T u$.

For now, let's choose $<_T$ to be a monomial order such that for any monomial M there are only a finite number of monomials $<_T M$. For example, let $<_T$ be the graded lexicographic order (but not pure lex). Now define

Definition 1.6.

$$B_u := \left\{ \sum_{\alpha >_T u} \lambda_\alpha \mathbf{x}^\alpha \right\} \subset B.$$

We have that B/B_u is a finite dimensional vector space. One can then define $Val_u(S)$, the set of polynomials that are "valid up to S_u", using the set B_u:

$$Val_u(S) := \Big\{ 0 \neq C(\mathbf{x}) \mid \text{ in } \overline{C(\mathbf{x}^{-1})S(\mathbf{x})}, \text{ for every } \beta \text{ with} \tag{1.6}$$

$$\beta + LE(C) \leq_T u, \text{ the term with exponent } \beta \text{ has coefficient zero } \} \cup \{0\}$$

$$= \Big\{ 0 \neq C(\mathbf{x}) \mid \text{ in } \overline{C(\mathbf{x}^{-1})S(\mathbf{x})} \text{ the only non-zero terms}$$

$$\text{are those with exponents } \beta \text{ where } \beta + LE(C) >_T u\} \cup \{0\}.$$

It follows that

$$Val_u(S) = \Big\{ 0 \neq C(\mathbf{x}) \mid \Pi_S\left(C(\mathbf{x}^{-1})\right) \in \mathbf{x}^{-LE(C)} B_u \Big\} \cup \{0\}.$$

So, $Val_u(S)$ is composed by polynomials C that give linear dependency relations modulo $\mathbf{x}^{-LE(C)}B_u$. $Val_u(S)$ is not necessarily an ideal but it is easy to prove that the set $LM\left(Val_u(S)\right)$ is closed under monomial multiplication, as follows.

Lemma 1.2. *$LM\left(Val_u(S)\right)$ is a monomial ideal.*

Proof. Say $0 \neq C\left(\mathbf{x}^{-1}\right) \in Val_u(S)$. Since $LM\left(\mathbf{x}^{-\alpha}C\left(\mathbf{x}^{-1}\right)\right) = \mathbf{x}^{-\alpha}LM\left(C\left(\mathbf{x}^{-1}\right)\right)$, it suffices to show that $\mathbf{x}^{-\alpha}C\left(\mathbf{x}^{-1}\right) \in Val_u(S)$.

$$\Pi_S\left(\mathbf{x}^{-\alpha}C\left(\mathbf{x}^{-1}\right)\right) = \overline{\mathbf{x}^{-\alpha}C\left(\mathbf{x}^{-1}\right)S(\mathbf{x})}.$$

Since $\Pi_S\left(C\left(\mathbf{x}^{-1}\right)\right) \in \mathbf{x}^{-LE(C)}B_u$, we see that

$$\Pi_S\left(\mathbf{x}^{-\alpha}C\left(\mathbf{x}^{-1}\right)\right) \in \mathbf{x}^{-\alpha}\mathbf{x}^{-LE(C)}B_u = \mathbf{x}^{-LE\left(\mathbf{x}^{-\alpha}C\left(\mathbf{x}^{-1}\right)\right)}B_u,$$

where the equality follows from the fact that $LE\left(\mathbf{x}^{-\alpha}C\left(\mathbf{x}^{-1}\right)\right) = \alpha + LE\left(C\left(\mathbf{x}^{-1}\right)\right)$. □

Since $LM\left(Val_u(S)\right)$ is a monomial ideal, $\Gamma := LE\left(Val_u(S)\right)$ satisfies part 2 of Lemma 1.1. Therefore, its complement $\mathbb{N}_0^m \backslash \Gamma$ is a delta set, denoted by Δ_u.

Let u^+ be the m-tuple that immediately follows u with respect to $<_T$. Note that $B_{u^+} \subseteq B_u$ implies $Val_{u^+}(S) \subseteq Val_u(S)$. Therefore

$LM\left(Val_{u^+}(S)\right) \subseteq LM\left(Val_u(S)\right)$ and $\Delta_u \subseteq \Delta_{u^+}$. In particular $Val(S) \subseteq Val_u(S)$ and $\Delta_u \subseteq \Delta_{Val(S)}$ for all $u \in \mathbb{N}_0^m$.

Definition 1.7. Let $G = \{g_1, \ldots, g_l\} \subset \mathcal{F}[\mathbf{x}]$. The set G is called a **lead monomial generating set for the set** $A \subset \mathcal{F}[\mathbf{x}]$ with respect to $<_T$ if $\langle LM\left(G\right)\rangle = \langle LM(A)\rangle$. G is called a **reduced lead monomial generating set for** A if $LC(g_i) = 1, i = 1, \ldots, l$ and $LM(g_i)$ does not divide any term of g_j for every $j \neq i$.

Note that this concept is very similar to a reduced Gröbner basis for an ideal. In fact, if A is an ideal and $G \subseteq A$ then a lead monomial generating set for A is a Gröbner basis for A.

1.5.1 *Analog to the Sweedler-Taylor algorithm*

Building on the Sweedler-Taylor algorithm gives an algorithm to compute a reduced lead monomial generating set G_u for $Val_u(S)$. The set G_u is referred in other papers [14,16] as a "minimal polynomial set" for $Val_u(S)$.

Unlike the Sweedler-Taylor algorithm which looks for linear dependency relations, one looks for "partial linear dependency" relations, where partial means modulo $\mathbf{x}^{-LE(C)}B_u$. In this setting, all the equations that give linear dependency relations, like equation (1.3), become:

$$\Pi_S\left(\left(t_{1,e_1}\right)^{-1}\right) \in B_{1,e_1-1} + \left(t_{1,e_1}\right)^{-1} B_u$$

$$\Pi_S\left(\left(t_{1,e_1}\right)^{-1}\right) = \sum_{j=0}^{e_1-1} \lambda_j \Pi_S\left(\left(t_{1,j}\right)^{-1}\right) + \left(t_{1,e_1}\right)^{-1} B_u \tag{1.7}$$

$$\Pi_S\left(\left(t_{1,e_1}\right)^{-1} - \sum_{j=0}^{e_1-1} \lambda_j \left(t_{1,j}\right)^{-1}\right) \in \left(t_{1,e_1}\right)^{-1} B_u.$$

The lead monomial generating set for $Val_u(S)$ is $G_u = \{g_1, \ldots, g_n\}$, where $g_i := t_{i,e_i} - \sum_{j=0}^{e_i-1} \lambda_{i,j} t_{i,j} - \sum_{j=0}^{e_{i-1}-1} \lambda_{i-1,j} t_{i-1,j} - \cdots - \sum_{j=0}^{e_1-1} \lambda_{1,j} t_{1,j}$.

Hence, by changing Π to Π_S and lines 9) and 10) of Algorithm 1.1 to

9) UNTIL $\Pi_S\left(\left(t_{l,e_l}\right)^{-1}\right) = \sum_{h=1}^{l} \sum_{j=0}^{e_h-1} \lambda_{h,j} \Pi_S\left(\left((t_{h,j}\right)^{-1}\right) + \left(t_{l,e_l}\right)^{-1} B_u$ or $A = \emptyset$

10) IF $\Pi_S\left(\left(t_{l,e_l}\right)^{-1}\right) = \sum_{h=1}^{l} \sum_{j=0}^{e_h-1} \lambda_{h,j} \Pi_S\left(\left(t_{h,j}\right)^{-1}\right) + \left(t_{l,e_l}\right)^{-1} B_u$,
THEN,

we obtain an analog to the Sweedler-Taylor algorithm to compute lead monomial generating sets for $Val_u(S)$. A description of the analog to the Sweedler-Taylor algorithm in a more general setting can be found in [11].

1.5.2 *Finding u such that* $Val_u(S) = Val(S)$

The periodicity of the array S makes the ideal quotient $\mathcal{F}[\mathbf{x}]/Val(S)$ into a finite dimensional vector space, and, at some point S_u, $Val_u(S) = Val(S)$ and the partial dependencies (1.7) are in fact (complete) linear dependencies. This implies that there exists u such that one can use the analog to the Sweedler-Taylor algorithm described above to compute a reduced lead monomial generating set for $Val_u(S)$ and obtain a Gröbner basis for $Val(S)$. We now give a bound for u that guarantees that $Val_u(S) = Val(S)$.

Suppose that the array S has period $n = (n_1, \ldots, n_m)$. Then, $x_1^{n_1} - 1, \ldots, x_m^{n_m} - 1 \in Val(S)$, and, by Lemma 1.1, the following result is clear:

Lemma 1.3. *Let S be an array with period $n = (n_1, \ldots, n_m)$, $Val(S)$ be the ideal of polynomials valid in S and $\Delta_{Val(S)}$ be the delta set of $Val(S)$. Also let $C \in Val(S)$ with $LE(C) = (l_1, \ldots, l_m)$. Then*

(1) $\Delta_{Val(S)} \subseteq \{(\delta_1, \ldots, \delta_m) \in \mathbb{N}_0^m \mid (\delta_1, \ldots, \delta_m) \leq (n_1 - 1, \ldots, n_m - 1)\}$,
(2) $|\Delta_{Val(S)}| \leq n_1 \cdots n_m$.
(3) If C is minimal in $Val(S)$ with respect to divisibility of $LM(C)$, then $l_i \leq n_i$ for $i = 1, \ldots, m$.

We now prove that if we have a minimal polynomial valid at all entries in a certain region of the array S then C is also valid outside that region and hence in the complete array.

Prop 1.1. Let S be an array with period $n = (n_1, \ldots, n_m)$. Suppose that C is valid at S_u for all $u \leq (2n_1 - 1, \ldots, 2n_m - 1)$ and it is minimal with this property with respect to divisibility of $LM(C)$. If $v \not\leq (2n_1 - 1, \ldots, 2n_m - 1)$, then C is valid at S_v, and hence $C \in Val(S)$.

Proof. If $v - LE(C) \not\geq 0$, then C is valid at S_v and there is nothing to prove. Suppose that $v - LE(C) \geq 0$. Then $v = LE(C) + \beta$, for some $\beta = (\beta_1, \ldots, \beta_m) \in \mathbb{N}_0^m$. We can rewrite $\beta_i = k_i n_i + r_i$, where $k_i, r_i \in \mathbb{N}_0$, $r_i < n_i$ and have

$$v = LE(C) + (r_1, \ldots, r_m) + (n_1 k_1, \ldots, n_m k_m)\,.$$

Since C is $\leq$ minimal, $LE(C) \leq (n_1, \ldots, n_m)$, and since also $r_i < n_i$, we have that

$$\gamma = LE(C) + (r_1, \ldots, r_m) \leq (2n_1 - 1, \ldots, 2n_m - 1)\,,$$

and, by hypothesis, C is valid for S_γ. Therefore, by the periodicity of S,

$$0 = \sum_{\alpha \in Supp(C)} C_\alpha S_{\alpha+\gamma-LE(C)} = \sum_{\alpha \in Supp(C)} C_\alpha S_{\alpha+\gamma+(n_1k_1,\ldots,n_mk_m)-LE(C)}$$

$$= \sum_{\alpha \in Supp(C)} C_\alpha S_{\alpha+v-LE(C)},$$

and C is valid at S_v.

□

Any point S_u with $u \leq (2n_1 - 1, \ldots, 2n_m - 1)$ satisfies $|u| \leq 2|n| - m$. So if $S' = \{S_u \mid |u| \leq 2|n| - m\}$, then S' contains all S_u with $u \leq (2n_1 - 1, \ldots, 2n_m - 1)$. This selection for S' is convenient for computing a Gröbner basis with respect to the *grlex* order; other choices can be used for other monomial orders.

Corollary 1.1. *Let S be an array with period $n = (n_1, \ldots, n_m)$ and $S' \subset S$ be such that $S' = \{S_u\}_{|u| \leq 2|n|-m}$. If C is valid at every point $S_u \in S'$ and it is minimal with this property with respect to divisibility of $LM(C)$, then C is valid for the infinite array S. This is, $C \in Val(S)$.*

If we select a monomial order $<_T$ and order the elements of S such that all the elements in the subarray $S' = \{S_u\}_{|u| \leq 2|n|-m}$ are among the first elements of the ordered array S, then the minimal polynomials valid for S' are the minimal polynomials valid for S. If u^+ is the smallest with respect to $<_T$ such that $u^+ \geq_T u$ for all u with $|u| \leq 2|n| - m$, then a reduced lead monomial generating set for $Val_{u^+}(S)$ is a reduced Gröbner basis for $Val(S)$. In particular, if we consider the *graded lexicographical* order we get the next proposition.

Prop 1.2. Let S be an array with period $n = (n_1, \ldots, n_m)$ and $S' \subset S$ be such that $S' = \{S_u\}_{|u| \leq 2|n|-m}$. If u^+ is the largest element in $\mathbb{N}_0^m$ with respect to $<_{grlex}$ such that $S_{u^+} \in S'$, then, the set of all minimal polynomials in $Val_{u^+}(S)$ forms a Gröbner basis for $Val(S)$ with respect to $<_{grlex}$. This is, $Val_{u^+}(S) = Val(S)$.

We now illustrate how to use the analog to the Sweedler-Taylor algorithm discussed in Section 1.5.1 to compute a Gröbner basis for $Val(S)$ with respect to $<_{grlex}$, where S is a 2-dimensional array with period $n = (n_1, n_2)$. By Proposition 1.2, it is enough to use the points S_u with $u_1 + u_2 \leq 2(n_1 + n_2) - 2$. Following the idea of Example 1.1, to find

the partial linear dependency relations we form a matrix where each row corresponds to $\mathbf{x}^{-\alpha}S(x)$, and there is a column for each monomial from 1 to $x^{2(n_1+n_2)-2}$. The matrix will have a form similar to the matrix below, where we used the *grlex* order with $y < x$.

$$\begin{array}{c} \\ \Pi_S(1) \\ \Pi_S(y^{-1}) \\ \Pi_S(x^{-1}) \\ \vdots \end{array} \begin{array}{c} \begin{array}{ccccccc} 1 & y & x & y^2 & xy & \cdots & x^{2(n_1+n_2)-2} \end{array} \\ \begin{pmatrix} S'(x,y) & & & & & & \\ \overline{y^{-1}S'(x,y)} & & & & & & \\ \overline{x^{-1}S'(x,y)} & & & & & & \\ \vdots & & & & & & \end{pmatrix} \end{array}$$

When a new row is adjoined to the matrix, it is reduced with the previous rows. We need to find relations that are valid up to $S_{(2(n_1+n_2)-2,0)}$. If the new row corresponds to the map $\Pi_S(\mathbf{x}^\alpha) = \Pi_S(x^{-\alpha_1}y^{-\alpha_2})$, we look for linear dependencies modulo $x^{-\alpha_1}y^{-\alpha_2}B_{(2(n_1+n_2)-2,0)}$, where $B_{(2(n_1+n_2)-2,0)} = \left\{\sum_{\gamma >_{grlex}(2(n_1+n_2)-2,0)} \lambda_\gamma \mathbf{x}^\gamma\right\}$. This is, the row $\Pi_S\left(x^{-\alpha_1}y^{-\alpha_2}\right)$ needs to be partial linearly dependent, which means that it should have 0 in every column x^iy^j, where $(\alpha_1+i, \alpha_2+j) \leq_T (2(n_1+n_2)-2, 0)$. Recall that we ignore any term that has negative exponents.

Example 1.2. Let S be the following 2-dimensional array with entries in $\mathbb{F}_{11}$ and period vector $n = (2, 2)$:

$$S = \begin{pmatrix} \vdots & \vdots & \vdots & \vdots & \\ 10 & 8 & 10 & 8 & \cdots \\ 3 & 1 & 3 & 1 & \cdots \\ 10 & 8 & 10 & 8 & \cdots \\ 3 & 1 & 3 & 1 & \cdots \end{pmatrix}$$

To find a Gröbner basis for $Val(S)$ with respect to $<_{grlex}$ we use the analog to the Sweedler-Taylor algorithm to compute a lead monomial generating set for $Val_u(S)$, where $u = (6, 0)$. We order the monomials from 1

to x^6 with respect to $<_{grlex}$ and construct a matrix for reduction, where we include additional columns to keep track of the row operations and be able to obtain the coefficients of the Gröbner basis elements.

	1	y	x	y^2	yx	$\cdots$	x^5	y^6	$\cdots$	x^6	1	y
$\Pi_S(1)$	3	10	1	3	8	$\cdots$	1	3	$\cdots$	3	1	0
$\Pi_S(y^{-1})$	10	3	8	10	1	$\cdots$	8				0	1

	1	y	x	y^2	yx	$\cdots$	x^5	y^6	$\cdots$	x^6	1	y
$\Pi_S(1)$	3	10	1	3	8	$\cdots$	1	3	$\cdots$	3	1	0
$\Pi_S(y^{-1})$	0	10	1	0	0	$\cdots$	1				4	1

Since the row corresponding to $\Pi_S(y^{-1})$ is independent, we adjoin the row corresponding to $\Pi_S(x^{-1})$ and reduce it with the previous rows.

	1	y	x	y^2	$\cdots$	x^5	y^6	$\cdots$	x^6	1	y	x
$\Pi_S(1)$	3	10	1	3	$\cdots$	1	3	$\cdots$	3	1	0	0
$\Pi_S(y^{-1})$	0	10	1	0	$\cdots$	1				4	1	0
$\Pi_S(x^{-1})$	1	8	3	1	$\cdots$	3				0	0	1

Multiplying the first row by 10, the second and third rows by 3, adding the three rows and substituting the result in the third row we obtain:

	1	y	x	y^2	$\cdots$	x^5	y^6	$\cdots$	x^6	1	y	x
$\Pi_S(1)$	3	10	1	3	$\cdots$	1	3	$\cdots$	3	1	0	0
$\Pi_S(y^{-1})$	0	10	1	0	$\cdots$	1				4	1	0
$\Pi_S(x^{-1})$	0	0	0	0	$\cdots$	0				0	3	3

From this, one obtains that $3x^{-1} + 3y^{-1} \in ker(\Pi_S)$ and the monic polynomial $g_1 = x + y$ is in the reduced Gröbner basis for $Val(S)$. We

continue the algorithm considering the next monomial that is not a multiple of x, and adjoin the row corresponding to $\Pi_S\left(y^{-2}\right)$:

	1	y	x	y^2	$\cdots$	x^5	y^6	$\cdots$	x^6	1	y	x	y^2
$\Pi_S(1)$	3	10	1	3	$\cdots$	1	3	$\cdots$	3	1	0	0	0
$\Pi_S(y^{-1})$	0	10	1	0	$\cdots$	1				4	1	0	0
$\Pi_S(y^{-2})$	3	10	1	3	$\cdots$	3				0	0	0	1

Multiplying the first row by 10 and adding the third row we obtain:

	1	y	x	y^2	$\cdots$	x^5	y^6	$\cdots$	x^6	1	y	x	y^2
$\Pi_S(1)$	3	10	1	3	$\cdots$	1	3	$\cdots$	3	1	0	0	0
$\Pi_S(y^{-1})$	0	10	1	0	$\cdots$	1				4	1	0	0
$\Pi_S(y^{-2})$	0	0	0	0	$\cdots$	0				10	0	0	1

This implies that the polynomial $y^2 + 10$ is in the reduced Gröbner basis. Since there are no monomials left that are not multiples of the leading monomials in the Gröbner basis, $G = \left\{y^2 + 10, x + y\right\}$ is the reduced Gröbner basis for $Val(S)$ with respect to $<_{grlex}$ and $y < x$.

1.5.3 *Conclusions*

We presented an algorithm for computing a Gröbner basis for the ideal of linear recurrence relations on m-dimensional periodic arrays. The algorithm is based on linear algebra computations and can be implemented easily. Since the algorithm does not assume that one already has a generating set for the ideal of linear recurrences, the fact that it gives a generating set is one of the applications of the algorithm. By Proposition 1.2, twice the period minus the dimension of the array is an upper bound for the degree of the polynomials required to form a Gröbner basis for the ideal of linear recurrence relations valid on the array with respect to the graded lexicographic order. Recent applications for the algorithm include the computation of the linear complexity of m-dimensional periodic arrays [9].

Bibliography

[1] J. Abbott, A. Bigatti, M. Kreuzer, and L. Robbiano. Computing ideals of points. *J. Symbolic Comput.*, 30(4):341–356, 2000.

[2] J. Abbott, M. Kreuzer, and L. Robbiano. Computing zero-dimensional schemes. *J. Symbolic Comput.*, 39(1):31–49, 2005.

[3] M. Borges-Quintana, M. A. Borges-Trenard, and E. Martínez-Moro. A general framework for applying FGLM techniques to linear codes. In *Applied algebra, algebraic algorithms and error-correcting codes*, volume 3857 of *Lecture Notes in Comput. Sci.*, pages 76–86. Springer, Berlin, 2006.

[4] M. A. Borges-Trenard, M. Borges-Quintana, and T. Mora. Computing Gröbner bases by FGLM techniques in a non-commutative setting. *J. Symbolic Comput.*, 30(4):429–449, 2000.

[5] Bruno Buchberger. Bruno Buchbergers phd thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal. *Journal of Symbolic Computation*, 41(34):475 – 511, 2006. Logic, Mathematics and Computer Science: Interactions in honor of Bruno Buchberger (60th birthday).

[6] David Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer, New York, third edition, 2007. An introduction to computational algebraic geometry and commutative algebra.

[7] J. C. Faugère, P. Gianni, D. Lazard, and T. Mora. Efficient computation of zero-dimensional Gröbner bases by change of ordering. *J. Symbolic Comput.*, 16(4):329–344, 1993.

[8] Patrizia Gianni, Barry Trager, and Gail Zacharias. Gröbner bases and primary decomposition of polynomial ideals. *J. Symbolic Comput.*, 6(2-3):149–167, 1988. Computational aspects of commutative algebra.

[9] Domingo Gomez-Perez, Tom Hoholdt, Oscar Moreno, and Ivelisse Rubio. Linear complexity for multidimensional arrays - a numerical invariant. In *Information Theory (ISIT), 2015 IEEE International Symposium on*, pages 2697–2701, June 2015.

[10] Ainhoa Aparicio Monforte and Manuel Kauers. Formal Laurent series in several variables. *Expositiones Mathematicae*, 31(4):350 – 367, 2013.

[11] Ivelisse María Rubio. *Gröbner bases for 0-dimensional ideals and applications to decoding, PhD thesis*. Cornell University, Jan., 1998.
[12] Keith Saints and Chris Heegard. On hyperbolic cascaded Reed-Solomon codes. In *Applied algebra, algebraic algorithms and error-correcting codes (San Juan, PR, 1993)*, volume 673 of *Lecture Notes in Comput. Sci.*, pages 291–303. Springer, Berlin, 1993.
[13] Keith Saints and Chris Heegard. Algebraic-geometric codes and multidimensional cyclic codes: a unified theory and algorithms for decoding using Gröbner bases. *IEEE Trans. Inform. Theory*, 41(6, part 1):1733–1751, 1995. Special issue on algebraic geometry codes.
[14] Shojiro Sakata. Finding a minimal set of linear recurring relations capable of generating a given finite two-dimensional array. *J. Symbolic Comput.*, 5(3):321–337, 1988.
[15] Shojiro Sakata. The BMS algorithm. In *Gröbner Bases, Coding, and Cryptography*, pages 143–163. Springer, 2009.
[16] Shojiro Sakata, Helge Elbrønd Jensen, and Tom Høholdt. Generalized Berlekamp-Massey decoding of algebraic-geometric codes up to half the Feng-Rao bound. *IEEE Trans. Inform. Theory*, 41(6, part 1):1762–1768, 1995. Special issue on algebraic geometry codes.
[17] Moss Sweedler and Lee Taylor. An algorithm for finding reduced Gröbner bases for 0-dimensional ideals (preprint). 1996.