Finding a Gröbner basis of a module defined by a vector of nD arrays

Saka??e

Shojiro Sakata
Toyohashi University of Technology
Dep. of Knowledge-Based Information Engineering
Tempaku, Toyohashi 441, Japan

Abstract: We consider a problem which occurs in connecting the concepts of Gröbner bases of modules of n-variate polynomial vectors and of linear recurrences satisfied by n-dimensional (nD) arrays. It also belongs to the class of problems which must be considered in the similar context of extending the algebraic theory on linear recurring 1D arrays, i.e. sequences, to nD arrays. We propose an algorithm for finding efficiently a minimal set of *correlated* linear recurrences capable of generating a given vector of finite nD arrays. This algorithm is also an extension of the Berlekamp-Massey algorithm for finding a Gröbner basis of an ideal defined by an nD array. Although it has a close connection with the nD Berlekamp-Massey algorithm for multiple nD arrays, the former will find a minimal set of *compound* linear recurrences which relate all the nD arrays of the given vector while the latter finds a minimal set of linear recurrences which are *common* to all the given nD arrays.

1. Introduction

Methods for finding Gröbner bases of modules over multivariable polynomial rings were investigated [3, 4, 5, 6]. From the standpoint of the theory of nD linear recurring arrays, a Gröbner basis of a module over the n-variate polynomial ring is a minimal set of compound linear recurrences by which one can generate any vector of linear recurring nD arrays. In other words, it is a mechanism of generating a given ordered set of n-dimensional (nD) arrays, i.e., an nD linear discrete system or a combination of nD linear feedback shift registers. In one of our previous papers, we proposed the nD Berlekamp-Massey algorithm for multiple nD arrays [9]. The latter is for finding a minimal set of linear recurrences which are *common* to all the given nD arrays. If one is required to generate all the given arrays at the same time or in a parallel fashion, the present compound scheme is much simpler with respect to the number of storage elements (registers) than the repetition of the same shift register circuits in parallel.

In this paper we propose an algorithm for finding a minimal set of poly-

nomial vectors defined by any vector of nD arrays, which turns out to be a Gröbner basis of a module over the multivariate polynomial ring under a certain condition. This is an extension of the Berlekamp-Massey algorithm [1, 2] to vectors of nD arrays, which also belongs to the series of our investigations on extending the theory of linear recurrences to n dimensions [7-12].

The contents of the paper are as follows: In Section 2, a Gröbner basis of a module over the n-variate polynomial ring is recognized as a mechanism of generating vectors of linear recurring nD arrays. In addition, some preliminary notations and concepts of a vector of nD arrays over any field and of a minimal set of compound nD recurrences for a given vector of nD arrays are explained and our problem is formulated. In Sections 3 and 4, our algorithm to solve the problem is presented and its validity is shown. In addition, several byproducts of the algorithm are given. In Section 5, an overview of our researches on the nD Berlekamp-Massey algorithm is given. Basically, the complexity of the algorithm is of order $O(s^2)$ for the given vector of arrays with the total size s, while that of the trite method based on matrix computation is of order $O(s^3)$. We mention only the case of $n = 2$ for simplicity, though it is possible to treat the general nD case in a similar way (confer [10]).

2. A system of compound nD linear recurrences

Sometimes we make use of terminologies different from our previous papers [7-12], which are necessary for some new concepts in this context. Only the case of $n = 2$ is treated, and we consider 2D arrays $u = (u_{\mathbf{p}})$ over a field F which are defined on a subset $\Gamma_{\mathbf{u}}$ (called the *support* of u) of the 2D integral lattice $\Sigma_0 := Z_0^2$, i.e., the set of pairs of nonnegative integers $\mathbf{p} = (p_1, p_2)$, $p_1, p_2 \in Z_0$. For the set A of 2D arrays, let a *vector of 2D arrays* $\mathbf{u} = (u^1, \cdots, u^N)$ be an element of A^N, where N is a specified integer and every component of $\mathbf{u}$ $u^k \in A, 1 \leq k \leq N$, is a finite or infinite 2D array with the same support $\Gamma_{\mathbf{u}} \subseteq \Sigma_0$. Over Σ_0 the *partial* order $\leq$ is defined by

$$\mathbf{p} = (p_1, p_2) \leq \mathbf{q} = (q_1, q_2) \Leftrightarrow (p_1 \leq q_1) \wedge (p_2 \leq q_2)$$

and an admissible *total* order $\leq_T$ is defined, for example, by

$$\mathbf{p} \leq_T \mathbf{q} \Leftrightarrow (p_1 + p_2 < q_1 + q_2) \vee ((p_1 + p_2 = q_1 + q_2) \wedge (p_2 \leq q_2))$$

(called *total-degree lexicographic* order). (By the way, $\mathbf{p} < \mathbf{q} \Leftrightarrow (\mathbf{p} \leq \mathbf{q}) \wedge (\mathbf{p} \neq \mathbf{q})$; $\mathbf{p} <_T \mathbf{q} \Leftrightarrow (\mathbf{p} \leq_T \mathbf{q}) \wedge (\mathbf{p} \neq \mathbf{q})$.) According to the total order, we have

the one-to-one correspondence ϕ: $\Sigma_0 \rightarrow Z_0$, i.e., $\phi((0,0)) = 0, \phi((1,0)) = 1, \phi((0,1)) = 2, \phi((2,0)) = 3, \cdots$. The next point of a point $p \in \Sigma_0$ is denoted as $p \dot{\oplus} 1$, where $\phi(p \dot{\oplus} 1) = \phi(p) + 1$. In addition to 2D arrays and vectors of them, we concern ourselves with bivariate polynomials $f \in K[\mathbf{x}] := K[x_1, x_2]$ and polynomial vectors $\mathbf{f} = (f^1, \cdots, f^N) \in (K[\mathbf{x}])^N$. A polynomial $f \in K[\mathbf{x}]$ is denoted in the form:

$$f = \sum_{\mathbf{q} \in exs(f)} f_{\mathbf{q}} \mathbf{x}^{\mathbf{q}},$$

where $exs(f) \subset \Sigma_0$ is the set of exponents $\mathbf{q}$ of nonzero terms of f, which is called the *exponent set* of f, and, for $\mathbf{q} = (q_1, q_2) \in exs(f)$, $f_{\mathbf{q}} \in K$ and $\mathbf{x}^{\mathbf{q}} := x_1^{q_1} x_2^{q_2}$. The elements of $exs(f)$ can be arranged according to the total order $\leq_T$ and the *leading exponent* of f is defined as $lex(f) := max_{\leq_T}\{\mathbf{q} | \, \mathbf{q} \in exs(f)\}$, i.e., the maximum element $\mathbf{q}$ in $exs(f)$ (with respect to the total order $\leq_T$). For a polynomial vector $\mathbf{f} = (f^1, \cdots, f^N)$, the *leading exponent* $lex(\mathbf{f})$, the *head position* $hp(\mathbf{f})$, and the *head coefficient* $hc(\mathbf{f})$ of $\mathbf{f}$ are defined as follows (with respect to the *highest-order largest-suffix component* order; confer [5, 6]):

$$\begin{aligned}
&lex(\mathbf{f}) := max_{\leq_T}\{lex(f^k) | \, 1 \leq k \leq N\};\\
&hp(\mathbf{f}) := max\{k | \, 1 \leq k \leq N,\, lex(f^k) = lex(\mathbf{f})\};\\
&hc(\mathbf{f}) := \quad \text{the coefficient } f^k_{\mathbf{q}} \text{ of the leading exponent term } f^k_{\mathbf{q}}\mathbf{x}^{\mathbf{q}} \text{ of } f^k,\\
&\qquad\qquad \text{for } k = hp(\mathbf{f}),\, \mathbf{q} = lex(\mathbf{f}).
\end{aligned}$$

Corresponding to a polynomial vector $\mathbf{f}$ and a subset $\Gamma \subseteq \Sigma_0$, we consider a correlated or *compound* linear recurrence for a vector of 2D arrays $\mathbf{u} = (u^1, \cdots, u^N)$ with support $\Gamma_{\mathbf{u}}$ as follows:

$$\mathbf{f}[\mathbf{u}]_{\mathbf{p}} := \sum_{k=1}^{N} \sum_{\mathbf{q} \in exs(f^k)} f^k_{\mathbf{q}} u^k_{\mathbf{q}+\mathbf{p}-\mathbf{s}} = 0,\, \mathbf{p} \in \Gamma, \tag{1}$$

where $f^k = \sum_{\mathbf{q} \in exs(f^k)} f^k_{\mathbf{q}} \mathbf{x}^{\mathbf{q}}$ is the k-th component polynomial, $1 \leq k \leq N$, of $\mathbf{f}$ and $\mathbf{s} = lex(\mathbf{f})$. In most cases, we consider vectors of 2D arrays with support of the form: $\Gamma_{\mathbf{u}} = \Sigma^{\mathbf{r}} := \{\mathbf{p} \in \Sigma_0 | \mathbf{p} <_T \mathbf{r}\}$ for a certain $\mathbf{r} \in \Sigma_0$ and we set Γ to equal $\Sigma^{\mathbf{r}}_{\mathbf{s}} := \Sigma_{\mathbf{s}} \cap \Sigma^{\mathbf{r}} = \{\mathbf{p} \in \Sigma_0 | \mathbf{s} \leq \mathbf{p} <_T \mathbf{r}\}$, where $\Sigma_{\mathbf{s}} := \{\mathbf{p} \in \Sigma_0 | \, \mathbf{s} \leq \mathbf{p}\}$. We define the set of *valid* polynomial vectors for $\mathbf{u}$ as

$$Valpol(\mathbf{u}) := \{\mathbf{f} \in (K[\mathbf{x}])^N | \, \mathbf{f}[\mathbf{u}]_{\mathbf{p}} = 0,\, \mathbf{p} \in \Sigma_{\mathbf{s}} \cap \Gamma_{\mathbf{u}},\, \mathbf{s} = lex(\mathbf{f})\}.$$

Then, we can easily prove

Lemma 1: For a vector of *perfect* 2D arrays $\mathbf{u}$ (with support $\Gamma_{\mathbf{u}} = \Sigma_0$), $Valpol(\mathbf{u})$ is a submodule of $(K[\mathbf{x}])^N$ over $K[\mathbf{x}]$.

Although one of our major problems is how to determine a Gröbner basis of such a submodule, we postpone it to the next section. Firstly we assume that a Gröbner basis $\mathbf{F} = \{\mathbf{f}_{(1)}, \cdots, \mathbf{f}_{(M)}\}$ of a submodule $\mathcal{M} \subset (K[\mathbf{x}])^N$ is given, where $\mathbf{F}$ is a union of N subsets $\mathbf{F}^k := \{\mathbf{f}_{k,1}, \cdots, \mathbf{f}_{k,i_k}\}, 1 \leq k \leq N$, the k-th of which is composed of the polynomial vectors $\mathbf{f}_{(l)} = (f^1_{(l)}, \ldots, f^N_{(l)}))$ such that the *head position* $hp(\mathbf{f}_{(l)})$ is equal to k. Consequently, we have an N-tuple of subsets $\Delta_k := \Sigma_0 \backslash \cup_{\mathbf{s} \in \mathbf{S}^k} \Sigma_{\mathbf{s}} \subset \Sigma_0$, where $\mathbf{S}^k := \{\mathbf{s}_{(k,i)} := lex(\mathbf{f}_{k,i}) | \, 1 \leq i \leq i_k\}$. From a given Gröbner basis, we can obtain uniquely the reduced Gröbner basis $\mathbf{F}$ such that $exs(f^k) \setminus \{lex(\mathbf{f})\}$ is contained in Δ_k for the k-th component polynomial f^k of any $\mathbf{f} \in \mathbf{F}$, $1 \leq k \leq N$. Then, we have

Lemma 2: Given any set of values $v^k_{\mathbf{q}} \in K$, $\mathbf{q} \in \Delta_k$, $1 \leq k \leq N$, it is possible to determine uniquely a vector of perfect arrays $\mathbf{u} = (u^1, \cdots, u^N)$ satisfying the initial condition:

$$u^k_{\mathbf{q}} = v^k_{\mathbf{q}}, \, \mathbf{q} \in \Delta_k, \, 1 \leq k \leq N,$$

by using the system of compound linear recurrences defined by the polynomial vectors $\mathbf{f}_{(l)}, 1 \leq l \leq M$, in a *reduced* Gröbner basis $\mathbf{F}$.

Example 1: We consider a vector of two 2D arrays over $K = GF(2)$, which can be generated by a reduced Gröbner basis $\mathbf{F} \subset (K[\mathbf{x}])^2$ composed of four polynomial vectors:

$$\mathbf{f}_{(1)} := (x^2 + 1, \, y + 1), \, \mathbf{f}_{(2)} := (y + 1, \, 1), \, \mathbf{f}_{(3)} := (1, \, x), \, \mathbf{f}_{(4)} := (x, \, y^2),$$

where $x := x_1$, $y := x_2$. From definition $\mathbf{F}$ is a union of $\mathbf{F}^1 = \{\mathbf{f}_{(1)}, \, \mathbf{f}_{(2)}\}$ and $\mathbf{F}^2 = \{\mathbf{f}_{(3)}, \, \mathbf{f}_{(4)}\}$, where $\mathbf{s}_{(1)} = lex(\mathbf{f}_{(1)}) = (2, 0)$, $\mathbf{s}_{(2)} = lex(\mathbf{f}_{(2)}) = (0, 1)$, $hp(\mathbf{f}_{(1)}) = hp(\mathbf{f}_{(2)}) = 1$; $\mathbf{s}_{(3)} = lex(\mathbf{f}_{(3)}) = (1, 0)$, $\mathbf{s}_{(4)} = lex(\mathbf{f}_{(4)}) = (0, 2)$, $hp(\mathbf{f}_{(3)}) = hp(\mathbf{f}_{(4)}) = 2$, and $\Delta_1 = \{(0, 0), (1, 0)\}$, $\Delta_2 = \{(0, 0), (0, 1)\}$. From the following initial values for u^1 and u^2, respectively:

$$\begin{array}{ll} 0 & 1 \quad 1 \\ 1 & \end{array}$$

Fig. 1a

we can obtain a couple of the following arrays u^1 and u^2 by using the compound linear recurrences defined by $\mathbf{F}$ alternately for both arrays and

iteratively according to the total order $\leq_T$ over Σ_0. (For example, $u^1_{(0,1)} = 1$ is determined by using $\mathbf{f}_{(2)}$, i.e., $u^1_{(0,1)} + u^1_{(0,0)} + u^2_{(0,0)} = 0$.)

0	1	0	1	0	0		1	1	1	1	0	0
1	1	0	0	1			0	1	0	1	0	
0	1	0	0				1	1	0	0		
0	0	1					0	1	0			
0	0	*					0	0	*			
1	1						0	0				
0							1					

Fig. 1b

In passing, we remark that, for $\mathbf{S} := \mathbf{S}^k$, the subset $\Delta := \Delta_k = \Sigma_0 \setminus \cup_{\mathbf{s}\in\mathbf{S}}\Sigma_\mathbf{s}$ introduced above is a union of some subsets of the form $\Gamma_\mathbf{c} := \{\mathbf{p} \in \Sigma_0 | \, \mathbf{p} \leq \mathbf{c}\}$, i.e., $\Delta = \Gamma_\mathbf{C} = \cup_{\mathbf{c}\in\mathbf{C}}\Gamma_\mathbf{c}$, where $\mathbf{C}$ is the set of maximal elements of Δ (with respect to the partial order $\leq$). The subsets $\mathbf{S}$ and $\mathbf{C} \subset \Sigma_0$ are *dual* in the sense that (1) one is determined uniquely from the other and (2) there exists no pair $(\mathbf{s}, \mathbf{c})$ of elements $\mathbf{s} \in \mathbf{S}$ and $\mathbf{c} \in \mathbf{C}$ satisfying $(\mathbf{s} \leq \mathbf{c}) \vee (\mathbf{s} \geq \mathbf{c})$. Furthermore, for any $\mathbf{c} = (c_1, c_2) \in \mathbf{C}$, there exists at least one $\mathbf{s} = (s_1, s_2) \in \mathbf{S}$ such that $(s_1 - 1, s_2) \leq \mathbf{c}$ or $(s_1, s_2 - 1) \leq \mathbf{c}$. Such an element $\mathbf{s} \in \mathbf{S}$ is said to be *correlated* with $\mathbf{c}$ and denoted as $\mathbf{s} \vdash \mathbf{c}$. For convenience we assume that $\mathbf{C}$ contains the artificial elements $(\infty, -1)$ and $(-1, \infty)$, which allows us to denote $\Sigma_\mathbf{S} = \Sigma_0 \setminus \Gamma_\mathbf{C}$, where, for the unit vectors $\mathbf{e}^1 = (1, 0)$, $\mathbf{e}^2 = (0, 1)$, $\mathbf{s}$ of the form $s\mathbf{e}^1$ (resp. $s\mathbf{e}^2$), $s \in Z_0$, is correlated with $(\infty, -1)$ (resp. $(-1, \infty)$) (confer [10]).

Any set of polynomial vectors $\mathbf{F} \subset (K[\mathbf{x}])^N$ is said to be *reduced* iff the conditions mentioned just above Lemma 2 are satisfied. Lemma 2 does not hold for a reduced set of polynomial vectors F which is not a Gröbner basis. At least, we can say that any polynomial vector $\mathbf{f}$ contained in the Gröbner basis corresponding to a given vector of perfect 2D arrays $\mathbf{u}$ must have a leading exponent $lex(\mathbf{f})$ which is *minimal* with respect to the partial order $\leq$ among the polynomial vectors in $Valpol(\mathbf{u})$. This consideration leads us to introduction of the following

Definition 1: For a vector of 2D arrays $\mathbf{u}$, a reduced set of polynomial vectors $\mathbf{F}$ is a *minimal polynomial vector set* of $\mathbf{u}$ if and only if the following conditions are satisfied:

(1) $\mathbf{F} \subset Valpol(\mathbf{u})$;

(2) $\neg(\exists \mathbf{g} = (g^1, \cdots, g^N))((\mathbf{g} \in Valpol(\mathbf{u})) \wedge (lex(g^k) \in \Delta_k, 1 \leq k \leq N))$,
where $\Delta_k, 1 \leq k \leq N$, are defined by the leading exponents $\mathbf{s}_{(l)}, 1 \leq l \leq$

M, of the polynomial vectors in $\mathbf{F} = \{\mathbf{f}_{(l)} | \, 1 \leq l \leq M\}$ as above-mentioned.

Now, let $\tilde{\mathbf{F}}(\mathbf{u}) \in 2^{(K[\mathbf{x}])^N}$ be the class of all minimal polynomial vector sets of $\mathbf{u}$ and $\Delta(\mathbf{u}) := (\Delta_1, \ldots, \Delta_N) \in (2^{\Sigma_0})^N$. From now on, we restrict $\tilde{\mathbf{F}}(\mathbf{u})$ to contain only $\mathbf{F}$ which are composed of *monic* polynomial vectors (i.e., any $\mathbf{f} \in \mathbf{F}$ has $hc(\mathbf{f}) = 1$.)

(Remark: $\Delta(\mathbf{u})$ does not depend on $\mathbf{F} \in \tilde{\mathbf{F}}(\mathbf{u})$, but only on $\mathbf{u}$.)

For a vector of finite (or infinite) 2D arrays $\mathbf{u}$ with support $\Gamma_{\mathbf{u}}$ and a point $\mathbf{p} \in \Gamma_{\mathbf{u}}$, the restriction of $\mathbf{u}$ within $\Sigma^{\mathbf{p}}$ is denoted as $\mathbf{u}^{\mathbf{p}}$. It is easy to see that, if $\mathbf{p} \leq_T \mathbf{q}$ and $\mathbf{u}^{\mathbf{p}} = (\mathbf{u}^{\mathbf{q}})^{\mathbf{p}}$, then $\Delta(\mathbf{u}^{\mathbf{p}}) \subseteq \Delta(\mathbf{u}^{\mathbf{q}})$, where the inclusion implies every component-wise inclusion. If $\#\tilde{\mathbf{F}}(\mathbf{u}^{\mathbf{p}}) = 1$, i.e., a minimal polynomial vector set of $\mathbf{u}^{\mathbf{p}}$ $\mathbf{F}$ is unique, $\mathbf{F}$ is likely to be a Gröbner basis corresponding to a perfect array $\mathbf{v}$ satisfying $\mathbf{v}_{\mathbf{q}} = \mathbf{u}_{\mathbf{q}}$, $\mathbf{q} \in \Sigma^{\mathbf{p}}$ (confer [12]). Although we can obtain $\mathbf{F} \in \tilde{\mathbf{F}}(\mathbf{u}^{\mathbf{p}})$ by solving a system of linear equations having the coefficients determined by $\mathbf{u}^{\mathbf{p}}$, this brute force method is quite inefficient. We can eliminate many wasteful computations by extending the Berlekamp-Massey algorithm to our case. Any lemma similar to the first key lemma (Lemma 4 of [7]), which makes the theory of the 2D Berlekamp-Massey algorithm concise and clear, does not hold in our situation. But, a lemma corresponding to the second key lemma (Lemma 5 of [7]) holds:

Lemma 3: For $\mathbf{q} <_T \mathbf{p}$, let

$$\mathbf{f} = (f^1, \cdots, f^N) \in Valpol(\mathbf{u}^{\mathbf{p}}),\ \mathbf{f}[\mathbf{u}]_{\mathbf{p}} = d_{\mathbf{p}} \neq 0, lex(\mathbf{f}) = \mathbf{s};$$
$$\mathbf{g} = (g^1, \cdots, g^N) \in Valpol(\mathbf{u}^{\mathbf{q}}),\ \mathbf{g}[\mathbf{u}]_{\mathbf{q}} = d_{\mathbf{q}} \neq 0, lex(\mathbf{g}) = \mathbf{t};$$

and $\mathbf{r} := max(\mathbf{s}, \mathbf{t} + \mathbf{p} - \mathbf{q})$, where, for $\mathbf{p} = (p_1, p_2)$, $\mathbf{q} = (q_1, q_2) \in \Sigma_0$, $max(\mathbf{p}, \mathbf{q}) := (max\{p_1, q_1\}, max\{p_2, q_2\}) \in \Sigma_0$. Then, the following polynomial vector defined by

$$\mathbf{h} := \mathbf{h}(\mathbf{f}, \mathbf{g}) := \mathbf{x}^{\mathbf{r}-\mathbf{s}}\mathbf{f} - (d_{\mathbf{p}}/d_{\mathbf{q}})\mathbf{x}^{\mathbf{r}-\mathbf{p}+\mathbf{q}-\mathbf{t}}\mathbf{g} \tag{2}$$

is valid also at the point $\mathbf{p}$, i.e., $\mathbf{h} \in Valpol(\mathbf{u}^{\mathbf{p}\oplus\mathbf{1}})$.

Remark 1: $\mathbf{x}^{\mathbf{r}-\mathbf{s}}$ and $\mathbf{x}^{\mathbf{r}-\mathbf{p}+\mathbf{q}-\mathbf{t}}$ act as scalars for vectors $\mathbf{f}$ and $\mathbf{g}$, respectively.

Remark 2: $lex(\mathbf{h}) = \mathbf{r}$, $hp(\mathbf{h}) = hp(\mathbf{f})$ and $hc(\mathbf{h}) = hc(\mathbf{f})$.

If the condition on a polynomial vector $\mathbf{f}$ with $lex(\mathbf{f}) = \mathbf{s}$ mentioned in the above lemma holds at $\mathbf{p}$, $\mathbf{p}$ is called the *order* of $\mathbf{f}$ and denoted as

$ord(\mathbf{f})$; Furthermore, $ord(\mathbf{f}) - lex(\mathbf{f}) = \mathbf{p} - \mathbf{s}$ is denoted as $span(\mathbf{f})$. Thus, $\mathbf{r} = max(ord(\mathbf{f}) - span(\mathbf{f}), ord(\mathbf{f}) - span(\mathbf{g}))$.

Corollary 1: If $span(\mathbf{f}) = \mathbf{p} - \mathbf{s} \leq \mathbf{c}(:= span(\mathbf{g}) = \mathbf{q} - \mathbf{t})$, then $\mathbf{r} = \mathbf{s}$.

3. Finding a minimal polynomial vector set of a vector of 2D arrays

In this section we present an algorithm which is an extention of the Berlekamp-Massey algorithm to the case of a vector of 2D arrays. Our problem is as follows:

Given: a vector of N finite 2D arrays (over a field K) with support $\Gamma_{\mathbf{u}} = \Sigma^{\mathbf{p}}$ $\mathbf{u} = (u^1, \ldots, u^N)$,

Find: a minimal polynomial vector set $\mathbf{F}_j \in \tilde{\mathbf{F}}(\mathbf{u}^{\mathbf{p}_j})$ $(\in 2^{(K[\mathbf{x}])^N})$ of the vector of subarrays $\mathbf{u}^{\mathbf{p}_j}$ at each point $\mathbf{p}_j$ iteratively for $j = 0, 1, \ldots, n$, where $n = \phi(\mathbf{p})$.

First we show our algorithm, the proof of which will be given later. In this algorithm we renew for $j = 0, 1, \ldots, n$ the following

Data: $\mathbf{F}_j \subset (K[\mathbf{x}])^N$ which is a union of N subsets $\mathbf{F}_j^k := \{\mathbf{f} = (f^1, \ldots, f^N) \in \mathbf{F}_j | \, hp(\mathbf{f}) = k\}$ with $\mathbf{S}_j^k := \{lex(\mathbf{f}) | \, \mathbf{f} \in \mathbf{F}_j^k\} \subset \Sigma_0$ and $\mathbf{C}_j^k \subset \Sigma_0$, $k = 1, \ldots, N$, such that $\Sigma_{\mathbf{S}_j^k} = \Sigma_0 \setminus \Gamma_{\mathbf{C}_j^k}$ $(\Delta^k := \Gamma_{\mathbf{C}_j^k})$, $k = 1, \ldots, N$;

$\hat{\mathbf{G}}_j \subset (K[\mathbf{x}])^N$ with $\hat{\mathbf{C}}_j = \{span(\mathbf{g}) | \, \mathbf{g} \in \hat{\mathbf{G}}_j\} \subset \Sigma_0$ and $\hat{\mathbf{S}}_j \subset \Sigma_0$ such that $\Sigma_{\hat{\mathbf{S}}_j} = \Sigma_0 \setminus \Gamma_{\hat{\mathbf{C}}_j}$,

where the last half of the above data also will be defined in the algorithm. (Remark: The data other than $\mathbf{F}_j = \cup_{1 \leq k \leq N} \mathbf{F}_j^k$ and $\hat{\mathbf{G}}_j$ are redundant.)

At the initial point $j = 0$, we have $\mathbf{F}_0^1 := \{\mathbf{e}_{(1)}\}$, $\mathbf{F}_0^2 := \{\mathbf{e}_{(2)}\}, \ldots, \mathbf{F}_0^N := \{\mathbf{e}_{(N)}\}$, $\mathbf{F}_0 = \cup_{1 \leq k \leq N} \mathbf{F}_0^k \in \tilde{\mathbf{F}}(\mathbf{u}^{\mathbf{p}_0})$, where $\mathbf{e}_{(k)} = (0, \ldots, 0, 1, 0, \ldots, 0)$ is the polynomial vector the k-th component of which is a constant polynomial 1 and any other component of which is a constant polynomial 0, $1 \leq k \leq N$.

In the main procedure of Step 2 in Algorithm, we have two alternative cases:

(1) $(\forall \mathbf{f} \in \mathbf{F}_j)(\mathbf{f}[\mathbf{u}]_{\mathbf{p}_j} = 0)$;

(2) $(\exists k, 1 \leq k \leq N)(\exists \mathbf{f} \in \mathbf{F}_j^k)(ord(\mathbf{f}) = \mathbf{p}_j$, i.e., $\mathbf{f}[\mathbf{u}]_{\mathbf{p}_j} \neq 0)$.

In the first case, $\mathbf{F}_j \subset Valpol(\mathbf{u}^{\mathbf{p}_{j+1}})$ and we can put $\mathbf{F}_{j+1} := \mathbf{F}_j$ and go. The second case can be divided further into two subcases:

(2a) $(\forall k, 1 \leq k \leq N) \neg (\exists \mathbf{f} \in \mathbf{F}_j^k, \exists \hat{\mathbf{s}} \in \hat{\mathbf{S}}_j)(ord(\mathbf{f}) = \mathbf{p}_j, \, lex(\mathbf{f}) \leq \mathbf{p}_j - \hat{\mathbf{s}})$;

(2b) $(\exists k, 1 \leq k \leq N)(\exists \mathbf{f} \in \mathbf{F}_j^k, \exists \hat{\mathbf{s}} \in \hat{\mathbf{S}}_j)(ord(\mathbf{f}) = \mathbf{p}_j, \, lex(\mathbf{f}) \leq \mathbf{p}_j - \hat{\mathbf{s}})$.

In case (2a), we can replace each polynomial vector $\mathbf{f} \in \mathbf{F}_j^k$ with $ord(\mathbf{f}) = \mathbf{p}_j$

by $\mathbf{h} = \mathbf{h}(\mathbf{f}, \mathbf{g})$, where $\mathbf{g} \in \hat{\mathbf{G}}_j$ with $span(\mathbf{g}) \geq span(\mathbf{f})$. Since $\hat{\mathbf{s}} \leq \mathbf{p}_j - lex(\mathbf{f})(= span(\mathbf{f}))$ does not hold for any $\hat{\mathbf{s}} \in \hat{\mathbf{S}}_j$, there must exist at least one $\mathbf{g} \in \hat{\mathbf{G}}_j$ with $span(\mathbf{g}) \geq span(\mathbf{f})$. In view of Corollary 1, the formula (2) gives $\mathbf{h}$ with $lex(\mathbf{h}) = lex(\mathbf{f})$, and so we have $\mathbf{S}_{j+1}^k = \mathbf{S}_j^k$ and $\mathbf{C}_{j+1}^k = \mathbf{C}_j^k$. In case (2b) $\bar{\mathbf{F}}_j^k := \{\mathbf{f} \in \mathbf{F}_j^k | ord(\mathbf{f}) = \mathbf{p}_j, lex(\mathbf{f}) = \mathbf{s}$ such that $(\exists \hat{\mathbf{s}} \in \hat{\mathbf{S}}_j)(\mathbf{p}_j \geq \mathbf{s} + \hat{\mathbf{s}})\} \neq \emptyset$, and we cannot have any $\mathbf{h} \in Valpol(\mathbf{u}^{\mathbf{p}_j+1})$ with $lex(\mathbf{h}) = lex(\mathbf{f})$ and $hp(\mathbf{h}) = hp(\mathbf{f})$ for $\mathbf{f} \in \bar{\mathbf{F}}_j^k$, as is shown later. In this case, $\mathbf{S}_{j+1}^k \supset \mathbf{S}_j^k$ (in the strict sense), and there are two possibilities of constructing $\mathbf{h} \in \mathbf{F}_{j+1}^k$ for each $\mathbf{f} \in \bar{\mathbf{F}}_j^k$:

(I) if there exists $\mathbf{g} \in \hat{\mathbf{G}}_j$ such that $span(\mathbf{f}) > span(\mathbf{g})$, then $\mathbf{h} = \mathbf{h}(\mathbf{f}, \mathbf{g})$ has $lex(\mathbf{h}) = ord(\mathbf{f}) - span(\mathbf{g})$ $(> ord(\mathbf{f}) - span(\mathbf{f}) = lex(\mathbf{f}))$.

(II) if there exists $\mathbf{g} \in \hat{\mathbf{G}}_j$ such that, for $\mathbf{s} = lex(\mathbf{f})$, $\hat{\mathbf{c}} = span(\mathbf{g})$, there exist a pair of $\mathbf{c} \in \mathbf{C}_j^k$ and $\hat{\mathbf{s}} \in \hat{\mathbf{S}}_j$ satisfying $\mathbf{p}_j \leq \hat{\mathbf{c}} + \mathbf{c}$, $\mathbf{p}_j \geq \hat{\mathbf{s}} + \mathbf{s}$, $\mathbf{s} \vdash \mathbf{c}$ (i.e., $\mathbf{s}$ is correlated with $\mathbf{c}$), and $\hat{\mathbf{s}} \vdash \hat{\mathbf{c}}$ (i.e., $\hat{\mathbf{s}}$ is correlated with $\hat{\mathbf{c}}$), then $\mathbf{h} = \mathbf{h}(\mathbf{f}, \mathbf{g})$ has $lex(\mathbf{h}) = max(\mathbf{s}, \mathbf{p} - \hat{\mathbf{c}})(\neq \mathbf{s}, \mathbf{p} - \hat{\mathbf{c}})$.

In the possibility (II) the following special case is contained:

(II') $\mathbf{g} = 0 \in \hat{\mathbf{G}}_j$ with $\hat{\mathbf{c}} = span(\mathbf{g}) = (\infty, -1)$ or $(-1, \infty)$,

for which we simply have $\mathbf{h} = \mathbf{x}^{\mathbf{r}-\mathbf{s}}\mathbf{f}$, where

$$\mathbf{r} = max(\mathbf{s}, \mathbf{p} - \hat{\mathbf{c}}) = \begin{cases} (p_1 + 1, s_2) & \text{if} \quad \hat{\mathbf{c}} = (-1, \infty); \\ (s_1, p_2 + 1) & \text{if} \quad \hat{\mathbf{c}} = (\infty, -1). \end{cases}$$

The function $Red(\mathbf{F})$ executes *reduction* of a set of polynomial vectors $\mathbf{F}$ in the sense described just above Definition 1.

Algorithm (Finding a system of compound linear recurrences for a vector of N 2D arrays)

Step 1: $j := 0$;

$\mathbf{F}_0^1 := \{\mathbf{e}_{(1)}\}; \mathbf{F}_0^2 := \{\mathbf{e}_{(2)}\}; \ldots; \mathbf{F}_0^N := \{\mathbf{e}_{(N)}\}$;

$\mathbf{S}_0^1 := \mathbf{S}_0^2 := \ldots \mathbf{S}_0^N := \{(0,0)\}$;

$\mathbf{C}_0^1 := \mathbf{C}_0^2 := \ldots \mathbf{C}_0^N := \{(\infty, -1), (-1, \infty)\}$;

$\hat{\mathbf{G}}_0 := \{0, 0\}; \hat{\mathbf{C}}_0 := \{(\infty, -1), (-1, \infty)\}; \hat{\mathbf{S}}_0 := \{(0,0)\}$;

Step 2: for $k = 1, \ldots, N$ do

begin

$\bar{\mathbf{F}}_j^k := \{\mathbf{f} \in \mathbf{F}_j^k | ord(\mathbf{f}) = \mathbf{p}_j, lex(\mathbf{f}) = \mathbf{s}$ such that

$(\exists \hat{\mathbf{s}} \in \hat{\mathbf{S}}_j)(\mathbf{p}_j \geq \mathbf{s} + \hat{\mathbf{s}})\}$;

$(\bar{\mathbf{S}}_j^k := \{lex(\mathbf{f}) | \mathbf{f} \in \bar{\mathbf{F}}_j^k\};)$

if $\bar{\mathbf{F}}_j^k = \emptyset$ [cases (1) and (2a)] then

begin

$\mathbf{F}^k_{j+1} := (\mathbf{F}^k_j \cup \{\mathbf{h} := \mathbf{h}(\mathbf{f},\mathbf{g}) | \mathbf{f} \in \mathbf{F}^k_j, \mathbf{g} \in \hat{\mathbf{G}}_j$ such that

$ord(\mathbf{f}) = \mathbf{p}_j, \mathbf{span}(\mathbf{f}) \leq \mathbf{span}(\mathbf{g})\}) \setminus \{\mathbf{f} \in \mathbf{F}^k_j | ord(\mathbf{f}) = \mathbf{p}_j\}$;

$(\mathbf{S}^k_{j+1} := \mathbf{S}^k_j; \mathbf{C}^k_{j+1} := \mathbf{C}^k_j;)$

end;

else [$\bar{\mathbf{F}}^k_j \neq \emptyset$, i.e., case (2b)]

begin

$\mathbf{F}^k_{j+1} := (\mathbf{F}^k_j \cup \{\mathbf{h} = \mathbf{h}(\mathbf{f},\mathbf{g}) | \mathbf{f} \in \mathbf{F}^k_j, \mathbf{g} \in \hat{\mathbf{G}}_j$ such that

$ord(\mathbf{f}) = \mathbf{p}_j$, $span(\mathbf{f}) \leq span(\mathbf{g})\}$

$\cup\{\mathbf{h} = \mathbf{h}(\mathbf{f},\mathbf{g}) | \mathbf{f} \in \bar{\mathbf{F}}^k_j, \mathbf{g} \in \hat{\mathbf{G}}_j$ such that $span(\mathbf{f}) > span(\mathbf{g})\}$

$\cup\{\mathbf{h} = \mathbf{h}(\mathbf{f},\mathbf{g}) | \mathbf{f} \in \bar{\mathbf{F}}^k_j$ with $lex(\mathbf{f}) = \mathbf{s}, \mathbf{g} \in \hat{\mathbf{G}}_j$ with $span(\mathbf{g}) = \hat{\mathbf{c}}$

such that $(\exists \mathbf{c} \in \mathbf{C}^k_j, \hat{\mathbf{s}} \in \hat{\mathbf{S}}_j)(\mathbf{p}_j \leq \hat{\mathbf{c}} + \mathbf{c}, \mathbf{p}_j \geq \hat{\mathbf{s}} + \mathbf{s}, \mathbf{s} \vdash \mathbf{c}, \hat{\mathbf{s}} \vdash \hat{\mathbf{c}})\})$

$\setminus\{\mathbf{f} \in \mathbf{F}^k_j | ord(\mathbf{f}) = \mathbf{p}_j\}$;

$(\mathbf{S}^k_{j+1} := (\mathbf{S}^k_j \cup \{\mathbf{p}_j - \hat{\mathbf{c}} | \hat{\mathbf{c}} \in \hat{\mathbf{C}}_j$ such that $(\exists \mathbf{s} \in \bar{\mathbf{S}}^k_j)(\mathbf{s} < \mathbf{p}_j - \hat{\mathbf{c}})\}$

$\cup\{max(\mathbf{s}, \mathbf{p}_j - \hat{\mathbf{c}}) | \mathbf{s} \in \bar{\mathbf{S}}^k_j, \hat{\mathbf{c}} \in \hat{\mathbf{C}}_j$ such that

$(\exists \mathbf{c} \in \mathbf{C}^k_j, \hat{\mathbf{s}} \in \hat{\mathbf{S}}_j)(\mathbf{p}_j \leq \hat{\mathbf{c}} + \mathbf{c}, \mathbf{p}_j \geq \hat{\mathbf{s}} + \mathbf{s}, \mathbf{s} \vdash \mathbf{c}, \hat{\mathbf{s}} \vdash \hat{\mathbf{c}})\})$

$\setminus\{lex(\mathbf{f}) | \mathbf{f} \in \bar{\mathbf{F}}^k_j\}$;

$\mathbf{C}^k_{j+1} := (\mathbf{C}^k_j \cup \{\mathbf{p}_j - \hat{\mathbf{s}} | \hat{\mathbf{s}} \in \hat{\mathbf{S}}_j$ such that $(\exists \mathbf{s} \in \bar{\mathbf{S}}^k_j)(\mathbf{s} \leq \mathbf{p}_j - \hat{\mathbf{s}})\})$

$\setminus\{\mathbf{c} \in \mathbf{C}^k_j | (\exists \hat{\mathbf{s}} \in \hat{\mathbf{S}}_j, \mathbf{s} \in \bar{\mathbf{S}}^k_j)(\hat{\mathbf{s}} < \mathbf{p}_j - \mathbf{c}, \mathbf{p}_j \geq \mathbf{s} + \hat{\mathbf{s}})\};)$

$\hat{\mathbf{G}}_{j+1} := (\hat{\mathbf{G}}_j \cup \bar{\mathbf{F}}^k_j) \setminus \{g \in \hat{\mathbf{G}}_j | (\exists \mathbf{f} \in \bar{\mathbf{F}}^k_j)(span(\mathbf{f}) > span(\mathbf{g}))\}$;

$(\hat{\mathbf{C}}_{j+1} := (\hat{\mathbf{C}}_j \cup \{span(\mathbf{f}) | \mathbf{f} \in \bar{\mathbf{F}}^k_j\})$

$\setminus\{\hat{\mathbf{c}} \in \hat{\mathbf{C}}_j | (\exists \mathbf{f} \in \bar{\mathbf{F}}^k_j)(\hat{\mathbf{c}} < span(\mathbf{f}))\}$;

$\hat{\mathbf{S}}_{j+1} := (\hat{\mathbf{S}}_j \cup \{\mathbf{p}_j - \mathbf{c} | \mathbf{c} \in \mathbf{C}^k_j$ such that

$(\exists \hat{\mathbf{s}} \in \hat{\mathbf{S}}_j, \mathbf{s} \in \bar{\mathbf{S}}^k_j)(\hat{\mathbf{s}} < \mathbf{p}_j - \mathbf{c}, \mathbf{p}_j \geq \mathbf{s} + \hat{\mathbf{s}})\}$

$\cup\{max(\mathbf{p}_j - \mathbf{c}, \hat{\mathbf{s}}) | \mathbf{c} \in \mathbf{C}^k_j, \hat{\mathbf{s}} \in \hat{\mathbf{S}}_j$ such that

$(\exists \mathbf{s} \in \bar{\mathbf{S}}^k_j, \hat{\mathbf{c}} \in \hat{\mathbf{C}}_j)(\mathbf{p}_j \leq \mathbf{c} + \hat{\mathbf{c}}, \mathbf{p}_j \geq \hat{\mathbf{s}} + \mathbf{s}, \mathbf{s} \vdash \mathbf{c}, \hat{\mathbf{s}} \vdash \hat{\mathbf{c}})\})$

$\setminus\{\hat{\mathbf{s}} | (\exists \mathbf{s} \in \bar{\mathbf{S}}^k_j)(\mathbf{p}_j \geq \mathbf{s} + \hat{\mathbf{s}})\};)$

end;

end;

$\mathbf{F}_{j+1} := Red(\cup_{1 \leq k \leq N} \mathbf{F}^k_{j+1})$;

Step 3: $j := j + 1$;

if $j = n$ then stop else go to Step 2.

Example 2: Applying our Algorithm to the vector of two arrays over $K = GF(2)$ $\mathbf{u} = (u^1, u^2)$ shown in Fig. 2b, we have the computation shown in Table 1.

Table 1: Application of Algorithm to the vector of 2D arrays shown in Fig. 2b.

$\mathbf{p}_j$	$\mathbf{F}_j^1$	$\mathbf{F}_j^2$	$\hat{\mathbf{G}}_j$
$(0,0)$	$(1,0)$	$(0,1)$	$(0,0)$
$(1,0)$	$(1,0)$	$(0,x),(0,y)$	$(0,1)$
$(0,1)$	$(x,1),(y,0)$	$(0,x),(0,y)$	$(1,0)$
$(2,0)$	$(x,1),(y,1)$	$(0,x),(0,y+1)$	.
$(1,1)$	$(x,1),(y,1)$	$(1,x),(0,y+1)$	.
$(0,2)$	$(x,1),(y+1,1)$	$(1,x),(1,y+1)$	.
$(3,0)$	$(x,1),(y+1,1)$	$(1,x),(1,y^2+y)$	$(1,0),(1,y+1)$
$(2,1)$	$(x^2,0),(y+1,1)$	$(1,x),(1,y^2+y)$	$(x,1),(1,y+1)$
$(1,2)$	$(x^2+1,y+1),(y+1,1)$	$(1,x),(1,y^2+y)$	.
$(0,3)$	$(x^2+1,y+1),(y+1,1)$	$(1,x),(1,y^2+y)$	.
$(4,0)$	$(x^2+1,y+1),(y+1,1)$	$(1,x),(0,y^2+1)$	.
$(3,1)$	$(x^2+1,y+1),(y+1,1)$	$(1,x),(0,y^2+1)$	.
$(2,2)$	$(x^2+1,y+1),(y+1,1)$	$(1,x),(0,y^2+1)$	.
$(1,3)$	$(x^2+1,y+1),(y+1,1)$	$(1,x),(x,y^2)$	.
$(0,4)$	$(x^2+1,y+1),(y+1,1)$	$(1,x),(x,y^2)$	.
.	.	.	.
.	.	.	.
.	.	.	.
$(4,2)$	$(x^2+1,y+1),(y+1,1)$	$(1,x),(x,y^2)$	$(x,1),(1,y+1)$

The result $\mathbf{F}=\{(x^2+1,y+1),(y+1,1),(1,x),(x,y^2)\}\in\tilde{\mathbf{F}}(\mathbf{u}^{(4,2)})$ is just identical with the reduced Gröbner basis of Example 1.

4. Verification of Algorithm

In this section we prove the following theorem which will verify the Algorithm.

Theorem 1: Let $\mathbf{F}_j$, $j=0,1,2,\ldots,$ be computed by the algorithm. Then, $\mathbf{F}_j\in\tilde{\mathbf{F}}(\mathbf{u}^{\mathbf{p}_j})$, $j=0,1,2,\ldots.$

Since $\mathbf{F}_0\in\tilde{\mathbf{F}}(\mathbf{u}^{\mathbf{p}_0})$, we must prove that, if $\mathbf{F}_j\in\tilde{\mathbf{F}}(\mathbf{u}^{\mathbf{p}_j})$ for any $j\in Z_0$, then $\mathbf{F}_{j+1}\in\tilde{\mathbf{F}}(\mathbf{u}^{\mathbf{p}_{j+1}})$, where $\mathbf{F}_{j+1}$ is determined by the procedure of Step 2 in the algorithm. We discriminate between the two cases $\bar{\mathbf{F}}_j:=\cup_{1\le k\le N}\bar{\mathbf{F}}_j^k=\emptyset$ and $\bar{\mathbf{F}}_j^k\neq\emptyset$ for some k, $1\le k\le N$. If $\bar{\mathbf{F}}_j=\emptyset$, then either we have $\mathbf{F}_{j+1}=\mathbf{F}_j\in\tilde{\mathbf{F}}(\mathbf{u}^{\mathbf{p}_{j+1}})$ (case (1)) or we can find each polynomial vector $\mathbf{f}\in\mathbf{F}_{j+1}^k$ by the formula (2) (case (2a)), where $\mathbf{S}_{j+1}^k=\mathbf{S}_j^k$, $1\le k\le N$, for either case.

If $\bar{\mathbf{F}}_j^k \neq \emptyset$, then there exists at least one $\hat{\mathbf{s}} \leq \hat{\mathbf{S}}_j$ such that $\mathbf{s} \leq \mathbf{p}_j - \hat{\mathbf{s}}$ for some $\mathbf{f} \in \bar{\mathbf{F}}_j^k$ with $lex(\mathbf{f}) = \mathbf{s}$. Therefore, in view of the duality between $\hat{\mathbf{S}}_j$ and $\hat{\mathbf{C}}_j$ we have only to show that there does not exist any polynomial vector $\mathbf{h} \in Valpol(\mathbf{u}^{\mathbf{p}_{j+1}})$ such that $lex(\mathbf{h}) = \mathbf{r} \leq \mathbf{p}_j - \hat{\mathbf{s}}$ and $hp(\mathbf{h}) = k$, where we remark that $(\exists k,\, 1 \leq k \leq N)(\mathbf{S}_j^k \neq \mathbf{S}_{j+1}^k)$ if and only if $\hat{\mathbf{S}}_j \neq \hat{\mathbf{S}}_{j+1}$. Now, let $\mathbf{p}_j = \mathbf{p}_{j(0)} := ord(\mathbf{f})$ for the polynomial vector $\mathbf{f} = \mathbf{e}_{(k)} \in \mathbf{F}_0^k$. Then, it is easy to see that there exists no polynomial vector $\mathbf{h} = (h^1, h^2, \ldots, h^N) \in Valpol(\mathbf{u}^{\mathbf{p}_{j+1}})$ such that $lex(\mathbf{h}) \leq \mathbf{p}_j - \hat{\mathbf{s}} = \mathbf{p}_j$ and $hp(\mathbf{h}) = k$, where $\hat{\mathbf{s}} = (0,0) \in \hat{\mathbf{S}}_0$. In this case we have two kinds of polynomial vectors $\mathbf{h} = \mathbf{x}^{\mathbf{r}-\mathbf{s}}\mathbf{f} \in \mathbf{F}_{j+1}^k$ with $lex(\mathbf{h}) = \mathbf{r} = (p_1+1, 0)$ and $(0, p_2+1)$, respectively (case (II')), and Theorem 1 is true. Therefore, we can assume that $j(0) < j$. Thus, for

$$\begin{aligned} J :=& \{i \in Z_0 \,|\, 0 \leq i < j, \mathbf{S}_i^k \neq \mathbf{S}_{i+1}^k \text{ for some } k,\ 1 \leq k \leq N\} \\ =& \{i \in Z_0 \,|\, 0 \leq i < j, \hat{\mathbf{S}}_i \neq \hat{\mathbf{S}}_{i+1}\}, \end{aligned}$$

we set

$$J = \{j(i) \in Z_0 \,|\, 0 \leq i \leq \tau\},$$

where $0 \leq \tau := \#J$ and $j(0) < j(1) < j(2) < \ldots < j(\tau) < j$.

Any polynomial vector $\mathbf{h}$ with $lex(\mathbf{h}) = \mathbf{r} \geq \mathbf{s}$ and $hp(\mathbf{h}) = k$ can be expressed in the following form:

$$\begin{aligned} \mathbf{h} =& h_{\mathbf{sr}}\mathbf{x}^{\mathbf{r}-\mathbf{s}}\mathbf{f} + \sum_{(\mathbf{s}',\mathbf{r}') \in \Pi'} h_{\mathbf{s}'\mathbf{r}'}\mathbf{x}^{\mathbf{r}'-\mathbf{s}'}\mathbf{f}_{(\mathbf{s}')} \\ &+ \sum_{i=0}^{\tau}\Big(\sum_{(\alpha(i),\beta(i)) \in \Pi(i)} h_{\alpha(i)\beta(i)}\mathbf{x}^{\beta(i)-\alpha(i)}\mathbf{f}_{(\alpha(i))}\Big), \quad (3) \end{aligned}$$

where

$$\begin{aligned} &\mathbf{f} \in \bar{\mathbf{F}}_j^k,\ lex(\mathbf{f}) = \mathbf{s},\ \mathbf{s} \leq \mathbf{r} \leq \mathbf{p}_j - \hat{\mathbf{s}},\ h_{\mathbf{sr}}(\in K) \neq 0; \\ &\mathbf{f}_{(\mathbf{s}')} \in \mathbf{F}_j,\ lex(\mathbf{f}_{(\mathbf{s}')}) = \mathbf{s}',\ \mathbf{s}' \leq \mathbf{r}' <_T \mathbf{r},\ h_{\mathbf{s}'\mathbf{r}'} \in K; \\ &\Pi' := \{(\mathbf{s}',\mathbf{r}') \in (\Sigma_0)^2 \,|\, \mathbf{s}' = lex(\mathbf{f}'),\ \mathbf{f}' \in \mathbf{F}_j,\ \mathbf{s}' \leq \mathbf{r}' <_T \mathbf{r}\}, \\ &\mathbf{f}_{(\alpha(i))} \in \bar{\mathbf{F}}_{j(i)},\ h_{\alpha(i),\beta(i)} \in K, \\ &\Pi(i) := \{(\alpha,\beta) \in (\Sigma_0)^2 \,|\, \alpha = lex(\mathbf{g}),\ \mathbf{g} \in \bar{\mathbf{F}}_{j(i)}, \\ &\quad \alpha \leq \beta \leq \mathbf{p}_{j(i)} - \hat{\mathbf{s}} \text{ for some } \hat{\mathbf{s}} \in \hat{\mathbf{S}}_{j(i)}\},\ 0 \leq i \leq \tau, \end{aligned}$$

Remark 1: For $ord(\mathbf{f}) = \mathbf{p}_j$, $\mathbf{f}_{(\mathbf{s}')} \in \mathbf{F}_j$ has $ord(\mathbf{f}_{(\mathbf{s}')}) \geq_T \mathbf{p}_j$, and $\mathbf{f}_{\alpha(i)} \in \bar{\mathbf{F}}_{j(i)}$ has $ord(\mathbf{f}_{\alpha(i)}) = \mathbf{p}_{j(i)},\ 0 \leq i \leq \tau$.

Remark 2: If $(\alpha,\beta),(\alpha',\beta') \in \Pi(i)$ and $(\alpha,\beta) \neq (\alpha',\beta')$, then we can assume that $\beta \neq \beta'$.

Now, we claim $ord(\mathbf{h}) >_T \mathbf{p}_j$ on the assumption that $lex(\mathbf{h}) = \mathbf{r}$, i.e., $h_{\mathbf{sr}} \neq 0$. To investigate the order of each term of the above expression (3), we define the (virtual) order of a polynomial vector $\mathbf{f}$ *raised to* a point $\mathbf{r} \geq lex(\mathbf{f})$ by

$$ord_{\mathbf{r}}(\mathbf{f}) := \mathbf{q} \overset{\mathbf{r}}{\Leftrightarrow} (\mathbf{f}[\mathbf{u}]^{\mathbf{r}}_{\mathbf{p}} := \sum_{k=1}^{N} \sum_{\mathbf{m} \in exs(f^k)} f^k_{\mathbf{m}} u^k_{\mathbf{m+p-r}} = 0,\ \mathbf{p} \in \Sigma^{\mathbf{q}}_{\mathbf{r}}) \wedge (\mathbf{f}[\mathbf{u}]^{\mathbf{r}}_{\mathbf{q}} \neq 0).$$

In particular, if $lex(\mathbf{f}) = \mathbf{s}$, then $ord_{\mathbf{s}}(\mathbf{f}) = ord(\mathbf{f})$. To prove Theorem 1, we require the following two lemmas, whose proofs are in Appendix.

Lemma 4: For any polynomial vector $\mathbf{f}$ with $lex(\mathbf{f}) \leq \mathbf{r} - \mathbf{q}$, the order raised to $\mathbf{r}$ is

$$ord_{\mathbf{r}}(\mathbf{x}^{\mathbf{q}}\mathbf{f}) = \mathbf{r} - \mathbf{q} + ord(\mathbf{f}) - lex(\mathbf{f}) = \mathbf{r} - \mathbf{q} + span(\mathbf{f}).$$

Lemma 5: For $(\alpha,\beta) \in \Pi(i)$, $(\alpha',\beta') \in \Pi(i')$, $0 \leq i,i' \leq \tau$, such that $(\alpha,\beta) \neq (\alpha',\beta')$, we have

$$ord_{\mathbf{r}}(\mathbf{x}^{\beta-\alpha}\mathbf{f}_{(\alpha)}) \neq ord_{\mathbf{r}}(\mathbf{x}^{\beta'-\alpha'}\mathbf{f}_{(\alpha')}).$$

Since $ord_{\mathbf{r}}(\mathbf{x}^{\mathbf{r}'-\mathbf{s}'}\mathbf{f}_{(\mathbf{s}')}) = \mathbf{r} - (\mathbf{r}' - \mathbf{s}') + ord(\mathbf{f}_{(\mathbf{s}')}) - \mathbf{s}' = \mathbf{r} - \mathbf{r}' + ord(\mathbf{f}_{(\mathbf{s}')}) >_T ord(\mathbf{f}_{(\mathbf{s}')} \geq_T p_j$, we have $ord_{\mathbf{r}}(\mathbf{x}^{\mathbf{r}'-\mathbf{s}'}\mathbf{f}_{(\mathbf{s}')}) >_T p_j$. When we arrange the terms of the expression (3) in the increasing order of $ord_{\mathbf{r}}(\ )$, every term $h_{\alpha(i)\beta(i)}\mathbf{x}^{\beta(i)-\alpha(i)}\mathbf{f}_{(\alpha(i))}$ with $ord_{\mathbf{r}}(\ ) <_T \mathbf{p}_j$ must vanish, i.e., $h_{\alpha(i)\beta(i)} = 0$, since $\mathbf{h}[\mathbf{u}]^{\mathbf{r}}_{\mathbf{q}} = 0$, $\mathbf{q} \in \Sigma^{\mathbf{p}_j}_{\mathbf{r}}$, and $ord_{\mathbf{r}}(\mathbf{x}^{\beta-\alpha}\mathbf{f}_{(\alpha)})$ are distinct not only from each other but also form $ord_{\mathbf{r}}(\mathbf{x}^{\mathbf{r}-\mathbf{s}}\mathbf{f})$. Therefore, if $ord(\mathbf{h}) >_T \mathbf{p}_j$, the first term $h_{\mathbf{sr}}\mathbf{x}^{\mathbf{r}-\mathbf{s}}\mathbf{f}$ must also vanish, i.e., $h_{\mathbf{sr}} = 0$, which is a contradiction. Consequently, $\mathbf{h}$ has $ord(\mathbf{h}) \leq_T \mathbf{p}_j$, and we have completed the proof of Theorem 1.

Now we inquire the totality of $\tilde{\mathbf{F}}(\mathbf{u}^{\mathbf{p}})$, where $\mathbf{p} = \mathbf{p}_j$. In other words, we enumerate all distinct monic reduced polynomial vectors $\mathbf{h} \in Valpol(\mathbf{u}^{\mathbf{p}})$ with $lex(\mathbf{h}) = lex(\mathbf{f})$ and $hp(\mathbf{h}) = hp(\mathbf{f})$ for any $\mathbf{f} \in \mathbf{F}_j (\in \tilde{\mathbf{F}}(\mathbf{u}^{\mathbf{p}}))$. (The proofs of the following two theorems are similar with those of Theorems 4 nd 5 of our previous paper [10] in the case of $n = 1$.)

Theorem 2: For $\mathbf{f} \in \mathbf{F}_j^k$ with $lex(\mathbf{f}) = \mathbf{s} \in \mathbf{S}_j^k$, let $\mathbf{p} = \mathbf{p}_j \in \mathbf{s} + \Gamma_{\hat{\mathbf{C}}_j} := \{\mathbf{s} + \mathbf{r} | \, \mathbf{r} \in \Gamma_{\hat{\mathbf{C}}_j}\}$. Then, any $\mathbf{h} \in Valpol(\mathbf{u}^{\mathbf{P}})$ with $lex(\mathbf{h}) = \mathbf{s}$ and $hp(\mathbf{h}) = k$ can be expressed as

$$\mathbf{h} = \mathbf{f} + \sum_{\mathbf{g} \in \hat{\mathbf{G}}'} h_{\mathbf{g}} \mathbf{g},$$

where $\hat{\mathbf{G}}' := \{\mathbf{g} \in \hat{\mathbf{G}}_j | \, span(\mathbf{g}) = \hat{\mathbf{c}}_{\mathbf{g}} \geq_T \mathbf{p} - \mathbf{s}\}$, $h_{\mathbf{g}} \in K[\mathbf{x}]$ with $lex(h_{\mathbf{g}}) \leq_T \mathbf{p}_{\mathbf{g}} := max_{\leq_T} \{\hat{\mathbf{c}}_{\mathbf{g}} + \mathbf{s} - \mathbf{m} | \, \mathbf{m} \geq \mathbf{s}, \, \mathbf{p} \leq_T \mathbf{m} \leq \hat{\mathbf{c}} + \mathbf{s}\}$.

If a reduced polynomial vector $\mathbf{f}$ does not satisfy the assumption of Theorem 2, $\mathbf{f}$ is unique in the sense that there does not exist any other reduced polynomial vector $\mathbf{h} \in Valpol(\mathbf{u}^{\mathbf{P}})$ with $lex(\mathbf{h}) = lex(\mathbf{f})$, $hp(\mathbf{h}) = hp(\mathbf{f})$, and $hc(\mathbf{h}) = hc(\mathbf{f})(= 1)$. In particular, we have

Theorem 3: If

$$\cup_{k=1}^{N} (\cup_{\mathbf{s} \in \mathbf{S}_j^k} (\mathbf{s} + \Gamma_{\hat{\mathbf{C}}_j})) \subseteq \Sigma_0^{\mathbf{P}_j},$$

then $\mathbf{F}_j \in \tilde{\mathbf{F}}(\mathbf{u}^{\mathbf{P}_j})$ is unique.

5. Concluding Remarks

In our previos works [7-10] we treated various problems in generalizing the Berlekamp-Massey algorithm [1, 2] to n dimensions. The problems are described as follows:

Given a finite set of N-dimensional vectors of n-dimensional arrays $\{\mathbf{u}_{(i)} = (u_{(i)}^1, \ldots, u_{(i)}^N) | \, 1 \leq i \leq m\}$ (over a field K),

Find a minimal set of systems of compound n-dimensional linear recurrences, or more precisely a minimal set of N-dimensional vectors of n-variate polynomials $\{\mathbf{f}_{(j)} = (f_{(j)}^1, \ldots, f_{(j)}^N) | \, 1 \leq j \leq M\}$ such that

$$\sum_{k=1}^{N} f_{(j)\mathbf{q}}^k u_{(i)\mathbf{q}+\mathbf{p}}^k = 0, \, \mathbf{p} \in \text{ a subset of } \Sigma_0, \, 1 \leq i \leq m, 1 \leq j \leq M.$$

The papers [7] and [10] treated the case of $m = 1$ and $N = 1$, where $n = 2$ in [7] and $n \geq 2$ in [10], respectively. While the case of $N = 1$ and an arbitrary m was treated in [9], the case of $m = 1$ and an arbitrary N is treated in this paper. Of course, the most general case of arbitrary pairs m, N can be investigated, which will be done in near future. This research can be extended to n-dimensional arrays over any ring, and the first trial was done in [11].

Acknowledgement

This work was supported in part by the Science Foundation of the Japanese Education Ministry under Grants # 02650262.

References

[1] E. R. Berlekamp, Nonbinary BCH decoding. *Algebraic Coding Theory*, McGraw-Hill Publ. Comp., Chapters 7 and 10, 1968.

[2] J. L. Massey, Shift-register synthesis and BCH decoding. IEEE Trans. Information Theory, vol.IT-15, pp.122-127, 1969.

[3] B. Buchberger, An algorithmic method in polynomial ideal theory. (N. K. Bose, ed.) *Recent Trends in Multidimesional Systems Theory*, D. Reidel Publ. Comp., pp.184-232, 1985.

[4] F. Mora, H. M. Möller, New constructive methods in classical ideal theory. J. of Algebra, vol.100, no.1, pp.138-178, 1986.

[5] A. Furukawa, T. Sasaki, H. Kobayashi, Gröbner basis of a module over $K[x_1, \ldots, x_n]$ and polynomial solutions of a system of linear equations. (B. W. Char, ed.) *Proc. SYMSAC'86*, Waterloo, Canada, pp.222-224, 1986.

[6] B. Wall, Computation of syzygies solution of linear systems over a multivariate polynomial ring. RISC-LINZ Series no.88-86.0, 1988.

[7] S. Sakata, Finding a minimal set of linear recurring relations capable of generating a given finite two-dimensional array. J. of Symbolic Computation, vol.5, pp.321-337, 1988.

[8] S. Sakata, Synthesis of two-dimensional linear feedback shift registers. (L. Huguet, A. Poli, eds.) *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Lecture Notes in Computer Science, Springer Verlag: Proc. of AAECC-5*, Menorca, Spain, pp.394-407, 1989.

[9] S. Sakata, N-dimensional Berlekamp-Massey algorithm for multiple arrays and construction of multivariate polynomials with preassinged zeros. (T. Mora, ed.) *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Lecture Notes in Computer Science, Springer Verlag: Proc. of AAECC-6*, Rome, Italy, pp.356-376, 1989.

[10] S. Sakata, Extension of the Berlekamp-Massey algorithm to N dimensions. Information and Computation, vol.84, no.2, pp.207-239, 1990.

[11] S. Sakata, Two-dimensional shift register synthesis and Gröbner bases for polynomial ideals over an integer residue ring. (H. F. Mattson, Jr., T. Mora, eds.) *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes: Proc. of AAECC-7*, Toulouse, France, 1989 (to appear).

[12] S. Sakata, A Gröbner basis and a minimal polynomial set of a finite nD array. (S. Sakata, ed.) *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes: Proc. of AAECC-8*, Tokyo, Japan, 1990 (to appear).

Appendix

Proof of Lemma 4: Since

$$\begin{aligned}\mathbf{x}^{\mathbf{q}}\mathbf{f}[\mathbf{u}]^{\mathbf{r}}_{\mathbf{p}} &= \sum_{k=1}^{N} \sum_{\mathbf{m}\in exs(f^k)} f^k_{\mathbf{m}} u^k_{\mathbf{m}+\mathbf{q}+\mathbf{p}-\mathbf{r}} \\ &= \sum_{k=1}^{N} \sum_{\mathbf{m}\in exs(f^k)} f^k_{\mathbf{m}} u^k_{\mathbf{m}+(\mathbf{p}-\mathbf{r}+\mathbf{q}+lex(\mathbf{f}))-lex(\mathbf{f})},\end{aligned}$$

we have $\mathbf{x}^{\mathbf{q}}\mathbf{f}[\mathbf{u}]^{\mathbf{r}}_{\mathbf{p}} = 0$ if $\mathbf{p}-\mathbf{r}+\mathbf{q}+lex(\mathbf{f}) <_T ord(\mathbf{f})$, and $\mathbf{x}^{\mathbf{q}}\mathbf{f}[\mathbf{u}]^{\mathbf{r}}_{\mathbf{p}} \neq 0$ if $\mathbf{p}-\mathbf{r}+\mathbf{q}+lex(\mathbf{f}) = ord(\mathbf{f})$. Q.E.D.

Proof of Lemma 5: First, let (α,β), $(\alpha',\beta') \in \Pi(i)$. Then, $\beta \neq \beta'$. From $ord(\mathbf{f}_\alpha) = ord(\mathbf{f}_{\alpha'})(= \mathbf{p}_{j(i)})$, it follows that $ord_{\mathbf{r}}(\mathbf{x}^{\beta-\alpha}\mathbf{f}_\alpha) = \mathbf{r} + ord(\mathbf{f}_\alpha) + \beta$ is not equal to $ord_{\mathbf{r}}(\mathbf{x}^{\beta'-\alpha'}\mathbf{f}_{\alpha'}) = \mathbf{r} + ord(\mathbf{f}_{\alpha'}) + \beta'$. Second, let $(\alpha,\beta) \in \Pi(i)$, $(\alpha',\beta') \in \Pi(i')$, $i < i'$. Then, $ord(\mathbf{f}_\alpha) - \beta$ and $ord(\mathbf{f}_{\alpha'}) - \beta'$ are distinct from each other, since, in view of the derivations of $\hat{\mathbf{C}}_{i+1}$, $\hat{\mathbf{S}}_{i+1}$ based on $\hat{\mathbf{C}}_i$, $\hat{\mathbf{S}}_i$ in Step 2 of Algorithm, we have $ord(\mathbf{f}_\alpha) = \mathbf{p}_{j(i)}$, $\mathbf{p}_{j(i)} - \beta \leq \mathbf{p}_{j(i)} - \alpha \leq \hat{\mathbf{c}}$ for some $\hat{\mathbf{c}} \in \hat{\mathbf{C}}_{j(i)+1} = \hat{\mathbf{C}}_{j(i+1)}$, $i+1 \leq i'$, and $ord(\mathbf{f}_{\alpha'}) = \mathbf{p}_{j(i')}$, $\mathbf{p}_{j(i')} - \beta' \geq \mathbf{p}_{j(i')} - (\mathbf{p}_{j(i')} - \hat{\mathbf{s}}) = \hat{\mathbf{s}}$ for some $\hat{\mathbf{s}} \in \hat{\mathbf{S}}_{j(i')}$, i.e., $\mathbf{p}_{j(i')} - \beta' \in \Sigma_{\hat{\mathbf{S}}_{j(i')}}$, $\mathbf{p}_{j(i)} - \beta \in \Gamma_{\hat{\mathbf{C}}_{j(i+1)}}$ and $\Gamma_{\hat{\mathbf{C}}_{j(i+1)}} \cap \Sigma_{\hat{\mathbf{S}}_{j(i')}} = \emptyset$. Q.E.D.