INFORMATION AND COMPUTATION 84, 207–239 (1990)

Extension of the Berlekamp–Massey Algorithm to N Dimensions*

SHOJIRO SAKATA

Department of Production Systems Engineering, Toyohashi University of Technology, Tempaku, Toyohashi 440, Japan

We present an algorithm for finding a minimal set of linear recurring relations which are valid for a given n-dimensional array over any field, where the "minimality" is defined with respect to the partial order over the n-dimensional lattice. The algorithm is an extension of our two-dimensional version of the Berlekamp–Massey algorithm to more than two dimensions. The n-dimensional theory is based on more general concepts which can be reduced into those of the two-dimensional theory in the previous paper. In a typical case, the resulting set of polynomials characterizing the minimal linear recurring relations proves to be a Groebner basis of the ideal defined by the array, and consequently the structure of an n-dimensional linear feedback shift register with the minimum number of storage devices which can generate the array is determined by it. © 1990 Academic Press, Inc.

1. INTRODUCTION

In the previous paper (Sakata, 1988), we gave an extension of the Berlekamp–Massey algorithm (Berlekamp, 1968; Massey, 1969) to two dimensions. By it we can find a minimal set of linear recurring (LR) relations which are valid for a given two-dimensional (2D) array over any finite field. In particular, if the 2D array is doubly periodic, the minimal set of LR relations just coincides with a Groebner basis of the polynomial ideal (Buchberger, 1970, 1985) which is defined by the given array. In this case, we can construct a 2D linear feedback shift register (LFSR) capable of generating the array on the basis of the connection polynomials which just constitute the Groebner basis of the ideal (Sakata, 1989). In the previous algorithm, its geometrical simplicity in the 2D space is fully exploited, which itself cannot be extended straightforwardly to more than two dimensions.

In this paper we present a general version of the algorithm in any (more than one) dimension. In case of two dimensions, this algorithm is reduced

* This paper was presented in part at the IEEE International Symposium of Information Theory, Kobe, June 1988.

0890-5401/90 $3.00

Copyright © 1990 by Academic Press, Inc.
All rights of reproduction in any form reserved.

643/84/2-6

to a more simplified version of the original 2D algorithm. We use some more general concepts and terminologies which are different from those of the 2D theory in the previous paper, since they are suitable for the n-dimensional description. All the proofs of lemmas and theorems except a few similar ones are newly presented, many of which cannot be derived automatically from the 2D versions. To make clear the intuitive meanings of several basic concepts, we often invoke 3D or 2D examples. The n-dimensional (nD) algorithm is useful not only for constructing nD LFSRs capable of generating nD periodic arrays (Imai, 1976; MacWilliams *et al.*, 1976; Sakata, 1978; Homer *et al.*, 1985), in particular, implementing encoders of nD cyclic codes which are also called Abelian codes (MacWilliams, 1970; Ikai *et al.*, 1976; Imai, 1977; Sakata, 1981), but also for identifying nD discrete linear shift-invariant systems (Justice, 1977; Marzetta, 1980; Prabhu *et al.*, 1982; Chaparro *et al.*, 1982; Bose, 1985a, 1985b; Sakata, 1988).

The contents of this paper are as follows. In Section 2, we introduce several preliminary concepts which are necessary to formulate our problem exactly. Some of them are natural extensions from the 2D case dealt with in our previous papers (Sakata, 1978, 1981, 1988). In Section 3, we give some fundamental lemmas, one of which motivates the concept of "excluded point set" for an array. That concept just suggests our main definition of "minimal polynomial set" for the given array in Section 4, where several lemmas and theorems ensuring the correctness of our nD Berlekamp algorithm are derived. In Section 5, the whole description of our algorithm accompanied with an example of computation and its performance are presented. Section 6 is devoted to showing the complete class of minimal polynomial sets and the relationship to the Groebner basis. An example of 3D LFSR is shown there. Concluding remarks are in Section 7. Our notation is summarized in Appendix 1; The proofs of all lemmas (Lemmas 1–9) are in Appendix 2, and that of Theorem 4 is in Appendix 3.

2. Arrays and Linear Recurring Relations

Our main concern is in n-dimensional (nD) arrays over a field K. To be precise, we begin with introducing the nD lattice Σ_0 defined as the set of all n-tuples of nonnegative integers: $\Sigma_0 := Z_0^n$. An element $x = (x_1, x_2, ..., x_n) \in \Sigma_0$ is called "point," and sometimes it is identified with the power product $z^x := z_1^{x_1} z_2^{x_2} \cdots z_n^{x_n}$, where $z := (z_1, ..., z_n)$ is an n-tuple of independent variables $z_1, ..., z_n$ and $x_i \in Z_0$ is the ith coordinate of x. For any subset $\Gamma \subseteq \Sigma_0$, an nD array (or, for simplicity, an "array") over the field K with the support $\Gamma_u := \Gamma$ is a mapping u from Γ into K, and it is

written as $u=(u_x)$, where the image $u_x := u(x)$, $x \in \Gamma$, is the "value" of u at x.

To scan an array, i.e., to generate or check successively the values of the array, we introduce a fixed total ordering $<_T$ ($\leqslant_T$) over Σ_0 (Buchberger, 1985) which is admissible in the sense that it satisfies the conditions:

(1) for any $p \in \Sigma_0$, $0 := (0, ..., 0) \leqslant_T p$;

(2) for $p, q, r \in \Sigma_0$, if $p <_T q$, then $p + r <_T q + r$,

where $p \leqslant_T q$ implies that either $p <_T q$ or $p = q$. In the examples of this paper, we will take the total degree ordering $<_T$ defined by

$$p = (p_i) <_T q = (q_i) \text{ iff either } \Sigma_{1 \leqslant i \leqslant n} p_i < \Sigma_{1 \leqslant i \leqslant n} q_i \text{ or}$$
$$(\Sigma_{1 \leqslant i \leqslant n} p_i = \Sigma_{1 \leqslant i \leqslant n} q_i) \wedge (\exists i)((1 \leqslant i \leqslant n)$$
$$\wedge (p_i < q_i,\ p_{i+1} = q_{i+1}, ...,\ p_n = q_n)).$$

For a point $x \in \Sigma_0$, we have the unique "next" point w.r.t. the total ordering $<_T$, which is denoted as "$x+1$" symbolically. Over Σ_0, we have the partial ordering $<$ ($\leqslant$) defined as usual:

$$x = (x_i) \leqslant y = (y_i) \qquad \text{iff } x_i \leqslant y_i,\ i \in I := \{1, ..., n\};$$
$$x < y \qquad \text{iff both } x \leqslant y \text{ and } x \neq y \text{ hold,}$$

and the vector sum and difference of $x = (x_i)$, $y = (y_i) \in \Sigma_0$:

$$x + y := (x_i + y_i) \qquad \text{and} \qquad x - y := (x_i - y_i).$$

(We sometimes allow that $x - y \notin \Sigma_0$ for $x, y \in \Sigma_0$, i.e., $x - y \in \Sigma := Z^n$.) For $s \in \Sigma_0$, let

$$\Sigma_s := \{x \in \Sigma_0 \mid s \leqslant x\}, \qquad \Gamma_s := \{x \in \Sigma_0 \mid x \leqslant s\}. \tag{1}$$

(For $s \in \Sigma$, we sometimes consider $\Sigma_s := \{x \in \Sigma \mid s \leqslant x\}$ and $\Gamma_s := \{x \in \Sigma \mid x \leqslant s\}$.) Furthermore, for $s, p \in \Sigma_0$ s.t. $s <_T p$, let

$$\Sigma_s^p := \{x \in \Sigma_0 \mid s \leqslant x <_T p\}. \tag{2}$$

In particular,

$$\Sigma^p := \Sigma_0^p = \{x \in \Sigma_0 \mid x <_T p\}. \tag{3}$$

(See Fig. 1.) An array u with the support $\Gamma_u = \Sigma^p$ is written as u^p, and if $q \leqslant_T p$, then u^q is the restriction (truncation) of $u = u^p$ within Σ^q. An array u with the support $\Gamma_u = \Sigma_0$ is called a "perfect" array.

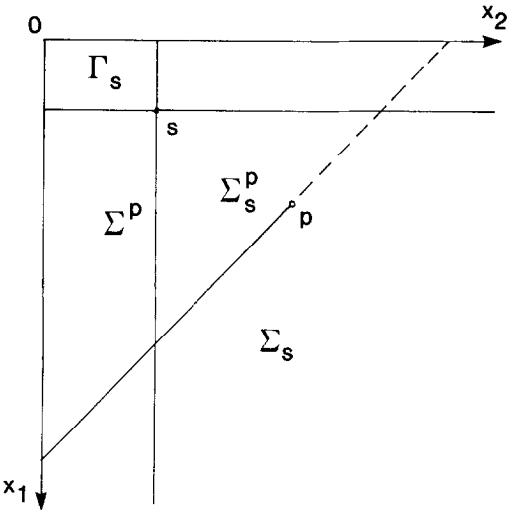

FIG. 1. Subsets of Σ_0: Σ_s, Γ_s, Σ_s^p, and Σ^p (in the 2D case).

EXAMPLE 1. An example of a 3D array u over $K = GF(2)$ with the support $\Sigma^{(5,0,1)}$ is shown in Fig. 2, where the total degree ordering $<_T$ is taken and $x := x_1$, $y := x_2$, $z := x_3$. This is a part of a triply periodic 3D array with the fundamental period vectors (4, 0, 0), (2, 3, 0), and (0, 4, 2) (Sakata, 1978), whose period is

$$\det \begin{vmatrix} 4 & 0 & 0 \\ 2 & 3 & 0 \\ 0 & 4 & 2 \end{vmatrix} = 24.$$

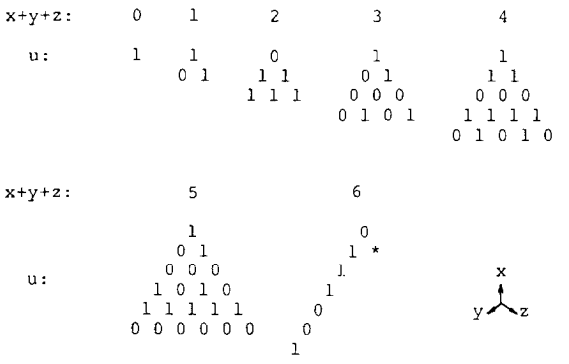

FIG. 2. Example of a 3D array $u = u^p$ over $K = GF(2)$, $p = (5, 0, 1)$.

We explore any linear recurring relations (or constant-coefficient homogeneous linear partial finite-difference equations) which are satisfied by a given array. It is convenient to represent any linear recurring relation by an n-variate polynomial $f \in K[z]$, where $K[z] := K[z_1, ..., z_n]$ is the n-variate polynomial ring over K. Any polynomial $f \in K[z]$ can be written as

$$f = \sum_{x \in \Gamma_f} f_x z^x, \tag{4}$$

where Γ_f is a finite subset of Σ_0 s.t. $f_x (\in K) \neq 0$ for $x \in \Gamma_f$. The maximum element (w.r.t. $<_T$) of Γ_f is called the "degree" of f and written as $\mathrm{Deg}(f)$ or $s = s_f$, which corresponds to the head term $f_s z^s$ of f ($f_s \neq 0$). Corresponding to a polynomial f with $\mathrm{Deg}(f) = s$, we consider a linear recurring (LR) relation at a point $x \in \Sigma_0$ for an array u:

$$f[u]_x := \sum_{y \in \Gamma_f} f_y u_{y+x-s} = 0, \tag{5}$$

where s is specified implicitly by f in the left-hand expression.

EXAMPLE 2. For the array u in Example 1, $f = xy + z + y$ satisfies $f[u]_q = 0$ at $q = (1, 1, 0)$, where $\mathrm{Deg}(f) = (1, 1, 0)$ and $x = x_1$, $y = x_2$, $z = x_3$.

For an array $u = u^p$, a polynomial f with $\mathrm{Deg}(f) = s$ is said to be "valid" (up to p) iff either $p \leqslant_T s$ or $f[u]_x = 0$, $x \in \Sigma_s^p$. The set of all valid polynomials for an array u is denoted as $\mathrm{VALPOL}(u)$. In particular, for any perfect array, we have

LEMMA 1. *If u is a perfect array,* $\mathrm{VALPOL}(u) = \{f \in K[z] \mid f[u]_x = 0, x \in \Sigma_s, s = \mathrm{Deg}(f)\}$ is an ideal in $K[z]$.

(The proofs of all lemmas are in Appendix 2.) The ideal mentioned in Lemma 1 is called the "maximum ideal" of u and is denoted as $I(u)$ (Sakata, 1978, 1981). One of our goals is to find a Groebner basis of $I(u)$.

3. EXCLUDED POINT SET AND MAXIMAL EX-POLYNOMIALS

From now on we will assume a fixed finite array $u = u^p$. The following lemma is our starting point.

LEMMA 2. *Let* $\mathrm{Deg}(f) = s$. *If* $f \in \mathrm{VALPOL}(u^q)$ *and* $f[u]_q \neq 0$ *for a point* q ($\leqslant_T p$), *then there exists no polynomial* g s.t. $g \in \mathrm{VALPOL}(u^{q+1})$ *and* $\mathrm{Deg}(g) \leqslant q - s$, *where* $q + 1$ *is the next point of* q.

Remark. $f \in \mathrm{VALPOL}(u^{q+1})$ implies that $f[u]_q = 0$, but $f \in \mathrm{VALPOL}(u^q)$ does not.

The point $r \in \Sigma_0$ at which f fails to be valid for the first time is called "order" of f (w.r.t. the array u) and written as $\mathrm{Ord}(f)$. Lemma 2 suggests introduction of a finite subset of Σ_0:

$$\Delta_e(u_q) := \bigcup_{r,t \in \Sigma_0^q} \Delta_{r,t}, \tag{6}$$

where

$$\Delta_{r,t} := \Gamma_{r,t}(=\{x \in \Sigma_0 \mid x \leqslant r-t\}), \qquad \text{if there exists a polynomial } g \text{ with } \mathrm{Deg}(g)=t \text{ and } \mathrm{Ord}(g)=r,$$

$$:= \varnothing, \qquad \text{otherwise}$$

DEFINITION 1. $\Delta_e(u^q)$ is called the "excluded point set" of u_q. Let C be the set of maximal points in $\Delta_e(u_q)$ and G be the set of polynomials g with $\mathrm{Deg}(g)=t$ and $\mathrm{Ord}(g)=r$ s.t. $c=r-t \in C$. G and C are called a "maximal ex-polynomial set" and the "maximal ex-point set" of u^q, respectively. (In the 2D case, an excluded point set $\Delta_e(u^q)$ looks like in Fig. 3.)

Motivated by the above definition and the Groebner basis theory (Buchberger, 1970, 1985; Sakata, 1981), we consider whether there exists for any $s \in \Sigma_0/\Delta_e(u_q)$ a polynomial $f \in \mathrm{VALPOL}(u^q)$ with $\mathrm{Deg}(f)=s$, where / denotes the set difference operator. In particular, we investigate any

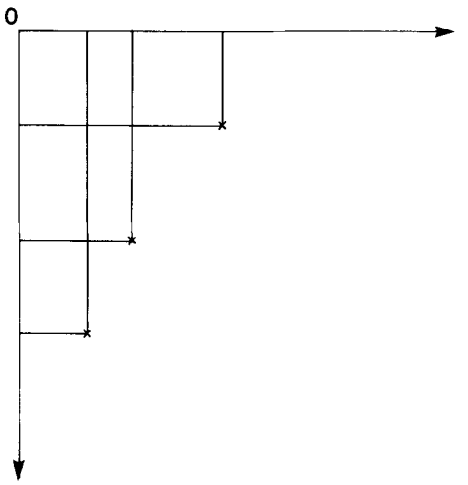

FIG. 3. Excluded point set $\Delta_e(u^q)$ in the 2D case.

"minimal" polynomial f, where the "minimality" implies that $\mathrm{Deg}(f)$ is minimal in $\Sigma_0/\Delta_e(u^q)$ (w.r.t. the partial ordering $<$).

Before formulating our major problem exactly, we introduce some additional terminologies. A finite subset S of Σ_0 is called a "nondegenerate set" (of points) iff, for any $s \in S$, there exists no other point $t \in S$ s.t. $s \leqslant t$. For a nondegenerate set $S \subset \Sigma_0$, every point $s \in S$ is minimal (w.r.t. the partial ordering $<$) in the subset of Σ_0 defined by

$$\Sigma_S := \bigcup_{s \in S} \Sigma_s. \tag{7}$$

On the other hand, every point $s \in S$ is maximal (w.r.t. $<$) in a subset of Σ_0 defined in a dual manner by

$$\Gamma_S := \bigcup_{s \in S} \Gamma_s. \tag{8}$$

The following lemma suggests the duality between the two kinds of subsets.

LEMMA 3. *For any nondegenerate set $S \subset \Sigma_0$, there exists a unique nondegenerate set $C \subset \Sigma_0$ s.t. $\Gamma_C = \Sigma_0/\Sigma_S$. Conversely, for a nondegenerate set C, there exists a unique nondegenerate set S s.t. $\Sigma_S = \Sigma_0/\Gamma_C$.*

The above relation is denoted as $S \vdash C$ and S is said to be "adjoined" to C. (See Fig. 4.) We remark that C may contain several "infinite" points which have some coordinates equal to ∞. Furthermore, if S contains any point s s.t. $s_i = 0$ for some $i \in I = \{1, ..., n\}$, then we allow C to contain a point $c \in \Sigma_0$ s.t. $c_i = -1$, $c_j = \infty$ $(j \neq i)$, which is denoted as $c^{(i)}$. Let $C_\infty := \{c^{(i)} \mid i \in I\} \subseteq C$. Thus, for any $s \in S$ and $i \in I$, there exists at least one $c \in C$ s.t.

$$s_i = c_i + 1, \qquad s_j \leqslant c_j \qquad (j \neq i), \tag{9}$$

where the above relation is denoted by $s \vdash c$, and s is said to be "adjoined" to c; The integer i is written as $i(s, c)$. Conversely, for any finite $c \in C$ and $i \in I$, there exists $s \in S$ s.t. $i = i(s, c)$. Therefore, we have a subset $C_s := \{c \in C \mid s \vdash c\}$ of C for each $s \in S$ and a subset $S_c := \{s \in S \mid s \vdash c\}$ of S for each $c \in C$. Trivially, $\Gamma_C \cap \Sigma_0$ is a finite subset of Σ_0 iff every point in C is either finite or outside of Σ_0.

Remark. In the 2D case, for each $s \in S$ there exist just two points c's s.t. $s \vdash c$ as shown in Fig. 5, where either $s_1 = c_1 + 1$, $s_2 < c_2$ or $s_1 < c_1$, $s_2 = c_2 + 1$.

For $p \in \Sigma_0$ and a couple of nondegenerate sets S and C s.t. $S \vdash C$, let $p - S := \{p - s \in \Sigma_0 \mid s \in S\}$ and $p - C := \{p - c \in \Sigma \mid c \in C\}$. The set $p - C$ sometimes may contain some points outside of Σ_0. Then, we have

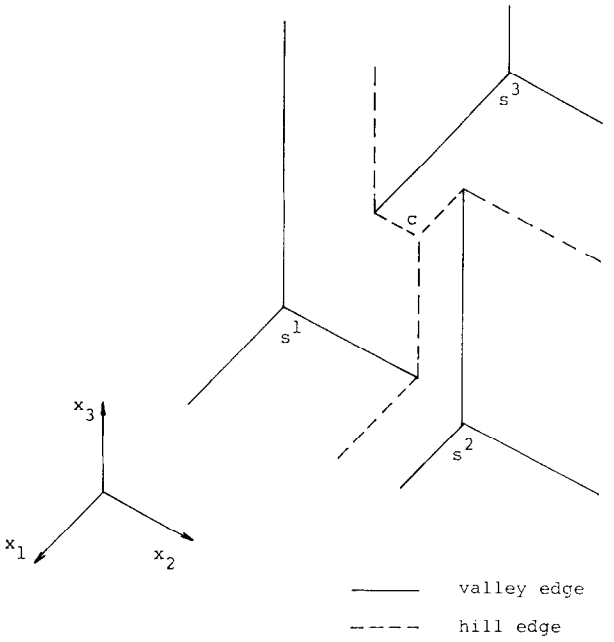

FIG. 4. Adjoinedness $s^1, s^2, s^3 \vdash c$ in the 3D case.

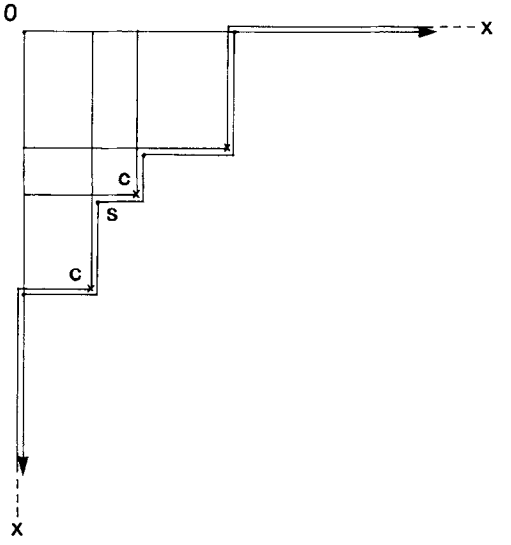

FIG. 5. Adjoinedness $s \vdash c$ in the 2D case.

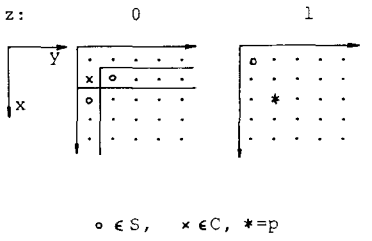

FIG. 6. Nondegenerate sets S and C s.t. $S \vdash C$ in the 3D case.

LEMMA 4. *If* $\Sigma_S = \Sigma_0/\Gamma_C$, *then* $\Sigma_0/\Gamma_{p-S} = \Sigma_{p-C} \cap \Sigma_0$.

EXAMPLE 3. For $n=3$, let $S=\{(2,0,0),\ (1,1,0),\ (0,0,1)\}$ and $p=(2,1,1)$. Then, $C=\{(1,0,0),\ (0,\infty,0)\} \cup C_\infty$ (See Fig. 6), $p-S=\{(0,1,1),(1,0,1),(2,1,0)\}$, $p-C=\{(1,1,1),(2,-\infty,1),(3,-\infty,-\infty),(-\infty,2,-\infty),(-\infty,-\infty,2)\}$. For example, for $s=(1,1,0)$, $C_s=\{(1,0,0),(0,\infty,0),(\infty,\infty,-1)\}$.

4. INDEPENDENT POINT SET AND MINIMAL POLYNOMIALS

Now we focus our attention on a set of polynomials $f \in \mathrm{VALPOL}(u)$ whose $\mathrm{Deg}(f)$ is minimal (w.r.t. $<$) among $\mathrm{VALPOL}(u)$.

DEFINITION 2. A finite subset F of $K[z]$ and a finite subset S of Σ_0 are called a "minimal polynomial set" and the "minimal degree set" of an array u, respectively, iff the following conditions are satisfied:

(1) $F \subset \mathrm{VALPOL}(u)$;

(2) $S := \{s = \mathrm{Deg}(f) \mid f \in F\}$ is a nondegenerate set;

(3) there exists no polynomial g s.t. $g \in \mathrm{VALPOL}(u)$ and $\mathrm{Deg}(g) \in \Delta(F) := \Sigma_0/\Sigma_S$.

In the above definition, we remark that, although F is not always unique for u, S and $\Delta(F)$ are unique for u. Thus, $\Delta(F)$ is written also as $\Delta(u)$, which is called the "independent point set" of u, and the class of minimal polynomial sets F's for u is written as $FF(u)$, which is not empty if $u=u^p$, $p \in \Sigma_0$. Furthermore, it is easy to see that, if $p \geqslant_T q$ and $u^q=(u^p)^q$, $\Delta(u^p) \supseteq \Delta(u^q)$. For any perfect array u, we have

LEMMA 5. *If* u *is a perfect array, then* $F \in FF(u)$ *is a Groebner basis of* $I(u)=\mathrm{VALPOL}(u)$.

For any array $u = u^p$, we necessarily have the inclusion $\Delta_e(u^q) \subseteq \Delta(u^q)$. In the following discussions we will show that, in fact, the identity

$$\Delta_e(u^q) = \Delta(u^q) \tag{10}$$

holds for any $q \in \Sigma^{p+1}$ and give an algorithm for finding $F \in FF(u^q)$ at each $q \in \Sigma^{p+1}$ iteratively. For that purpose, we take an inductive reasoning w.r.t. $q \in \Sigma^{p+1}$ in the total ordering $<_T$. At the beginning, for $q = 0$, we can take $F = \{1\} \in FF(u^0)$, $S = \{0\}$, $G = \{0, ..., 0\}$, $C = C_\infty$ and we have $\Delta(u^0) = \Delta_e(u^0) = \varnothing$. From the discussions in the previous section, it follows that the identity (10) holds iff there exists a couple of polynomial sets (F, G) corresponding to a couple of nondegenerate sets (S, C) s.t.

(1) $F \subset \mathrm{VALPOL}(u^q)$ and, for each $s \in S$, there exists a polynomial $f \in F$ with $\mathrm{Deg}(f) = s$;

(2) $\Gamma_C \cap \Sigma_0 = \Sigma_0 / \Sigma_S$, in other words, S is adjoined to $C = \{c = \mathrm{Ord}(g) - \mathrm{Deg}(g) \mid g \in G\} \cup C_\infty$, where every $g \in G$ corresponding to an infinite $c^{(i)} \in C_\infty$ is defined to be the constant polynomial 0.

F and G are a minimal polynomial set and a maximal ex-polynomial set of $u = u^q$, respectively; S and C are the minimal degree set and the maximal ex-point set of $u = u^q$, respectively.

Now, on assuming that, at a point $q \in \Sigma^p$, the identity (10) holds and that the above condition is satisfied with F, G and S, C, we explore a minimal polynomial set $F^+ \in FF(u^{q+1})$ and the minimal degree set S^+ together with a maximal ex-polynomial set G^+ and the maximal ex-point set C^+ at the next point $q+1$. Some polynomials f in F may be valid also at q. Thus, let

$$\begin{aligned}
&F_V := \{f \in F \mid f[u]_q = 0\},\\
&F_N := F/F_V := \{f \in F \mid f[u]_q = d_f \neq 0\};\\
&S_V := \{\mathrm{Deg}(f) \mid f \in F_V\} \subseteq S,\\
&S_N := S/S_V = \{\mathrm{Deg}(f) \mid f \in F_N\}.
\end{aligned}$$

Trivially, $F_V \subseteq F^+$. If $F \subset \mathrm{VALPOL}(u^{q+1})$, i.e., $F = F_V$, then we need have nothing to do at this point, i.e., $\Delta(u^{q+1}) = \Delta_e(u^{q+1})$, $G^+ = G$, and $F^+ = F \in FF(u^{q+1})$. Otherwise, we must have some method to get each polynomial f^+ in F^+/F_V s.t. $\mathrm{Deg}(f^+) \in S^+$, where, in view of Lemma 2, G^+ and C^+ can be determined from F_N and S_N on the basis of G and C, and S^+ is defined from C^+ as in Lemma 3. To obtain F^+, we define $\max(x, y) := r = (r_i)$ and $\min(x, y) := s = (s_i)$ for $x, y \in \Sigma_0$ by

$$\begin{aligned}
&r_i := \max\{x_i, y_i\}, \qquad i \in I = \{1, ..., n\};\\
&s_i := \min\{x_i, y_i\}, \qquad i \in I.
\end{aligned} \tag{11}$$

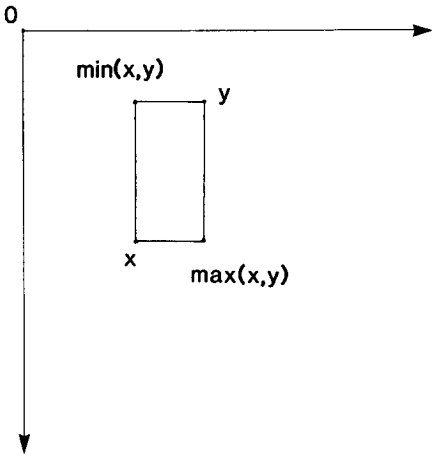

FIG. 7. $\max(x, y)$ and $\min(x, y)$ in the 2D case.

(See Fig. 7.) We remark that, if $p \geqslant x, y$, $\max(p-x, p-y) = p - \mathrm{mix}(x, y)$. Therefore, $\max(s, p-q+t) = p - \min(p-s, q-t)$. In view of this idenity, we have

LEMMA 6. *Let* $p >_T q$ *and* $f, g \in K[z]$, $\mathrm{Deg}(f) = s$, $\mathrm{Deg}(g) = t$. *If*

$$f \text{ has } \mathrm{Ord}(f) = p, \qquad \text{i.e. } f[u]_p = d_f (\neq 0),$$

$$g \text{ has } \mathrm{Ord}(g) = q, \qquad \text{i.e. } g[u]_q = d_g (\neq 0),$$

then the polynomial

$$h := h(f, g) := z^{r-s} f - (d_f/d_g)\, z^{r-p+q-t} g \tag{12}$$

satisfies the condition that $h \in \mathrm{VALPOL}(u^{p+1})$, *where* r *is defined by*

$$r := \max(s, p-q+t)$$

and $\mathrm{Deg}(h) = r$.

In the above, we remark that $p-q+t$ may not be within Σ_0, but $r \in \Sigma_0$. The above construction of a new valid polynomial h from f and g is called "Berlekamp procedure" (See Fig. 8). In our context, we can take a couple of $f \in F_N$ and $g \in G$. In case of $g = 0$ corresponding to an infinite $c^{(i)} \in C_\infty$, the Berlekamp procedure is reduced to the "subsidiary procedure":

$$r := s + (p_i - s_i + 1)\, e^i;$$

$$h := z^{r-s} f,$$

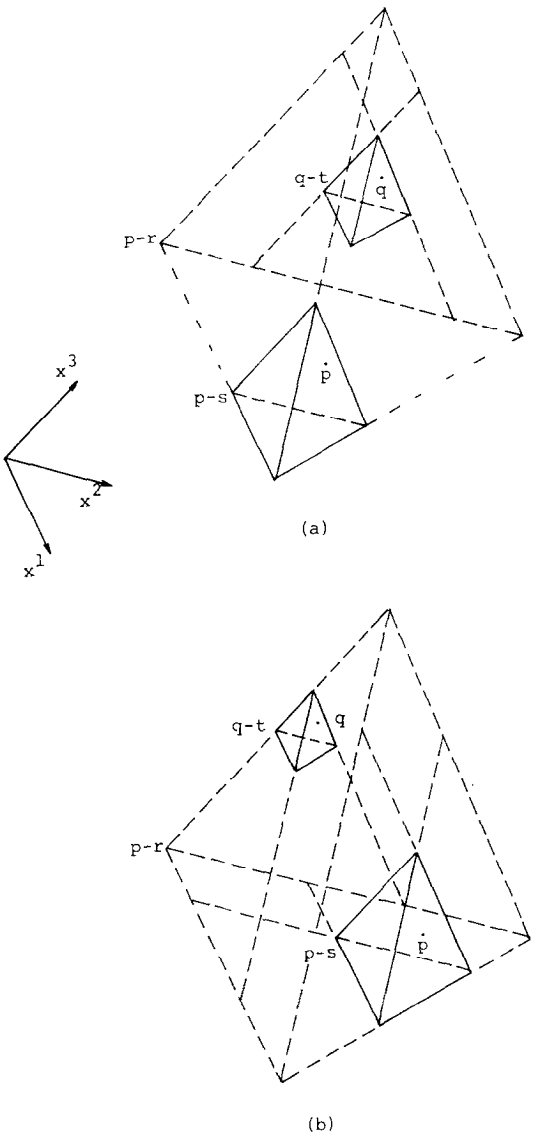

FIG. 8. Berlekamp procedures in the 3D case: (a) Case of $p_1-s_1>q_1-t_1$, $p_2-s_2<q_2-t_2$, and $p_3-s_3<q_3-t_3$; (b) Case of $p_1-s_1>q_1-t_1$, $p_2-s_2>q_2-t_2$, and $p_3-s_3<q_3-t_3$.

where $e^i=(\delta^i_j)\in\Sigma_0$ is the ith unit vector. We remark that each component r_j of r is given by $r_i=p_i+1$, $r_j=s_j$ $(j\neq i)$. (See Fig. 9).

On constructing every $f^+\in F^+/F_V$ by using the Berlekamp procedure (or the subsidiary procedure), we must distinguish between the two cases:

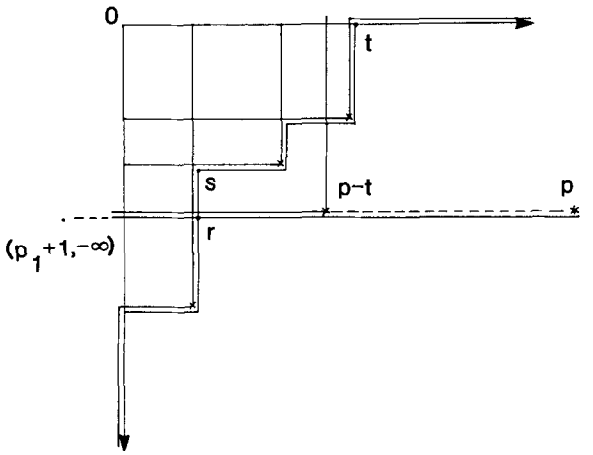

FIG. 9. $r = s + (p_i - s_i + 1)e^i$ $(i = 1)$ in the 2D case.

(A) $\Delta_e(u^{q+1}) = \Delta(u^q)$; (B) $\Delta_e(u^{q+1}) \supset \Delta(u^q)$. In view of Lemma 2, the case (B) occurs iff there exists a couple $f^1, f^2 \in F_N$ s.t.

$$\mathrm{Deg}(f^1) + \mathrm{Deg}(f^2) \leqslant q. \tag{13}$$

Thus, for each $s_f := \mathrm{Deg}(f)$, $f \in F$, we are led to introducing a subset of Σ_0 defined by

$$s_f + \Delta(u^q) := \{s_f + y \mid y \in \Delta(u^q)\}, \tag{14}$$

(See Fig. 10) which has the property that, if $f \in F_N$ does not satisfy $q \in s_f + \Delta(u^q)$, there exists no polynomial $f^+ \in F^+$ s.t. $\mathrm{Deg}(f^+) = \mathrm{Deg}(f)$. On the other hand, if $f \in F_N$ satisfies the condition that $q \in s_f + \Delta(u^q)$, there exists at least one ex-polynomial $g \in G$ s.t. the corresponding $c = \mathrm{Ord}(g) - \mathrm{Deg}(g)$ satisfies $s_f \leqslant q - c$. Consequently, in view of Lemma 6, we have $f^+ := h(f, g) \in F^+$ s.t. $\mathrm{Deg}(f^+) = \mathrm{Deg}(f)$. From the above discussions, we have

THEOREM 1. *Let* $F \in FF(u^q)$, $F^+ \in FF(u^{q+1})$, *and* $f \in F_N$. *There exists* $f^+ \in F^+$ *s.t.* $\mathrm{Deg}(f^+) = \mathrm{Deg}(f)$ *iff* $q \in \mathrm{Deg}(f) + \Delta(u^q)$.

We remark that the condition mentioned in Theorem 1 can be rephrased as follows: the set $C_{\geqslant q-s} := \{c \in C \mid c \geqslant q - s\}$ is not empty for $s = s_f$. Thus,

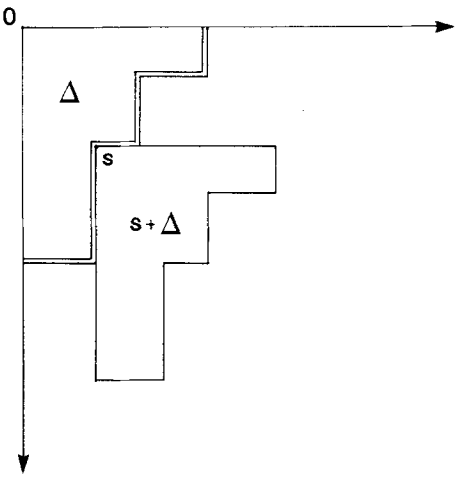

FIG. 10. $s+\Delta$ in the 2D case.

if every $f \in F_N$ with $\mathrm{Deg}(f)=s$ satisfies the condition that $C_{\geqslant q-s}$ is not empty, we have $\Delta_e(u^{q+1})=\Delta_e(u^q)=\Delta(u^q)=\Delta(u^{q+1})$.

On the other hand, if there exists a polynomial $f \in F_N$ s.t. $q \notin s_f + \Delta(u^q)$, we have, in view of Lemma 2.

$$\Delta_e(u^{q+1}) = \Delta(u^q) \cup \left(\bigcup_{f \in F_{NN}} \Gamma_{q-\mathrm{Deg}(f)} \right) \supset \Delta(u_q), \tag{15}$$

where

$$F_{NN} := \{ f \in F_N \mid q \notin \mathrm{Deg}(f) + \Delta(u^q) \}.$$

A nondegenerate set S^+ s.t. $\Sigma_{S^+} := \Sigma_0/\Delta_e(u^{q+1})$ is defined. For each $s^+ \in S^+$, we must explore $f^+ \in F^+$ s.t. $\mathrm{Deg}(f^+)=s^+$. If $s^+ = s \in S$, i.e., $q \in s+\Delta(u^q)$, then we can get $f^+ \in F^+$ s.t. $\mathrm{Deg}(f^+)=s^+$ by the Berlekamp procedure as shown in Theorem 1. Let $s^+ \in (S^+/S) \cap \Sigma_s$ for some $s \in S_N$. Then, it is obvious that $s < s^+$, and that s^+ must be minimal in $\Sigma_s \cap \Gamma_{q-S_{NN}}$, where $S_{NN} := \{ s = \mathrm{Deg}(f) \in S \mid f \in F_{NN} \}$. Such a point s^+ is either of the following two kinds.

LEMMA 7. *If* $s < s^+$, *then* $s^+ = q - c$ *or* $\max(q-c, s)$ *for some* $c \in C$. (*See Fig.* 11.)

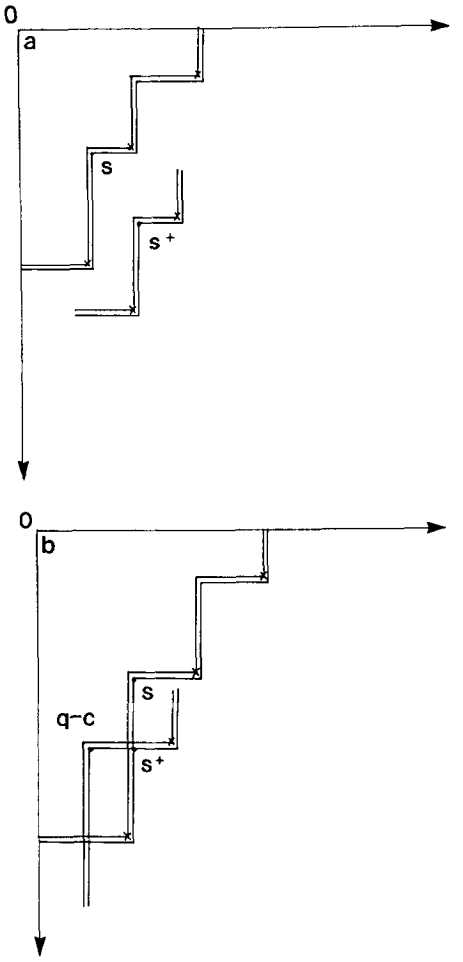

FIG. 11. (a) $s^+ = q - c$ in the 2D case. (b) $s^+ = \max(q - c, s)$ in the 2D case.

For both kinds of new minimal points $s^+ \in S^+$, we have the two lemmas, where we introduce the following subsets of $I := \{i \mid 1 \leqslant i \leqslant n\}$:

$$I_{s>q-c} := \{i \mid s_i > q_i - c_i\},$$

$$I_{s<q-c} := \{i \mid s_i < q_i - c_i\},$$

$$I_{s=q-c} := \{i \mid s_i = q_i - c_i\};$$

$$I_{s;q-c} := \{i \mid \exists a \in C_s \text{ s.t. } i = i(s, a),\ q - c \leqslant a\},$$

$$I_{c;q-s} := \{i \mid \exists t \in S_c \text{ s.t. } i = i(t, c),\ t \leqslant q - s\},$$

$$I_{s;q-c-e} := \{i \mid \exists a \in C_s \text{ s.t. } i = i(s, a),\ q - c - e^i \leqslant a\},$$

$$I_{c;q-s+e} := \{i \mid \exists t \in S_c \cap S_N \text{ s.t. } i = i(t, c),\ t \leqslant q - s + e^i\}.$$

LEMMA 8. *Let $c \in C \cap \Gamma_q$. $s^+ := q - c$ is minimal in Σ_{S^+}/S iff the following conditions are satisfied*:

(1) $\exists s \in S_N$ *s.t.* $s < q - c$, *i.e.*, $I_{s>q-c} = \varnothing$;

(2) $I_{c;q-s} \supseteq I_{s<q-c} (\neq \varnothing)$;

(3) $I_{s;q-c-e} \cup I_{c;q-s+e} \supseteq I_{s=q-c}$.

LEMMA 9. *Let $s \in S_N$ and $c \in C$. $s^+ := \max(q - c, s) (\neq s, q - c)$ is minimal in Σ_{S^+}/S and $s^+ \vdash q - c$ iff the following conditions are satisifed*:

(1) $I_{s;q-c} \supseteq I_{s>q-c} \neq \varnothing$;

(2) $I_{c;q-s} \supseteq I_{s<q-c} \neq \varnothing$;

(3) $I_{s;q-c-e} \cup I_{c;q-s+e} \supseteq I_{s=q-c}$.

Remark. In case of $n = 2$, the above result is simplified into the following statements:

(A) Let $c \in C \cap \Gamma_q$. $s^+ = q - c$ is minimal in Σ_{S^+}/S iff the following conditions are satisfied:

(1) there exists $s \in S$ s.t. $s < q - c$;

(2) if $q_i - c_i = s_i$ for some $i \in I := \{1, 2\}$, then either there exists $a \in C_s$ s.t. $i = i(s, a)$, $q - c - e^i \leqslant a$ or there exists $t \in S_N \cap S_c$ s.t. $i = i(t, c)$, $s \leqslant q - t + e^i$ (in this case, there also exists $t \in S_N \cap S_c$ s.t. $s \leqslant q - t$).

(B) Let $s \in S_N$ and $c \in C$. $s^+ = \max(q - c, s)$ is minimal in Σ_{S^+}/S iff there exists a quartet of $i, j \in I$, $a \in C_s$ and $t \in S_N \cap S_c$ s.t. $i \neq j$, $i = i(s, a)$, $j = i(t, c)$, $q - c \leqslant a$, $s \leqslant q - t$. (See Fig. 12.)

The above cases (A) and (B) correspond respectively to the cases B and $C - F$ in the proof of Theorem 2 of the previous paper (Sakata, 1988).

About the adjoinedness of S^+ to C^+, we have

COROLLARY 1. *Let $s \in S_N$ and $s^+ = q - c > s$. Then,*

(1) *$q - t \in C^+$ and $s^+ \vdash q - t$ for each $t \in S_N \cap S_c$ satisfying either of the following conditions*:

(a) *there exists $i \in I$ s.t. $i = i(t, c)$, $s \leqslant q - t + e^i$ and there exists no $a \in C_s$ s.t. $q - t \leqslant a$;*

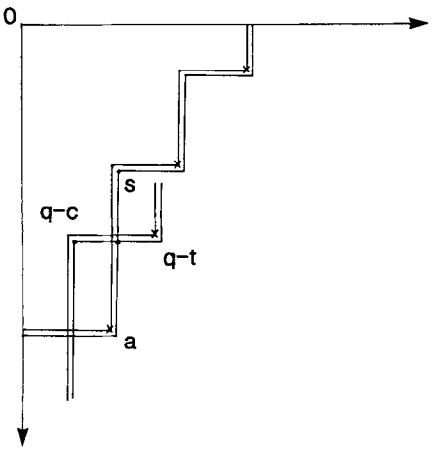

FIG. 12. $s, t \in S$ and $c, a \in C$ s.t. $q-c \leqslant a$, $s \leqslant q-t$, $s \vdash a$, $t \vdash c$ (in the 2D).

(b) *there exists a couple of* $i \in I$ *and* $a \in C_s$ *s.t.* $i = i(s, a)$, $q - c - e^i \leqslant a$, $a < q - t$;

(c) *there exists* $i \in I$ *s.t.* $i = i(t, c)$, $s \leqslant q - t$;

(2) $a \in C^+$ *and* $s^+ \vdash a$ *for each* $a \in C_s$ *satisfying either of the following conditions*:

(a) *there exists a couple of* $i \in I$ *and* $t \in S_N \cap S_c$ *s.t.* $i = i(t, c)$, $s \leqslant q - t + e^i$, $q - t \leqslant a$;

(b) *there exists* $i \in I$ *s.t.* $i = i(s, a)$, $q - c - e^i \leqslant a$, *and there exists no* $t \in S_N \cap S_c$ *s.t.* $a < q - t$.

COROLLARY 2. *Let* $s^+ := \max(q - c, s)$ *and* $s^+ \neq q - c, s$. *Then,*

(1) $q - t \in C^+$ *and* $s^+ \vdash q - t$ *for each* $t \in S_N \cap S_c$ *satisfying either of the following conditions*:

(a) *there exists* $i \in I$ *s.t.* $i = i(t, c)$, $s \leqslant q - t + e^i$, *and there exists no* $a \in C_s$ *s.t.* $q - t \leqslant a$;

(b) *there exists a couple of* $i \in I$ *and* $a \in C_s$ *s.t.* $i = i(s, a)$, $q - c - e^i \leqslant a$, $a < q - t$;

(c) *there exists* $i \in I$ *s.t.* $i = i(t, c)$, $s \leqslant q - t$;

(2) $a \in C^+$ *and* $s^+ \vdash a$ *for each* $a \in C_s$ *satisfying either of the following conditions*:

(a) *there exists a couple of* $i \in I$ *and* $t \in S_N \cap S_c$ *s.t.* $i = i(t, c)$, $s \leqslant q - t + e^i$, $q - t \leqslant a$;

(b) *there exists* $i \in I$ *s.t.* $i = i(s, a)$, $q - c - e^i \leqslant a$, *and there exists no* $t \in S_N \cap S_c$ *s.t.* $a < q - t$.

(c) *there exists* $i \in I$ *s.t.* $i = i(s, a)$, $q - c \leqslant a$.

To get polynomials f^+ with $\mathrm{Deg}(f^+) = s^+$ mentioned in Lemma 7 (or more precisely in Lemmas 8/9), we can use the Berlekamp procedure $f^+ = h(f, g)$, where g is the ex-polynomial corresponding to c mentioned in Lemmas 8/9.

Thus, $S^+ = (S/S_{NN}) \cup \{q - c \mid c \in C$ satisfying the condition in Lemma $8\} \cup \{\max(q - c, s) \mid c \in C,\ s \in S_{NN}$ satisfying the condition in Lemma $9\}$, and we can obtain a polynomial $f^+ \in F^+$ s.t. $\mathrm{Deg}(f^+) = s^+$ for each $s^+ \in S^+$. Thus, we obtain a minimal polynomial set F^+ of u^{q+1} as well as the minimal degree set S^+. Consequently, we have just completed the proof of the identity (10) at $q+1$, i.e., $\Delta_e(u^{q+1}) = \Delta(u^{q+1})$. Furthermore, we also have a couple of $G^+ \subset K[z]$ and $C^+ \subset \Sigma_0$ s.t. $\Gamma_{C^+} = \Delta(u^{q+1}) = \Sigma_0/\Sigma_{S^+}$. Summarizing the discussions in this section, we have

THEOREM 2. *For any* $q \leqslant_T p$, $\Delta(u^q) = \Delta_e(u^q)$, *i.e., the minimal degree set* S *of* u^q *is adjoined to the maximal ex-point set* C *of* u^q, *and we can obtain a couple of a minimal polynomial set* F *and a maximal ex-polynomial set* G *of* u^q.

5. ALGORITHM AND ITS PERFORMANCE

In the previous section, we have found an algorithm for obtaining iteratively a couple of a minimal polynomial set and a maximal ex-polynomial set of a given array $u = u^p$. During the process of executing the algorithm, we update the following data, if necessary, at every point $q \in \Sigma_0^{p+1}$:

$$F = F_V \cup F_N \in FF(u^q),\ S = \{s_f = \mathrm{Deg}(f) \mid f \in F\} = S_V \cup S_N;$$

$$G \subset K[z],\ C = \{c = c_g (= \mathrm{Ord}(g) - \mathrm{Deg}(g)) \mid g \in G\} \cup C_\infty,$$

$$D = \{d = d_g \in K \mid g \in G\};$$

$$ISC \subseteq S \times C,$$

where $|F| = |S|$, $|G| = |C| = |D|$, and $\Delta := \Delta(u^q) = \Sigma_0/\Sigma_S = \Gamma_C$; $(s, c) \in ISC$ iff $s \vdash c$. We remark that $l := |F|$ and $m := |G|$ depend on q, and that Δ is nondecreasing when q increases w.r.t. $<_T$. In the following, "$\rightarrow$" and "$\leftarrow$" imply respectively "insert" and "delete"; e.g., "$s^+ \rightarrow S$" implies "insert s^+ into S" and "$f \leftarrow F$" implies "delete f out of F."

ALGORITHM.

Step 1: $q := 0$; $F := \{1\}$; $G := \{0, ..., 0\}$; $S := \{0\}$;
$C := C_\infty = \{c^{(i)} | i \in I\}$;
$ISC := \{(0, c^{(1)}), ..., (0, c^{(n)})\}$;

Step 2: $F_V := F_N := \varnothing$; $S_V := S_N := \varnothing$;
for every $f \in F$ do
begin
$s := \mathrm{Deg}(f)$;
calculate $d := f[u]_q$;
if $d = 0$ then begin $f \to F_V$; $s \to S_V$ end;
else begin $f \to F_N$; $s \to S_N$ end;
end;

Step 3: if $S_N = \varnothing$ then goto Step 6;

Step 4: for each $c \in C$ do
begin
$S_{\geqslant q-c} := \{s \in S | s \geqslant q - c\}$; $S_{<q-c} := \{s \in S | s < q - c\}$;
end; [Remark: either $S_{\geqslant q-c}$ or $S_{<q-c}$ is empty.]

Step 5: for each $f \in F_N$ with $\mathrm{Deg}(f) = s \in S_N$ do
begin
$C_{\geqslant q-s} := \{c \in C | c \geqslant q - s\}$; $C_{<q-s} := \{c \in C | c < q - s\}$;
[Remark: Either $C_{\geqslant q-s}$ or $C_{<q-s}$ is empty.]
if $C_{\geqslant q-s} \neq \varnothing$ then
begin
$f^+ := h(f, g)$ for any $g \in G$ s.t. $c = \mathrm{Ord}(g) - \mathrm{Deg}(g) \in C_{\geqslant q-s}$;
$f := f^+$;
end;

if $C_{<q-s} \neq \varnothing$ then
begin
for each $c \in C_{<q-s}$ do
if $I_{s<q-c} \subseteq I_{c;q-s}$ and $I_{s=q-c} \subseteq I_{s;q-c-e} \cup I_{c;q-s+e}$ then
begin
$f^+ := h(f, g)$ for $g \in G$ with $c = \mathrm{Ord}(g) - \mathrm{Deg}(g)$; $s^+ := q - c$;
for each $i \in I_{s<q-c}$ do
for each $t \in S_N \cap S_c$ s.t. $i = i(t, c)$, $s \leqslant q - t$ do
$(s^+, q - t) \to ISC$;
for each $i \in I_{s=q-c}$ do
begin
for each $t \in S_N \cap S_c$ s.t. $i = i(t, c)$, $s \leqslant q - t + e^i$ do
if $C_s \cap C_{\geqslant q-t} = \varnothing$ then $(s^+, q - t) \to ISC$
else for each $a \in C_s \cap C_{\geqslant q-t}$ do $(s^+, a) \to ISC$;
for each $a \in C_s$ s.t. $i = i(s, a)$, $q - c - e^i \leqslant a$ do
if $S_N \cap S_c \cap S_{<q-a} = \varnothing$ then $(s^+, a) \to ISC$
else for each $t \in S_N \cap S_c \cap S_{<q-a}$ do $(s^+, q - t) \to ISC$;
end;
$f^+ \to F$; $s^+ \to S$; $g \leftarrow G$; $c \leftarrow C$; $(*, c) \leftarrow ISC$;
end;
if $C_{<q-s} \neq C$ then
for each $c \in C/C_{<q-s}$ do
if $I_{s>q-c} \subseteq I_{s;q-c-e}$ and $I_{s<q-c} \subseteq I_{c;q-s}$ and
$I_{s=q-c} \subseteq I_{s;q-c-e} \cup I_{c;q-s+e}$ then

```
begin
  f⁺ := h(f, g); s⁺ := max(q − c, s);
  for each i ∈ I_{s<q−c} do
    for each t ∈ S_N ∩ S_c s.t. i = i(t, c), s ≤ q − t do
      (s⁺, q − t) → ISC;
  for each i ∈ I_{s>q−c} do
    for each a ∈ C_s s.t. i = i(s, a), q − c ≤ a do
      (s⁺, a) → ISC;
  for each i ∈ I_{s=q−c} do
  begin
    for each t ∈ S_N ∩ S_c s.t. i = i(t, c), s ≤ q − t + e^i do
      if C_s ∩ C_{≥q−t} = ∅ then (s⁺, q − t) → ISC
      else for each a ∈ C_s ∩ C_{≥q−t} do (s⁺, a) → ISC;
    for each a ∈ C_s s.t. i = i(s, a), q − c − e^i ≤ a do
      if S_N ∩ S_c ∩ S_{<q−a} = ∅ then (s⁺, a) → ISC
      else for each t ∈ S_N ∩ S_c ∩ S_{<q−a} do
        (s⁺, q − t) → ISC;
  end;
  f⁺ → F; s⁺ → S;
 end;
 f ← F; s ← S; (s, *) ← ISC;
 f → G; q − s → C;
 end;
end;
```

Step 6: $q := q + 1$; if $q <_T p$ then goto Step 2 else stop.

EXAMPLE 4. For the 3D array $u = u^p$, $p = (5, 0, 1)$, shown in Fig. 2, part of the computation by Algorithm is shown in Table I. At $q = 0$, (2, 0, 0), (0, 1, 1), (1, 2, 1), and (2, 3, 0), we have $\Delta(u^q) \neq \Delta(u^{q+1})$. For example, the polynomials $y + x + 1$, $z + 1$ have order (0, 1, 1), and, at $q = (0, 1, 1)$, from the calculations of $\max(s, q - c)$:

$\max(s, q-c)$	G	$x+1$	0	0	0
F_N	$q-c$ / s	$(-1, 1, 1)$	$(1, -\infty, -\infty)$	$(-\infty, 2, -\infty)$	$(-\infty, -\infty, 2)$
$y+x+1$	(0, 1, 0)	(0, 1, 1)	(1, 1, 0)	(0, 2, 0)	—
$z+1$	(0, 0, 1)	—	(1, 0, 1)	—	(0, 0, 2)

we have

$$(x(y + x + 1) \to) xy + 1, (y(y + x + 1) \to) y^2 + y + 1, (x(z + 1) =) xz + x,$$
$$(z(y + x + 1) + x(x + 1) \to) yz + z + x + 1, (z(z + 1) =) z^2 + z \in F^+$$
$$\subset \mathrm{VALPOL}(u^{q+1}),$$

TABLE I

Example of Computation
(Application of Algorithm to the 3D Array Shown in Fig. 1)

Iteration	Point	F	G	C
0	(0, 0, 0)	1	0^a	$(-1, \infty, \infty)^a$
			0^a	$(\infty, -1, \infty)^a$
			0^a	$(\infty, \infty, -1)^a$
1	(1, 0, 0)	x	1	(0, 0, 0)
		y		
		z		
⋮				
6	(2, 0, 0)	$x+1$	1	(0, 0, 0)
		y		
		$z+1$		
7	(1, 1, 0)	x^2+x+1	$x+1$	(1, 0, 0)
		y		
		$z+1$		
⋮				
10	(0, 1, 1)	x^2+x+1	$x+1$	(1, 0, 0)
		$y+x+1$		
		$z+1$		
11	(0, 0, 2)	x^2+x+1	$x+1$	(1, 0, 0)
		$xy+1$	$y+x+1$	(0, 0, 1)
		y^2+y+1	$z+1$	(0, 1, 0)
		$xz+x$		
		$yz+z+x+1$		
		z^2+z		
⋮				
30	(0, 3, 1)	$x^2+z+y+1$	$y^2+z+x+1$	(1, 0, 1)
		$xy+z+y$	$xz+y+x$	(0, 2, 0)
		$y^3+z+y+1$		
		$yz+y+1$		
		$z^2+z+x+1$		
⋮				
35	(0, 1, 3)	$x^2+z+y+1$	$y^2+z+x+1$	(1, 0, 1)
		$xy+z+y$	$xz+y+x$	(0, 2, 0)
		$y^3+z+y+1$		
		$yz+y+1$		
		z^2+y^2		
⋮				
62	(2, 4, 0)	$x^2+z+y+1$	$y^2+z+x+1$	(1, 0, 1)
		$y^3+z+y+1$	$xy+z+y$	(1, 2, 0)
		$yz+y+1$		
		z^2+y^2		

[a] In this table, these data are not shown at all points except here.

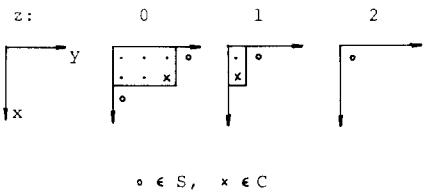

FIG. 13. The independent point set $\Delta(u^p)$ of the 3D array u^p in Fig. 2.

where $\rightarrow$ implies "reducing w.r.t. the other polynomials in F^+" (Buchberger, 1985). Consequently, we have $F^+ = \{x^2+x+1,\ xy+1,\ y^2+y+1,\ xz+x,\ yz+z+x+1,\ z^2+z\}$ for $q+1=(0,0,2)$. At $p=(5,0,1)$, we have the final result

$$F=\{x^2+z+y+1,\ y^3+z+y+1,\ yz+y+1,\ z^2+y^2\} \in FF(u^p),$$

which turns out to be the reduced Groebner basis of the ideal $I(u)$ for the triply periodic array mentioned in Example 1, where the independent point set $\Delta(u)$ is shown in Fig. 13.

Now we consider the complexity of the algorithm under the assumption that l and m are bounded. About the space complexity, at each iteration, we need the storage for F, S, G, C, ISC as well as either $S_{\geqslant q-c}$ or $S_{<q-c}$ for each $c \in C$ and either $C_{\geqslant q-s}$ or $C_{<q-s}$ for each $s \in S$. Thus, we have the total space complexity of order $O(((l+m)n\,|\Delta|+lm)\,|p|) < O(((l+m)n\,|p|+lm)\,|p|) \approx O(|p|^2)$, where $|p|$ is the size of the given array $u=u^p$. About the time complexity, at each iteration, we have

(1) $O(ln\,|q|)$ to calculate all $d=f[u]_q$;

(2) $O(lmn)$ to obtain $S_{\geqslant q-c}$, $S_{<q-c}$, $C_{\geqslant q-s}$ and $C_{<q-s}$;

(3) $O(lm)$ to update ISC;

(4) $O(ln\,|q|)$ for the Berlekamp procedures.

Thus, we have

THEOREM 3. *If $l := |F|$ and $m := |G|$ are bounded, then the total time and space complexity of Algorithm applied to an array of size k is of order $O(k^2)$.*

6. THE COMPLETE CLASS $FF(u^p)$

In this section, we restrict $FF(u)$ to be the class of minimal polynomial sets F composed of "monic" polynomials f in "reduced normal form" in the sense that for any $f \in F$, $\Gamma_f \subseteq \{\mathrm{Deg}(f)\} \cup \Delta(F)$, where such reduction can

be made as in the Groebner basis algorithm (Buchberger, 1970, 1985; Sakata, 1981). Then, we have

THEOREM 4 (Uniqueness of $F \in FF(u^p)$). *Let* $F \in FF(u^p)$. $|FF(u^p)| = 1$ *iff*

$$\bigcup_{f \in F} (\mathrm{Deg}(f) + \Delta(u^p)) \subseteq \Sigma^p,$$

or in other words,

$$\max_T \{\mathrm{Deg}(f) + \mathrm{Ord}(g) - \mathrm{Deg}(g) \mid f \in F,\ g \in G\} <_T p,$$

where $\max_T\{\ldots\}$ *is the maximum (w.r.t.* $<_T$*) element of the set* $\{\ldots\}$.

THEOREM 5 (The complete class $FF(u^p)$). *Let* $F \in FF(u^p)$ *and* $\Delta = \Delta(u^p)$ *be a minimal polynomial set and the independent point set of* u^p; G *and* $C = \{c = \mathrm{Ord}(g) - \mathrm{Deg}(g) \mid g \in G\}$ *are a maximal ex-polynomial set and the maximal ex-point set, where* $\Delta = \Gamma_C \cap \Sigma_0 = \Sigma_0/\Sigma_S$. *For any* $F^1 \in FF(u^p)$, $f^1 \in F^1$ *with* $\mathrm{Deg}(f^1) = \mathrm{Deg}(f) = s$ *is of the form*

$$f + \sum_{g \in G_s} h_g g,$$

where $h_g \in K[z]$, $\mathrm{Deg}(h_g) \leqslant_T q_g := s + \mathrm{Ord}(g) - \mathrm{Deg}(g) - p$, *and*

$$G_s := \{g \in G \mid s + \mathrm{Ord}(g) - \mathrm{Deg}(g) \geqslant p\}.$$

(For the proof of Theorem 4, see Appendix 3. Once Theorem 4 has been established, the proof of Theorem 5 is almost the same as in the 2D case (Sakata, 1989).)

EXAMPLE 5. For the 3D array in Fig. 2 and $p = (0, 3, 1)$, $F \in FF(u^p)$, and the corresponding ex-polynomial set G are given respectively by

$$F = \{x^2 + z + y + 1,\ xy + z + y,\ y^3 + z + y + 1,\ yz + y + 1,\ z^2 + z + x + 1\},$$
$$G = \{y^2 + z + x + 1,\ xz + y + x\}.$$

(See Table I.) For $f = yz + y + 1 \in F$ with $s = \mathrm{Deg}(f) = (0, 1, 1)$, G_s is a singleton $\{g\}$, where $g = xz + y + x$ and $s + \mathrm{Ord}(g) - \mathrm{Deg}(g) = (0, 3, 1) = p$. Thus,

$$\{f + \alpha g \mid \alpha \in GF(2)\} = \{yz + y + 1,\ yz + xz + x + 1\}$$

is the complete set of polynomials f^1 s.t. $\mathrm{Deg}(f^1)=s$ and $f^1\in \mathrm{VALPOL}(u^p)$. Similarly, for $f=y^3+z+y+1$ with $s=\mathrm{Deg}(f)=(0,3,0)$, $G_s=\{g\}=\{y^2+z+x+1\}$, where $s+\mathrm{Ord}(g)-\mathrm{Deg}(g)=(1,3,1)>p$. Thus,

$$\{f+(\alpha x+\beta)g \mid \alpha,\beta\in GF(2)\}$$
$$=\{y^3+z+y+1,\ y^3+y^2+y+x,$$
$$y^3+xy^2+xz+x^2+z+y+x+1,\ y^3+xy^2+xz+y^2+x^2+y\}$$

is the complete set of polynomials f^1 s.t. $\mathrm{Deg}(f)=s$ and $f^1\in \mathrm{VALPOL}(u^p)$.

About the relationship of a minimal polynomial set F to the Groebner basis, we have

THEOREM 6. *Let $F\in FF(u^{2p})$ and $\Delta=\Delta(u^{2p})$. If*

$$\bigcup_{f\in F}(\mathrm{Deg}(f)+\Delta)\subseteq \Sigma^p,$$

then F is a Groebner basis.

COROLLARY 3. *$F\in FF(u^p)$ is a Groebner basis of an ideal I iff there exists a perfect array v s.t. $F\subset \mathrm{VALPOL}(v)$ and $I=I(v)$.*

(The proof of Theorem 6 is also quite the same as in the 2D case (Sakata, 1989).)

Remark. In Example 4, the final result $F\in FF(u^p)$, $p=(5,0,1)$, is a Groebner basis as mentioned above. We note that the condition of Theorem 6 has not been satisfied yet at this point p, though the condition for uniqueness (Theorem 4) is satisfied. It is conjectured that, if the uniqueness condition is fullfiled at p, then $f\in FF(u^p)$ is a Groebner basis of the ideal $I(v)$ defined by a perfect array v s.t. $v^p=u^p$.

For any $F\in FF(u^p)$ which satisfies the condition of Corollary 3, we can construct an nD linear feedback shift register (LFSR) which is characterized by the polynomials of F.

EXAMPLE 6. The polynomial set $F=\{x^2+z+y+1,\ y^3+z+y+1,\ yz+y+1,\ z^2+y^2\}\in FF(u^p)$ of Example 4 characterizes a 3D LFSR shown in Fig. 14, which has three kinds of shift clocks corresponding to x-, y-, and z-shifts of any 3D array, where $x=x_1$, $y=x_2$, $z=x_3$. It has two layers

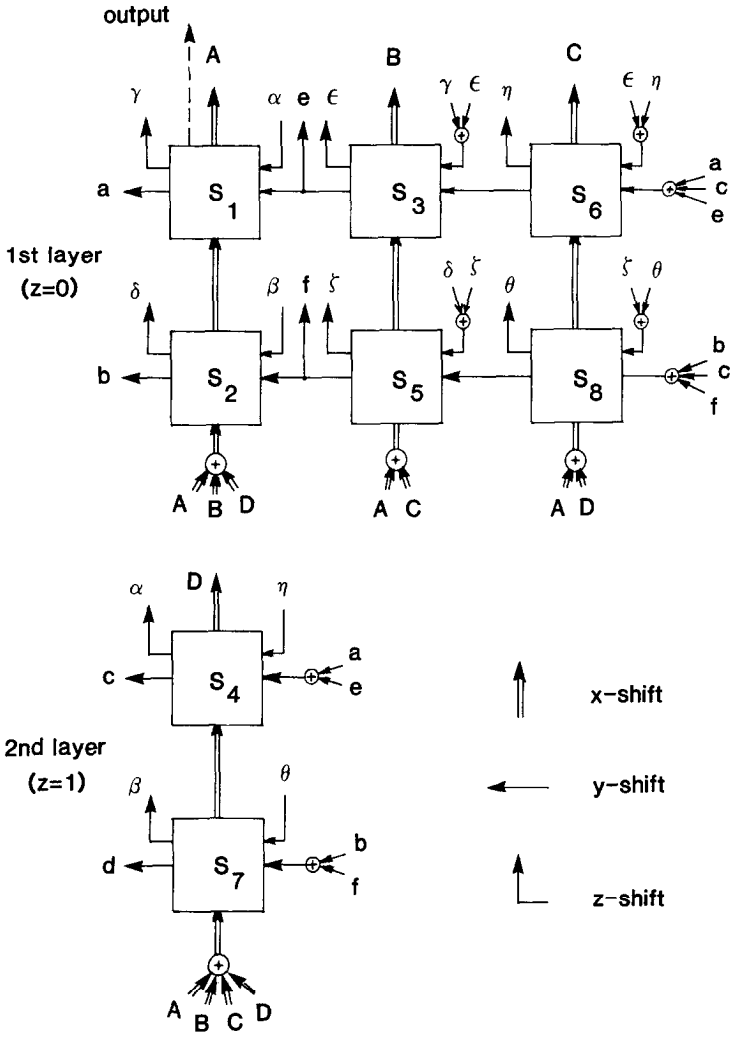

FIG. 14. A 3D linear feedback shift register.

of storage devices $S_1, ..., S_8$ numbered according to the total order $<_T$, where the first and second layers correspond respectively to $z=0$ and 1, and the current contents of the storage devices represent a state. As either of the x-, y- and z-shift clocks advances by one unit of time, the corresponding state transition occurs; i.e., the contents of the storage are updated by feeding the new values through the corresponding connection lines. The state transition matrices determined by F are

$$T_x = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix},$$

$$T_y = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix},$$

$$T_z = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

After i x-shifts, j y-shifts, and k z-shifts, the content of the storage device S_1 takes the value u_{ijk} of the triply periodic array, where the value u_{ijk} is independent from the order of these $(i+j+k)$ times shifts.

7. Concluding Remarks

Our algorithm has computational complexity of order $O(k^2)$ for an nD array which has nD periodicity of size k. In particular, one can apply the algorithm to find a Groebner basis of the ideal defined by a given set of zeros. For an array which neither has any periodicity nor satisfies any LR relation, our algorithm might not have much importance. Our objective is to disclose any significant structure, in particular any LR relations which are incorporated into the given array.

APPENDIX 1: NOTATION

We use the following variables:

i, j, k, l, m	integers
$x, y, p, q, r, s, t, c, a$	n-tuples of nonnegative integers
u, v, w	n-dimensional (nD) arrays over a field K
$f, g, h, f^1, f^2, f*$	n-variate polynomials $\in K[z]$
S, T, C, Γ, Δ	(finite) subsets of Σ_0 (or of Σ)
F, G, F^1	finite subsets of $K[z]$

and the notation:

K	a field
n	dimension (a positive integer)
$I := \{1, 2, ..., n\}$	
$z = (z_1, z_2, ..., z_n)$	n-tuple of independent variables
$K[z] := K[z_1, ..., z_n]$	the n-variate polynomial ring over the field K
Z	the set of integers
Z_0	the set of nonnegative integers
$\Sigma := Z^n$	the set of all n-tuples of integers
$\Sigma_0 := Z_0^n$	the set of all n-tuples of nonnegative integers
$e^i \in \Sigma_0$	the i-th unit vector
$<_T (\leqslant_T)$	the total ordering over Σ_0
$< (\leqslant)$	the partial ordering over Σ_0
$q+1$	the next point of q (w.r.t. $<_T$)
$x_1, x_2, ..., x_n$	the first, second, ..., nth components of $x \in \Sigma_0$
$z^x := z_1^{x_1} z_2^{x_2} \cdots z_n^{x_n}$	power product
u_x, v_y, w_p	values of arrays u, v, w
f_x, g_y, h_p	coefficients of polynomials f, g, h
$\Sigma_s := \{x \in \Sigma_0 \mid s \leqslant x\}$	
$\Sigma_s^p := \{x \in \Sigma_0 \mid s \leqslant x <_T p\}$	
$\Sigma^p := \Sigma_0^p$	
$\Sigma_S := \bigcup_{s \in S} \Sigma_s$	
$\Gamma_c := \{x \in \Sigma_0 \mid x \leqslant c\}$	(sometimes, $\Gamma_c := \{x \in \Sigma \mid x \leqslant c\}$)
$\Gamma_C := \bigcup_{c \in C} \Gamma_c$	
Γ_u	the support of u
Γ_f	the set of points corresponding to the nonzero terms of f
$s_f = \mathrm{Deg}(f)$	degree of f
$\mathrm{Ord}(f)$	order of f
u^p	an array defined over Σ^p

$\mathrm{VALPOL}(u)$	the set of all valid polynomials for u
$I(u)$	the maximum ideal for a perfect array u
$\Delta_e(u)$	the excluded point set of u
$\Delta(u)$	the independent point set of u
$c^{(i)}=(c_j^{(i)})$,	where $c_i^{(i)}=-1$, $c_j^{(i)}=\infty$ $(j\neq i)$
$C_\infty := \{c^{(i)} \mid i\in I\}$	
$s \vdash c$	s is adjoined to c, i.e., there exists $i\in I$ s.t. $i=i(s,c)$
$i=i(s,c)$	$s_i=c_i+1$ and $s_j\leqslant c_j$ $(j\neq i)$
$FF(u^q)$	the class of minimal polynomial sets for u^q
$F\in FF(u^q)$	a minimal polynomial set of u^q
G	a maximal ex-polynomial set of u^q
S	the minimal degree set of u^q
C	the maximal ex-point set of u^q
$C_s := \{c\in C \mid s\vdash c\}$	
$S_c := \{s\in S \mid s\vdash c\}$	
$S\vdash C$	S is adjoined to C
$F^+\in FF(u^{q+1})$	a minimal polynomial set of u^{q+1}
G^+	a maximal ex-polynomial set of u^{q+1}
S^+	the minimal degree set of u^{q+1}
C^+	the maximal ex-point set of u^{q+1}

$s+\Delta(u) := \{s+x \mid x\in\Delta(u)\}$.

APPENDIX 2: PROOFS OF LEMMAS

Proof of Lemma 1. Let f, $g\in\mathrm{VALPOL}(u)$ and $h\in K[z]$. From the linearity of LR relations, it is clear that $f+g\in\mathrm{VALPOL}(u)$. On the other hand, the left-hand side of the LR relation $hf[u]_x=0$ is decomposed into the sum of terms

$$c\sum_{y\in r+\Gamma_f} f_{y-r}u_{y+x-(t+s)} = c\sum_{y\in\Gamma_f} f_y u_{y+x-s+r-t},$$

where $c\in K$, $\mathrm{Deg}(f)=s$, $\mathrm{Deg}(h)=t$, and $r\in\Sigma^{t+1}$. The right-hand expression vanishes for any $x\in\Sigma_{t+s}\subseteq\Sigma_{s-r+t}$. Q.E.D.

Proof of Lemma 2. We may assume that $q>s$, since otherwise Lemma 2 is trivial. Let $t=\mathrm{Deg}(g)\leqslant q-s$ for some $g\in\mathrm{VALPOL}(u^{q+1})$. By the assumption, we have

$$-(1/f_s)\sum_{y\in\Gamma_f\setminus\{s\}} f_y u_{y+x-s} = u_x, \qquad x\in\Sigma_s^q,$$
$$\neq u_q, \qquad x=q, \tag{A1}$$

and

$$-(1/g_t)\sum_{y\in\Gamma_g/\{t\}} g_y u_{y+x-t}=u_x, \qquad x\in\Sigma_t^{q+1}, \tag{A2}$$

from which it follows that

$$\begin{aligned}-(1/f_s)&\sum_{y\in\Gamma_f/\{s\}} f_y u_{y+q-s}\\ &=(1/(f_s g_t))\sum_{y\in\Gamma_f/\{s\}} f_y \sum_{r\in\Gamma_g/\{t\}} g_r u_{r+y+q-s-t},\end{aligned} \tag{A3}$$

since $y+q-s\in\Sigma_t^{q+1}$ for $y\in\Gamma_f/\{s\}$ in view of $t\leqslant q-s$. Upon interchange of the order of summation, the right-hand side of (A3) becomes

$$\begin{aligned}&-(1/g_t)\sum_{r\in\Gamma_g/\{t\}} g_r(-1/f_s)\sum_{y\in\Gamma_f/\{s\}} f_y u_{y+r+q-t-s}\\ &\quad=-(1/g_t)\sum_{r\in\Gamma_g/\{t\}} u_{r+q-t}=u_q,\end{aligned}$$

where the first and second equalities follow from (A1) and (A2), respectively, since $r+q-t\in\Sigma_s^{q+1}$ for $r\in\Gamma_g/\{t\}$. The result contradicts the last inequality of (A1). Q.E.D.

Proof of Lemma 3. Let $x\in\Sigma_0/\Sigma_S$ and $y\in\Sigma_0$ s.t. $x\geqslant y$. Then, $y\in\Sigma_0/\Sigma_S$, since otherwise $x\in\Sigma_S$. Thus, for the set C of all maximal points in Σ_0/Σ_S, we have $\Sigma_0/\Sigma_S=\Gamma_C$, where we allow some infinite points with several coordinates equal to ∞ as maximal points. The converse part can be proved similarly. Q.E.D.

Proof of Lemma 4. For any $x\in\Sigma_0$, there exists either $s\in S$ satisfying $p-x\geqslant s$ or $c\in C$ satisfying $p-x\leqslant c$. Therefore, $\Sigma_0\subseteq\Gamma_{p-S}\cup\Sigma_{p-C}$. Since $\Gamma_{p-S}\cap\Sigma_{p-C}=\varnothing$, $\Sigma_0/\Gamma_{p-S}=\Sigma_{p-C}\cap\Sigma_0$. Q.E.D.

Proof of Lemma 5. Let $f^1, f^2\in F$ s.t. $f^1\neq f^2$. Then, if the S-polynomial Spolynomial (f^1, f^2) is reduced to a nonzero normal form g s.t. $\mathrm{Deg}(g)\in\Delta(F)$, it is easy to see that $g\in\mathrm{VALPOL}(u)$, since u is perfect and g is a linear combination (with polynomial coefficients) of polynomials in F. The result contradicts the minimality of F. Q.E.D.

Proof of Lemma 6. It is easy to see that $\mathrm{Deg}(h)=r$. Furthermore, we have

$$\begin{aligned}\sum_{y\in\Gamma_h} h_y u_{y+x-r}&=\sum_{y\in\Gamma_f} f_y u_{y+x-s}-(d_f/d_g)\sum_{y\in\Gamma_g} g_y u_{y+x-p+q-t}\\ &=0, \qquad x\in\Sigma_r^p,\\ &=d_p-(d_p/d_q)d_q=0, \qquad x=p,\end{aligned}$$

which follows from the inclusion $\Sigma_r^p \subseteq \Sigma_s^p$ and $x-p+q \in \Sigma_t^q$ for $x \in \Sigma_r^p$ in view of

$$x \in \Sigma_r^p \Rightarrow r \leqslant x <_T p \Rightarrow t+p-q \leqslant r \leqslant x <_T p$$
$$\Rightarrow t \leqslant x-(p-q) <_T p-(p-q)=q,$$

where the last inequality is valid, because, for $s, t \in \Sigma_0$ and a $a \in \Sigma := Z^n$ s.t. $s <_T t$, $s+a$, $t+a \in \Sigma_0$, we have $s+a <_T t+a$. Q.E.D.

Proof of Lemma 7. $s^+ \in \Sigma_0/\Gamma_{q-S_N}$ in view of Lemma 2. For any $t \in S$ s.t. $s^+ \leqslant q-t$, we have $t \in S_N$, since $t \leqslant q-s^+ < q-s$, $s \in S_N$. Let $s^+ \in \Gamma_{q-S} \cap (\Sigma_0/\Gamma_{q-S_N})$. Then, $s^+ \leqslant q-t$ for some $t \in S$. But, from $t \in S_N$, it follows that $s^+ \in \Gamma_{q-S_N}$, which is a contradiction. Therefore, $s^+ \in \Sigma_0/\Gamma_{q-S}$. Thus, in view of Lemma 4, there exists $c \in C$ s.t. $s^+ \geqslant q-c$. From $s^+ > s$, it follows that $s^+ \geqslant \max(s, q-c)$. On the other hand, since $\max(s, q-c)$ is minimal in $\Sigma_S \cap (\Sigma_0/\Gamma_{q-S_N})$, we have $s^+ = \max(s, q-c)$, where $s^+ = q-c$ only if $q-c > s$. Q.E.D.

Proof of Lemma 8. (Sufficiency) From $s < q-c$, $I_{s<q-c} \neq \emptyset$ and $q-c \in \Sigma_S/S$. In view of $q-c \in \Sigma_0/\Gamma_{q-S} \subseteq \Sigma_0/\Gamma_{q-S_N}$, we have $q-c \in \Sigma_{S^+}/S$. First, let $i \in I_{s<q-c}$. Then, there exists $t \in S_c$ s.t. $i=i(t, c)$, $t \leqslant q-s$. Thus, $t \in S_N$. On the other hand, $q_i-c_i-e_i^i = q_i-t_i$, and $q_j-c_j \leqslant q_j-t_j$, $j \neq i$. Therefore, $q-c-e^i \leqslant q-t$. Thus, $q-c-e^i \in \Gamma_{q-S_N}$. Second, let $i \in I_{s=q-c}$. Then, there exists either $a \in C_s$ s.t. $i=i(s, a)$, $q-c-e^i \leqslant a$ or $t \in S_c \cap S_N$ s.t. $i=i(t, c)$, $t \leqslant q-s+e^i$. In the first case, $q-c-e^i \in \Gamma_C$, and, in the second case, we have $q-c-e^i \leqslant q-t$. Thus, $q-c-e^i \in \Gamma_{q-S_N}$. Consequently, $q-c$ is minimal in Σ_{S^+}/S.

(Necessity) Trivially, $q-c > s$ for some $s \in S_N$. We have the following two cases:

(1) For $i \in I_{s<q-c}$, let $q-c-e^i \in \Gamma_C \cup \Gamma_{q-S_N}$. First, let $s \leqslant q-c-e^i \in \Gamma_C$. Then, for some $a \in C$, $s \leqslant a$, which is impossible. Consequently, we have $q-c-e^i \in \Gamma_{q-S_N}$. Thus, $s \leqslant q-c-e^i \leqslant q-t$ for some $t \in S_N$. From $t \leqslant c+e^i$, it follows that $i=i(t, c)$ and $t \in S_c$. Therefore, $i \in I_{c;q-s}$.

(2) For $i \in I_{s=q-c}$, let $q-c-e^i \in \Gamma_C \cup \Gamma_{q-S_N}$. First, let $q-c-e^i \in \Gamma_C$. Then, for some $a \in C$, $s-e^i \leqslant a$, from which it follows that $a \in C_s$, $i=i(s, a)$. Consequently, $i \in I_{s;q-c-e}$. Second, let $q-c-e^i \in \Gamma_{q-S_N}$. Then, $q-c-e^i \leqslant q-t$ for some $t \in S_N$. From $t \leqslant c+e^i$, it follows that $i=i(t, c)$ and $t \in S_c$. Therefore, $i \in I_{c;q-s+e}$. Q.E.D.

Proof of Lemma 9. (Sufficiency) We have only to consider the following three cases:

(1) For $i \in I_{s>q-c}$, there exists $a \in C_s$ s.t. $i=i(s, a)$ and $q-c \leqslant a$.

(2) For $i \in I_{s<q-c}$, there exists $t \in S_c$ s.t. $i=i(t, c)$ and $s \leqslant q-t$.

(3) For $i \in I_{s=q-c}$, either there exists $a \in C_s$ s.t. $i = i(s, a)$ and $q - c - e^i \leqslant a$ or there exists $t \in S_c \cap S_N$ s.t. $i = i(t, c)$ and $s - e^i \leqslant q - t$.

In the first case, we have $q_j - c_j - e^i_j \leqslant a_j$, $j \neq i = i(s, a)$ and $q_i - c_i - 1 < s_i - 1 = a_i$; $s_j - e^i_j \leqslant a_j$ for any $j \in I$. Thus, $r - e^i \leqslant a$. Therefore, $r - e^i \notin \Sigma_{S^+}$. In the second case, we have $q - c - e^i \leqslant q - t$, since $q_i - c_i - e^i_i = q_i - t_i$ and $q_j - c_j \leqslant q_j - t_j$, $j \neq i$. Thus, $r - e^i \leqslant q - t$. Therefore, $r - e^i \notin \Sigma_{S^+}$. In the third case, the above relations hold similarly.

(Necessity) From $r \neq s$, $q - c$, we have $I_{s>q-c} \neq \varnothing$, $I_{s<q-c} \neq \varnothing$. Trivially, $s \in S_N$. Now we consider the following three cases:

(1) For $i \in I_{s>q-c}$, $r - e^i \in \Gamma_C \cup \Gamma_{q-S_N}$, since r is minimal in Σ_{S^+}/S. First, let $r - e^i \leqslant q - t$ for some $t \in S_N$. Then, we have $q - c \leqslant q - t$ and so $t \leqslant c$, which is impossible. Consequently, $r - e^i \leqslant a$ for some $a \in C$. Then, in view of $q - c \leqslant r - e^i \leqslant a$, we have $q - c \leqslant a$. On the other hand, we have $s_i - 1 \leqslant a_i$ and $s_j \leqslant a_j$, $j \neq i$, from which it follows that $a \in C_s$ and $i = i(s, a)$.

(2) For $i \in I_{s<q-c}$, $r - e^i \in \Gamma_C \cup \Gamma_{q-S_N}$. First, let $r - e^i \in \Gamma_C$. Then, for some $a \in C$, $s \leqslant a$, which is impossible. Consequently, we have $r - e^i \in \Gamma_{q-S_N}$. Thus, $s \leqslant r - e^i \leqslant q - t$ for some $t \in S_N$. On the other hand, since $q - c \leqslant r \leqslant q - t + e^i$, $t \leqslant c + e^i$. Therefore, $t_i \leqslant c_i + 1$ and $t_j \leqslant c_j$, $j \neq i$, from which it follows that $t_i = c_i + 1$, $t \in S_c$, and $i = i(t, c)$.

(3) For $i \in I_{s=q-c}$, $r - e^i \in \Gamma_C \cup \Gamma_{q-S_N}$. First, let $r - e^i \in \Gamma_C$. Then, $s - e^i \leqslant a$ for some $a \in C$, from which it follows that $a \in C_s$, $i = i(s, a)$. Second, let $r - e^i \in \Gamma_{q-S_N}$. Then, $q - c - e^i \leqslant q - t$ for some $t \in S_N$. From $t \leqslant c + e^i$, it follows that $t_i = c_i + 1$, $t \in S_c$, and $i = i(t, c)$. Q.E.D.

APPENDIX 3: PROOF OF THEOREM 4

Let $S = \{\mathrm{Deg}(f) \mid f \in F\}$ and $\Delta = \Delta(u^p)$. Assume that there exists a monic polynomial $f^1 \in \mathrm{VALPOL}(u^p)$ s.t. $f^1 \neq f \in F$, $\Gamma_{f^1} \subseteq \Delta^*[s]$ and $\mathrm{Deg}(f^1) = \mathrm{Deg}(f) = s$. Let $q \in \Sigma^p$ be the point where $\Delta_q := \Delta(u^q) \subset \Delta_{q+1} := \Delta(u^{q+1}) = \Delta$. From the assumption, we have a nonzero polynomial $h := f^1 - f$, which has $t := \mathrm{Deg}(h) \in \Delta$ and $r := \mathrm{Ord}(h) <_T p$. Since, for $s \leqslant x <_T p$,

$$h[u]_{x-s+t} = \sum_{y \in \Gamma_h} u_{y+x-s+t} \cdot t$$

$$= \sum_{y \in \Gamma_{f^1}} f^1_y u_{y+x-s} - \sum_{y \in \Gamma_f} f_y u_{y+x-s} = 0,$$

we have $p - s + t \leqslant_T r$. Thus, $p - s \leqslant_T r - t$. Therefore, there exists $f^* \in F$ with $\mathrm{Deg}(f^*) = a \in S$ s.t. $a < r - t$. Now, we have the two cases:

(1) In case of $r \leqslant_T q$, $f^* \in \mathrm{VALPOL}(u^{q+1}) \subseteq \mathrm{VALPOL}(u^{r+1})$. But, in view of Lemma 2, there exists no $h \in \mathrm{VALPOL}(u^{r+1})$ s.t. $\mathrm{Deg}(h) \leqslant r - t$.

(2) In case of $q <_T r (<_T p)$, the polynomial h with $\mathrm{Deg}(h) = t \in \Delta(u^p)$ has order between q and p, which, by the definition of q, contradicts the fact that each element of any minimal polynomial set having order between q and p must have degree equal to some $s \in S$.

Q.E.D.

ACKNOWLEDGMENTS

The author wishes to express his sincere gratitude to Professor Bruno Buchberger of Johannes Kepler University of Linz, Austria, for kind support and encouragement during his stay for this research at the Research Institute of Symbolic Computation (RISC) in June/July 1987.

RECEIVED March 30, 1988; FINAL MANUSCRIPT RECEIVED February 27, 1989

REFERENCES

BERLEKAMP, E. R. (1968), Binary BCH codes for correcting multiple errors; The Gorenstein–Zierler generalized nonbinary BCH codes for the Hamming metric, *in* "Algebraic Coding Theory", Chapts. 7, 10, pp. 176–199, 218–240, McGraw–Hill, New York.

BOSE, N. K. (1985a), Trends in multidimensional systems theory, *in* "Multidimensional Systems Theory" (N. K. Bose, Ed.), Chapt. 1, pp. 1–40, Reidel, Dordrecht.

BOSE, N. K. (1985b), Multivariate rational approximations of the Pade-type in systems theory, *in* "Multidimensional Systems Theory" (N. K. Bose, Ed.), Chap. 2, pp. 41–51, Reidel, Dordrecht.

BUCHBERGER, B. (1970), An algorithmic criterion for the solvability of algebraic systems of equations, *Aequationes Math.* **4**, No. 3, 374–383. [in German]

BUCHBERGER, B. (1985), Groebner bases: An algorithmic method in polynomial ideal theory, *in* "Multidimensional Systems Theory" (N. K. Bose, Ed.), Chap. 6, pp. 184–232, Reidel, Dordrecht.

CHAPARRO, L. F., AND JURY, E. I. (1982), Rational approximation of $2-D$ linear discrete systems, *IEEE Trans. Acoust. Speech Signal Process.* **ASSP-30**, No. 5, 780–787.

HOMER, S., AND GOLDMANN, J. (1985), Doubly-periodic sequences and two-dimensional recurrences, *SIAM J. Algebraic Discrete Methods* **6**, No. 3, 360–370.

IKAI, T., KOSAKO, H., AND KOJIMA, Y. (1976), Basic theory of two-dimensional cyclic codes—Periods of ideals and fundamental theorems, *IECE Trans.* **59-A**, No. 3, 216–223. [in Japanese]

IMAI, H. (1976), A theory of two-dimensional cyclic codes and two-dimensional linear shift registers, *IECE Trans.* **59-A**, No. 9, 710–717. [in Japanese]

IMAI, H. (1977), A theory of two-dimensional cyclic codes, *Inform. and Control* **34**, 1–21.

JUSTICE, J. H. (1977), A Levinson-type algorithm for two-dimensional Wiener filtering using bivariate Szegoe polynomials, *Proc. IEEE* **65**, No. 6, 882–886.

MACWILLIAMS, F. J. (1970), Binary codes which are ideals in the group of an Abelian group, *Bell. Systems Tech. J.* **49**, No. 6, 987–1011.

MACWILLIAMS, F. J., AND SLOANE, N. J. A. (1976), Pseude-random sequences and arrays, *Proc. IEEE* **64**, No. 12, 1715–1729.

MARZETTA, T. L. (1980), Two-dimensional linear prediction: Autocorrelation arrays, minimum-phase prediction error filters, and reflection coefficient arrays, *IEEE Trans. Acoust. Speech Signal Process.* **ASSP-28**, No. 6, 725–733.

MASSEY, J. L. (1969), Shift-register synthesis and BCH decoding, *IEEE Trans. Inform. Theory* **IT-15**, No. 1, 122–127.

PRABHU, K. A., AND BOSE, N. K. (1982), Impulse response arrays of discrete-space systems over a finite field, *IEEE Trans. Acoust. Speech Signal Process.* **ASSP-30**, No. 1, 10–18.

SAKATA, S. (1978), General theory of doubly periodic arrays over an arbitrary finite field and its applications," *IEEE Trans. Inform. Theory* **IT-24**, No. 6, 719–730.

SAKATA, S. (1981), On determining the independent point set for doubly periodic arrays and encoding two-dimensional cyclic codes and their duals, *IEEE Trans. Inform. Theory* **IT-27**, No. 5, 556–565.

SAKATA, S. (1988), Finding a minimal set of linear recurring relations capable of generating a given finite two-dimensional array, *J. Symbolic Comput.* **5**, 321–337.

SAKATA, S. (1989), Synthesis of two-dimensional linear feedback shift registers, *in* "Applied Algebra, Algebraic Algorithms and Error-Correcting Codes: Proceedings, AAECC-5, Menorca, 1987" (L. Huguet and A. Poli, Eds.), pp. 394–407, Springer, Berlin.