J. Symbolic Computation (1988) **5**, 321–337

Finding a Minimal Set of Linear Recurring Relations Capable of Generating a Given Finite Two-dimensional Array

SHOJIRO SAKATA

Toyohashi University of Technology, Dept of Production Systems Engineering, Tempaku-cho, Toyohashi 440, *Japan*

(*Received* 20 *May* 1986)

We present an algorithm for finding a minimal set of two-dimensional linear recurring relations capable of generating a prescribed finite two-dimensional array. This is a two-dimensional extension of the Berlekamp–Massey algorithm for synthesizing a shortest linear feedback shift-register capable of generating a given finite sequence. The complexity of computation for an array of size n is $O(n^2)$ under some reasonable assumptions. Furthermore, we make clear some relationship between our algorithm and Gröbner bases of bivariate polynomial ideals, where polynomials correspond one-to-one to linear recurring relations.

1. Introduction

In previous papers (Sakata, 1978, 1981), we have considered how to find a Gröbner basis of the maximum ideal for a given (finite set of) doubly periodic array(s) and proposed a simple algorithm based on Gaussian elimination for a system of linear equations. From an engineering point of view, this is the problem of synthesising a simplest two-dimensional linear feedback shift-register (Imai, 1977), which is an extension of shortest feedback shift-register synthesis into two dimensions.

The complexity of our previous algorithm is $O(p^3)$, where p is the (least common multiple of) period(s) of a given doubly periodic array(s). We should try to design some algorithm having complexity $O(p^2)$ because the corresponding one-dimensional problem can be solved by the well-known Berlekamp–Massey algorithm (Berlekamp, 1968; Massey, 1969) having complexity $O(p^2)$, where p is the period (or length) of a given sequence (one-dimensional array).

In the previous works, we have made clear that there exist several difficulties for two-dimensional linear recurring arrays which are not encountered in treating one-dimensional cases. Thus, our goal is to connect our synthesis problem with the notion of Gröbner basis in the constructive theory of multivariable polynomial ideals (Buchberger, 1970, 1985) and to devise a two-dimensional extension of the Berlekamp algorithm.

The contents of the paper is as follows: In section 2, some preliminary notations and concepts for two-dimensional linear recurring arrays are introduced and, in addition, a simple lemma which connects our problem with polynomial ideal theory is described. In section 3 some further definitions and lemmas on which our problem is based are described. Sections 4 and 5 provide our main results, i.e. some fundamental lemmas, theorems and the synthesis algorithm whose correctness is assured by these theorems. A

0747–7171/88/030321 + 17 $03.00/0

complexity estimate of the algorithm is given. In section 6, some relationship with Gröbner bases is discussed. The concluding remarks are in section 7.

2. Preliminaries

We use the following notation:

K	a field
x	a pair (x_1, x_2) of variables
$K[x]$	the ring $K[x_1, x_2]$ of bivariate polynomials over K.

The following variables will be used:

f, g, h	polynomials in $K[x]$
F, G, H	finite subsets of $K[x]$
i, j, k, l	integers
m, n, p, q, r, s, t	pairs of non-negative integers
u, v, w	two-dimensional arrays over K
f_m, g_n, h_r	coefficients of polynomials f, g, h
u_m, v_n, w_r	components of arrays u, v, w
$f^{(i)}, g^{(j)}, h^{(k)}$	numbered polynomials in F, G, H
m_1 and m_2	the first and second components of m
u^p	the p-truncate of a two-dimensional array u
Ideal(F)	the ideal generated by the polynomials in F

Let Σ_0 be the set of all ordered pairs $m = (m_1, m_2)$ of non-negative integers m_1 and m_2, where each element m of Σ_0 is called a point. We consider both the partial ordering $<$ and the graduated total degree ordering $<_T$ over Σ_0, where $<$ is defined as usual by

$$m = (m_1, m_2) < n = (n_1, n_2) \text{ if and only if } (m_1 \leqq n_1) \wedge (m_2 \leqq n_2) \wedge (m \neq n),$$

and

$$0 := (0, 0) <_T (1, 0) <_T (0, 1) <_T (2, 0) <_T (1, 1) <_T (0, 2) <_T (3, 0) <_T \ldots,$$

respectively. We write $m \leqq_T$ (resp. $\leqq$) n if and only if $m <_T$ (resp. $<$) n or $m = n$. By the total degree ordering $<_T$, we have the one-to-one correspondence $|\ | : \Sigma_0 \to Z_+$ (:= the set of non-negative integers), $|q| = (1/2)[(q_1 + q_2)^2 + q_1 + 3q_2]$. Thus, $|(0, 0)| = 0$, $|(1, 0)| = 1$, $|(2, 1)| = 7$, etc. Furthermore, for $n \in \Sigma_0$, let

$$\begin{aligned} n+1 &:= (n_1 - 1, n_2 + 1) \text{ if } n_1 > 0; \\ &:= (n_2 + 1, 0) \text{ if } n_1 = 0. \end{aligned}$$

For $m, n \in \Sigma_0$, the usual vector sum and difference are denoted by $m+n$ and $m-n$ (provided that $m \geqq n$), respectively. For $t, p \in \Sigma_0$, let

$$\begin{aligned} \Sigma_t &:= \{m \in \Sigma_0 \mid t \leqq m\}, \\ \Sigma_t^p &:= \{m \in \Sigma_0 \mid (t \leqq m) \wedge (m <_T p)\}. \end{aligned}$$

In particular,

$$\Sigma_0^p := \{m \in \Sigma_0 \mid m <_T p\}.$$

For $q \in \Sigma_0$, a finite two-dimensional (2D) array $u = (u_n)$ of size $|q|$ over a field K is a mapping from Σ_0^q into K, where $u_n \in K$ is called the nth component of u. Similarly, an infinite 2D array $u = (u_n)$ over K is a mapping from Σ_0 into K. For a 2D array u and $p \in \Sigma_0$, $u^p = (u_m \mid m \in \Sigma_0^p)$ is called p-truncate of u.

Let

$$f := \sum_{m\in\Gamma_f} f_m x^m$$

be an element of $K[x] := K[x_1, x_2]$, where

$$x^m := x_1^{m_1} x_2^{m_2} \quad \text{and} \quad \Gamma_f := \{m \in \Sigma_0 \mid f_m \neq 0\}.$$

$\mathrm{LP}(f) := \max\{m \mid m \in \Gamma_f\}$ is called the leading power product exponent of f, where the max(imum) is taken w.r.t. $<_T$. Corresponding to a polynomial

$$f = \sum_{m\in\Gamma_f} f_m x^m \in K[x]$$

with $\mathrm{LP}(f) = s$, a linear recurring (LR) relation at a point $n \in \Sigma_0$ for a (finite or infinite) 2D array u is as follows:

$$\sum_{m\in\Gamma_f} f_m u_{m+n-s} = 0, \tag{1}$$

which is simply written as

$$f[u]_n = 0.$$

The polynomial f (or the LR relation corresponding to f) is said to be valid for u at $n \in \Sigma_0$ if and only if

$$f[u]_n = 0.$$

For a finite 2D array $u = u^p$, f is said to generate u if and only if either f is valid at any point $n \in \Sigma_s^p$ for u (see Fig. 1) or $p \leqq_T s$. For an infinite array u, f is said to generate u if and only if f is valid at any point $n \in \Sigma_s$ for u. For a finite or infinite array u, we write

$$f[u] = 0$$

if and only if f generates u. f is said to generate u "up to p" if and only if

$$f[u^p] = 0.$$

EXAMPLE 1. Let $K = \mathrm{GF}(2) = \{0, 1\}$ be the Galois field of two elements 0 and 1. A finite 2D array u of size 16 is shown in Fig. 2. For $f = x_1^2 x_2 + x_1 + 1$, $f[u]_{(2,1)} = 0$ but $f[u]_{(3,1)} \neq 0$.

For a (finite or infinite) array u, let

$$\mathrm{VALPOL}(u) := \{f \in K[x] \mid f[u] = 0\}.$$

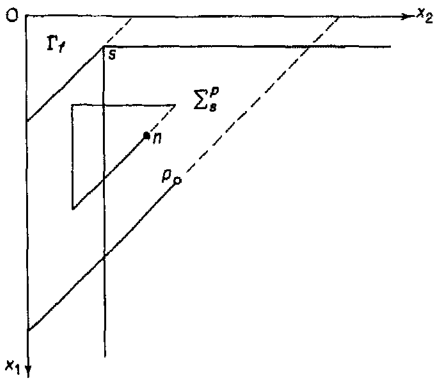


Fig. 1. LR relation.

$n_1 \backslash n_2$	0	1	2	3	4	5
0	0	1	0	1	0	
1	1	1	0	0		
2	0	1	0			
3	0	0				
4	0	*				
5	1					

Fig. 2. A finite 2D array.

Then we have the following lemma which is proved in Appendix 1.

Lemma 1. *For any infinite array u,* VALPOL(u) *is an ideal in* $K[x]$.

The ideal mentioned in Lemma 1 is called the maximum ideal of u and is denoted by I(u).

An infinite 2D array u is said to be doubly periodic (DP) if and only if $u = (u_n)$ satisfies the following LR relations for a certain pair of positive integers $p = (p_1, p_2)$

$$u_{n_1, n_2} = u_{n_1 + p_1, n_2} = u_{n_1, n_2 + p_2}, \quad n \in \Sigma_0.$$

We remark that a DP array is composed of infinite translational repetitions of a fundamental period parallelogram (FPP) which is a minimal unit of its DP structure. The size of an FPP is called "period" of the DP array (Sakata, 1978).

Example 2. An example of a DP array over $K = \mathrm{GF}(2)$ having period 12 is shown together with its FPP in Fig. 3.

For a DP array u, I(u) is always a zero-dimensional ideal in $K[x]$, which has been already made clear in the previous paper (Sakata, 1978).

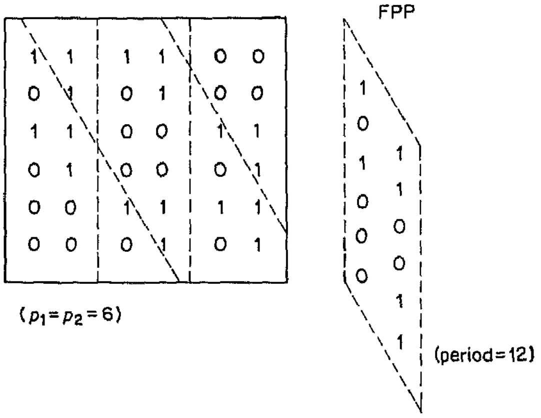


Fig. 3. A DP array.

3. Minimal Set of Polynomials and Excluded Points Set

The study of Gröbner bases in $K[x]$ leads to the following definitions. Let $s^{(1)}, \ldots, s^{(l)} \in \Sigma_0$ satisfy the condition:

$$s_1^{(1)} > s_1^{(2)} > \ldots > s_1^{(l)} = 0, \qquad 0 = s_2^{(1)} < s_2^{(2)} < \ldots < s_2^{(l)}. \tag{2}$$

Then we have a finite subset of Σ_0

$$\Delta = \bigcup_{k=1}^{l-1} \Delta_k, \tag{3}$$

where

$$\Delta_k := \{m \in \Sigma_0 \mid m \leqq (s_1^{(k)} - 1, s_2^{(k+1)} - 1)\}, \quad 1 \leqq k \leqq l-1.$$

A finite subset of Σ_0 of the form (3) is called "delta set", and the points $s^{(1)}, \ldots, s^{(l)}$ are called the "defining points of Δ" (see Fig. 4).

Next, let $\mathbb{F}$ be the class of all finite subsets $F = \{f^{(1)}, \ldots, f^{(l)}\}$ of polynomials with $\mathrm{LP}(f^{(k)}) = s^{(k)}$, $1 \leqq k \leqq l$, s.t. the above condition (2) is satisfied. For $F = \{f^{(1)}, \ldots, f^{(l)}\} \in \mathbb{F}$, the delta set defined by $s^{(k)} = \mathrm{LP}(f^{(k)})$, $1 \leqq k \leqq l$, is called "delta set of F" and denoted by $\Delta(F)$; F is said to be "of delta type". (Note that the polynomials $f^{(1)}, \ldots, f^{(l)}$ in any $F \in \mathbb{F}$ are numbered s.t. (2) is satisfied.)

Now we remark that any reduced Gröbner basis F of a zero-dimensional ideal in $K[x]$ is of delta type (Sakata, 1978). Thus we are led to introduce the following definition:

Definition 1. $F = \{f^{(1)}, \ldots, f^{(l)}\}$ is a minimal set of polynomials (or LR relations) for a 2D array $u = u^q$ if and only if

(1) $F \subseteq \mathrm{VALPOL}(u)$;
(2) $F \in \mathbb{F}$, i.e. we have a delta set $\Delta(F)$;
(3) $\neg(\exists g)((g \in \mathrm{VALPOL}(u)) \wedge (\mathrm{LP}(g) \in \Delta(F)))$.

Let $\mathbb{F}(u)$ be the class of all minimal sets of monic polynomials for u, where we remark that $\Delta(F)$ is unique for u by (3) of the above definition; $\Delta(F)$ is denoted also by $\Delta(u)$. On the other hand, $F \in \mathbb{F}(u^q)$ is not necessarily unique for u^q. Obviously we have the following lemmas by the definitions of $\mathrm{VALPOL}(u)$ and $\mathbb{F}(u)$.

Lemma 2. $\mathbb{F}(u^q) \neq \phi$.

Lemma 3. *If* $p \leqq_T q$ *and* $u^p = (u^q)^p$, *then* $\Delta(u^p) \subseteq \Delta(u^q)$.

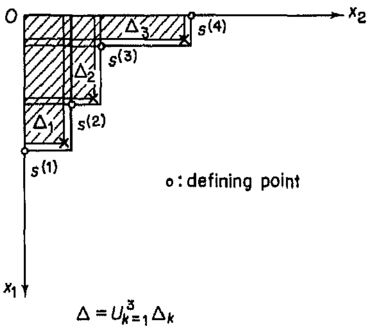


Fig. 4. A delta set ($l = 4$).

We can obtain $\Delta(u^q)$ and $F \in \mathbb{F}(u^q)$ by checking $u^n = (u^q)^n$ successively w.r.t. $n \in \Sigma_0^q$, i.e. by solving each system of linear equations w.r.t. the unknown coefficients of $f \in F$ which is derived from the LR relations (1) at all points $n \in \Sigma_0^q$. This brute force method is, however, quite inefficient because we must perform many useless computations during the process. In the following, we will consider how to eliminate such wasteful computations by extending the idea of Berlekamp and Massey to our 2D case.

First, we begin with two key lemmas (the proofs are given in Appendices 2 and 3, respectively).

LEMMA 4. *Let* $f, h \in K[x]$, $\mathrm{LP}(f) = s$, $\mathrm{LP}(h) = t$. *If* $f \in \mathrm{VALPOL}(u^p)$ *but* $f[u]_p \neq 0$ *and* $h \in \mathrm{VALPOL}(u^{p+1})$, *then*

$$(t_1 \geqq p_1 - s_1 + 1) \vee (t_2 \geqq p_2 - s_2 + 1). \tag{4}$$

LEMMA 5. *Let* $p <_T q$ *and* $g, f \in K[x]$ *with* $\mathrm{LP}(g) = t$, $\mathrm{LP}(f) = s$. *If* $g \in \mathrm{VALPOL}(u^p)$ *but* $g[u]_p \neq 0$, *and* $f \in \mathrm{VALPOL}(u^q)$ *but* $f[u]_q \neq 0$, *i.e.*

$$\sum_{m \in \Gamma_g} g_m u_{m+n-t} \begin{cases} = 0, & \text{if } n \in \Sigma_t^p, \\ = d_p (\neq 0), & \text{if } n = p, \end{cases} \tag{5}$$

$$\sum_{m \in \Gamma_f} f_m u_{m+n-s} \begin{cases} = 0, & \text{if } n \in \Sigma_s^q, \\ = d_q (\neq 0), & \text{if } n = q, \end{cases} \tag{6}$$

then

$$h := x^{r-s} f - (d_q/d_p) x^{r-q+p-t} g \in \mathrm{VALPOL}(u^{q+1}), \tag{7}$$

where $r = (r_1, r_2)$ *is defined by*

$$r_1 := \max\{s_1, t_1 + q_1 - p_1\}, \qquad r_2 := \max\{s_2, t_2 + q_2 - p_2\}. \tag{8}$$

($t_1 + q_1 - p_1$ *and/or* $t_2 + q_2 - p_2$ *can be negative.)*

The polynomial h defined by (7) is written as $h = h(f, q, s; g, p, t)$ (see Fig. 5, which

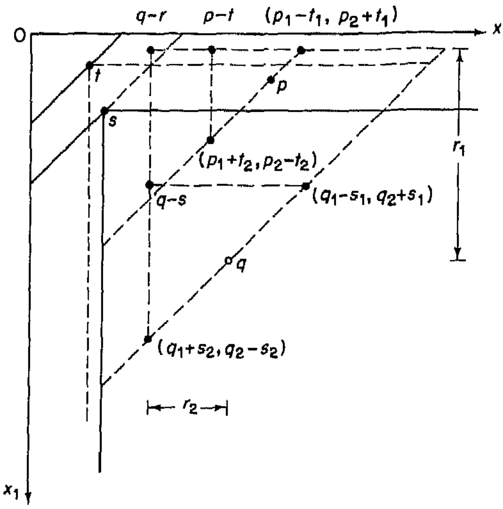


Fig. 5. Construction of a new polynomial.

illustrates the case of $r_1 = t_1 + q_1 - p_1 > s_1$ and $r_2 = s_2 > t_2 + q_2 - p_2$). The value d_p (resp. d_q) is called the discrepancy of g (resp. f) at p (resp. q).

Lemma 4 suggests introduction of the following delta set

$$\Delta_e(u^p) := \bigcup_{q,s \in \Sigma_0^p} \Delta_{qs}, \tag{9}$$

where

$$\Delta_{qs} := \{m \mid m \leqq q - s\}, \text{ if } \exists f \in \mathrm{VALPOL}(u^q) \text{ s.t. } f[u]_q \neq 0, \ \mathrm{LP}(f) = s;$$
$$:= \phi, \text{ otherwise.}$$

$\Delta_e(u^p)$ is called the delta set of excluded points for u^p. Obviously, $\Delta(u^p) \supseteq \Delta_e(u^p)$. Is it true that, for all u and p,

$$\Delta(u^p) = \Delta_e(u^p)?$$

We will prove this identity by an inductive reasoning, which will be completed at the end of the next chapter.

Now, assuming that $\Delta(u^n) = \Delta_e(u^n)$ at all points $n \leqq_T p$, we have the following two sets of polynomials:

$$F = \{f^{(k)} \mid 1 \leqq k \leqq l\} \in \mathbb{F}(u^p), \tag{10}$$

$$G = \{g^{(k)} \mid 1 \leqq k \leqq l-1\}, \tag{11}$$

s.t., for certain points $p^{(k)} <_T p$, $1 \leqq k \leqq l-1$, $g^{(k)} \in \mathrm{VALPOL}(u^{p^{(k)}})$, but $g^{(k)}[u]p^{(k)} \neq 0$,

$$s_1^{(k)} = p_1^{(k)} - t_1^{(k)} + 1, \qquad s_2^{(k+1)} = p_2^{(k)} - t_2^{(k)} + 1, \quad 1 \leqq k \leqq l-1, \tag{12}$$

where $s^{(k)} := \mathrm{LP}(f^{(k)})$ for $1 \leqq k \leqq l$ and $t^{(k)} := \mathrm{LP}(g^{(k)})$ for $1 \leqq k \leqq l-1$.

$$\Delta(u^p) = \bigcup_{k=1}^{l-1} \Delta p^{(k)} t^{(k)}. \tag{13}$$

G is said to be an auxiliary set of polynomials associated with a minimal set F of polynomials for u^p. From Lemma 5 we have immediately the following lemma.

LEMMA 6. *If* $\exists f^{(i)} \in F, f^{(i)}[u]_p \neq 0$, *then, for* $1 \leqq j \leqq l-1$,

$$h := h(f^{(i)}, p, s^{(i)}; g^{(j)}, p^{(j)}, t^{(j)}) \in \mathrm{VALPOL}(u^{p+1}), \tag{14}$$

and $\mathrm{LP}(h) = r = (r_1, r_2)$, *where*

$$r_1 := \max\{s_1^{(i)}, p_1 - s_1^{(j)} + 1\}, \qquad r_2 := \max\{s_2^{(i)}, p_2 - s_2^{(j+1)} + 1\}.$$

The construction of $h(f^{(i)}, p, s^{(i)}; g^{(j)}, p^{(j)}, t^{(j)})$ described in Lemma 6 is called "Berlekamp procedure of type $\langle i, j \rangle$".

The following lemma is an easy consequence of Lemma 4.

LEMMA 7. *If* $s^{(k)}$, $1 \leqq k \leqq l$, *are the defining points of* $\Delta(u^p)$ $(= \Delta_e(u^p))$, *any defining point of* $\Delta_e(u^{p+1})$ *is either of the following types:*

(1) $(s_1^{(i)}, s_2^{(i)})$;
(2) $(p_1 - s_1^{(i)} + 1, p_2 - s_2^{(j)} + 1)$;
(3*a*) $(p_1 - s_1^{(i)} + 1, s_2^{(j)})$;
(3*b*) $(s_1^{(i)}, p_2 - s_2^{(j)} + 1)$.

4. Main Results

Now, under the above assumption that we have such a pair (F, G) as in (10), (11), the following set of points is defined (see Fig. 6):

$$s^{(i)}+\Delta(u^p):=\{s^{(i)}+n \mid n\in\Delta(u^p)\}.$$

If $p\in s^{(i)}+\Delta(u^p)$, then ${}^{\exists}j$, $1\leqq j\leqq l-1$, s.t.

$$(s_1^{(i)}+s_1^{(j)}>p_1)\wedge(s_2^{(i)}+s_2^{(j+1)}>p_2).$$

Thus, the polynomial $h=h(f^{(i)}, p, s^{(i)}; g^{(j)}, p^{(j)}, t^{(j)})$ constructed by the Berlekamp procedure of type $\langle i,j\rangle$ has the leading power product exponent $\mathrm{LP}(h)=s^{(i)}=\mathrm{LP}(f^{(i)})$. For this reason $s^{(i)}+\Delta(u^p)$ is called the set of degree-invariant points for $f^{(i)}$. From this consideration, we have the following theorem, by which we can treat the easy case as follows.

THEOREM 1. *If $p\in s^{(i)}+\Delta(u^p)$, then there exists a polynomial h s.t.*

$$(h\in\mathrm{VALPOL}(u^{p+1}))\wedge(\mathrm{LP}(h)=s^{(i)}).$$

Next, we must treat the difficult case that $p\notin s^{(i)}+\Delta(u^p)$, where, for any j, $1\leqq j\leqq l-1$, $h:=h(f^{(i)}, p, s^{(i)}; g^{(j)}, p^{(j)}, t^{(j)})$ has $\mathrm{LP}(h)\neq\mathrm{LP}(f^{(i)})$. Again, under the same assumptions as above, let $F_V:=F\cap\mathrm{VALPOL}(u^{p+1})$, and $F_N:=F/F_V$. Then, if there exists at least one $f^{(i)}$ in F_N s.t. $p\notin s^{(i)}+\Delta(u^p)$, F_N and $\Delta(u^p)$ $(=\Delta_e(u^p))$ define a new set of excluded points $\Delta_e(u^{p+1})$ s.t. $\Delta(u^p)\subset\Delta_e(u^{p+1})$. We must give an answer to the following question:

$$\Delta(u^{p+1})=\Delta_e(u^{p+1})?$$

In other words, is it possible to determine for every defining point t of $\Delta_e(u^{p+1})$ a new polynomial h with $\mathrm{LP}(h)=t$ s.t. $h\in\mathrm{VALPOL}(u^{p+1})$?

Before giving the answer, we must inquire on what condition a defining point of each type (1), (2), (3a) and (3b) in Lemma 7 occurs. The following observation is immediately obtained:

A defining point t of $\Delta_e(u^{p+1})$

(1) of type (1) occurs only if

$$(f^{(i)}\in F_V)\vee(p\in s^{(i)}+\Delta(u^p));$$

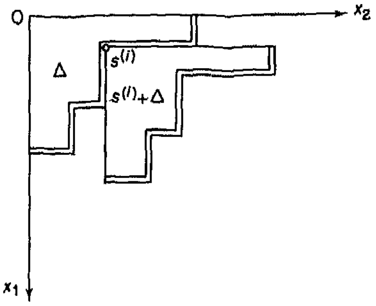


Fig. 6. A degree-invariant region.

(2) of type (2) occurs only if

$$(f^{(i)}, f^{(j)} \in F_N) \wedge (i < j, \text{ i.e. } (s_1^{(i)} > s_1^{(j)}) \wedge (s_2^{(i)} < s_2^{(j)}));$$

(3) of type (3a) and (3b) occurs only if

$$(f^{(i)}, f^{(j)} \in F_N) \wedge (p \geqq s^{(i)} + s^{(j)}).$$

(In the third case, it is also possible that $i = j$.)

More precisely, we have the following two lemmas which are crucial in solving our problem. (The proofs are given in Appendices 4 and 5, respectively.)

LEMMA 8. *A defining point t of type* (2) (*of* $\Delta_e(u^{p+1})$) *occurs only if* $j = i + 1$.

LEMMA 9. *A defining point t of type* (3*a*) *occurs only if* $p_2 - s_2^{(k)} < s_2^{(j)}$ *for* $\forall\, k > i$. *A defining point t of type* (3*b*) *occurs only if* $p_1 - s_1^{(k)} < s_1^{(i)}$ *for* $\forall\, k < j$.

On the basis of the above considerations, we have our main theorem.

THEOREM 2. *We can construct a minimal set of polynomials for* u^{p+1}, *i.e. there exists* $H = \{h^{(1)}, \ldots, h^{(m)}\} \in \mathbb{F}(u^{p+1})$, *even in case that there exists an* $f^{(i)} \in F_N$ *s.t.* $p \notin s^{(i)} + \Delta(u^p)$, *where m is the number of defining points of* $\Delta_e(u^{p+1})$, *and each polynomial h in H can be constructed by the Berlekamp procedure of an appropriate type* $\langle .,. \rangle$ *or some subsidiary procedure* (*which will be introduced in the following proof*).

PROOF. We have only to distinguish and treat the following six cases:

(1) Case A: For a defining point $t = (s_1^{(i)}, s_2^{(i)})$ of type (1), it has been already proved by Theorem 1.

(2) Case B: For a defining point $t = (p_1 - s_1^{(i)} + 1,\ p_2 - s_2^{(i+1)} + 1)$, $1 \leqq i \leqq l - 1$, of type (2), let $f^{(k)}$ be the polynomial which appears in the proof of Lemma 8 (Fig. 7), i.e. $f^{(k)}$ has $\mathrm{LP}(f^{(k)}) = s^{(k)}$ s.t. $s^{(k)} < (p_1 - s_1^{(i)} + 1,\ p_2 - s_2^{(i+1)} + 1)$. Then, on the basis of Lemma 6, the Berlekamp procedure of type $\langle k, i \rangle$ produces the desired new polynomial $h \in H$ s.t. $\mathrm{LP}(h) = t$.

(3) Case C: For a defining point $t = (p_1 - s_1^{(i)} + 1,\ s_2^{(j)})$, $1 \leqq i \leqq l - 1$, of type (3a) (Fig. 8), on the basis of Lemma 6, the Berlekamp procedure of type $\langle j, i \rangle$ produces the desired new polynomial $h \in H$ s.t. $\mathrm{LP}(h) = t$, since, in view of Lemma 9, $s_1^{(j)} < p_1 - s_1^{(i)} + 1$ and $s_2^{(j)} \geqq p_2 - s_2^{(i+1)} + 1$.

(4) Case D: For a defining point $t = (p_1 + 1, s_2^{(j)})$ of type (3a) (i.e. $i = l$) (Fig. 9), $h := x_1^{p_1 - s_1^{(j)} + 1} f^{(j)}$ satisfies the condition that $h \in \mathrm{VALPOL}(u^{p+1})$ and $\mathrm{LP}(h) = t$, since $p_1 + 1 > s_1^{(j)}$ and $s_2^{(j)} \leqq p_2 - s_2^{(l)}$.

(5) Case E: For a defining point $t = (s_1^{(i)},\ p_2 - s_2^{(j)} + 1)$, $2 \leqq j \leqq l$, of type (3b) (Fig. 10), on the basis of Lemma 6, the Berlekamp procedure of type $\langle i, j - 1 \rangle$ can be applied (similarly to Case C).

(6) Case F: For a defining point $t = (s_1^{(i)}, p_2 + 1)$ of type (3b) (i.e. $j = 1$) (Fig. 11), $h := x_2^{p_2 - s_2^{(j)} + 1} f^{(i)}$ satisfies the condition that $h \in \mathrm{VALPOL}(u^{p+1})$ and $\mathrm{LP}(h) = t$.

REMARK. The Berlekamp procedure can be applied except for the cases D and F, where the subsidiary procedures do instead.

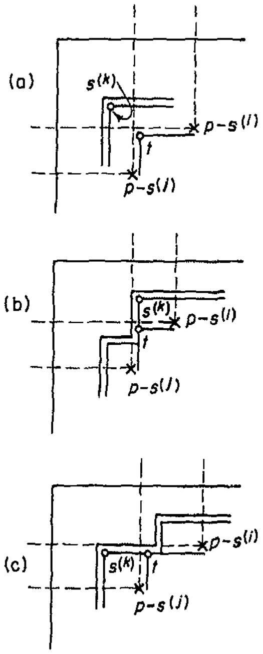


Fig. 7. Case B ($j > i$).

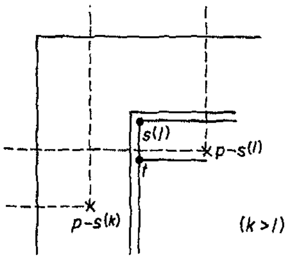


Fig. 8. Case C.

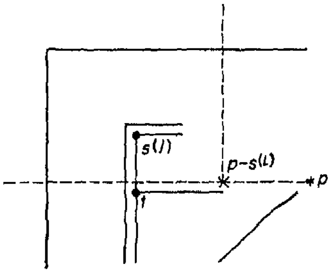


Fig. 9. Case D.

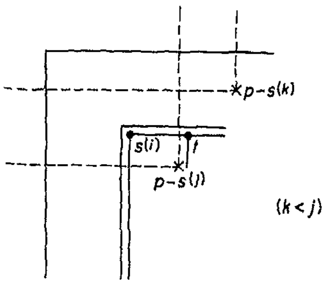


Fig. 10. Case E.

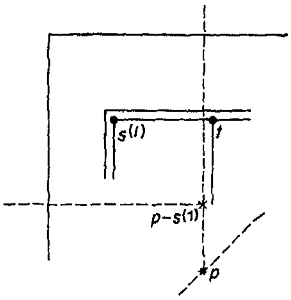


Fig. 11. Case F.

By the above Theorems 1 and 2, we can conclude that

$$\Delta(u^{p+1}) = \Delta_e(u^{p+1}),$$

and that we have a minimal set $F'\,(=H)$ of polynomials for u^{p+1}, i.e.

$$F' \in \mathbb{F}(u^{p+1}),$$

where the set of polynomials which determine the $\Delta_e(u^{p+1})$ becomes an auxiliary set G' of polynomials associated with the new minimal set F' of polynomials for u^{p+1}. The members of G' are selected from among $G \cup F_N$ and $|G'| = |F'| - 1$, where every member of F' and G' should be renumbered so that (2) and (12) are satisfied. Thus, we have already concluded our inductive reasoning, since, at the starting point 0, we can put $F = \{1\}$, $G = \phi$, $\Delta = \phi$.

5. Algorithm and its Complexity

We have already shown the correctness of the following algorithm for obtaining iteratively a minimal set of polynomials that generate a given finite 2D array $u = u^p$, where we keep and/or renew the following data iteratively at every point $n \in \Sigma_0^p$ during the process:

$$\begin{aligned}
F &= \{f^{(k)} \mid 1 \leqq k \leqq l\} \in \mathbb{F}(u^n),\\
S &= \{s^{(k)} = \mathrm{LP}(f^{(k)}) \mid 1 \leqq k \leqq l\},\\
G &= \{g^{(k)} \mid 1 \leqq k \leqq l-1\},\\
T &= \{t^{(k)} = \mathrm{LP}(g^{(k)}) \mid 1 \leqq k \leqq l-1\},\\
PG &= \{p^{(k)} \mid 1 \leqq k \leqq l-1\},\\
DG &= \{d^{(k)} \mid 1 \leqq k \leqq l-1\},
\end{aligned}$$

where G is an auxiliary set associated with F, and each element $d^{(k)}$ of DG is the discrepancy at $p^{(k)}$ of the corresponding polynomial $g^{(k)}$ in G. (S and T are redundant data.) We remark that the number l of elements in F depends on n and $\Delta = \Delta(u^n)$ is determined by S. (Δ is also determined by PG and T.)

```
Algorithm:
Step 1: $n := (0,0)$, F := {1}, G := $\phi$, $DG := \phi$ ($\Delta = \phi$);
Step 2: if $^\exists f \in F_N$ (i.e. $f[u]_n \neq 0$), then do
  begin if $n \in \mathrm{LP}(f) + \Delta$ for any $f$ in $F_N$, then replace $F$ by a new $F$ using the procedure
      described in Theorem 1;
    else replace $\Delta$ and $F$ by the new $\Delta$ and a new $F$ using the procedure described in
      Theorem 2, and replace $G$ and $DG$ by a new $G (\subseteq F_N \cup G)$ associated with the new
      $F$ and the corresponding new $DG$;
  end;
Step 3: $n := n+1$; if $n = p$, then stop; else go to Step 2.
```

Example 3. For the 2D array u of size 16 over $K = \mathrm{GF}(2)$ shown in Fig. 2, the computation of the algorithm proceeds as shown in Fig. 12. For example, at $n = (1, 0)$, $f = 1$ is not valid and the procedures in both Cases D and F are applicable, by which we obtain $\{x_1^2, x_2\} \in \mathbb{F}(u^{(0,1)})$. At $n = (0, 1)$, we have Case A w.r.t. $f^{(i)} = x_2$ $(g^{(j)} = 1)$ and we get $x_2 + x_1$. At $n = (2, 1)$, we have Case D w.r.t. $f^{(j)} = x_1^2$, Case C w.r.t. $f^{(i)} = x_1^2$, $f^{(j)} = x_2 + x_1 + 1$ $(g^{(i)} = 1)$, and Case F w.r.t. $f^{(i)} = x_2 + x_1 + 1$. Thus, we get x_1^3 for

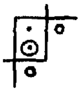
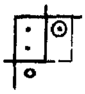
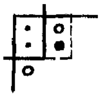
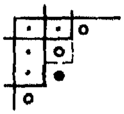
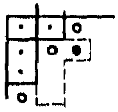
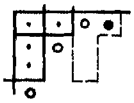
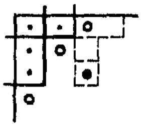
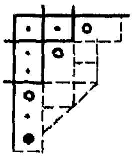
$\lvert n \rvert$	n	u_n	F	S	G	T	P	Δ
0	0, 0	0	1	0, 0	ϕ			
1	1, 0	1	as above					
2	0, 1	1	x_1^2 x_2	2, 0 0, 1	1	0, 0	1, 0	
3	2, 0	0	x_1^2 x_2+x_1	2, 0 0, 1	1	0, 0	1, 0	
4	1, 1	1	as above					
5	0, 2	0	x_1^2 x_2+x_1+1	2, 0 0, 1	1	0, 0	1, 0	
6	3, 0	0	as above					
7	2, 1	1	as above					
8	1, 2	0	x_1^3 $x_1x_2+x_1^2+x_1+1$ $x_2^2+x_1x_2+x_2$	3, 0 1, 1 0, 2	x_2+x_1+1 x_1^2	0, 1 2, 0	2, 1 2, 1	
9	0, 3	1	x_1^3 $x_1x_2+x_1+1$ $x_2^2+x_1x_2+x_2$	3, 0 1, 1 0, 2	x_2+x_1+1 x_1^2	0, 1 2, 0	2, 1 2, 1	
10	4, 0	0	x_1^3 $x_1x_2+x_1+1$ $x_2^2+x_1x_2+x_1^2+x_2$	3, 0 1, 1 0, 2	as above			
11	3, 1	0	as above					
12	2, 2	0	as above					
13	1, 3	0	x_1^3 $x_1x_2+x_1+1$ $x_2^2+x_1x_2+x_1^2+x_1+1$	3, 0 1, 1 0, 2	as above			
14	0, 4	0	as above					
15	5, 0	1	as above					
16	4, 1	*	$x_1^3+x_2+x_1+1$ $x_1x_2+x_1+1$ $x_2^2+x_1x_2+x_1^2+x_1+1$	3, 0 1, 1 0, 2	as above			

Fig. 12. An example of computation.

$t=(3,0)$, $x_1x_2+x_1^2+x_1+1$ for $t=(1,1)$ and $x_2^2+x_1x_2+x_2$ for $t=(0,2)$. Finally, the result of the computation is

$$F = \{x_1^3+x_2+x_1+1,\ x_1x_2+x_1+1,\ x_2^2+x_1x_2+x_1^2+x_1+1\} \in \mathbb{F}(u),$$

which proves to be a Gröbner basis of Ideal (F) (which is not yet reduced), and which coincides with a basis of the maximum ideal of the DP array shown in Fig. 3. The finite array u is a part of that DP array.

Now we consider the complexity of the algorithm. At each point n, we must make computations as follows:

(1) check of $f[u]_n=0$ or not, which requires $O(l|n|)$ computations;
(2) check of degree-invariancy, and (if some degree change occurs) determination of the new Δ, which requires $O(l)$ computations;
(3) Berlekamp procedures, which, in totality, require $O(l|n|)$ computations;

where l is the number of elements in the current F, which in general changes itself depending on n. Thus, we have the following theorem.

THEOREM 3. *If $l=|F|$ is bounded, then the (total) complexity of the algorithm applied to u of size k is $O(k^2)$.*

REMARK. The boundedness of $|F|$ is assured, for example, in either case as follows:

(1) u is a DP array, where k can be identified with the period of u;
(2) u is an impulse response array of a discrete 2D system, i.e. u is obtained by expanding a rational transfer function into a formal power series (Prabhu & Bose, 1982), e.g.

$$\frac{g(x_1,x_2)}{f(x_1,x_2)} = \sum_{i,j\geq 0} u_{ij}x_1^i x_2^j,$$

where $f(x_1,x_2)$, $g(x_1,x_2)\in K[x]$ and $f_{00}\neq 0$.

6. Uniqueness and Gröbner Bases

A given polynomial $f\in F$ can be reduced into a reduced normal form g modulo Ideal(F) (Buchberger, 1985), where $\Gamma_g/\{\mathrm{LP}(f)\}\subset\Delta(F)$. From now on, let $\mathbb{F}(u)$ be the class of minimal sets F of monic polynomials in reduced normal form. Then, as for the uniqueness of $F\in\mathbb{F}(u)$, we have the following theorem (which is proved in Appendix 6).

THEOREM 4. *Let $F\in\mathbb{F}(u^p)$. If $\mathrm{LP}(f)+\Delta(u^p)\subseteq\Sigma_0^p$ for any $f\in F$, then F is unique (i.e. $|\mathbb{F}(u^p)|=1$).*

Before discussing about some relationship between Gröbner bases and $\mathbb{F}(u)$, we need several definitions. For a finite set $F=\{f^{(1)},\ldots,f^{(l)}\}$ of polynomials, let

$$N(F):=\bigcup_{i=1}^{l}\Sigma_{\mathrm{LP}(f^{(i)})}.$$

In particular, if $F\in\mathbb{F}$, i.e. F is of delta type, then $N(F)=\Sigma_0/\Delta(F)$.

DEFINITION 2. A finite set F of polynomials is said to be consistent if and only if F is a Gröbner basis of Ideal(F).

DEFINITION 3. A finite set F of polynomials is said to be compatible for a finite 2D array $u = u^p$ if and only if there exists an infinite 2D array v s.t. $v^p = u$ and $F \subseteq \mathrm{I}(v)$.

The following lemma makes clear the relationship between consistency and compatibility (the proof is given in Appendix 7).

LEMMA 10. *There exists a finite 2D array $u = u^p$ s.t. $F \in \mathbb{F}(u)$ and F is compatible for u if and only if F is consistent.*

For a DP array u, let FPP(u) be a fundamental period parallelogram of u and $\Phi(u)$ be a subset of Σ_0 which corresponds one-to-one to an FPP(u), i.e. for each $n \in \mathrm{FPP}(u)$, there exists $m \in \Phi(u)$ s.t. $u_{m+r} = u_{n+r}$ for any $r \in \Sigma_0$ and vice versa (of course, $|\Phi(u)| = \mathrm{per}(u) = |\mathrm{FPP}(u)|$). Thus, in view of Lemma 10, we have the following theorem.

THEOREM 5. *Let u be a DP array and $F = \{f^{(1)}, \ldots, f^{(l)}\} \in \mathbb{F}(u^p)$. If*

$$\bigcup_{i=1}^{l} (\mathrm{LP}(f^{(i)} + \Delta(u^p)) \subseteq \Sigma_0^p$$

and some $\Phi(u) \subseteq \Sigma_0^p / \Delta(u^p)$, then F is consistent.

7. Concluding Remarks

A (finite or infinite) 2D array can be regarded as a 1D array by rearranging the components linearly in some order (e.g. correspondingly to the total degree order). For such a 1D image of a 2D array, the Berlekamp algorithm (w.r.t. 1D arrays) cannot find any 2D LR relation. For example, even a simple 2D LR relation such as $f = x_1 x_2 + 1$ cannot be represented by any 1D LR relation w.r.t. the 1D array which is obtained from the original 2D array. Thus, our result gives an essentially new aspect which cannot be disclosed by any 1D treatment.

The author wishes to express his sincere gratitude to Prof. Dr Bruno Buchberger for hospitality and kind support during the period this paper was written at the Johannes Kepler University in Linz, Austria. Furthermore, the author is very much obliged to him for many suggestions in improving this paper. This research has been made on the fellowship of the exchange programme between the Japanese Society for Promotion of Science and the Austrian Academy of Science.

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*, pp. 176–199, 218–240. New York: McGraw-Hill.

Buchberger, B. (1970). An algorithmic criterion for the solvability of algebraic systems of equations (in German). *Aequ. Math.* **4**, 374–383.

Buchberger, B. (1985). Gröbner bases: An algorithmic method in polynomial ideal theory. In: (Bose, N. K. ed.) *Multidimensional Systems Theory*, pp. 184–232. Dordrecht: Reidel.

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

Massey, J. L. (1969). Shift-register synthesis and BCH decoding. *IEEE Trans. Inform. Theory*, **15**, 122–127.

Prabhu, K. A., Bose, N. K. (1982). Impulse response arrays of discrete-space systems over a finite field. *IEEE Trans. Acoustics, Speech Signal Processing*, **30**, 10–18.

Sakata, S. (1978). General theory of doubly periodic arrays over an arbitrary finite field and its applications. *IEEE Trans. Inform. Theory*, **24**, 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*, **27**, 556–565.

Appendices

PROOFS OF LEMMAS AND THEOREMS

(APPENDIX 1) LEMMA 1. *Assume that* $f, g\in \mathrm{VALPOL}(u)$ *and* $h=f+g$. *Then,*

$$\sum_{m\in\Sigma_0^q} f_m u_{m+n} = 0, \quad n\in\Sigma_0,$$

$$\sum_{m\in\Sigma_0^q} g_m u_{m+n} = 0, \quad n\in\Sigma_0,$$

where $\Sigma_0^q \supseteq \Gamma_f \cup \Gamma_g \supseteq \Gamma_h$. *Therefore, we have*

$$\sum_{m\in\Sigma_0^q} h_m u_{m+n} = 0, \quad n\in\Sigma_0.$$

Thus, $f+g\in \mathrm{VALPOL}(u)$. *Next, let* $f\in \mathrm{VALPOL}(u)$. *Then*

$$\sum_{m\in\Gamma_f} f_m u_{m+n} = 0, \quad n\in\Sigma_0.$$

Clearly,

$$\sum_{m\in\Gamma_f} f_m u_{m+(1,0)+n} = 0, \quad n\in\Sigma_0,$$

$$\sum_{m\in\Gamma_f} f_m u_{m+(0,1)+n} = 0, \quad n\in\Sigma_0.$$

Therefore, we have $x_1 f$, $x_2 f\in \mathrm{VALPOL}(u)$. *Thus, in view of the former part of the proof,* $gf\in \mathrm{VALPOL}(u)$ *for any* $g\in K[x]$. □

(APPENDIX 2) LEMMA 4. *We may assume that* $p>s$, *since otherwise Lemma* 4 *is trivial. Let* $(t_1\leqq p_1-s_1)\wedge(t_2\leqq p_2-s_2)$, *i.e.* $t\leqq p-s$. *We may put* $f_s=h_t=1$ *without loss of generality. By the assumption, we have*

$$\begin{aligned} -\sum_{m\in\Gamma_f'} f_m u_{m+n-s} &= u_n, \quad n\in\Sigma_s^p, \\ &\neq u_p, \quad n=p, \end{aligned} \tag{A1}$$

and

$$-\sum_{r\in\Gamma_h'} h_r u_{r+n-t} = u_n, \quad n\in\Sigma_t^{p+1}, \tag{A2}$$

where $\Gamma_f' := \Gamma_f/\{s\}$ *and* $\Gamma_h' := \Gamma_h/\{t\}$. *Therefore, it follows that*

$$-\sum_{m\in\Gamma_f'} f_m u_{m+p-s} = \sum_{m\in\Gamma_f'} f_m \sum_{r\in\Gamma_h'} h_r u_{r+m+p-s-t}, \tag{A3}$$

since $m+p-s\in\Sigma_t^{p+1}$ *for* $m\in\Gamma_f'$ *in view of* $t\leqq p-s$. *Upon interchange of the order of summation, the right-hand side of* (A3) *becomes*

$$\sum_{r\in\Gamma_h'} h_r \sum_{m\in\Gamma_f'} f_m u_{m+r+p-t-s},$$

which, in view of (A1) *and* (A2), *is equal to*

$$-\sum_{r\in\Gamma_h'} h_r u_{r+p-t} = u_p,$$

since $r+p-t\in\Sigma_s^p$ *for* $r\in\Gamma_h'$. *The result contradicts with* (A1). □

(Appendix 3) Lemma 5. *We can easily show that* $\mathrm{LP}(h)=r$. *Furthermore,*

$$\begin{aligned}\sum_{m\in\Gamma_h} h_m u_{m+n-r} &= \sum_{m\in\Gamma_f} f_m u_{m+n-s}-(d_q/d_p)\sum_{m\in\Gamma_g} g_m u_{m+n-q+p-t},\\ &= 0, \quad n\in\Sigma_r^q,\\ &= d_q-(d_q/d_p)d_p = 0, \quad n=q,\end{aligned}$$

where the former equality follows from the inclusions $\Sigma_r^q\subseteq\Sigma_s^q$ *and* $n-q+p\in\Sigma_t^p$ *for* $n\in\Sigma_r^q$. *The last relation can be proved as follows:*

$$\begin{aligned}n\in\Sigma_r^q &\Rightarrow r\leqq n<_T q\Rightarrow t+q-p\leqq r\leqq n<_T q\\ &\Rightarrow t\leqq n-(q-p)<_T q-(q-p)=p,\end{aligned}$$

where the last inequality is valid in view of the following lemma.

Lemma A. *Let* $s<_T t$ *for* $s,t\in\Sigma_0$. *If* $s+u\in\Sigma_0$ *and* $t+u\in\Sigma_0$ *for some* $u\in Z\times Z$, *then* $s+u<_T t+u$.

Proof. If $s<_T t$, then we have only to consider the following two cases:

(1) In case of $s_1+s_2<t_1+t_2$, we have $s_1+s_2+u_1+u_2<t_1+t_2+u_1+u_2$. Hence, $s+u<_T t+u$.
(2) In case of $s_1+s_2=t_1+t_2$ and $s_1>t_1$, we have $s_1+s_2+u_1+u_2=t_1+t_2+u_1+u_2$ and $s_1+u_1>t_1+u_1$. Hence, $s+u<_T t+u$. □

(Appendix 4) Lemma 8. *From the assumption it follows that* $t=(p_1-s_1^{(i)}+1, p_2-s_2^{(j)}+1)\notin\Delta(u^p)$. *Hence, there exists a polynomial* $f^{(k)}\in F$ with $\mathrm{LP}(f^{(k)})=s^{(k)}$ *s.t.* $s^{(k)}<t$. *Then we can distinguish the following three cases (see Fig.* 7)*:*

(*a*) $(p_1-s_1^{(i)}+1>s_1^{(k)})\wedge(p_2-s_2^{(j)}+1>s_2^{(k)})$,
(*b*) $(p_1-s_1^{(i)}+1>s_1^{(k)})\wedge(p_2-s_2^{(j)}+1=s_2^{(k)})$,
(*c*) $(p_1-s_1^{(i)}+1=s_1^{(k)})\wedge(p_2-s_2^{(j)}+1>s_2^{(k)})$.

In either case, from $p_1-s_1^{(j)}\geqq p_1-s_1^{(i)}+1$, $p_2-s_2^{(i)}\geqq p_2-s_2^{(j)}+1$, *it follows that* $(p-s^{(i)}>s^{(k)})\vee(p-s^{(j)}>s^{(k)})$. *Hence, in view of Lemma* 4 *and* $f^{(i)},f^{(j)}\in F_N$, $f^{(k)}\in F_N$. *Now, let* $j>i+1$, *then* $f^{(i+1)},\ldots,f^{(j-1)}\in F_V$, *since otherwise* $t\in\Delta_e(u^{p+1})$. *From* $s^{(k)}<t$, *it follows that*

$$\begin{aligned}p_1-s_1^{(k)} &\geqq s_1^{(i)}-1\geqq s_1^{(i+1)}>\ldots>s_1^{(j-1)},\\ p_2-s_2^{(k)} &\geqq s_2^{(j)}-1\geqq s_2^{(j-1)}>\ldots>s_2^{(i+1)}.\end{aligned}$$

Consequently, $p-s^{(k)}\geqq s^{(i+1)},\ldots,s^{(j-1)}$, *which contradicts with* $f^{(i+1)},\ldots,f^{(j-1)}\in F_V$. □

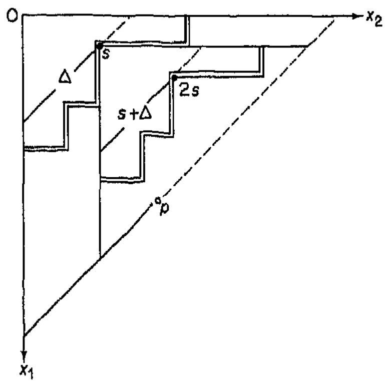


Fig. 13. $(s+\Delta)\cap\Sigma_s^{2s}$.

(Appendix 5) Lemma 9. *We have only to prove the first part. The second part is proved similarly. From the assumption,* $p_1-s_1^{(i)}+1>s_1^{(j)}$. *Let* $p_2-s_2^{(k)}\geqq s_2^{(j)}$ *for some* $k>i$. *Then,* $f^{(i+1)},\ldots,f^{(k)}\in F_V$, *since otherwise* $t=(p_1-s_1^{(k)}+1,\ s_2^{(j)})\in\Delta_e(u^{p+1})$. *But, since*

$$p_1-s_1^{(k)}>p_1-s_1^{(k-1)}>\ldots>p_1-s_1^{(i+1)}>p_1-s_1^{(i)}\geqq s_1^{(j)},$$
$$p_2-s_2^{(i)}>p_2-s_2^{(i+1)}>\ldots>p_2-s_2^{(k-1)}>p_2-s_2^{(k)}\geqq s_2^{(j)},$$

we have $p-s^{(j)}\geqq s^{(i+1)},\ldots,s^{(k)}$, *which contradicts with* $f^{(i+1)},\ldots,f^{(k)}\in F_V$. □

(Appendix 6) Theorem 4. *Let* $f\in F$ *with* $\mathrm{LP}(f)=s$ *and* $\Delta=\Delta(u^p)$. *From* $f[u]_n=0$ *at each* $n\in\Sigma_s^p$ $(\supseteq(s+\Delta)\cap\Sigma_s^{2s})$, *we can construct a linear equation whose unknowns are* $\{f_n\mid n\in\Delta\cap\Sigma_0^s\}$, *where* $2s=(2s_1,2s_2)$ *(see Fig. 13). The coefficient matrix of the system of these linear equations has size* $q\times r$ *and rank* r, *where*

$$q:=|\Sigma_s^p|\geqq r:=|(s+\Delta)\cap\Sigma_s^{2s}|=|\Delta\cap\Sigma_0^s|,$$

because otherwise F *is not minimal. Thus,* $\{f_n\mid n\in\Delta\cap\Sigma_0^s\}$ *is uniquely determined.* □

(Appendix 7) Lemma 10. *(Sufficiency part) Since* F *is consistent, for any point* $n\in N(F):=\Sigma_0/\Delta(F)$, *there exists a unique polynomial*

$$f^{(n)}:=x^n-\sum_{m\in\Delta(F)}f_m^{(n)}x^m\ \text{s.t.}\ f^{(n)}\in\mathrm{Ideal}(F).$$

We can define uniquely an infinite 2D array $v=(v_n)$ *s.t.*

$$\begin{aligned} v_n &= u_n, \quad n\in\Delta(F),\\ &= \sum_{m\in\Delta(F)}f_m^{(n)}u_m, \quad n\in N(F). \end{aligned}$$

Clearly $v^p=u$ *and* $f^{(n)}\in\mathrm{VALPOL}(v)=\mathrm{I}(v)$, *for any* $n\in N(F)$. *In particular, for any* $f\in F$ *with* $\mathrm{LP}(f)=s$, $f=f^{(s)}\in\mathrm{I}(v)$. *Thus,* $F\subseteq\mathrm{I}(v)$. *Therefore,* F *is compatible for* u. *(In fact,* $\mathrm{Ideal}(F)=\mathrm{I}(v)$ *and* v *is a DP array.)*

(Necessity part) There exists an infinite 2D array v *s.t.* $u=v^p$ *and* $F\subseteq\mathrm{I}(v)$. *If* F *is not consistent, then there exists a polynomial* f *s.t.* $f\in\mathrm{Ideal}(F)\subseteq\mathrm{I}(v)$ *and* $\mathrm{LP}(f)\notin N(F)$. *Since* $f\in\mathrm{I}(v)=\mathrm{VALPOL}(v)$, $f\in\mathrm{VALPOL}(u)$. *This contradicts with the minimality of* F *for* u. □