J. Symbolic Computation (1998) **26**, 301–314
Article No. sy980213

Properties of Gröbner Bases and Applications to Doubly Periodic Arrays[†]

MULAN LIU[‡] AND LEI HU[§]

[‡] *Institute of Systems Science, Academia Sinica, Beijing 100080, China*
[§] *Guangzhou Normal College, Guangzhou 510400, China*

In this paper the properties of Gröbner bases of zero-dimensional ideals are studied. A basis of the space of linear recurring arrays and the trace expression of linear recurring arrays are given.

1. Introduction

Recently, many people have studied two-dimensional arrays over finite fields because they can be used in two-dimensional range-finding, scrambling, two-dimensional cyclic codes and other applications in communication and coding. There are two types of problems on two-dimensional arrays. The first type of problem concerns nonlinear arrays or perfect maps, the second type concerns linear recurring arrays. Nomura *et al.* (1972) were the first to study linear recurring arrays. In fact they studied linear recurring m-arrays or pseudo-random arrays. In their paper they proposed a problem on the structure of pseudo-random arrays. Siu (1985) proposed that problem again when he visited Beijing. MacWilliams and Sloane (1976) constructed some pseudo-random arrays, Van Lint *et al.* (1979) studied some linear recurring arrays with special window properties. Lin and Liu solved Nomura's problem and gave the structure of pseudo-random arrays (Lin and Liu, 1993a; Liu and Li, 1993). Sakata (1978) considered the general theory of linear recurring arrays over finite fields. But further results on the structural general theory of linear recurring arrays were not forthcoming, even though some people (e.g., Lin (1993) and Lin and Liu (1993b)) considered more general linear recurring arrays than pseudo-random arrays, but they were still some specific cases. However, when the Gröbner basis theory was utilized to study linear recurring arrays, some progress was made (Sakata, 1988; Liu and Hu, 1994). In this paper we study doubly periodic arrays, as they are linear recurring arrays and more useful. We apply the properties of Gröbner bases to the space of linear recurring arrays. This yields an explicit basis of the space of linear recurring arrays and gives a pretty, as well as important, trace expression. It is well known that the trace expression of one-dimensional linear recurring sequences is a strong tool for studying their structure and enumeration. Our trace expression of linear recurring arrays can also be used to study their structure as a linear space and as a module, and to calculate the number of translation equivalent classes of linear recurring arrays. But the two-dimensional case is much more complicated than the one-dimensional case. We differ from others in

[†]Research supported by NNSF of China and K. C. Wong Education Foundation, Hong Kong.

0747–7171/98/090301 + 14 $30.00/0

that we use the theory of Gröbner bases to prove various properties, instead of giving or discussing an algorithm.

In what follows we introduce some basic concepts. In Section 2 we give a refined characterization for a reduced Gröbner basis of any zero-dimensional ideals. In Section 3, we construct a special basis of the space of linear recurring arrays which is an explicit expression. In Section 4, we give the trace expression of linear recurring arrays.

Let F be an arbitrary finite field with q elements, Z the ring of integers, and Z_+ the set of non-negative integers. Let $R = F[x, y]$ be the polynomial ring in two indeterminates x and y, then $S = \{x^m y^n \mid m \geq 0, n \geq 0\}$ is a multiplicatively closed subset of R. We denote by $R' = S^{-1}F[x, y]$ the ring of fractions of R with respect to S. An array A of dimension 2 is an infinite matrix $A = (A_k)_{k \in Z^2}$ over F. For $j \in Z^2$, the j-translation of A, written ${}_jA$, is defined by $({}_jA)_i = A_{i+j}$ for all $i \in Z^2$. If ${}_jA = A$, then j is called a period of A. The set $P = \{l \in Z^2 \mid {}_lA = A\}$ is a Z-module according to ordinary addition and scalar multiplication. If P has a basis with two elements, then A is called a doubly periodic array. It is easy to see that if A is doubly periodic then there are two positive integers r and s such that $A_{i+(r,0)} = A_i = A_{i+(0,s)}$ for all $i \in Z^2$.

Let $f(z) = \sum_i f_i z^i \in R'$ where $z = (x, y), i = (i_1, i_2) \in Z^2, z^i = x^{i_1} y^{i_2}$. We define the action of $f(z)$ on an array A by

$$fA = \sum_k f_k \ {}_kA.$$

If $fA = 0$, then the array A satisfies the linear recurring relation determined by f and is called a linear recurring array or LRA in short. Obviously, any doubly periodic array is linear recurring. Throughout the paper any linear recurring array considered is doubly periodic. Let $I(A) = \{f(z) \in R' \mid fA = 0\}$ that is an ideal of R' and is called the characteristic ideal of A. Let $W(F)$ be the linear space of all doubly periodic arrays over F according to ordinary addition and scalar multiplication of arrays, and $G(I) = \{A \in W(F) \mid fA = 0 \text{ for all } f \in I\}$ where I is an ideal of R'. Then $G(I)$ is a linear subspace of $W(F)$ and is called the space of linear recurring arrays over F determined by I.

In the following we only consider ideals in the ring R, as every ideal of the ring R' can be generated by some polynomials of the ring R.

Define the total order $\preceq$ on Z_+^2 by the inverse lexicographical order, i.e. $(a, b) \preceq (c, d)$ iff $b \leq d$, or $b = d$ and $a \leq c$. Define the partial order $\leq$ of Z_+^2 as the following:

$$(a, b) \leq (c, d) \text{ iff } a \leq c \text{ and } b \leq d.$$

Let $T^{(2)} = \{z^i \mid i \in Z_+^2\}$. Define $z^i \preceq z^j$ iff $i \preceq j$. Then for any $f(z) \in R$ with $f \neq 0$ we may write

$$f(z) = a_1(f)T_1 + a_2(f)T_2 + \cdots + a_l(f)T_l,$$

where for $t = 1, 2, \ldots, l$, $0 \neq a_t(f) \in F, T_t \in T^{(2)}$, and $T_1 \succ T_2 \succ \cdots \succ T_l$. We will write our polynomials in this way. Let

$$Lt(f) = T_1, \quad \text{the leading term of } f \text{ and } Lc(f) = a_1(f), \text{ the leading coefficient of } f.$$

As the ring R is a polynomial ring over a field, any ideal I of R has a unique reduced Gröbner basis with respect to the order $\preceq$ denoted by $RGB(I)$. If I contains $x^r - 1$ and $y^s - 1$ for some positive integers r and s, then the fact that $RGB(I)$ is reduced implies

$$RGB(I) = \{f_0(x), f_1(x, y), \ldots, f_l(x, y)\}$$

where $f_t(x,y) \in F[x,y]$. Suppose $Lt(f_t) = x^{m_t}y^{n_t}$ and $Lt(f_t) \prec Lt(f_{t+1})$ for $t = 0,1,\ldots,l-1$. Then

$$m_0 > m_1 > \cdots > m_l = 0,$$
$$0 = n_0 < n_1 < \cdots < n_l.$$

Let

$$\Gamma(I) = \{k \in Z_+^2 \mid k \not\geq (m_t, n_t),\ \text{for } t = 0,1,\ldots,l\}$$

and $t = |\Gamma(I)|$, the number of points of $\Gamma(I)$. The set $\Gamma(I)$ is called the Gröbner window of I and t is called the size of $\Gamma(I)$. Notice that $\Gamma(I)$ is exactly the set of exponents of reduced terms w.r.t. the ideal I.

Because we are interested in doubly periodic arrays, throughout the rest of the paper we will always suppose that any ideal of a ring R that we study includes the polynomials $x^r - 1$ and $y^s - 1$ for some positive integers $r$and s, unless we specify otherwise. In fact, an ideal including $x^r - 1$ and $y^s - 1$ is a zero-dimensional ideal.

2. Reduced Gröbner Bases of Zero-dimensional Ideals

In this section we apply some properties of reduced Gröbner bases to give a refined characterization for reduced Gröbner bases of zero-dimensional ideals. Then we apply this result to find a basis of the space of linear recurring arrays in the next section. Throughout this section the letters i and j denote non-negative integers unless we specify otherwise. As every ideal I of the ring R has a minimal primary decomposition $I = \bigcap_j I_j$ and it is easy to see that the linear space $G(I) = \bigoplus_j G(I_j)$, in order to obtain a basis of the linear space $G(I)$ for any ideal I of the ring R, we only need to study $G(I)$ for any primary ideal I of the ring R. Furthermore, there exists a finite extension field K of F such that a minimal primary decomposition of the extension ideal I^e of I in the ring $K[x,y]$ $I^e = \bigcap_i J_i$ with the set of zero points of J_i having only one element for each i over K. It means that for each i there are two elements α_i and β_i of K such that the radical ideal of J_i $\sqrt{J_i} = \langle x - \alpha_i, y - \beta_i\rangle$, i.e. it is generated by $x - \alpha_i$ and $y - \beta_i$. In the following we characterize $RGB(I)$ for a zero-dimensional ideal I of the ring $K[x,y]$ with the radical ideal $\sqrt{I} = \langle x - \alpha, y - \beta\rangle$ where α and β are two non-zero elements of K in detail. It is very useful for finding a basis of the linear space $G(I)$ for any zero-dimensional ideal I of the ring R.

Theorem 2.1. *Let K be a finite extension field of F, α and β two non-zero elements of K. Let I be an ideal of the ring $K[x,y]$ with $\dim I = 0$ and its radical ideal $\sqrt{I} = \langle X, Y\rangle$, i.e. it is generated by X and Y where $X = x - \alpha, Y = y - \beta$. Suppose*

$$RGB(I) = \{X^{a_0} = f_0(X,Y), f_1(X,Y), \ldots, f_l(X,Y)\},$$

and $Lt(f_i) = X^{a_i}Y^{b_i}, Lt(f_i) \prec Lt(f_{i+1})$ for all $i = 0,1,\ldots,l-1$. Then

$$f_i(X,Y) = X^{a_i}Y^{b_i} + \sum_{\substack{j_1 > a_i \\ j_2 < b_i}} f^{(i)}_{j_1 j_2} X^{j_1} Y^{j_2}.$$

Proof. Suppose

$$f_i(X,Y) = g_0(X)Y^{b_i} + g_1(X)Y^{b_i - 1} + \cdots + g_{b_i - 1}(X)Y + g_{b_i}(X)$$

and

$$\gcd(g_0(X), X^{a_0}) = X^c.$$

Then $0 \le c \le a_i$ and there are two polynomials $u(X)$ and $v(X)$ such that

$$g_0(X)u(X) + X^{a_0}v(X) = X^c.$$

This implies

$$-(g_1(X)Y^{b_i-1} + \cdots + g_{b_i-1}(X)Y + g_{b_i}(X))u(X) \equiv Y^{b_i}X^c \pmod{I},$$

but

$$Lt(Y^{b_i}X^c + u(X)(g_1(X)Y^{b_i-1} + \cdots + g_{b_i-1}(X)Y + g_{b_i}(X))) = Y^{b_i}X^c.$$

If $c < a_i$, then it is impossible to have $X^{a_j}Y^{b_j}|X^cY^{b_i}$for any $j = 1, 2, \ldots, l$, because it contradicts the properties of reduced Gröbner bases. Thus $c = a_i, X^{a_i}|g_0(X)$, and we have that $g_0(X) = X^{a_i}$ and

$$f_i(X,Y) = X^{a_i}Y^{b_i} + g_1(X)Y^{b_i-1} + \cdots + g_{b_i-1}(X)Y + g_{b_i}(X).$$

We prove $X^{a_i+1}|f_i(X,Y) - X^{a_i}Y^{b_i}$ by induction on i. For $i = 1$, suppose

$$f_1(X,Y) = X^{a_1}Y^{b_1} + X^cG(Y) + X^{c+1}H(X,Y),$$

where

$$c \ge 0, \deg_Y G(Y) < b_1, \deg_Y H(X,Y) < b_1.$$

If $c < a_1$ and $G(Y) \ne 0$, then

$$f_1(X,Y)X^{a_0-(c+1)} = X^{a_0-(c+1)+a_1}Y^{b_1} + X^{a_0-1}G(Y) + X^{a_0}H(X,Y) \equiv 0 \pmod{I}.$$

This implies $X^{a_0-1}G(Y) \equiv 0 \pmod{I}$ which is impossible.

If $c = a_1$ and $G(Y) \ne 0$, then

$$f_1(X,Y) = X^{a_1}(Y^{b_1} + G(Y)) + X^{a_1+1}H(X,Y).$$

There is a positive integer N such that $Y^N \in I$ and

$$\gcd(Y^{b_1} + G(Y), Y^N) = Y^d.$$

Thus $d < b_1$ and there are two polynomials $u(Y)$ and $v(Y)$ such that

$$(Y^{b_1} + G(Y))u(Y) + v(Y)Y^N = Y^d.$$

This implies

$$\begin{aligned} X^{a_0-1-a_1}(f_1(X,Y) - X^{a_1+1}H(X,Y))u(Y) &\equiv -X^{a_0}H(X,Y)u(Y) \\ &\equiv 0 \equiv X^{a_0-1}Y^d \pmod{I}. \end{aligned}$$

We can deduce that $d \ge b_1$ which is impossible. Hence,

$$f_1(X,Y) = X^{a_1}Y^{b_1} + \sum_{\substack{j_1 > a_1 \\ j_2 < b_1}} f^{(1)}_{j_1 j_2} X^{j_1}Y^{j_2}.$$

Suppose for $t = 1, 2, \ldots, i-1$,

$$f_t(X,Y) = X^{a_t}Y^{b_t} + \sum_{\substack{j_1 > a_t \\ j_2 < b_t}} f^{(t)}_{j_1 j_2} X^{j_1}Y^{j_2},$$

and

$$f_i(X,Y) = X^{a_i}Y^{b_i} + X^cG(Y) + X^{c+1}H(X,Y)$$

where $c \ge 0$, $\deg_Y G(Y) < b_i$, $\deg_Y H(X,Y) < b_i$.

If $c < a_i$ and $G(Y) \neq 0$, then

$$X^{a_{i-1}-(c+1)} f_i(X,Y) = X^{a_{i-1}-(c+1)+a_i} Y^{b_i} + X^{a_{i-1}-1} G(Y) + X^{a_{i-1}} H(X,Y),$$

and there exists a polynomial $K(X,Y)$ such that

$$X^{a_i} Y^{b_i} X^{a_{i-1}-c-1} + X^{a_{i-1}} H(X,Y) \equiv K(X,Y) \ (\operatorname{mod} f_0, f_1, \ldots, f_{i-1})$$

where $\deg_X K(X,Y) \geq a_{i-1}$, $\deg_Y K(X,Y) < b_{i-1}$ and $K(X,Y)$ is reduced. Thus

$$X^{a_{i-1}-1} G(Y) + K(X,Y) \equiv 0 \ (\operatorname{mod} RGB(I))$$

but $X^{a_{i-1}-1} G(Y) + K(X,Y) \neq 0$ and cannot be reduced to 0 via $RGB(I)$. Clearly this is impossible. Thus, we have that $c \geq a_i$.

If $c = a_i$ and $G(Y) \neq 0$, then

$$f_i(X,Y) = X^{a_i}(Y^{b_i} + G(Y)) + X^{a_i+1} H(X,Y).$$

There is a positive integer N such that $Y^N \in I$ and

$$\gcd(Y^{b_i} + G(Y), Y^N) = Y^d.$$

Then $0 \leq d < b_i$ and there are two polynomials $u(Y)$ and $v(Y)$ such that

$$u(Y)(Y^{b_i} + G(Y)) + v(Y) Y^N = Y^d$$

and

$$\begin{aligned} u(Y) X^{a_i}(Y^{b_i} + G(Y)) + v(Y) X^{a_i} Y^N &= Y^d X^{a_i}, \\ u(Y) X^{a_i+1} H(X,Y) + Y^d X^{a_i} &\equiv 0 \ (\operatorname{mod} I). \end{aligned}$$

Notice that

$$u(Y) X^{a_i+1} H(X,Y) \equiv \sum_{\substack{c \geq a_i+1 \\ d < b_i}} k_{cd} X^c Y^d \ (\operatorname{mod} I).$$

This implies that $u(Y) X^{a_i+1} H(X,Y) + Y^d X^{a_i} \neq 0$ and cannot be reduced to zero via $RGB(I)$. As before, this is impossible. The theorem is completely proved. □

For an ideal I of the ring R, if $RGB(I) = \{f(x), g(x,y)\}$ and the extension ideal of I $I^e = \bigcap_{i=0}^{t} I_i$ in the ring $K[x,y]$, where K is an extension field of F, with the set of zero points of I_i having only one element for each i over K, then we can prove that the reduced Gröbner basis of I_i consists of two polynomials for each i also and in the next section we will see that it is easy to show a basis of the linear space $G(I_i)$ for this type of I_i and, furthermore, we can obtain a basis of $G(I)$ by starting with a basis of $G(I_i)$.

Theorem 2.2. *Let I be an ideal of the ring R and $RGB(I) = \{f(x), g(x,y)\}$ where $f(x)$ and $g(x,y)$ are two polynomials of the ring R. Furthermore, suppose that K is an extension field of F such that for the extension ideal I^e of I in the ring $K[x,y]$ its minimal primary decomposition $I^e = \bigcap_{i=0}^{t} I_i$ with the set of zero points of I_i having only one element for each i over K. Then $RGB(I_i)$ consists of two polynomials for each i also.*

Proof. Without loss of generality we can suppose that I is an ideal of the ring $K[x,y]$ and $f(x) = (x-\alpha)^m$, where α is a non-zero element of K. If $g(\alpha,y) = \prod_j (y - \beta_j)^{n_j}$ over K, where the β_j are different and non-zero, then there is a positive integer k such that $q^k \geq m$, and $g(x,y)^{q^k} \equiv g(\alpha,y)^{q^k} \ (\operatorname{mod} (x-\alpha)^{q^k})$ which means that $g(\alpha,y)^{q^k} \in I$. Suppose $I \bigcap K[y] = \langle G(y) \rangle$, i.e. the ideal $\langle G(y) \rangle$ is generated by $G(y)$.

Thus, $G(y)|g(\alpha,y)^{q^k}$ which implies that $G(y)=\prod_j(y-\beta_j)^{l_j}$ and $I=\bigcap_j\langle(y-\beta_j)^{l_j},I\rangle$. Let $I_j=\langle(y-\beta_j)^{l_j},I\rangle$, and $I_j\bigcap K[x]=\langle(x-\alpha)^{m_j}\rangle$. Then $m_j\le m$. Suppose $RGB(I_j)=\{(x-\alpha)^{m_j},f_1^{(j)}(x,y),\ldots,f_{t_j}^{(j)}(x,y)\}$ with $Lt(f_i^{(j)})\prec Lt(f_{i+1}^{(j)})$ and $\deg_y f_{t_j}^{(j)}=N_j$. Then

$$\dim G(I_j)\le m_jN_j \tag{2.1}$$

and $\dim G(I_j)=m_jN_j$ iff $|RGB(I_j)|=2$, i.e. $RGB(I_j)$ consists of two elements. As

$$\sum_j m_jN_j\ge\sum_j\dim G(I_j)=\dim G(I)=m\deg_y g(x,y)=m\sum_j n_j\ge\sum_j m_jn_j, \tag{2.2}$$

if we can prove for each j, $N_j\le n_j$, then $m=m_j, n_j=N_j$ and $\dim G(I_j)=m_jN_j$. It implies $|RGB(I_j)|=2$ from (2.1) and (2.2). Theorem 2.2 is proved. It is easy to see that $g(\alpha,y)\in\bigcap_j\langle f_{t_j}^{(j)}(\alpha,y)\rangle$. As I_j has only one zero point (α,β_j) and the β_j are different, $\prod_j f_{t_j}^{(j)}(\alpha,y)|g(\alpha,y)$, $N_j\le n_j$. $\Box$

Usually, for an ideal I of the ring R, even if $RGB(I^e)=RGB(I)$ and $I^e=\bigcap_j I_j$, we cannot say anything about $RGB(I_j)$, as we only know that $I_j\supset I^e\supset I$.

The next theorem will show us when an ideal generated by two polynomials $f(x)$ and $g(x,y)$ contains x^r-1 and y^s-1 for some positive integers r and s .

Theorem 2.3. *Suppose that I is an ideal of the ring R generated by two polynomials $f(x)$ and $g(x,y)$. Then I contains x^r-1 and y^s-1 for some positive integers* r *and* s *iff $f(0)\ne 0$ and* $\gcd(f(x),g(x,0))=1$.

Proof. If I contains x^r-1 and y^s-1, then $f(x)|x^r-1, f(0)\ne 0$. Suppose $y^s-1=a(x,y)f(x)+b(x,y)g(x,y)$ where $a(x,y),b(x,y)\in R$. Then $-1=a(x,0)f(x)+b(x,0)g(x,0)$, i.e. $\gcd(f(x),g(x,0))=1$.

On the other hand, if $f(0)\ne 0$ and $\gcd(f(x),g(x,0))=1$, then there is a positive integer r such that $f(x)|x^r-1$ and there are two polynomials $a(x)$ and $b(x)$ such that $a(x)f(x)+b(x)g(x,0)=1$. Suppose $g(x,y)=g(x,0)+yh(x,y)$. Then $yb(x)h(x,y)\equiv 1 \pmod I$. It implies that there is a positive integer s such that $y^s-1\equiv 0 \pmod I$, i.e. $y^s-1\in I$. $\Box$

3. A Basis of the Space of Linear Recurring Arrays

Let K be a finite extension field of F, I a zero-dimensional ideal of the ring $K[x,y]$ and $G(I)$ the linear space of linear recurring arrays over K determined by I. Let the radical ideal of $I\sqrt{I}$ have only one zero point (α,β) where α and β are two non-zero elements of K. In this section we give a basis of $G(I)$ that we apply for giving the trace expression of linear recurring arrays over the base field F in the next section.

Let

$$\binom{n}{r}=\frac{n(n-1)\cdots(n-r+1)}{r(r-1)\cdots 1} \pmod p,$$

where n is an integer, r a positive integer, $p=char\,F$. By convention $\binom{n}{0}=1$. Let the sequence $S^{(t)}=\left(\binom{i}{t}\right)_{i\in Z}$ where t is a non-negative integer and define for $k=(k_1,k_2)\in Z_+^2$ an array $A^{(k)}$ as follows:

$$A^{(k)}=A^{(k_1,k_2)}=(\alpha^{i-k_1}\beta^{j-k_2}S_i^{(k_1)}S_j^{(k_2)})_{(i,j)\in Z^2},$$

where α and β are two non-zero elements of K.

Lemma 3.1.

$$(x-\alpha)^i(y-\beta)^j A^{(k_1,k_2)} = \begin{cases} A^{(k_1-i,k_2-j)}, & \textit{if } k_1 \geq i, k_2 \geq j \\ 0, & \textit{otherwise.} \end{cases}$$

Let H be a subset of the ring R. Then $\langle H \rangle$ denotes the ideal of R generated by H.

Remark 3.2. The sequences $S^{(t)}$ above are translations of Zierler's corresponding sequences (Zierler and Mills, 1973).

Lemma 3.3. *Let I be an ideal of the ring $K[x,y]$ where $I = \langle (x-\alpha)^a, (y-\beta)^b \rangle$. Then the set $\{A^{(k_1,k_2)} | 0 \leq k_1 < a_1, 0 \leq k_2 < b\}$ is a basis of the space $G(I)$.*

Suppose $f(X,Y) = Y^b - g(X,Y)$ where $X = x-\alpha, Y = y-\beta$, $\deg_X g > 0$ and $\deg_Y g < b$. Define an action of the operator ϕ_f on $A^{(k)}$ as follows:

$$\phi_f(A^{(k)}) = \sum_{i \in Z_+} g(X,Y)^i A^{(k)+i(0,b)}. \tag{3.1}$$

Notice that there are only finitely many summands in (3.1).

Lemma 3.4. *Let I be an ideal of the ring $K[x,y]$ and $X = x-\alpha, Y = y-\beta$,*

$$RGB(I) = \{X^a, f(X,Y) = Y^b - g(X,Y)\},$$

and $\deg_X g > 0, \deg_Y g < b$.
Then

1. *$f(X,Y)\phi_f(A^{(k)}) = A^{(k)-(0,b)}$.*
2. *Let $B^{(k)} = \phi_f(A^{(k)})$. Then the set*

$$B = \{B^{(k)} \mid k = (k_1,k_2), 0 \leq k_1 < a, 0 \leq k_2 < b\}$$

is a basis of the linear space G(I).

Proof. (1)

$$\begin{aligned} f(X,Y)\phi_f(A^{(k)}) &= (Y^b - g(X,Y)) \sum_{i \geq 0} g(X,Y)^i A^{(k)+i(0,b)} \\ &= \sum_{i \geq 0} g(X,Y)^i A^{(k)+(i-1)(0,b)} - \sum_{i \geq 0} g(X,Y)^{i+1} A^{(k)+i(0,b)} \\ &= A^{(k)-(0,b)}. \end{aligned}$$

(2) It is easy to check that $X^a\phi_f(A^{(k)}) = 0$, and $f(X,Y)\phi_f(A^{(k)}) = A^{(k)-(0,b)} = 0$.

Hence, $B^{(k)} = \phi_f(A^{(k)}) \in G(I)$. Furthermore, B is a linearly independent set over F. In fact, if there are α_k such that $\sum_k \alpha_k B^{(k)} = 0$, i.e.

$$\sum_k \alpha_k \Big(\sum_{i \geq 0} g(X,Y)^i A^{(k)+i(0,b)} \Big) = 0$$

then obviously

$$X^{a-1} \sum_k \alpha_k \Big(\sum_{i \geq 0} g(X,Y)^i A^{(k)+i(0,b)} \Big) = 0.$$

It follows that $\alpha_{(a-1,j)} = 0$ for $j = 1, 2, \ldots, (b-1)$. In the same way it is easy to prove

$\alpha_k = 0$ for all k. Notice that $\dim G(I) = ab = |B|$ where $|B|$ denotes the number of elements of the set B. Hence (2) holds. □

Let W' be a linear space generated by the arrays $A^{(k)}$, where $k \in Z_+^2$, over K. Define an action of the lifting operator ψ^l on W' as follows:

$$\psi^l\Big(\sum_k a_k A^{(k)}\Big) = \sum_k a_k A^{(k+l)},$$

where $l \in Z_+^2$.

Lemma 3.5. *Let $D \in W', f(X,Y) \in R, l = (l_1, 0)$. Then*

$$f(\psi^l(D)) = \psi^l(fD) + \sum_{k_1 < l_1} c_k A^{(k)},$$

where $k = (k_1, k_2)$ and c_k are uniquely determined by l_1, f, and D.

Notice that the operator ψ and $f(X,Y)$ are non-commutative.

Let I be an ideal of the ring $K[x,y]$ and

$$RGB(I) = \{X^{a_0}, X^{a_1}h_1(X,Y), X^{a_2}h_2(X,Y), \ldots, X^{a_r}h_r(X,Y)\},$$

where $X = x - \alpha$, $Y = y - \beta$, $h_i(X,Y) = Y^{b_i} - g_i(X,Y)$, $\deg_X g_i \geq 1$, $\deg_Y g_i < b_i$, $Lt(X^{a_i}h_i(X,Y)) \prec Lt(X^{a_{i+1}}h_{i+1}(X,Y))$, $i = 1, 2, \ldots, r$. Let

$$J_i = \langle X^{a_0 - a_i}, X^{a_1 - a_i}h_1, \ldots, X^{a_{i-1} - a_i}h_{i-1}, h_i\rangle.$$

It is obvious that

$$RGB(J_i) = \{X^{a_0 - a_i}, X^{a_1 - a_i}h_1, \ldots, X^{a_{i-1} - a_i}h_{i-1}, h_i\}.$$

Lemma 3.6. *For $1 \leq i \leq r - 1, h_{i+1}(X,Y) \in J_i$.*

Proof. Suppose $f_i(X,Y) = X^{a_i}h_i(X,Y)$ for each i. Consider the S-polynomial of f_{i+1} and f_i

$$S(f_{i+1}, f_i) = X^{(a_i - a_{i+1})}X^{a_{i+1}}h_{i+1} - X^{a_i}Y^{b_{i+1} - b_i}h_i \in \langle f_0, f_1, \ldots, f_i\rangle.$$

Hence $h_{i+1}(X,Y) \in J_i$. □

For $r = 1$ we have already obtained a basis of $G(I)$in Lemma 3.4 . In the following we will construct a basis of $G(I)$ for $r > 1$ by induction on r which is more complicated than the case when $r = 1$.

Define $\Gamma_1 = \{k = (k_1, k_2) \mid 0 \leq k_1 < a_0 - a_1, 0 \leq k_2 < b_1\}$ and for $k \in \Gamma_1, \phi_{J_1}(A^{(k)}) = \phi_{h_1}(A^{(k)})$ which is given in (3.1). Define $\phi_{J_r}(A^{(k)})$ by induction on r when $r > 1$.

For $i = 2, \ldots, r$, let $\Gamma_i = \Gamma_{i_1} \bigcup \Gamma_{i_2}$, where

$$\begin{aligned} &\Gamma_{i_1} = \{k = (k_1, k_2) \mid 0 \leq k_1 < a_{i-1} - a_i, 0 \leq k_2 < b_i\}, \\ &\Gamma_{i_2} = (a_{i-1} - a_i, 0) + \Gamma_{i-1}. \end{aligned} \tag{3.2}$$

Suppose that $\phi_{J_1}, \phi_{J_2}, \ldots, \phi_{J_{i-1}}$ are defined. Then for $k \in \Gamma_{i_1}$, we define

$$\phi_{J_i}(A^{(k)}) = \phi_{h_i}(A^{(k)}) = \sum_{j \geq 0} g_i(X,Y)^j A^{(k)+j(0,b)}, \tag{3.3}$$

for $k \in \Gamma_{i_2} = (a_{i-1} - a_i, 0) + \Gamma_{i-1}$, we define

$$\phi_{J_i}(A^{(k)}) = \psi^{(c_{i-1},0)}\phi_{J_{i-1}}(A^{(k)-(c_{i-1},0)}) - \phi_{h_i}(\psi^{(0,b_i)}h_i)\psi^{(c_{i-1},0)}\phi_{J_{i-1}}(A^{(k-(c_{i-1},0))}) \tag{3.4}$$

where we let $c_{i-1} = a_{i-1} - a_i$. Now we can state the main theorem of this section.

THEOREM 3.7. *Let I be a zero-dimensional ideal of the ring $K[x,y]$ and $\sqrt{I} = \langle X, Y\rangle$, where $X = x-\alpha, Y = y-\beta$. Then the reduced Gröbner basis of I has the following properties:*

$$RGB(I) = \{X^{a_0}, X^{a_1}h_1(X,Y), X^{a_2}h_2(X,Y), \ldots, X^{a_r}h_r(X,Y)\},$$

and for $i = 1,\ldots,r$, $h_i(X,Y) = Y^{b_i} - g_i(X,Y)$, $\deg_X g_i \geq 1$, $\deg_Y g_i < b_i$, $Lt(X^{a_i}h_i(X,Y)) \prec Lt((X^{a_{i+1}}h_{i+1}(X,Y))$. Let $\phi_I(A^{(k)}) = \phi_{J_r}(A^{(k)})$ be defined by (3.3) and (3.4), and $\Gamma(I) = \Gamma_r$ by (3.2). Then the set $\{\phi_I(A^{(k)}) \mid k \in \Gamma(I)\}$ is a basis of the linear space $G(I)$ of linear recurring arrays determined by the ideal I.

PROOF. The first statement is obvious by Theorem 2.1.

Prove the second by induction on r. For $r = 1$, it is obvious by Lemma 3.4. Suppose that for $r = 1, 2, \ldots, i-1$ the theorem is true; we will prove that it is also true for $r = i$. First we claim that $\phi_{J_i}(A^{(k)}) \in G(J_i)$.

For $k \in \Gamma_{i_1}$, it is easy to see that

$$h_i(\phi_{J_i}(A^{(k)})) = A^{(k)-(0,b_i)} = 0$$

and

$$X^{a_j-a_i}h_j\phi_{J_i}(A^{(k)}) = 0 \text{ where } j \leq i-1.$$

For $k \in \Gamma_{i_2}$, let $D_k = \psi^{(c_{i-1},0)}\phi_{J_{i-1}}(A^{(k)-(c_{i-1},0)})$. From Lemmas 3.5 and 3.6, $h_i(D_k) = \sum_{u<c_{i-1}} \alpha_{uv}A^{(u,v)}$. This implies

$$\begin{aligned}\phi_{h_i}(\psi^{(0,b_i)}h_i(D_k)) &= \phi_{h_i}\Big(\psi^{(0,b_i)} \sum_{u<c_{i-1}} \alpha_{uv}A^{(u,v)}\Big)\\ &= \phi_{h_i}\Big(\sum_{u<c_{i-1}} \alpha_{uv}A^{(u,v)+(0,b_i)}\Big).\end{aligned}$$

Hence, $h_i(\phi_{h_i}(\psi^{(0,b_i)}h_i(D_k))) = h_i(D_k)$ and $h_i\phi_{J_i}(A^{(k)}) = 0$. Furthermore, for $j \leq i-1$, as $h_i\phi_{J_{i-1}}(A^{(k)-(c_{i-1},0)}) = 0$ and $X^{a_j-a_i}\sum_{u<c_{i-1}} \alpha_{uv}A^{(u,v)} = 0$, we have

$$\begin{aligned}X^{a_j-a_i}h_j\phi_{J_i}(A^{(k)}) &= X^{a_j-a_i}h_j((D_k) - \phi_{h_i}(\psi^{(0,b_i)}h_i(D_k)))\\ &= X^{a_j-a_i}h_j((D_k) - \phi_{h_i}(\psi^{(0,b_i)}(\psi^{(c_{i-1},0)}h_i\phi_{J_{i-1}}(A^{(k)-(c_{i-1},0)})\\ &\quad + \sum_{u<c_{i-1}} \alpha_{uv}A^{(u,v)})))\\ &= X^{a_j-a_i}h_j(D_k)\\ &= 0\end{aligned}$$

by the induction hypothesis, Lemma 3.6, and $a_j - a_i \geq c_{i-1}$. Hence $\phi_{J_r}(A^{(k)}) \in G(I)$. Secondly, we claim that the sets $B_i = \phi(J_i)$, $i \in 1, 2, \ldots, r$, are linearly independent. We prove it also by induction on i. For $i = 1$, it follows from Lemma 3.4. Suppose that it is true for $i-1$, and there are $\alpha_k, k \in \Gamma_i$, such that

$$\sum_{k\in\Gamma_{i_1}} \alpha_k\phi_{J_i}(A^{(k)}) + \sum_{k\in\Gamma_{i_2}} \alpha_k\phi_{J_i}(A^{(k)}) = 0.$$

Obviously
$$X^{a_{i-1}-a_i}\Big(\sum_{k\in\Gamma_{i_1}}\alpha_k\phi_{J_i}(A^{(k)})+\sum_{k\in\Gamma_{i_2}}\alpha_k\phi_{J_i}(A^{(k)})\Big)=0.$$
By Lemma 3.1
$$X^{a_{i-1}-a_i}\sum_{k\in\Gamma_{i_2}}\alpha_k\phi_{J_i}(A^{(k)})=0.$$
That is
$$X^{a_{i-1}-a_i}\sum_{k\in\Gamma_{i_2}}\alpha_k(D_k-\phi_{h_i}(\psi^{(0,b_i)}h_i(D_k)))=0.$$
As
$$h_i(D_k)=\sum_{u<c_{i-1}}a_{uv}A^{(u,v)}$$
and by Lemma 3.4,
$$\begin{aligned}X^{a_{i-1}-a_i}\sum_{k\in\Gamma_{i_2}}\alpha_kD_k&=X^{a_{i-1}-a_i}\sum_{k\in\Gamma_{i_2}}\alpha_k(\psi^{(c_{i-1},0)}\phi_{J_{i-1}}(A^{(k)-(c_{i-1},0)}))\\&=X^{a_{i-1}-a_i}\sum_{k\in\Gamma_{i_2}}\alpha_k\phi_{J_{i-1}}(A^{(k)})\\&=\sum_{k\in\Gamma_{i_2}}\alpha_k\phi_{J_{i-1}}(A^{(k)-(c_{i-1},0)})\\&=0\end{aligned}$$
this implies
$$\sum_{k\in\Gamma_{i-1}}\alpha_k\phi_{J_{i-1}}(A^{(k)})=0.$$
By the induction hypothesis $\alpha_k=0$ for all $k\in\Gamma_{i_2}$. Hence,
$$\sum_{k\in\Gamma_{i_1}}\alpha_k\phi_{J_i}A^{(k)}=0.$$
It follows immediately that $\alpha_k=0$ for all $k\in\Gamma_{i_1}$ from Lemma 3.4. Finally, the dimension of $G(I)$, $\dim G(I)=|\{\phi_{J_r}(A^{(k)})\mid k\in\Gamma_r\}|$, the number of elements of the set. The theorem holds. □

4. The Trace Expression of Linear Recurring Arrays

All ideals considered will be zero-dimensional. In this section we give the trace expression of linear recurring arrays, also written LRA in short, by using the basis of $G(I)$ that is given in the above section.

Let I be a primary ideal of the ring $R=F[x,y], P=\sqrt{I}$ the radical ideal of I, and $V(P)$ be the set of zero points of P in an extension field K of F where
$$V(P)=\{(\alpha,\beta),(\alpha^q,\beta^q),\ldots,(\alpha^{q^{l-1}},\beta^{q^{l-1}})\},$$
and where $\alpha,\beta\in K$, $l=[F[\alpha,\beta]:F]$. Consider the extension ideal I^e of I in the ring

$K[x, y]$. There is minimal primary decomposition in the ring $K[x, y]$

$$I^e = \bigcap_{i=0}^{t} I_i, P_i = \sqrt{I}_i,$$

where for each i, I_i is primary, and

$$V(P_i) = \{(\alpha^{q^i}, \beta^{q^i})\}, P_i = \langle x - \alpha^{q^i}, y - \beta^{q^i} \rangle.$$

Consider the map $\xi : K[x, y] \to K[x, y]$ defined by

$$\xi\Big(\sum_{k \in Z_+^2} f_k z^k\Big) = \sum_{k \in Z_+^2} f_k^q z^k.$$

Then the map ξ has the following properties.

Lemma 4.1.

(1) ξ is an automorphism of $K[x, y]$.
(2) For an ideal I of $K[x, y], I$ is prime (primary) iff $\xi(I)$ is prime (primary).
(3) $\xi(P_i) = P_{(i+1)}$ and $\xi(I_i) = \xi(I_{i+1})$ for $i = 0, 1, \ldots, t-1$.

Proof. (1) and (2) are obvious.
(3) Consider

$$\begin{aligned}\xi(P_i) &= \xi\langle x - \alpha^{q^i}, y - \beta^{q^i} \rangle \\ &= \langle x - \alpha^{q^{i+1}}, y - \beta^{q^{i+1}} \rangle = P_{i+1}.\end{aligned}$$

As $\dim P_i = 0$, P_i is maximal and I_i is uniquely determined by I and P_i. It is known that $\xi(I^e) = I^e$, hence, $\xi(I_i) = I_{i+1}$. □

Furthermore, the automorphism ξ of $K[x, y]$ induces an automorphism of the linear space $W(K)$ of arrays over K, also written ξ, defined by $\xi(A) = A^q$, where $A = (A_i)$, $A^q = (A_i^q)$.

Lemma 4.2. *Let I be an ideal of $K[x, y]$. Then $G(\xi(I)) = \xi G(I)$.*

Proof. It is easy to check. □

Lemma 4.3. $G(I^e) = \bigoplus_{i=0}^{t} \xi^i(G(I_0))$.

Theorem 4.4. *Suppose that I is a primary ideal of the ring $R = F[x, y]$ and the set of zero points of I*

$$V(I) = \{\ (\alpha, \beta), (\alpha^q, \beta^q), \ldots, (\alpha^{q^{l-1}}, \beta^{q^{l-1}})\},$$

where $\alpha, \beta \in K \setminus \{0\}$. Let

$$I^e = \bigcap_{i=0}^{t} I_i, P_i = \sqrt{I}_i,$$

be a minimal primary decomposition of the extension ideal I^e of I in the ring $K[x, y]$ with

$$V(P_i) = \{(\alpha^{q^i}, \beta^{q^i})\}, \quad P_i = \langle x - \alpha^{q^i}, y - \beta^{q^i} \rangle.$$

Then for any array $D = (D_i)_{i\in Z^2} \in G(I)$ *there are* $u_k \in F[\alpha, \beta]$, $k \in Z_+^2$ *such that*

$$D_i = \sum_{k\in\Gamma(I_0)} Tr_{K/F}(u_k B_i^{(k)}),$$

where $i = (i_1, i_2)$, $B^{(k)} = \phi_{I_0}(A^{(k)})$, *and the set* $\{B^{(k)} \in W(K) \mid k \in \Gamma(I_0)\}$ *is a basis of* $G(I_0)$.

Proof. As $\sqrt{I_0} = \langle x - \alpha, y - \beta\rangle$, the set $\{B^{(k)} \mid k \in \Gamma(I_0)\}$ is a basis of $G(I_0)$ by Theorem 3.7 and $\xi^r G(I_0)$ has a basis $\{(B_i^{(k)})^{q^r} \mid k \in \Gamma(I_0)\}$ for $r = 1, 2, \ldots, t$. Hence, $G(I^e)$ has a basis

$$\{(B_i^{(k)})^{q^r} \mid k \in \Gamma(I_0), r = 1, \ldots, t\}.$$

For any array $D \in G(I)$ there exists $u_{k,r} \in K$ such that

$$D = (D_i), \quad D_i = \sum_{r=1}^{t} \sum_{k\in\Gamma(I_0)} u_{k,r}(B_i^{(k)})^{q^r}.$$

As $D_i \in F, D_i^q = D_i$, and

$$\sum_r (u_{k,r})^q (B_i^{(k)})^{q^{r+1}} = \sum_r u_{k,r}(B_i^{(k)})^{q^r}$$

for all $i \in Z^2$, it follows that $u_{k,r+1} = (u_{k,r})^q = (u_{k,0})^{q^r}$. Hence

$$D_i = \sum_{k\in\Gamma(I_0)} Tr_{K/F}(u_{k,0} B_i^{(k)}).$$

The theorem is completely proved. □

As any ideal of the ring $R' = S^{-1}F[x, y]$ is finitely generated by some polynomials of the ring $R = F[x, y]$, in order to obtain the trace expression for $G(I)$, where I is any ideal of the ring R', it is enough to consider any ideals of the ring R. Now we can state the main theorem of this section.

Theorem 4.5. (Trace Expression) *Suppose that* J *is an ideal of* R', $J = S^{-1}I$, *where* I *is an ideal of the ring* $R = F[x, y]$ *and* $I = \cap_{j=1}^t I_j$ *is a minimal primary decomposition in the ring R, for each* $j = 1, \ldots, t$, *the set of zero points of* I_j

$$V(I_j) = \{(\alpha_j, \beta_j), (\alpha_j^q, \beta_j^q), \ldots, (\alpha_j^{q^{l_j-1}}, \beta_j^{q^{l_j-1}})\}, \quad l_j = [F[\alpha_j, \beta_j] : F], \alpha_j, \beta_j \in K$$

where K *is a suitable extension field of* F. *The* $(I_j)_0$ *is a primary component of the minimal primary decomposition of the extension ideal* I_j^e *of* I_j *in* $K[x, y]$ *with* $V((I_j)_0) = \{(\alpha_j, \beta_j)\}$. *Then, for any* $D = (D_i) \in G(J)$,

$$D_i = \sum_{j=1}^{t} \sum_{k_j\in\Gamma((I_j)_0)} Tr_{K/F}(u_{k_j,0} B_i^{(k_j)}),$$

where the set $\{B^{(k_j)} = \phi_{(I_j)_0}(A^{(k_j)}) \mid k_j \in \Gamma((I_j)_0)\}$ *is a basis of*$G((I_j)_0)$.

Proof. From Theorem 4.4. □

Definition 4.6. *We call the above formula the trace expression of D.*

Corollary 4.7. *Suppose that* $s = (s_i)_{i\in Z_+}$ *is a periodic sequence over* F, $f(x)$ *is a polynomial of the ring* $F[x], f(x) = p_1^{e_1}(x)\cdots p_t^{e_t}(x)$ *is its unique factorization in* $F[x]$, *the zero set of* $P_i(x)$ *is* $V(p_i) = \{\alpha_i, \alpha_i^q, \dots, \alpha_i^{q^{l_i-1}}\}$ *where* $\alpha_i \in K, l_i = [F[\alpha_i] : F]$. *Let* $s \in G(f)$. *Then*

$$s_i = \sum_{j=1}^{t}\sum_{k_j=0}^{e_{l_j}-1}\binom{i}{k_j}Tr(u_{k_j}\alpha_j^i).$$

Remark 4.8. The result above is a translation of the trace expression of the sequence $s = (s_i)_{i\in Z_+}$ in Zierler and Mills (1973).

In fact, we can directly prove the above corollary by the same idea that was used in the case of arrays. We only need to see that if $p(x) = \prod_{i=0}^{n-1}(x-\alpha^{q^i})$, where $n = \deg p(x)$, then

$$G(p^e(x)) = G((x-\alpha)^e) \oplus G((x-\alpha^q)^e) \oplus \cdots \oplus G((x-\alpha^{q^{n-1}})^e).$$

Corollary 4.9. *Suppose that* P *is a prime ideal of the ring* $F[x, y]$ *and the zero set of* P

$$V(P) = \{(\alpha, \beta), (\alpha^q, \beta^q), \dots, (\alpha^{q^{l-1}}, \beta^{q^{l-1}})\},$$

where K *is a suitable extension field of* F *and* α *and* β *are two non-zero elements of* K. *Then, for any* $D = (D_i) \in G(P)$,

$$D_i = Tr_{F[\alpha,\beta]/F}(u\alpha^{i_1}\beta^{i_2}),$$

where $i = (i_1, i_2)$, $u \in F[\alpha, \beta]$.

Proof. As $P = \bigcap_{j=0}^{l-1}\langle x-\alpha^{q^j}, y-\beta^{q^j}\rangle$, the corollary holds by Theorem 4.4. □

Remark 4.10. This is a result of Lin and Liu (1993a).

Corollary 4.11. *Suppose that* I *is an ideal of* $R = F[x, y]$, $RGB(I) = \{f_0(x), f_1(x, y)\}$, $I = \bigcap_{i=1}^{t} I_i$ *is a minimal primary decomposition in the ring* R *and the zero set of* $I_jV(I_j) = \{(\alpha_j^{q^t}, \beta_j^{q^t}) \mid t = 1, 2, \dots, l_j\}$. $RGB(I_j) = \{(x-\alpha_j)^{a_j}, f(x-\alpha_j, y-\beta_j) = (y-\beta_j)^{b_j} + g(x-\alpha_j, y-\beta_j)\}$. *Then for any* $D = (D_i)_{i\in Z^2} \in G(I)$

$$D_i = \sum_{j=1}^{t}\sum_{k_j\in\Gamma((I_j)_0)} Tr_{F[\alpha_j,\beta_j]/F}(u_{k_j,0}B_i^{(k_j)}).$$

where $B^{(k_j)} = \phi_f(A^{(k_j)})$. *Particularly, if* $RGB(I_j) = \{(x-\alpha_j)^{a_j}, (y-\beta_j)^{b_j}\}$ *then*

$$D_i = \sum_{j=1}^{t}\sum_{\substack{0\le(k_j)_1<a_j\\0\le(k_j)_2<b_j}}\binom{i_1}{(k_j)_1}\binom{i_2}{(k_j)_2}Tr_{K/F}(v_{k_j}(\alpha_j^{i_1}\beta_j^{i_2})),$$

where $v_{k_j} = u_{k_j,0}\alpha_j^{-(k_j)_1}\beta_j^{-(k_j)_2}$.

5. Conclusion

In this paper, on the basis of a detailed characterization of the reduced Gröbner basis for the ring R of Laurent polynomials in two variables, we have given an explicit basis of the linear space $G(I)$ consisting of linear recurring arrays determined by I. Moreover, we have given a trace expression of linear recurring arrays over F by using the basis.

It is much more complicated than the trace expression of linear recurring sequences over F. The trace expression of linear recurring arrays can be applied to study the structures of linear recurring arrays as R-modules and linear spaces over F, and their Hadamard products, and to calculate the number of the translation equivalence classes of linear recurring arrays and others. In fact, we have applied our results and obtained the necessary and sufficient conditions for the modules of doubly periodic arrays to be cyclic.

Acknowledgements

Finally the authors thank the referees for their very helpful comments and Dr Ethel Wheland for correcting our English.

References

Lin, D. (1993). The characteristic pair and trace expression of linear recurring arrays. *Syst. Sci. Math. Sci.*, **6**, 150–160.

Lin, D., Liu, M. (1993a). Structure and properties of linear recurring m-arrays. *IEEE Trans. Inf. Theory*, **3**, 1758–1762.

Lin, D., Liu, M. (1993b). The equivalent classes of LR arrays. *Discr. Appl. Math.*, **43**, 47–61.

Liu, M., Hu, L. (1994). *Gröbner Basis and Linear Recurring Arrays.* Chinacrypt'94, Beijing, Academic Press.

Liu, M., Li, J. (1993). Coset correlation of linear recurring m-arrays. *Discr. Appl. Math.*, **47**, 263–273.

MacWilliams, F.J., Sloane, N.J.A. (1976). Pseude-random sequences and arrays. *Proc. IEEE*, **64**, 1715–1729.

Nomura, T., Miyakawa, H., Imai, H., Fukuda, A. (1972). A theory of two-dimensional linear recurring arrays. *IEEE Trans. Inf. Theory*, **18**, 775–785.

Sakata, S. (1978). General theory of doubly periodic arrays over an arbitrary finite field and its applications. *IEEE Trans. Inf. Theory*, **24**, 719–730.

Sakata, S. (1988). On determining the independent point set for doubly periodic arrays and encoding two-dimensional cyclic codes and their duals. *IEEE Trans. Inf. Theory*, **27**, 556–565.

Siu, M.K. (1985). M-arrays and m-arrays. Preprint.

Van Lint, J.H., MacWilliams, F.J., Sloane, N.J.A. (1979). On the pseudo-random arrays. *SIAM J.Appl. Math.*, **36**, 62–72.

Zierler, N., Mills, W. (1973). Products of linear recurring sequences. *J. Algebra*, **27**, 147–157.

Originally received 6 December 1995
Accepted 18 March 1998