数理解析研究所講究録
941 巻 1996 年 1-6

1.

On Solving the Initial Problem of LR Arrays

Dongdai Lin(日大・理工)
小林英恒 (日大・理工)

Let $\mathbf{F_q}$ be a finite field with q elements. By an array A of dimension 2, we mean an infinite matrix $A=(a_{ij})_{i\geq 0,j\geq 0}$ over $\mathbf{F_q}$. If there exist two positive integer r and s such that

$$a_{i+r,j}=a_{ij}=a_{i,j+s} \qquad i\geq 0, j\geq 0$$

then we say that A is a periodic array. Furthermore, if r, s are the smallest positive integers for which above condition is satisfied, we call A an array of period $r\times s$.

An $m\times n$ submatrix $A(i,j)=(a_{i+i',j+j'})_{0\leq i'<m,0\leq j'<n}$ of A is called $m\times n$ window of A at (i,j). $\overline{A}(i,j)$ is the row vector $(a_t)_{0\leq t<mn}$ of dimension mn, where $a_t=a_{i+i',j+j'}$, i'=the integer part $\left[\frac{t}{n}\right]$ of $\frac{t}{n}$, and $j'=t-n\left[\frac{t}{n}\right]$. The entry a_{ij} of A is called $(i,j)-$component of A.

Definition 1: Let $A=(a_{ij})_{i\geq 0,j\geq 0}$, $B=(b_{ij})_{i\geq 0,j\geq 0}$ be two arrays. If there exist two non-negative integers c, d such that

$$b_{ij}=a_{i+c,j+d} \qquad for\ all\ i\geq 0,\ j\geq 0$$

then B is called (c,d)-translation of A, denoted by $B=A_{c,d}$.

Definition 2: Let $A=(a_{ij})_{i\geq 0,j\geq 0}$ be an array, m and n be two positive integers. If there exist two mn by mn matrices over $\mathbf{F_q}$ of the following form

$$T_v = \begin{pmatrix} 0 & 0 & \cdots & 0 & t_{0,0} & \cdots & t_{0,n-1} \\ 0 & 0 & \cdots & 0 & t_{1,0} & \cdots & t_{1,n-1} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & t_{n-1,0} & \cdots & t_{n-1,n-1} \\ 1 & 0 & \cdots & 0 & t_{n,0} & \cdots & t_{n,n-1} \\ 0 & 1 & \cdots & 0 & t_{n+1,0} & \cdots & t_{n+1,n-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 & t_{mn-1,0} & \cdots & t_{mn-1,n-1} \end{pmatrix}$$

$$T_h = \begin{pmatrix} 0 & 0 & \cdots & 0 & r_{0,0} & 0 & \cdots & 0 & r_{0,1} & \cdots & 0 & \cdots & 0 & r_{0,m-1} \\ 1 & 0 & \cdots & 0 & r_{1,0} & 0 & \cdots & 0 & r_{1,1} & \cdots & 0 & \cdots & 0 & r_{1,m-1} \\ 0 & 1 & \cdots & 0 & r_{2,0} & 0 & \cdots & 0 & r_{2,1} & \cdots & 0 & \cdots & 0 & r_{2,m-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & & \vdots & \vdots & & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & r_{n-1,0} & 0 & \cdots & 0 & r_{n-1,1} & \cdots & 0 & \cdots & 0 & r_{n-1,m-1} \\ 0 & 0 & \cdots & 0 & r_{n,0} & 0 & \cdots & 0 & r_{n,1} & \cdots & 0 & \cdots & 0 & r_{n,m-1} \\ 0 & 0 & \cdots & 0 & r_{n+1,0} & 1 & \cdots & 0 & r_{n+1,1} & \cdots & 0 & \cdots & 0 & r_{n+1,m-1} \\ \vdots & \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & r_{2n-1,0} & 0 & \cdots & 1 & r_{2n-1,1} & \cdots & 0 & \cdots & 0 & r_{2n-1,m-1} \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & r_{mn-n,0} & 0 & \cdots & 0 & r_{mn-n,1} & \cdots & 0 & \cdots & 0 & r_{mn-n,m-1} \\ 0 & 0 & \cdots & 0 & r_{mn-n+1,0} & 0 & \cdots & 0 & r_{mn-n+1,1} & \cdots & 1 & \cdots & 0 & r_{mn-n+1,m-1} \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & r_{mn-1,0} & 0 & \cdots & 0 & r_{mn-1,1} & \cdots & 0 & \cdots & 1 & r_{mn-1,m-1} \end{pmatrix}$$

such that

$$\left.\begin{array}{l} \overline{A}(i,j)T_h = \overline{A}(i,j+1) \\ \overline{A}(i,j)T_v = \overline{A}(i+1,j) \end{array}\right. \quad \text{for all } i,j \geq 0$$

then we call A a linear recurring (or LR in short) array of order $m \times n$ and write $A \in G(T_h, T_v)$.

¿From the definition, we can see that any LR array A of order $m \times n$ is determined by the window $A(0,0)$, we call the window $A(0,0)$(or $\overline{A}(0,0)$) the initial state of A.

Generally speaking, for two given matrices T_h, T_v, the initial state can not be any $m \times n$ matrix over $\mathbf{F_q}$. Sometimes, a non-zero initial state even does not exist. Please see the following examples:

Example 3. Let $m = n = 2$,

$$T_h = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}, T_v = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

Then there is no non-zero 2×2 matrix can be chosen to be an initial state.

Example 4. Let $m = n = 2$,

$$T_h = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, T_v = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

Then we can get an array for $A(0,0) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, but we can not for $A(0,0) = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$.

¿From the above examples, we can see that for two given $mn \times mn$ matrices T_h and T_v, some $m \times n$ matrices can be chosen to be initial states of arrays, while the others can not. The obvious problems are how to determin if a non-zero initial state exists, which m by n matrices can be chosen to an initial state, and how many such legal initial states there are. Furthermore, if the initial state has been given, how to determine the $(i, j)-$components of the array.

Proposition 5 Let T_h, T_v be two given matrices as in Definition 2, $G(T_h, T_v)$ is the set of all arrays generated by T_h, T_v, $A \in G(T_h, T_v)$, then

(1) For any two non-negative integers c and d, $A_{c,d} \in G(T_h, T_v)$.

(2) $G(T_h, T_v)$ is a vector space over $\mathbf{Fq}$ under the usual addition and scalar multiplication, and dim $G(T_h, T_v) \leq mn$.

Let S_A be the set of all arrays over $\mathbf{Fq}$, $t(x,y) = \sum_{(i,j)\in Supp(t)} t_{ij}x^iy^j$ a polynomial over $\mathbf{Fq}$, where $supp(t)$ is the support of $t(x, y)$. Then we can treat $t(x, y)$ as a linear operator from S_A to itself as following

$$t(x,y)A = (\sum_{(I,J)\in Supp(t)} t_{IJ}a_{I+i,J+j})_{i\geq 0, j\geq 0},$$

where $A = (a_{ij})_{i\geq 0, j\geq 0} \in S_A$.

Obviously, $t(x, y)A = \sum_{(I,J)\in Supp(t)} t_{IJ}A_{IJ}$, where A_{IJ} is the (I, J)-translation of A.

Proposition 6 Let $t_1(x, y)$ and $t_2(x, y)$ be two polynomials in $\mathbf{Fq}[x, y]$, $A \in S_A$. Then

$$\begin{aligned} (t_1(x,y) + t_2(x,y))A &= t_1(x,y)A + t_2(x,y)A \\ (t_1(x,y)t_2(x,y))A &= t_1(x,y)(t_2(x,y)A) \\ &= t_2(x,y)(t_1(x,y)A) \end{aligned}$$

Proof By check directly.

Proposition 7 For any polynomial $f(x,y) \in \mathbf{Fq}[\mathrm{x},\mathrm{y}]$, $f(x,y)$ is a linear operator from $G(T_h,T_v)$ to itself.

Proof Seeing that for any $A \in G(T_h,T_v)$, $f(x,y)A = \sum_{(I,J)\in supp(f)} f_{IJ}A_{IJ}$, the proposition is clear by Proposition 5.

Let $T_h,\ T_v$ be two matrices over $\mathbf{Fq}$ as in (2), construct polynomials as follows:

$$\begin{array}{ll} f_k(x,y) = x^k y^n - (\sum_{c=0}^{m-1}\sum_{d=0}^{n-1} r_{cn+d,k}\cdot x^c y^d) & k=0,1,\cdots,m-1 \\ g_k(x,y) = x^m y^k - (\sum_{c=0}^{m-1}\sum_{d=0}^{n-1} t_{cn+d,k}\cdot x^c y^d) & k=0,1,\cdots,n-1 \end{array},$$

and let $PS = \{f_1(x,y),\cdots,f_{m-1}(x,y); g_1(x,y),\cdots,g_{n-1}(x,y)\}$, $< PS >$ be the ideal generated by PS. Then we have

Proposition 8 An array A over $\mathbf{Fq}$ is contained in $G(T_h,T_v)$ if and only if for any polynomials $t(x,y)$ in $< PS >$, we have $t(x,y)A = O$, the zero array.

Let GB be the Gröbner basis of $< PS >$, Δ the Support of $< PS >$ with respect to GB. Then

Theorem 9 Let $A = (a_{ij})_{i\geq 0,j\geq 0} \in G(T_h,T_v)$, $R = \sum_{(k,l)\in\Delta} r_{kl}x^k y^l$ be the normal form of polynomial $x^i y^j$ modulo GB, then $a_{ij} = \sum_{(k,l)\in\Delta} r_{kl}a_{kl}$.

Proof Since $x^i y^j - R \in < PS >$, hence by Proposition 8, we have $(x^i y^j - R)\cdot A = O$, thus $a_{ij} - \sum_{(k,l)\in\Delta} r_{kl}a_{kl} = 0$, i.e. $a_{ij} = \sum_{(k,l)\in\Delta} r_{kl}a_{kl}$.

Proposition 10 For any arbitrary set of values a_{ij} in $\mathbf{Fq}$ for $(i,j)\in\Delta$, there is a unique array $A \in G(T_h,T_v)$ such that $a_{ij}((i,j)\in\Delta)$ are the $(i,j)-$components of A.

Proof Let $R = \sum_{(I,J)\in\Delta} r_{IJ}x^I y^J$ be the normal form of $x^i y^j$ modulo GB. Take $a_{ij} = \sum_{(I,J)\in\Delta} r_{IJ}a_{IJ}$ and $A = (a_{ij})_{i\geq 0,j\geq 0}$. Then $A \in S_A$ and for any polynomial $t(x,y)\in GB$, $t(x,y)A = O$. Since GB is a basis of the ideal $< PS >$, so by Proposition 8, $A \in G(T_h,T_v)$.

The uniqueness is obvious.

Corollary 11 dim $G(T_h,T_v) = |\Delta|$, the number of elements in Δ.

By the discussion above, we can see that any array is determined by the components located in the support of $< PS >$. Generally speaking, for two given matrices as in (1.3), $\overline{\Delta} = \{(i,j)|0 \leq i < m, 0 \leq j < n\}$ is not necessarily the support of the ideal $< PS >$, i.e. there may be a polynomial in $< PS >$ supported by $\overline{\Delta}$ and this polynomial gives a relation among these a_{ij}'s, $(i,j)\in\overline{\Delta}$.

Suppose Δ and $\overline{\Delta}$ have elements arranged in the following order:

$$\Delta : T_0 > T_1 > \cdots > T_{|\Delta|-1},$$

$$\overline{\Delta} : T_0' > T_1' > \cdots > T_{mn-1}',$$

$$Rest(X^I y^J/GB) = \sum_{(i,j)\in\Delta} R_{ij}^{(I,J)} x^i y^j \qquad (I,J)\in\overline{\Delta}.$$

Construct a mn by $|\Delta|$ matrix $M = (m_{ij})_{0\leq i<mn, 0\leq j<|\Delta}$ with $m_{ij} = R^{(I,J)}_{I'J'}$, where $T'_i = (I', J'), T_j = (I, J)$. Then

Theorem 12 An mn-dimensional row vector $\mathbf{u}$ can be chosen to be an initial state of some array of $G(T_h, T_v)$ if and only if there is a $|\Delta|$-dimensional row vector $\mathbf{v}$ such that $\mathbf{u} = \mathbf{Mv}$, where an mn-dimensional row vector $\mathbf{u} = (\mathbf{u_1}, \mathbf{u_2}, \cdots, \mathbf{umn})$ is said to be initial state of array A if

$$A(0,0) = \begin{pmatrix} u_1 & u_{m+1} & \cdots & u_{m(n-1)+1} \\ u_2 & u_{m+1} & \cdots & u_{m(n-1)+2} \\ \vdots & \vdots & \vdots & \vdots \\ u_m & u_{2m} & \cdots & u_{mn} \end{pmatrix}.$$

Proof Use Theorem 9 and Proposition 10.

Proposition 13 Let $t(x, y) \in \mathbf{F_q}[\mathrm{x}, \mathrm{y}]$. Then $t(x, y) \in< PS >$ if and only if for all $A \in G(T_h, T_v)$, we have $t(x, y)A = O$.

Proof Sufficiency: Let GB be the Gröbner basis of $< PS >$, Δ the support of $< PS >$ w.r.t. GB, $R(x, y)$ is the normal form of $t(x, y)$ modulo GB. Then $t(x, y) - R(x, y) \in< PS >$, so for all $A \in G(T_h, T_v)$ we have

$$O = (t(x, y) - R(x, y))A = t(x, y)A - R(x, y)A = R(x, y)A.$$

Suppose $R(x, y) = \sum_{(I,J)\in\Delta} r_{IJ}x^I y^J$, then by expanding the leftmost side of above equality we can get

$$\sum_{(I,J)\in\Delta} r_{IJ}a_{IJ} = 0$$

for all $A = (a_{ij})_{i\geq 0, j\geq 0} \in G(T_h, T_v)$. But by Proposition 1, $a_{IJ}, (I, J) \in \Delta$, can be chosen to be arbitrary set of values in $\mathbf{F_q}$, so $r_{IJ} = 0$ for all $(I, J) \in \Delta$, thus $R(x, y) = 0$. Therefore $t(x, y) \in< PS >$.

Necessity: It is consequence of Proposition 8.

Theorem 14 If all the arrays in $G(T_h, T_v)$ are periodic, then the ideal $< PS >$ is of dimension [1] zero. Conversely, if the ideal $< PS >$ is of dimension zero, then any array $A \in G(T_h, T_v)$ has a periodic translation, i.e. there are two positive integers c and d such that $A_{c,d}$ is periodic.

Proof By Proposition 5, there are at most q^{mn} arrays in $G(T_h, T_v)$. Let $r \times s$ be the common period of all the arrays in $G(T_h, T_v)$. Then $(x^r - 1)A = O$ and $(y^s - 1)A = O$ for all $A \in G(T_h, T_v)$, so $x^r - 1 \in< PS >$, $y^s - 1 \in< PS >$, hence the dimension of $< PS >$ is zero.

Let $GB = \{f_1, \cdots, f_N\}$ be Gröbner basis of $< PS >$. If $< PS >$ is of dimension zero, then by the Theorem 6 of [7] and Theorem 4 of section 3.1.3 of [1], there is a univariate polynomial

[1] The dimension of an ideal is defined to be the smallest possible number of parameter which are needed in the parametric representation of the totality of all zeros common to the polynomials of the ideal

$f(x)$ of x in GB. Write $f(x) = f_1(x) \cdot x^I$, where $t \geq 0, f_1(x)$ a polynomial with non-zero constant term, then there is an integer r such that $f_1(x) | (x^r - 1)$ and for any array $A \in G(T_h, T_v)$, $O = f(x)A = (f_1(x)x^I)A = f_1(x)A_{I,0}$, hence $(x^r - 1)A_{I,0} = O$. Similarly, if we choose a appropriate order of indeterminates, we can find an integer J and s such that for any array $A \in G(T_h, T_v)$, $(y^s - 1)A_{0,J} = O$. Therefore for any array $A \in G(T_h, T_v)$, $(x^r - 1)A_{I,J} = O$, $(y^s - 1)A_{I,J} = O$, i.e. $A_{I,J}$ is periodic.

References

[1] J.H. Davenport, Y. Siera and E. Tournier, "Computer Algebra", Academic Press, Harcourt Brace Jovanovich, London.

[2] Dongdai Lin and Mulan Liu, *Linear Recurring m-Arrays*, Lecture Notes in Computer Science, No. 330(1988) pp 351-357.

[3] T. Nomura, H. Miyakawa, H. Imai and A. Fukuda, *A theory of two dimensional linear recurring arrays*, IEEE Trans. Inform. Theory vol. IT-18 pp 775-785,1972

[4] I. S. Reed and R. M. Stewart, *Notes on the existence of perfect maps* IRE Trans. Inform. Theory vol. IT-8 pp 10-12, Jan. 1962