1.

On Solving the Initial Problem of LR Arrays

Dongdai Lin (日大·理工)
小林英恒 (日大·理工)

Let $\mathbb{F}_q$ 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 $\mathbb{F}_q$. If there exist two positive integers $r$ and $s$ such that

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

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 $a_{t} = a_{i+i',j+j'}$, $i' = \text{the integer part} \left[ \frac{t}{n} \right]$, 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

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

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 $\mathbb{F}_q$ of the following form

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

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

such that

\[
\overline{A}(i,j)T_h = \overline{A}(i,j+1) \quad \text{for all } i, j \geq 0
\]

\[
\overline{A}(i,j)T_v = \overline{A}(i+1,j)
\]

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 $A(0,0)$) 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 $\mathbb{F}_q$. Sometimes, a non-zero initial state even does not exist. Please see the following examples:
Example 3. Let $m = n = 2$,

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

Then there is no non-zero $2 \times 2$ 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 $A(0, 0) = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$.

From the above examples, we can see that for two given $m \times n$ 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 determine 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 $\mathbb{F}_q$ 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 $\mathbb{F}_q$, $t(x, y) = \sum_{(i,j) \in \text{supp}(t)} t_{i,j} x^i y^j$ a polynomial over $\mathbb{F}_q$, where $\text{supp}(t)$ 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

$$t(x, y)A = \sum_{(I,J) \in \text{supp}(t)} t_{I,J} A_{I+J},$$

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

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

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

$$(t_1(x, y) + t_2(x, y))A = t_1(x, y)A + t_2(x, y)A$$

$$(t_1(x, y)t_2(x, y))A = t_1(x, y)t_2(x, y)A$$

**Proof** By check directly.
Proposition 7 For any polynomial \( f(x, y) \in \mathbb{F}_q[x, y] \), \( f(x, y) \) is a linear operator from \( G(T_h, T_v) \) to itself.

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

Let \( T_h, T_v \) be two matrices over \( \mathbb{F}_q \) as in (2), construct polynomials as follows:

\[
f_k(x, y) = x^k y^k - \left( \sum_{c=0}^{m-1} \sum_{d=0}^{n-1} r_{cn+d,k} \cdot x^c y^d \right) \quad k = 0, 1, \ldots, m - 1
\]
\[
g_k(x, y) = x^m y^k - \left( \sum_{c=0}^{m-1} \sum_{d=0}^{n-1} t_{cn+d,k} \cdot x^c y^d \right) \quad k = 0, 1, \ldots, n - 1
\]

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

Proposition 8 An array \( A \) over \( \mathbb{F}_q \) is contained in \( G(T_h, T_v) \) if and only if for any polynomials \( t(x, y) \) in \( <PS> \), we have \( t(x, y)A = 0 \), the zero array.

Let \( GB \) be the Gröbner basis of \( <PS> \), \( \Delta \) the Support of \( <PS> \) with respect to \( GB \). Then \( \text{Theorem 9} \) 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 \( (x^i y^j - R) \cdot A = 0 \), 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 \( \mathbb{F}_q \) for \( (i, j) \in \Delta \), there is a unique array \( A = (a_{ij})_{i\geq 0, j\geq 0} \) 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 \( t(x, y) \in GB \), \( t(x, y)A = 0 \). 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 \( \Delta \).

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), \( \bar{\Delta} = \{(i, j)|0 \leq i < m, 0 \leq j < n \} \) is not necessarily the support of the ideal \( <PS> \), i.e. there may be a polynomial in \( <PS> \) supported by \( \bar{\Delta} \) and this polynomial gives a relation among these \( a_{ij} \)'s, \( (i, j) \in \bar{\Delta} \).

Suppose \( \Delta \) and \( \bar{\Delta} \) have elements arranged in the following order:

\[
\Delta : T_0>T_1>\cdots>T_{|\Delta|-1},
\]
\[
\bar{\Delta} : T_0'>T_1'>\cdots>T_{m+n-1},
\]

\[
\text{Rest}(X^i y^j/GB) = \sum_{(i,j)\in \Delta} R^{(i,j)}_{i,j} x^i y^j \quad (I, J) \in \bar{\Delta}.
\]
Construct a \( mn \) by \(|\Delta| \) matrix \( M = (m_{ij})_{0 \leq i < mn, 0 \leq j < |\Delta|} \) with \( m_{ij} = R_{ij}^{(I', J')}, \) where \( T_i' = (I', J'), T_j = (I, J) \). Then

**Theorem 12** An \( mn \)-dimensional row vector \( u \) 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 \( v \) such that \( u = Mv \), where an \( mn \)-dimensional row vector \( u = (u_1, u_2, \cdots, umn) \) is said to be initial state of array \( A \) if

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

**Proof** Use Theorem 9 and Proposition 10.

**Proposition 13** Let \( t(x, y) \in F_q[x, y] \). Then \( t(x, y) < PS > \) 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 \( < PS > \), \( \Delta \) 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 \( F_q \), 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
\[ f(x) \text{ of } x \text{ in } GB. \text{ Write } f(x) = f_1(x)x^t, \text{ where } t \geq 0, f_1(x) \text{ a polynomial with non-zero constant term, then there is an integer } r \text{ such that } f_1(x)|(x^r - 1) \text{ and for any array } A \in G(T_h, T_v), \]
\[ O = f(x)A = (f_1(x)x^t)A = f_1(x)A_{I,0}, \text{ hence } (x^r - 1)A_{I,0} = O. \text{ Similarly, if we choose an appropriate order of indeterminates, we can find an integer } J \text{ and } s \text{ such that for any array } A \in G(T_h, T_v), \]
\[ (y^s - 1)A_{0,J} = O. \text{ Therefore for any array } A \in G(T_h, T_v), (x^r - 1)A_{I,J} = O, \]
\[ (y^s - 1)A_{I,J} = O, \text{ i.e. } A_{I,J} \text{ is periodic.} \]

References


