The equivalence classes of LR arrays

Dongdai Lin and Mulan Liu

Institute of Systems Science, Academia Sinica, Beijing 100080, China

Received 28 November 1990

Abstract


In this paper, the number of translation equivalence classes of linear recurring arrays with same period and the number of different arrays in an equivalence class are counted. Where and how many times a window appears in a period of the array are determined.

Introduction

The translation equivalence properties are very important in studying two-dimensional linear recurring arrays (or LR arrays in short) since the translation equivalent arrays are identified in practice. Unlike the case of linear recurring sequences, the number of different arrays in a translation equivalence class containing an array of period $r \times s$ is not necessarily $rs$, because a state (or a window) of the array can appear several times in one period of the array. Nomura et al. [8] studied where a window of an irreducible array (i.e., Nomura’s $\gamma\beta$-array) can appear. Sakata [10] studied equivalent doubly periodic arrays. In the present paper we study systematically the translation properties of general linear recurring arrays. We show where a window of the linear recurring array appears, give the number of elements in each equivalence class of the arrays, and count the number of translation equivalence classes of the array. In Section 1, we list the basic concepts and results on linear recurring arrays which we need. In Section 2, we study irreducible LR arrays. In Section 3, we discuss general LR arrays.

Correspondence to: Professor M. Liu, Institute of Systems Science, Academia Sinica, Beijing 100080, China.
1. Basic concepts

By an array $A$ of dimension 2 and period $r \times s$ (or an array of period $r \times s$ in short) we mean an infinite matrix $A = (a_{ij})_{i \geq 0, j \geq 0}$ over an arbitrary finite field $\mathbb{F}_q$ such that

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

(1.1)

where $r, s$ are the smallest positive integers for which the condition (1.1) is satisfied.

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 an $m \times n$ window or state of $A$ at $(i, j)$. $A(i, j)$ is the row vector obtained by arranging the rows of $A(i, j)$ one by one.

**Definition 1.1.** Let $A$ be an array of period $r \times s$ over $\mathbb{F}_q$. If all $m \times n$ windows in a period of $A$ are exactly all nonzero $m \times n$ matrices over $\mathbb{F}_q$, then we call $A$ an $m$-array of period $r \times s$ and order $m \times n$ or $(r, s; m, n)$ $m$-array in short.

**Definition 1.2.** Let $A = (a_{ij})_{i \geq 0, j \geq 0}$ be an array, $m$ and $n$ be two positive integers. If there exist elements of $\mathbb{F}_q$ such that

$$a_{i+k,j+n} = \sum_{c=0}^{m-1} \sum_{d=0}^{n-1} a_{i+c,j+d} r_{cn+dk}, \quad k = 0, 1, \ldots, m-1,$$

$$a_{i,m+n+k} = \sum_{c=0}^{m-1} \sum_{d=0}^{n-1} a_{i+c,j+d} t_{cn+dk}, \quad k = 0, 1, \ldots, n-1$$

(1.3)

then we call $A$ a linear recurring array (or LR array in short) of order $m \times n$.

**Definition 1.3.** If an LR array of order $m \times n$ is also an $m$-array of order $m \times n$, then we call it an LR $m$-array of order $m \times n$.

Equation (1.3) does not always represent a linear recurring relation if the elements (1.2) are arbitrarily chosen. A necessary and sufficient condition for (1.2) to define a linear recurring relation has already been given by Nomura et al.

**Definition 1.4.** Let $A = (a_{ij})_{i \geq 0, j \geq 0}$, $B = (b_{ij})_{i \geq 0, j \geq 0}$ be two periodic arrays. If there exist two nonnegative integers $c$, $d$ such that

$$b_{ij} = a_{i+c,j+d}$$

for all $i \geq 0, j \geq 0$

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

Obviously, the translation relation is an equivalence relation.
Definition 1.5. Let
\[
f(x) = c_0 + c_1 x + \cdots + c_{m-1} x^{m-1} + x^m \in F_q[x],
\]
\[
g(x, y) = y^n + \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} g_{ij} x^i y^j \in F_q[x, y].
\]
Then we call \((f, g)\) an LR relation (or LR pair) of order \(m \times n\).

Let \(A = (a_{ij})_{i \geq 0, j \geq 0}\) be an array over \(F_q\). If
\[
a_{I+m, J} + \sum_{i=0}^{m-1} c_i a_{I+i, J} = 0 \quad \text{for all } I \geq 0, J \geq 0,
\]
\[
a_{I,J+n} + \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} g_{ij} a_{I+i, J+j} = 0 \quad \text{for all } I \geq 0, J \geq 0
\]
then we call \(f(x)\) the \(v\)-characteristic polynomial of \(A\), \(g(x, y)\) the \(h\)-characteristic polynomial of \(A\) with respect to \(f(x)\), \((f, g)\) the characteristic pair of \(A\) and write \(A \in G(f, g)\).

Remark. In fact in the definition of \(h\)-characteristic polynomials, the phrase "with respect to \(f(x)\)" only means \(\deg x g(x, y) \leq \deg f(x)\), so we can change it to "with respect to \(\deg f(x)\)".

Proposition 1.6. Let \((f, g)\) be an LR pair. \(G(f, g) = \{A = (a_{ij})_{i \geq 0, j \geq 0}, a_{ij} \in F_q \mid A\) satisfies the relations (1.5)\}. For any two elements \(A = (a_{ij}), B = (b_{ij})\) of \(G(f, g)\), we define \(A + B = (a_{ij} + b_{ij})\) and \(c \cdot A = (c \cdot a_{ij})_{i, j \geq 0}\) for any \(c \in F_q\). Then \(G(f, g)\) is a vector space over \(F_q\) with dimension \(mn\).

Theorem 1.7. If \(A = (a_{ij})_{i, j \geq 0}\) is an LR array over \(F_q\), then there exists an LR pair \((f(x), g(x, y))\) such that \(A \in G(f, g)\).

In this paper, we study mainly the translation equivalence properties of the arrays of \(G(f, g)\).

Theorem 1.8. Let \(A\) be a periodic array. Then there exists a polynomial \(f(x) \in F_q[x]\) such that \(h(x) \in F_q[x]\) is a \(v\)-characteristic polynomial of \(A\) if and only if \(f(x) \mid h(x)\). Furthermore, the polynomial \(f(x)\) having the above property is uniquely determined by \(A\) if \(A \neq 0\), \(\deg f \geq 1\).

We call the unique polynomial \(f(x)\) determined by Theorem 1.8 the \(v\)-minimal polynomial of \(A\).

From now on, unless otherwise stated, we always assume that any array mentioned is periodic.
Let $f(x)$ be a $u$-characteristic polynomial of $A$ and $H = \{g(x, y) | g(x, y) \in F_2[x, y]\}$ is an $h$-characteristic polynomial of $A$ with respect to $f(x)$. Then $H \neq \emptyset$. We call the polynomials in $H$ which have the least degree in $y$ the $h$-minimal polynomials of $A$ with respect to $f(x)$. Generally, the degree in $y$ of an $h$-minimal polynomial with respect to a $v$-characteristic polynomial is uniquely determined, but the $h$-minimal polynomial itself is not.

**Definition 1.9.** If $f(x)$ is a $v$-minimal polynomial of $A$ and $g(x, y)$ is an $h$-minimal polynomial of $A$ with respect to $f(x)$, we call $(f, g)$ the minimal pair of $A$.

**Theorem 1.10.** Let $A$ be an array with irreducible polynomial $f(x)$ as its $v$-minimal polynomial. Then the $h$-minimal polynomial of $A$ with respect to $f(x)$ is uniquely determined by $A$ up to $\mod f(x)$.

We denote the greatest common divisor of $a_i (i = 1, \ldots, t)$ by $\bigwedge_{i=1}^{t} a_i$ and denote the least common multiple of $a_i (i = 1, \ldots, t)$ by $\bigvee_{i=1}^{t} a_i$, where $a_i (i = 1, \ldots, t)$ are polynomials or integers.

**Theorem 1.11** (Decomposition I) [5]. Let $(f(x), g(x, y))$ be an LR relation. If $f(x) = f_i(x) \cdots f_j(x), \bigwedge\{f_i, f_j\} = 1$ for $i \neq j$, then

$$G(f, g) = \bigoplus G(f_i, g_i)$$

as vector spaces over $F_q$, where $g_i = (g(x, y))_{f_i(x)}$.

**Theorem 1.12** (Decomposition II) [5]. Let $(f, g)$ be an LR relation. If $f(x)$ is an irreducible polynomial over $F_q$ and $g(x, y) = g_i(x, y)g_2(x, y) \cdots g_t(x, y)$ over $F_q[x]/\langle f(x) \rangle$, then

$$G(f, g) = \bigoplus G(f_i, g_i).$$

**Theorem 1.13** [5]. Let $(f, g)$ be a minimal pair of array $A = (a_{ij})_{i \geq 0, j \geq 0}$. Then $f$ is irreducible polynomial over $F_q$ and $g(x, y)$ is irreducible polynomial of $y$ over the field $F_q[x]/\langle f(x) \rangle$ if and only if there exist $\alpha$, $\beta$ in some extension field $K$ of $F_q$ such that $a_{ij} = L(\alpha^i \beta^j)$ for all $i \geq 0, j \geq 0$ for some nonzero linear function $L$ of $K$ to $F_q$.

**Definition 1.14.** We call an array $A = (a_{ij})_{i \geq 0, j \geq 0}$ irreducible if there exist $\alpha$, $\beta$ in some extension field $K$ of $F_q$ such that $a_{ij} = L(\alpha^i \beta^j)$ for all $i \geq 0, j \geq 0$ for some nonzero linear function $L$ of $K$ to $F_q$.

We call the LR relation $(f, g)$ in Theorem 1.13 the irreducible LR relation or irreducible pair.

**Remark 1.15.** In some papers, irreducible arrays are called $\alpha\beta$-arrays.
2. Equivalence classes of irreducible arrays

In this section, we consider only irreducible arrays. Notice that any two arrays with different irreducible pairs are not translation equivalent to each other.

**Theorem 2.1.** Let $G$ be an equivalence class of irreducible arrays of period $r \times s$ and let $\wedge \{r, s\} = d$. Then $|G| = rs/d = \sqrt[\wedge]{r, s}$.

In order to prove this theorem, we need several lemmas. At first we shall introduce some notation.

Let $\alpha \in F_q$, $\alpha \neq 0$, we use $\langle \alpha \rangle$ to denote the subgroup generated by $\alpha$ in the multiplicative group $F_q^*$ of $F_q$, and $o(\alpha)$ to denote the order of $\alpha$ in $F_q^*$.

Let $\alpha \in F_q^*$, $o(\alpha) = r$, $\gamma$ be a primitive element in $F_q$. Then there exists a unique positive integer $x$: $0 \leq x < r$ such that

$$\alpha = \gamma^{(q-1)/r} \text{ and } \wedge \{x, r\} = 1.$$ 

We denote $x$ and its inverse element $x^{-1}$ in the group $F_q^*$ by $\chi(\alpha, \gamma)$ and $\tilde{\chi}(\alpha, \gamma)$ respectively.

**Lemma 2.2.** Let $\gamma_1, \gamma_2$ be two primitive elements in $F_q$. Then for any two elements $\alpha, \beta$ in $F_q^*$, we have

$$\tilde{\chi}(\alpha, \gamma_1)\chi(\beta, \gamma_1) = \tilde{\chi}(\alpha, \gamma_2)\chi(\beta, \gamma_2) \pmod{\wedge \{o(\alpha), o(\beta)\}}.$$ 

**Proof.** Let $d = \wedge \{o(\alpha), o(\beta)\}$. If $d = 1$, the proposition is trivial. Now suppose $d > 1$ and $\gamma_1 = \gamma_2^p$. Then

$$\chi(\alpha, \gamma_1) = p\chi(\alpha, \gamma_1), \chi(\beta, \gamma_1) = p\chi(\beta, \gamma_1) \pmod{d}.$$ 

Since

$$\chi(\alpha, \gamma_1)\tilde{\chi}(\alpha, \gamma_1) = 1, \chi(\alpha, \gamma_2)\tilde{\chi}(\alpha, \gamma_2) = 1 \pmod{o(\alpha)},$$

so

$$\chi(\alpha, \gamma_1)\tilde{\chi}(\alpha, \gamma_1) = 1, \chi(\alpha, \gamma_2)\tilde{\chi}(\alpha, \gamma_2) = 1 \pmod{d},$$

i.e., $\tilde{\chi}(\alpha, \gamma_1)$ and $\tilde{\chi}(\alpha, \gamma_2)$ are the inverse elements of $\chi(\alpha, \gamma_1)$ and $\chi(\alpha, \gamma_2)$ respectively in the ring $Z_d$. Working in $Z_d$, we have

$$\tilde{\chi}(\alpha, \gamma_2)\chi(\beta, \gamma_2) = (\chi(\alpha, \gamma_2))^{-1}\chi(\beta, \gamma_2)$$

$$= p^{-1}\chi(\alpha, \gamma_1)p\chi(\beta, \gamma_1)$$

$$= \tilde{\chi}(\alpha, \gamma_1)\chi(\beta, \gamma_1)$$

where $p^{-1}$ is the inverse element of $p$ in $Z_d$. \hfill \Box

**Lemma 2.3.** Let $\alpha, \beta \in F_q^*$, $o(\alpha) = o(\beta) = r$. Then equation $\alpha^x \beta^y = 1$ has $r$ solutions:

$$x = -\tilde{\chi}(\alpha, \gamma)\chi(\beta, \gamma)t \pmod{r}, \quad y = t \pmod{r}, \quad t = 0, 1, \ldots, r-1,$$
The equivalence classes of LR arrays

or

\[
\begin{cases}
  x \equiv t \pmod{r}, \\
  y \equiv -\chi(\alpha, \gamma)\bar{\chi}(\beta, \gamma)t \pmod{r},
\end{cases}
\]

\(t = 0, 1, \ldots, r - 1,
\]

where \(\gamma\) is a primitive element of \(F_q\) and the solutions are independent of the choice of \(\gamma\).

**Proof.** Since \(o(\alpha) = o(\beta) = r\), we have \(\langle \alpha \rangle = \langle \beta \rangle\), so for any \(0 < x < r\), there exist \(0 \leq y < r\) such that \(\alpha^x\beta^y = 1\). Hence \(\alpha^x\beta^y = 1\) has exactly \(r\) solutions.

If \(x = t\) and \(\alpha^x\beta^y = 1\), then

\[
y^{(\chi(\alpha, \gamma) + \chi(\beta, \gamma)(q - 1)/r)} = 1,
\]

where \(\gamma\) is a primitive element of \(F_q\), so that

\[
\alpha^x\beta^y = 1 \quad \text{(mod } r),
\]

hence

\[
\begin{cases}
  x \equiv t \pmod{r}, \\
  y \equiv -\chi(\alpha, \gamma)\bar{\chi}(\beta, \gamma)t \pmod{r},
\end{cases}
\]

\(t = 0, 1, \ldots, r - 1
\]

are all the \(r\) solutions of equation \(\alpha^x\beta^y = 1\).

Similarly we can prove

\[
\begin{cases}
  x = -\frac{\chi(\alpha, \gamma)\bar{\chi}(\beta, \gamma)t}{d} \pmod{r}, \\
  y = t \pmod{s},
\end{cases}
\]

\(t = 0, 1, \ldots, d - 1
\]

are also all the \(r\) solutions of equation \(\alpha^x\beta^y = 1\).

By Lemma 2.2, the solutions are obviously independent of the choice of \(\gamma\). \(\square\)

**Lemma 2.4.** Let \(\alpha, \beta \in F_q^*, o(\alpha) = r, o(\beta) = s, \bigwedge \{r, s\} = d\) and \(\gamma\) be a primitive element of \(F_q\). Then equation \(\alpha^x\beta^y = 1\) has \(d\) solutions:

\[
\begin{cases}
  x \equiv -\frac{\chi(\alpha, \gamma)\bar{\chi}(\beta, \gamma)}{d}t \pmod{r}, \\
  y \equiv \frac{s}{d}t \pmod{s},
\end{cases}
\]

\(t = 0, 1, \ldots, d - 1
\]

or

\[
\begin{cases}
  x = \frac{r}{d}t \pmod{r}, \\
  y = -\frac{s}{d}t \pmod{s},
\end{cases}
\]

\(t = 0, 1, \ldots, d - 1
\]

**Proof.** Obviously, there exists \(\delta \in F_q^*, o(\delta) = \bigwedge \{r, s\}\) such that

\(\langle \alpha \rangle \cap \langle \beta \rangle = \langle \delta \rangle = \langle \alpha^{r/d} \rangle = \langle \beta^{s/d} \rangle\).
If $\alpha^x \beta^y = 1$, then $\alpha^x, \beta^y \in \langle \delta \rangle$, hence $x = (r/d)x_0$, $y = (s/d)y_0$ for some $x_0, y_0$. Put $\alpha_1 = \alpha^{r/d}$, $\beta_1 = \beta^{s/d}$. Then $o(\alpha_1) = o(\beta_1) = d$, and $\alpha^x \beta^y = 1$ if and only if $\alpha_1^{x_0} \beta_1^{y_0} = 1$.

By Lemma 2.3,

$$\begin{cases}
x_0 \equiv -\bar{x}(\alpha^{r/d}, y) x(\beta^{s/d}, y) t \pmod{d}, \\
y_0 \equiv t \pmod{d},
\end{cases}$$

are all the solutions of $\alpha_1^{x_0} \beta_1^{y_0} = 1$, so equation $\alpha^x \beta^y = 1$ has exactly $d$ solutions:

$$\begin{cases}
x \equiv -\bar{x}(\alpha^{r/d}, y) x(\beta^{s/d}, y) t \pmod{r}, \\
y \equiv \frac{s}{d} t \pmod{s},
\end{cases}$$

Since $\alpha_1 = \gamma^{x(\alpha^{r/d}, y)(q-1)/d}$, $\alpha^{r/d} = \gamma^{x(\alpha, y)(q-1)/d}$, but $\alpha^{r/d} = \gamma^{x(\alpha, y)(q-1)/d}$, so we have

$\gamma^{x(\alpha, y)(q-1)/d} = \gamma^{x(\alpha, y)(q-1)/d}$.

Similarly,

$\chi(\beta, y) \equiv \chi(\beta^{s/d}, y) \pmod{d}$.

Thus the $d$ solutions of equation $\alpha^x \beta^y = 1$ can be written as

$$\begin{cases}
x \equiv -\bar{x}(\alpha, y) x(\beta, y) t \pmod{r}, \\
y \equiv \frac{s}{d} t \pmod{s},
\end{cases}$$

In the same way, we can prove

$$\begin{cases}
x \equiv \frac{r}{d} t \pmod{r}, \\
y \equiv -\bar{x}(\alpha, y) x(\beta, y) \frac{s}{d} t \pmod{s},
\end{cases}$$

are also all the $d$ solutions of $\alpha^x \beta^y = 1$. $\square$

**Proof of Theorem 2.1.** Let $A = (L(\alpha^j \beta^i))_{i\geq 0, j\geq 0}$ be an irreducible array in $G$. Then $o(\alpha) = r$, $o(\beta) = s$ and $G = \{A_{ij} = BL^*_{i j} | i = 0, 1, \ldots, r-1, j = 0, 1, \ldots, s-1\}$, where $B = (\alpha^i \beta^j)_{i \geq 0, j \geq 0}$ and $BL^*_{i j} = (L^*_{i j})^*(\alpha^i \beta^j)$. In order to compute $|G|$, we must know how many times an array $A_{ij}$ appears in $G$.

Since $\{\alpha^i \beta^j | 0 \leq i < m, 0 \leq j < n\}$ is a basis of $F_q(\alpha, \beta)$ over $F_q$, where $m = o(q \mod r)$ and $n = o(q \mod s)$, so we have

$$A_{ij} = A_{i'j'} \iff B(L^*_{i' j'} - L^*_{i j}) = 0$$
$$\iff L^*_{i j} - L^*_{i' j'} = 0$$
$$\alpha^i \beta^j = \alpha^{i'} \beta^{j'}$$
$$\alpha^{i-i'} \beta^{j-j'} = 1,$$
hence by Lemma 2.4, \( A_{ij} = A_{ij'} \) if and only if
\[
\begin{align*}
  i - i' &= \frac{r}{d} \pmod r, \\
  j - j' &= -\chi(\beta, \gamma)\chi(\alpha, \gamma)\frac{s}{d} \pmod s,
\end{align*}
\]
\( t = 0, 1, \ldots, d - 1 \).

It means that any \( A_{ij} \) appears \( d \) times in \( G \), thus \( |G| = \frac{rs}{d} = V(r, s) \).

Theorem 2.1 tells us that any equivalence class of irreducible arrays of period \( r \times s \) contains exactly \( V(r, s) \) different arrays.

**Corollary 2.5.** Let \( A \) be an array of period \( r \times s \). Then \( A \) is an LR \( m \)-array if and only if \( A \) is irreducible and \( \bigwedge \{r, s\} = 1 \), \( rs = q^{\nu\{0(q \equiv r)\Psi(q \equiv s)\} - 1} \).

**Proof.** Use [3, Theorem 4.4].

Let \( I(\alpha, \beta) = \{(L(\alpha', \beta'))_{i \geq 0, j \geq 0} \mid L \) is a nonzero linear function of \( F_q(\alpha, \beta) \) to \( F_q) \}. \) Then any array in \( I(\alpha, \beta) \) has the same minimal (also irreducible) pair, say \((f, g)\) and \( G(f, g) = I(\alpha, \beta) \cup \{O\} \). \( \bigwedge (f, g) = q^{mn} \) if \( [F_q(\alpha): F_q] = m \), \([F_q(\alpha, \beta): F_q(\alpha)] = n \). But any equivalence class of irreducible arrays of period \( r \times s \) contains exactly \( V(r, s) \) different arrays by Theorem 2.1, so \( I(\alpha, \beta) \) is a union of \( (q^{mn} - 1)/(\bigwedge \{o(\alpha), o(\beta)\}) \) disjoint equivalence classes.

**Theorem 2.6.** Let \((f, g)\) be an irreducible pair of order \( m \times n \). Then \( G(f, g) \) is a union of \((q^{mn} - 1)/(\bigwedge \{o(f), o(g(x, y))\}) \) disjoint equivalence classes, where \( o(g(x, y)) \) is the period of \( g(x, y) \) over the field \( F_q[x]/(f(x)) \).

**Lemma 2.7.** Let \( A = (L(\alpha', \beta'))_{i \geq 0, j \geq 0} \), \( B = (L_1(\alpha_1', \beta_1'))_{i \geq 0, j \geq 0} \) be two irreducible arrays, where \( L \) is a nonzero linear function of \( F_q(\alpha, \beta) \) over \( F_q \) and \( L_1 \) is a nonzero linear function of \( F_q(\alpha_1, \beta_1) \) over \( F_q \). \( A \) and \( B \) have the same minimal LR relation if and only if
1. \( \alpha \) and \( \alpha_1 \) are conjugate over \( F_q \);
2. if \( \alpha = \alpha_1^t \) (for some \( t \geq 0 \)), then \( \beta \) and \( \beta_1^t \) are conjugate over \( F_q(\alpha) = F_q(\alpha_1) \).

**Proof.** Sufficiency: Let \((f, g)\) be a minimal pair of \( B \), then \( f(\alpha_1) = 0 \), \( g(\alpha_1, \beta_1) = 0 \). Since \( \alpha = \alpha_1^q \), so we have \( f(\alpha) = 0 \), \( 0 = (g(\alpha_1, \beta_1))^q = g(\alpha_1^q, \beta_1^q) = g(\alpha, \beta_1^q) \), but \( \beta \) and \( \beta_1^q \) are conjugate over \( F_q(\alpha) = F_q(\alpha_1) \), hence \( g(\alpha, \beta) = 0 \), thus \((f, g)\) is a characteristic pair of \( A \). Because \((f, g)\) is irreducible, \((f, g)\) is also a minimal pair of \( A \).

Necessity: Let \((f, g)\) be the common minimal pair of \( A \) and \( B \). Then \((f, g)\) is an irreducible pair and \( f(\alpha) = f(\alpha_1) = 0 \), \( g(\alpha, \beta) = g(\alpha_1, \beta_1) = 0 \), so there exists \( t \) such that \( \alpha = \alpha_1^t \), hence \( (g(\alpha_1, \beta_1))^q = g(\alpha_1^q, \beta_1^q) = g(\alpha, \beta_1^q) = 0 \). But \( g(\alpha, y) \) is irreducible over \( F_q(\alpha) \), hence \( \beta \) and \( \beta_1^q \) are conjugate over \( F_q(\alpha) = F_q(\alpha_1) \).
Let $I_{r \times s}$ be the set of all irreducible arrays of period $r \times s$, where $(rs, q) = 1$. Then

$$I_{r \times s} = \bigcup_{o(\alpha) = r, o(\beta) = s} I(\alpha, \beta).$$

Obviously, for any two pairs $(\alpha, \beta)$ and $(\alpha_1, \beta_1)$ either $I(\alpha, \beta) = I(\alpha_1, \beta_1)$ or $I(\alpha, \beta) \cap I(\alpha_1, \beta_1) = \emptyset$ so

$$I_{r \times s} = I(\alpha_1, \beta_1) \cup \cdots \cup I(\alpha_t, \beta_t)$$

for some pairs $(\alpha_i, \beta_i)$ $(i = 1, 2, \ldots, t)$. Now let us determine $t$.

Let $S = \{(\alpha, \beta) \mid o(\alpha) = r, o(\beta) = s\}$ and define a relation on $S$: $(\alpha, \beta) \sim (\alpha_1, \beta_1)$ if and only if $I(\alpha, \beta) = I(\alpha_1, \beta_1)$, i.e., $\alpha$ and $\alpha_1$ are conjugate over $F_q$ and if $\alpha = \alpha_1^q$, then $\beta$ and $\beta_1^q$ are conjugate over $F_q(\alpha) = F_q(\alpha_1)$ by Lemma 2.7. Obviously, this relation is an equivalence relation and $t$ is just the number of equivalence classes of $S$ with respect to $\sim$.

Denote the equivalence class containing $(\alpha, \beta)$ by $[(\alpha, \beta)]$. Then $[(\alpha, \beta)]$ contains $\sqrt{\{o(q \mod r), o(q \mod s)\}}$ elements, where $o(q \mod r)$ (or $o(q \mod s)$ respectively) denotes the order of $q$ in $\mathbb{Z}_r$ (or in $\mathbb{Z}_s$ respectively), since any element equivalent to $(\alpha, \beta)$ is of one of the forms:

$$(\alpha, x_0), (\alpha q, x_1), \ldots, (\alpha q^{(o(q \mod r) - 1)} \mod r), x_{o(q \mod r) - 1})$$

where $x_i \in F_q(\alpha, \beta)$ is a conjugate element of $\beta^q$ with respect to $F_q(\alpha)$. For each pair there are exactly $o(q^{o(q \mod r) \mod s})$ elements in $S$ equivalent to $(\alpha, \beta)$. Obviously $|S| = \phi(r)\phi(s)$, so $t = (\phi(r)\phi(s))/(\sqrt{\{o(q \mod r), o(q \mod s)\}})$.

**Theorem 2.8.** $I_{r \times s}$ is a union of $(\phi(r)\phi(s)\sqrt{o(q \mod r)\sqrt{o(q \mod s)}} - 1))/(\sqrt{\{r, s\}})(\sqrt{\{o(q \mod r), o(q \mod s)\}})$ disjoint equivalence classes, where $(rs, q) = 1$.

**Corollary 2.9.** The number of equivalence classes of LR $m$-arrays of period $r \times s$ is $(\phi(rs))/(\sqrt{\{o(q \mod r), o(q \mod s)\}})$.

### 3. Equivalence classes of linear recurring arrays

In this section, we further discuss the equivalence properties of arrays with general minimal pairs.

**Theorem 3.1.** Let $(f, g)$ be the minimal pair of array $A$ of period $r \times s$ with $f$ irreducible, $\alpha$ a root of $f(x)$, $u$ the least positive integer for which $y^u$ is congruent to a power of $\alpha \mod g(\alpha, y)$, say $\alpha^u$. Then

$$\begin{cases} i \equiv -tu \pmod{r}, & \text{for } 0 \leq i < r, \\ j \equiv tu \pmod{s}, & \text{for } 0 \leq j < s. \end{cases}$$

$$t = 0, 1, \ldots, \frac{o(\alpha)}{u} - 1 = \frac{s}{u} - 1$$
are all solutions of $A_{ij} = A_{00}$. Furthermore the equivalence class containing $A$ contain $ru$ different arrays.

In order to get Theorem 3.1, we first give several lemmas.

**Lemma 3.2.** Let $(f, g)$ be a minimal pair of a nonzero periodic array $A$. Then $\deg_y g(x, y) \geq 1$ and $g(x, 0) \not\equiv 0 \pmod{f(x)}$.

**Proof.** Since $A$ is a nonzero array, so $\deg_y g(x, y) \geq 1$. Now assume that $g(x, 0) \equiv 0 \pmod{f(x)}$. Then $b_0(x) = 0$. Since $A$ is a periodic array, $g(x, y) = y^{n-1} + \sum_{i=1}^{n-2} b_i(x)y^i$ is an $h$-characteristic polynomial of $A$ with respect to $f(x)$. It contradicts the fact that $(f, g)$ is a minimal pair of $A$, hence $g(x, 0) \not\equiv 0 \pmod{f(x)}$. 

**Lemma 3.3.** Let $A$ be an array with minimal pair $(f, g)$ of order $m \times n$. If $f(x)$ is an irreducible polynomial over $F_q$ and $\alpha$ is a root of $f(x)$, then $A_{00} = A_{ij}$ if and only if $y^j = \alpha^{-t} \pmod{g(\alpha, y)}$.

**Proof.** According to Theorem 1.13, we can write

$$A = (\text{Tr}(\beta_i \alpha^j))_{i \geq 0, j \geq 0}$$

where the sequence $\beta = (\beta_i)_{i \geq 0}$ have minimal polynomial $g(\alpha, y)$, so that

$$A_{00} = A_{ij} \quad \text{if and only if} \quad \text{Tr}(\beta_i \alpha^j) = \text{Tr}(\beta_{j+t} \alpha^{t+i}) \quad \text{for} \quad p > 0, \ t > 0$$

$$\text{Tr}_{a^t}(\beta_i) = \text{Tr}_{a^{t+i}}(\beta_{j+t} \alpha^t) \quad \text{for} \quad p \geq 0, \ t \geq 0.$$ 

Since $1, \alpha, \ldots, \alpha^{n-1}$ is a basis of $F_q(\alpha)$ over $F_q$, we have $A_{00} = A_{ij}$ if and only if $\beta_i = \beta_{j+t} \alpha^t$ for all $t \geq 0$, i.e., $y^j = \alpha^{-t}$ is a characteristic polynomial of sequence $\beta$. But $g(\alpha, y)$ is the minimal polynomial of $\beta$, so that $A_{00} = A_{ij}$ if and only if $y^j = \alpha^{-t} \pmod{g(\alpha, y)}$. 

**Lemma 3.4.** Let $g(x)$ be a polynomial over $F_q$ with $g(0) \not\equiv 0$ and $\deg g(x) \geq 1$, $\alpha \in F_q^\times$, $u$ be the least positive integer such that $x^u = \alpha^v$ (mod $g(x)$) for some $v$. Then for any $u'$, if there exists $v'$ such that $x^{u'} = \alpha^{v'}$ (mod $g(x)$), we have $u \mid u'$ and $v' = (u'v)/u$ (mod $o(\alpha)$). Conversely, if $u' = tu$ for some $t \in \mathbb{N}$, $t \geq 0$, then $x^{u'} = \alpha^{v(t)}$ (mod $g(x)$).

**Proof.** Put $u' = au + t$, $t \in \mathbb{N}$, $0 \leq t < u$. Then we have

$$\alpha^{v'} = x^{u'} = x^{au + t} = x^{au}x^t = \alpha^{av}x^t \quad \text{(mod} \ g(x))$$

so $x^t = \alpha^{u'-av}$ (mod $g(x)$). Because of the definition of $u$, this is only possible if $t = 0$, thus $u' = au$, i.e., $u \mid u'$. We also have $1 = \alpha^{v' - av}$ (mod $g(x)$), hence $\alpha^{v' - av} = 1$, $v' = av = (u'v)/u$ (mod $o(\alpha)$).

The remainder of the theorem is obvious. 

Proof of Theorem 3.1. Combining Lemmas 3.3 and 3.4. □

Next we will compute $u$.

Lemma 3.5. Let $g(x)$ be a polynomial over $\mathbb{F}_q$ with $g(0) \neq 0$ and $\deg g(x) \geq 1$, $\alpha \in \mathbb{F}_q^*$, $u$ be the least positive integer such that $x^u = \alpha^v \pmod{g(x)}$ for some $v$. Then $o(g(x)) = o(\alpha^u)u$.

Proof. Put $o(g(x)) = e$, then $x^e = 1 \pmod{g(x)}$, so $e \geq u$. Thus we can write $e = au + t$ with $t \in \mathbb{N}$ and $0 \leq t < u$. Just as in the proof of Lemma 3.4, we have $t = 0$ and $\alpha^{eu} = 1$, so $a = o(\alpha^u)$ and $e = au + t = au \geq o(\alpha^u)u$. On the other hand, $x^{o(\alpha^u)u} \equiv (\alpha^u)^{o(\alpha^u)u} \equiv 1 \pmod{g(x)}$, hence $o(g(x)) = o(\alpha^u)u$. □

Remark 3.6. The $u$ defined in Lemma 3.4 is somewhat like the integral order of $g(x)$ which is defined in the book “Finite Fields” written by Lidl et al., but they are indeed different. Generally speaking, $u$ is greater than the integral order of the same polynomial.

Lemma 3.7. Let $g(x)$ be a polynomial over $\mathbb{F}_q(\alpha)$ with $g(0) \neq 0$, $\deg g(x) \geq 1$ and let $o(\alpha) = r$, $o(g(x)) = s$, $(r,s) = d$, $u$ be the least positive integer such that $x^u = \alpha^v \pmod{g(x)}$ for some $v$; then the $u$ is one of $(s/d)(\mathbb{N} \{ d,t \})$ ($t = 1, 2, \ldots, d - 1$) and the corresponding $v$ is $(rt)/d$.

Proof. By Lemma 3.5, we have $o(g) = u o(\alpha^u)$, hence $s = ur / \mathbb{N} \{ v,r \} = (s/d)(\mathbb{N} \{ v,r \}) = u(r/d)$, $(r/d) \mathbb{N} \{ v,r \} = u(r/d)/\mathbb{N} \{ d,t \}$, $u = s/o(\alpha^u) = s(\mathbb{N} \{ d,t \})/d$. Hence the $u$ is one of $(s/d)(\mathbb{N} \{ d,t \})$ ($t = 1, 2, \ldots, d - 1$) and the corresponding $v$ is $(tr)/d$. □

Lemma 3.8. Let $o(\alpha) = r$, $g(x)$ be an irreducible polynomial over $\mathbb{F}_q(\alpha)$ with $g(0) \neq 0$ and $\deg g(x) \geq 1$. Then for any positive integer $e$, the least positive integer $u$ such that $x^u = \alpha^v \pmod{g(x)^e}$ for some $v$ is $q^k s / \mathbb{N} \{ r,s \}$, where $s = o(g(x))$ and $k$ is an integer such that $q^k \geq e > q^{k-1}$.

Proof. From $o(g^e) = q^k o(\alpha) = q^k s$, $\mathbb{N} \{ q,s \} = \mathbb{N} \{ q,s \} = 1$, we have $\mathbb{N} \{ o(g^e), o(\alpha) \} = \mathbb{N} \{ q^k s, r \} = \mathbb{N} \{ r,s \}$. Let $\beta$ be a root of $g(x)$, construct an array $A = (L(\alpha^{jq^k r}))_{i \geq 0, j \geq 0}$, where $L$ is a nonzero linear function of $\mathbb{F}_q(\alpha, \beta)$ over $\mathbb{F}_q$. Then $A$ is an irreducible array of period $r \times s$. By Lemmas 2.4 and 3.3, we know the least positive integer $u$ such that $x^u = \alpha^v \pmod{g(x)}$ for some $v$ is $s / \mathbb{N} \{ r,s \}$ and the corresponding $v$ is $\chi(\alpha, \gamma) (r / \mathbb{N} \{ r,s \})$ (mod $r$).

Since $x^{q^k u} + \alpha^{q^k v} = (x^u + \alpha^v)^{q^k} \equiv 0 \pmod{g(x)}$, so $u \leq q^k u' = q^k (s / \mathbb{N} \{ r,s \})$. But Lemma 3.7 asserts that $u \geq q^k (s / \mathbb{N} \{ r,s \})$, hence $u = q^k (s / \mathbb{N} \{ r,s \})$ and the corresponding $v = q^k \chi(\alpha, \gamma)(\beta, \gamma)(r / \mathbb{N} \{ r,s \})$ (mod $r$). We can easily prove that $v$ is independent of the choice of $\beta$ □
Theorem 3.9. Let \( o(\alpha) = r \), \( g(x) \) be a polynomial over \( F_q(\alpha) \) with \( g(0) \neq 0 \) and \( \deg g(x) \geq 1 \), \( g(x) = \prod_{i=1}^{t} g_i(x) \), \( \bigwedge \{ g_i, g_j \} = 1 \) for \( i \neq j \). If \( u_i \) is the least positive integer for which \( x^u_i \) is congruent to a power of \( \alpha \mod g_i \), say \( \alpha^{u_i} \), and \( u \) is the least positive integer for which \( x^u \) is congruent to a power of \( \alpha \mod g(x) \), say \( \alpha^v \), then

\[
u = \frac{r \prod_{i=1}^{t} u_i}{\bigwedge_{i \neq j} \prod_{1 \leq i, j \leq t} (u_i u_j - u_j u_i) \prod_{1 \leq k \leq t} u_k}, \]

Thus

\[
u = \frac{u_1 u_2 r}{\bigwedge \{ u_2v_1 - u_1v_2, r(\bigwedge \{ u_1, u_2 \}) \}} \quad (\mod r), \]

so the least positive integer \( d \) for which (3.1) holds is

\[
d = \frac{r}{\bigwedge \{ (u_2v_1 - u_1v_2)/\bigwedge \{ u_1, u_2 \}, r \}} = \frac{\bigwedge \{ u_1, u_2 \} r}{\bigwedge \{ u_2v_1 - u_1v_2, r(\bigwedge \{ u_1, u_2 \}) \}}, \]

thus

\[
u = \frac{u_1 u_2 r}{\bigwedge \{ u_2v_1 - u_1v_2, r(\bigwedge \{ u_1, u_2 \}) \}} \quad (\mod r). \]

Now suppose that we have proved the theorem for \( 2 \leq t \leq k - 1 \), we want to show that the theorem is also true for \( t = k \).

Put \( g(x) = \prod_{i=1}^{k-1} g_i(x) \), then \( g(x) = \bar{g}(x)g_k(x) \). Let \( \bar{u} \) be the least positive integer
for which $x^o$ is congruent mod $g(x)$ to a power of $\alpha$, say $\alpha^o$. Then by the assumption of induction, we have

$$u = \frac{\prod_{i=1}^{k-1} u_i}{\prod_{i \neq j} (u_i v_j - u_j v_i)}$$

(3.2)

and

$$v \equiv \frac{\prod_{i=1}^{k-1} u_i}{u_i} \pmod{r} \quad i = 1, 2, \ldots, k-1$$

(3.3)

Put (3.2), (3.3) and (3.4) together we can get

$$u = \frac{\prod_{i=1}^{k-1} u_i}{\prod_{i \neq j} (u_i v_j - u_j v_i)}$$

(3.4)

for all $h = 1, 2, \ldots, k-1$.

Thus

$$v \equiv \frac{\prod_{i=1}^{k-1} u_i}{u_i} \pmod{r}, \quad i = 1, 2, \ldots, k. \quad \square$$

**Theorem 3.10.** Let $A^{(i)}$ be an array of period $r_i \times s_i$ ($i = 1, 2$), $f_i(x)$ be the $u$-minimal polynomial of $A^{(i)}$ with $\{f_1(x), f_2(x)\} = 1$ and $u_i$ be the least positive integer such that $A_{v_i u_i}^{(i)} = A_{u_i}^{(i)}$ for some $v_i$. If $u$ is the least positive integer such that $(A^{(1)} + A^{(2)})_{v u} = (A^{(1)} + A^{(2)})_{u u}$ for some $v$, then
The equivalence classes of LR arrays

\[ u = \frac{u_1 u_2 (\bigwedge \{ r_1, r_2 \})}{\bigwedge \{ u_1 u_2 - u_2 u_1, (\bigwedge \{ r_1, r_2 \}) (\bigwedge \{ u_1, u_2 \}) \}} , \]

\[ v \equiv \frac{u_{ij}}{u_i} \pmod{r_i} \]

and the equivalence class containing \( A^{(1)} + A^{(2)} \) contains \( \bigvee \{ r_1, r_2 \} u \) different arrays.

**Theorem 3.11.** Let \((f(x), g(x, y))\) be an LR relation with \( \deg f(x) = m \), \( \deg g(x, y) = n \) and \( e \geq 1 \). If \( f(x) \) irreducible over \( F_q \), \( g(x, y) \) irreducible over the field \( F_q[x]/\langle f(x) \rangle \), then \( G(f, g^e) \) is a union of

\[ \bigcup_{i=1}^e q^{mn} - q^{(i-1)mn} \bigvee \{ r, s \} q^k \]

disjoint equivalence classes, where \( r = o(f(x)), s = o(g(x, y)) \) over \( F_q[x]/\langle f(x) \rangle \), \( k_i \) is the least positive integer such that \( q^{k_i} \equiv 1 \).

**Theorem 3.12.** Let \((f(x), g(x, y))\) be an LR pair, \( f(x) = \prod_{i=1}^l f_i(x), \ (g(x, y))_{f_i(x)} = \prod_{j=1}^{[f]} g_{ij}^q (x, y) \), where the \( f_i(x) \) are distinct irreducible polynomials over \( F_q \) and for any \( i \), the \( g_{ij}(x, y) \) are distinct irreducible polynomials of \( y \) over the field \( F_q[x]/\langle f_i(x) \rangle \). Let \( \deg f_i(x) = m_i, \ \deg g_{ij}(x, y) = n_{ij} \). Then the number of disjoint equivalences in \( G(f, g) \) is

\[ \sum_{1 \leq i \leq l} \frac{1}{t} \sum_{1 \leq j \leq \left[ k_{ij} \right]} \sum_{1 \leq c \leq d \leq e} \frac{N_i \cdots N_j}{ru} \]

where

\[ N_h = \sum_{n=1}^{k_{ij}^h(a)} (q^{m_{kn}} n_{kn}^{k_{ij}^h(a)-1} a_{kn}^h k_{ij}^h(a)) - q^{m_{kn} n_{kn}^{k_{ij}^h(a)-1} a_{kn}^h k_{ij}^h(a)} \]

\[ r = o(f_{k_{ij}}(x)) \cdots f_{k_{ij}}(x) \]

and \( u \) is the least positive integer such that \( x^u \) is congruent \( \pmod{\prod_{h=1}^{i} g_{ij}^h(a)} \) to a power of \( \alpha_{k_{ij}} \) for all \( j \), where \( \alpha_{k_{ij}} \) is a root of \( f_{k_{ij}}(x) \).

**References**


