LINEAR RECURRING m-ARRAYS

Dongdai Lin, Mulan Liu
Institute of Systems Science, Academia Sinica
Beijing, 100080, China

ABSTRACT

In this paper, the properties, structures and translation equivalence relations of linear recurring m-arrays are systematically studied. The number of linear recurring m-arrays is given.

1. Intrduction

Reed and Steward [11], Spann [5] and [2] have studied the arrays of so-called perfact maps. This has led to research on various types of window properties for arrays(see [2]-[11]).

In this paper, we make a systematic study of the linear recurring m-arrays of dimension 2. We characterize their structure, discuss their properties of translation - addition, pseudo-random and sampling. We also give the number of linear recurring m-arrays.

All the results in this paper are obtained over the finite field GF(2). One can easily generalize the results to any finite field GF(q).

2. Basic concepts

Let $A=(a_{ij})_{i\geqslant 0,j\geqslant 0}$ be an array. An $m\times n$ submatrix $A(i,j)=(a_{ij})_{0\leqslant i<m,0\leqslant j<n}$ of A is called an $m\times n$ window of A at (i,j). $\bar{A}(i,j)$ is the row vector $(a_t)_{0\leqslant t<mn}$ of dimension mn, where $a_t=a_{i+i',j+j'}$, i'=the integer part $[t/n]$ of t/n, and $j'=(t/n)=t-n[t/n]$.

Definition 2.1: Let A be an array of period $r\times s$. If all $m\times n$ windows in a period of A are exactly all non-zero $m\times n$ matrices over GF(2), then we call A an $m\times n$th order m-array of period $r\times s$ or $(r,s;m,n)$ m-array in short.

Corollary 2.1.1: There exists an $(r,s;m,n)$ m-array only if $rs=2^{mn}-1$.

Definition 2.2: Let $A=(a_{ij})_{i\geqslant 0,j\geqslant 0}$ be an array, m and n are two positive integers. If there exist two $mn\times mn$ matrices T_h and T_v as in (2.2) such that

$$\begin{aligned}\bar{A}(i,j)T_h&=\bar{A}(i,j+1)\\ \bar{A}(i,j)T_v&=\bar{A}(i+1,j)\end{aligned}\qquad \text{for all } i,j\geqslant 0 \tag{2.1}$$

and

C.G. Guenther (Ed.): Advances in Cryptology - EUROCRYPT '88, LNCS 330, pp. 351-357, 1988.

$$T_h = \begin{bmatrix} 00\ldots0{*}0\ldots0{*}\ldots0\ldots0{*} \\ 10\ldots0{*}0\ldots0{*}\ldots0\ldots0{*} \\ 01\ldots0{*}0\ldots0{*}\ldots0\ldots0{*} \\ \cdots \\ 00\ldots1{*}0\ldots0{*}\ldots0\ldots0{*} \\ 00\ldots0{*}0\ldots0{*}\ldots0\ldots0{*} \\ 00\ldots0{*}1\ldots0{*}\ldots0\ldots0{*} \\ \cdots \\ 00\ldots0{*}0\ldots1{*}\ldots0\ldots0{*} \\ \vdots \\ 00\ldots0{*}0\ldots0{*}\ldots0\ldots0{*} \\ 00\ldots0{*}0\ldots0{*}\ldots1\ldots0{*} \\ \cdots \\ 00\ldots0{*}0\ldots0{*}\ldots0\ldots1{*} \end{bmatrix} \qquad T_v = \begin{bmatrix} 00\ldots0{*} & \ldots{*} \\ 00\ldots0{*} & \ldots{*} \\ \vdots & \vdots \\ 00\ldots0{*} & \ldots{*} \\ 10\ldots0{*} & \ldots{*} \\ 01\ldots0{*} & \ldots{*} \\ \vdots & \vdots \\ 00\ldots1{*} & \ldots{*} \end{bmatrix} \tag{2.2}$$

where the entries at *s' positions are elements in F_2, then we say A is an LR array of order m×n. The window A(0,0) (or $\bar{A}(0,0)$) is called the initial state of A.

Definition 2.3: If an LR array of order m×n is also an m-array of order m×n, then we call it an LR m-array of order m×n.

Definition 2.4: Let $A=(a_{ij})_{i\geq0,j\geq0}$, $B=(b_{ij})_{i\geq0,j\geq0}$ be two periodic arrays. If there exist two non-negative integers p, q such that

$$b_{ij}=a_{i+p,j+q} \qquad \text{for all } i\geq0,\ j\geq0$$

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

Obviously, the translation relation is an equivalence relation.

Proposition 2.1: Given T_h, T_v as in (2.2), let $G(T_h,T_v)$ be the set of all LR arrays with linear recurring relations (2.1) and let $A,B\in G(T_h,T_v)$. Then

1) $A_{p,q}\in G(T_h,T_v)$ for any integers $p,q\geq0$.
2) Define $1*A=A$, $0*A=0$. Then $G(T_h,T_v)$ is a vector space over GF(2).
3) If there exists one LR m-array of order m×n in $G(T_h,T_v)$, then every one in $G(T_h,T_v)$ is an LR m-array of order m×n. Futhermore $T_hT_v=T_vT_h$ and T_h,T_v are non-degenerate.

Definition 2.5: We call an array A non-degenerate, if (2.1) holds for some non-degenerate matrices T_h and T_v as in (2.2).

Corollary 2.5.1: A non-degenerate LR array must be periodic.

Since we are interested in studying LR m-arrays, from now on, we always assume that T_h,T_v are non-degenerate and that they commute.

3. $\alpha\beta$-Array

We call an array $A=(a_{ij})_{i\geq0,j\geq0}$ $\alpha\beta$-array if its component $a_{ij}=L(\alpha^i\beta^j)$ for all $i,j\geq0$, where $\alpha,\beta\in GF(q)$, L is a linear function on GF(q) over GF(2)($GF(2)\subset GF(q)$).

In this section, we will mainly study linear recurring relations of $\alpha\beta$-arrays and the necessary and sufficient condition for an $\alpha\beta$-array to be an m-array. We will also compute the number of equivalence classes of $\alpha\beta$-m-arrays.

Lemma 3.1: Let $rs=2^{mn}-1$, $(r,s)=1$, $o(2 \bmod r)=m$ (i.e. the order of 2 in $\mathbb{Z}_r$ is m) or $o(2 \bmod s)=n$ and let $A=(a_{ij})_{i\geqslant 0, j\geqslant 0}$, where $a_{ij}=L(\gamma^{is+jr})$ for all $i\geqslant 0$, $j\geqslant 0$, L is a non-zero linear function on $GF(2^{mn})$ over $GF(2)$, γ is a primitive element of $GF(2^{mn})$. Then A is an $(r,s;m,n)$ LR m-array.

Proof: See [13].

Let L be a non-zero function on the field GF(q) over its prime field GF(p). We define L^* to be an elementwise transformation between vectors or matrices over GF(q) and those over GF(p) respectively as follows

$$(a_t)L^*=(L(a_t)) \text{ and } (a_{ij})L^*=(L(a_{ij}))$$

where (a_t) is a row or column vector over GF(q) and (a_{ij}) is a finite or infinite matix over GF(q).

Proposition 3.2: Let $\alpha, \beta \in GF(2^m)$, $o(\alpha)=r$, $o(\beta)=s$. If $rs=2^m-1$ for some m and $(r,s)=1$, then there exists a primitive element γ of $GF(2^m)$ such that $\alpha=\gamma^s$ and $\beta=\gamma^r$.

Theorem 3.3: Let $A=(\alpha^i\beta^j)L^*$ be an $\alpha\beta$-array, where L is a non-zero linear function on $F_2(\alpha,\beta)$. Then A is a non-degenerate LR arrays. Furtermore, A is an $(r,s;m,n)$ m-array if and only if the following conditions are satisfied.

1) $o(\beta)=s$, $o(\alpha)=r$ and $rs=2^{mn}-1$.
2) $\{\beta^i\alpha^j \mid 0\leqslant i<s, 0\leqslant j<r\}$ is the set of all non-zero elements of $GF(2^{mn})$.
3) $\{\alpha^i\beta^j \mid 0\leqslant i<m, 0\leqslant j<n\}$ is a basis of $GF(2^{mn})$ over $GF(2)$.

In fact, A is an $(r,s;m,n)$ LR m-array.

Corollary 3.3.1: Let $r\times s$ be the period of an $\alpha\beta$-m-array. Then $(r,s)=1$.

Let $f(x)=x^m+\sum_{i=1}^{m} c_i x^{m-i}$ be a monic polynomial of degree m over GF(2). Let $T=(d_{ij})_{0\leqslant i<m, 0\leqslant j<n}$ be an $m\times n$ matrix over GF(2) and $A=(a_{ij})_{i\geqslant 0, j\geqslant 0}$ an arbitrary array. If

$$\begin{aligned} a_{I+m,j}&=\sum_{i=1}^{m} c_i a_{m+I-i,j} \\ a_{I,J+n}&=\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} d_{ij}a_{I+i,J+j} \end{aligned} \qquad \text{for all } I,J\geqslant 0 \tag{3.1}$$

we say $A\in G(f,T)$.

Proposition 3.4: Suppose f, T as above. Then there exist T_h, T_v, such that $T_hT_v=T_vT_h$, $G(T_h,T_v)=G(f,T)$.

Proposition 3.5: Let f, T be as in prop. 3.4. If all non-zero arrays in $G(f,T)$ are m-array of order $m\times n$, then $f(x)$ must be irreducible.

Proposition 3.6: Let $A\in G(f,T)$ be an m-array of order $m\times n$ and period $r\times s$. Then r=the period $p(f)$ of $f(x)$ and $o(2 \bmod r)=m$.

Proposition 3.7: If $rs=2^{mn}-1$, then either $o(2 \bmod r)=mn$ or $o(2 \bmod s)=mn$.

Proposition 3.8: Let f, T be as in prop. 3.4, all arrays in G(f,T) be (r,s;m,n) m-arrays, o(2 mod r)=m and α be a root of f(x). Construct a polynomial g(x) of degree n over $F_2(\alpha)=GF(2^m)$ as follows:

$$g(x)=x^n+\sum_{t=0}^{n-1}\sum_{t'=0}^{m-1} d_{t',t}\alpha^{t'}x^t$$

then g(x) is irreducible over $F_2(\alpha)$ and p(g)=s.

Theorem 3.9: Let $A=(L(\beta_1^j\alpha_1^i))_{i\geqslant 0,j\geqslant 0}$, $B=(L(\beta_2^j\alpha_2^i))_{i\geqslant 0,j\geqslant 0}$ be two $\alpha\beta$-m-arrays of period r×s. Then A and B are equivalent if and only if the following statements are satisfied.

1) α_1 and α_2 are conjugate over GF(2).
2) if $\alpha_1=\alpha_2^{2^{i_0}}$ (for some i_0), then β_1 and $\beta_2^{2^{i_0}}$ are conjugate over $F_2(\alpha_1)=F_2(\alpha_2)$.

Theorem 3.10: The number of equivalence classes of $\alpha\beta$-m-arrays of period r×s is $\phi(rs)/\log_2(rs+1)$, where ϕ is Euler function.

4. General LR m-Array

In this section, we discuss general LR m-arrays. The main results are about their structure, enumeration and the necessary and sufficient conditions for existence of arrays with given period r×s.

Proposition 4.1: Suppose $A\in G(T_h,T_v)$ is an (r,s;m,n) LR m-array. Then $p(T_h)=s$, $p(T_v)=r$ and the order of any eigenvalue of T_h(T_v resp.) is s(r resp.).

Proposition 4.2: Suppose $A\in G(T_h,T_v)$ is an (r,s;m,n) LR m-array and o(2 mod s)=mn. Then

1) the characteristic polynomial of T_h is irreducible, and both T_h and T_v are similar to a diagonal form under same transformation.
2) the minimal polynomial g(x) of T_v is irreducible and deg(g(x))=m' if o(2 mod r)=m'.

Theorem 4.3(Existence): For given positive integers r and s, there exists an m-array with period r×s, if and only if (r,s)=1 and $rs=2^m-1$(for some m).

Theorem 4.4(Structure): Any LR m-array must be an $\alpha\beta$-m-array.

Remark 4.5: By Prop. 3.2, we know that there is a primitive element γ in $GF(2^{mn})$ such that

$$A=(L(\gamma^{is-jr}))_{i\geqslant 0,j\geqslant 0}. \tag{4.1}$$

Therefore each LR m-array can be determined by a primitive element γ and a linear function L. We denote A by $A_{r\times s}(\gamma,L)$, where r×s is the period of A. Obviously, for different linear functions, $A_{r\times s}(\gamma,L)$'s are equivalent.

Corollary 4.4.1: An (r,s;m,n) LR m-array is also an (r,s;mn,1) or (r,s;1,mn) LR m-array according which one of $o(2 \bmod r)$ and $o(2 \bmod s)$ is mn.

Corollary 4.4.2: The number of equivalence classes of LR m-arrays of period $r\times s$ is $\phi(rs)/\log_2(rs+1)$.

Remark 4.6: By Prop. 3.9, it is easy to prove that, for any two conjugate primitive elements γ_1 and γ_2 of $GF(2^{mn})$ with respect to $GF(2)$, $A_{r\times s}(\gamma_1,L)$ and $A_{r\times s}(\gamma_2,L)$ are equivalent. But the number of conjugate classes of primitive elements of $GF(2^{mn})$ with respect to $GF(2)$ is also $\phi(rs)/\log_2(rs+1)$, so that there is a 1-1 correspondence between the equivalence classes of $r\times s$ periodic LR m-arrays and the conjugate classes of primitive elements of $GF(2^{mn})$ (or all primitive polynomials of degree mn over GF(2))(see Remark 4.5 and Corollary 4.4.2). This map can be obtained by (4.1) of Remark 4.5.

The above correspondence is very powerful in Section 5 for studying the properties of LR m-arrays. From now on, $G_{r\times s}(f)$ will denote the set of all the arrays of period $r\times s$ which are corresponded to a primitive polynomial f.

5. Properties of LR m-Arrays

LR m-arrays can be thought of as generalized m-sequences. LR m-arrays have many good properties, as m-sequences do. In this section, we study the properties of translation-addition, sampling and correlation.

Proposition 5.1: An infinite matrix A of period $r\times s$ is an LR m-array if and only if

1) $(r,s)=1$
2) For any given integers $p_1,p_2,q_1,q_2\geq 0$, either $A_{p_1,q_1}+A_{p_2,q_2}=0$ or $=A_{p,q}$ for some $p,q\geq 0$.

The property given above is a characteristic property of LR m-arrays called the translation-addition property of LR m-arrays.

Proposition 5.2: For any LR m-array of order $m\times n$, the mn vectors $\bar{A}(i,j)(0\leq i<m, 0\leq j<n)$ are linearly independent and all $\bar{A}(i,j)$ can be linearly expressed by them.

Definition 5.1: Let $A=(a_{ij})_{i\geq 0,j\geq 0}$, (r,s) be a pair of positive integers. We call $A^{(r,s)}=(a_{ir,js})_{i\geq 0,j\geq 0}$ an (r,s)-sample of A. Especilly, $A^{(t,t)}$ is called a diagonal sample of A.

Theorem 5.3: Let A be an LR array with period $P_v\times P_h$ and (r,s) be a pair of positive integers. If $(r,P_v)=1=(s,P_h)$, then $A^{(r,s)}$ is again an LR m-array with period $P_v\times P_h$ and any LR m-array of period $P_v\times P_h$ are equivalent to some (diagonal) sample of A. Furthermore, if $(r',P_v)=(r,P_v)=(s',P_h)=(s,P_h)=1$, then $A^{(r,s)}$ and $A^{(r',s')}$ are equivalent if and only if

$$r'\equiv r2^t \bmod 2^m-1 \text{ and } s'\equiv s2^{t+mnt'} \bmod 2^{mn}-1 \text{ for some } t \text{ and } t'$$

Definition 5.2: Let $A=(a_{ij})_{i\geq 0,j\geq 0}$ be an array of period $r\times s$. The autocorrelation function of A is defined as the function

$$C_A: Z\times Z \longrightarrow Z: \quad C_A(p,q)=\sum_{i=1}^{r-1}\sum_{j=0}^{s-1} \eta(a_{ij})\ \eta(a_{i+p,j+q})$$

where η is a function from GF(2) to $\{1,-1\}$ such that $\eta(0)=1$, $\eta(1)=-1$.

Difinition 5.3: Let A be a binary array with period r s. If

$$C_A(p,q)=\begin{cases} rs & \text{when } p\equiv 0 \bmod r \text{ and } q\equiv 0 \bmod s \\ -1 & \text{others} \end{cases}$$

then we call A a pseudo-random array.

Theorem 5.4: Suppose A is a pseudo-random array with period $r\times s$. Then $rs\equiv 3 \bmod 4$ and the difference between the numbers of 1's and 0's in a period of A is 1.

Theorem 5.5: Any LR m-array is a pseudo-random array.

Definition 5.4: Let $A=(a_{ij})_{i\geqslant 0, j\geqslant 0}$, $B=(b_{ij})_{i\geqslant 0, j\geqslant 0}$ be two arrays of period $r\times s$. Define their crosscorrelation function as follows:

$$C_{A,B}: Z\times Z \longrightarrow Z: \quad C_{A,B}(p,q)=\sum_{i=0}^{r-1}\sum_{j=0}^{s-1} \eta(a_{ij})\ \eta(b_{i+p,j+q})$$

where η is just as in Definition 5.2.

Theorem 5.6: Sppose γ is a primitive element of $GF(2^n)$, $\gamma^{u_1}, \gamma^{u_2}, \ldots, \gamma^{u_k}$ $(0<K<2^n-1)$ are the first roots of primitive polynomials $f_{u_1}(x),\ldots,f_{u_k}(x)$ respectively, $u_1>u_2>\cdots>u_k$, $(r,s)=1$, $rs=2^n-1$. Then for any arrays $A\in G_{r\times s}(f_{u_i})$, $B\in G_{r\times s}(f_{u_j})$ and any t_1, $t_2\geqslant 0$, we have

$$C_{A,B}(t_1,t_2) \leqslant 2^n-1-2u_k$$

Theorem 5.7(gold Optimum Pair): Let γ be a primitive element of $GF(2^n)$.

$$u_1=2^{n-1}-1$$

$$u_2=\begin{cases} 2^{n-1}-2^{(n-1)/2}-1 & \text{if } 2\nmid n \\ 2^{n-1}-2^{n/2}-1 & \text{if } 2\mid n \text{ but } 4\nmid n \end{cases}$$

and $(r,s)=1$, $rs=2^n-1$. Then for any $A\in G_{r\times s}(f_{u_1})$, $B\in G_{r\times s}(f_{u_2})$ and t_1, $t_2\geqslant 0$, we have:

$$C_{A,B}(t_1,t_2)=\begin{cases} 2^{(n+1)/2}+1 & \text{if } 2\nmid n \\ 2^{(n+2)/2}+1 & \text{if } 2\mid n \text{ but } 4\nmid n \end{cases}$$

REFERENCE

[1]. Zhe-xian Wan, "Algebra and Coding Theory." Science Press, Beijing. 1980, revised edition.

[2]. B. Gordon, "On the existence of perfect maps" IEEE Trans. Inform. Theory Vol. IT-12 486-487 1966.

[3]. F.J. Macwilliams and N.J.A. Sloane, "Pseudo-random sequences and arrays". Proc.

IEEE vol.64 pp 1715-1729. 1976.

[4]. T. Normura, 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.

[5]. R. Spann, "A two-dimensional correlation property of pseudo-random maximal-length sequences". Proc. IEEE vol.53 pp 2137, 1963.

[6]. J. H. van Lint, F. J. Macwilliams and N. J. A. Sloane, "On pseudo-random arrays". SIAM J. Appl. Math. vol 36 pp 62-72, 1979.

[7]. C. T. Fan, S. M. Fan, S. L. Ma and M. K. Siu, "On de-Bruijn arrays". ARS Combin. vol. 19A (1985), 205-213.

[8]. S. Homer, Jerry Goldman, "Doubly-periodic sequences and two-dimensional recurrence", SIAM J. Alg. disc. Math. vol 6 (1985), 360-370.

[9]. S.L. Ma, "A note on binary arrays with a certain window property", IEEE Tran. Inform. Theory vol IT-30 (1984), 774-775.

[10]. T. Nomura and A. Fukuda, "Linear recurring planes and two-dimensional cyclic codes" Trans. Inst. Electron. Commun. Eng. Jap. vol. 54-A pp 147-154 Mar. 1971

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

[12]. D. Calabro and J. K. Wolf, "On the synthesis of two-dimensional arrays with desirable correlation properties:, Inform. Contr. vol. 11 pp 537-560 Nov/Dec. 1967.

[13]. M. K. Siu, "m-Arrays and M-Arrays." (1985).

[14]. L. E. Diccson, "On the cyclotomic function", Amer. Math. Monthly vol. 12 (1905) 86-89.