GENERALIZED MULTIPLEXED SEQUENCES

Mu-lan Liu and Zhe-xian Wan
Institute of Systems Science, Academia Sinica
Beijing, 100080 China

1. Introduction

Let $LSR_1, LSR_2, \ldots, LSR_k$ and LSR be k+1 linear feedback shift registers with characteristic polynomials $f_1(x), f_2(x), \ldots, f_k(x)$ and $g(x)$ over $\mathbb{F}_2$ and output sequences $\underline{a}_1, \underline{a}_2, \ldots, \underline{a}_k$ and $\underline{b}$ respectively, where $\underline{a}_i=(a_{io}, a_{i1}, \ldots)$, $i=1,2,\ldots,k$, $\underline{b}=(b_o, b_1, \ldots)$. Let $\mathbb{F}_2^k = \{(c_1, c_2, \ldots, c_k) \mid c_i \in \mathbb{F}_2\}$ be the k-dimensional space over $\mathbb{F}_2$ and γ be an injective map from $\mathbb{F}_2^k$ into the set $\{0,1,2,\ldots,n-1\}$, $2^k \leqslant n$, of course. Constructing k-dimensional vector sequence $A=(A_o, A_1, \ldots)$ where $A_t=(a_{1t}, a_{2t}, \ldots, a_{kt})$, $t=0,1,2,3,\ldots$ and applying γ to each term of the sequence A, we get the sequence $\gamma(A)=(\gamma(A_o), \gamma(A_1), \ldots)$ where $\gamma(A_t) \in \{0,1,\ldots,n-1\}$, for all t. Using $\gamma(A)$ to scramble the output sequence $\underline{b}$ of LSR, we get the sequence $\underline{u}=(u_o, u_1, \ldots)$ where $u_t=b_{t+\gamma(A_t)}$, for all t. we call γ a scrambling function and $\underline{u}$ the Generalized Multiplexed Sequence (generalizing Jenning's Multiplexed Sequence, see ref.[1]), in brief, GMS. In the present paper, the period, characteristic polynomial, minimum polynomial and translation equivalence properties of the GMS are studied under certain assumptions. Let Ω be the algebraic closure of $\mathbb{F}_2$. Throughout this paper, any algebraic extension of $\mathbb{F}_2$ are assumed to be contained in Ω. Let $f(x)$ and $g(x)$ be polynomials over $\mathbb{F}_2$ without multiple roots. Let $f*g$ be the monic polynomial whose roots are all the distinct elements of the set $S=\{\alpha\cdot\beta \mid \alpha, \beta \in \Omega,\ f(\alpha)=0,\ g(\beta)=0\}$. It is well known that $f*g$ is a polynomial over $\mathbb{F}_2$. Let $G(f)$ denote the vector space consisting of all output sequences of LSR with characteristic polynomial $f(x)$.

F. Pichler (Ed.): Advances in Cryptology - EUROCRYPT '85, LNCS 219, pp. 135-141, 1986.

2. The minimum polynomial and characteristic polynomial of GMS u

For proof of the following, we list some familiar results.

Lemma 1. 1) Suppose $f(x)=p_1(x)^{e_1}\dots p_m(x)^{e_m}$ is the characteristic polynomial of LSR, where $e_1,e_2,\dots,e_m$ are integers, $p_1(x),\dots,p_m(x)$ are irreducible polynomials of degrees $n_1,n_2,\dots,n_m$ over $\mathbb{F}_2$ respectively. For $i=1,2,\dots,m$, let α_i be one of the roots of $p_i(x)$. Let $\underline{a}\in G(f)$, then there exist uniquely determined elements $\xi_{ri}\in \mathbb{F}_{2^{n_r}}$, $r=1,2,\dots,m$, $i=1,2,\dots,e_r$, such that

$$a_t=\sum_{r=1}^{m}\sum_{i=1}^{e}\binom{i+t-1}{i-1}Tr_{2^{n_r}}(\xi_{ri}\alpha_r^t),\quad t=0,1,\dots. \tag{1}$$

where $Tr_{2^{n_r}}$ is the trace function from $\mathbb{F}_{2^{n_r}}$ to $\mathbb{F}_2$.

2) $f(x)$ is the minimum polynomial of the sequence $\underline{a}$ iff $\xi_{re_r}\neq 0$, $r=1,2,\dots,m$.

3) If there exist elements $\xi_{ri}\in\mathbb{F}_2[\alpha_1,\dots,\alpha_m]$, $r=1,2,\dots,m$, $i=1,2,\dots,e_r$, such that (1) holds and $a_t\in\mathbb{F}_2$, $t=0,1,2,\dots$. Then $f(x)$ is the characteristic polynomial of the sequence $\underline{a}$.

Corollary 1. 1) Under the conditions of Lemma 1, if $e_1=e_2=\dots=e_m=1$, i.e. $f(x)=p_1(x)p_2(x)\dots p_m(x)$, then there exist uniquely determined elements ξ_r, $r=1,2,\dots,m$, such that

$$a_t=\sum_{r=1}^{m}Tr_{2^{n_r}}(\xi_r\alpha_r^t),\qquad t=0,1,2,\dots \tag{2}$$

2) $f(x)$ is the minimum polynomial of $\underline{a}$ iff $\xi_r\neq 0$, $r=1,2,\dots,m$.

3) If there exist elements ξ_r such that (2) holds and $a_t\in\mathbb{F}_2$, $t=0,1,2,\dots$. Then $f(x)$ is a characteristic polynomial of $\underline{a}$.

Lemma2. Let m,n be two integers, l be the least common multiple of m and n, i.e. $l=[m,n]$, d be the greatest common divisor of m and n, i.e. $d=(m,n)$. Then $\mathbb{F}_{2^d}=\mathbb{F}_{2^m}\cap\mathbb{F}_{2^n}$, $\mathbb{F}_{2^l}=\langle\mathbb{F}_{2^m},\mathbb{F}_{2^n}\rangle$, i.e. $\mathbb{F}_{2^l}$ is generated by $\mathbb{F}_{2^n}$ and $\mathbb{F}_{2^m}$.

Lemma 3. Let $f(x)$ and $g(x)$ be two irreducible polynomials of degrees m and n respectively and $(m,n)=1$. Then

1) $f*g$ is irreducible.

2) Suppose α is a root of $f(x)$, β is a root of $g(x)$. Then for $\lambda\in\mathbb{F}_{2^m}$, $\mu\in\mathbb{F}_{2^n}$, we have

$$Tr_{2^m}(\lambda\cdot\alpha^t)Tr_{2^n}(\mu\cdot\beta^t)=Tr_{2^{m\cdot n}}(\lambda\mu(\alpha\beta)^t),\ t=0,1,2,\dots.$$

Theorem 1. Suppose the characteristic polynomials $p_1(x),p_2(x),\dots,p_k(x)$ and $g(x)$ of $LSR_1,LSR_2,\dots,LSR_k$ and LSR are irreducible of degrees $m_1,m_2,\dots,m_k$ and n respectively where $m_1,\dots m_k$ and n are relatively prime in pairs and greater than 1. Suppose $\underline{a}_1, \underline{a}_2, \ldots, \underline{a}_k$ and $\underline{b}$ are output sequences of $LSR_1, LSR_2, \ldots, LSR_k$ and LSR respectively. Then the GMS $\underline{u}$ obtained from $\underline{a}_1, \underline{a}_2, \ldots, \underline{a}_k$, $\underline{b}$ and the scrambling function γ has

$$F(x) = \prod_{\substack{j=0 \\ 0 \leqslant i_1 < i_2 < \ldots < i_j \leqslant k}}^{k} (p_{i_1} * p_{i_2} * \ldots * p_{i_j} * g) \tag{3}$$

as its minimum polynomial where $p_0(x)=1$ and $1*g=g$ by convention. Denote the degree of $F(x)$ by N, then

$$N=n(m_1+1)(m_2+1)\ldots(m_k+1). \tag{4}$$

Proof. For every k-dimensional vector $\vec{a}=(a_1,a_2,\ldots,a_k)\in \mathbb{F}_2^k$, we construct a monomial as follows. If $a_{i_1}=a_{i_2}=\ldots a_{i_j}=1$, and all other components are 0, then let $\vec{a}$ correspond to the monomial $p_{\vec{a}}=a_{i_1}\cdot a_{i_2}\cdot\ldots\cdot a_{i_j}$. The weight $w(\vec{a})$ of $\vec{a}$ is the number of 1's among $a_1,a_2,\ldots,a_k$, i.e. $w(\vec{a})=\sum_{i=1}^{k} a_i$. We arrange the elements of $\mathbb{F}_2^k$ such that $\vec{a}$ proceeds $\vec{b}$ iff $w(\vec{a})\leqslant w(\vec{b})$ and arrange the corresponding monomials and function values of γ in the same manner.Denote the monomials and function values of γ by $p_0,p_1,\ldots,p_{2^k-1}$ and $\rho_0, \rho_1, \ldots \rho_{2^k-1}$ respectively. Then

$$u_t=\bar{a}_{1t}\bar{a}_{2t}\ldots\bar{a}_{kt}b_{t+\rho_0}+a_{1t}\bar{a}_{2t}\ldots\bar{a}_{kt}b_{t+\rho_1}+$$
$$+\bar{a}_{1t}a_{2t}\bar{a}_{3t}\ldots\bar{a}_{kt}b_{t+\rho_2}+\ldots+a_{1t}a_{2t}\ldots a_{kt}b_{t+\rho_{2^k-1}},$$

where $\bar{a}_{it}=a_{it}+1$, $i=1,2,\ldots,k$. Substituting $\bar{a}_{it}=a_{it}+1$ into u_t, we find that the coefficient of $b_{t+\rho_j}$ in u_t is of the form

$$\sum_{l=j}^{2^k-1} c_{jl}\cdot p_l(t),$$

where $c_{jj}=1$ and $p_l(t)=p_l(a_{1t},\ldots,a_{kt})$. Putting $c_{jl}=0$ if $l<j$, we may write

$$u_t=\sum_{j=0}^{2^k-1}\Big(\sum_{l=j}^{2^k-1} c_{jl}\cdot p_l(t)\Big)b_{t+\rho_j}=\sum_{l=0}^{2^k-1}\Big(\sum_{j=0}^{2^k-1} c_{jl}\cdot b_{t+\rho_j}\Big)p_l(t)=$$
$$=\sum_{l=0}^{2^k-1} b'_{\tau_l t}\, p_l(t) \tag{5}$$

where

$$b'_{\tau_l t}=\sum_{j=0}^{2^k-1} c_{jl}\cdot b_{t+\rho_j}, \quad l=0,1,2,\ldots,2^k-1. \tag{6}$$

Put $\underline{b}_i=(b_{i-1},b_i,\ldots,b_{i+t},\ldots)$, $i=1,\ldots,n$ and $\underline{b}'_{\tau_l}=(b'_{\tau_l 0},b'_{\tau_l 1},\ldots,b'_{\tau_l t},\ldots)$, $l=0,1,2,\ldots,2^k-1$. Since $g(x)$ is an irreducible polynomial with degree n and $\underline{b}\in G(g)$, $\underline{b}_1,\underline{b}_2,\ldots,\underline{b}_n$ form a basis of $G(g)$, thus $\underline{b}_{\rho_0}$, $\underline{b}_{\rho_1}$, $\ldots$, $\underline{b}_{\rho_{2^k-1}}$ $(0\leqslant \rho_j \leqslant n-1)$ are linearly independent. From (6), we have

$$(\underline{b}'_{\tau_0}, \underline{b}'_{\tau_1}, \ldots, \underline{b}'_{\tau_{2^k-1}})=(\underline{b}_{\rho_0}, \underline{b}_{\rho_1}, \ldots, \underline{b}_{\rho_{2^k-1}})C$$

where

$C=(c_{jl}),\ c_{jj}=1, c_{jl}=0,$ if $l<j$ (7)

therefore $\underline{b}'_{\tau_0}, \underline{b}'_{\tau_1}, \ldots, \underline{b}'_{\tau_{2^k-1}}$ are also linearly independent sequences and g(x) is their minimum polynomial. Let β be a root of g(x), from Corollary 1, for every l there is a uniquely determined non-zero element $\mu_l \in \mathbb{F}_{2^n}$ such that

$$b'_{\tau_l t} = Tr_{2^n}(\mu_l \beta^t).$$

Let α_i be a root of $P_i(x)$, i=1,2,...,k, again from Corollary 1 of Lemma 1, for every i, there is a uniquely determined non-zero element $\lambda_i \in F_{2^{m_i}}$ such that

$$a_{it} = Tr_{2^{m_i}}(\lambda_i \alpha_i^t),\ t=0,1,2,\ldots;\ i=1,2,\ldots,k.$$

Now we can calculate the general term u_t of the GMS $\underline{u}$ by using the above root expressions of the sequences $\underline{b}'_{\tau_l}$ and $\underline{a}_i$. We have

$$u_t = \sum_{l=0}^{2^k-1} p_l(t) b'_{\tau_l t} = \sum_{l=0}^{2^k-1} a_{i_1 t} a_{i_2 t} \cdots a_{i_{s(l)} t} \cdot b'_{\tau_l t}$$

where s(l) = degree of p_l. Then, By Lemma 3,

$$u_t = \sum_{l=0}^{2^k-1} Tr(\lambda_{i_1} \cdot \alpha_{i_1}^t) Tr(\lambda_{i_2} \cdot \alpha_{i_2}^t) \ldots Tr(\lambda_{i_{s(l)}} \alpha_{i_{s(l)}}^t) Tr(\mu_l \beta^t)$$

$$= \sum_{l=0}^{2^k-1} Tr(\lambda_{i_1} \lambda_{i_2} \cdots \lambda_{i_{s(l)}} \mu_l (\alpha_{i_1} \alpha_{i_2} \cdots \alpha_{i_{s(l)}} \beta)^t)$$

where $\alpha_{i_1} \alpha_{i_2} \cdots \alpha_{i_{s(l)}} \beta$ is a root of the irreducible polynomial $p_{i_1}^* p_{i_2}^* \ldots ^* p_{i_{s(l)}}^* g$ of degree $m_{i_1} \cdot m_{i_2} \ldots m_{i_{s(l)}} \cdot n$. Therefre, by Corollary 1, (3) is the minimum polynomial of $\underline{u}$.And it follows that the degree of F(x) is (4).

Note that from Theorem 1, it follows that the minimum polynomial of the GMS $\underline{u}$ is independent from the scrambling function γ and the complexity of GMS is increased considerably.

For characteristic polynomials with multiple roots, we need some results of [2].

Let $\underline{a}=(a_0,a_1,\ldots)$ and $\underline{b}=(b_0,b_1,\ldots)$ be two arbitrary binary sequences, we define the product $\underline{a}.\underline{b}$ of $\underline{a}$ and $\underline{b}$ to be $\underline{a}.\underline{b}=(a_0b_0,a_1b_1,\ldots)$. For two vector spaces G(f),G(g), the product G(f).G(g) of G(f) and G(g) is defined to be the vector space generated by all products $\underline{a}.\underline{b}$, where $\underline{a} \in G(f)$ and $\underline{b} \in G(g)$.

Lemma 4. Let

$$s^{(k)} = \left(\binom{k}{k}, \binom{k+1}{k}, \ldots, \binom{k+t}{k}, \ldots \right).$$

then $s^{(0)},\dots,s^{(e-1)}$ form a basis of the vector space $G((x+1)^e)$.
For two arbitrary positive integers e_1 and e_2, write

$$e_1-1 = \sum_{\nu} j_\nu 2^\nu \quad , j_\nu = 0 \text{ or } 1,$$
$$e_2-1 = \sum_{\nu} k_\nu 2^\nu \quad , k_\nu = 0 \text{ or } 1.$$

Let λ be the smallest nonnegative integer such that $j_\nu + k_\nu < 2$ for all $\nu \geqslant \lambda$, then Zierler and Mills [2] defined

$$e_1 \vee e_2 = 2^\lambda + \sum_{\nu \geqslant \lambda} (j_\nu + k_\nu) 2^\nu .$$

Lemma 5 (Zieler, Mills).

$$G((x+1)^{e_1})\ G((x+1)^{e_2}) = G((x+1)^{e_1 \vee e_2}).$$

We have

Theorem 2: Let the k+1 polynomials $p_1(x)^{e_1}, p_2(x)^{e_2},\dots,p_k(x)^{e_k}$ and $g(x)^e$ be characteristic polynomials of $LSR_1,\dots,LSR_k$ and LSR respectively, where $p_1(x),\dots,p_k(x),g(x)$ are irreducible of degrees $m_1,m_2,\dots,m_k$ and n. Assume $m_1,m_2,\dots,m_k$ and n are relatively prime in pairs. Let the sequences $\underline{a}_1,\dots,\underline{a}_k$ and $\underline{b}$ are output sequences of these k+1 linear shift registers respectively. Then the GMS $\underline{u}$ generated by $\underline{a}_1,\dots,\underline{a}_k$ and $\underline{b}$ has the characteristic polynomial

$$F(x) = \prod_{\substack{j=0 \\ 0 \leqslant i_1 < i_2 < \dots < i_j \leqslant k}}^{k} (p_{i_1} * \dots * p_{i_j} * g)^{e_{i_1} \vee \dots \vee e_{i_j} \vee e}$$

Next, let's consider the period of GMS. At first, we have the following two lemmas.

Lemma 6. Let f(x), g(x) be two irreducible polynomials over $\mathbb{F}_2$ of degrees m,n respectively, and (m,n)=1. Then

$$p(f*g) = p(f)p(g),$$

where p(f) denotes the period of f(x).

Lemma 7. Suppose that f(x) and g(x) are two polynomials over $\mathbf{F}_2$ with (f,g)=1. Then $p(f.g) = [p(f),p(g)]$.

From Lemmas 6 and 7 we deduce immediately

Theorem 3. Suppose that $f_1(x),\dots,f_k(x)$ and g(x) are irreducible over $\mathbb{F}_2$ and the degrees of these polynomials are relatively prime in pairs. Then the period $p(\underline{u})$ is $p(f_1)\dots p(f_k)p(g)$.

3. The translation equivalence properties of GMS's

Throughout this section we suppose that $p_1(x),\dots p_k(x)$ and g(x) are irreducible and their degrees $m_1, m_2, \ldots, m_k$ and n are relatively prime in pairs.

Theorem 4. Let $\underline{a}_i$ and $\underline{a}_i'$ are two non-zero output sequences of LSR_i which are translates of each other, $i=1,2,\ldots,k$. And let $\underline{b}$ and $\underline{b}'$ are two output sequences of LSR which are also translates of each other. Then for a given scrambling function γ, the GMS $\underline{u}$ obtained from $\underline{a},\ldots,\underline{a}_k,\underline{b}$ and the GMS $\underline{u}'$ obtained from $\underline{a}_1',\ldots,\underline{a}_k',\underline{b}'$ are translates of each other.

Proof. From the sequences $\underline{a}_1,\ldots\underline{a}_k$, we get the sequence

$$\gamma(A) = (\gamma(A_o), \gamma(A_1), \ldots)$$

where $\gamma(A_t) = \gamma(A_{1t}, a_{2t}, \ldots, a_{kt})$. The same, we get

$$\gamma(A') = (\gamma(A_o'), \gamma(A_1'), \ldots),$$

where $\gamma(A_t') = \gamma(a_{1t}', a_{2t}', \ldots, a_{kt}')$. Then $u_t = b_{t+\gamma(A_t)}$, $u_t' = b_t' + \gamma(A_t')$. Since $\underline{a}_i$ and $\underline{a}_i'$ are translates of each other, there exists τ_i, $0 \leqslant \tau_i \leqslant p(\underline{a}_i)$ such that $a_{it}' = a_{i(t+\tau_i)}$, $i=1,2,\ldots,k$. Since $\underline{b}$ and $\underline{b}'$ are translates of each other, there exists an integer s, $0 \leqslant s \leqslant p(\underline{b})$, such that $b_t' = b_{t+s}$. Since $p(\underline{a}_i) \mid 2^{m_i}-1$, $i=1,2,\ldots,k$, $p(\underline{b}) \mid 2^n-1$, and $m_1,\ldots m_k$ and n are relatively prime in pairs, $p(\underline{a}_1),\ldots,p(\underline{a}_k)$ and $p(\underline{b})$ are also relatively prime in pairs. By Chinese Remainder Theorem the following simultaneous congruences

$$\begin{cases} x \equiv \tau_1 & (\mathrm{mod}\ p(\underline{a}_1)) \\ x \equiv \tau_2 & (\mathrm{mod}\ p(\underline{a}_2)) \\ \quad\vdots & \\ x \equiv \tau_k & (\mathrm{mod}\ p(\underline{a}_k)) \\ x \equiv s & (\mathrm{mod}\ p(\underline{b})) \end{cases}$$

have a solution $x \in \mathbb{Z}$ which is unique mod $p(\underline{a}_1)\ldots p(\underline{a}_k)p(\underline{b})$. It follows that $u'_t = u_{t+x}$ for all t. This proves that $\underline{u}$ and $\underline{u}'$ are translates of each other.

Corollary 2. For a given scrambling function γ, if the characteristic polynomials of the k+1 linear shift registers $LSR_1,\ldots.LSR_k$ and LSR are primitive polynomials whose degrees are relatively prime in pairs then the GMS's obtained from any non-zero initial states are all translates of each other.

Lemma 8. If

$$\sum_{i=0}^{2^k-1} d_i p_i = 0, \quad d_i \in \mathbb{F}_2, \tag{8}$$

then $d_i=0$ for all i.

Theorem 5. For different scrambling functions γ and γ', the GMS's $\underline{u}$ and $\underline{u}'$ obtained from the non-zero output sequences $\underline{a}_1,\underline{a}_2,\ldots,\underline{a}_k$, $\underline{b}$ of the k+1 linear shift registers $LSR_1,\ldots, LSR_k$, LSR are translates of each other iff there exist two fixed integers M and M' such that for all

$(a_1,a_2,\ldots,a_k)\in \mathbf{F}_2{}^k$, we have

$$\gamma'(a_1,a_2,\ldots,a_k)=\gamma(a_1,a_2,\ldots,a_k)+M \text{ or } \gamma(a_1,a_2,\ldots,a_k)+M'$$

where $0\leqslant |M|,|M'|\leqslant n-1$ and $M+M'\equiv 0 \pmod{p(\underline{b})}$.

Proof. We follow the notation of the proof of Theorem 1. For a given γ, we have (5) and (6). Substituting (6) into (5), we obtain

$$u_t=(b_{\rho_0+t},\ b_{\rho_1+t},\ldots,b_{\rho_{2^k-1}+t})C\,(p_0(t),p_1(t),\ldots,p_{2^k-1}(t))'$$

where C is the matrix (7), thus

$$\underline{u}=(\underline{b}_{\rho_0},\underline{b}_{\rho_1},\ldots,\underline{b}_{\rho_{2^k-1}})\ C\ (p_0,p_1,\ldots,p_{2^k-1})'$$

where ' denotes the transpose of a matrix. Similarly, for γ', we have

$$\underline{u}'=(\underline{b}_{\rho_0'},\underline{b}_{\rho_1'},\ldots,\underline{b}_{\rho_{2^k-1}'})\ C\ (p_0,p_1,\ldots,p_{2^k-1})'$$

Let

$$\rho_j'=\rho_j+\delta_j,\ -(n-1)\leqslant \delta_j\leqslant n-1,\ j=1,2,\ldots,2^k-1.$$

Denote the left translate operator by L, i.e. $L(a_0,a_1,\ldots)=(a_1,a_2,\ldots)$, then

$$\underline{u}'=(L^{\delta_0}\ \underline{b}_{\rho_0},L^{\delta_1}\ \underline{b}_{\rho_1},\ldots,L^{\delta_{2^k-1}}\ \underline{b}_{\rho_{2^k-1}})\ C\ (p_0,p_1,\ldots,p_{2^k-1})'$$

The sequences $\underline{u}$ and $\underline{u}'$ are translates of each other iff there exists an integer M such that $\underline{u}'=L^M\underline{u}$, i.e.

$$(L^{\delta_0}\ \underline{b}_{\rho_0},L^{\delta_1}\ \underline{b}_{\rho_1},\ldots,L^{\delta_{2^k-1}}\ \underline{b}_{\rho_{2^k-1}})\ C\ (p_0,p_1,\ldots,p_{2^k-1})'=$$
$$=(L^M\underline{b}_{\rho_0},L^M\underline{b}_{\rho_1},\ldots,L^M\underline{b}_{\rho_{2^k-1}})\ C\ (p_0,p_1,\ldots,p_{2^k-1})' \tag{9}$$

By Lemma 8 and C being invertible, (9) holds iff

$$(L^{\delta_0}\underline{b}_{\rho_0},\ldots,L^{\delta_{2^k-1}}\underline{b}_{\rho_{2^k-1}})=(L^M\underline{b}_{\rho_0},\ldots,L^M\underline{b}_{\rho_{2^k-1}}) \tag{10}$$

Clearly (10) holds iff the following simultaneous congruences have a solution M:

$$M\equiv \delta_i \pmod{p(\underline{b})}\qquad i=0,1,\ldots,2^k-1$$

Without loss of generality, suppose that $\delta_0,\delta_1,\cdots,\delta_i$ are non-negative and $\delta_{i+1},\ldots,\delta_{2^k-1}$ are negative, then

$$\delta_0=\delta_1=\ldots=\delta_i=\delta,\quad \delta_{i+1}=\ldots=\delta_{2^k-1}=\delta'$$

and

$$\delta\equiv\delta' \pmod{p(\underline{b})}.$$

Taking $M=\delta$, $M'=-\delta'$, the proof is complete.

Corollary 2. In Theorem 5, if the characteristic polynomial g(x) of LSR is primitive, then $M=M'$, $0\leqslant|M|\leqslant n-1$.

References

[1] S.M.Jennings, Multiplexed Sequences:Some Properties of the Minimum Polynomial. Lecture Notes in Computer Science, No.149,Springer-Verlag, 1983, 189-206.

[2] N. Zierler and W.H.Mills, Products of Linear Recurring Sequences. J. of Algebra 27(1973), 147-157.