Lecture Four

Basic Efficiency Criteria of LFSR's-Systems

3. Periodicity Criterion

The sequence S has period P(S) when $s_0=s_{P(S)}$, $s_1=s_{P(S)+1},\ldots$, the period of $LFSR_i$ denotes by $P(S_i)$, P(S) and $P(S_i)$ are least possible positive integers. The definition of periodicity introduced before lecture three. And, as mentioned before, P(S) will be the least common multiple of all $P(S_i)$, $\forall\ 1\le i\le n$.

$$P(S) = \text{lcm}(P(S_1),P(S_2),\ldots,P(S_k)) \qquad \ldots(3.1)$$

Of course if $P(S_i)$ are relatively prime to each other $\forall i$, $1\le i\le k$, then

$$P(S)=\prod_{i=1}^{k} P(S_i) \qquad \ldots(3.2)$$

Its important the show the relation between lcm and gcd of $P(S_i)$ by using the next theorem.

Definition (3.1): Let $GCD_2=\gcd(\prod_{i=1}^{1} m_i, m_2.GCD_1)=\gcd(m_1,m_2)$, for convenient let $GCD_1=1$ and so on the general form of the recursion equation will be:

$$GCD_n=\gcd(\prod_{i=1}^{n-1} m_i, m_n.GCD_{n-1}) \qquad \ldots(3.3)$$

where $n\ge 2$ s.t m_i are positive integers, $\forall 1\le i\le n$.

Theorem (3.1): Let $m_i \in Z^+$, $\forall 1\le i\le n$ then:

$$\text{lcm}(m_1,m_2,\ldots,m_n)=\frac{\prod_{i=1}^{n} m_i}{GCD_n(m_i)} \qquad \ldots(3.4)$$

Proof:

We suggest using the mathematical induction,

Let n=2 and as known from definition (4.1):

$$\text{lcm}(m_1,m_2)=\frac{m_1.m_2}{\gcd(m_1,m_2)} \qquad \ldots(3.5)$$

$$\frac{\prod_{i=1}^{2} m_i}{GCD_2}=\frac{m_1.m_2}{\gcd(m_1.m_2)} \qquad \ldots(3.6)$$

Equations (3.5) and (3.6) are equals, then, for n=2, equation (3.4) is true.

Assume equation (3.4) is true is true, we have to prove it's true for n+1, this means:

$$\text{lcm}(m_1,m_2,\ldots,m_n,m_{n+1})=\frac{\prod_{i=1}^{n+1} m_i}{GCD_{n+1}(m_i)}$$

Where $GCD_{n+1}=\gcd(\prod_{i=1}^{n} m_i, m_n.GCD_n)$

Let $m_i=\prod_{j=1}^{k} p_j^{a_{ij}}$, where p_j are distinct prime numbers, a_{ij} are non-negative integers, then:

$\text{lcm}(m_1,m_2,\ldots,m_n)=\prod_{j=1}^{k} p_j^{e_{ij}}$, where $e_{nj}=\max(a_{1j},a_{2j},\ldots,a_{nj})$.

Let $\varepsilon_{2j}=\min(a_{1j},a_{2j})$, then $e_{nj}=\max(\sum_{i=1}^{2} a_{ij}-\varepsilon_{2j},a_{3j},\ldots,a_{nj})$.

From reapplying the above equation we get:

$e_{nj}=\sum_{i=1}^{n} a_{ij}-\varepsilon_{nj}$, where $e_{nj}=\max(\sum_{i=1}^{n-1} a_{ij},a_{nj}+\varepsilon_{n-1,j})$

Assuming equation (4.2) is true means:

$\text{lcm}(m_1,m_2,\ldots,m_n,m_{n+1})=\prod_{j=1}^{k} p_j^{e_{n+1,j}}$ where

$e_{n+1,j}=\max(e_{nj}, a_{n+1,j})=e_{nj}+a_{n+1,j}-\min(e_{nj}, a_{n+1,j})$

$$=\sum_{i=1}^{n} a_{ij} - \varepsilon_{nj} + a_{n+1,j} - \min(e_{nj}, a_{n+1,j}) = \sum_{i=1}^{n+1} a_{ij} - \varepsilon_{nj} - \min(e_{nj}, a_{n+1,j})$$

$$=\sum_{i=1}^{n+1} a_{ij} - \min(e_{nj}+\varepsilon_{nj}, a_{n+1,j}+\varepsilon_{nj}) = \sum_{i=1}^{n+1} a_{ij} - \min(e_{nj}+, a_{n+1,j}+\varepsilon_{nj}) = \sum_{i=1}^{n+1} a_{ij} - \varepsilon_{n+1,j}$$

where $\varepsilon_{n+1,j} = \min(\sum_{i=1}^{n+1} a_{ij}, a_{n+1,j}+\varepsilon_{nj})$.

$$\text{lcm}(m_1,m_2,\ldots,m_n,m_{n+1}) = \prod_{j=1}^{k} p_j^{e_{n+1,j}} = \prod_{j=1}^{k} P_j^{\sum_{i=1}^{n+1} a_{ij} - \varepsilon_{n+1,j}} = \frac{\prod_{j=1}^{k} P_j^{\sum_{i=1}^{n+1} a_{ij}}}{\prod_{j=1}^{k} P_j^{\sum_{i=1}^{n+1} \varepsilon_{n+1,j}}}$$

$$= \frac{\prod_{i=1}^{n+1} \prod_{j=1}^{k} P_j^{a_{ij}}}{\prod_{j=1}^{k} P_j^{\min\left(\sum_{i=1}^{n} a_{ij}, \varepsilon_{nj}, a_{n+1,j}\right)}} = \frac{\prod_{i=1}^{n+1} m_i}{\gcd\left(\prod_{i=1}^{n} m_i, m_{n+1}, GCD_n\right)}$$

$\therefore$ equation (3.4) is true for n+1, then its true $\forall$n. ■

Example (3.1): Let m_1=4, m_2=10 and m_3=15, then:

L.H. of equation (3.4), lcm(4,10,15)=60.

R.H. of equation (3.4):

(4*10*15)/GCD(4,10,15)=600/gcd(4*10,15*gcd(4,10))=600/gcd(40,30)=600/10=60.

From theorem (3.1), we obtain:

$$P(S) = \frac{\prod_{i=1}^{n} P(S_i)}{GCD_n(P(S_i))} \qquad \ldots(3.7)$$

s.t. $GCD_n(P(S_i)) = \gcd\left[\prod_{i=1}^{n-1} P(S_i), P(S_n) \cdot GCD_{n-1}(P(S_i))\right]$

The period of S which product from KG depends on the LFSR unit only and there is no effect of CF unit, so we need no discussion for any studied cases of the three KG's.

P(S) will has lower bound when $r=r_i$ $\forall 1\le i\le n$, and upper bound when $P(S_i)$ are relatively prime with each other $\forall i$, then $GCD_n(P(S_i))=1$, therefore:

$$P(S_r)\le P(S)\le \prod_{i=1}^{n} P(S_i)$$

The objective is that KG efficiency must have an upper bound to P(S)

s.t. $P(S)=\prod_{i=1}^{n} P(S_i)$ …(3.8)

The condition to construct efficient KG is "The periods (and automatically lengths) of combined LFSR's must be relatively prime".

It's known earlier that $P(S_i)\le 2^{r_i}-1$, and if the $LFSR_i$ has maximum period then $P(S_i)= 2^{r_i}-1$, to gain maximum P(S), so if the 2nd condition has been satisfied, then $P(S)=\prod_{i=1}^{n}(2^{r_i}-1)$, so the other condition is "Each of the combined LFSR's in KG must have maximum period". Let's suppose that the 2nd and 3rd conditions are holding from know.

Example (3.2):

Table (1) shows some examples of periods of KG's.

Table (1) Periods of different examples of KG's.

n	r_i	$P(S_i)$	P(S)
3	2,3,5	3, 7, 31	651
3	4,5,7	15, 31, 127	59055
4	2,3,5,7	3, 7, 31, 127	82677