Lecture Four

Basic Efficiency Criteria of LFSR's-Systems

6. Randomness Criterion

The sequence that is satisfied the 3-randomness properties called PRS. The randomness criterion depends on LFSR's and CF units, therefore from the important conditions to get PRS is, the sequence must be maximal and CF must be balance, the condition can be deduced, which is said "CF must be balance".

To guarantee the KG produces PRS, the sequence must pass randomness tests with complete period, these tests applied in two ways, on:

1. Global sequence for complete period and that is the right way (but it's hard to apply for high periods).
2. Local sequence for many times for various lengths less than the period.

In this part, the 1st way will be applied theoretically for any period.

In general, if $GCD_n(P(S_i))=1$ then,

$$P(S)=2^{\sum_{i=1}^{n} r_i}+(-1)\cdot(2^{r_1+\cdots+r_{n-1}}+\cdots+2^{r_2+\cdots+r_n})+\cdots+(-1)^{n-1}\cdot(2^{r_1}+\cdots+2^{r_n})+(-1)^n \ldots(6.1)$$

Let R_m^t denotes the combination to sum m of numbers r_i from n of the numbers r_i, R_m denotes the set of all possibilities of R_m^t s.t.

$$R_m^t=\begin{pmatrix} r_1,r_2,\ldots,r_n \\ \sum_{j=1}^{m} r_{i_j} \end{pmatrix} 0\le m\le n,\ 1\le i\le n,\ t\in\{1,2,\ldots,C_m^n\}$$

define $R_0=\{R_0^1\}$, $R_0^1=0$.

For instance let m=1 then $R_1=\{R_1^1,R_1^2,\ldots,R_1^{C_1^n}\}, R_1^1=r_1,\ldots,R_1^n=r_n$

If m=n then $R_n=\{R_n^1\}$, $R_n^1=\sum_{i=1}^{n} r_i$

So equation (6.1) can be written in compact formula:

$$P(S)=\sum_{k=0}^{n}(-1)^k\cdot\sum_{t=1}^{C_k^n}2^{R_{n-k}^t} \quad \ldots(6.2)$$

Golomb deduced three theorems about the Maximal Sequence (MS) generated from LFSR. The three Golomb' theorems deduced from the three randomness postulates; **frequency**, **run** and **autocorrelation**. In the next sections we will introduce new theorems, as Golomb do on LFSR to calculate theses postulates to a system of LFSR's.

6.1 Frequency Postulate

1st theorem about frequency s.t. $N_r(0)=2^{r-1}-1$, $N_r(1)=2^{r-1}$, $N_r(a)$ denotes the number of bit "a" in the MS S_r which generates from LFSR with length r s.t.

$$P(S_r)=2^r-1=(2^{r-1}-1)+2^{r-1}=\sum_{a=0}^{1}N_r(a)$$

Let $N_S(a)$ be the frequency of bits "a" in S then

$$P(S)=\sum_{a=0}^{1}N_S(a)=N_{r_1}(0)\cdots N_{r_n}(0)+N_{r_1}(0)\cdots N_{r_n}(1)+\cdots+N_{r_1}(1)\cdots N_{r_n}(1)\ldots(6.3)$$

From equation (6.3) the act of CF will starts to distribute the proportion of "0" and "1" in S. If the terms of equation (6.3) rearranged s.t. $0=F(a_{i1},a_{i2},..,a_{in})$, $1\le i\le m_0$ for the 1st m_0 terms, and $1=F(a_{i1},a_{i2},..,a_{in})$, $1\le i\le m_1$ for 2nd m_1 terms $2^n=m_0+m_1$ then,

$$N_S(a)=\sum_{i=1}^{m_a}\prod_{j=1}^{n}N_{r_j}(a_{ij})$$

subject to $a=F(a_{i1},a_{i2},..,a_{in})$ s.t. $1\le i\le m_a$,a=0,1

m_a denotes the number of states which are subject to above condition.

Now we will apply this postulate on the three KG's.

The linear function is balance and symmetric (which expect that the LKG will produces PRS).

e.g. using equation (6.4), let n=2, then

$$N_S(0) = N_{r_1}(0) \cdot N_{r_2}(0) + N_{r_1}(1) \cdot N_{r_2}(1) = 2^{r_1+r_2-1} - (2^{r_1-1} + 2^{r_2-1}) + 1$$

$$N_S(1) = N_{r_1}(0) \cdot N_{r_2}(1) + N_{r_1}(0) \cdot N_{r_2}(1) = 2^{r_1+r_2-1} - (2^{r_1-1} + 2^{r_2-1})$$

from above equations, $N_S(0)=N_S(l)+1$.

In general:

$N_S(0)= N_S(1)+(-l)^n$ ...(6.4)

Directly from equation (6.4), a new equation which is easy to calculate $N_S(a)$ is obtained by using the next theorem.

Theorem (6.2): Let $N_S(a)$ be the number of a-bit in the sequence S generated from n-LKG, $a \in \{0,1\}$, then:

$N_S(a)=\frac{1}{2}(P(S)+(-1)^{n+a})$, a=0,1. ...(6.5)

Example (6.3): Table (5) shows various examples for $N_S(0)$ and $N_S(1)$ of n-LKG.

Table (5) various frequency examples of n-LKG.

n	**r_i**	**P(S)**	**$N_S(0)$**	**$N_S(1)$**
2	3,5	217	109	108
3	2,3,5	651	325	326
4	2,3,5,7	82677	41339	41338

6.2 Run Postulate

The next equation shows a linear relation between the periodicity of n-KG and the periodicity of combination of one or number of combined LFSR in the system.

$$P(S)=\sum_{k=0}^{n-1}(-1)^k\sum_{t=1}^{C_k^n}P(R_{n-k}^t) \qquad \ldots(6.6)$$

Where R_m^n represents the combination of m LFSR's of n-KG, where $1\le m\le n$, s.t.

$$P(R_m^t)=2^{R_m^t}-1=2^{R_m^{t-1}}-1+2^{R_m^{t-1}}=\sum_{a=0}^{1}N_{R_m^t}(a) \qquad \ldots(6.7)$$

$N_{R_m^t}(a)$ denotes the number of binary of kind "a" of the sequence which is generated from the component R_m^t.

Now we can calculate the runs of S depending on the runs of the maximal Sequences which are generated from the combinations R_m^t which are known.

Let $N_j^{R_m^t}(a)$ be the number of runs (a=0 for gaps and a=1 for blocks) with length j for the combinations R_m^t, and $N_j^S(a)$ be the number of runs of kind a with length j for the sequence S.

We can reformulate the **second Golomb's postulate** by:

$$\left.\begin{array}{ll} 1. & N_{R_m^t}^{R_m^t}(1)=N_{R_m^t-1}^{R_m^t}(0)=1 \\ 2. & N_{R_m^t}^{R_m^t}(0)=N_{R_m^t-1}^{R_m^t}(1)=0 \\ 3. & N_j^{R_m^t}(a)=2^{R_m^t-j-2} \quad \text{When } 1\le j\le R_m^t-2,\ a=0,1 \end{array}\right\} \qquad \ldots(6.8)$$

The next lemma discuses the relation between the $P(R_m^t)$ and the elements of the equation (6.7).

Lemma (6.1): $$P(R_m^t) = \sum_{j=1}^{R_m^t} j \sum_{a=0}^{1} N_j^{R_m^t}(a) \quad \ldots(6.9)$$

Now we are ready to calculate the runs of the sequence S generated from linear system.

Theorem (6.3): $$\overset{S}{N}_j(a) = \sum_{k=0}^{n-1} (-1)^k \sum_{t=1}^{C_k^n} N_j^{R_{n-k}^t}(a) \quad \ldots(6.10)$$

From equation (6.10) we can calculate the runs j of S, $1 \le j \le R_n^1$ for the linear system.

Example (6.4): Table (6) describes the calculating of runs j of the sequence S generated from the linear system using $r_1=2$, $r_2=3$.

Table (6) Calculating of runs j of S generated from the 2-LKG.

		+1	**-1**			
j	**a**	R_2^1**=5**	R_1^1**=2**	R_1^2**=3**	$\overset{S}{N}_j(a)$	$N_S(a)$
1	0	4	1	1	2	2
	1	4	0	1	3	3
2	0	2	0	1	1	2
	1	2	1	0	1	2
3	0	1	0	0	1	3
	1	1	0	1	0	0
4	0	1	0	0	1	4
	1	0	0	0	0	0
5	0	0	0	0	0	0
	1	1	0	0	1	5
Sum		$2^5-1=31$	$2^2-1=3$	$2^3-1=7$	**21**	**P(S)**

Notice that from table (6) and equation (6.10), there is a little difference between the $\overset{S}{N}_j(0)$ and $\overset{S}{N}_j(1)$ values that will gives a balance output which implies that S will pass the run test successfully. The next lemma proves the 2nd Golomb randomness for runs of linear system.

Lemma (6.2): For the sequence S generated from linear system:

1. $\overset{S}{N}_{j+1}(a) = \frac{1}{2}\overset{S}{N}_j(a)$, for $1 \le j \le R_n^1$
2. $\overset{S}{N}_j(0) = \overset{S}{N}_j(1)$, for $1 \le j \le R_n^1 - 2$

6.3 Auto Correlation Postulate

Before we involve in details of calculating this part of randomness criterion we have to give some preliminaries.

Let $S_r = \{a_j\}_{j=0}^{p(S_r)-1}$ be the sequence generated from maximum LFSR, s.t. $a_j \in \{0,1\}$. In corresponding let $Q_r = \{b_j\}_{j=0}^{p(S_r)-1}$ denotes the transform sequence gotten from the following linear transform:

$b = 1 - 2a$ ...(6.11)

Where $b_j \in \{-1,1\}$.

a=0,1, then is corresponding b=-1, 1 respectively.

Definition (6.1): When the LFSR has maximum period st. $P(S_r) = 2^r - 1$, then its can generates k sequences A_k, $1 \le k \le P(S_r)-1$, each generated using the initial vector v_k s.t. $A_k = \{a_{k_j}\}_{j=0}^{p(S_r)-1}$, $(A_0 = \{0,0,\ldots,0\})$, then the set $A = \{A_0, A_1, \ldots, A_{P(Sr)-1}\}$ with XOR $\oplus$ operation $\langle A, \oplus \rangle$ form a group.

Golomb mentioned that for MS the $\sum_{i=0}^{P(S_r)-1} a_i = 1$ and $\sum_{i=0}^{P(S_r)-1} b_i = -1$, and $P(S_r) = P(Q_r) = N_Q(1) + N_Q(-1)$.

Definition (6.2): Let $B_k=\{b_{k_j}\}_{j=0}^{P(S_r)-1}$ be the corresponding to A_k mentioned above when $0\le k\le P(S_r)-1$, ($B_0=\{1,1,\ldots,1\}$), then they form a set $B=\{B_0,B_1,\ldots,B_{P(Sr)-1}\}$.

Lemma (6.3): Let $B=\{B_0,B_1,\ldots,B_{P(r)-1}\}$ be a non-empty set as defined above, then $\langle B,\cdot\rangle$ is group.

Definition (6.3): Lets $C_r(\tau)$ be the auto correlation function of maximal function which is generates from LFSR with length r and shifted by integer τ s.t

$$C_r(\tau)=\frac{1}{P(S_r)}d_r(\tau),\ \text{where}$$

$$d_r(\tau)=\sum_{k=0}^{P(S_r)-1}b_k b_{k+\tau}=\begin{cases}1 & \tau=0,P(S_r)\\ -\dfrac{1}{P(S_r)} & 0\le\tau\le P(S_r)\end{cases} \qquad \ldots(6.12)$$

Remark (6.1): $d_r(\tau)$ can represents the difference between $N_r(1)$ and $N_r(-1)$ of the sequence Q_r after shifted by τ.

Definition (6.4): The auto correlation function $C_S(\tau)$ of the sequence S (or the corresponding sequence Q) which is generated from system of LFSR's can be defined as follows:

$$\left.\begin{aligned}C_S(\tau)&=\frac{1}{P(S)}d_S(\tau),\ \text{where}\\ d_S(\tau)&=\sum_{k=0}^{P(S)-1}q_k q_{k+\tau}\end{aligned}\right\} \qquad \ldots(6.13)$$

Where $q_k\in\{-1,1\}$ is the element k of the sequence Q.

Remark (6.2): $d_S(\tau)$ represents the difference between $N_r(1)$ and $N_r(-1)$ of the sequence Q after shifted τ.

Definition (6.5): Let T_k^t denotes the combination to multiply k of $P(S_i)$ from the total number n of $P(S_i)$, $1\le i\le n$.

Let T_k denotes the set of all possibilities of T_k^t, s.t.

$$T_k^t = \begin{pmatrix} P(S_1),..P(S_n) \\ \prod_{i=1}^{k} P(S_{ij}) \end{pmatrix},\ 0\le k\le n,\ t\in\{1,2,\ldots,\ C_k^n\},$$

we defined $T_0=\{T_0^1\},\ T_0^1=1$

For instance, let k=1, then $T_1=\{T_1^1,T_1^2,...,T_1^n\},\ T_0^i=P(S_i),\ 1\le i\le n$.

When k=n, then $T_1=\{T_n^1\}$, s.t. $T_n^1=\prod_{j=1}^{n} P(S_j)$

Definition (6.6): Let the CF be F_n, s.t. $F_n:A\to\{0,1\}$, let H_n be the corresponding function of F_n s.t. $H_n:B\to\{-1,1\}$.

Lemma (6.4): If F_n is the linear function s.t. $s=F_n(a_1,a_2,\ldots,a_n)=\sum_{i=1}^{n}{}^{\oplus} a_i$, then

$q=H_n(b_1,b_2,\ldots,b_n)=\prod_{i=1}^{n} b_i$

Where s and q are the output element of the functions F_n and H_n respectively.

Now we will apply the autocorrelation on n-LKG theoretically.

$q_m=\prod_{i=1}^{n} b_{im}$, therefore,

$$\sum_{m=0}^{P(S)-1} q_m = \sum_{m=0}^{P(S)-1}\prod_{i=1}^{n} b_{im} \qquad \ldots(6.14)$$

This relation shows the difference between $N_S(-1)$ and $N_S(1)$ in the sequence S, since the sequence $\{b_{im}\}$ represents MS with period $P(S_i)=2^{r_i}-1$, so the above relation can be written as:

$$\sum_{m=0}^{P(S)-1} q_m = (-1)^n \qquad \ldots(6.15)$$

Now we will shifting S (or Q) by τ, $0<\tau<P(S)$ to find $C_S(\tau)$ by using the next theorem.

Theorem (6.4): $$d_S(\tau)=\prod_{i=1}^{n} d_{r_i}(\tau_i) \qquad \ldots(6.16)$$

s.t. τ_i denotes the phase shift of the sequence Q_i, and,

$$d_{r_i}(\tau_i) = \begin{cases} P(S_i), & \tau_i=0, P(S_i). \\ -1, & 0<\tau<P(S_i). \end{cases} \qquad \ldots(6.18)$$

From equation (6.18) and by using 3rd Golomb postulate, two states can be concluded when $0<\tau<P(S_i)$:

1. if $\tau \not\equiv 0 \pmod{T_k^t}$, $\forall 1\le k\le n$, $t\in\{1,2,\ldots,C_k^t\}$, then:

   $$d_S(\tau)=\prod_{i=1}^{n} d_{r_i}(\tau_i) = \prod_{i=1}^{n}(-1) = (-1)^n \qquad \ldots(6.19)$$

   this implies $C_S(\tau)=(-1)^n/P(S)$.

2. if $\tau \equiv 0 \pmod{T_k^t}$, for some $1\le k\le n$, then:

   if k=1 this implies $d_S(\tau)=(-1)^n.P(S_i)=(-1)^{n-1}.T_1^i$, $1\le i\le n$.

   since the linear system is symmetric (we can rearrange the LFSR's in the KG),

   if $k=j \Rightarrow d_S(\tau)=(-1)^{n-j}.\prod_{i=1}^{j} P(S_i)=(-1)^{n-j}.T_j^t$, $1\le i,j\le n$, $t\in\{1,2,\ldots,C_k^t\}$.

   If $k=n \Rightarrow d_S(\tau)=(-1)^{n-n}.\prod_{i=1}^{n} P(S_i)=P(S)$.

   In general,

$d_S(\tau)=(-1)^{n-k}.\ T_k^t = t\in\{1,2,\ldots,\ C_k^t\}$ …(6.20)

$\therefore C_S(\tau)=(-1)^{n-k}.\ T_k^t/P(S).$

Example (6.4):

Let n=3, $r_1=2$, $r_2=3$, $r_3=5$, $C_1^3=3$, $C_2^3=3$, $C_3^3=1$.

$\therefore T_1^1=3,\ T_1^2=7,\ T_1^3=31,\ T_2^1=21,\ T_2^2=93,\ T_2^3=217,\ T_3^1=651.$

1. if $\tau\not\equiv 0\ (\mathrm{mod}\, T_k^t)$, $\forall 1\le k\le 3$, then:

   $d_S(\tau)=-1$ and $C_S(\tau)=-1/651$.

2. if $\tau\equiv 0\ (\mathrm{mod}\, T_k^t)$, for $1\le k\le 3$, then:

   a. k=1, $d_S(\tau)=3, 7, 21$.

   b. k=2, $d_S(\tau)=-21, -93, -217$.

   c. k=3, $d_S(\tau)=651$.

Table (7) shows $d_S(\tau)$ for some values of τ from the example (6.4).

Table (7) $d_S(\tau)$ for some values of τ of linear system.

τ	$d_S(\tau)$	τ	$d_S(\tau)$	τ	$d_S(\tau)$	τ	$d_S(\tau)$	τ	$d_S(\tau)$
1	-1	11	-1	21	-21	31	31	61	-1
2	-1	12	3	22	-1	32	-1	62	31
3	3	13	-1	23	-1	33	3	63	-21
4	-1	14	7	24	3	34	-1	92	-1
5	-1	15	3	25	-1	35	7	93	-93
6	3	16	-1	26	-1	36	3	94	-1
7	7	17	-1	27	3	37	-1	216	3
8	-1	18	3	28	7	38	-1	217	-217
9	3	19	-1	29	-1	39	3	650	-1

10	-1	20	-1	30	3	40	-1	651	651

Notice that from table (7) the frequency of $d_S(\tau)=-1$ is more than other values, that because of the 1st state occurs more than the 2nd state. The 1st state occurs exactly $\Phi(P(S))$, since its represents the number of the relatively prime numbers with P(S). Actually, we know that $P(S)=\prod_{i=1}^{n} P_i=\prod_{i=1}^{n}(2^{r_i}-1)=\prod_{i=1}^{n} p_i^{q_i}$, where p_i are primes chosen as large as possible and q_i are non-negative integers, then p_i-1 approaches p_i, that implies $\Phi(P(S))$ approaches P(S), and that what will proved in the next lemma.

Lemma (6.5): The proportion of $\Phi(P(S))$ to P(S) is approach 1, i.e. $\frac{\Phi(P(S))}{P(S)}\approx 1$.

Example (6.5):

Table (8) shows the proportion of Φ(P(S)) to P(S) for various lengths.

Table (8) the proportion of Φ(P(S)) to P(S) for various lengths.

n	r_i	$P(S_i)$	P(S)	Φ(P(S))	Proportion
2	2,5	3,31	93	60	65%
	3,4	7,15	105	48	46%
3	2,3,5	3,7,31	651	360	55%
	3,5,7	7,31,127	27559	22580	82%
	5,7,13	31,127,8191	32247967	3095820	96%