Linear Complexity Measures of Binary Multisequences

Sindhu. M
Amrita Vishwa Vidyapeetham
Coimbatore, Tamil Nadu
India

M. Sethumadhavan
Amrita Vishwa Vidyapeetham
Coimbatore, Tamil Nadu
India

ABSTRACT

The joint linear complexity and k - error joint linear complexity of an m fold 2^n periodic multisequence can be efficiently computed using Modified Games Chan algorithm and Extended Stamp Martin Algorithm respectively. In this paper we derived an algorithm for finding the joint linear complexity of 3.2^n periodic binary multisequence with the help of Modified Games Chan algorithm. Here we derived the minimum value of k for which k-error joint linear complexity is strictly less than the joint linear complexity of binary m fold multisequences of period 2^n and an algorithm which, given a constant c and an m fold 2^n periodic binary multisequence S, computes the minimum number k of errors and the associated error multisequence needed over a period of S for bringing the joint linear complexity of S below c .

General Terms

Cryptography, Applied Number theory, Word Based Stream Ciphers, Linear Complexity of sequences, Joint Linear Complexity of sequences

Keywords

Word based stream ciphers, multisequences, error multisequence, joint linear complexity, k-error joint linear complexity, k_{min} .

1. INTRODUCTION

Complexity measures for keystream sequences over finite fields, such as the linear complexity and the k-error linear complexity, is of great relevance to cryptology, in particular, to the area of stream ciphers. The immense majority of proposed keystream generators are based on the use of linear feedback shift registers (LFSR). The length of the shortest LFSR which generates the given sequence is known as the linear complexity of the sequence. A necessary requirement for unpredictability of keystream sequence is long period, which can be attained by large linear complexity. Recent developments in stream ciphers point towards an interest in word based stream ciphers which require the study of complexity theory of multisequences i.e., of parallel streams of finitely many sequences, and of their complexity properties ([3],[4],[11]). A cryptographically strong sequence should not only have a large linear complexity, but also changing a few terms should not cause any significant decrease of the linear complexity. This unfavorable property leads to the concept of k-error linear complexity [11]. Recently many authors studied various properties of k-error linear complexity of single and multisequences ([2],[4],[5],[8],[9],[10],[11],[13],[14],16],[18] and [19]). In [17] Stamp and Martin presented an efficient algorithm for finding the k-error linear complexity of N periodic binary sequences, where $N = 2^{\nu}, \nu \geq 0$ for $0 \leq k \leq N$ in linear time, which was a generalization of the Games Chan algorithm [3] which computes the linear complexity of 2^{ν} periodic binary sequences in linear time. Further Lauder-Paterson algorithm [8] was generalized to compute the k-error linear complexity spectrum of sequences over F_q with period 2^{ν} in [6]. In [1], Anna Salagean developed an algorithm which, given a constant c and a binary sequence with period 2^{ν} , computes the minimum number k of errors needed over a period for bringing the linear complexity of the sequence to below the value c.

In [19] a survey of existing algorithms for finding the linear complexity and k-error linear complexity of N periodic sequences over a finite field F_q were given. Algorithms for finding Joint linear complexity and error joint linear complexity of m fold p^v periodic (p prime) sequences over $GF(p^m)$ were also discussed in [18]

2. MULTISEQUENCES

Multisequences are parallel streams of finitely many single sequences. Let $S = (S^{(1)}, S^{(2)}, ..., S^{(m)})$ denote an m fold N periodic multisequence consisting of m parallel sequences $S^{(1)}$, $S^{(2)}$, ..., $S^{(m)}$ each of period N over a finite field F_q where $q = p^n$, p prime.

3. Joint Linear complexity

Consider an m fold N periodic multisequence $S = (S^{(1)}, S^{(2)}, ..., S^{(m)})$ over F_q. Then the *joint linear complexity* of S denoted by $JLC(S)$ is defined as the least order of a linear recurrence relation over F_q that $S^{(1)}$, $S^{(2)}$, ..., $S^{(m)}$ satisfy simultaneously. The polynomial of minimal degree which generates a given multisequence is called its *minimal connection polynomial*. This polynomial generates each sequence of the multisequence ([15]).

3.1 Theorem 1 ([15])

The necessary and sufficient condition for the polynomial $C(D)$ to be the minimal connection polynomial of the given N periodic m fold multisequence $S = (S^{(1)}, S^{(2)}, ..., S^{(m)})$ over F_q where $S^{(h)} = (s_0^{(h)}, s_1^{(h)}, ..., s_{N-1}^{(h)})$, h =1,2, …, m are the following

(i) $S^{(i)}(D)C(D) = P_i(D)(1 - D^N)$, i = 1,2, …, m.

(ii) deg $P_i(D)$ < deg $C(D)$, i = 1, 2, ..., m

(iii) gcd ($P_1(D)$, $P_2(D)$, ..., $P_m(D)$, $C(D)$) = 1

3.2 Corollary 1

Let $S = (S^{(1)}, S^{(2)}, .., S^{(m)})$ where $S^{(h)} = (s_0^{(h)}, s_1^{(h)}, .., s_{N-1}^{(h)})$ for h =1,2, …,m be an m fold N periodic multisequence over

F_q. Then its minimal connection polynomial is given by

$$C(D)=\frac{1-D^N}{\gcd(S^{(1)}(D),S^{(2)}(D),\ \dots,S^{(m)}(D),1-D^N)}.$$

Then the joint linear complexity of the given multisequence is given by([19])

$$JLC(S)=N-\deg(\gcd(S^{(1)}(D),$$
$$S^{(2)}(D),\dots,S^{(m)}(D),1-D^N))$$

3.3 An algorithm for computing the joint linear complexity of *m* fold 3.2^v periodic multisequence ([17])

In order to reduce the computations for finding the joint linear complexity of *m* fold 3.2^v periodic binary multisequences, we are reducing it into *m* fold 2^v periodic multisequences and applying the Modified Games Chan algorithm on them in a particular way. For that we modify an algorithm due to Meidl [12] derived for single sequences of period 3.2^v to the case of *m* fold multisequences of period 3.2^v

3.3.1 Algorithm 1

Consider an *m* fold $N = 3.2^v$ periodic multisequence $S=(S^{(1)},S^{(2)},\dots,S^{(m)})$ where $S^{(h)}=(s_0^{(h)},s_1^{(h)},\dots,s_{N-1}^{(h)})$, h = 1, 2, …, *m*. For *i* = 0, 1, 2 let

$$S_i^{[h,3]}=(s_0^{(h,i)},s_1^{(h,i)},\dots,s_{N-1}^{(h,i)})$$

where

$$s_p^{(h,i)}=\begin{cases} s_p^{(h)} \ \mathit{if}\ \ p\, \mathit{is\, not\, congruent\, to}\, i (\mathrm{mod}\, 3) \\ 0 \ \ \mathit{otherwise}\end{cases}$$

for $h = 1, 2, \dots, m$, $p = 0, 1, \dots, N-1$

Build *m* fold 2^v periodic multisequences as follows.

$$A=(A^{(1)},A^{(2)},\dots,A^{(m)})$$

where $A^{(h)}=(a_0^{(h)},a_1^{(h)},\dots,a_{2^v-1}^{(h)})$

with $a_p^{(h)}=s_p^{(h)}+s_{p+2^v}^{(h)}+s_{p+2*2^v}^{(h)}$ for h = 1 , 2, …, *m* and p = 0 , 1, …, 2^v - 1

for *i* = 0,1,2 compute

$$A_i^{[h,3]}=(a_0^{[h,i]},a_1^{[h,i]},\dots,a_{2^v-1}^{[h,i]})$$

where $a_p^{[h,i]}=s_p^{(h,i)}+s_{p+2^v}^{(h,i)}+s_{p+2*2^v}^{(h,i)}$ for h = 1,2,…,*m* and p = 0, 1, …, 2^v - 1.

Then

$$JLC(S)=JLC(A)+\max(JLC(A_1^{[h,3]}),JLC(A_0^{[h,3]}))+$$
$$\max(JLC(A_2^{[h,3]}),JLC(A_0^{[h,3]}))$$

It is possible to reduce the calculation of the joint linear complexity of *un* periodic sequence over a finite field F_{p^m} to the calculation of the joint linear complexities of *u* multisequences over F_{p^m} of period *n* under the condition that *u* divides $p^m-1$and *gcd* (*n*, p^m-1) = 1. These conditions guarantee that there exist exactly *u* distinct *u*th roots of unity x_0 = 1, x_1, …, x_{u-1} in $S=(S^{(1)},S^{(2)},\dots,S^{(m)})$ and we can find unique $b_i\in F_{p^m}$ such that $b_i^n=x_{i,}, i=0,1,\dots,u-1$. Following proposition is a generalization of a result in [5].

3.3.2 Proposition 1

Suppose *p, m, u , n*, x_0, … , $x_{u\text{-}1}$, b_0, … , b_{u-1} are given as above. Let $S=(S^{(1)},S^{(2)},\dots,S^{(m)})$ be a multisequence over F_{p^m} where $S^{(h)}=(s_0^{(h)},s_1^{(h)},\dots,s_{N-1}^{(h)})$, for *h* = 1, 2, … , *m* and *i* = 0, 1, … , *u* – 1 and let $S_i^{[h,u]}=(s_0^{(h,i)},s_1^{(h,i)},\dots,s_{n-1}^{(h,i)})$ for *h* = 1, 2, … , *m* be the *n* periodic sequence with *k*th term $s_k^{(h,i)}=s_k^{(h)}b_i^k+s_{n+k}^{(h)}b_i^{n+k}+\dots+s_{(u-1)n+k}^{(h)}b_i^{(u-1)n+k}$ for $0\le k\le n-1$. Then the joint linear complexity of *S* is given by

$$JLC(S)=JLC(S_0^{[h,u]})+JLC(S_1^{[h,u]})+\dots+$$
$$JLC(S_{u-1}^{[h,u]}).$$

From this we can observe that this proposition can be utilized for finding the joint linear complexity of a *un* periodic multisequence over a finite field F_q if *u* does not divide *q* – 1. In practice we want to obtain all binary component multisequences directly from the 3.2^v periodic binary *m* fold multisequence. The smallest integer such that 3|2*m* – 1 is *m* = 2. We will get $b_0=1, b_1=\alpha\ and\ b_2=\alpha^2$. Since b_0 = 1 the multisequence $S_0^{[h,u]}$ is binary. Rest of the proof follows from that for the single sequence case as the results used there can be extended directly to the multisequence case. Time complexity of this algorithm is $O(mN)$ where *m* is the number of sequence in the given multisequence and $N=2^v$.

4. *k*-error joint linear complexity

Let $S=(S^{(1)},S^{(2)},\dots,S^{(m)})$ and $T=(T^{(1)},T^{(2)},\dots,T^{(m)})$ be two *m* fold multisequence over F_q of the same length. A term in *S* is defined to be a term of $S^{(j)}, 1\le j\le m$. Then the term distance between *S* and *T* denoted by $\delta_T(S,T)$ is defined as the number of terms in S that are different from the corresponding terms in *T*([19]).

4.1 Definition 1

Let *S* be an *m* fold *N* periodic multisequence over F_q . For an integer *k* with $0\le k\le mN$, the *k* error joint linear complexity of *S* is defined to be the smallest possible joint linear complexity obtained by changing *k* or fewer terms of *S* in its first period of length *N* and then continuing the changes periodically with period *N*. In other words $L_{N,k}(S)=\min_T L(T)$ where the minimum is taken over all *m* fold *N* periodic multisequences *T* over F_q with term distance $\delta_T(S,T)\le k$.

We can also define the error joint linear complexity of periodic multisequences in terms of error sequence as follows

4.2 Definition 2

Let $e=(e^{(1)},e^{(2)},...,e^{(m)})$ denote an *m* fold binary multisequence of period *N* = 2^n where $e^{(i)}=(e_0^{(i)},e_1^{(i)},...,e_{N-1}^{(i)})$, *i* = 1, 2 , …. , *m*. Then *k* error joint linear complexity of an *m* fold *N* periodic binary multisequence *S* is

$$L_{N,k}(S)=\min_{W_H(E^{(i)})\le k_i} JLC(S+e),$$

$$0\le k_i\le N, k=\sum_i k_i, 0\le k\le mN, i=1,2,...,m$$

4.3 Definition 3

Define k_{min}(S) as the minimum value of *k* such that $L_{N,k}(S)<JLC(S),0\le k\le mN$.

4.4 Remark 1

We know that [7]

$$W((1-x)^t)=2^{W_H(t)} \quad and$$

$$W((1-x)^t f(x))\ge 2^{W_H(t)},\ f(1)\ne 0.)$$

Let S be an *m* fold *N* = 2^n periodic binary multisequence. Then

$$\gcd(1-x^N,S^N(x))=\gcd(1-x^N,S^{(1)}(x),$$
$$S^{(2)}(x),...\ S^{(m)}(x))=(1-x)^t$$

for some integer *t*.

Then *JLC*(*S*) = *N* – *t* ………….(1)

Also $\gcd(1-x^N,S^N(x)+e^N(x))=(1-x)^z$ for some integer *z*.

Then

$$JLC(S+\mathrm{E})=N-z \quad ……….(2)$$

So $$L_{N,k}(S)=\min_{W_H(E^{(i)})\le k_i} JLC(S+\mathrm{E})$$
$$=\min_{W_H(E^{(i)})\le k_i}(N-z)=N-\max_{W_H(E^{(i)})\le k_i} z \quad ……(3)$$

From equations (1) and (3), we can conclude that $L_{N,k}(S)<JLC(S)$ if and only if there exist an *m* fold *N* = 2^n periodic error multisequence e such that *z* > *t*.

4.5 Theorem 2

$JLC(S+e)<JLC(S)$ if and only if $e^N(x)=(1-x)^t$ $\mathcal{G}(x)$ where $\mathcal{G}(x)$ = ($g_1(x)$, $g_2(x)$, … , $g_m(x)$) and $\mathcal{G}(1)\ne 0$.

Proof: It is equivalent to show that *z* > *t* if and only if $e^N(x)=(1-x)^t$ $\mathcal{G}(x)$, (1) ≠ 0 where *z* is such that $JLC(S+e)$ = *N* – *z* and *t* is such that JLC(*S*) = *N* – *t* .

Suppose $e^N(x)=(1-x)^c$ $\mathcal{G}(x)$ and S^N(x) = (1-x)^tf(x) where $f(1)\ne 0$

Let *c* > *t*. We have

$S^N(x)+e^N(x)$ = (1-*x*)^tf(*x*)+ (1-*x*)^c $\mathcal{G}(x)$

= (1-*x*)^t$\hbar(x)$ where $\hbar(1)\ne 0$.

So *JLC*(*S*) = *N* – *t* which implies *z* = *t*. Similarly when *c* > *t* we get z < t.

When *c* = *t* we get $S^N(x)+e^N(x)$ = (1-*x*)^t [$f(x)$+ $\mathcal{G}(x)$].

Case 1: When (1) + (1) = 0, we get $S^N(x)+e^N(x)$ = (1-*x*)$^{t+1}$$\hbar$(x), $\hbar(1)\ne 0$.

Then *JLC*(*S*) = *N* – (*t*+1) which shows *z* = *t*+1 > *t*.

Case 2: When f (1)+ $\mathcal{G}(1)\ne 0$, we get *JLC*(*S*) = *N* – *t* , which shows *z* = *t*.

4.6 Theorem 3

If *N* = 2^n , then $k_{\min}(S)=2^{W_H(N-JLC(S))}$.

Proof:

From Theorem 2 we get

$$k_{\min}(S)=\min\{W[(1-x)^t\mathcal{G}(x)],\mathcal{G}(1)\ne 0\}$$

where W [(1-x)^t $\mathcal{G}(x)$] = min { W [(1-x)^t $g_i(x)$], *i* = 1,2,…. *N* –1. Then by extending the concept used in remark to the multisequence polynomial case, we get $k_{\min}(S)=2^{W_H(N-JLC(S))}$.

4.7 Remark 2

In [19] it is given that for an *m* fold $p^n,n\ge 1$ periodic multisequence *S* over F_q, where *p* is an odd prime for which *q* is a primitive root modulo p^2 and if for a unique integer *r*, $1\le r\le n$ with $(p-1)p^{n-r}\le L(S)\le p^{n-r+1}$, then $k_{\min}(S)\ge p^{r-1}$ and $L_{p^n,p^{r-1}}(S)\ge p^{n-r+1}-JLC(S)$.

In the next section we are applying Extended Stamp Martin Algorithm for multisequences of period 2^n so that given a constant *c* the proposed algorithm gives out the minimum number of errors needed so that the joint linear complexity of the given multisequence will be at least *c*.

4.8 An Algorithm for computing an error multisequence *e* of minimum cost such that $JLC(S+e)\le c$ ([17])

Ana Salagean [1] derived an algorithm for computing an error sequence *e* of minimum cost for a binary sequence of period 2^n such that $LC(S+e)\le c$. Here we derive an extension of above algorithm to the case of multisequences. Given an *m* fold binary multisequence of period 2^n and a given constant *c*, this algorithm computes the minimum number *k* of errors needed so that the joint linear complexity of given multisequence is less than or equal to *c* and the corresponding error multisequence. For this purpose we suitably modified the Extended Stamp Martin algorithm derived in [15].

Consider an *m* fold *l* = 2^n periodic multisequence

$$S = (S^{(1)}, S^{(2)}, \ldots, S^{(m)})$$

where $S^{(h)} = (s_0^{(h)}, s_1^{(h)}, \ldots, s_{N-1}^{(h)})$, $h = 1, 2, \ldots, m$.

First we are initializing $l = 2^n$, $c' = 0, k' = 0$, cost [i][j] = 1, flag [i][p] = 0, error[i][p][k] for $i = 1, 2, \ldots, m$, $j = 0, 1, \ldots, l - 1$, $p = 0, 1, \ldots, n - 1$and $k = 0, 1, \ldots, 2^{n-p} - 1$.

For $j = 0, 1, \ldots, n - 1$ do the following

Let $l = l/2$ and for $p = 0, 1, \ldots, l - 1$ compute $b = \mathrm{L}(S) \oplus \mathrm{R}(S) = (b^{(1)}, b^{(2)}, \ldots, b^{(m)})$ where $b^{(h)} = b_0^{(h)}, b_1^{(h)}, \ldots., b_{l-1}^{(h)}$ and $b_p^{(h)} = s_p^{(h)} \oplus s_{p+l}^{(h)}$ and

$$T = \sum_{k=1}^{m} \sum_{p=0}^{l-1} b[k][p] \min(\cos t[k][p], \cos t[k][p+l])$$

```
If $T = 0$ or $c' + l \geq c$, then $k' = k' + T$
   flag [$k$][$j$] = 1 for $k$ = 1 to $m$
      for $k$ = 1,2,...,m
         for $i$ = 0, 1, ...,$l - 1$
            If $b[k][i] = 1$ , then
              If cost [$k$][$i$] ≤ cost[$k$][i + $l$]
                 $s_i^{(k)} = s_{i+l}^{(k)}$,
                 cost[$k$][$i$] = cost[$k$][$i + l$] – cost [$k$][$i$] ,
                 error [$k$][$j$][$i$] = 1
             else
                 $s_i^{(k)} = s_i^{(k)}$,
                 cost [$k$][$i$] = cost [$k$][$i$] – cost [$k$][$i+l$],
                 error [$k$][$j$][$i + l$] = 1
         else
              $c' = c' + l$
              for $k$ = 1, 2, ...,$m$
                 for $i$ = 0, 1, ..., $l - 1$
                    $s_i^{(k)} = b_k^{(i)}$
                    If cost [$k$][$i$] ≤ cost [$k$][$i + l$ ] ,
                      then error[$k$][$j$][$i$] = 1
                    else cost [$k$][$i$] = cost [$k$][$i + l$ ] ,
                    error[$k$][$j$][$i + l$] = 1
for $i$ = 1, 2, ...., $m$ let $e[i][0] = 0$
for $i$ = 1, 2, ..., $m$
If $s_0^{(i)} = 1$ and $c' + l > c$ ,then
     $k' = k' + \cos t[i][0], e[i][0] = 1$,
else $e[i][0]$ = 0
for $k$ = 0,1, …,$m$ – 1, let $p$ = 1;
 for $j = n - 1, n - 2$ ,..,0 ,let $p = p * 2$;
   for $i = p/2, p/2+1, \ldots, p - 2$, let $e[k][i] = e[k][i-1]$;
    if flag[$k$][$j$] =1
       for $i$ = 0 to $p - 1$, $e[k][i] = e[k][i]$ + error[$k$][$j$][$i$]
    else
       for $i$ = 0 to $p - 1$,$e$ [$k$][$i$] = $e$ [$k$][$i$]*error[$k$][$j$][$i$].
```

We prove this algorithm using the principle of mathematical induction on *n*. We can easily see that the cost vector values *cost*[*i*][*j*] is updated at any step so that this value reflects the cost of changes in the original multisequence *S* in order to change the current element *s*[*i*][*j*] without disturbing the results of the previous steps.

We are going to show that the quantity k' computed by the above algorithm is minimal such that $LC_{k', 2^n}(S, \cos t) \leq c$. When *n* = 0, the result is obvious. Now suppose that the result is true for *n* – 1. Consider the first execution of the main *for* loop, when *j* = 0. Here the cost [i][j] vector calculates the "cost"---in terms of the number of bit changes required in the original sequence *S*---of changing the current element of the sequence without disturbing the results of any previous steps. We denote by *S*(0) and *cost*(0) the values of *S* and *cost* at the beginning of the first run of the *for* loop, and by *S*(1) and *cost*(1) their values at the end of the first run. The value *T* represents the minimal cost of making changes in the current sequence *S*(0) such as to make its left half multisequence equal to the right half. The condition "if *T* = 0 or $c' + l \geq c$" will decide whether we make these changes or not. If *T* = 0, we obviously should make these changes, as they decrease the complexity of the multisequence at no cost. If $c' + l \geq c$ it means *S*(0) has to be changed so that it has period 2^{n-1} or less. So we have to force the left half to be equal to the right half. Now we are left with the case when *T* > 0 but $2^{n-1} < c$. Not doing changes in this case will mean that we add 2^{n-1} to the current value c' of the complexity and then process the sequences *S*(1) = *b*, effectively computing the value k' as the minimal quantity such that $LC_{k', 2^{n-1}}(S(1), \cos t(1)) \leq c - 2^{n-1}$. By the induction hypothesis, this algorithm computes k' correctly. Note that *T* is exactly the minimum cost of changing all entries of *S*(1) = *b* to 0. Hence $k' \leq T$. That is not doing changes at this step is guaranteed to lead to a final cost no greater than the cost of doing changes at this step, while still keeping the complexity below the target *c*. The correctness of the computation of the error multisequence follows directly from the correctness proof as in the single sequence case. This algorithm has the time complexity $O(mN)$, where *m* is the number of sequence in the given multisequence and $N = 2^n$.

5. Conclusion

In this paper we derived algorithms for finding the complexity measures of binary multisequences of different period lengths with the help of Modified Games Chan Algorithm and Extended Stamp Martin Algorithm. Above algorithms for 2^n periodic multi sequences can also be further extended to the case of p^n periodic multisequences.

6. REFERENCES

[1] Ana Salagean, " *On the computation of the Linear Complexity and the k-Error Linear Complexity of Binary*

Sequences with Period a Power of Two" , IEEE Trans on Inform. Theory, 51:1145-1150.

[2] Ding, Xiao and Shan, "*Stability Theory of Stream Ciphers*", LNCS, Vol. 561, Springer Verlag, 1991

[3] R. A. Games and A. H. Chan, "*A fast algorithm for determining the linear complexity of a pseudorandom sequence with period* 2^n", IEEE Trans. Inf. Theory IT-29. pp 144-146 , Jan 1983.

[4] T. Kaida, "*On Algorithms for the k-Error Linear Complexity of Sequences over GF*(p^m) *with Period* p^n", Ph. D. Thesis, Kyusu Institute of Tech. Mar'99.

[5] T. Kaida, S. Uehara and K. Imamaura, *"An Algorithm for the k-Error Linear Complexity of Sequences over GF(p^m) with period p^n, p a prime",* Information and Computation 151, 147,1999.

[6] T.Kaida, "*On the generalized Lauder Paterson algorithm and profiles of the k-error linear complexity for exponent periodic sequences*", in SETA 2004, LNCS,Vol 3486, pp 166-178, 2005.

[7] Kurosawa. K**,** Sato. F, Sakata.T, Kishimoto.W, "*A relationship between linear complexity and k-error* linear *complexity* ", Information Theory, IEEE Transactions on, Vol 46, issue 2, pp 694- 698, 2000.

[8] A. Lauder, K. Paterson*, "Computing the Error Linear Complexity Spectrum of a Binary Sequence of Period 2^n",* IEEE Trans Inf. Theory, Vol. 49, pp. 273-281, Jan 2003.

[9] W. Meidl, "*Discrete Fourier Transform, Joint Linear Complexity and Generalised Joint Linear Complexity of Multisequences*", SETA 2004, LNCS, Vol.3486, pp.101 – 112, Springer, Berlin, 2005.

[10] W. Meidl and Ayineedi Venkateswarlu, "*Remarks on the k-error linear complexity of* p^n *- periodic sequences*" , Des Codes Crypt (2007) 42:181–193, 14 Nov 2006.

[11] W. Meidl, H. Niederreiter and Ayineedi Venkateswarlu, "*Error linear complexity Measures for Multisequences*" Journal of Complexity, Volume 23, Issue 2, Pages: 169-192, April 2007.

[12] W. Meidl, "*Reducing the calculation of the linear complexity of* $u2^v$ *- periodic binary sequences to Games Chan algorithm*", Des. Codes Cryptography,46:57-65,2008.

[13] H. Niederreiter, "*Linear Complexity and Related measures for Sequences*", LNCS, Vol.2094, pp. 1-7, Springer 2003.

[14] H. Niederreiter, "*The probabilistic theory of the joint linear complexity of multisequences*", in: G.Gong, T. Helleseth, H.-Y. Song, K. Yang (Eds.), SETA 2006, Lecture Notes in Computer Science, vol. 4086, Springer, Berlin, pp. 5–16, 2006.

[15] M. Sethumadhavan, Sindhu. M, Chungath Srinivasan, Kavitha.C, "*An algorithm for k-error joint linear complexity of binary multisequences*" , Journal of Discrete Mathematical Sciences & Cryptography, volume 11, No 3, June 2008

[16] M. Sethumadhavan, C. Yogha Laxmie and C.Vijaya Govindan, *"A construction of p- ary balanced sequence with large k-error linear complexity",* Journal of Discrete Mathematical Sciences and Cryptography, Vol. 9, No.2, pp.253-261, 2006.

[17] Sindhu.M, Sajan Kumar.S, M.Sethumadhavan, "*Error Linear Complexity Measures of Binary Multisequences*", Cyber Security, Cyber Crime and Cyber Forensics: Applications and Perspectives, pp 240- 249, 2011.

[18] M. Stamp and C. F. Martin, "*An Algorithm for the k-Error Linear Complexity of Binary Sequences with Period* 2^n", IEEE Trans. Inf. Theory 39, 1398-1407, 1993.

[19] A. Venkateswarlu, "*Studies on error linear complexity measures for multisequences*", PhD thesis, 2007.