J.Basrah Researches (Sciences) Vol.32. Part.2.53- 58 (2006)

Determining the linear equivalent of NLFFS by using cyclotomic cose

Kadhim Hasen Kuban
1999

ISSN –1817 –2695
Accepted, 11/11/1998

ABSTRACT

Any given periodic sequence can be generated by a family of linear feedback shift registers (LFSR) . The member of this family with least number of stages is called the linear equivalent of the given periodic sequence. Nonlinear logic (multiplication ofachosen number of bits and modulo 2 addition of the resultant), when applied to the LFSR sequences gives an output sequence called the nonlinear feedforward sequence (NLFFS) with increased complexity .

The problem of finding the complexity (linear equivalent) of NLFFS has been studied by using cyclotomic costs for the case when feedback is a primitive polynomial.

INTRODUCTION

Binary sequences generated through shift registers (see fig. 1) have been commonly used for security digital data either by bit-by-bit addition of the binary sequence to the data or by feedback encoding . In either case , the effective security provided through such devices is the complexity of the generated binary sequencer] In the study of linear sequences and their characteristic polynomials , a major role is played by the so-called cyclotomic cosets [2] . although many of the principles involved apply to every Galois field , the case of greatest practical interest, for that reason , the most widely studied ,is that of sequences and polynomials over GF(2).Section II presents a necessary background of some well-known results on the mutual relationships , and pseudo-noise (PN) sequences . Section III presents Galois field representation , section IV presents a nonlinear generators and the full steps required to determining the linear equivalent of nonlinear feedforward generators .

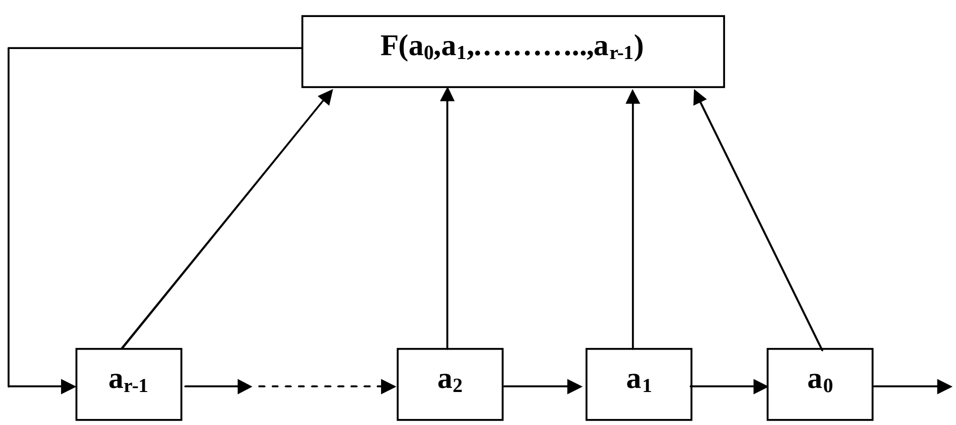

Fig.1: General feedback shift register

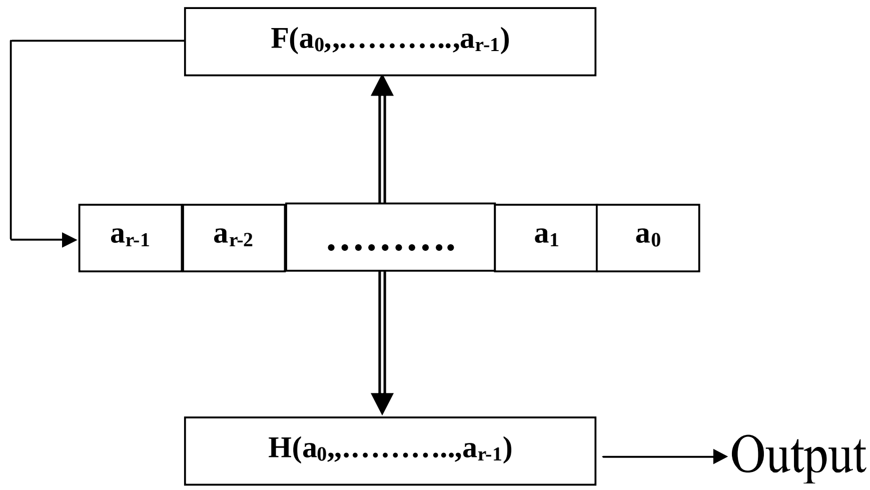

Fig.2: Nonlinear feedforward generator

BACKGROUND:

In the content of GF(2) and for a given degree n the sets referred to as cyclotomic cosets are
Obtained by partitioning the set N=(0,l,....,2n-2)mto subsets of the form

$$S(k)=\{k,2k,4k,...,2^{n-1}k\},\ k \in n \qquad (1)$$

Where the proudcts $2^i k$ are taken modulo $p=2^n-l$,$0 \leq i \leq n-1$
(k,p) denote the greatest common divisor of k and p. when (k,p)=l,S(k) is a true coset , in the usual sense of group theory , subgroup S(1)={1, 2, 4, ... ,2^{n-1} } of the multiplicative group modulo p. Cyclotomic cosets of this type will be reffered to as primitive cosets while primitive cosets always contain n distinict elements , the size of a nonprimitive cosets S(k),(k,p) $\neq$ 1 , may be either n or a divisor of n [2] .

The partitioning of n into cyclotomic cosets is closly related to the factorization of x^p+l into irreducible factors over GF(2) that are the minimal polynomails for the non-zero elements of GF(2^n) over GF(2).

Let α be a primitive root of unity so that the a powers α^i ,i Є N exhaust the nonzero elements of GF(2^n), and let R be a set of distinct representative of the cyclotomic cosets . There exists a one-to-one correspondance between the minimal polynomails $m_k(x)$ and the cyclotomic s(k) ,k Є R , under which the factorization of $m_k(x)$ into linear factors over GF(2^n) is given by [3]

$$m_k(x)=\prod_{i \in s(k)}(x+\alpha^i) \qquad (2)$$

The degree of $m_k(x)$ is equal to | s(k) |, the size of s(k) , and thus is either n or some divisor of n.(see example in section IV).

Ill GALIOS FIELD REPRESENTATION:

Consider a binary sequence $\{a_n\}$ where a_n is the nth member of the sequence , n=0, 1, 2,... if the sequence generated by an r-stage LFSR, it is completely perified by the initial loading a_o , a_1 , ... , a_{r-1} and by the linear recursion that specified feedback .

$$a_n+\sum_{i=1}^{r} c_i a_{n-i}=0 \quad ,n \geq r \qquad (3)$$

Where the sequence members an and the feedback constants ci are members of GF(2) . Also the operations of(3) are the defined operations of GF(2); namely , addition and multiplication modulo 2. In all that follows , the constant Cr is one , otherwise the register would have only r-1 effective stages . The linear recusion can be expressed as a linear difference equation

$$(E^r+\sum_{i=1}^{r} c_i E^{r-i})a_n=0 \;,\; n\geq 0 \qquad (4)$$

Where E is the shifting operation which operates on an to give an+1 , i.e , Ean=an+1 Associated with (4) is the characteristic equation .

$$x^r+\sum_{i=1}^{r} C_i X^{r-i} =0 \qquad (5)$$

An equation such as (5) with coefficient c; in GF(2) is said to be over GF(2) . Equation (5) is know to have roots in GF(2^m), where m is the least common multiple of the degree of the irreducible factors of(5). Let α be such a root. Then Aαn is asolution of(3), where A is an arbitrary constant. Likewise, each distinct root of (5) has r roots, there are r linearly independent solutions with r arbitrary constants determined by the initial values a_o ,a_1,.... ,a_{r-1}[4].

IV NONLINEAR GENERATORS :

From our prior discusion, it has been seen that the output sequence of an LFSR with irreducible polynomials is given by

$$a_n=\sum_{i=0}^{r-1} A_i\,(\alpha^{2^i})^n \qquad (6)$$

Where **α** is a root of the characteristic polynomial.

Let a^*_n be a sequence from different stage , a^*_n have the same roots as in a_n . If it is multiplied a_n , a^*_n it becomes a sequence with high complexity .In this section it is considered as sequence of that type and we present a full steps required to determined the linear equivalent of NLFFS as explained in the following
example:

<u>Example:</u> consider the generator of Fig.3

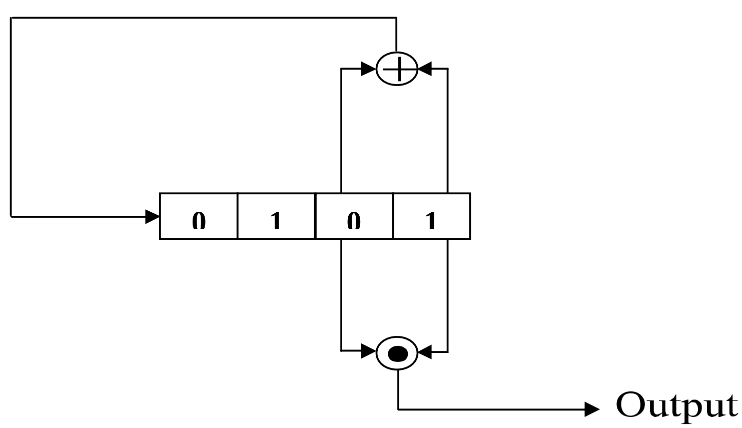

Fig .3: Nonlinear generator

To determine the linear equivalent of that generator follow the following steps:

1. **Identify the feedback relation of a given generator**

$$a_4 = a_0 + a_1$$
$$a_{n+4} = a_n + a_{n+1}$$
$$a_n = a_{n-4} + a_{n-3} \quad , n \geq 4 \qquad (7)$$

2. **Identify the characteristic polynomial associated with (7)**

$$f(x) = x^4 + x + 1 \qquad (8)$$

3. Partition the length of shift register (r=4) to corresponding cyclotomic cosets

K	s(k)	$m_k(x)$	roots of $m_k(x)$
0	0	$X+1$	$\alpha°$
1	1,2,4,8	X^4+X^3+1	$\alpha, \alpha^2, \alpha^4, \alpha^8$
3	3,6,12,9	$X^4+X^3+X^2+X+1$	$\alpha^3, \alpha^6, \alpha^{12}, \alpha^9$
5	5, 10	X^2+X+1	α^5, α^{10}
7	7,14,13,11	X^4+X+1	$\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}$

4. Use (8) to generate elements of $GF(2^4)$ as follows:

α
α^2 α is the pth root of unity
α^3
$\alpha^4 = \alpha + 1$
$\alpha^5 = \alpha^2 + \alpha$
$\alpha^6 = \alpha^3 + \alpha^2$
$\alpha^7 = \alpha^3 + \alpha + 1$
$\alpha^8 = \alpha^2 + 1$
$\alpha^9 = \alpha^3 + \alpha$
$\alpha^{10} = \alpha^2 + \alpha + 1$
$\alpha^{11} = \alpha^3 + \alpha^2 + \alpha$
$\alpha^{12} = \alpha^3 + \alpha^2 + \alpha + 1$
$\alpha^{13} = \alpha^3 + \alpha^2 + 1$
$\alpha^{14} = \alpha^3 + 1$
$\alpha^{15} = 1$

<u>5. Solve for A_i 's the following system of equations :</u>

$$l = A_0 + A_1 + A_2 + A_3$$
$$0 = A_0\,\alpha + A_1\,\alpha^2 + A_2(\alpha+l) + A_3(\alpha^2+l)$$
$$l = A_0\,\alpha^2 + A_l(\alpha+l) + A_2(\alpha^2+l) + A_3\,\alpha$$
$$0 = A_0\,a^3 A_1(\alpha^3 + \alpha^2) + A_2(\alpha^3 + \alpha^2 + \alpha + l) + A_3(\alpha^3 + \alpha)$$

the general solution is :

$$\mathbf{a_n = (\alpha^3 + \alpha + 1)\,\alpha^n + (\alpha^3 + l)\,\alpha^{2n}\,(\alpha^3 + \alpha^2 + l)(\alpha + l)^n + (\alpha^3 + \alpha^2 + \alpha)(\alpha^2 + l)^n} \qquad (9)$$

6. Achieve the multiplication of binary sequences a_n, a_{n+I}

$$a_{n+1}=(\alpha^2+l)\,\alpha^n+\alpha\,\alpha^2 n+\alpha^2(\alpha+l)^n+(\alpha+l)(\alpha^2+l)^n \qquad (10)$$

$$a_n.a_{n+1}=\alpha^n+\alpha^{2n}+(\alpha+l)^n+(\alpha^2+l)^n+(\alpha^3+\alpha^2+\alpha)\,\alpha^{3n}+(\alpha^2+\alpha)\,(\alpha^2+\alpha)^n+(\alpha^3+\alpha+l)(\alpha^3+\alpha^2)^n+(\alpha^3+\alpha^2+1)(\alpha^3+\alpha)^n+(\alpha^2+\alpha+l)(\alpha^2+\alpha+l)^n+(\alpha^3+l)(\alpha^3+\alpha^2+\alpha+1)^n \qquad (11)$$

7. Achieve multiplication of polynomials associated with roots present in (11) $m_1(x)$, $m_5(x)$, $m_7(x)$

$g(x)=m_1(x).\ m_5(x).\ m_7=x^{10}+x^5+1$
$g(x)$ is a connection polynomial of a linear equivalent.

8. Identify initial state of a linear equivalent using

$e_n=a_n\ .a_n+1$

$e_0=a_0.a_1=1.0=0$

$e_1=a_1\ ,a_2=0.1=0$

$e_2=a_2.a_3=1.0=0$

$e_9=a_9.a_{10}=0.0=0$

Finaly the connection of linear equivalent shown in Fig.4

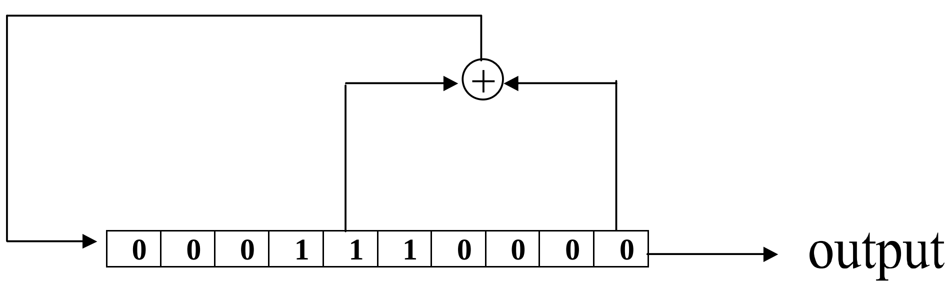

Fig.4 Linear equivalent of generator shown in fig.3

SUMMARY AND COLCLUSIONS:

The security achieved through the addition of binary sequence to a text depends upon the complexity of the added sequence. As linear operations cannot increase the complexity , a feedforward logic based on nonlinear operation (multiplication of bits) can be used to produce sequences of any desired complexity . In this paper a unified method has been formulated for determining the complexity of a nonlinear feedforward binary sequence with the aprimitive feedback polynomial. The method is based on the enumeration of the cyclotomic cosets , also it can be used to determine the complexity of feedforword sequences with any level of non-linear logic, and in addition provides the minimal generators of these sequences .

REFERENCES:

[l]-Meena Kumari, " complexity analysis of binary nonlinear feedforward sequences through minimum polynomials of compound matrices", Discrete Mathematics 56(1985)203-215, North-Holland.

[2]-S.W.Golomb, "shift register sequences". San Francisco Holden Day, 1967 .

[3]-Abraham Lempel , "Analysis and synthesis of polynomials and sequences over GF(2)", IEEE Transaction on information theory, vol. IT-17, no. 3, may 1971.

[4]-E.L.Key, " AN analysis of the structure and compelity of nonlinear binary sequences", IEEE Transaction on information theory , vol IT. 22, No.6 November 1976.

ملخص البحث :

أي متتابعة دورية periodic sequence يمكن توليدها بواسطة مسجل زاحف ذو تغذية مرتدة خطية (LFSR). اقصر مسجل زاحف أي يحوي اقل عدد من الخزانات Stages ويولد المتتابعة الدورية المعطاة يسمى بالمكافئ الخطي لتلك المتتابعة . في حالة ضرب عدد من الثنائيات bits من المسجل الزاحف ذو التغذية المرتدة الخطية وجميع الثنائيات الناتجة بالمعيار 2 نحصل على متتابعات يصطلح لها متتابعات التغذية الأمامية اللاخطية NLFFSوهذا النوع من المتتابعات يكون على درجة عالية من التعقيد . إن مسالة إيجاد التعقيد (أي المكافئ الخطي) لمتتابعات التغذية الأمامية اللاخطية تم دراستها باستخدام cyclotomic cosets عندما تكون دالة التغذية المرتدة للمسجل الزاحف عبارة عن متعدد حدود بدائي.