Complexity analysis of Geffe’s generator

Kadhim Hasen Kuban ,Msc computer science
Dept. of computer science , college of education ,university of Thi-Qar
Thiqaruni.org

Abstract:

A method of analysis is presented for the class of binary sequence generators employing the product of outputs of two or more linear feedback shift registers with maximum period.The linear feedback shift registers are represented in terms of the roots of their characteristic equations in a finite field , and it is shown that nonlinear operation inject additional roots into the representation .The number of roots required to represent a generator is a measure of its complexity , and equal to the length (number of stages) of the shortest linear feedback shift register that produces the same sequence .The analysis procedure can be applied to any arbitrary combination of binary shift registers , and is also applicable to the synthesis of complex generators having desired properties.Although the discussion in this paper is limited to binary sequences, the analysis is easily extended to similar devices that generate sequences with numbers in any finite field.

ملخص البحث

في هذا البحث أستخدمت طريقة لتحليل تعقيد متتابعة ثنائية ناتجة من ضرب مخرجات مسجلي ازاحة اوأكثر ذوات تغذية مرتدة خطية Linear Feedback Shift Registers لكل مسجل ازاحة دورة عظمى. مسجلات الازاحة الخطية تم تمثيلها بدلالة جذور متعدد الحدود المميز لدالة التغذية المرتدة وقد لوحظ ان العملية اللاخطية (عملية الضرب) تؤدي الى اضافة جذور اضافية لعملية التمثيل أي تعمل على زيادة تعقيد المولد حيث ان عدد الجذور في متعدد الحدود المميز لدالة التغذية المرتدة هو مقياس لتعقيد المولد اللاخطي وهو (أي التعقيد) مساوي الى طول اقصر مسجل ازاحة ذو تغذية خطية مرتدة يولد المتتابعة الثنائية. طريقة التحليل يمكن تطبيقها لأي عدد من مسجلات الازاحة ويمكن استخدامها لتصميم مولدات بتعقيد عالي وتمتلك الخصائص المطلوبة. في هذا البحث تم تطبيق طريقة التحليل على المتتابعات الثنائية binary sequences وبالامكان تطبيقها على متتابعات أخرى في حقول منتهية.

1-Introduction:

Shift register generators are commonly used to produce binary sequences for various purposes.Most of these generators have nonlinear feedback which is difficult to analyze , and they frequently exhibit undesirable properties , such as output sequences with very short periods.Linear feedback Shift Registers(LFSR's) figure-1 are more readily analyzed and more commonly used.However there are 2^r linear feedback connections possible with an r-stage register .It is easy to that any given periodic binary sequence can be generated by a family of LFSR's[1] The member of this family with least number of stages is called the linear equivalent of whatever generator was actually used to generate the given periodic sequence. Although there are several ways to determine the linear equivalent of a given binary sequence or to analyze its complexity, the algorithm described by Massey[2] seems at most ideal , Meena Kumari [3] uses compound matrices to analyze the complexity of such sequences also cyclotomic cosets are used to the same purpose [4].In this paper we define the complexity as the number of different roots in a characteristic polynomial of feedback function of a given r-stage LFSR.This paper presents a method of analysis based on Galios field theory that enables one to predict the generator complexity resulting from nonlinear operations .

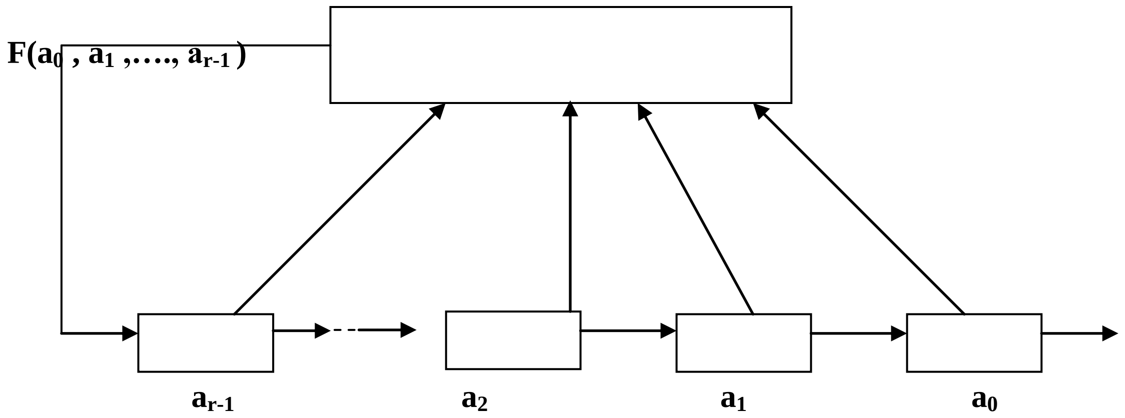

Figure-1 Linear Feedback Shift Register LFSR

2-Nonlinear generators:

LFSR's can be representeds by the roots of their characteristic equation in a Galios field[5].This representation is well suited to the analysis of nonlinear feedforward operations on LFSR's.Such nonlinear operations increase the complexity of the resulting sequence by the process of introducing new roots.The representation is also a powerful aid to the synthesis of complex generators.There are two kind of nonlinear operations applied to the LFSR:

1-The product of two or more phases of the same sequence from an r-stage primitive LFSR gives

a nonlinear feedforward sequence and the complexity (linear equivalent)of such sequences given by $\sum_{i=1}^{m}\binom{r}{i}$ r!/m!(r-m)! = r!/1!(r-1)!+r!/2!(r-2)!+….+

where m is the number of stages entered to a nonlinear operation [5,6].

2-The product of two or more binary sequence from different fields each sequence generated by LFSR

with irreducible polynomail.In the following section we introduce a mathematical analysis of complexity of such sequences.

3-Geffe's generator:

a- Generator description:

Geffe's generator consists of three LFSR's connected as shown in figure-2.The concept is to use LFSR#2 as a control generator to connect either LFSR#1 or LFSR#3 , but not both to the output.If the control generator produces a 1, then LFSR#1 is connected ,if it produces a 0, then LFSR#2 is connected.

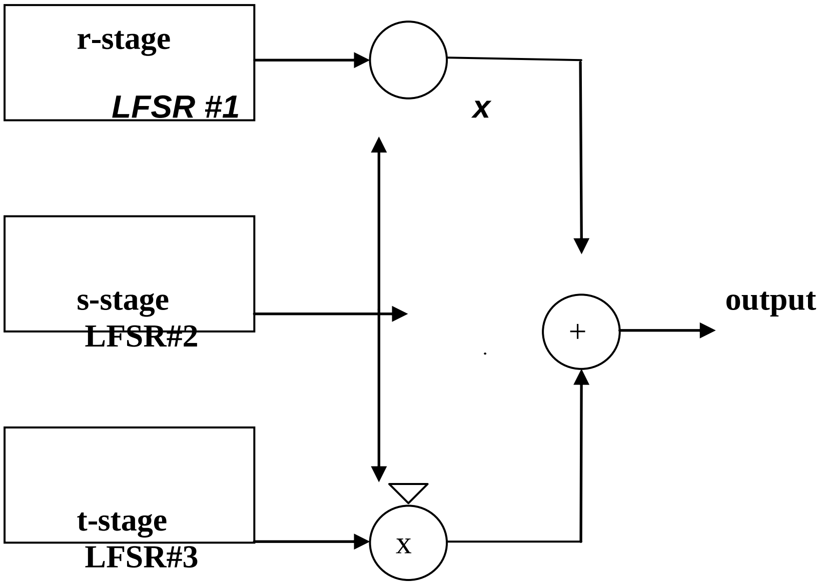

Figure-2 Geffe's generator

In a sense there are really four LFSR's being employed.The operation of complementing the output of the control generator in its relationship to LFSR#3 is equivalent to modulo 2 addition of a single-stage LFSR.This device has the characteristic equation x+1=0 , which has the single root 1.

b- complexity analysis:

Suppose that the three LFSR's have distinct primitive characteristic polynomials of degree r,s , and t respectively.Let r,s and t be relatively prime in pairwise.The roots of the characteristic polynomials are in GF(2^r),GF(2^s) and GF(2^t)respectively.Consider the first two registers , since r and s are relatively prime , the intersection of GF(2^r)and GF(2^s) contains only GF(2).This follows from the fact that every subfield of GF(2^n) is a field GF(2^m) where m is a divisor of

n.Suppose that α and β are elements of GF(2^r) and GF(2^s) respectively, and that neither is in GF(2)Then their product α β is in neither GF(2^r) nor GF(2^s) as we can easily demonstrate.Since GF(2^r) contains α , it also contains $α^{-1}$,and if it contains α β ,it also contains $α^{-1}$ α β= β however, since β is not in GF(2^r),neither is α β .Likewise α is not in GF(2^s).The product α β is contained in the superfield GF(2^{rs}).The situation is illustrated in figure -3.The first register has r conjugate roots in GF(2^r), and the other has s conjugate roots in GF(2^s).If their outputs are muliplied, the product sequence from the above arguments has rs distinict roots in GF(2^{rs}).It can be shown that these roots are the conjugate roots of an irreducible polynomial of degree rs . It can also shown that the product of two elements β€ GF(2^s) and σ € GF(2^t) contained in the superfield GF(2^{st}),finally the linear equivalent (complexity) of Geffe's generator is rs+(s+1)t.

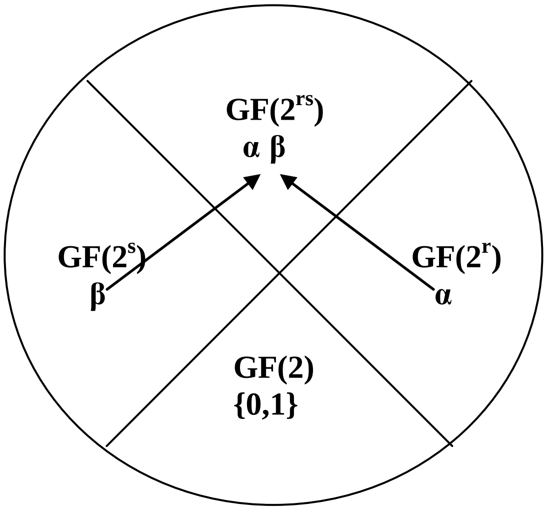

figure-3 product of elements of different fields

4-conclusions:

a- The complexity of Geffe's generator could be greater in a different configuration of the stages,i.e multiplication different phases from the same shift register before multiply the outputs of registers this operation produce what is called nonlinear feedforward sequences with high complexity.

b- The output sequence have some desirable properties such as a balanced distribution of zeros and ones

c- Geffe generator offers the advantage of being useful as a module of a superstructure of similer arrangements, i.e. , the entire generator of figure-2 could play the role of LFSR#2 in the same arrangement with like generator.

d- The output sequence has no immunity to autocorrelation attack.

5- references:

1- S.W.Golomb, shift register sequences.San Francisco:Holden Day, 1967.
2- J.L.Massey,"shift-register synthesis and BCH decoding," IEEE,Trans, information

theory vol. IT-15,pp.122-127, Jan 1969.

3-Meena Kumari,"complexity of binary nonlinear feedforward sequences through minimum polynomials of compound matrices",in discrete Mathematics 1985,North Holland.

4- Kadhim Hasen "determining the linear equivalent of NLFFS by using cyclotomic cosets",accepted in the journal of Basrah researches,University of Bsarah 1998

5- Edwin Key,"An analysis of the structure and complexity of nonlinear binary sequence generators",Transaction on information theory ,Vol. IT-22 No.6 November 1976.

6-.J.Groth,"Generation of binary sequences with contollable complexity",IEEE Trans ,Information theory, vol It-17,May 1971