An improved (n,k)-NLFSR generating any a given binary sequence

Jizhi Wang[1] Xueli Wu[2] Guang Yang[1]

[1]Shandong Provincial Key Laboratory of Computer Networks, Shandong Computer Science Center, Jinan, China, 250014
[2]Information Support Center, Jinan Branch of China United Network Communications Group Co., Ltd, Jinan, China, 25002

Abstract - Recently, a novel (n,k)-NLFSR was proposed by E. Dubrova etc.. In this paper, we develop a novel type of (n,k)-NLFSR, called D-FSR, which can generate all the binary sequences with period p ($2^{n-1}<p\leq 2^n$). We derive several properties of D-FSR. First, we demonstrate that they are capable of generating output sequences which can not be generated by (n,k)-NLFSR or Fibonacci type of NLFRs. Second, an algorithm is presented for constructing sequences with period p based on any a known (n,k)-NLFSR with period p. Third, we prove that D-FSR can generate all the binary sequence with period p.

Index Terms - Feedback Shift Register, Binary Sequence, Period

1. Introduction

Feedback shift registers (FSR) are used to generate many kinds of binary sequences that are applied widely on cryptographic systems, communication systems, computer systems, control systems and so on. However, construction of large FSRs with guaranteed long periods remains an open problem.

Recently, an novel type of NLFSRs called (n,k)-NLFSRs[1] is presented. Each bit *i* in an (n,k)-NLFSR is updated according to its next-state function, which is a non-linear function of the bit i+1 and up to k other bits. In contrast to the Fibonacci NLFSR in which feedback is applied to the n-1 th bit only, in (n,k)-NLFSRs feedback is potentially applied to every bit.

Although (n,k)-NLFSRs can generate some binary sequences which Fibonacci NLFSRs can not generate, we find that there are some sequences that (n,k)-NLFSRs can not generate. So we develop a novel type of (n,k)-NLFSRs, called D-FSR, that can generate all the binary sequence with period p.

The paper is organized as follows. Section 2 point out the drawback of (n,k)-NLFSRs. Section 3 introduces the definition of D-FSRs. Section 4 describes the constructing algorithm. Section 5 concludes the paper.

2. Related work

In [2], a algorithm for a random generation of feedback functions for Boolean full-length shift register sequence was presented. Seven properties of full-length shift register sequence was stated using the exhaustive search in the set of all n-bit (for n=3,4 and 5) Boolean functions. The paper assumed that these properties was true for n-bit (n>=6) functions. Then a algorithm was given to search functions satisfying these properties. There is no counter-example in their computational experiments for n from 6 to 20. However, they can not prove the assumption.

In [3], nonlinear feedback shift registers were studied from the view of autoregressive models. For a given sequence, an algorithm was proposed to determine the minimal nonlinear feedback shift register.

In [4], two algorithms were proposed for the generation of full-length shift register. The two algorithms also generate some full cycles of length 2^n using p-bits (p>n) registers.

In [5], many algorithms proposed for the generation of full length shift register before 1980 were surveyed.

In [6], a approach was given to construct shift register sequences of length l=2^m-4.

In [7], a Galois architecture FCSR (feedback with carry shift register) is introduced. The feedback computations of this kind of FCSR can be performed in parallel.

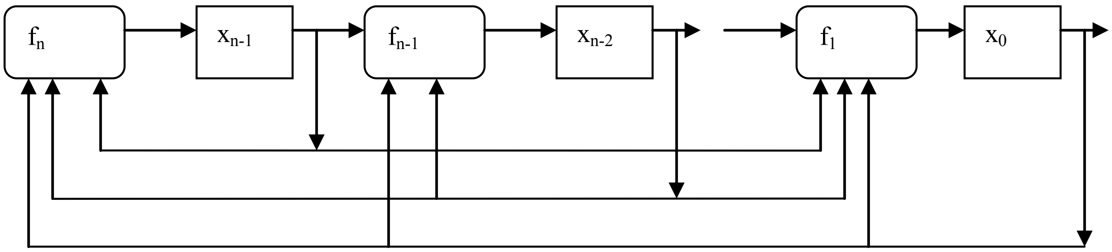

Fig.1 a n-bit (n,k)-NLFSR

© 2013. The authors - Published by Atlantis Press

3. The drawback of (n,k)-NLFSR

Although some sequences were listed in [1] that can be generated by (n,k)-NLFSRs instead of Fibonacci type of NLFSRs, there are many sequences that (n,k)-NLFSRs can not generate. So we have the Theorem 1 following:

Theorem 1: Suppose $s=a_1a_2\ldots a_p$ is a sequence with period p, where $2^{n-1}<p\leq 2^n$. If the number of 0 or 1 is more than 2^{n-1} in s, the sequence s can not be generated by (n,k)-NLFSRs with n registers.

Proof. Reduction to Absurdity.

Suppose the sequence s can be generated by (n,k)-NLFSRs with n registers. Because the output of (n,k)-NLFSRs is x_0, shown in Fig.1, then

$$x_0^i=a_i \qquad i=1,2,\ldots p$$

where x_0^i denotes the value of x_0 in *i* th clocking instance. Because the period of the sequence s is p, then the each states of (n,k)-NLFSRs are not equal each other, i.e.

$(x_0\, x_1 \ldots x_{n-1})_i \neq (x_0\, x_1 \ldots x_{n-1})_j$ $i\neq j$ $i,j=1,2,..p$

where $(x_0\, x_1 \ldots x_{n-1})_j$ denotes the state of (n,k)-NLFSR in *j* th clocking instance. Because the number of 0 or 1 is more than 2^{n-1} in s, then the number of state $(0, x_1 \ldots x_{n-1})$ or $(1, x_1 \ldots x_{n-1})$ is more than 2^{n-1}. But the maximum number of state $(0, x_1 \ldots x_{n-1})$ or $(1, x_1 \ldots x_{n-1})$ is 2^{n-1}. Thus, reduce to absurdity.

Hence, the sequence s can not be generated by (n,k)-NLFSRs with n registers. □

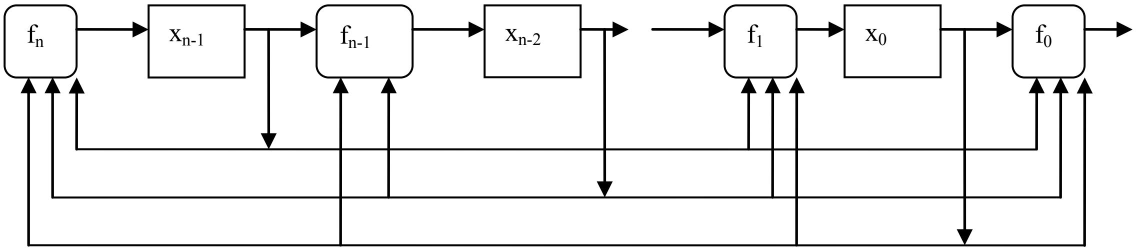

Fig.2 a n-bit D-FSR

4. The definition of D-FSR

Considered the drawback of (n,k)-NLFSRs, a novel FSR called D-FSR is shown in Fig. 2. Compared with n-bit (n,k)-NLFSRs, n-bit D-FSRs add a feedback function f_0 whose value is the output of D-FSR.

In fact, D-FSR is a special degradation form of (n+1,k)-NLFSRs, shown in Fig.3, because the value of register x does not influence feedback functions. Thus it still can be considered as a n-bit FSR, so we do not draw register x in Fig.2 in order to avoid misunderstanding.

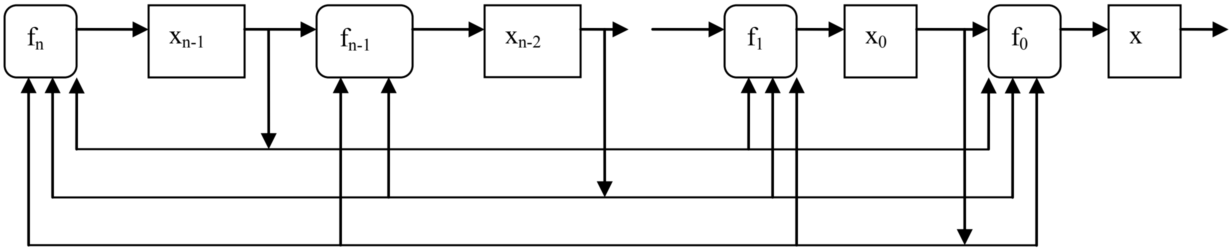

Fig.3 a special degradation form of (n+1,k)-NLFSR

In Table 1, two sequences with period 4 are listed that can not be generated by 2-bit (n,k)-NLFSRs

Table 1 2-bit D-FSR

f_2	f_1	f_0	Output Sequence
x_2+1	x_1+x_2	x_1x_2	0001
x_2+1	x_1+x_2	x_1x_2+1	1110

5. The constructing algorithm

If a n-bit (n,k)-NLFSR with period p is known, we can construct any a sequence with period p using D-FSR. The constructing algorithm is as follows:

Problem: Supposed a (n,k)-NLFSR with period p ($2^{n-1}<p\leq 2^n$) is known, solve a D-FSR that can generate the sequence $s=(a_0, a_1, \ldots, a_{p-1})$ with period p.

Constructing Algorithm: Because a (n,k)-NLFSR with period p is known, i.e. its feedback functions f_1, f_2, …, f_n are known, then the states transformation of the FSR is known that can be denoted as follows:

1st clocking instance: $(x_0^1, x_1^1, …, x_{n-1}^1)$

2nd clocking instance: $(x_0^2, x_1^2, …, x_{n-1}^2)$

…

p th clocking instance: $(x_0^p, x_1^p, …, x_{n-1}^p)$

where, x_i^j denotes the value of x_i in *j* th clocking instance, i=0,1,…,n-1 j=1,2,..p.

Define:

$f(x_0^1, x_1^1, …, x_{n-1}^1) = a_0$

$f(x_0^2, x_1^2, …, x_{n-1}^2) = a_1$

…

$f(x_0^p, x_1^p, …, x_{n-1}^p) = a_{p-1}$

Thus

$$f(x_0,x_1,...,x_{n-1}) = \sum_{(c_0,c_1,...,c_{n-1})=(x_0^1,x_1^1,...,x_{n-1}^1)}^{(x_0^p,x_1^p,...,x_{n-1}^p)} f(c_0,c_1,...c_{n-1})x_0^{c_0}x_1^{c_1}...x_{n-1}^{c_{n-1}}$$

where,

$$x_0^{c_0}x_1^{c_1}...x_{n-1}^{c_{n-1}} = \begin{cases} 0 & (x_0,x_1,...,x_{n-1}) \neq (c_0,c_1,...,c_{n-1}) \\ 1 & (x_0,x_1,...,x_{n-1}) = (c_0,c_1,...,c_{n-1}) \end{cases}$$

Then, f is the feedback function f_0 of D-FSR that we try to find. Hence, because all the feedback functions f_0, f_1, …, f_n are all known, we can get the D-FSR. □

Theorem 2: The D-FSR constructed by Constructing Algorithm can generate the sequence s=(a_0, a_1, …, a_{p-1}) with period p.

Proof.(Sketch) The output of D-FSR is the value of feedback function f_0. Then, according to the Constructing Algorithm, the output of f_0 is the sequence a_0, a_1, …, a_{p-1}. In addition, the state of D-FSR has period p according to the Constructing Algorithm. So the sequence a_0, a_1, …, a_{p-1} has period p. Hence, the Constructing Algorithm is soundness.

Theorem 3: Supposed any a (n,k)-NLFSR with period p ($2^{n-1}<p\leq 2^n$) is known, all the sequences with period p can be generated by our FSR with n registers.

Proof.(Sketch) Reduction to Absurdity.

Suppose there is a sequence s=(a_0, a_1, …, a_{p-1}) with period p that can not be generated by D-FSR with n registers.

According to the Constructing Algorithm, the feedback function f_0 can be constructed. Thus, all the feedback functions f_0, f_1, …, f_n are all known, so the sequence s can be generated by D-FSR with n registers. Thus, reduce to absurdity.

Hence, all the sequences with period p can be generated by D-FSR with n registers.

6. Conclusion

In this paper, we introduce a novel FSRs called D-FSR and derive some of their properties. The n-bit D-FSRs can generate all the sequences with period p ($2^{n-1}<p\leq 2^n$).

Acknowledge

This work was supported by the Natural Science Foundation of Shandong Province, China (No.ZR2011FM023).

Reference

[1] Elena Dubrova, Maxim Teslenko, Hannu Tenhunen. On analysis and synthesis of (n,k)-non-linear feedback shift registers. In Proceedings of the Conference on Design, Automation and Test in Europe, 2008, 1286-1291

[2] Izabela Janicka-Lipska, Janusz Stoklosa. Boolean feedback functions for full-length nonlinear shift registers. Telecommunications and Information Technology, 2004, Vol.5 28-29

[3] D.Linardatos, N.Kalouptsidis. Synthesis of minimal cost nonlinear feedback shift registers. Signal Process., 2002, Vol.82 No.2, 157-176

[4] Tuvi Etzion, Abraham Lempel. Algorithms for the generation of full-length shift-register sequences. IEEE Trans. Inform. Theory, 1984, Vol.IT-30 No.3 480-484

[5] Harold Fredricksen. A survey of full length nonlinear shift register cycle algorithms. Siam Review, 1982, Vol.24 No.2 195-221

[6] Farhad Hemmati. A large class of nonlinear shift register sequences. IEEE Trans. Inform. Theory, 1982, Vol.IT-28, No.2 355-359

[7] Mark Goresky, Andrew M. Klapper. Fibonacci and galois representations of feedback-with-carry shift registers. IEEE Trans. Inform. Theory, 2002, Vol.48 No.11 2826-2836