Emirates Journal for Engineering Research

Volume 26 | Issue 3 Article 5

7-13-2021

Representation of Nonlinear Pseudo-Random Generators Using State-Space Equations

Raghad K. Salih
University of Technology, Iraq, Raghad.k.Salih@uotechnology.edu.iq

REPRESENTATION OF NONLINEAR PSEUDO-RANDOM GENERATORS USING STATE-SPACE EQUATIONS

Raghad K. Salih

University of Technology, Applied Science Department, Iraq.

Raghad.k.Salih@uotechnology.edu.iq

(Received April 6 and accepted July 13, 2021)

تمثيل المولدات الشبه-عشوائية اللاخطية باستخدام معادلات فضاء الحالة

ملخص

فكرة البحث تمثيل للمولدات الشبه عشوائية اللاخطية باستخدام معادلات فضاء الحالة . يعتمد هذا التمثيل على المصفوفات حيث يتم توليد المتتابعة باستخدام المصفوفات و ليس كما هو متعارف عليه عند توليد متتابعات المولدات باستخدام مسجلات الإزاحة. كما تم تقديم خوارزميات لانواع مختلفة من المولدات الشبه عشوائية اللاخطية و استخراج متتابعاتها. علاوة على ذلك تم اعطاء مثالين لتوضيح هذا التمثيل.

Abstract

The idea of research is a representation of the nonlinear pseudo-random generators using state-space equations that is not based on the usual description as shift register synthesis but in terms of matrices. Different types of nonlinear pseudo-random generators with their algorithms have been applied in order to investigate the output pseudo-random sequences. Moreover, two examples are given for conciliated the results of this representation.

1. INTRODUCTION

Pseudo-random generators (PRG) are used as spectrum modulations for direct sequence spread spectrum design for digital communication system, in wireless technique and as a key in encryption to produce the ciphertext in cipher systems. The sequence appears random in nature but in reality, it is deterministic and available to the privileged users [1].

The state space equations SSE has emerged in the last fifty years in the field of control theory. This method uses vector and matrices for system representation, so it permits a simple notation that is easily accepted and processed by digital computer [2]. In this work the nonlinear PRGs were viewed using SSEs.

2. Pseudo-Random Generators PRG

2.1 Nonlinear Feedback Shift Register (NLFSR) Generators [3,4]

A NLFSR of length n is commonly used for producing PR-sequence. It is made up of two parts: shift registers (SR) and a feedback function. The SR is a storage element of a sequence of (n) bits. These (n) binary storage are called the stages of the SR. The algorithm is shown below.

NLFSR Algorithm

Step 1

Input :-

(1) The length (n) of the NLFSR.

(2) The initial state of the NLFSR as $[s_0\ s_1\ .\ .\ .\ s_{n-1}]$.

(3) The nonlinear feedback function $f\ (s_k, s_{k+1},\dots,s_{k+n-1})$.

Step 2

Set $k = 0$

Step 3

Shift the bits in the register by one position to the left and calculate the feedback bit s_{k+n} from the nonlinear function $f\ (s_k, s_{k+1},\dots,s_{k+n-1})$.

Step 4

Set a new state $[s_{k+1}\ s_{k+2}\ .\ .\ .\ s_{k+n}]$ of NLFSR.

Step 5

If the new state is equal to the initial state then :

a) Stop

b) Print the output s_k , $k = 0,1,2,\dots$ of NLFSR.

c) Print the period (k+1) of the sequence of NLFSR.

else

a) k = k+1

b) go to (step 3).

Example

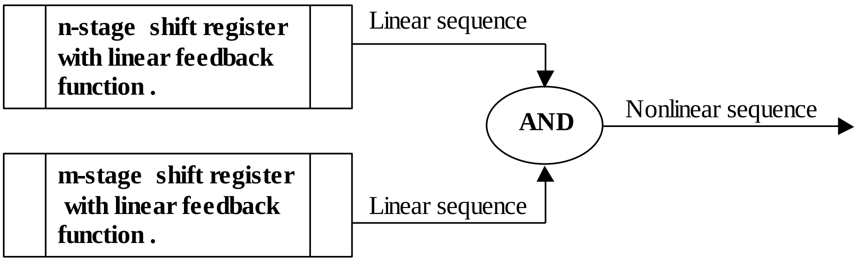
Consider the following NLF function (3-stage):

$f(s_k, s_{k+1}, s_{k+2}) = s_k + s_{k+1} + s_{k+1}.s_{k+2} + 1$

with initial state 101. The output sequence can be generated by applying NLFSR algorithm the produced sequence is : 10100011 .

2.2 Hadmard Generator HG [5,6]

A nonlinear generator consists of two LFSRs, one with (n-stage) and the other with (m-stage) where the gcd (m,n) =1 and each of which produces a sequence with maximal period. The two LFSR's are combined with nonlinear function "AND" to produce a nonlinear sequence with period $((2^n-1)\times(2^m-1))$ as illustrated in figure (1).



Figure(1) Hadmard generator.

Hadmard Algorithm

Step 1:

Input:

(1) The (n,m) stages of two LFSR's.

(2) The initial states of them .

(3) The coefficients of the linear feedback functions of them .

Step 2:

Use (step 1) and call LFSR algorithm to find their sequences.

Step 3:

Combine the two linear sequences in (step 2) with "AND" function to produce the Hadmard sequence .

3. State - Space Equations SSE [7,8,9,10]

The SSE of the linear system is:

$$\left.\begin{aligned} x(k+1) &= Ax(k) + Bu(k) \\ y(k) &= Cx(k) + Du(k) \end{aligned}\right\} \qquad \ldots(1)$$

Where A is ($n\times n$) matrix, B is the ($n\times m$) input matrix, C is the $p\times n$ output matrix and D is the $p\times m$ transmission matrix.

A mathematical model of a nonlinear system was described using SSE as follows:

$$\left.\begin{aligned} x_{k+1} &= f(x_k, u_k) \\ y_k &= h(x_k, u_k) \end{aligned}\right\} \quad , \quad k = 0,1,2,\ldots \qquad \ldots(2)$$

where x_k is the state of the system, u_k is the input of the system and y_k is the output of the system.

4. SSE of Non-Linear PRG:

If we have NLFSR n-stage with nonlinear feedback function $f(s_k, s_{k+1}, \ldots, s_{k+n-1})$, where $s_{k+n} = f(s_k, s_{k+1}, \ldots, s_{k+n-1})$, k = 0,1,2,... ; then the nonlinear SSE can be derived using Eq.(2) as:

$$x(k+1) = f(x(k)) \qquad \ldots(3)$$

$$y(k) = h(x(k)) \quad , \quad k = 0,1,2,\ldots \qquad \ldots(4)$$

where ,

$$x(k) = \begin{bmatrix} x_1(k) \\ x_2(k) \\ \vdots \\ x_n(k) \end{bmatrix} = \begin{bmatrix} s_k \\ s_{k+1} \\ \vdots \\ s_{k+n-1} \end{bmatrix}$$

therefore,

$$x(k+1) = \begin{bmatrix} x_1(k+1) \\ x_2(k+1) \\ \vdots \\ x_n(k+1) \end{bmatrix} = \begin{bmatrix} x_2(k) \\ x_3(k) \\ \vdots \\ s_{k+n} = f(s_k, s_{k+1}, \ldots, s_{k+n-1}) = f(x_1(k), x_2(k), \ldots, x_n(k)) \end{bmatrix}$$

$$= f(x(k)) \qquad \ldots(5)$$

while the output equation of the nonlinear state space model is

$$y(k) = s_k = x_1(k) = h(x(k)) \quad , \quad k = 0,1,2,\ldots. \qquad \ldots(6)$$

When the nonlinear PRG is constructed from a nonlinear combination of two or more LFSR's, the state space model can be derived as follows

Let $x_1, x_2, \ldots, x_j$ be j LFSR's , j >1 with $n_1, n_2, \ldots, n_j$ stages and $f_1(x), f_2(x), \ldots, f_j(x)$ characteristic polynomials respectively , where :

$$\left.\begin{array}{l} f_1(x)=c_0+c_1x+c_2x^2+\cdots+c_{n_1-1}x^{n_1-1}+x^{n_1} \\ f_2(x)=c_0+c_1x+c_2x^2+\cdots+c_{n_2-1}x^{n_2-1}+x^{n_2} \\ \vdots \\ f_j(x)=c_0+c_1x+c_2x^2+\cdots+c_{n_j-1}x^{n_j-1}+x^{n_j} \end{array}\right\} \quad \ldots(7)$$

The linear recursion relations of the above LFSR's are :

$$\left.\begin{array}{l} s_1(k+n_1)=\sum_{i=0}^{n_1-1}c_i s_1(k+i) \\ s_2(k+n_2)=\sum_{i=0}^{n_2-1}c_i s_2(k+i) \\ \vdots \\ s_j(k+n_j)=\sum_{i=0}^{n_j-1}c_i s_j(k+i) \end{array}\right\} \quad \ldots(8)$$

where $k=0,1,2,\ldots$.

The state variables are:

$$\left.\begin{array}{l} x_1(k)=s_1(k) \\ x_2(k)=s_1(k+1) \\ \vdots \\ x_{n_1}(k)=s_1(k+n_1-1) \\ x_{n_1+1}(k)=s_2(k) \\ x_{n_1+2}(k)=s_2(k+1) \\ \vdots \\ x_{n_1+n_2}(k)=s_2(k+n_2-1) \\ \vdots \\ x_{n_1+n_2+\cdots+n_{j-1}+1}(k)=s_j(k) \\ \vdots \\ x_{n_1+n_2+\cdots+n_j-1}(k)=s_j(k+n_j-2) \\ x_{n_1+n_2+\cdots+n_j}(k)=s_j(k+n_j-1) \end{array}\right\} \quad \ldots(9)$$

From Eq.(8) and Eq.(9) the SSE is

$$x(k+1)=A\,x(k) \quad \ldots(10)$$

where x (k) , $k\geq 0$ is the state vector :

$$x(k)=\begin{bmatrix} x_1(k) \\ x_2(k) \\ \vdots \\ x_{n_1}(k) \\ x_{n_1+1}(k) \\ \vdots \\ x_{n_1+n_2}(k) \\ \vdots \\ x_{n_1+n_2+\cdots+n_j-1}(k) \\ x_{n_1+n_2+\cdots+n_j}(k) \end{bmatrix}_{(n_1+n_2+\cdots+n_j)\times 1}$$

and A is $(n_1+n_2+\cdots+n_j)\times(n_1+n_2+\cdots+n_j))$ matrix

$$A=\begin{bmatrix} 0 & 1 & 0 & \ldots & 0 & & & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \ldots & 0 & & & 0 & 0 & & 0 \\ \vdots & & & & \vdots & & & \vdots & & \ddots & \vdots \\ c_0 & c_1 & c_2 & \ldots & c_{n_1-1} & & & 0 & 0 & \cdots & 0 \\ & & & & & \ddots & & & & & \\ & & & & & & \ddots & & & & \\ 0 & 0 & \cdots & 0 & & & & 0 & 1 & 0 \ldots & 0 \\ 0 & 0 & & 0 & & \cdots & & 0 & 0 & 1 \ldots & 0 \\ \vdots & & \ddots & \vdots & & & & \vdots & & & \vdots \\ 0 & 0 & \cdots & 0 & & & & c_0 & c_1 & c_2 \ldots & c_{n_j-1} \end{bmatrix}_{(n_1+n_2+\cdots+n_j)\times(n_1+n_2+\cdots+n_j)}$$

The nonlinear output equation of SSE can be obtained by using Eq.(2)

$$y(k)=h(x(k))=x_1(k)\,x_{n_1+1}(k)\,x_{n_1+n_2+1}(k)\ldots x_{n_1+n_2+\cdots+n_{j-1}+1}(k) \quad , \; k=0,1,2,\ldots \quad \ldots(11)$$

5. Test Examples

Example (1)

Retrieval the example in section (2.1). To represent the NLFSR by using SSE, use Eq.(5) and Eq.(6):

$$x(k+1)=\begin{bmatrix} x_1(k+1) \\ x_2(k+1) \\ x_3(k+1) \end{bmatrix}=\begin{bmatrix} x_2(k) \\ x_3(k) \\ x_1(k)+x_2(k)+x_2(k)x_3(k)+1 \end{bmatrix}=$$

f (x(k))

$$y(k)=x_1(k)=h(x(k)).$$

Example (2) :

Consider HG with two LFSRs

$f_1(x)=x^3+x+1$ with initial state 100 ,

and $f_2(x)=x^2+x+1$ with initial state 10 .

By applying Hadmard algorithm, the following nonlinear sequence with period $(2^3-1)\times(2^2-1)$ is obtained :

$Seq\,(Hadmard\,)=100101100000101001001$

Use Eq.(10) and Eq.(11) to represent HG by using SSE

$$x(k+1)=A\,x(k)$$

$$\begin{bmatrix} x_1(k+1) \\ x_2(k+1) \\ x_3(k+1) \\ x_4(k+1) \\ x_5(k+1) \end{bmatrix}=\begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}\begin{bmatrix} x_1(k) \\ x_2(k) \\ x_3(k) \\ x_4(k) \\ x_5(k) \end{bmatrix}$$

and the output is $y(k)=x_1(k)x_4(k)=h(x(k))$.

Conclusion

State space models have been derived to represent PRG's. From solving some test examples, the following points are included:

1- State space model represent nonlinear PRG's in a simplified mathematical way using matrices of first-order difference equations.

2- State space model of PRG gives rapid generation because its simple logic where it is computed easily in digital computer.

References

1. Masanao Aoki , State Space Modeling of Time Series, Printed in Germany, Springer-Verlag , 1987.
2. Kalmyk G. State-Space Models with Regime Switching, The MIT Press, 2017.
3. Hetzel, P. ,Time dissemination via the LF transmitter DCF77 using a pseudo-random phase-shift keying of the carrier, 2nd European Frequency and Time Forum. Neuchâtel. pp. 351–364. 2011.
4. Baker , H.J. and Piper, F.C., Cipher Systems: The Protection of Communications, Northwood Publications ,London ,1982.
5. Kadhim A.J., A Mathematical Development of Gordon, Mills and Welch Generator Using Galois Field and Trace Polynomials. Engi. & Techno. J. 2007;25(8):958-68.
6. Martínez LH, Khursheed S, Reddy SM. LFSR generation for high test coverage and low hardware overhead. IET Computers & Digital Techniques. 2019.
7. Vladimir Strejc , State Space Theory of Discrete Linear Control , Printed in Czechoslovak Academy of Sciences 2014.
8. Salih RK, Salih SH, Kadhim AJ. Block Method for Solving State-Space Equations of Linear Continuous-Time Control Systems. Baghdad Science Journal ;4(2), 2007.
9. Stock, J.H.; Watson, M.W., "Dynamic Factor Models, Factor-Augmented Vector Autoregressions, and Structural Vector Autoregressions in Macroeconomics", Handbook of Macroeconomics, Elsevier, 2, pp. 415–525, 2016.
10. Salih RK, Kadhim AJ., Hassan IH. Scraton Method for Solving nth Order State-Space Equations of Linear Continuous-Time Control Systems. journal of the college of basic education. 21(87), 2015.