Discrete models of the NLFSR generators

Janusz Walczak, Rafał Stępień
Silesian University of Technology
44-100 Gliwice, ul. Akademicka 10, e-mail: janusz.walczak@polsl.pl,
rafal.stepien @polsl.pl

In this article a class of pseudo random signal generators, build with static nonlinear feedback block, is described. The feedback block function is modeled as a linear combination of sums and products of the register's taps. A discrete model of the generator is proposed as a nonlinear discrete circuit. The simulation results from Matlab-Simulink and Multisim are shown. Also an experimental results of the example generator on FPGA implementation is shown.

1. Introduction

The pseudo random signal generators are widely used in technical applications, including key stream generators in cryptography [2], telecommunication [6], [7] and in many other applications [6]. The wide class of pseudorandom signal generators is based on linear shift registers that works with feedback loop. This class can be divided into four groups depending on the used feedback loop, Fig 1.

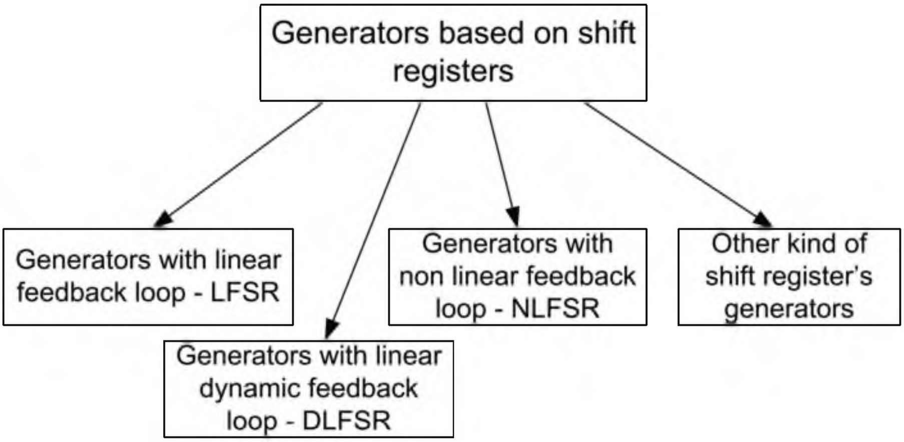
Generators based on shift registers
Generators with linear feedback loop - LFSR
Generators with non linear feedback loop - NLFSR
Other kind of shift register's generators
Generators with linear dynamic feedback loop - DLFSR

Fig. 1. The classification of the generators based on shift registers

The linear feedback generators with static or dynamic feedback loop were described in the following papers [1], [2], [5], [7] and the analysis of non linear feedback loop generators (NLFSR) can be found in [4], [10]. The following article is a continuation of [10] that was devoted to the NLFSR analysis.

2. The binary model of NLFSR generator

The considered circuit (Fig. 2) is constructed from a linear shift register (LSR) and a nonlinear feedback block, that can be made from the combinational logic.

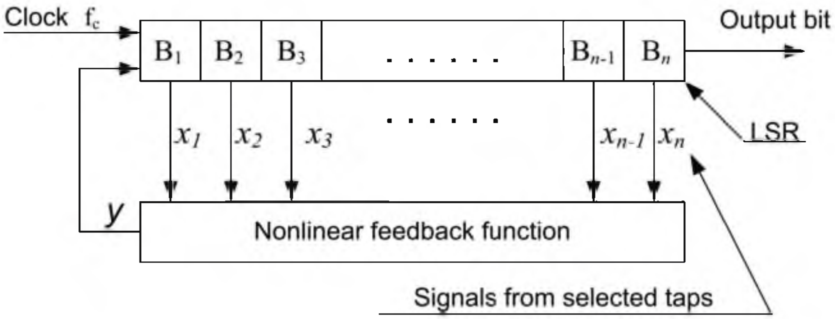

Fig. 2. The NLFSR generator

The formula (1) that is often used to describe non inertial circuits cannot be used to describe a nonlinear feedback loop of the NLFSR generator (fig 2.). The shift register, that is a part of NLFSR generator, works with binary signals. The feedback loop also works with binary values. Every cell of shift register contains only one of two values {0;1}. For variables $x_1 \ldots x_n$ that can only contain binary values and for any values of coefficients a_{ik}, the nonlinear function (1) becomes a linear function. This is caused by the exponent part of formula (1). For binary values the exponent value does not matters because the formula (1) will return as result also binary value.

$$y = \sum_{i=1}^{M} \sum_{k=1}^{N} a_{ik} (x_i)^k, a_{ik} \in R, x_i \in GF(2). \qquad (1)$$

In circuit shown on figure 2, the y value (output of the feedback loop) needs to have a value from *GF(2)* finite field. Coefficients values from formula (1) and the sum and product operators needs to belong to *GF(2)* finite field.

3. The time discrete model of the NLFSR

The proposed description of the non linear feedback loop (fig. 2) can be realized with the following formula:

$$y = \sum_{i=1}^{k} \sum_{j=1}^{n} m_{ij} x_j \; y \in GF(2), x_j (j = 1,2,\ldots,n) \in GF(2), \qquad (2)$$

where: y - binary signal from the feedback loop, x_j - binary signals from selected register's taps, m_{ij} -zero-one elements of the M matrix, n – number of register cells, k – number of sum components.

It follows that formula (2) has k ($k \leq n$) components. Every one corresponds to the product of j components ($j \leq n$). Some of these components can be equal to zero. That can be interpreted as a signal from register's tap was not connected to the feedback loop block. The M matrix defines which signals from linear shift register are connected to the feedback loop. The following example shows this idea.

Example 1

The NLFSR generator contains a shift register with n=4 cells. The M matrix is defined as follows:

$$M = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \tag{3}$$

Determined from (2) output signal y of the feedback loop block is described with following equation:

$$y = x_1 \otimes x_3 \otimes x_4 \oplus x_1 \otimes x_2 \oplus x_4, \tag{4}$$

where: $\oplus$ - the sum symbol in GF(2) finite field, $\otimes$ - the product symbol in GF(2) finite field.

The scheme of the considered generator is show on Fig 3.

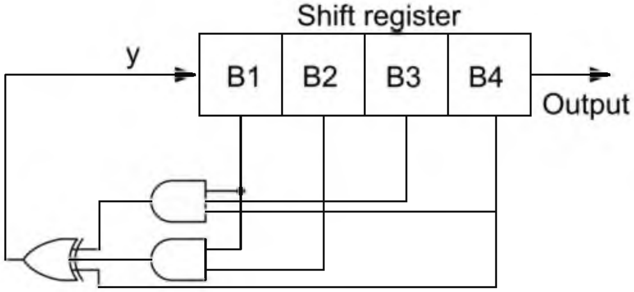

Fig. 3. Schematic of NLFSR generator described by matrix (3)

From the above considerations it follows that the feedback loop function (2) is a sum of products in *GF(2)* finite field. This function can be considered as a modulo 2 sum (XOR) of component products from formula (2). The modulo 2 sum can be written as a discrete form shown in the following formula:

$$A \oplus B = A + B - 2AB \tag{5}$$

where symbols of sum and product that appears on the right side of formula (5) needs to be considered as a classical operations in a set of real numbers. Formula (5) can be used to transform the formula (2) to discrete time circuits and systems relations that can describes the NLFSR generators. In order to perform that the formula (2) needs to be decompose into a form of sums and products and then all obtained components needs to be added as it is shown in formula (5). The example 2 shows the described idea.

Example 2

The M matrix that describes the feedback loop block is given as follows:

$$M = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}. \tag{6}$$

Based on the formula (2) (see also example 1) the feedback loop block model for signals from *GF(2)* finite field is described by the following formula:

$$y = x_1 \oplus x_2 \oplus (x_1 \otimes x_3) \tag{7}$$

The formula described with (7) is made from three components: x_1,x_2 and ($x_1 \otimes x_3$). Every component needs to be added to the result of previous sum. The algorithm of transformation is given as follows:

Step 1: sum of $x_1 \oplus x_2$:

$$x_1 \oplus x_2 \Rightarrow x[n-1] + x[n-2] - 2x[n-1]x[n-2] \tag{8}$$

Step 2: sum of $(x_1 \oplus x_2) \oplus (x_1 \otimes x_3)$:

$$\begin{aligned}(x_1 \oplus x_2) \oplus x_1 x_3 \Rightarrow x[n-1] + x[n-2] - 2x[n-1]x[n-2] + x[n-1]x[n-3] \\ - 2(x[n-1] + x[n-2] - 2x[n-1]x[n-2])x[n-1]x[n-3] = y[n]\end{aligned} \tag{9}$$

Figure 4 shows the structure of a discrete circuit that corresponds to the difference equation (9).

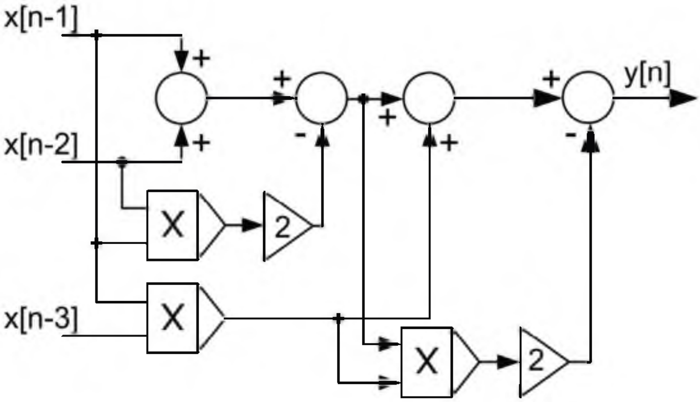

Fig. 4. The feedback function structure that is obtained from equation (9)

4. The simulations results

Simulations of the exemplary NLFSR generator where conducted in the Matlab Simulink environment and in the Multisim 9.0. The *M* matrix that describes the simulated NLFSR generator is given as follows (10):

$$M = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{10}$$

If matrix elements are substituted into formula (2) the feedback loop formula is describes as follows (11):

$$y = x_1 \otimes x_2 \otimes x_3 \oplus x_4 \tag{11}$$

The multiplication and sum operations in above formula should be interpreted as operations in *GF(2)* finite field. Transforming formula (11) similarly as it was shown in example 2 leads to the discrete form of (11). The discrete form of formula (11) is defined as follows (12):

$$y[n] = x[n-1]x[n-2]x[n-3] + x[n-4] - 2x[n-1]x[n-2]x[n-3]x[n-4] \tag{12}$$

The feedback loop block of the considered generator, made from discrete systems block, is shown on Fig 5.

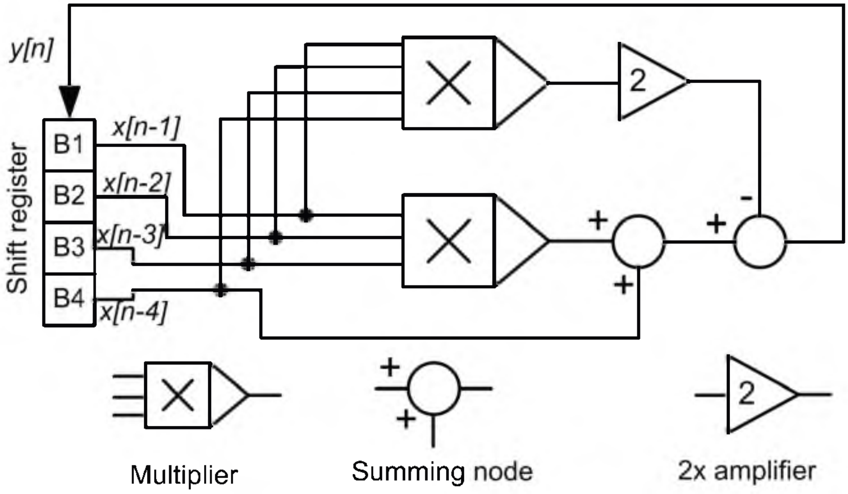

Fig. 5. The structure of the feedback loop

The output sequence *y[n]* from the generator is shown on Fig 7. Simulated in Matlab Simulink circuit is shown on Fig. 6.

The shift register is made from unit delay blocks z^{-1}. The default state of the shift register is set to $1111_{BIN.}$ The sampling rate was set to 0,1s. The output signal taken from the forth register's tap is shown on Fig. 7.

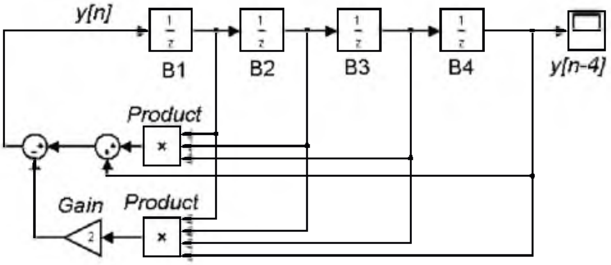

Fig. 6. The simulated NLFSR generator

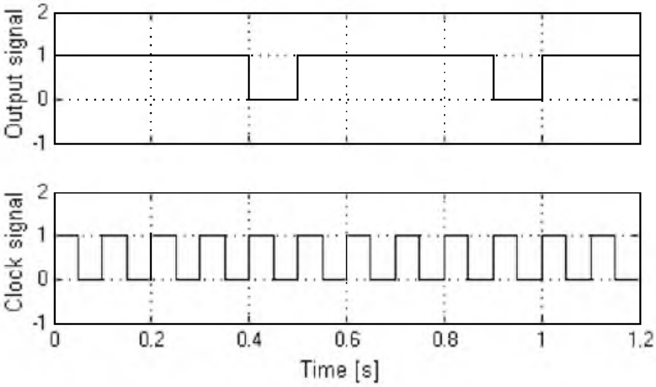

Fig. 7. The output signal of simulated NLFSR generator

Based on Fig. 7 and analytical calculations the obtained output sequence is as follows: 1111011110111... This sequence is periodic with period 5. The next simulation was conducted in the Multisim 9.0 environment. The simulated circuit is shown on Fig. 8.

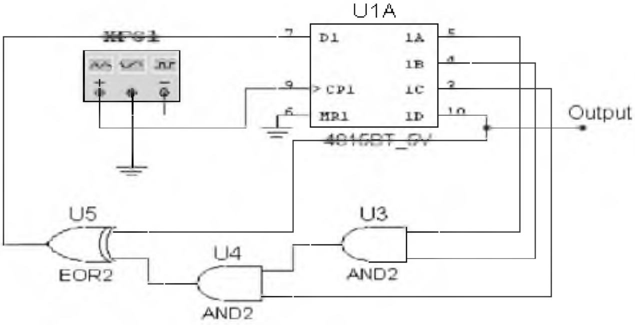

Fig. 8. Schematic of the simulated NLFSR generator

The simulated circuit is build from a shift register CD4015 supplied from 5V. Logic gates U3, U4, U5 are used as a feedback block. The signal generator XFG1 is used as a clock source. The output signal is taken from the last, forth tap of the shift register. The output signal and clocking signal are shown on figure 9. These signals are identical as obtained from previous circuit (Fig. 7). This proves that change from electronic circuit into discrete model is correct.

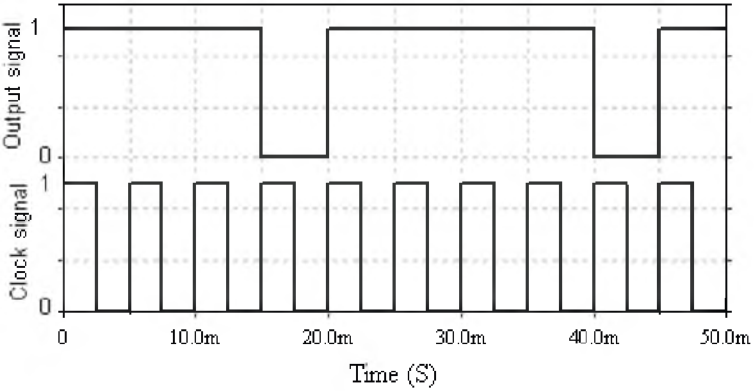

Fig. 9. The output signal of considered generator

5. The experimental results

The physical generator was constructed as a FPGA implementation. Used FPGA integrated circuit XC3S200 [12] is produced by Xilinx and belongs to the Spartan III family. This FPGA chip is mounted on a development board, ZL9PLD, that is produced by Kamami [13], [14]. JTAG is used as a programming interface and all schematics and codes are generated by the ISE WebPack environment.

The schematic of NLFSR generator is show on Fig. 10.

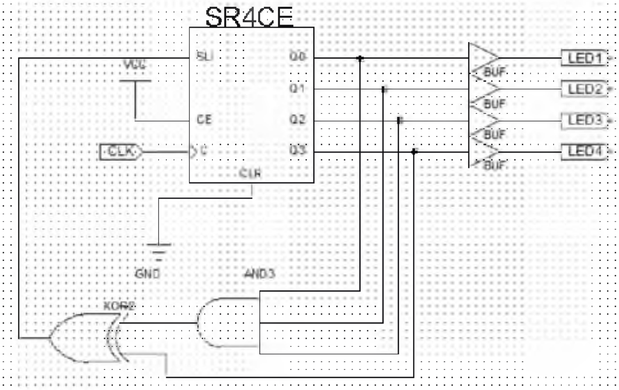

Fig. 10. The schematic of NLFSR generator implemented in FPGA

The initial state of the shift register is set exactly as it was set in simulation results. The output signal obtained as a signal from buffered line Q3 and the clocking signal are shown on Fig. 11.

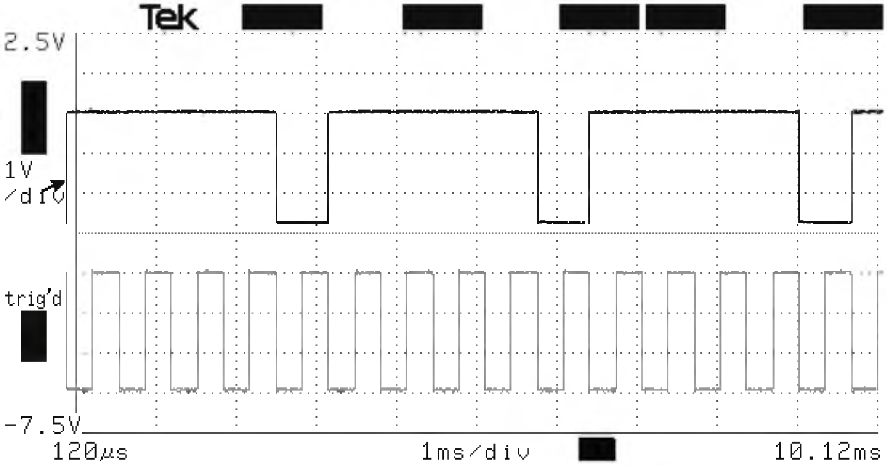

Fig. 11. The output signal of NLFSR generator

The obtained waveforms are exactly the same as in previous cases. This proves that carried out considerations and obtained formulas are correct. The output sequence 1111011110111... is periodic with period 5.

6. Summary

In this article a method of describing the non linear feedback loop block of the NLFSR generators is proposed. An effective method of transformation from the binary model of the feedback loop to the model of time-discrete systems is given. Obtained results are supported with examples. The simulation results of exemplary NLFSR generators in Matlab and Multisim are given. More over a physical model of the NLFSR was implemented on the Spartan III FPGA and some results of its implementation were shown. A full consent was obtained between theoretical and physical models. That proves that proposed method is correct.

REFERENCES

[1] Chen L., Gong G.: Communication Systems Security, Appendix A, Draft, 2008.

[2] Golomb S. W.: Shift Register Sequences. Laguna Hills, C A Aegean. Park Press, 1982.

[3] Schneier B.: Kryptografia dla praktyków, Vol. 2, WNT, Warszawa 2002.

[4] Dubrova E.: How to Speed-Up Your NLFSR-Based Stream Cipher, Royal Institute of Technology (KTH), Stockholm, Sweden, 2009.

[5] Walczak J., Stępień R.: Modeling of the pseudo random signal generators using digital filters. Proceedings of XXXIII Conference IC-SPETO May, 2010,pp. 85-86.

[6] Kotulski Z.: Generatory liczb losowych: algorytmy, testowanie, zastosowania, Matematyka Stosowana 2,2001, pp.1-6.

[7] Mutagi R.N.: Pseudo noise sequences for engineers, Electronics & Communication Engineering Journal,Vol.8 Issue 2, April 1996, pp.79-87.

[8] J. Massey, "Shift-register synthesis and bch decoding," IEEE Transactions on Information Theory, vol. 15, pp. 122–127, 1969.

[9] Walczak J., Stępień R.: Discrete Model of the NLFSR Generators, Proceedings of XVI Conference ZKwE April, 2011,pp. 35-36.

[10] Walczak J., Stępień R.: Shift Registers with Dynamic Feedback Loop, Proceedings of XXXIV Conference IC-SPETO May, 2011,pp. 125-126.

[11] Alfke P.: Efficient Shift Registers, LFSR Counters, and Long Pseudo-Random Sequence Generators, Xilinx application note, July 7,1996, Vol 1.1.

[12] Xilinx corporation.: Spartan III family data scheet, http://www.xilinx.com/support/documentation/data_sheets/ds099.pdf

[13] Kamami development tools, dipPLD module, www.kamami.pl/dl/zl10pld.pdf

[14] Kamami development tools, mother board for dipPLD modules, www.kamami.com/dl/zl9pld_en.pdf