THE METHOD OF IMPROVING PSEUDO RANDOM SIGNAL GENERATING RATE OF THE LFSR GENERATORS

Janusz Walczak, Rafał Stępień
Faculty of Electrical Engineering
Silesian University of Technology
Gliwice, Poland
janusz.walczak@polsl.pl, rafal.stepien@polsl.pl

***Abstract*— The following paper describes a method to increase the rate of the generating pseudo random numbers. The proposed solution, that works according to described method, consists of shift register generator and additional data output blocks. Through adding these functional blocks, connected with a classical LFSR generator, increase of the pseudo random number generating rate was obtained. A number of these additional blocks were discussed in the following paper. Operation of these additional blocks was shown on a example.**

Keywords—pseudo random signal; LFSR; shift register generator; pseudo random sequence rate

I. Introduction

The pseudo random generators are widely used in modern science and technology [1], [2], [3], [4]. One of the pseudo random signal generators class is a linear feedback shift register generators – LFSR [5], [6]. The LFSR generators are easy in hardware and software implementation, and they generate one pseudo random bit on each clock cycle [6]. In many applications the pseudo random signal rate, generated by the shift register generator, is too low [9]. In case when the statistical test results [10] are not a primary requirement, but the pseudo random signal rate is essential, the proposed additional output blocks might be used with the LFSR generator.

II. Pseudo Random Signal Generating Methods

Basic pseudo random generator types include the congruential generators [1], its modifications and the generators that uses shift registers [3], [5]. The LFSR generators and majority of the complex pseudo random signal generators build on a shift registers [7], [8], generate only one bit of the pseudo random sequence for each clock cycle [5].

III. Proposal of the Pseudo Random Sequence Rate Increase

For the applications requiring significant generation rate of pseudo random numbers [2], in which statistical properties of the sequence are of non-priority, structure as shown in figure 1 may be used.

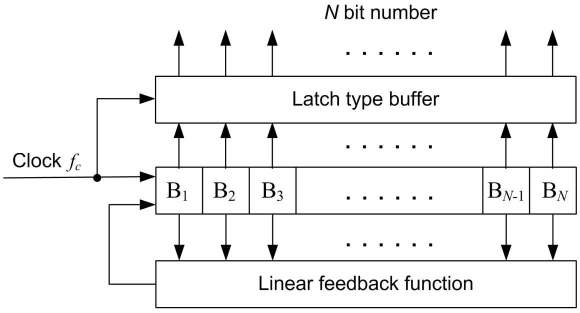

Fig. 1. The LFSR generator with *N* bit parallel output

The structure shown in figure 1 generates the binary pseudo random sequence with the rate larger than the typical LFSR structure. The clock signal f_c controls the LFSR generator and the output buffer. The output buffer task is to transfer the LFSR register bit content to the *N* bit buffered output. Every single clock period generates *N* bits (as an *N* bit number) sequence on the buffer output. Pseudo random *N* bit number sequence rate is given by the formula (1).

$$R_B = f_c \quad numbers/s \tag{1}$$

Generalized proposed scheme of the modified pseudo random signal generator, that uses the LFSR generator, is shown in figure 2.

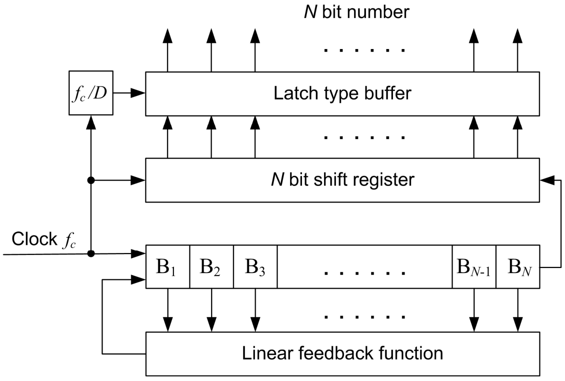

Fig. 2. One of the proposed modifications with LFSR generator

In a circuit shown in figure 2, the generating rate of the *D* bit pseudo random numbers, equals the buffer clock frequency divided by the division ratio set by *D*, according to the formula (3). The binary pseudo random sequence rate, made from the generated *D* bit numbers, is *N* times longer and is defined by formula (4). The additional shift register, that co-operates with the LFSR generator, is shifted and filled by the LFSR output bits, synchronously with the clock signal.

$$R_N = \frac{f_c}{D} \quad numbers/s \tag{3}$$

$$R_B = f_c \frac{N}{D} \quad bits/s \tag{4}$$

The division ratio *D* determines the statistical properties of the pseudo random numbers generated by the proposed structures. If division ratio is high (very close to *N*), the statistical properties are very approximate the statistical properties of the typical LFSR generator. The pseudo random sequence rate in this case is the lowest and very approximate the rate of the LFSR generator. The high rate of the pseudo random sequence can be obtained when division ratio *D* is approximate 1. In this case the pseudo random rate is the highest, but the statistical properties of the sequence are the worst.

Example:

The 5 bits (*N*=5) LFSR generator works with a shift register and output latch buffer. The division ratio of output buffer clock frequency equals *D*=4. The LFSR feedback polynomial is given by the formula (5) and the initial state of the LFSR generator equals 11111_{BIN}. The scheme of this circuit is shown in figure 3. Beginning of the generator output sequence shall be determined.

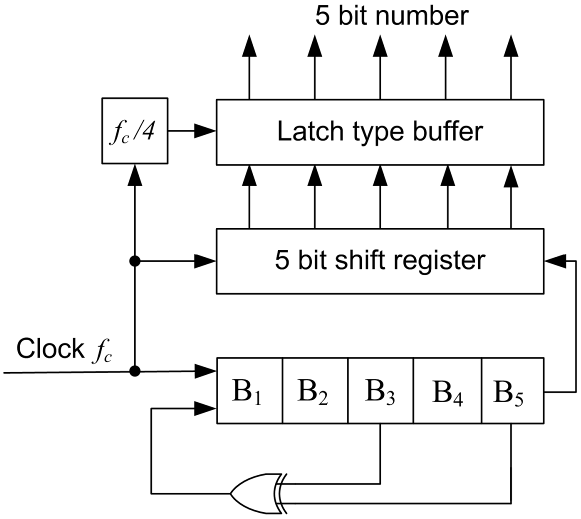

Fig. 3. An exemplary modification of the 5 bit LFSR generator

$$L(x) = \mathrm{x}^5 + \mathrm{x}^3 + 1 \tag{5}$$

The 5 bit pseudo random number appears on the output buffer every 4 f_c clock cycles. The binary pseudo random sequence from the LFSR output and the binary sequence made from the 5 bit number are given as follows:

1. LFSR output: 11111000110111010100
2. Buffet output: 0001110110101110010101000

During 20 clock cycles, the circuit shown in figure 3, generated 25 bits of the pseudo random sequence. According to the formula (4) the bit rate equals 1,25f_c.

IV. Summary

The following article discusses methods of increasing the rate of pseudo random numbers generation. In order to do the above, LFSR generator was expanded to include additional functional blocks. A number of possible modifications to LFSR generator structure was discussed and presented in this article. On the example presented in the paper, the principle of operation was described. Results of pseudo random signal statistical tests, depend on the modification type chosen and on the desired rate of pseudo random numbers sequence generated by described structures. Statistical tests results analysis shall be discussed in the full version of this article.

References

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

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

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

[4] S. W. Golomb: *Shift-Register Sequences And Spread-Spectrum Communications*, IEEE Third International Symposium on Spread Spectrum Techniques & Applications Oulu, Finland, July 4 - 6, 1994, pp.14-15

[5] L. Chen , G. Gong : *Pseudo-random Sequence (Number) Generators*, Communication Systems Security, Appendix A, 2008.

[6] P. Alfke: *Efficient Shift Registers, LFSR Counters and Long Pseudo-Random Sequence Generators*, Xilinx application note, 1996, Vol 1.1, pp.1-6.

[7] J. Walczak, R. Stępień: *Shift Registers with Dynamic Feedback Loop*, XXXIV konferencja IC-SPETO, Ustroń, 2011, pp.125-126

[8] J. Walczak, R. Stępień.: *Application of the DLFSR generators in spread spectrum communication*, 19th International Conference “MIXDES Design of Integrated Circuits and Systems” ,MIXDES-2012, Warszawa, maj 2012, pp.555-558

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

[10] P. Czernik: *Metodyka testowania bezpieczeństwa generatorów liczb pseudolosowych w systemach pomiarowo-sterujących*, Prace Instytutu Lotnictwa, Kwartalnik naukowy 6/2009 (201), ss. 20-34.