TECHNICAL TRANSACTIONS | CZASOPISMO TECHNICZNE
AUTOMATIC CONTROL | AUTOMATYKA
3-AC/2013

VOLODYMYR MAKSYMOVYCH*, OLEH HARASYMCHUK**, YURIY KOSTIV*

POISSON PULSE SEQUENCE GENERATORS BASED UPON MODIFIED GEFFE GENERATORS

GENERATORY CIĄGÓW IMPULSÓW POISSONA OPARTE NA ZMODYFIKOWANYCH GENERATORACH GEFFEGO

Abstract

The article presents principles of optimizing the parameters of structural elements Geffe generator. The quality of this optimization is confirmed by statistical tests package NIST STS. The article provides methodology for research into the settings of the output signals of the Poisson pulse sequence generators using Pearson's chi-squared test.

Keywords: *Geffe generator, pseudo-random sequence, tests NIST STS*

Streszczenie

W artykule zawarto zasady optymalizacji parametrów elementów strukturalnych generatora Geffego. Jakość optymalizacji została potwierdzona za pomocą pakietu testów statystycznych NIST STS. Przedstawiono metodykę badania parametrów wyjściowych sygnałów generatorów kolejności impulsów Poissona z zastosowaniem zmodyfikowanego kryterium Pearsona.

Słowa kluczowe: *generator Geffego, ciąg pseudolosowy, testy NIST STS*

* Prof. D.Sc. Ph.D. Volodymyr Maksymovych, M.Sc. Yuriy Kostiv, Chair of Information Technology Security, Lviv Polytechnic National University.

** Ph.D. Oleh Harasymchuk, e-mail: garasymchuk@ukr.net, Chair of Data Protection, Lviv Polytechnic National University.

1. Introduction

As information technology undergoes rapid development, random and pseudorandom sequence generators (PRSGs) substantially widen the scope of their application.

As it stands at present, multiple methodologies and principles exist supporting the generation of pseudorandom sequence, each of the said methodologies and principles having their respective advantages and disadvantages [1–5]. Among the aforementioned pseudorandom sequence generators, the merits of the Geffe generator stand out [6–10] – however, its qualitative characteristics have so far been unsufficcently researched. Thus, a necessity arises to improve the characteristics of the Geffe generator in order to ensure that the output sequences that it generates could be used directly and/or indirectly, to face and approach challenges that arise in the sphere of data protection.

In order to come to a certain conclusion as of whether it is or is not possible to use a certain pseudorandom sequence generator for the purpose of solving specific tasks, one should assess its quality and operation reliability. Conducting tests on generators, especially those being used in data protection systems (cryptographic applications in particular) is a pressing and practically important task. As of today, a number of graphic and evaluating tests are used to evaluate pseudorandom sequences. Additionally, several software products have been developed which contain packages of tests and these packages are used to verify a variety of statistical properties pertaining to pseudorandom generators, the most well-known of these being the package of NIST STS statistical tests [11, 12].

The purpose of this paper is to use the NIST STS package of statistical tests to ascertain which settings are optimal for the structural elements of a Geffe generator, by way of modification of the structural principles of its basic generators. It is the intention to develop new and means methods of building Poisson pulse generators (PPG), to conduct a comparative analysis providing insight into their characteristics, and to develop methodologies allowing their quality to be assessed.

2. Assessment of Geffe generator's statistical characteristics

A Geffe generator enables the mixing of two sequences (x_1 and x_2) from the outputs of two M-sequence generators the latter also being known as generators based upon linear feedback shift registers (LFSR) by way of controlling the LFSR output sequence 3. Such mixing takes place pursuant to the following function:

$$F\left(x_1, x_2, x_3\right) = x_1 \overline{x_3} + x_2 x_3 = x_3 \oplus x_1 x_2 \oplus x_2 x_3 \tag{1}$$

which can be performed using the multiplexer $2 \rightarrow 1$ – see Fig. 1 [1].

M-sequence generators being fundamental to a Geffe generator can be created in a variety of ways, pursuant to the following equation:

$$Q\left(t+1\right) = T^r Q\left(t\right) \tag{2}$$

where $Q(t)$ and $Q(t + 1)$ – represent the generator's register state in the t i $t + 1$ instants of time respectively (i.e. prior to and following the arrival of a synchronising pulse); T stands for square matrix of order N, whereas r stands for a degree of a primitive polynomial.

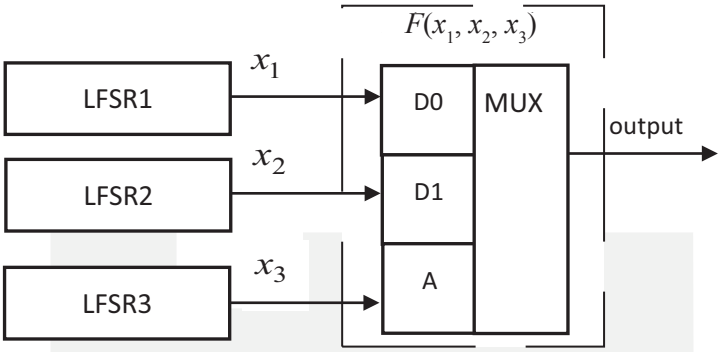


Fig. 1. A Geffe generator

We have taken a decision to use statistical tests and a change in the r degree (and thus a change in the structure of the generator itself) to ascertain whether such actions will or will not influence the quality of the Geffe generator's output pseudorandom sequence.

In order to assess the quality, we have not only opted for basic M-sequence generators with varying degrees of generative polynomial but also modified the degree of r to which the T matrix is elevated.

Assessment of output sequences from the generator was conducted using a package of NIST STS statistical tests. As of the present moment, no similar assessments of the Geffe generator can be found in research literature. In order to receive sequences from such a generator, we have turned to Delphi language choosing it to be our medium to develop simulation models of the said generator which allowed us to produce output sequences depending upon how the settings are changed.

A package of NIST STS tests includes 15 statistical tests developed to verify the hypothesis of randomness of binary sequences of arbitrary length are generated by PRSGs [11].

If the result of the P test falls within the 0.98–1.00 range, such a test result is pronounced successful. If the probability of P is below 0.98, the test is considered unsuccessful. Using the results procured in such a manner, we proceed to develop a statistical portrait of generators which is comprised of a matrix with a size of $m \times q$, where m stands for the number of binary sequences which are being verified and q stands for the number of statistical tests which are being performed to test each sequence. The ultimate resolution as to whether the sequence has or has not turned out to be random is taken following the obtaining of a cumulative result for all tests [12].

The testing was conducted at the significance level $\alpha = 0.01$, as recommended by the developers of NIST STS. Statistical portraits which can be seen upon observing Fig. 2 and Fig. 3 have the appearance of a size 1000 × 188 matrix which contains 188 000 values of respective probabilities. All of the figures display the confidence range in red lines.

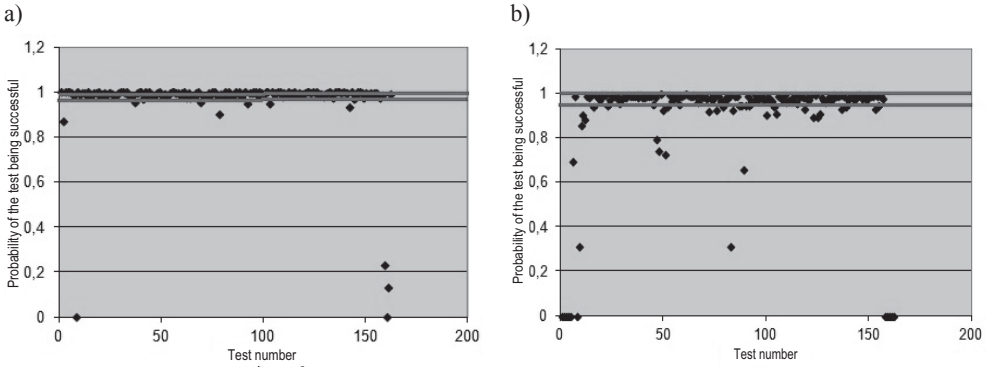


Fig. 2. A statistical portrait of Geffe generator No. 1: a) $r = 1$, b) $r = 5$

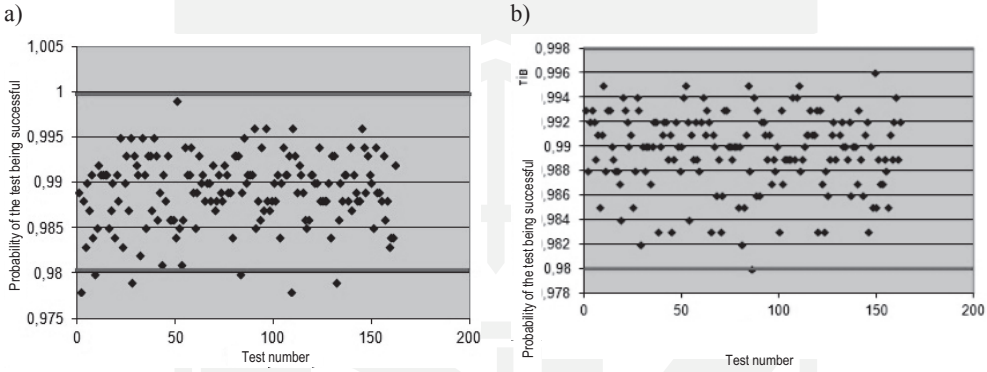


Fig. 3. A statistical portrait of Geffe generator No. 4: a) $r = 1$, b) $r = 5$

We have researched a large number of generators, but the optimisation of working settings is best shown using several of the following combinations:

1. *Geffe generator No. 1:* LFSR 1 and LFSR 2 based upon polynomial $\Phi(x) = 1 \oplus x^{12} + x^{17}$; LFSR 3 – $\Phi(x) = 1 \oplus x^{6} + x^{7}$;
2. *Geffe generator No. 2:* LFSR 1 based upon polynomial $\Phi(x) = 1 \oplus x^{12} + x^{17}$ and LFSR 2 based upon polynomial $\Phi(x) = 1 \oplus x^{18} + x^{25}$; LFSR 3 – $\Phi(x) = 1 \oplus x^{6} + x^{7}$;
3. *Geffe generator No. 3:* LFSR 1 and LFSR 2 based upon polynomial $\Phi(x) = 1 \oplus x^{18} + x^{25}$; LFSR 3 – $\Phi(x) = 1 \oplus x^{6} + x^{7}$;
4. *Geffe generator No. 4:* LFSR 1 and LFSR 2 based upon polynomial $\Phi(x) = 1 \oplus x^{18} + x^{31}$; LFSR 3 – $\Phi(x) = 1 \oplus x^{6} + x^{7}$.

A detailed report on the assessment of Geffe generators for each test is provided in Table 1.

Results of the research provided in Fig. 2 and Fig. 3, as well as in Table 1 testify to the fact that an increase of the degree *r* of basic M-sequence generators, the quality of a Geffe generator improves, since a number of failed tests decreases.

Table 1

Results of the testing of Geffe generators

No.	Statistical Test	Generators number							
		1		2		3		4	
		$r=1$	$r=5$	$r=1$	$r=5$	$r=1$	$r=5$	$r=1$	$r=5$
1	Frequency (Monobit) Test	–	–	–	+	–	+	+	+
2	Frequency Test within a Block	–	–	–	+	–	+	–	+
3	Cumulative Sums (Cusum) Test	–	–	–	–	–	+	+	+
4	Runs Test	–	–	+	+	+	+	+	+
5	Test for the Longest Run of Ones in a Block	–	–	+	+	+	+	+	+
6	Binary Matrix Rank Test	+	+	+	+	+	+	+	+
7	Discrete Fourier Transform (Specral) Test	–	–	–	–	–	–	+	+
8	Non-Overlapping Template Matching Test	–	–	+	+	+	+	–	+
9	Overlapping Template Matching Test	–	–	+	+	+	+	+	+
10	Maurer's 'Universal Statistical' Test	+	–	+	+	+	+	+	+
11	Approximate Entropy Test	–	–	+	+	+	+	+	+
12	Serial Test	–	–	+	+	+	+	+	+
13	Linear Complexity Test	+	–	+	+	+	+	+	+
14	Random Excursions Test	–	+	+	+	+	+	+	+
15	Random Excursions Variant Test	–	+	+	+	+	+	+	+

3. Poisson Pulse Sequence Generators created on the basis of modified Geffe generators

Poisson pulse sequence generators (PPSGs) can be created on the basis of pseudorandom sequence generators PRSGs [13] using both software and hardware. The primary advantage of the latter is its high performance. Another paper [13] offered PPSG structures based upon linear congruential pseudorandom sequence generators. Partial research into statistical characteristics of their output signals has shown that they mainly satisfy the requirements stipulated for devices meant to be used in computing technology. However, the fact that the algorythm of their work includes multiplication and division operators and thus also multiplication and division circuits, this causes substantial performance losses, thereby reducing the principal advantage that hardware has. Therefore, a problem arises of how to find efficient and fast methods and means to perform PPSG and find methods to assess their quality.

The main requirements stipulated for the attention of developers in the process of building a PPSG are stated below:

– a PPSG must have satisfactory statistical characteristics;
– a PPSG must have a long repetition period;

– high performance (for both hardware and software);
– a wide frequency range for output signal;
– ability to control the average frequency of the output signal;
– maximum possible simplicity of the build (for both hardware and software).

One of the most successful structures to form a pulse sequence with Poisson law of distribution which allows for the prompt control of the average frequency of PPSG output pulses is presented on Fig. 4. It is comprised of a PRSG, a comparing element (CE) and a logical element AND. PRSG, in turn, is comprised of generators based on generators built upon shift registers with linear feedback and a multiplexer 2 → 1.

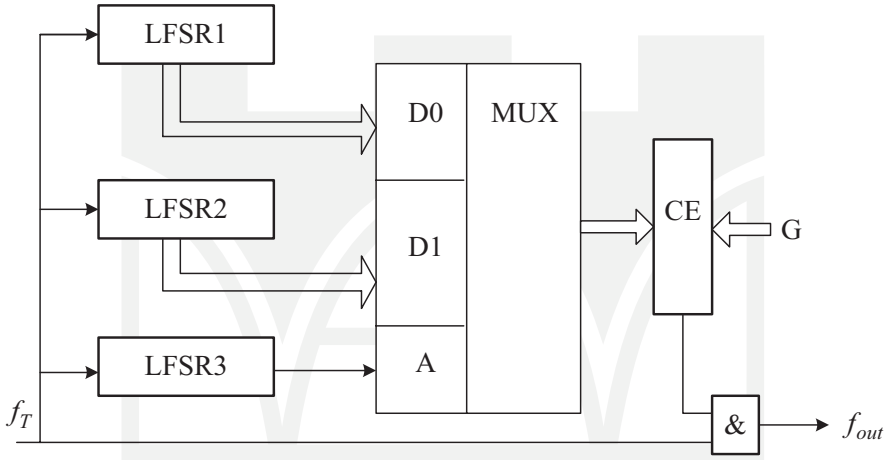


Fig. 4. PPSG based upon modified Geffe generator

Timed pulses arrive at the output of PPSG if the X number at the output of PPSG is smaller than the Control Code G. The average frequency of generator's input pulses is determined via the following equation:

$$f_{\text{out}} = \frac{\text{G}}{\text{X}_{\text{max}}} f_{\text{n}} \tag{3}$$

where:

X_{max} – stands for the maximum value of X,
f_T – stands for frequency of repetition of timed pulses,
G – stands for control code.

One of the possible options for building a PPSG is to build it on the basis of a Geffe generator which has the multiplication operator removed from its algorithm. Thus, a prospective direction in which the PPSG's characteristics may be improved is if it has such generators used in its structure, and if modifications can be performed if necessary, and if the settings of output pulse sequence can be controlled.

Since we have now researched the optimal settings of Geffe generators, we have attempted to create a model of PPSG on the basis of Geffe generators and assess the quality of output sequence.

4. Methodology for assessment of PPSG on the basis of Geffe generators

At the present time, there exist a great number of tests (graphic and evaluative) as well as packages of tests for the assessment of the quality of PPSG and PSG. We have applied one such test to assess the quality of the Geffe generator.

However, if we want to assess the quality of sequences obtained from generators with distributions diverging from a uniform distribution, we shall find far fewer of such tests. In particular, if one wants to assess the quality of a PPSG, one will also find few applicable tests for that purpose, and those that do exist are mostly graphic, whereby the conclusion of whether a certain sequence is or isn't applicable, may be quite subjective. It is far better to conduct such a research using assessment tests.

We, in order to research statistical characteristics, have offered the following methodology.

A sequence of PPSG input pulses is distributed into n equal groups, each of which contains $i_{\max}$ pulses (see Fig. 5). The maximum allowable number of groups is $n_{\max}$. Groups of input pulses correspond to groups of output pulses with the number of pulses k_1, k_2, ..., $k_{n\max}$.

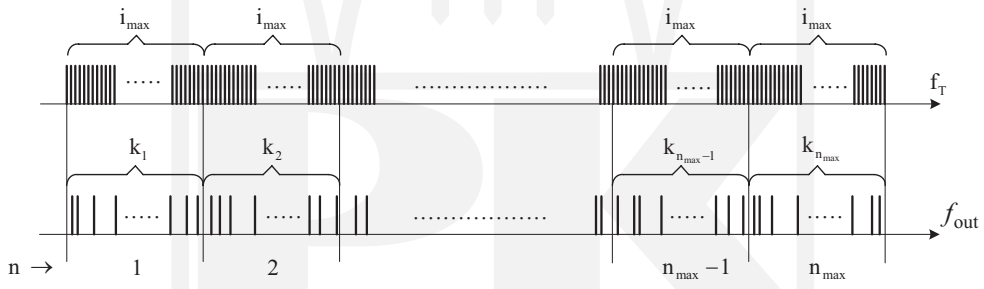


Fig. 5. Breakdown of input and output pulses into groups

The methodology offered by us is based upon classical methodology employed to verify the hypothesis of parent distribution pursuant to the Poisson law using Pearson's chi-squared test (the χ^2 test) [14]. That said, considering the specific characteristics of PPSG's architecture, the following supplements have been offered:

- for the k_1, k_2, ..., $k_{n\max} - k_c$ numbers, a nominal (theoretical) average value is set, regardless of what the value of the G control code is,
- the $i_{\max}$ is variable, depends upon what the value of G is, and is determined using the following equation:

$$i_{\max} = \frac{x_{\max}}{G} k_c \tag{4}$$

Further verification of the mentioned hypothesis proceeds as follows:

1. Using the empiric distribution obtained as a result of PPSG simulation, we determine the average value of $k_1, k_2, ..., k_{n_{max}} - k_B$.
2. For the λ parameter of Poisson's distribution, a random average $\lambda = k_B$ is taken.
3. Using the Poisson's formula:

$$P_j = \lambda^j \frac{e^{-\lambda}}{j!} = k_B{}^j \frac{e^{-k_B}}{j!} \tag{5}$$

we determine the probability of the appearance of exactly j pulses (within the i_{max} range) in n_{max} tests ($j = 0, 1, 2, ...$).

4. Theoretic frequencies are obtained as follows:

$$Q_j = P_j \cdot n_{max} \tag{6}$$

5. In the process of simulation, empiric frequencies – N_j – are determined.
6. For each value of j, Pearson's chi-squared test is used to determine the following:

$$S_j = \frac{(N_j - Q_j)^2}{Q_j} \tag{7}$$

$$\chi_c^2 = \sum_{j=0}^{j_{max}} S_j \tag{8}$$

7. If necessary, the N_j, P_j and Q_j values corresponding to the unlikely probabilities of P_j may be summarised into one or two groups; in this case, the (7) and (8) calculations are performed with that fact having been taken into due consideration.
8. The number of degrees of freedom is determined as follows:

$$r = d - 2 \tag{9}$$

where d stands for the number of groups remaining after possible summarisation.

9. Using the tables of χ^2 critical distribution points [14]; using a selected level of significance α (usually, α is given one of the following three variants of value: 0.1; 0.05; or 0.01) and using the number of degrees of freedom, r, the critical χ^2_{kp} value is determined. If $\chi^2_c < \chi^2_{kp}$ – then there is no grounds to reject the hypothesis stating that the pulse sequence is in compliance with Poisson's law of distribution.

The proposed methodology was applied primarily in the process of examination of PPSG parameters implemented in software whereby the Random function of the Delphi programming language (environment) was used.

The Fig. 6 displays the results of a research into ГПППП on the basis of a modified Geffe generator whereby the following values of parameters of its structural elements were taken: polynomial $F(x) = 1 + 18x + 25x$, matrix T1, LFSR 1 – $r = 10$; LFSR 2 – $r = 5$; LFSR 3 – $r = 3$.

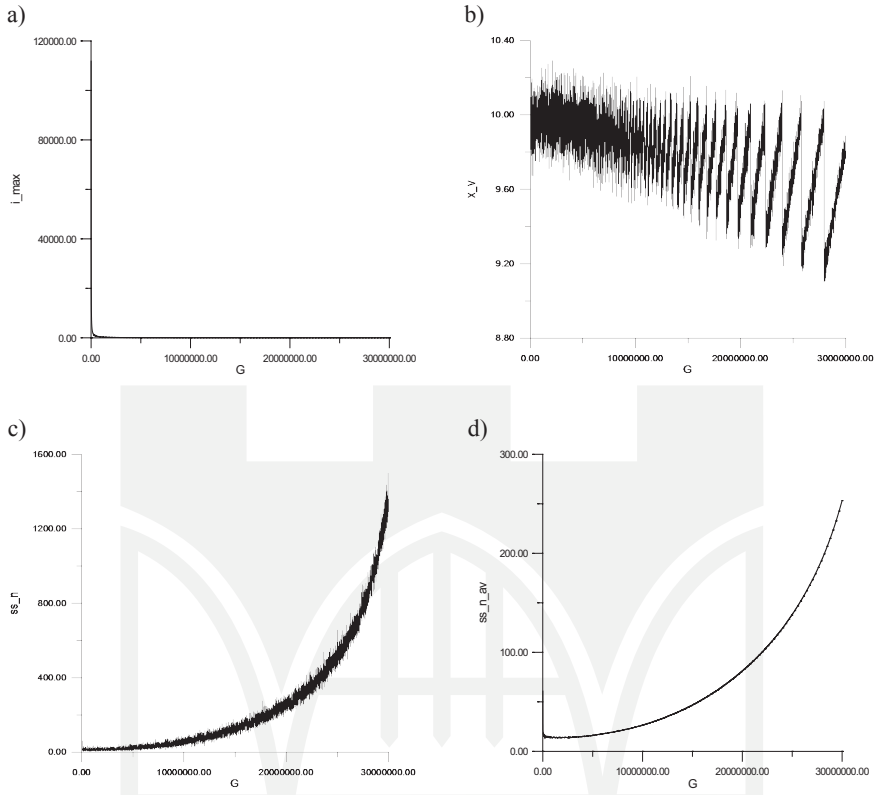


Fig. 6. Research results of PPSG on the basis of a Geffe generator whereby G changes its value within the 0–30000 range

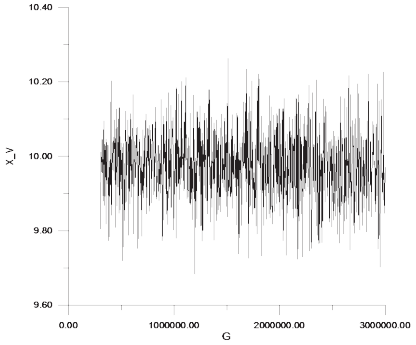
Here one can see how the following values are dependent upon the control code G:

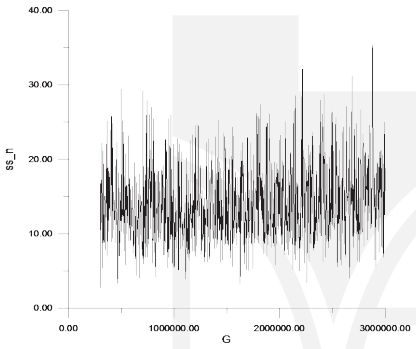
- $i\_{\max}$ – number of input pulses in the group i_{max} (Fig. 6a);
- x_v – statistical (selected) average number of output pulses in the group k_B (Fig. 6b);
- ss_n – value of the Pearson's chi-squared test χ^2_c (Fig. 6c);
- ss_n_av – current average value of Pearson's chi-squared test χ^2_{ccep} (Fig. 6d).

The results of the application of the proposed methodology for research into statistical characteristics of the input signals of PPSG for some variants of PPSG architecture on the basis of Geffe generators are provided in Fig. 7–8.

The provided results allow us to come to the conclusion that the statistical characteristics of the output signal of PPSG substantially depend upon the architecture of PSG. The PPSG is built in compliance with the offered structure (Fig. 4) which not only allows for the improvement of statistical characteristics but also for extending/increasing the period of repetition.

Statistical characteristics of the output signal of PPSG substantially depend upon the degree of the r matrix which sets the structure of LFSR linear feedbacks.





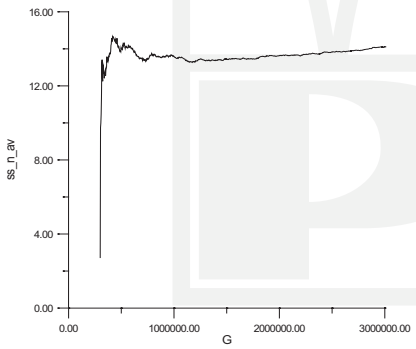
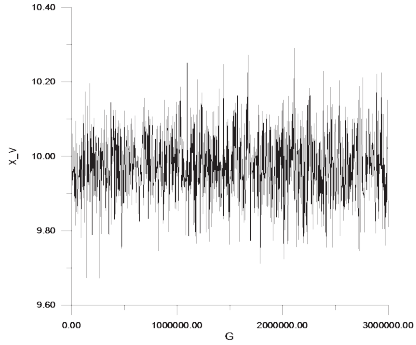
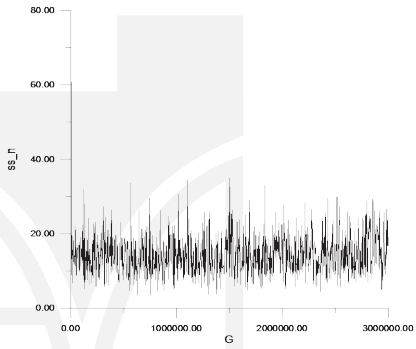


Fig. 7. Research results of PPSG on the basis of a Geffe generator whereby G changes its value within the 300–3000 range





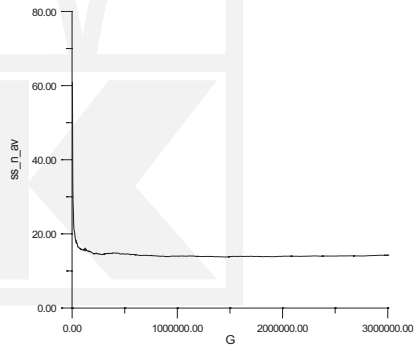


Fig. 8. Research results of PPSG on the basis of a Geffe generator whereby G changes its value within the 0–3000 range

5. Conclusions

By way of using simulation modelling and statistical testing, it has been ascertained that by modifying the structure of basic LFSR generators, specifically by increasing the value of the *r* degree and by choosing the generative polynomial with a larger degree, one may

substantially improve the quality of Geffe generator's output pulse sequence. Research has shown that $r = 5$ is the optimal value here. Further augmentation of r for large degrees of the generative polynomial does not cause substantial improvement in the quality of the output sequence; however, in this case the creation of such a generator requires higher equipment expenditures.

The paper proposes to build a PPSG on the basis of a modified Geffe generator which, in order to create pseudorandom numbers, resorts to the multiplexing of PSG bits on the basis of LFSR with the help of output of one of the bits of the control LFSR which allowed for expanding the range of values of the control code enough to be able to obtain satisfactory statistical characteristics of the output signal.

The statistical characteristics of PPSG are satisfactory enough for it to be used, in particular, to test radiation dosage metres. The proposed methodology for testing can be efficiently applied to test PPSGs built on the basis of other basic generators.

References

[1] Ivanov M.A., *Cryptographic methods for data protection in computer systems and networks*, Moscow 2001, 368.

[2] Ivanov M.A., *Theory, application, and quality assessment of pseudorandom sequence generators*, Moscow 2003, 240.

[3] Harasymchuk O.I., *Pseudorandom number generators, their application, classification, principal methods of construction and assessment of quality*, Kyiv 2002, 7.

[4] Harasymchuk O.I., *Poisson Pulse Sequence Generators based on m-sequence generators*, Herald of Lviv Polytechnic National University, Computer Sciences and Information technologies, No. 521, 2004, 17-23.

[5] Rock A., *Pseudorandom Number Generators for Criptographic Applications*, Salzburg 2005, 57-65.

[6] Rosenthal J., *Detection and Exploitation of Small Correlations in Stream Ciphers*, Institute of Mathematics, University of Zurich, 2008.

[7] Qi D., *Modified Geffe Test Pattern Generator for Built-in Self-test*, IEEE Pacific Rim Conference, 22–24 Aug. 2007, 210-213.

[8] Oujezský V., *Cryptographic Sequence Generators for Stream Cipher and Their Behavioral Description*, International Journal of Advanced Research in Computer Science and Software Engineering Research Paper, Vol. 4, Issue 3, March 2014.

[9] Khamees H.Th., *Encryptoin and decryption of data by Using Geffe Algorithm*, International Journal of Modern Engineering Research (IJMER), Vol. 2, Issue 3, May–June 2012, 1354-1359.

[10] Wei S., *On Generalization of Geffe's Generator*, IJCSNS International Journal of Computer Science and Network Security, Vol. 6, No. 8A, August 2006, 161-165.

[11] *NIST statistical tests*, aviable on: http://csrc.nist.gov/groups/ST/toolkit/rng/documents/nissc-paper.pdf

[12] NIST SP 800-22. *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, aviable on: http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf

[13] Harasymchuk O.I., *Test pulse sequence generators for radiation dosage metres*, Herald of Lviv Polytechnic National University, Thermal engineering. Environmental engineering. Automatisation, No. 06, 2004, 186-192.

[14] *Pearson's chi-squared test*, aviable on: http://en.wikipedia.org/wiki/Pearson%27s_chi-squared_test.