Parameters estimation of random sequence in the stochastic calculating devices

Gennady Galustov, Viacheslav Voronin, Sergei Makov

***Abstract* — In this article we introduce the concept of probabilistic binary element provides requirements, which ensure compliance with the criterion of "uniformity" in the implementation of the basic physical generators uniformly distributed random number sequences. Based on these studies, we obtained an analytic relation between the parameters of the binary sequence and parameters of a numerical sequence with the shift register output.**

***Keywords* — density of probability, stochastic processes, physical noise generator, shift register.**

I. INTRODUCTION

IN solving problems of simulation one of the main points of the decision is the right choice of quality parameters of the basic random perturbations, from which to a large extent depend on the variance estimates of the output parameters of the models.

Recently, very often these problems are used as input to the pseudo-random number sequences, followed by transformation of the statistical characteristics [1]. No additional difficulties arise when it comes to just about measuring the average values or the mean square values or the output of the study of correlations between input and output values of linear systems with constant parameters. The results of such studies depend only on the autocorrelation function of the pseudo-random input signal, which in this sense is very good approximation of white noise. However, the results of statistical analysis of nonlinear systems can have a marked effect of the distribution of the second and higher orders used by the pseudo-random noise signal, and these are not necessarily Gaussian distribution [2]. In addition, the law of distribution of the output of the linear system under the influence of pseudo-random noise is not derived theoretically, but it is difficult to assess the dispersion of the output parameters of the simulation model [3].

All this sometimes leads to the fact that at each subsequent solution of the parameter estimates are scattered so much that lead to uncertainty solutions and in theory, these parameters cannot be calculated.

II. METHODOLOGY

In contrast to the pseudo-random effects using a random process can be theoretically calculated values of the unknown parameters (here can be used by the central limit theorem). In addition, there is no need to correct approach to the selection of averaging intervals as in the study of linear systems and the study of nonlinear systems.

In constructing the random number generator (*RNG*), based on the use of natural sources of stochastic processes, very often there is the problem of choosing relationships between the parameters of the random number sequence and the characteristics of the original random process. The most common block diagram *RNG* with a uniform distribution is a scheme using a probabilistic binary element (*PBE*) and the shift register [4, 5].

Binary sequence output *PBE* generally prepared by polling rate $F = 1/T_0$ through the valve state ("*B*"), which is in time of the survey one arm symmetric trigger the counting input of which is fed formed of sufficient broadband random process (noise) Poisson stream of random pulses. The block diagram *PBE* shown in Figure 1, where 1 is the source of the noise; 2 is the threshold device; 3 is the power-generator; 4 is the symmetrical trigger; 5 is the coincidence circuit.

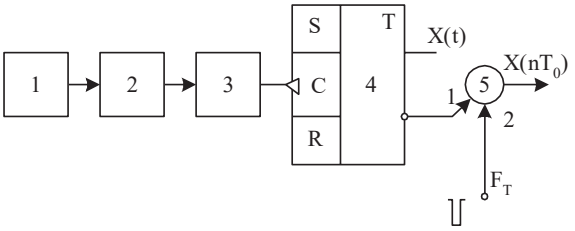

Fig 1. The block diagram

The noise as a narrow-band random process from the noise source 1 receives a threshold device 2 through which the emission of a random process that exceed the set threshold value U_0. Emissions that exceed the threshold value offset U_0, fed to the amplifier-shaper 3, which are formed on the duration and amplitude. The stream of random pulses from the output of the amplifier-shaper 3 is supplied to the count input of symmetrical trigger 4.

It is known that if the output of the threshold device will appear in a random process emissions that exceeded the threshold value $U_0 \geq 2\sigma_u$, where σ_u is the standard deviation of the amplitude distribution of the random process (noise), the intervals $\Delta\tau$ between occurrences of pulses at the output of the threshold device will be distributed approximately Poisson.

Viacheslav Voronin is from dept. of radio-electronics systems, Don State Technical University, Shevchenko street 147, Shakhty, 346500, Rostov reg., Russia (phone: +79885343459; e-mail: voroninslava@gmail.com).

If the performance of the amplifier-shaper is sufficient to form each incoming pulse stream of pulses is generated by amplitude and duration to retain the Poisson distribution. The random function $X(t)$ that takes two values - zero and one - with a trigger input 4 is fed to the input of the coincidence circuit 5. The second input of the coincidence circuit 5 is fed a regular sequence of pulses with frequency $F_T = \frac{1}{T_0}$. The output of the coincidence circuit 5 is the output probability of a binary element. Timing diagram of *PBE* is shown in Figure 2, which shows that the random function at the output of *PBE* has only two possible values 0 and 1, representing the function of a discrete argument nT_0.

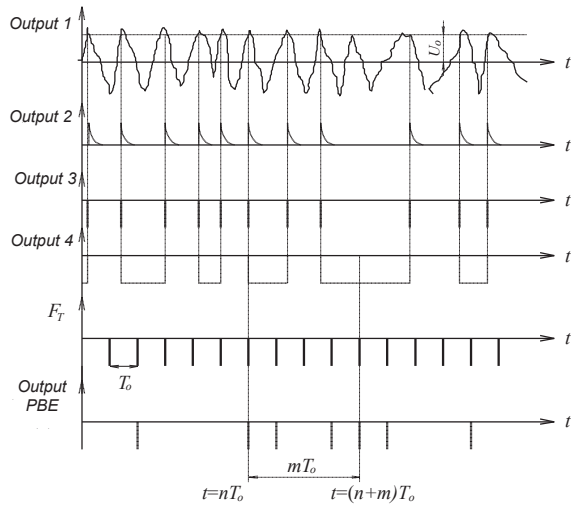

Fig 2. The timing diagram of *PBE*

Realization of these functions are usually called binary sequences. Note that in a case where a sequence of pulses at the input of flip-flop 4 obeys the Poisson distribution, the probability of occurrence of the output *PBE* units - p and scratch – equal $q = 1 - p$, and, hence, equal to *0,5*. The random function $X(nT_0)$ output *PBE* is fixed only when $p = q = 0{,}5$.

Assume that $p \neq q \neq 0{,}5$. The two-dimensional differential distribution law $f_{\xi}(x_1, x_2; \tau = mT_0)$ of the random function $X(nT_0)$ at the output of *PBE*. We define all the possible values of pairs of random variables ξ_1 and ξ_2 the corresponding values $X(nT_0)$ in the points nT_0 and $(n+m)T_0$, and the likelihood that they will take these values. The probability of occurrence *PBE* output unit at a time $(n+m)T_0$ provided that the time nT_0 was *PBE* output unit will be equal to the product of the probability of occurrence of a unit p on the conditional probability $P_t(mT_0)$ that during mT_0 the trigger 4 will go even number of Poisson impulses. The probability of occurrence of units, with the proviso that it is preceded by a zero, respectively, will be equal to the product of the conditional probabilities q on the probability $P(mT_0)$ that a time trigger 4 will go to an odd number of Poisson impulses.

The probabilities of occurrence of a zero output, respectively, *PBE* will be equal to the product of probability $p \cdot P(mT_0)$ and $q \cdot P_t(mT_0)$.

The binary sequence output *PBE* is a random function of discrete time $X(n \cdot T_0)$.

Since the sequence at the output of the flip-flop obeys Poisson:

$$f_k = \frac{(\lambda \cdot m \cdot T_0)^k}{k!} \cdot \exp(-\lambda \cdot m \cdot T_0), \quad (1)$$

where λ - the average frequency random pulses, the occurrence probability output *PBE* units $P_1(m \cdot T_0)$ and zero $P_2(m \cdot T_0)$ can be written as [1, 2]:

$$P_1(m \cdot T_0) = \frac{1 + \exp(-2 \cdot \lambda \cdot m \cdot T_0)}{2};$$

$$P_2(m \cdot T_0) = \frac{1 - \exp(-2 \cdot \lambda \cdot m \cdot T_0)}{2}.$$

A binary sequence $X(n \cdot T_0)$ is used for the preparation of N - uniformly distributed random bit binary numbers by providing the shift register via its *N*- groups of neighboring values (see. Figure 3).

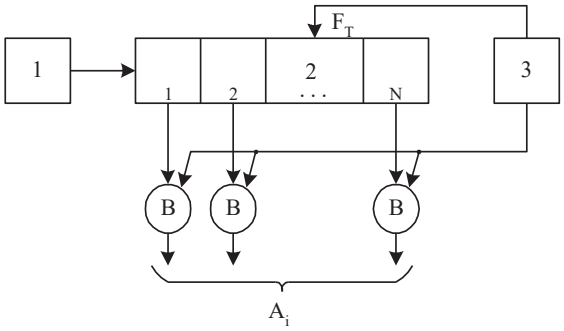

Fig 3. The shift register

If we denote

$$P_1(T_0) = \frac{1 + \exp(-2 \cdot \lambda \cdot T_0)}{2} = \alpha \text{ and}$$

$$P_2(T_0) = \frac{1 - \exp(-2 \cdot \lambda \cdot T_0)}{2} = \beta,$$

the probability of an *N*-bit number can be calculated a priori. It will consist of (*N*-1) and the product multiplied α and β by the probability of occurrence of the first $p = q = 0{,}5$.

For example: *A* = the number 100101101, will have the conditional probability of occurrence.

It is easy to see that the most likely to have a number *A* = 1111111; or A = 0000000, i.e.:

$$P_{\max} = \frac{1}{2} \cdot \alpha^{N-1}. \quad (2)$$

The minimum probability will have the number A = 101010; or *A* = 010101, that is:

$$P_{\min} = \frac{1}{2} \cdot \beta^{N-1}. \quad (3)$$

It is known [1, 2] that the *N*-bit uniformly distributed binary numbers has an equal probability of $1/2^N$. Using (2) and (3) one can find the value of the maximum deviation of the distribution law of probabilities *N*-bit

random numbers derived from the binary sequence from uniform. Relative deviation from the uniform can be written as:

$$\Delta_1 = \frac{P_{\max} - 1/2^N}{1/2^N};\ \Delta_2 = \frac{1/2^N - P_{\min}}{1/2^N};$$

$$\Delta_1 = (2\cdot\alpha)^{N-1} - 1;\ \Delta_2 = 1 - (2\cdot\beta)^{N-1}.$$

Since $\Delta_1 > \Delta_2$ then we shall determine $\Delta_1 = \Delta$.

$$(\Delta+1)^{1/(N-1)} = 2\cdot\alpha,$$

$$1 + \exp(-2\cdot\lambda\cdot T_0) = (1+\Delta)^{1/N+1} \qquad (4)$$

The expression on the right side of (4) in a series in the binomial theorem while limiting the first three terms

$$1 + \exp(-2\cdot\lambda\cdot T_0) \approx 1 + \frac{\Delta}{N-1} + \frac{1}{2}\cdot\left(\frac{1}{N-1} - 1\right)\cdot\Delta^2 + \ldots,$$

$$\exp(2\cdot\lambda\cdot T_0) \approx \frac{2\cdot(N-1)^2}{2\cdot\Delta\cdot(N-1) - \Delta^2\cdot(N-2)}.$$

Taking the logarithm of both sides, we finally obtain

$$\lambda\cdot T_0 \approx \frac{1}{2}\cdot \mathrm{Ln}\left[\frac{2\cdot(\mathrm{N}-1)^2}{2\cdot\Delta\cdot(N-1) - \Delta^2\cdot(N-2)}\right]. \qquad (5)$$

Expression (5) shows what should be the ratio between the average frequency of a Poisson flow λ and the clock frequency $F = 1/T_0$ of the survey in the *PBE* to the relative deviation probabilities of *N*-bit numbers from a uniform made up no more than Δ.

III. EXPERIMENTS

Figure 4 shows a graph of the probability distribution of digital five-digit combination ($N = 5$) uniformly distributed at random code $\lambda\cdot T_0 = 2$ and $\lambda\cdot T_0 = 1$. The occurrence of unevenness digital output *PBE* combinations depends strongly on the frequency characteristics of noise, which are determined by a clock frequency and λ poll *PBE* $F = 1/T_0$.

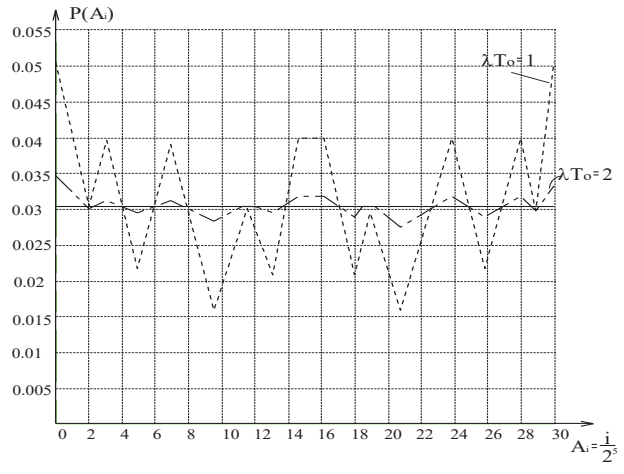

Fig 4. Probability distribution of digital five-digit combination

Conditions equiprobability appearance *PBE* digit output can be defined as

$$\varepsilon \le P_1(T_0) - P_2(T_0) = \alpha - \beta = \exp(-2\cdot\lambda\cdot T_0)\ . \qquad (6)$$

If we designate through $n = 2\cdot F_m\cdot T_0$ - number of independent samples that can be obtained by implementing a noise duration T_0 (by Nyquist theorem); F_m - Band noise, which is determined by the bandwidth of the amplifier noise; P - probability of exceeding the reference value in times of realization of the noise shaper restrictive threshold in U_0 *PBE*:

$$P = \int_{U_0}^{\infty} f(u)du,$$

where f - density of distribution of the instantaneous values of noise.

Given that imbalance probability *P1 (T0)* and *P2(T0)* is always there, it is possible to determine the condition (6), that is,

$$\varepsilon \le P_1(2\cdot k) - P_2(2\cdot k - 1) = [P - (1-P)]^n = [2\cdot P - 1]^n\ .$$

where k = 1,2,3, ...

If you are not interested with ε, the last expression can be rewritten as:

$$\varepsilon \le |(2\cdot P - 1)|^n = (1 - 2\cdot P)^n. \qquad (7)$$

Comparing (7) and (6), we have:

$$(1-2\cdot P)^n = \exp(-2\cdot\lambda\cdot T_0) \cong \frac{2\cdot\Delta\cdot(N-1) - \Delta^2\cdot(N-2)}{2\cdot(N-1)^2}.$$

How $n = 2\cdot F_m\cdot T_0$, given that can be written:

$$F_m = \frac{1}{2\cdot T_0}\cdot\frac{Ln\left[2\cdot\Delta\cdot(N-1) - \Delta^2\cdot(N-2)/\left(2\cdot(N-1)^2\right)\right]}{Ln(1-2\cdot P)}. \qquad (8)$$

Expression (8) to evaluate the band amplifier noise, wondering relative deviation of the probability of occurrence of numerical combinations in the *PBE* output - Δ, the probability of exceeding the threshold U_0 in the shaper *PBE* - *P*, a clock frequency of random numbers $f = \frac{1}{N\cdot T_0}$ and the number of bits in the shift register *N*.

For example: If you want to generate random ten-digit number (N = 10) with a frequency of $f = \frac{1}{10\cdot T_0} = 10^4$ Hz, wherein the relative deviation to numerical combinations of equiprobable $\left(P = 1/2^N\right)$ was not more than 1% (Δ = 0,01) at a probability P = 0,05 (a Gaussian the distribution of the instantaneous values of the noise P = 0,05 – correspondence $U_0 \cong 1{,}65\cdot\sigma$), we obtain $F_m = 3{,}2\cdot 10^6$ *Hz*.

The dependence of the noise bandwidth of the amplifier on the number N of bits of the random number at random $F_A = 1/NT_0 = 10^5$ *Hz* with a deviation $\Delta = 0{,}01$ with different probabilities P is shown in Figure 5. The bandwidth amplifier F_m in *PBE* little depends on the number of bits in the register N and changes significantly the probability of exceeding the limiting threshold generator P.

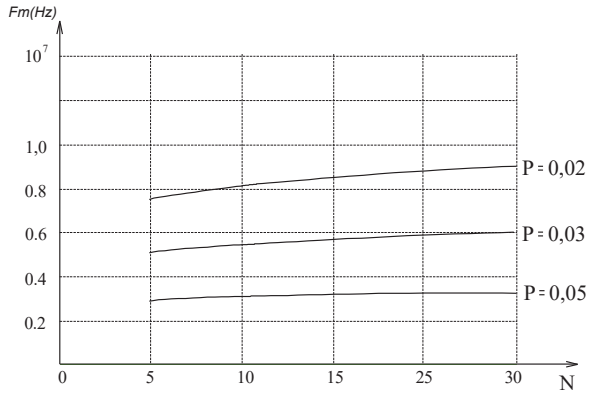

Fig 5. The dependence of the noise bandwidth of the amplifier

IV. Conclusion

The concept of probabilistic binary element provides requirements, which ensure compliance with the criterion of "uniformity" in the implementation of the basic physical generators uniformly distributed random number sequences was proposed. An analytic relation between the parameters of the binary sequence and parameters of a numerical sequence obtained with the shift register output.

V. Acknowledgments

This work was supported by Russian Ministry of Education and Science in frame of the Federal Program "Research and development on priority directions of scientific-technological complex of Russia Federation in 2014-2020" (contract №14.576.21.0080 (RFMEFI57614X0080)).

References

[1] Stojanovski T., Kocarev L. Chaos-based random number generators — part I: analysis/ IEEE Trans. Circ. Sys. I, 48 (2001), pp. 281–288.

[2] Kanso A., Smaoui N. Logistic chaotic maps for binary numbers generations/ Chaos, Solitons & Fractals, 40 (2009), pp. 2557–2568.

[3] Behnia S., Akhavan A., Akhshani A., Samsudin A. A novel dynamic model of pseudo random number generator. Journal of Computational and Applied Mathematics, Volume 235, Issue 12, 15 April 2011, pp. 3455–3463.

[4] Galustov G.G. Simulation of stochastic processes and estimation of their statistical characteristics. M.: Radio and Communications, 1999, 120 p.

[5] Chetverikov V.N., Bakanovich E.A. Stochastic modeling systems computing devices. M.: Engineering, 1989, 271 p.