Proceedings of the International Multiconference on
Computer Science and Information Technology pp. 309–315
ISBN 978-83-60810-27-9
ISSN 1896-7094

Analysis of Pseudo-Random Properties of Nonlinear Congruential Generators with Power of Two Modulus by Numerical Computing of the *b*-adic Diaphony

Ivan Lirkov
Institute of Information and Communication Technologies
Bulgarian Academy of Sciences
Acad G. Bonchev, bl. 25A, 1113 Sofia, Bulgaria
E-mail: ivan@parallel.bas.bg

Stanislava Stoilova
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
Acad. G. Bonchev, bl. 8, 1113 Sofia, Bulgaria
E-mail: stoilova@math.bas.bg

***Abstract*—We consider two nonlinear methods for generating uniform pseudo-random numbers in [0, 1), namely quadratic congruential generator and inversive congruential generator. The combinations of the Van der Corput sequence with the considered nonlinear generators are proposed. We simplify the mixed sequences by a restriction of the *b*-adic representation of the points.**

We study numerically the *b*-adic diaphony of the nets obtained through quadratic congruential generator, inversive congruential generator, their combinations with the Van der Corput sequence, and the simplification of the mixed sequences. The value of the *b*-adic diaphony decreases with the increase of the number of the points of the simplified sequences which proves that the points of the simplified sequences are pseudo-random numbers. The analysis of the results shows that the combinations of the Van der Corput sequence with these nonlinear generators have good pseudo-random properties as well as the generators.

I. Introduction

Many branches of the contemporary science research as stochastic simulation, stochastic optimization techniques, computational statistics, Monte Carlo simulation, molecular dynamics, cryptography, computer graphics, etc., depend on the random numbers [3], [4], [16], [19]–[21], [29]. In practice, random numbers are generated by deterministic recursive rules, formulated in terms of simple arithmetic operations. Obviously the emerging numbers can at best be pseudo-random. To design random number generators that approximate "true randomness" as closely as possible, is a great challenge. Except this obvious requirement, pseudo-random number generators should possess reproducible results, they should be portable between different computer architectures, and since in most applications millions of random numbers are needed, generators should be as efficient as possible.

The fields of probability and statistics are built over the abstract concepts of probability space and random variable. This has given rise to elegant and powerful mathematical theory, but exact implementation of these concepts on conventional computers seems impossible. Random variables and other random objects are simulated by deterministic algorithms. The purpose of these algorithms is to produce sequences of numbers or objects whose behavior is almost undistinguishable from that of their "truly random" counterparts, at least for the application of interest. Depending on the context, pseudo-random number generators must satisfy different requirements.

For Monte Carlo methods, the main aim is to reproduce the statistical properties on which these methods are based, so that the Monte Carlo estimators have a behavior as expected. On the other hand, for gambling machines and cryptology, observing the sequence of output values for some time should provide no practical advantage for predicting the forthcoming numbers better than by just guessing at random. In computational statistics, random variate generation is usually made in two steps. The first step is generating imitate ions of independent and identically distributed (i.i.d.) random variables having the uniform distribution over the interval (0, 1). And the second step is applying transformations to these i.i.d. $U(0,1)$ random variates in order to generate (or imitate) random variates and random vectors from arbitrary distributions. The expression (pseudo-)random number generator (RNG) usually refers to an algorithm used for first step. In principle, the simplest way of generating a random variate X with distribution function F from a $U(0,1)$ random variate U is to apply the inverse of F to $U : X = F^{-1}(U) \stackrel{\text{def}}{=} \min\{x|F(x) \geq U\}$. This is the inversion method. It is easily seen that X has the desired distribution: $P[X \leq x] = P[F^{-1}(U) \leq x] = P[U \leq F(x)] = F(x)$. Other methods are sometimes preferable when F^{-1} is too difficult or expensive to compute.

The basic ingredients of any stochastic simulation are uniform pseudo-random numbers in the interval $[0,1)$. The outcome of a typical stochastic simulation strongly depends on the structural and statistical properties of the underlying pseudo-random number generators. That is why their quality is of fundamental importance for the success of the simulation. The classical and most frequently used method for the generation of pseudo-random numbers is still the linear congruential

method. However, its simple linear nature implies several undesirable regularities. Mainly for this reason, a variety of nonlinear methods for the generation of pseudo-random numbers has been introduced and studied as alternatives to the linear congruential method. These nonlinear congruential generators provide a very attractive alternative to linear congruential generators and have been extensively studied in the literature [1], [5], [7]–[10], [15], [16], [23], [25]–[28]. Two special cases: the quadratic congruential generator and the inversive congruential generator, are of special interest. A good survey of this important research area is given in [4], [17], [19]–[21], [29]. Many authors study pseudo-random properties of the sequences, generated by quadratic and inversive congruential generators by using the bounds of the discrepancy [2], [6], [11]–[13], [22], [24].

We use the $b-$adic diaphony to study pseudo-random numbers, generated by quadratic and inversive congruential generators. We will recall some known notions and definitions.

Let $\xi = (\mathbf{x}_j)_{j\geq 0}$ be a sequence in $[0,1)^s$ and $J = [\boldsymbol{\alpha}, \boldsymbol{\beta}) \subseteq [0,1)^s$, where $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_s)$ and $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_s)$. For arbitrary integer M $A_M(\xi; J)$ is the number of belonging to J points of ξ. The sequence $\xi = (\mathbf{x}_j)_{j\geq 0}$ is uniformly distributed mod 1 in $[0,1)^s$ if for every $J = [\boldsymbol{\alpha}, \boldsymbol{\beta}) \subseteq [0,1)^s$ the equality

$$\lim_{M\to\infty} \frac{A_M(\xi; J)}{M} = \prod_{i=1}^{s} (\beta_i - \alpha_i)$$

is hold, see [30].

The above equality shows when a sequence of points in $[0,1)^s$ is uniformly distributed but it does not allow to compare the distributions of two sequences. For that purpose various measures of the distribution of the sequences are used. Such measure is the $b-$adic diaphony [14].

Let $b \geq 2$ be a fixed integer and b denotes the base of the number system everywhere in this paper. Also, let an arbitrary $x \in [0,1)$ have a $b-$adic representation $x = \sum_{l=0}^{\infty} x_l b^{-l-1}$, where for $l \geq 0$, $x_l \in \{0, 1. \ldots, b-1\}$ and for infinitely many values of l, $x_l \neq b-1$. The integer part of $b-$adic logarithm of x is $\lfloor \log_b x \rfloor = -g-1$, if $x_l = 0$ for $l < g$ and $x_g \neq 0$. We denote the operation $x \dot{-} y = \sum_{l=0}^{\infty} [(x_l - y_l) (\mathrm{mod}\ b)] b^{-1-l}$ and for vectors $\mathbf{x}, \mathbf{y} \in [0,1)^s$ we note $\mathbf{x} \dot{-} \mathbf{y} = (x_1 \dot{-} y_1, x_2 \dot{-} y_2, \ldots, x_s \dot{-} y_s)$, where $\mathbf{x} = (x_1, x_2, \ldots, x_s), \mathbf{y} = (y_1, y_2, \ldots, y_s)$.

We define the functions $\gamma : [0,1) \to \mathbb{R}$ and $\Gamma : [0,1)^s \to \mathbb{R}$ as

$$\gamma(x) = \begin{cases} b+1-(b+1)b^{1+\lfloor \log_b x \rfloor}, & \text{if } x \in (0,1) \\ b+1, & \text{if } x = 0 \end{cases}$$

and

$$\Gamma(\mathbf{x}) = -1 + \prod_{d=1}^{s} \gamma(x_d), \mathbf{x} = (x_1, x_2, \ldots, x_s).$$

The $b-$adic diaphony $F_N(\xi)$ of the first N elements of the sequence $\xi = (\mathbf{x}_i)_{i\geq 0}$ in $[0,1)^s$ is defined as

$$F_N(\xi) = \left(\frac{1}{(b+1)^s - 1} \frac{1}{N^2} \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} \Gamma(\mathbf{x}_i \dot{-} \mathbf{x}_j) \right)^{\frac{1}{2}},$$

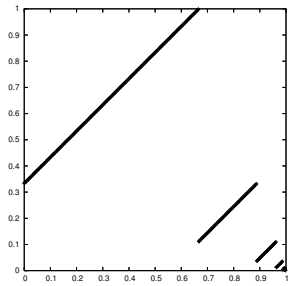


Fig. 1. The distribution of points of the Van der Corput sequence with $N = 1024$, $b = 3$.

where the coordinates of all points of the sequence ξ are $b-$adic rational.

Let $i = \sum_{l=0}^{\infty} i_l b^l$ be the $b-$adic representation of the non-negative integer i. Then the i-th element of the Van der Corput sequence is defined as

$$\zeta_b(i) = \sum_{l=0}^{\infty} i_l b^{-l-1}.$$

The Van der Corput sequence is deterministic sequence and does not have pseudo-random properties. The distribution of 1024 points of the net

$$(\zeta_b(i), \zeta_b(i+1))$$

is seen on Fig. 1.

II. Nonlinear Congruential Generators

Let $M \geq 2$ be modulus of a nonlinear congruential generator. The sequence of pseudo-random numbers $\left\{ x_i = \frac{y_i}{M} \right\}$ is produced by nonlinear congruential generator $y_{i+1} = f_M(y_i), \quad y_i \in [0, M), \quad \forall i = 0, 1, \ldots$, where $y_0 \in [0, M)$ is the initial starting point. The study of the pseudo-randomness of the sequence $x_i, i = 0, 1, \ldots$ is connected with the estimation of the distribution of the two-dimensional net

$$(x_i, x_{i+1}) = \left(\frac{y_i}{M}, \frac{y_{i+1}}{M} \right). \tag{1}$$

Our aim is a numerical computing of the $b-$adic diaphony F_N of these two-dimensional nets. For the function f_M we use two nonlinear congruential generators: quadratic generator and inversive generator.

The quadratic congruential generator (QCG) is introduced by Knuth [17] and studied by [2], [11], [12]. This generator is defined as

$$f_M^{QCG}(y_i) \equiv q_2 y_i^2 + q_1 y_i + q_0 (\mathrm{mod}\ M),$$
$$y_{i+1} = f_M^{QCG}(y_i), \quad y_i \in [0, M), \tag{2}$$

where q_2, q_1, q_0 are three integer parameters.

The inversive congruential generator (ICG) is defined as

$$f_M^{ICG}(y_i) \equiv \begin{cases} r_{-1} y_i^{-1} + r_0 (\mathrm{mod}\ M), & \text{if } y_i \geq 1, \\ r_0, & \text{if } y_i = 0, \end{cases}$$

TABLE I
THE DIAPHONY F_N OF QUADRATIC AND INVERSIVE GENERATORS, $b = 3$.

M	QCG	ICG
16	0.175682	0.310316
32	0.122138	0.175682
64	0.074016	0.198416
128	0.057257	0.159625
256	0.039630	0.123801
512	0.028726	0.053107
1024	0.020017	0.046659
2048	0.014486	0.029463
4096	0.011113	0.023956
8192	0.007010	0.015353
16384	0.005087	0.011706
32768	0.003595	0.007119
65536	0.002502	0.006440

where r_{-1}, r_0 are integer parameters and y_i^{-1} denotes the inversive element of y_i, i.e. $y_i^{-1} y_i \equiv 1 (\mathrm{mod}\ M)$,

$$y_{i+1} = f_M^{ICG}(y_i), \quad y_i \in [0, M). \tag{3}$$

In this paper we consider generators with modulus $M = 2^\mu$, $\mu \geq 4$. In this case the quadratic congruential generator (2) is purely periodic with maximum possible period length $M = 2^\mu$ if and only if

$$q_0 \equiv 1(\mathrm{mod}\ 2), \quad q_2 \equiv 0(\mathrm{mod}\ 2), \quad q_2 \equiv q_1 - 1(\mathrm{mod}\ 4).$$

In [10] it is proved that for $M = 2^\mu$ the inversive congruential generator (3) has maximal period length $2^{\mu-1}$ if and only if

$$r_{-1} \equiv 1(\mathrm{mod}\ 4) \quad \text{and} \quad r_0 \equiv 2(\mathrm{mod}\ 4).$$

Further in this paper we will denote the period of the generators by N.

III. PSEUDO-RANDOMNESS OF THE SEQUENCES PRODUCED BY QUADRATIC AND INVERSIVE CONGRUENTIAL GENERATORS

In this section the $b-$adic diaphony of two-dimensional nets (1), obtained by quadratic and inversive congruential generators, is numerically computed. We used PRNG library [31] created by Otmar Lendl to obtain the sequences. The parameters used in the numerical experiments in this work are: $q_2 = 8, q_1 = 5, q_0 = 3, r_{-1} = 9, r_0 = 6, y_0 = 1$, i. e.

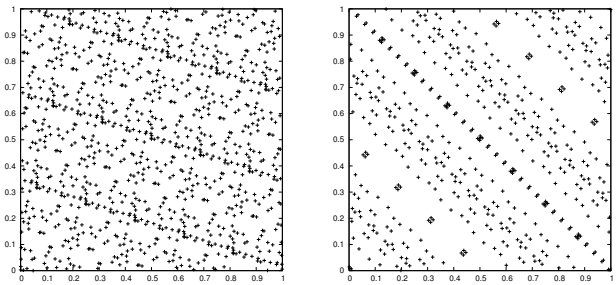
$$y_{i+1} = f_M^{QCG}(y_i) \equiv 8y_i^2 + 5y_i + 3(\mathrm{mod}\ M),$$
$$y_{i+1} = f_M^{ICG}(y_i) \equiv 9y_i^{-1} + 6(\mathrm{mod}\ M).$$

The distribution of the points of two-dimensional nets (1) with $M = 1024$ can be seen at Fig. 2. Table I contains the results for the $b-$adic diaphony of such two-dimensional nets.

IV. PSEUDO-RANDOMNESS OF THE COMBINATION OF THE VAN DER CORPUT SEQUENCE WITH QUADRATIC AND INVERSIVE CONGRUENTIAL GENERATORS

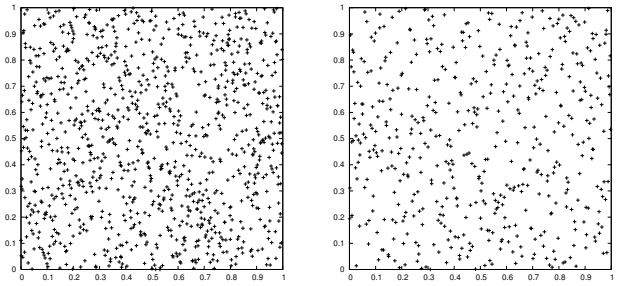
We consider the net

$$(\zeta_b(y_i), \zeta_b(y_{i+1})), i = 0, 1, \ldots, N-1. \tag{4}$$



QCG, $N = 1024$ ICG, $N = 512$

Fig. 2. The distribution of points of quadratic and inversive generators, $M = 1024$.



QCG, $N = 1024$ ICG, $N = 512$

Fig. 3. The distribution of points of the combination $\zeta_b(y_i)$ of quadratic and inversive generators with Van der Corput sequence with $M = 1024$, $b = 3$.

We compute the $b-$adic diaphony of the combination of the Van der Corput sequence ζ_b with quadratic and inversive generators, i.e. $y_{i+1} = f_M^{QCG}(y_i)$ and $y_{i+1} = f_M^{ICG}(y_i)$. The combination of the Van der Corput sequence with quadratic generator is proposed by Oto Strauch. We consider the combination of the Van der Corput sequence with inversive generator, too. In such way, the obtained nets have a better pseudo-random property than original sequences. The distribution of such nets for $M = 1024$ can be seen at Fig. 3. The obtained results for the $b-$adic diaphony of these combinations are presented in Table II. Fig. 4 shows a comparison between the computed $b-$adic diaphony of the nets (1) and (4) using two nonlinear generators.

TABLE II
THE DIAPHONY F_N OF THE COMBINATION OF THE VAN DER CORPUT SEQUENCE WITH QUADRATIC AND INVERSIVE GENERATORS, $b = 3$.

M	QCG	ICG
16	0.189215	0.310316
32	0.118721	0.161015
64	0.084152	0.155085
128	0.059790	0.084913
256	0.045328	0.075950
512	0.029762	0.063425
1024	0.022144	0.054596
2048	0.015634	0.036257
4096	0.010938	0.033067
8192	0.008214	0.019782
16384	0.005680	0.016421
32768	0.003888	0.010836
65536	0.002777	0.007971

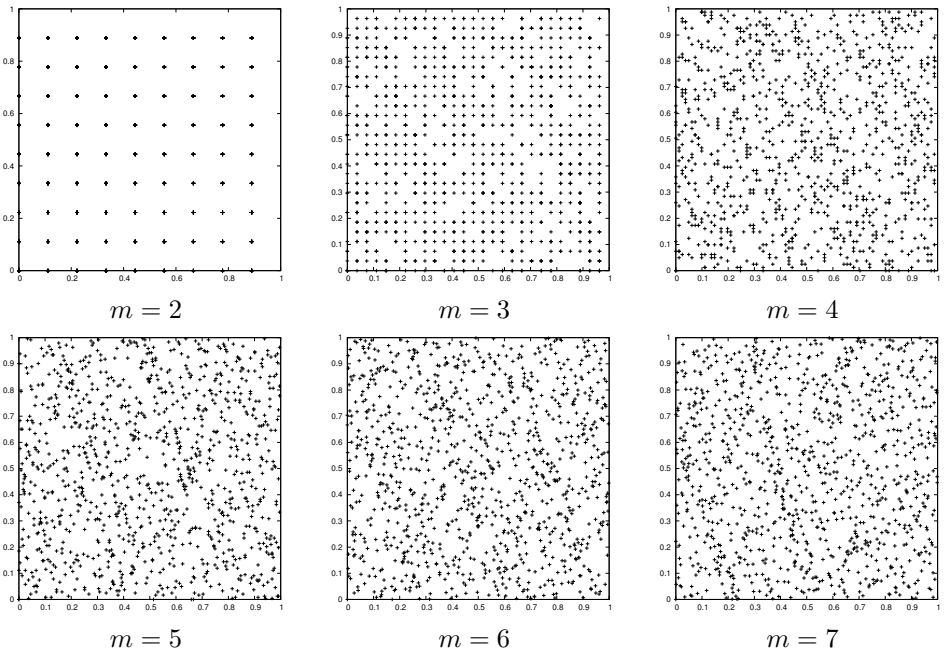


Fig. 5. The distribution of the simplification of the quadratic generator with $M = 1024$, $b = 3$.

TABLE III
THE DIAPHONY F_N OF THE NETS (6) WITH A QUADRATIC GENERATOR, $b = 3$, $M = 2^\mu$, $\mu = 4, \ldots, 16$.

M	F_N									
	m=2	m=3	m=4	m=5	m=6	m=7	m=8	m=9	m=10	m=11
16	0.20184	0.19245								
32	0.14672	0.12360	0.13709							
64	0.11102	0.09234	0.08944							
128	0.09456	0.06650	0.06661	0.06359						
256	0.08285	0.04829	0.04651	0.04376	0.04438					
512	0.07757	0.03722	0.03151	0.03000	0.03060					
1024	0.07392	0.03195	0.02310	0.02256	0.02162	0.02022				
2048	0.07248	0.02785	0.01767	0.01518	0.01543	0.01550				
4096	0.07163	0.02573	0.01368	0.01117	0.01094	0.01079	0.01157			
8192	0.07131	0.02478	0.01087	0.00824	0.00734	0.00836	0.00743	0.00728		
16384	0.07112	0.02408	0.00940	0.00620	0.00530	0.00559	0.00534	0.00560		
32768	0.07102	0.02380	0.00878	0.00479	0.00411	0.00387	0.00412	0.00407	0.00388	
65536	0.07097	0.02359	0.00823	0.00383	0.00293	0.00281	0.00275	0.00273	0.00287	0.00274

More detailed analysis of the results is presented in section VI.

V. SIMPLIFICATION

Let $m \geq 1$ be an arbitrary integer and $x \in [0, 1)$ then for the $b-$adic expression

$$x = 0.x_1 x_2 \ldots x_{m-1} x_m x_{m+1} \ldots$$

we define

$$\zeta^*_{b^m}(x) = 0.x_m x_{m-1} \ldots x_2 x_1.$$

In fact we truncate the $b-$adic expression of the number x to the m digits and we reverse the digits. O. Strauch proposed the net

$$\zeta^*_{b^m}\left(\frac{y_i}{M}\right), i = 0, 1, \ldots, N-1. \qquad (5)$$

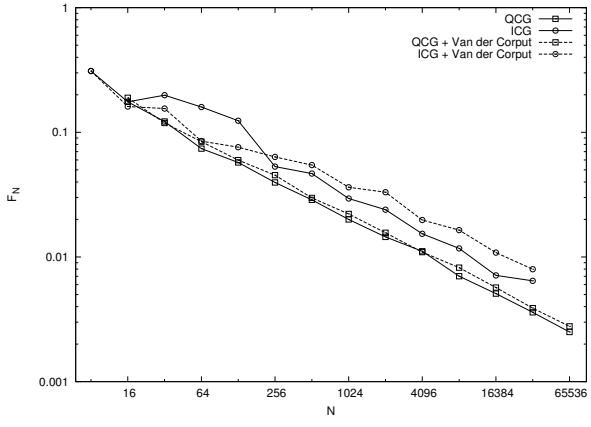


Fig. 4. The Diaphony F_N of the nets (1) and (4) with quadratic and inversive generators.

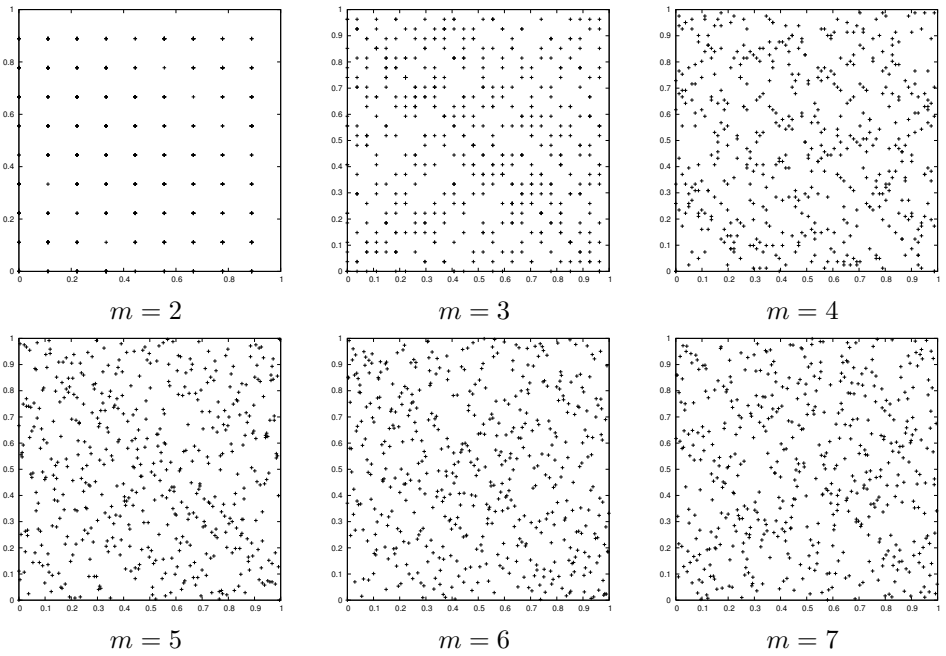


Fig. 6. The distribution of the simplification of the inversive generator with $M = 1024$, $b = 3$.

TABLE IV
THE DIAPHONY F_N OF THE NETS (6) WITH AN INVERSIVE GENERATOR, $b = 3$, $M = 2^\mu$, $\mu = 4, \ldots, 16$.

M	F_N									
	m=2	m=3	m=4	m=5	m=6	m=7	m=8	m=9	m=10	m=11
16	0.31032	0.31032								
32	0.16102	0.20387	0.16480							
64	0.19425	0.11520	0.14865							
128	0.11662	0.07514	0.11154	0.07343						
256	0.09570	0.10746	0.05317	0.05888	0.08200					
512	0.09331	0.07922	0.05841	0.04082	0.05530					
1024	0.08536	0.05432	0.02671	0.03312	0.05335	0.03935				
2048	0.07907	0.03706	0.02297	0.02626	0.02243	0.04587				
4096	0.07568	0.03023	0.01977	0.02686	0.02510	0.02545	0.01777			
8192	0.07359	0.02582	0.01783	0.01611	0.01029	0.01503	0.01139	0.01639		
16384	0.07252	0.02576	0.01542	0.01038	0.00661	0.01147	0.01323	0.00816		
32768	0.07146	0.02398	0.01180	0.00633	0.00556	0.01108	0.00838	0.00887	0.00451	
65536	0.07133	0.02411	0.01127	0.00576	0.00522	0.00577	0.00410	0.00723	0.00635	0.00369

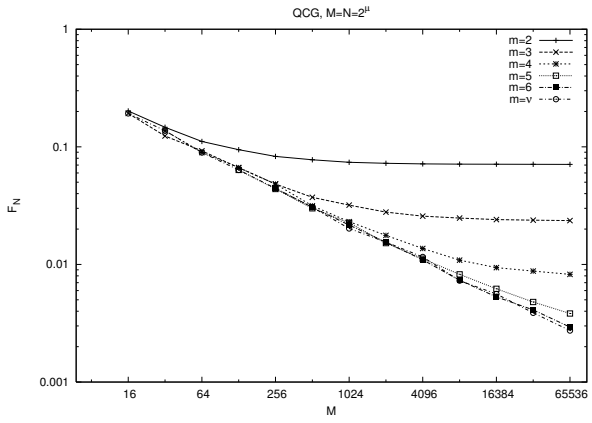


Fig. 7. The Diaphony F_N of the nets (6) with a quadratic generator.

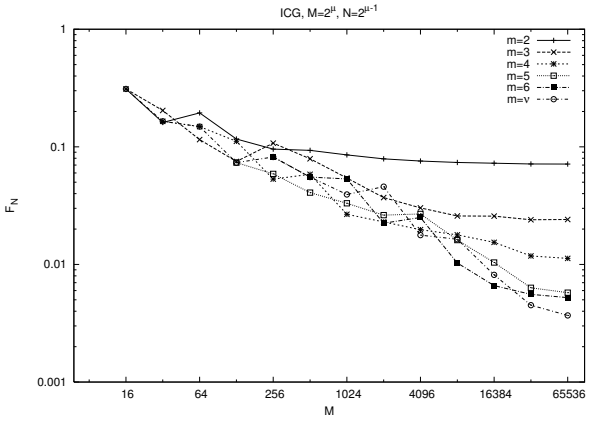


Fig. 8. The Diaphony F_N of the nets (6) with an inversive generator.

For pseudo-randomness of (5) we study the $b-$adic diaphony F_N of the two-dimensional net

$$\left(\zeta^*_{b^m}\left(\frac{y_i}{M}\right), \zeta^*_{b^m}\left(\frac{y_{i+1}}{M}\right)\right), i = 0, 1, \ldots, N-1. \quad (6)$$

Let ν be an integer such that $b^{\nu-1} < N \leq b^{\nu}$. For two-dimensional net with N points we choose $m = 2, \ldots, \nu$. The distribution of the points of the nets (6) for $M = 1024$ for six values of the number m is shown in Figs. 5 and 6. Tables III and IV as well as Figs. 7 and 8 show the computed $b-$adic diaphony of such nets using two nonlinear generators.

VI. Analysis of the Results

The results in Table I show that the $b-$adic diaphony of the two-dimensional net (1) tends to zero with the increase of the number of the points for both considered nonlinear generators. The $b-$adic diaphony has the same order for both generators. We will note a fact that for one and the same modulus the number of the points produced by an inversive generator is twice less than the number of the points from a quadratic generator. The fast convergence of the $b-$adic diaphony of the quadratic generator shows that it has better pseudo-random properties. In other words, this deterministic algorithm simulates better random number. The same conclusion can be made for the $b-$adic diaphony of the combination of the Van der Corput sequence with considered nonlinear generators. The comparison between Fig. 1 and Fig. 3 shows that the combination of the deterministic Van der Corput sequence with the nonlinear generators improves the distribution of two-dimensional net. Hence, the pseudo-random properties of the sequence $\zeta_b(y_i)$ are similar to the properties of the generators. Although the values of the $b-$adic diaphony of the combination are greater than the values of the $b-$adic diaphony of the generators, from the comparison between Tables I and II it is seen that the $b-$adic diaphony of the combination has a faster convergence to zero. The two-dimensional net (4) with the used nonlinear generators have better uniform distribution than (1), therefore, the combination $\zeta_b(y_i)$ has better pseudo-random properties than original sequences. Fig. 4 illustrates this fact.

The usage of the proposed simplification leads to a restriction of the number of the sequence points. This simplification maps the points produced by the generators to uniformly distributed nets with b^{2m} points in $[0, 1)^2$. Under too strong restriction, i.e. $m = 2$ or $m = 3$, the value of the $b-$adic diaphony of the net (6) for quadratic generator stays big independently of the increase of points number. It is true for inversive generator, too. However, for big m the behavior of the $b-$adic diaphony using both generators is different. This behavior for different restrictions $m = 2, 3, \ldots, 11$ can be seen in the last two tables and the last two figures. Comparing Fig. 7 and 8 we conclude that F_N of the simplification of the quadratic generator has faster convergence to zero. The diaphony F_N of the simplification of the inversive generator also tends to zero but for $N < b^{2m}$ there are some intervals where the distribution worsen and F_N increases.

VII. Conclusions and Future Work

In practice, different pseudo-random number generators are used depending on the application. A generator is good, if it has some properties as large period length, good uniform distribution qualities, lattice structure, efficiency, fast generation algorithm, repeatability, portability, unpredictability.

The combination of the Van der Corput sequence with nonlinear generators, in fact, is a new generator. This combination saves the properties of the generators. The obtained generators have the same period length as the original generators. The good uniform distribution qualities are shown on Fig. 3. Obviously, the new generators have lattice structure, efficiency, fast generation algorithm, reproduce exactly the same sequence on different computers and we can not predict the next generated value by the algorithm from the previous ones. In this way the combination of the Van der Corput sequence with quadratic and inversive generators is a good pseudo-random number generator.

The comparison between the combinations of the Van der Corput sequences with quadratic generator and inversive generator shows that the $b-$adic diaphony of the first combination tends to zero faster than $b-$adic diaphony of the second combination. It means that the first combination has better simulation of the pseudo-random numbers. On the other hand, the second combination has less points than the first combination, but the behavior of the $b-$adic diaphony for this combination is similar. The proposed simplification of quadratic and inversive generators can also be considered as a generator. Depending on the purpose of the application, the combination of the Van der Corput sequence with quadratic and inversive generators or proposed simplification can be used. The results show that the $b-$adic diaphony is a good tool to study pseudo-randomness of the sequences.

These research can be continued in several directions: from theoretical point of view — to find estimations of the $b-$adic diaphony of all considered generators; from the viewpoint of Monte Carlo and quasi-Monte Carlo applications — to find connection between the error of the numerical integration and the $b-$adic diaphony and to study applications of the considered generators in the area of the computer graphics for uniform sampling.

Acknowledgments

We would like to thank Prof. Oto Strauch for the wonderful ideas about the combination of the Van der Corput sequence with quadratic generator and the simplification of this combination. The study of pseudo-randomness of the proposed by Prof. Oto Strauch sequences is very interesting and useful for us. This work is supported by the project Bg-Sk-207, Bulgarian NSF.

References

[1] Blackburn, S. R., Gomes-Perez, D., Gutierrez, J., Shparlinski, I. E., Predicting Nonlinear Pseudorandom Number Generators, *Mathematics of Computation*, **74**, No 251, pp. 1471–1494, (2004).

[2] Blaževková, O., Strauch, O., Pseudo-randomness of quadratic generators, *Uniform distribution theory*, **2**, No 2, pp. 105–120, (2007).

[3] Dimov, I. T., Penzov, A. A., Stoilova, S. S., Parallel Monte Carlo, Sampling Scheme for Sphere and Hemisphere, *Lecture Notes in Computer Science*, **4310**, Springer, Berlin, Heidelberg, pp. 148–155, (2007).

[4] Drmota, M., Tichy, R. F., Sequences, Discrepancies and Applications, *Lecture Notes in Mathematics*, **1651**, Springer, Berlin, Heidelberg, (1997).

[5] Eichenauer-Herrmann, J., Inversive congruential pseudorandom numbers avoid the planes, *Mathematics of Computation*, **56**, No 193, pp. 297–301, (1991).

[6] Eichenauer-Herrmann, J., On the discrepancy of inversive congruential pseudorandom numbers with prime power modulus, *Manuscripta Mathematica*, **71**, pp. 153–161, (1991).

[7] Eichenauer-Herrmann, J., Emmerich, F., Compound Inversive Congruential Pseudorandom Numbers: An Average-Case Analysis, *Mathematics of Computation*, **65**, No 213, pp. 215–225, (1996).

[8] Eichenauer, J., Lehn, J., A non-linear congruential pseudorandom number generator, *Statist. Helfe*, **27**, pp. 315–326, (1986).

[9] Eichenauer, J., Grothe, H., Lehn, J., On the Period Length of Pseudorandom Vector Sequences Generated by Matrix Generators, *Mathematics of Computation*, **52**, No 185, pp. 145–148, (1989).

[10] Eichenauer, J., Lehn, J., Topuzoğlu, A., A Nonlinear Congruential Pseudorandom Number Generator with Power of Two Modulus, *Mathematics of Computation*, **51**, No 184, pp. 757–759, (1988).

[11] Eichenauer-Herrmann, J., Niederreiter, H., On the discrepancy of quadratic congruential pseudorandom numbers, *J. Comput. Appl. Math.*, **34**, No 2, pp. 243–249, (1991).

[12] Eichenauer-Herrmann, J., Niederreiter, H., An improved upper bound for the discrepancy of quadratic congruential pseudorandom numbers, *Acta Arithmetica*, **69**, No 2, pp. 193–198, (1995).

[13] Eichenauer-Herrmann, J., Niederreiter, H., Lower Bounds for the Discrepancy of Triples of Inversive Congruential Pseudorandom Numbers with Power of Two Modulus, *Monatshefte für Mathematik*, **125**, pp. 211–217, (1998).

[14] Grozdanov, V., Stoilova, S. The $b-$adic diaphony, *Rendiconti di Matematica*, **22**, pp. 203–221, (2002).

[15] Gutierrez, J., Niederreiter, H., Shparlinski, I. E., On the Multidimensional Distribution of Inversive Congruential Pseudorandom Numbers in Parts of the Period, *Monatshefte für Mathematik*, **129**, pp. 31–36, (2000).

[16] Hellekalek, P., Inversive Pseudorandom Generators: Concepts, Results and Links, *Proceedings of the* 27^{th} *conference on Winter simulation*, Arlington, Virginia, US, IEEE CS, Washington, DC, USA, pp. 255–262, (1995).

[17] Knuth, D. E., Seminumerical algorithms. The art of computer programming, **2**, 2nd edition, Addison Wesley, Reading, MA, (1981).

[18] Kuipers, L., Niederreiter, H., Uniform distribution of sequences, John Wiley, New York, (1974).

[19] L'Ecuyer, P., Uniform Random Number Generation, *Annals of Operations Research*, **53**, No 1, Springer-Verlag, pp. 77–120, (1994).

[20] Niederreiter, H., Quasi-Monte Carlo Methods and Pseudo-Random Numbers, *Buletin of the American Mathematical Society*, **84**, No 6, pp. 957–1041, (1978).

[21] Niederreiter, H., Random number generation and quasi-Monte Carlo methods, *CBMS-NSF Regional Conference Series in Applied Mathematics*, **63**, SIAM, Philadelphia, PA, (1992).

[22] Niederreiter, H., A Discrepancy Bound for the Hybrid Sequences Involving Digital Explicit Inversive Pseudorandom Numbers, *Uniform Distribution Theory*, **5**, No 1, pp. 53–63, (2010).

[23] Niederreiter, H., The Serial Test for Congruential Pseudorandom Numbers Generated by Inversions, *Mathematics of Computation*, **52**, No 185, pp. 135–144, (1989).

[24] Niederreiter, H., Lower Bounds for the Discrepancy of Inversive Congruential Pseudorandom Numbers, *Mathematics of Computation*, **55**, No 191, pp. 277–287, (1990).

[25] Niederreiter, H., Shparlinski, I. E., On the distribution of inversive congruential pseudorandom numbers in parts of the period, *Mathematics of Computation*, **70**, No 236, pp. 1569–1574, (2000).

[26] Niederreiter, H., Shparlinski, I. E., Exponential sums and the distribution of inversive congruential pseudorandom numbers with prime-power modulus, *Acta Arithmetica*, **XCII**, No 1, pp. 89–98, (2000).

[27] Niederreiter, H., Shparlinski, I. E., On the Distribution and Lattice Structure of Nonlinear Congruential Pseudorandom Numbers, *Finite Fields and Their Applications*, **5**, pp. 246–253, (1999).

[28] Niederreiter, H., Shparlinski, I. E., On the Distribution of Pseudorandom Numbers and Vectors Generated by Inversive Methods, *Applicable Algebra in Engineering, Communication and Computing*, **10**, Springer-Verlag, pp. 189–202, (2000).

[29] Strauch, O., Porubský, Š., Distribution of Sequences: A Sampler, Peter Lang, Frankfurt am Main, (2005).

[30] Weil, H., Über die Gleichverteilung von Zahlen mod. Eins., *Mathematische Annalen*, **77**, No 3, Springer, pp. 313–352, (1916).

[31] Pseudo-Random Number Generator, http://statmath.wu.ac.at/prng/