A Study of a New Class of Congruential Generators for Monte Carlo Methods

T. Gurov, S. Ivanovska, A. Karaivanova, N. Manev

Key words: *Monte Carlo methods; Pseudo Random Number Generators; multidimensional integratio; integral equations.*

Abstract. *In this paper we propose a new class of congruential pseudo random number generators based on sequences generating permutations and study Monte Carlo numerical methods for solving multidimensional integrals and integral equations based on them. These sequences have been developed for other applications but our analysis and experiments show that they are appropriate for approximation of multiple integrals and integral equations.*

Introduction

Monte Carlo Methods (MCMs) are based on the simulation of stochastic processes whose expected values are equal to computationally interesting quantities. MCMs offer simplicity of construction, and are often designed to mirror some process whose behaviour is understood only in a statistical sense. However, there are a wide class of problems where MCMs are the only known computational methods of solution. Despite the universality of MCMs, a serious drawback is their slow convergence, which is based on the $O(N^{-1/2})$ behaviour of the size of statistical sampling errors with N samples.

The MCMs are based on use of **p**seudo**r**andom **n**umbers (PRNs) which are constructed to mimic the behaviour of truly random numbers. If it is necessary, these variables are later transformed to random variables (vectors) with the desired distribution. The PRNs are scrutinized via batteries of statistical tests that check for statistical independence in a great variety of ways. In addition, these tests check for uniformity of distribution, but not with excessively stringent requirements. Thus, one can think of computational random numbers as either ones that possess considerable independence, namely the PRNs, or those that possess considerable uniformity – the quasirandom sequences.

Many studies show that the outcome of the simulation may be sensitive to the random generators being used, which means that obtaining unbiased estimates requires careful selection of the random generators. In this paper we propose and study a new class of congruential pseudo random number generators based on sequences generating permutations.

Real-valued random variables $\{u_j\}_{j=0}^{\infty}$ are i.i.d. $U(0, 1)$, if for all integers $i \geq 0$ and $t > 0$ the vectors $(u_i, u_{i+1}, \ldots, u_{i+t-1})$ are uniformly distributed over the t-dimensional hypercube $(0, 1)^t$.

Such sequences of random variables are generated by so called Pseudo Random Number Generators (PRNG). A short introduction to them is given in Section 2.

In Section 3 we describe in brief a new class of PRNGs based on a special linear recursions modulo prime power. These recursions have been originally constructed and studied in order to be applied to areas too far from stochastic simulations, but whose statistical properties have inspired (suggested to) us to test whether these recursions can be utilized by Monte Carlo methods.

The numerical experiments that we have carried out by using two generators from the proposed new class are: computing multidimensional integrals, and solving integral equations. They are described in Section 4. The obtained results are compared with the results of integrations based on using Mersenne Twister random number generator.

Preliminaries

The quality of pseudorandom numbers determines the success of the Monte Carlo computations. A lot of generators have been proposed and studied during the time (or in the past years). We start here with the following definition [6]:

Definition (L'Ecuyer) A PRNG is a structure (S, μ, f, U, g) where

- S is a finite set called **the state space**;
- μ is the probability distribution on S;
- $f : S \to S$ is a function called **transition function** starting with a given initial state s_0, which is selected according to the distribution μ, all elements of S are generated according to $s_i = f(s_{i-1})$.
- U is the **output space**;
- $g : S \to U$ is the **output function**: $u_i = g(s_i)$.

The above definition well (corresponds to) fits the PRNGs used in Monte Carlo simulations. In most such PRNGs we have

- $S = Z^k_m$, where is the ring of integers modulo m;
- The output set U is i.i.d. $U(0, 1)$ (or $U(0, 1)^t$);
- $u_i = s_i/m$.

To some extent, the quality requirements for PRNGs depend on applications to which they are applied. There are some properties that are relevant to (required by) any application. Such most important properties are listed below.

Efficiency

The generator has to be implementable by a deterministic polynomial-time algorithm, i.e., to run in time bounded by a polynomial of the length of the initial state. The implementation has to be realized by as few as possible arithmetical operations and use little memory.

Long period

The period T of the generator has to be a square, or sometimes a cube of the required number of points, that is, even for not heavy applications we need $T>10^{18}$.

Repeatability and Portability

These properties guarantee the ability exactly the same sequence of random numbers to be generated at different machines and at a different time. For the purposes of testing and development these properties are very important.

Uniformity and Independence

They are relevant to the ability to generate the i.i.d. $U(0, 1)$ sequence.

Ability "to skip ahead"

This property characterizes the ability of calculating u_k for large k without generating all values $u_0, u_1, \ldots, u_{k-1}$. It is a property important for parallel realizations.

Pseudorandomness

This is a very important characteristic for random number generators. Informally pseudorandomness means **"The generators output has to look random"**. This is quite vague statement and different trends in its understanding can be observed. Indeed there are three main approaches to formalization of pseudorandomness:

- **Probabilistic** (Shannon): Shannon's information theory considers perfect randomness as the extreme case and it is associated with a unique distribution, the uniform one.
- **Computational Complexity** (Kolmogorov, Chaitin, Solomonov): This approach is based on the Kolmogorov's computational complexity [5,9].
- **Computational Indistinguishability** (Blum, Goldwasser, Micali, Yao, Goldreich): A distribution is pseudorandom if no efficient procedure can distinguish it from the uniform distribution [2,3].

We will not enter into details since the discussion on such topics is far from the goals of this paper. Such considerations concern in higher degree cryptography. For Monte Carlo integration, for example, it is not so important if the next generated value is unpredictable. We refer the interested reader to the cited literature.

The most popular types of generators used in MCMs are:

- Linear congruential: $x_n=ax_{n-1}+c$(**mod** m)
- Shift register: $y_n=y_{n-s}+y_{n-r}$(**mod** 2); $r > s$
- Additive lagged-Fibonacci: $z_n=z_{n-s}+z_{n-r}$(**mod** 2^k); $r > s$
- Combined: $w_n = y_n + z_n$ (**mod** p)
- Multiplicative lagged-Fibonacci: $x_n=x_{n-s}x_{n-r}$(**mod** 2^k); $r> s$
- Implicit inversive congruential
- Explicit inversive congruential

As examples of often used generator we give the following PRNGs which are included in the GNU Library:

1) Fifth-order multiple recursive with period 10^{46}: $x_n=107374182x_{n-1}+104480x_{n-5}(mod\ 2^{31}-1)$.
2) Combined multiple recursive $z_n=x_n-y_n$(**mod** $2^{31}-1$), where x_n and y_n are 3rd order linear recurrent sequences modulo $2^{31}-1$ and 2145483479, respectively. Its period is $\approx 2^{185}$.
3) Generalized (lagged) Fibonacci: $y_n=y_{n-s}\theta\, y_{n-r}$, $r>s$, where θ is +, -, * modulo m, or xor. If θ is the addition modulo 2^k, then the period is $(2^r-1)2^{k-1}$.
4) Mersenne Twister generator. It is equi-distributed in 623 dimensions and has period $2^{19937}-110^{6000}$.

The last generator has recently become popular for simulation and it has been installed as the default PRNG for the most used mathematical packages. That is why we have chosen to compare our random number generator with the Mersenne Twister generator.

A New Class of Congruential Generators

Definition [10]. Let $\mathbf{S} = \{s_n\}_{n\geq 0}$ be a sequence with terms in a finite ring R. The sequence **S** is called **strictly balanced** (in short SB) **sequence**, if it is periodic and each element of R occurs equal number of times in one period of the sequence. If each element of R appears exactly once in a period, the sequence **S** is called **sequence generating permutation** (in short SGP).

The period of an SGP sequence is equal to the cardinality $|R|$ of the ring.

Both from algebraic and practical points of view, the most important case is $R = Z_{p^m}$.

Recall that k^{th}-*order homogeneous linear recurrence sequence*, $\mathbf{S} = \{s_n\}$, *with constant terms* in R is defined by the recursion

(1) $s_{n+k}=a_{k-1}s_{n+k-1}+a_{k-2}s_{n+k-2}+ \ldots +a_1s_1+a_0s_n$

and *initial terms* $s_0, s_1, \ldots, s_{k-1}$. It is obvious that any such sequence over a finite ring is periodic.

Theorem 1 [10]: Let $\{s_n\}$ be a second-order sequence defined by

(2) $s_{n+2}=as_{n+1}+bs_n$, (**mod** p^m).

It is an SGP sequence if and only if

(3) $\mu(x^2-ax-b)=(x-1)^2$,

where μ: $Z_{p^m}[x] \rightarrow Z_p[x]$ for $p>2$

and

μ: $Z_{2^m}[x] \rightarrow Z_4[x]$ for $p=2$.

In the case $p=3$ the condition $u+v\not\equiv 2 \pmod 3$, where $a=2+3u$, $b=-1+3v$, has to be added to (3) in order the theorem to be true.

The higher order case is more complicated and the necessary and sufficient condition cannot be formulated in a simple form. But if $f(x) = x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - \ldots - a_1x - a_0$ is the minimal polynomial of the recursion of order $k \geq 3$

with $M=p^m$, the following conditions are sufficient for generating an SGP sequence:

- $f(x) \equiv (x-1)^k \pmod p$
- $s_0, s_1, \ldots, s_{k-1}$ must be different modulo p, e.g., 0, 1, 2, … , k-1.

Using the Chinese Reminder Theorem we can construct an SGP sequence for any $M = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$.

Given an SGP sequence $\{s_n\}$ over Z_M we can transform it into a sequence of numbers in [0, 1) dividing each element by M. Hence the resulting sequence of M elements is a permutation of the numbers

(4) $\left\{ \frac{i}{M} \middle| i = 0,1,2,\ldots,M-1 \right\}$.

Consider the second-order sequence with terms in $\mathbf{Z}_M$, where $M=5^{19}$ defined by $s_{n+2}=(5^{10}+2)s_{n+1}-5556s_n$.

We start with $s_0=0$ and $s_1=1$ (or any $s_1 \equiv 1 \pmod 5$). Similarly, the coefficients $a_1=5^{10}+2$ and $a_0=-5556$ can be replaced with any $a_1 \equiv 2$, $a_0 \equiv -1 \pmod 5$.

Consider the third-order sequence with terms in $\mathbf{Z}_M$ $(M=2^{61})$ defined by

$$s_{n+3}=(2^{10}-1)s_{n+2}+(2^8+2^6+1)\, s_{n+1} + s_n \pmod{2^{61}}.$$

Any elements s_0, s_1, s_2 of $\mathbf{Z}_M$ such that $s_0 \equiv 0$, $s_1 \equiv 1$, $s_2 \equiv 2 \pmod 4$ are suitable for initial parameters. The coefficients a_2, a_1, a_0 can be replaced with any $a_2 \equiv -1$, $a_1 \equiv 1$, $a_0 \equiv 1 \pmod 4$ but they should be taken with large absolute values in order to improve the uniformity of the distribution of segments $(u_{n+1}, u_{n+2}, \ldots, u_{n+t})$.

Bellow some features which characterize the proposed class of PRNGs are listed:

- **Good lattice structure can be arranged**.

We can make the lower bound $\left(\sum_{i=0}^{k-1} a_i^2\right)^{-1/2}$ for the minimal distance between hyperplanes, d_t, sufficiently small by choosing large coefficients.

- **The generators modulo 2^m are very efficient**.

For instance, the implementation of Example 2 gives a two times faster generator than the Mersenne Twister. The generation is realized by shifting and addition and only in the last step of the algorithm a multiplication by $1/2^m$ is used.

- **There is no theoretical limit for the period**.

But in order to keep the advantage in speed and low complexity of the considered class of PRNGs the period should be less than 2^{128} in practical implementation. This is a relatively short period in comparison to the one of Mersenne Twister but enough long for many applications. Indeed we can lengthen the period without enlarging M by permitting the repetition of the elements of (4).

The proposed class of PRNGs is significantly different from algebraic point of view. In contrast to other congruential generators the minimal polynomial of each generator is a purely inseparable polynomial (this corresponds to purely inseparable extensions of the basic field).

Computational Experiments

A. Study Case 1: Monte Carlo integration

We have carried out our computational experiments with the following d-dimensional test integrals:

$$I_1 = \int_{(0,1)^d} F_1(x)dx \quad \text{and} \quad I_2 = \int_{(0,1)^d} F_2(x)dx$$

where $x = (x_1, x_2, \ldots, x_d)$ and

$$F_1(x) = \prod_{i=1}^{d} (x_i^3 + 0.75) \quad \text{and} \quad F_2(x) = \prod_{i=1}^{d} \left|4x_i - 2\right|.$$

The values of I_1 and I_2 are both equal to 1.

The first of these test functions is taken from Schmid and Uhl [13]. I_2 is known as Roos and Arnold's example and it is suggested as a test function by Owen [12].

It is straightforward to calculate the variances σ_1^2 and σ_2^2 of F_1 and F_2:

(5) $\sigma_1 = \sigma[F_1] = \sqrt{\left(\frac{121}{112}\right)^d - 1}$ and $\sigma_2 = \sigma[F_2] = \sqrt{\left(\frac{4}{3}\right)^d}$

In partial we have

d=10:	$\sigma_1 = 1.07984949546134$	$\sigma_2 = 4.09362023566092$
d=20:	$\sigma_1 = 1.92142671333385$	$\sigma_2 = 17.72954751823117$
d=30:	$\sigma_1 = 3.02703898016620$	$\sigma_2 = 74.82423185191648$

As it is well known the error of integration tends asymptotically to

$$e_N[F_i] \approx \frac{\sigma_i}{\sqrt{N}} \nu ,$$

where ν is a standard normal $N(0,1)$ random variable and σ_i is the square root of the variance of F_i.

Here are in brief the items we have tested in our experiments:

- Tested generators: *the Mersenne Twister, Example 1, and Example 2;*
- Dimensions: $d=10, 20, 30$.
- Number of points: $N=2^m$ where $m=10, 11, \ldots, 20$.
- 200 calculations have been done for each generator and for each pair (d, m). The presented value of the error is the average over these 200 calculations of the absolute values of the error for each pair (d, m).

The described experiments can be considered as a continuation of the research given in [1].

B. Obtained results

Two of the obtained results are graphically represented in *figure 1*. The term "asymptotic"' is used for the graph of $\sigma_i / \sqrt{N}$ $(N = 2^m)$. The experiments show that generators from the new class demonstrate modestly even better behaviour than the Mersenne Twister. The generators (Examples 1 and 2 and many others not described here)

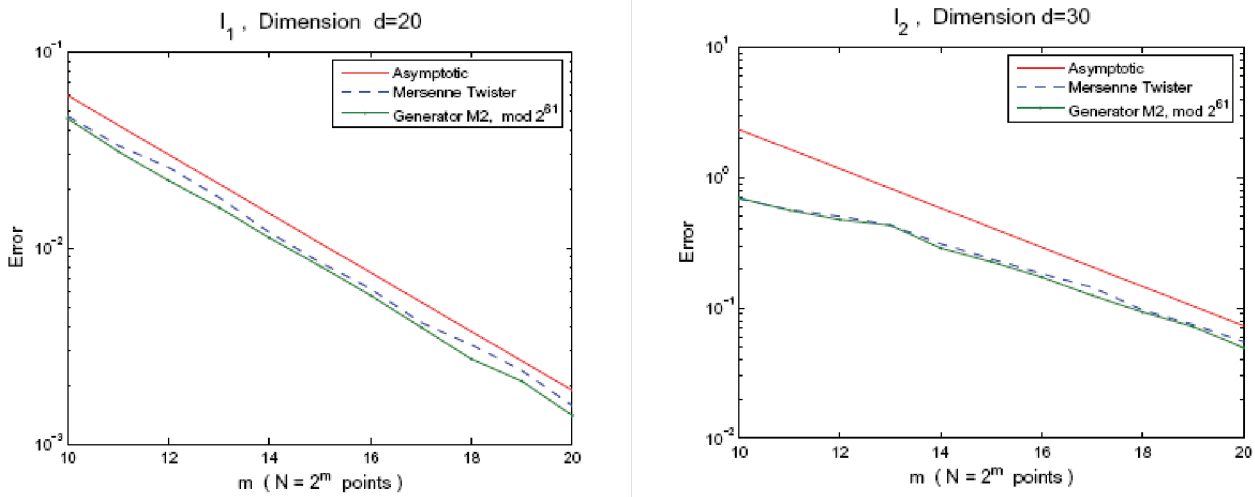

Figure 1. Graphical presentations of the experimental results

have been chosen at random. Hence we believe that their behaviour is intrinsic to all class.

C. Study Case 2: Simulation of Electron transport

As a second study case we consider the quantum kinetic equation describing a electron-phonon interactions in presence of applied electric field [11]. This equation can be written in the following integral form [11]:

$$f(k,t)=\phi(k)+\int_0^t dt''\int_G dk'K(k,k')\times$$

$$(6)\quad \left\{\int_{t''}^{t} dt'S_1(k,k',F,t',t'')f(k',t'')+\int_{t''}^{t} dt'S_2(k,k',F,t',t'')f(k',t'')\right\}$$

where the kernel is separated in two terms:

$$(7)\quad K(k,k')=\frac{2V}{2\pi^3\hbar^2}\left|g(q)^2\right|,$$

and

$$S_1(k,k',F,t',t'')=-S_2(k,k',F,t',t'')=\exp(-\Gamma(t'-t''))\times$$

$$\left[(n_q+1)\cos\left(\frac{\varepsilon(k)-\varepsilon(k')+\hbar\omega_q}{\hbar}(t'-t'')-\frac{\hbar}{2m}(k'-k)F(t'^2-t''^2\right)\right.$$

$$\left.+n_q\cos\left(\frac{\varepsilon(k)-\varepsilon(k')-\hbar\omega_q}{\hbar}(t'-t'')-\frac{\hbar}{2m}(k'-k)F(t'^2-t''^2\right)\right].$$

Here, k and t are the momentum and the evolution time, respectively. $f(k, t)$ is the distribution function. φ (k) is the initial electron distribution function. $F=eE/\hbar$, where E is the applied electric field. $n_q = 1/(\exp(\hbar\omega_q/KT)-1)$ is the Bose function, where K is the Boltzmann constant and T is the temperature of the crystal, that corresponds to an

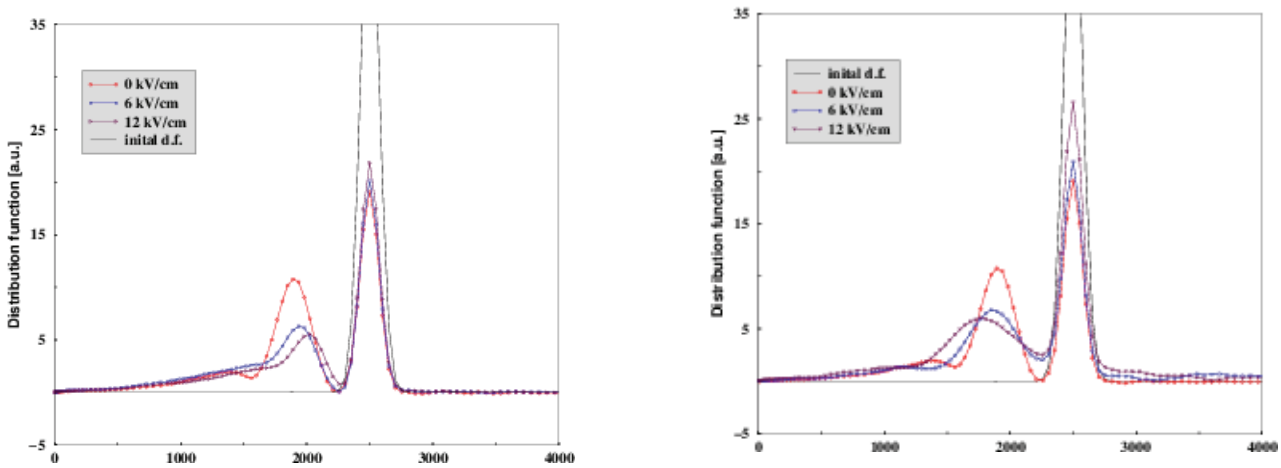

Figure 2. Solutions |k|f(0, 0, k_z, t) versus $|k|^2 10^{14} m^{-2}$, evolution time *t=200 fs* and at positive direction on the *z*-axis (left picture), and at negative direction on the *z*-axis (right picture). The electric field is 0, 6 kV/cm, and *12 kV/cm* and the number of random walks per point is 1 million

equilibrium distributed phonon bath. $\hbar\omega_q$ is the phonon energy which generally depends on $q=k'$-k, and $\varepsilon(k)=(\hbar^2k^2)/2m$ is the electron energy. A Fröhlich coupling is considered

$$g(q)=-i\left[\frac{2\pi e^2\hbar\omega_q}{V}\left(\frac{1}{\alpha_\infty}-\frac{1}{\alpha_s}\right)\frac{1}{q^2}\right]^{1/2}$$

where α_∞ and α_s are the optical and static dielectric constants. The damping factor Γ is considered independent of the electron states k and k'. This is reasonable since Γ weakly depends on k and k' for states in the energy region above the phonon threshold, where the majority of the electrons reside due to the action of the electric field. The solution of the quantum kinetic equation (6) is evaluated by a Monte Carlo algorithm suggested in [4] and using the generator described in *Example 2*.

The numerical tests have been performed on the High Performance cluster deployed at the Institute of Information and Communication Technologies of the Bulgarian Academy of Sciences (IICT-BAS). This cluster has the following hardware: HP Cluster Platform Express 7000 enclosures with 36 blades BL 280c with dual Intel Xeon X5560 @ 2.8 Ghz (total 576 cores), 24 GB RAM; 8 controlling nodes HP DL 380 G6 with dual Intel X5560 @ 2.8 Ghz, 32 GB RAM; non-blocking low-latency 20 Gpbs DDR interconnection via Voltaire Grid director 2004 switch; two SAN switches for redundant access to storage; and MSA2312fc with 96 TB SAN storage, available under /home and /gscratch filesystems.

The numerical results presented in the *figure 2* are obtained for zero temperature and *GaAs* material parameters: the electron effective mass is *0.063*, the optimal phonon energy is *36 meV*, the static and optical dielectric constants are α_s = 10.92 and α_∞=12.9. The initial condition at $t=0$ is given by a function which is Gaussian in energy, ($\varphi(k)=exp(-(b_1 k^2-b_2)^2)$, $b_1=96$ and $b_2=24$), scaled in a way to ensure, that the peak value is equal to unity.

A value $Q=66\times10^7 m^{-1}$ is chosen for a radius of the integration domain G. The solution $f(0, 0, k_z, t)$ is estimated in 2×96 points that are symmetrically located on z-axes, the direction of applied field. The truncation parameter ε= 0.001. The quantity presented on the y-axes in all *figures* is $|k|*f(0, 0, k_z, t)$, i.e. it is proportional to the distribution function multiplied by the density of states. It is given in arbitrary units. The quantity k^2, given on the x-axes in units of $10^{14}/m^2$, is proportional to the electron energy.

The numerical results show that this class of RNGs can be used to investigate the quantum kinetic equation under consideration.

Conclusion

The study of the consider class of PRNGs is at the initial stage but the obtained results encourage us to continue. We are looking for PRNGs in the proposed class that produced sequences of points that demonstrate high level of uniform distribution in high dimensional hypercubes. We cannot recommend yet concrete parameters (i.e., a concrete generators) since we have not enough knowledge about the discrepancy and lattice structure of the generated sequences. This is the subject of a further research.

Also, we are going to analyze the efficiency of generators modulo p^m, $p>2$, that are implemented by the Montgomery arithmetic.

Acknowledgments

This work was financially supported by the PRACE 2 IP, WP3, funded in part by the EUs 7th Framework Program (FP7 2007-2013) under grant agreement no. RI-211528 and FP7-261557. The work is achieved using the PRACE Research Infrastructure resources IBM Blue Gene/P computer located in Sofia, Bulgaria. This work was supported by DNS7FP-01/7 and in part by the European Commission under EU FP7 project HP-SEE (under contract number 261499).

References

1. Atanassov, E. et al. Quasi-Monte Carlo Integration on the Grid for Sensitivity Studies. – *Earth Sci. Inform.*, 3, 2010, 289-296.

2. Blum, M. and S. Micali. How to Generate Cryptographically Strong Sequences of Pseudo-Random Bits. – *SIAM J. Comput.*, 13 (4), November 1984, 850-864.

3. Oded, Goldreich. Pseudorandomness. – *Notices*, 46, Nov. 1999, No. 10, 1209-1216.

4. Gurov, T. V. and I. T. Dimov. A Parallel Monte Carlo Method for Electron Quantum Kinetic Equation. Lect. Notes in Comp. Sci., 2907, Springer-Verlag, 2004, 153-161.

5. Kolmogorov, A. N. Three Approaches to the Concept of the Amount of Information. – *Probl. Inf. Transm.*, 1, 1965, No. 1, 1-7.

6. L'Ecuyer, P. Uniform Random Number Generation. Annals of Operations Research, 53, 1994, 77-120.

7. L'Ecuyer, P. Uniform Random Number Generation. S. G. Henderson and B. L. Nelson, Editors. Simulation, Handbooks in Operations Research and Management Science. Amsterdam, The Netherlands, Elsevier, Chapter 3, 2006, 55-81.

8. L'Ecuyer, P. Pseudorandom Number Generators. Encyclopedia of Quantitative Finance. R. Cont, Ed., in Volume Simulation Methods in Financial Engineering, E. Platen and P. Jaeckel Eds., UK, Chichester, John Wiley, 2010, 1431-1437.

9. Li, M. and P. Vitanyi. An Introduction to Kolmogorov Complexity and its Applications. New York, Springer-Verlag, 1993.

10. Manev, N. L. Sequences Generating Permutations. – *Applied Mathematics and Computation*, Elsevier, 216, 2010, No. 3, 708-718.

11. Nedjalkov, M., T. V. Gurov, H. Kosina, and P. A. Whitlock. Statistical Algorithms for Simulation of Electron Quantum Kinetics in Semiconductors – Part II. Lect. Notes in Comp. Sci., 2179, Springer, 2001, 183-190.

12. Owen, A. The Dimension Distribution and Quadrature Test Functions. – *Stat Sin*, 13, 2003, 1-17.

13. Schmid, W., A. Uhl. Techniques for Parallel Quasi-Monte Carlo Integration with Digital Sequences and Associated Problems. – *Math. Comp. Sim.*, 55, 2001, 249-257.

Manuscript received on 5.10.2012

Todor Gurov *is an Associate Professor at IICT-BAS since 2004. In 1999, he received a PhD degree in comput. and appl. Math. His major research interests are: statistical modeling in semiconductors, parallel, HPC and grid computing. He specialized at ID-IMAG Inform. and Distrib. lab, Grenoble, France (1995) and at Edinburgh Parallel Computer Centre, UK (2002). He worked as a post-doctoral research associate at the Dep. of CIS, Brooklyn College-CUNY, USA, 1999/2001. Within the last 10 years he published more than 50 papers in peer reviewed conferences and journals. He has been involved in several European and National Projects working on ICT scientific developments. He leads the Bulgarian team in several FP6 and FP7 projects as SEEGRID-2, SEEGRID-SCI, and HP-SEE.*

Contacts:
Institute of Information and Communication Technologies – Bulgarian Academy of Sciences
Acad. G. Bonchev St., Bl. 25A
1113 Sofia, Bulgaria
e-mail: gurov@parallel.bas.bg

Sofiya Ivanovska *received a M.Sc. degree in Mathematics from the Faculty of Mathematics and Informatics, Sofia University "St. Kliment Ohridski", and a PhD degree from the Institute for Parallel Processing at Bulgarian Academy of Sciences. Her current position is Assistant Professor of the Department of GRID Technologies and Applications, Institute of Information and Communication Technologies, Bulgarian Academy of Sciences. Her research interests include Monte Carlo and quasi-Monte Carlo methods, parallel processing and grid technologies.*

Contacts:
Institute of Information and Communication Technologies – Bulgarian Academy of Sciences
Acad. G. Bonchev St., Bl. 25A, 1113 Sofia, Bulgaria
e-mail: sofia@parallel.bas.bg

Aneta Karaivanova *is a Professor at the IICT-BAS, Sofia, Bulgaria. She holds a PhD in Computer Science since 1997. In 1999 she was awarded with the 1st prize for Computer Science research. Her research interests include parallel algorithms, Monte Carlo and quasi-Monte Carlo methods, and computational linear algebra. She is an author of more than 70 scientific papers published in international journals and international conference proceedings. She spent more than 3 years as a guest researcher at Florida State University, USA. She had key position in many European and is a coordinator of various national R&D projects related to HPC.*

Contacts:
Institute of Information and Communication Technologies – Bulgarian Academy of Sciences
Acad. G. Bonchev St., Bl. 25A
1113 Sofia, Bulgaria
e-mail: anet@parallel.bas.bg

Nikolai Manev *received his M.Sc. in mathematics in 1977 from Sofia University and Ph.D. in 1984 from the Institute of Mathematics and Informatics of the Bulgarian Academy of Sciences. In 1977 he joined the Institute of Mathematics and Informatics of the Bulgarian Academy of Sciences as a Researcher. Since 1990 he is an Associate Professor in the same institute. Recently, he is also with the civil engineering university VSU "L. Karavelov", Sofia. His research interests are in coding theory, cryptography, number theory and the applications of grid computing technologies to these research areas.*

Contacts:
Institute of Mathematics and Informatics – Bulgarian Academy of Sciences
Acad. G. Bonchev St., Bl. 8
1113 Sofia, Bulgaria
e-mail: nlmanev@math.bas.bg