Fast K system generator of pseudorandom numbers

N.Z.Akopov,E.M.Madounts
Yerevan Physics Institute,375036 Yerevan,Armenia

A.B.Nersesian
Institute of Mathematics,375019 Yerevan,Armenia

G.K.Savvidy
Physics Department,University of Crete,71409 Iraklion,Greece
and
Institut für Theoretische Physik,D-6000 Frankfurt am Main, Germany

W.Greiner
Institut für Theoretische Physik, D-6000 Frankfurt am Main,Germany

Abstract

We suggest a new fast algorithm for the matrix generator of random numbers which has been earliar proposed in [1, 2]. This algorithm reduces N^2 operation of the matrix generator to $NlnN$ and essentially reduces the generation time. It also clarifies the algebraic structure of this type of K system generators.

In the articles [1, 2] the authors suggested the matrix generator of pseudorandom numbers based on Kolmogorov-Anosov K systems [3, 4]. This systems are the most stochastic systems, with nonzero entropy [3, 4, 5, 6, 7]. The properties of this new class of matrix generators were investigated with the criterion χ^2 and the discrepancy D_N in different dimensions. In all cases it shows very good statistical properties [2] (for another examples see also [8]). Matrix generators based on different ideas are proposed in [9, 10].

In the recent article [11] this matrix generator was tested in the Monte- Carlo simulations of the Ising model in one and two-dimensions where we have defined control of the calculations. The same simulation was carried out with the RANECU generator. As it was shown in this particular case the quality of those generators are nearly the same, but the speed of the matrix generator, which we will call MIXMAX, is slower than that of the RANECU generator. It take place because the number of operations of the MIXMAX generator is of order N^2, where N is the dimension of the matrix.

The aim of this article is to suggest a new fast algorithm, which reduces N^2 operations of MIXMAX to $N \ln N$ and allows to gain the generation time. It also clarifies the algebraic structure of this type of K system matrix generators.

The essence of the algorithm is that the almost *Toeplitz* structure of the matrix generator earliar proposed in [1, 2] rises up to *circulant*. The operations with the circulant matrix can be exchanged to the calculations with the diagonal matrix. The diagonalisation is performed by the direct and inverse discrete *Fourier* transformations and as it is well known, the fast *Fourier* transformation reduces N^2 operations to $N \ln N$. At this point the new algorithm accelerates the generation time.

Let us pass to the details of the algorithm. The matrix generator is defined as [1, 2],

$$X_{n+1} = A \cdot X_n, (mod\ 1), \tag{1}$$

where A is $N \times N$ dimensional matrix [2]

$$A = \begin{pmatrix} 2,3,4,......., N\ \ ,1 \\ 1,2,3,....., N-1,1 \\ 1,1,2,....., N-2,1 \\ .... \\ .... \\ 1,1,1,...,2,3,4,1 \\ 1,1,1,...,1,2,2,1 \\ 1,1,1,...,1,1,2,1 \\ 1,1,1,...,1,1,1,1 \end{pmatrix} \tag{2}$$

and X_0 is an initial vector, whose components must be irrational. For example $X_0^{(i)} = 1/\sqrt{\pi + i}$ and $i = 1,..,N$. The *trajectory* of the K system (1) $X_0, X_1, X_2....$ represents desired sequense of the random numbers [1]. This approach allows a large freedom in choosing of the matrices A for the K system generators and of the initial vectors [1].

Let's present the matrix (2) in the form $A = A_1 - A_2$, where

$$A_1 = \begin{pmatrix} 2,3,4,...,\ N\ ,N+1 \\ 1,2,3,...,N-1,\ N \\ 1,1,2,..,N-2,N-1 \\ .... \\ 1,1,1,...,1,2,3,4 \\ 1,1,1,...,1,1,2,3 \\ 1,1,1,...,1,1,1,2 \end{pmatrix}, A_2 = \begin{pmatrix} 0,0,0,...,0\ \ ,N \\ 0,0,0,...,0,N-1 \\ 0,0,0,...,0,N-2 \\ .... \\ 0,0,0,...,0,0,0,4 \\ 0,0,0,...,0,0,1,3 \\ 0,0,0,...,0,0,0,2 \\ 0,0,0,...,0,0,0,1 \end{pmatrix}. \tag{3}$$

So A_1 is Toeplitz matrix and A_2 is almost zero matrix. Let us extend the matrix A_1 up to *circulant* $\hat{A}_1$ of the dimension $2N \times 2N$

$$\hat{A}_1 = \begin{pmatrix} 2,3,4,...,\ N\ ,N+1,\ 1\ ,\ 1\ ,..,1 \\ 1,2,3,..,N-1,\ N\ ,N+1,\ 1\ ,..,1 \\ 1,1,2,..,N-2,N-1,N,N+1,..,1 \\ .... \\ .... \\ 5,6,7,...,1\ \ ,1\ \ ,1\ \ ,1\ \ ,..,4 \\ 4,5,6,...,1\ \ ,1\ \ ,1\ \ ,1\ \ ,..,3 \\ 3,4,5,..,N+1,1\ ,1\ ,1\ ,..,2 \end{pmatrix}. \tag{4}$$

The following matrices

$$S_1 = (E, 0), \qquad S_2 = \begin{pmatrix} E \\ 0 \end{pmatrix}, \tag{5}$$

where E is identity matrix of the dimension $N \times N$, S_1 is the matrix of the dimension $N \times 2N$ and S_2 has dimension $2N \times N$ allow to represent A_1 in the form

$$A_1 = S_1 \hat{A}_1 S_2.$$

Now the initial generator (1) can be written in the form,

$$X_{n+1} = (A_1\ X_n - A_2\ X_n), (mod\ 1), \tag{1a}$$

where

$$A_1\ X_n = S_1 \hat{A}_1 S_2\ X_n. \tag{6}$$

As it is known, the circulant matrix $\hat{A}_1$ can be represented in the form:

$$\hat{A}_1 = F^{-1} D F^1, \tag{7}$$

where D is a diagonal matrix, F^1 and F^{-1} are accordingly direct and inverse discrete Fourier transformations

$$F_{n,m} = \left(\frac{1}{\sqrt{2N}} exp\ \{\ \frac{2\pi i}{2N}(n-1)(m-1)\ \} \right)_{n,m=1}^{2N}, \tag{8a}$$

and

$$D = diag\,(D_1.....D_{2N})\,. \tag{8b}$$

Diagonal elements $D_1,..,D_{2N}$ of the matrix (4) are counted by the formula:

$$D_j = 2 + 3r_j + ... + Nr_j^{N-2} + (N+1)r_j^{N-1} + r_j^N + r_j^{N+1} + ... + r_j^{2N-1}, \tag{9}$$

where $r_j = exp(\ \frac{2\pi i}{2N}(j-1)\ ),\ j = 1,..,2N$. Taking into consideration the last equation we may get the following formulae:

$$D_1 = (N+5)N/2,$$

$$D_2 = -D_1,$$

$$D_j = \frac{(2+(-1)^{j-1})\ (1-(-1)^{j-1})}{(1-r_j)} + \frac{((-1)^{j-1}((N-1)r_j - N) + r_j)}{(r_j-1)^2}, \tag{10}$$

where $j = 3,..,2N$. Now the algorithm of the matrix generator is realized by the scheme:

$$X_{n+1} = (S_1\ F^{-1}\ D\ F\ S_2\ X_n + A_2\ X_n)\ \ (mod\ 1) \tag{1b}$$

The representation (1b) of the MIXMAX (1) completely solves the problem.

This algebraic approach makes clear that at the "heart" of the generator (1) [1, 2] is the *Toeplitz* matrix A_1 in (3). Indeed one can check that the determinant of A_1 is equal to one and the absolute values of all it's eigenvalues are different from one, therefore the matrix A_1 also represents equally good the K system generator

$$X_{n+1} = A_1\ X_n = S_1\ F^{-1}\ D\ F\ S_2\ X_n$$

In fact the algebraic structure of this K system generators become more transparant in the sense that as we have seen one can embed the *Toeplitz* matrix A_1 into the circulant of order $2N$ and decompose the last one into the sum of the powers of the *basic* permutation matrix,Ω

$$\hat{A}_1 = 2 + 3\Omega + 4\Omega^2 + ... + (N+1)\Omega^{N-1} + \Omega^N + \Omega^{N+1} + ... + \Omega^{2N-1}, \tag{9a}$$

where

$$\Omega = \begin{pmatrix} 0,1,0,.....,0 \\ 0,0,1,.....,0 \\ .... \\ .... \\ 0,0,0,.....,1 \\ 1,0,0,.....,0 \end{pmatrix}. \tag{11}$$

This also clearly demonstrates the fact that the growth of the matrix elements of the matrix A [1, 2] in (2) and A_1 in (3) in the vertical direction produces reach spectrum of eigenvalues (9), the additional condition which is necessary to produce

$many - scale$ mixing of the system and to ensure a slower growth of the discrepancy $D_N(A)$ [1].

It is also possible to modify the basic permutation matrix Ω in (11) to get a class of K system generators with very simple structure

$$A = \begin{pmatrix} 0, \ 1\ , \ 0\ ,....., \ 0 \\ 0, \ 0\ , \ 1\ ,....., \ 0 \\ .... \\ .... \\ 0, \ 0\ , \ 0\ ,....., \ 1 \\ (-1)^{N+1}, a_1, a_2, .., a_{N-1} \end{pmatrix}. \tag{12}$$

In the last case it is easy to compute the characteristic polynomial of A

$$\lambda^N - a_{N-1}\ \lambda^{N-1} - ... - a_1\ \lambda + 1 = 0 \tag{13}$$

and therefore it's eigenvalues $\lambda_1, ..., \lambda_N$

$$\lambda_1 \cdots \lambda_N = 1$$
$$...........$$
$$\lambda_1 + ... + \lambda_N = a_{N-1}. \tag{14}$$

This formulas allow to choose eigenvalues and then to construct matrix A for K system generators.

For example if N=4 and $a_1 = 0,\ a_2 = 3,\ and\ a_3 = 0$, then

$$\lambda_1 = \sqrt{\frac{3+\sqrt{5}}{2}},\ \lambda_2 = -\sqrt{\frac{3+\sqrt{5}}{2}},$$
$$\lambda_3 = \sqrt{\frac{3-\sqrt{5}}{2}},\ \lambda_4 = -\sqrt{\frac{3-\sqrt{5}}{2}}, \tag{15}$$

with an additional simplectic structure of A.

To convince that this algorithm produces the numbers of the same "quality" as before [2] we check this algorithm for the matrix of the size 128×128. Bellow we present numerical results which were obtained for MIXMAX generator (1) realized though the algorithm (1b) together with RANECU generator. We have considered χ^2_D criterion when $D = 1, .., 5$

$MIXMAX$	D	χ^2	$RANECU$	D	χ^2
	1	10.90		1	7.625
	2	88.89		2	96.7
	3	992.896		3	990.52
	4	9941.92		4	9976.64
	5	100012.0		5	100416.25

The programm which compares generation time of the MIXMAX and RANECU shows that they work nearly with the same speed.

In conclusion the authors would like to thank F.James for interest and H.Niederreiter for provision of [9, 10]. This work was supported in part by the Alexander von Humboldt Foundation.

References

[1] G.K.Savvidy,N.G.Ter-Arutyunian-Savvidy, On the Monte-Carlo Simulation of Physical Systems, Preprint EPI-865(16)-86, Yerevan Jun.1986 [Russian]; J.Comput.Phys. 97, 566 (1991).

[2] N.Z.Akopov,G.K.Savvidy,N.G.Ter-Arutyunian-Savvidy, Matrix Generator of Pseudorandom Numbers, Preprint EPI-867(18)-86, Yerevan Jun.1986 [Russian]; J.Comput.Phys.97, 573 (1991).

[3] A.N.Kolmogorov, Dokl.Akad.Nauk SSSR 119, 861 (1958) [Russian].

[4] D.V.Anosov, Geodezicheskiye Potoki na Zamknutych Rimanovych Mnogoobraziyach Otrizatelnoi Krivizny (Geodesic flows on closed Riemannian manifolds of negative curvature) (Nauka, Moscow, 1967) [Russian].

[5] I.P.Kornfeeld, S.V.Fomin, Ya.G.Sinai, Ergodic theory (Springer-Verlag, New York, 1982) (Engl.transl).

[6] G.K.Savvidy, Nucl.Phys.B246, 302 (1984).

[7] G.K.Savvidy.Phys.Lett.130B, 303 (1983).

[8] R.O.Abramyan, N.Z.Akopov, G.K.Savvidy, N.G.Ter-Arutyunian-Savvidy, Sinai Billiards as a Pseudorandom Number Generator, Preprint EPI-922(73)- 86, Yerevan 1986 [Russian]; G.A.Galperin, N.I.Chernov.Billiardi i Chaos. Matematika i Kibernetika 5, 10 (1991), (Znanie, Moskva, 1991),[Russian].

[9] H.Niederreiter. Math. Japonica 31, 759 (1986).

[10] H.Grothe. Zufallszahlen und Simulation (Teubner, Stuttgard, 1986); Statist. Papers 28, 233 (1987).

[11] N.Z.Akopov, E.M.Madunts, G.K.Savvidy, A new matrix generator for lattice simulation, in Proceedings of Computing in High Energy Physics'91 International Conference, pp.477-479 (Tsukuba, Japan, 1991).