New Elements in the Method of McLaren-Marsaglia

Dimitar Tyanev, Yulka Petkova, Antoniya Tyaneva

Abstract: *According to the analysis of the McLaren-Marsaglia's method for random sequences generation is established the possibility that the function which services the temporary buffer to be interpreted as a hash-function. As a result of this conclusion a new function of multiplicative type is suggested. There are described the results of the modified algorithm compared to the original one, based on Kolmogorov's criteria.*

1. INTRODUCTION

Computer modeling and Monte-Carlo's method are based on a chosen model of a basic random value (BRV), which approximates an one-dimensional standard law of distribution with the power density function

(1) $$P(x) = \begin{cases} 1, & x \in [0,1); \\ 0, & x \notin [0,1). \end{cases}$$

The quality of BRV computer model is determined first of all by the uniformity degree of generated numbers in every fraction $\{x_i\}$ with arbitrary size $i = \overline{1,n}$. This quality is providing by the period of generated sequence and the properly chosen initial values of the parameters in the algorithmic scheme, which realizes it.

It is known [1, 2 etc.], that the increasing of generated sequence is the condition, which is necessary for achieving the desirable quality, but it is not enough. That is the reason many existent models, for instance [3], lead to different results at the same applications [4].

2. CHOICE OF THE METHOD

The basic criteria to choose the model of BRV is the period of generated numeric sequence. In this respect one of the most proposed methods is the method of MacLaren-Marsaglia [5].

The method is based on two independent random sequences X : $\{x_i\}$ and Y : $\{y_i\}$. In the subsidiary buffer V there are stored k numbers from the sequence X. The outgoing sequence Z : $\{z_i\}$ obtains from the chosen elements of the subsidiary buffer, i.e.

(2) $$z_i := V[j].$$

The choice of the j-th element from the buffer V is accomplished by the following function:

(3) $$j = \lfloor k.y_i \rfloor.$$

Considering (1) and (3), it follows that

(4) $$j \in [0, k-1].$$

There are two schemes to substitute the current chosen element from the buffer V. According to the first one [1], it makes a direct substitution after the assuming

(5) $$V[j] := x_i \ ,$$

In this case the j-th element from the buffer V substitutes by the current number from the sequence X .

The second scheme [6] supposes substitution

(6) $$V[j] := x_{i+k}.$$

In this case the j-th element from the buffer V does not substitute by the current number, but it substitutes by the number, which the sequence X generates in k steps, i.e. x_{i+k}.

3. SUGGESTIONS

3.1. SUGGESTION A

The basic point in described method is dynamical changing of buffer V content. The random choice in reading and writing its element s is defined by the combining of two using algorithmic schemes qualities. The choice of the current element from the buffer is achieved by function (3), which behavior looks like a hash-function:

(7) $$h(R) = R \bmod \omega \ ,$$

where for *R* it can use integer number

(8) $$R = \lfloor (y_i)^{-1} \rfloor .$$

It is necessary to define the correct j for the every y_i. Because of that it follows:

(9) $$\omega = k \ .$$

Hash-function (7) is too elementary and its ability to “disperse” the choice of current element from the buffer V is limited. Because of that it is desirable to force its ability, which will positively reflected on the outgoing sequence Z. Thus, the multiplicative equation

(10) $$j = h(R) = (P.R) \bmod k \ ,$$

is to be suggested for the hash-function.

In this equation *P* is a properly chosen large and mutual prime number to k [7], [8].

3.2. SUGGESTION B

The described method doesn't have any preliminary requirements to the generators of sequences X and Y, included in its scheme. This is the reason of using generator suggested in [9] to realize the random sequence Y in the algorithmic scheme of McLaren-Marsagia's method. This algorithmic scheme uses an onedimentional array as a FIFO-buffer. The existence of this buffer originates the idea to use it by two algorithmic schemes together.

So, after this suggestion we can maintain that the buffer V in the method of McLaren-Marsaglia is a FIFO-buffer.

4. EXPERIMENTS

According to understanding that there are not criteria, which guarantees becoming absolutely random sequence, the estimation of random sequence is made only in the means of Kolmogorov’s statistical criteria [6].

We have realized two suggestions made before to generate random sequences using the method of McLaren-Marsaglia. Primary number used in realization is $P = 2147483647$. The behavior of suggested generator was compared to the generator of sequence X in the cases of fraction with different sizes, which vary from 500 to 1000000 numbers. The becoming estimations for the Kolmogorov’s criteria with the level of significant $\varepsilon_0 = 0{,}05$ for two fractions (respectively $K_{(3)}$ and $K_{(10)}$) were values, which satisfied

(11) $$K_{(3)} < K_{(10)},$$

for more than 70% of cases. This result gives us ground to affirm that the suggested function is positively reflected to the method.

It carried out a comparison of the schemes for the current element substitution. This comparison was carried out on the basis of estimation for such criteria. We can confidently point out that the scheme of substitution (6) is better than the scheme (5). But it is necessary to point out that the speed of generation by the scheme of substitution (6) is lower. It is because of missing k-1 numbers before number x_{i+k}.

REFERENCES:

[1]. Knuth D. E., *The Art of Computer Programming. Seminumerical Algorithms*, vol. 2, 2nd ed., 1981, Addison Wesley, Reading, MA.

[2]. Niederreiter H., *Random Number Generation and Quasi-Monte Carlo Methods*, SIAM, Philadelphia, PA, 1992.

[3]. Matsumoto M., Nishimura T., *Mersenn Twister: a 623-Dimensionally Equidistributed Uniform Pseudo-Random Number Generator*, ACM Transactions on Modeling and Computer Simulation, vol. 8, N 1, 1998, p. 3-30.

[4]. Tyanev D. S., *Random Vectors Computer Generating with Statistical Parameters Guarantee*, Journal of Electrotechnics and Electronics, vol. 5-6, 1999, p. 37-41.

[5]. MacLaren M. D., Marsaglia G., *Uniform Random Number Generators*, Journal of the Association for Computing Machinery, vol. 12, N 1, Jan. 1965.

[6]. Harin, Stepanova, *Practicum of Mathematical Statistics*, Minsk, University, 1987.

[7]. Knuth D. E., *The Art of Computer Programming. Seminumerical Algorithms*, vol. 3, 2nd ed., 1981, Addison Wesley, Reading, MA.

[8]. Graham R. L., Knuth D. E., Patashnik O., *Conckrete Mathematics – a Foundation for Computer Science*, 2nd ed., 1998, Addison Wesley, Reading.

[9]. Rabiner L. R., Gold B., *Theory and application of digital signal processing*, Prentice-Hall, 1975.

[10]. http://random.mat.sbg.ac.at/