Random number generators and their implementation and use

Veronika Stoffová

Department of Mathematics and Informatics, Trnava University in Trnava, Slovakia

veronika.stoffova@truni.sk, NikaStoffova@seznam.cz

The paper deals with random number generators (RNG) and their implementation on a computer. Most computer random numbers use pseudorandom generators (PRNGs) which are algorithms. The series of values generated by such algorithms is generally determined by a fixed number called a seed. One of the most common PRNG is the linear congruental generator which produces random numbers by recurrence function:

$$X_{n+1} = (a * X_n + b) \ mod \ m$$

Programming languages and programming environments use different pseudorandom number sequence generators, which are formed on the basis of congruental method or based on physical phenomena random nature of sampling.

Characteristics, properties and quality of the random number sequence determine the accuracy of numerical methods, which use them. Therefore, the RNG is paid increased attention in the computer modelling of dynamic systems. Presenting the random events of different nature it is also based on a random number generator with different distribution. Output values of the random generators are also used as an input of mathematical model of a dynamic system. The use of a random number sequence with uniform distribution in various numerical methods is also presented in this article.

References

[1] Mersenne Twiste: *A 623-Dimensionally Equidistributed Uniform Pseudo-Random Number Generator.* Nishimura, Makoto Matsumoto and Takuji. 1, January 1998, ACM Transactions on Modeling and Computer Simulation, Vol. 8.

[2] Gutterman, Z., Pinkas, B., Reinman, T. Analysis of the Linux Random Number Generator. [Online] March 2006. http://software.intel.com/sites/default/files/m/6/0/9/gpr06.pdf.

[3] CVE-2008-0166. *Common Vulnerabilities and Exposures.* [Online] January 9, 2008. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0166.

[4] Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised). [Online] January 2012. http://csrc.nist.gov/publications/nistpubs/800-90A/SP800-90A.pdf.

[5] https://software.intel.com/en-us/articles/intel-digital-random-number-generator-drng-software-implementation-guide

[6] Stoffová, V.: Metóda Monte Carlo na počítači. *XVIII. Mezinárodní vědecké kolokvium o řízení osvojovacího procesu.* Vyškov : Vysoká vojenská škola pozemního vojska vo Vyškově, 2000. s. 311-316.

[7] Stoffa, V.: Modelling and simulation as a recognising method in the education, Educational Media International 40 (2), 2004. Taylor and Francis, London