Three-dimensional generalization of the random point generator LFSR

A.N.Kalugin[1]
[1]*Samara State Aerospace University (SSAU)*

Abstract:

The paper considers a new method for generating pseudo-random sequences of points, which is a generalization of the Tausworth generator. The blocks of the sequence generated at the first stage of the basic scheme are interpreted as digits representing the element of the ring of algebraic integers in a cubic extension of the field of rational numbers using canonical number systems. Comparative results of using the generator for integration by the Monte Carlo method are presented.

Keywords: LFSR, three-dimensional generalization, pseudo-random sequences, Tausworth generator, Monte Carlo method

Acknowledgments: This work was financially supported by the Ministry of Education and Science of the Russian Federation, the Administration of the Samara Region, the US Civilian Research and Development Fund (CRDF Project SA-014-02) in the framework of the joint Russian-American program "Basic Research and Higher Education" (BHRE), as well as the Russian Foundation for Basic Research (grants No. 05-01-96501, 03-01-00736).

Citation: Kalugin AN. Three-dimensional generalization of the random point generator LFSR. Computer Optics 2005; 27: 131-134.

Access full text (in Russian)

References:

[1] L’Ecuyer P. Uniform random number generation. Ann Oper Res 1994; 53: 77-120. DOI: 10.1007/BF02136827.

[2] Knuth DE. The art of computer programming. Vol 2. Seminumerical algorithms. 2nd ed. Reading, Massachusetts: Addison-Wesley Pub (Sd); 1981. ISBN: 978-0-201-03822-4.

[3] Coddington P. Random number generators for parallel computers. Northeast Parallel Architectures Center, 1996. Source: □https://surface.syr.edu/npac/13□.

[4] Entacher K. Parallel streams of linear random numbers in the spectral test. ACM Trans Model Comput Simul 1999; 9(1): 31-44. DOI: 10.1145/301677.301682.

[5] Entacher K, Uhl A, Wegenkittl S. Parallel random number generation: Long-range correlations among multiple processors. In Book: Zinterhof P, Vajteršic M, Uhl A, eds. Parallel computation. Berlin, Heidelberg: Springer; 1999: 107-116. DOI: 10.1007/3-540-49164-3_11.

[6] Sirinvasan A, Ceperley D, Mascagni M. Random number generators for parallel applications. Adv Chem Phys 1999; 105: 13-36. DOI: 10.1002/9780470141649.CH2.

[7] Tausworthe RC. Random numbers generated by linear recurrence modulo two. Math Comput 1965; 19(90): 201-209. DOI: 10.1090/S0025-5718-1965-0184406-1.

[8] L’Ecuyer P. Maximally equidistributed combined Tausworthe generators. Math Comput 1996; 65(213): 203-213. DOI: 10.1090/S0025-5718-96-00696-5.

[9] Lidl R, Niederreiter H. Finite fields. Cambridge: Cambridge University Press; 1984. ISBN: 978-0-521-30240-1.

[10] Kátai I, Kovács B. Canonical number systems in imaginary quadratic fields. Acta Math Hung 1981; 37(1-3): 159-164. DOI: 10.1007/bf01904880.

[11] Thuswardner J. Elementary properties of canonical number systems in quadratic fields. In Book: Bergum GE, Philippou AN, Horadam AF, eds. Applications of Fibonacci numbers, Vol 7. Dordrecht: Springer; 1998: 405-415. DOI: 10.1007/978-94-011-5020-0_45.

[12] Kovács A. Generalized binary number systems. Annales Univ Sci Budapest Sect Comp 2001; 20: 195-206.

[13] Chernov VM. Fast uniform distribution of sequences for fractal sets. In Book: Wojciechowski K, Smolka B, Palus H, Kozera R, Skarbek W, Noakes L, eds. Computer Vision and Graphics. Computational Imaging and Vision, Vol 32. Dordrecht: Springer; (in print). DOI: 10.1007/1-4020-4179-9_102.

[14] Coddington P. Analysis of random number generators using Monte Carlo simulation. Int J Mod Phys C 1994; 5(03): 547-560. DOI: 10.1142/S0129183194000726.

[15] Korobov NM. Number-theoretic methods in approximate analysis [In Russian]. Moscow: "MCNMO" Publisher; 2004.

[16] Coddington P. Tests of random number generators using Ising model simulations. Int J Mod Phys 1996; 7(3): 295-303. DOI: 10.1142/S0129183196000235.