Modification of multidimensional pseudo-random sequences using dual LFSR-CNS generators

A.N. Kalugin [1,2]
[1] *Image Processing Systems Institute of RAS*
[2] *Samara State Aerospace University named after academician S.P. Korolev*

Abstract

The article considers a new method for modifying a multidimensional pseudo-random sequence of points based on the use of a pair of dual LFSR-CNS generators. The generator state restored on the basis of an element of the multidimensional sequence is interpreted as the state of the dual generator, which allows to generate a point that is different from the point of the initial sequence. Comparative results of the study of the initial and the modified sequence using the weighted spectral criterion are presented.

Keywords: LFSR-CNS generators, pseudo-random sequence, spectral criterion.

Citation: Kalugin AN. Modification of multidimensional pseudo-random sequences using dual LFSR-CNS generators. Computer Optics 2005; 28: 112-118.

Access full text (in Russian)

References

[1] Wolfram S. Random sequence generation by cellular automata. Adv Appl Math 1986; 7: 123.
[2] Kalugin AN. Three-dimensional generalization of the random point generator LFSR. Computer Optics 2005; 27: 131-134.
[3] Coddington P. Random number generators for parallel computers. NHSE Review. Issue 2. Northeast Parallel Architectures Center; 1996. Source: ⟨http://nhse.cs.rice.edu/NHSEreview/RNG⟩.
[4] Entacher K. Parallel streams of linear random numbers in the spectral test. ACM Trans Model Comput Simul 1999; 9(1): 31-44.
[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. New York: Springer; 1999: 107-116.
[6] Vattulainen I. Framework for testing random numbers in parallel calculations. Phys Rev E 1999; 59(6): 7200.
[7] Coddington P. Analysis of random number generators using Monte Carlo simulation. Int J Mod Phys C 1994; 5(3): 547-560.
[8] Coddington P. Tests of random number generators using Ising model simulations. Int J Mod Phys C 1996; 7(3): 295-303.
[9] Ferrenberg AM, Landau DP, Wong YJ. Monte Carlo simulations: Hidden errors from "good" Random number generators. Phys Rev Lett 1992; 69: 3382-3384.
[10] Golomb SW. Shift register sequence. San Francisco: Holden-Day; 1967.
[11] Gantmakher FR. The theory of Matrices. 2nd ed. Providence, Rhode Islands: American Mathematical Society; 1990. ISBN: 978-0-8218-1376-8.
[12] Kátai I, Kovács B. Canonical number systems in imaginary quadratic fields. Acta Mathematica Academiae Scientiarum Hungarica 1981; 37(1-3): 159-164.
[13] Kovács A. Generalized binary number systems. Annales Univ Sci Budapest, Sect Comp 2001; 20: 195-206.
[14] Chernov VM. Fast uniform distribution of sequences for fractal sets. Proceedings of International Conference on Computer Vision and Graphics 2004; (accepted for publication).
[15] Grunwald V. Intorno all'aritmetica dei sistemi numerici a base negativa con particolare riguardo al sistema numerico a base negativo-decimale per lo studio delle sue analogie coll'aritmetica ordinaria (decimale). Giornale di Matematiche di Battaglini 1885; 367: 203-221.
[16] Pawlak Z, Wakulicz A. Use of expansions with a negative basis in the arithmometer of a digital computer. Bulletin de l'Academie Polonaise des Scienses 1957; Classe III, 5: 233-236; Serie des Sciences Techniques 7 (1959), 713-721.
[16.1] Pawlak Z. An electronic digital computer based on the minus 2 system. Bulletin de l'Académie Polonaise des Sciences, Série des Sciences Techniques 1959; VII(12): 713-721.
[17] Hellekalk P, Niedderreiter H. The weighted spectral test: Diaphony. ACM Trans Model Comput Simul 1998; 8(1): 43-60.
[18] Ripley B. Stochasitc simulation. New York: John Wiley and Sons; 1987.
[19] Ireland K, Rosen M. A classical introduction to modern number theory. New York: Springer-Verlag; 1990.
[20] Zinterhof P. ÜbereinigeAbschätzungenbei der Approximation von Funktionen met Gleivhverteilundsmethoden. Sitzungsber Österr Akad Wiss Math-Natur 1976; Kl. II(185): 121-132.
[21] Fishman G, Moore L. An exhaustive analysis of multiplicative congruential random number generators with modulus 231-1. SIAM J Sci Comput 1986; 7: 24-45.
[22] Celmaster W, Moriarty KJM. A method for vectorized random number generators. J Comput Phys 1986; 64(1): 271-275.

Замечание: В п. 16 Литературы приведены данные по сразу 2м источникам, в References разделены пока на [16] и [16.1]. Возможно, лучше просто удалить [16.1]