The 8th International Conference "Distributed Computing and Grid-technologies in Science and Education" (GRID 2018)

Contribution ID: **240** Type: **Poster presentations**

Pseudo-random number generator based on neural network

Monday 10 September 2018 16:00 (1 hour)

Pseudorandom uniform distributed number generators are used in many fields of science and technology [1]. It is very important to test the quality of pseudo-random sequence produced by an algorithm. An overview of a large number of criteria for testing the quality of the sequence produced by pseudo-random generators can be found in the third chapter of [2], as well as in the article [3]. One of the most robust software packages that implements such tests is the DieHarder utility [4]. Among the algorithms that show good results when passing the entire set of DieHarder tests, the following three groups of algorithms should be mentioned.

- The Mersenne Twister (MT —Mersenne Twister) [5] gives a very qualitative sequence, but is relatively complex. It is currently used as default for many modern programming languages.
- Algorithms xorshift, xorshift+ and xorshift* [6] pass all sorts of tests from the DieHarder package on a level with Mersenne Twister, but algorithmically they are more simple than MT, although they have a slightly shorter period.
- The family of KISS algorithms [5] (Keep It Simple Stupid), whose name indicates the extreme simplicity, are almost as good as Mersenne Twister and even simpler then xorshift.

In this paper, we test our pseudo-random number generator based on the neural network, comparing it with the above algorithms. This comparison imposes strict requirements for the efficiency of the neural network, as each of these three algorithms has the potential for parallelization, requires for initialization from one to three initial seeds, uses only arithmetic and bitwise operations, and does not fail any DieHarder test, showing weak results in only 4 of them (of more than 100).

References

1. M.N. Gevorkyan, M. Hnatich, I.M. Gostev, A.V. Demidova, A.V. Korolkova, D.S. Kulyabov, L.A. Sevastianov, The Stochastic Processes Generation in OpenModelica, in: V.M. Vishnevskiy, K.E. Samouylov, D.V. Kozyrev (Eds.), DCCN 2016, Moscow, Russia, November 21-25, 2016, Revised Selected Papers, Springer International Publishing, 2016: pp. 538–552.
2. Knuth Donald E. The Art of Computer Programming, Volume 2 (3rd Ed.): Seminumerical Algorithms. —Boston, MA, USA : Addison-Wesley Longman Publishing Co., Inc., 1997.—Vol. 2.—ISBN: 0-201-89684-2
3. L'Ecuyer Pierre, Simard Richard. TestU01: A C library for empirical testing of random number generators // ACM Transactions on Mathematical Software (TOMS). —2007. —Vol. 33, no. 4. —P. 22
4. Brown Robert G., Eddelbuettel Dirk, Bauer David. Dieharder: A Random Number Test Suite. —2013. —Access mode: http://www.phy.duke.edu/~rgb/General/rand_rate.php .
5. Rose Greg. KISS: A Bit Too Simple. —2011. —Access mode: https://eprint.iacr.org/2011/007.pdf
6. Marsaglia George. Xorshift RNGs // Journal of Statistical Software. —2003. —Vol. 8, no. 1. —P. 1–6.

Author: Dr KULYABOV, Dmitry (PFUR & JINR)

Co-authors: Mrs DEMIDOVA, Anastasiya (RUDN University); KOROLKOVA, Anna (Peoples' Friendship University of Russia); Mr GEVORKYAN, Migran (PFU)

Presenter: Mr GEVORKYAN, Migran (PFU)

Session Classification: Poster Session