Torus random numbers generators

G. Makris, I. Antoniou

Mathematics Department, Aristotle University of Thessaloniki

We construct a class of mathematical models of random number generators based on chaotic Torus Automorphisms, called Torus-RNG. The proposed Torus-RNG are designed to have any desired entropy production and provide aperiodic sequences of non-negative integers of a given desired length that are uniformly distributed. The construction is based on our previous work on Torus Automorphisms [1], [2]. The Torus-RNG is a co-called linear RNG, satisfying all criteria proposed by Knuth [3], namely: 1) Randomness. The Torus-RNG has successfully passed the standard DIEHARD and NIST tests. 2) Long Period. The length of the random sequence is limited only by the maximal integer representable by the computer. This number depends of course on the processor and on the programming language. 3) Efficiency. As the memory requirements are limited to the bytes required to store the Torus-RNG parameters, the software runs very fast without any observable limitations. 4) Repeatability. The produced random sequence is the orbit of the seed, considered as an initial condition of the Torus Dynamical System. The seed may take any non-negative value smaller than the desired period. 5) Portability. The Torus-RNG can be implemented in any operating system and any programming language producing identical sequences. The Torus-RNG is a grid simulation of discretized Torus Automorphisms. The integer seed is inserted in the plane grid and transformed iteratively according to the selected Torus Automorphism. The product of the dimensions of the grid should be equal to the selected period. Although, the Torus Automorphisms act by definition on the unit square, we have transformed any rectangular grid to a square grid, in order to increase the parameters of the generators. The input parameters defining the Torus-RNG are the following: 1) The selected Period T. 2) The length m of the specific Random Sequence. 3) The three Torus parameters, selected independently are either three Integers, or two Integers and the desired Entropy Production. 4) The number of iterations of the Torus Automorphism. After fixing the Torus-RNG by specifying the input parameters, any selected seed defines a unique random sequence. The Torus-RNG is applicable to cryptography, steganography, simulation applications, gaming applications, statistical sampling, computer programming, numerical analysis, decision making.

[l] G. Makris, I. Antoniou, Chaotic Modeling **4**, 571 (2013).

[2] G. Makris, I. Antoniou, Chaotic Modeling **1**, 169 (2013).

[3] D.E. Knuth, the Art of Computer (1981).