The Additive Congruential Random Number (ACORN) Generator - pseudo-random sequences that are well distributed in k-dimensions.

Roy S Wikramaratna, REAMC Limited
University of Oxford Numerical Analysis Group Internal Seminar, 11th June 2019

Abstract. ACORN generators represent an approach to generating uniformly distributed pseudo-random numbers which is straightforward to implement for arbitrarily large order $k$ and modulus $M=2^{30t}$ (integer $t$). They give long period sequences which can be proven theoretically to approximate to uniformity in up to $k$ dimensions, while empirical statistical testing demonstrates that (with a few very simple constraints on the choice of parameters and the initialisation) the resulting sequences can be expected to pass all the current standard tests.

The standard TestU01 Crush and BigCrush Statistical Test Suites are used to demonstrate for ACORN generators with order $8 \leq k \leq 25$ that the statistical performance improves as the modulus increases from $2^{60}$ to $2^{120}$. With $M=2^{120}$ and $k \geq 9$, it appears that ACORN generators pass all the current TestU01 tests over a wide range of initialisations; results are presented that demonstrate the remarkable consistency of these results, and explore the limits of this behaviour.

This contrasts with corresponding results obtained for the widely-used Mersenne Twister MT19937 generator, which consistently failed on two of the tests in both the Crush and BigCrush test suites.

There are other pseudo-random number generators available which will also pass all the TestU01 tests. However, for the ACORN generators it is possible to go further: we assert that an ACORN generator might also be expected to pass any more demanding tests for $p$-dimensional uniformity that may be required in the future, simply by choosing the order $k>p$, the modulus $M=2^{30t}$ for sufficiently large $t$, together with any odd value for the seed and an arbitrary set of initial values. We note that there will be $M/2$ possible odd values for the seed, with each such choice of seed giving rise to a different $k$-th order ACORN sequence satisfying all the required tests.

This talk builds on and extends results presented at the recent discussion meeting on “Numerical algorithms for high-performance computational science” at the Royal Society London, 8-9 April 2019, see download link at bottom of web page [http://acorn.wikramaratna.org/references.html](http://acorn.wikramaratna.org/references.html).