Random number generation on FPGA-s

Tamás Herendi, Roland Major

University of Debrecen
herendi.tamas@inf.unideb.hu, major.sandor@inf.unideb.hu

Abstract

Linear recurring sequences over residue class rings can be basic components of particular pseudo random number generators. Finding such recurring sequences may be based on checking some well defined but computationally rather expensive properties of some related object.

Let a sequence $\{x_n\}_{n=0}^{\infty}$ of integers be a linear recurring sequence of order k. The coefficients of the sequence determine the corresponding characteristic polynomial and companion matrix.

In [1] sufficient condition is given for the uniform distribution of x_n modulo powers of 2. However, this requires the computation of the 2^kth power of the $k \times k$ companion matrix modulo 4. In [2] a highly parallel solution is presented, based on FPGA computation, which achieved a speedup factor of 200.

In the present work we provide a refined condition on the uniform distribution of linear recurring sequences. This condition requires the computation of high powers of a given polynomial reduced by the characteristic polynomial. Denoting the characteristic polynomial by $p(x)$, we have to find the smallest N, such that $x^N - 1$ is divisible by $p(x)$ modulo 2.

Based on this method a parallel solution is presented. This improved FPGA implementation allows for the computation of sequences with periods at least one order of magnitude larger. The presented work uses custom built hardware that contains multiple FPGA chips to further improve the scale of parallelism.

Keywords: random numbers, FPGAs

References

[1] T. Herendi: *Construction of uniformly distributed linear recurring sequences modulo powers of 2*, (to appear)

[2] T. Herendi, R.S. Major: *Modular exponentiation of matrices on FPGA-s*, Acta Univ. Sapientiae, Informatica, 3, 2 (2011) 172 - 191