

Field Programmable Gate Array Implementations of Cellular Automata for Pseudo-Random Number Generation

Jason C. Isaacs, Robert K. Watkins, and Simon Y. Foo

Department of Electrical and Computer Engineering
Florida A&M University
Tallahassee, FL 32310

isaacs@eng.fsu.edu, rwatkins@eng.fsu.edu, foo@eng.fsu.edu

Abstract — The consumption of random numbers is universal to computer-life simulations. Our research aims at evolving Ant Colony Systems (ACS) in reprogrammable hardware (specifically, an FPGA). In addition to moving the virtual ants, we require random numbers for virtual environments, and Monte Carlo simulations to provide input for various Genetic Algorithm (GA) fitness functions. As such, we have looked for compact and effective means of producing random numbers. Some cellular automata (CA) are especially well suited to this purpose. Since they are essentially Boolean logic operators, CA can be compactly implemented in hardware. In addition, some CA perform outstandingly as pseudo-random number generators (PRNG). Through experiments with several one- and 2-Dimensional CA, varying array size, connectivity, seeding methods, and cell geometries, we have identified several efficient means of producing CA PRNGs that perform exceptionally well compared to well-known PRNGs. After describing our implementations, we will report on their performance on standard statistical tests for randomness, and discuss tradeoffs between required hardware space and PRNG performance.