Chapter 6
Methods and Models for the Formation of Pseudo-Random Number Sequences Based on Cellular Automata

ABSTRACT

The chapter describes well-known models and implementation options for pseudorandom number generators based on cellular automata. Pseudorandom number generators based on synchronous and asynchronous cellular automata are briefly reviewed. Pseudorandom number generators based on one-dimensional and two-dimensional cellular automata, as well as using hybrid cellular automata, are described. New structures of pseudorandom number generators based on asynchronous cellular automata with a variable number of active cells are proposed. Testing of the proposed generators was carried out, which showed the high quality of the generators. Testing was conducted using graphical and statistical tests.

INTRODUCTION

The formation and obtaining of pseudorandom numbers is a necessary operation, which is widely used in various fields. The great need for pseudo-random number generators consists in the modeling of various dynamic processes. In other areas, the need for pseudo random number generators

DOI: 10.4018/978-1-7998-2649-1.ch006

(PRNG) has increased significantly. At the same time, there is a need for PRNG with specific properties for each problem. These properties satisfy his positive decision (Schneier, 1996; Marsaglia 2003). PRNG are implemented on the basis of various mathematical, hardware and software approaches. PRNG, which is implemented on the basis of cellular automata (CA), gained wide popularity and development. CA allow to implement a simple and understandable PRNG. Moreover, there are many paradigms that have a high quality pseudo-random bit sequence. Today, the properties of many CA have already been studied and methodological recommendations for building a PRNG based on CA of various configurations have been described (Bilan, 2017). The first generator that was implemented on the one-dimensional CA has been proposed by S. Wolfram (Wolfram, 1986). PRNGs, which are implemented on the hybrid CAs were considered in later works (Ruboi, et al 2004; Cattell, & Muzio, 1996). Hybrid cellular automata among a large number of identical cells contain cells that differ in their functional resources. Inhomogeneous cells can have different local logical functions, different neighborhoods, and other properties. The combination of rules for different CA cells are used in such generators. There were proposed some developed PRNGs, which are based on CA, that are implemented with usage of few CAs and additional generator. Such generators significantly improve the quality of work.. Additional generator is built on the linear feedback shift register (LFSR), as well as CA can be used to generate an additional sequence, for example, for LFSR bits (Suhinin, 2010a; Suhinin, 2010b; Hoe, et al 2012). Different approaches are used to analyze the properties of the PRNG. They are implemented as software products that are available in the Internet in appropriate sites (Walker, 2008; NIST Special Publications 800-22, 2001; NIST Special Publications 800-22, 2010; Marsaglia, 2003). They include such software as ENT, DIEHARD and NIST etc.

The paper analyzes three PRNGs based on the CA and there are the results of using NIST tests for analysis presented here. The more tests that are positive, the higher the quality of the generator. The most commonly used graphics tests are the DIEHARD and NIST tests.

This chapter discusses the use of ACA with a varying number of active cells for constructing pseudo-random number generators, with a large repetition period and high statistical properties.

Optimization-Based Data Science for an IoT Service Applicable in Smart Cities

Vinit Juneja, Sonakshi Singh, Vipin Jain, Kamal Kishor Pandey, Dharmesh Dhabliya, Ankur Guptaand Digvijay Pandey (2023). *Handbook of Research on Data-Driven Mathematical Modeling in Smart Cities (pp. 300-321).*
www.irma-international.org/chapter/optimization-based-data-science-for-an-iot-service-applicable-in-smart-cities/318826