Chapter 5

The Pseudorandom Number Generators Based on Cellular Automata With Inhomogeneous Cells

ABSTRACT

The fifth chapter deals with the use of hybrid cellular automata for constructing high-quality pseudo-random number generators. A hybrid cellular automaton consists of homogeneous cells and a small number of inhomogeneous cells. Inhomogeneous cells perform a local function that differs from local functions that homogeneous cells realize. The location of inhomogeneous cells and the main cell is chosen in advance. The output of the main cell is the output of a pseudo-random number generator. A hardware implementation of a pseudo-random number generator based on hybrid cellular automata is described. The local function that an inhomogeneous cell realizes is the majority function. The principles of constructing a pseudo-random number generator based on cellular automata with inhomogeneous neighborhoods are described. In such cellular automata, inhomogeneous cells have a neighborhood whose shape differs from that of neighborhoods of homogeneous cells.

DOI: 10.4018/978-1-5225-2773-2.ch005
THE METHOD AND MODELS OF PSEUDORANDOM NUMBER GENERATION BASED ON CELLULAR AUTOMATA WITH INHOMOGENEOUS CELLS

Generators considered above have a number of the structural disadvantages. These generators require the constant additional operations, which for the additional bits of formation are intended. In addition, generators use complex switching circuit for constant connection of the generator output to the output of the active ACA cells. Both generators have a large number of connections, which reduces the reliability of operation.

To eliminate these drawbacks and of increasing of the period of repeating pseudo-random sequence in the work the pseudorandom number generator that contains cellular automata with homogeneous and inhomogeneous cells, is investigated.

The homogeneous cells are called all cellular automata cells, which the same local transition function perform. Inhomogeneous cells are called cells, which perform a different function than local transition function of the homogeneous cells. At the same time an inhomogeneous cells is much less of the homogeneous cells. Such cellular automata else are called as hybrid cellular automata (HCA).

The locations of the cells, as well as their number are an important moment for the initial settings.

Such a pseudorandom number generator consists of one cellular automata. For the operation of the generator is initially being made the advanced settings.

1. The size of cellular automata is being selected.
2. The number of inhomogeneous cells are being selected and their location are being created.
3. The local transition function for homogeneous and inhomogeneous cells are being selected.
4. The cell, whose output is the output of the generator, is being selected.

After the initial settings, a generator starts to generate a pseudo-random bit sequence at the output of the selected cells. At each time step, the homogeneous cells perform local transition function for homogeneous cells and inhomogeneous cells will perform the local transition function for inhomogeneous cells.
Related Content

Privacy Preserving Principal Component Analysis Clustering for Distributed Heterogeneous Gene Expression Datasets
www.igi-global.com/article/privacy-preserving-principal-component-analysis/67529?camid=4v1a
Application of Meta-Heuristic Optimization Algorithms in Electric Power Systems
[www.igi-global.com/chapter/application-meta-heuristic-optimization-algorithms/69898?camid=4v1a](www.igi-global.com/chapter/application-meta-heuristic-optimization-algorithms/69898?camid=4v1a)

Medical Outcome Prediction for Intensive Care Unit Patients
[www.igi-global.com/chapter/medical-outcome-prediction-intensive-care/65162?camid=4v1a](www.igi-global.com/chapter/medical-outcome-prediction-intensive-care/65162?camid=4v1a)

Core-Based GRASP for Delay-Constrained Group Communications
[www.igi-global.com/article/core-based-grasp-for-delay-constrained-group-communications/101777?camid=4v1a](www.igi-global.com/article/core-based-grasp-for-delay-constrained-group-communications/101777?camid=4v1a)