国際シンポジウム第2日目 ポスターセッション2

Searching a maximum cycle length in pseudo-random numbers generated by cellular automata

Cong-Kha Pham*

There are many studies on generating pseudo-random numbers by cellular automata [2]-[5]. The first work is presented by Wolfram [1] in 1986, which exams the application of cellular automata into pseudo-random numbers generation. In which, rule CA30 is studied and cellular space is one-dimensional with $k = 2$ and $r = 1$, where k denotes the number of states per cell and r denotes the radius of a cell. This work demonstrated an ability to produce highly pseudo-random numbers by uniform cellular automata. In [2] and [3], a pseudo-random numbers generator using a non-uniform cellular automata was studied which consists two rules of CA90 and CA150. Evolutionary approaches for generating pseudo-random numbers are studied in [4] and [5]. In [5], a pseudo-random numbers generator has a non-uniform cellular automata with a combination of rules (CA90 and CA150) using a cellular programming is presented. All of the generated pseudo-random numbers resulted in [2]-[4] were at least at good as that of the results presented in [1].

A finite cellular automaton with size $N = 16$ has a total of 2^{16} possible states and each state has a possible maximum cycle length $\Pi_{16} = 2^{16}$ when this finite cellular automaton evolves to the successive time step over than $t = 2^{16}$. However, there has been no any discussion about an improvement on a maximum pseudo-random number of a maximum cycle length Π_N which can be generated better than the result presented in [1]. That is, the maximum cycle length Π_N found for a uniform cellular automata with rule CA30 in circular register of size $N = 16$ is 6016. If we can find a more longer maximum cycle length, this means we can generate a more greater pattern of the pseudo-random numbers.

In this work, a procedure for searching the maximum cycle length over than 6016 in the case of $N = 16$ is described. Rule CA30 is substituted with rule CA45 before the generated numbers become periodic in the future along with the successive time step t. As a result, the presented searching procedure is able to generate the pseudo-random numbers using uniform cellular automata which has rule CA30 with a stable maximum cycle length is 8595. The presented procedure also is effected for the other sizes N of cellular automaton in circular register.

* Department of Information Systems, Tokyo University of Information Sciences

References

[1] S. Wolfram, "Random Sequence Generation by Cellular Automata" ***Advances in Applied Mathematics***, 7, pp.123-169, June 1986.

[2] P.D.Hortensius, R.D. McLeod, W. Pries, D.M. Miller, and H.C.Card, "Cellular Automata based Pseudorandom Number Generator for Built-in-self-test" ***IEEE Trans. CAD***, Vol.8, No.8, pp.842-859, Aug.1989.

[3] P.D. Hortensius, R.D. McLeod, and H.C.Card, "Parallel Random Number Generation for VLSI Systems using Cellular Automata" ***IEEE Trans.Comp.***, Vol.38, No.10, pp.1466-1473, Oct.1989.

[4] J.R.Koza, "Genetic Programming" ***The MIT Press, Cambridge, Massachusetts***, 1996.

[5] M.Sipper, and M.Tomassini, "Generating Parallel Random Number Generators by Cellular Programming" ***Int. Journal of Modern Phys. C***,Vol.7, No.2, pp.181-190, 1996.