2007 International Symposium on Nonlinear Theory and its Applications
NOLTA'07, Vancouver, Canada, September 16-19, 2007

A Deterministic Cellular Array Model of Reaction-Diffusion Systems for Parallel Generation of Pseudo-Random I.I.D. Sequences

Shunsuke Soga, Hisato Fujisaka, Takeshi Kamio and Kazuhisa Haeiwa

Faculty of Information Sciences, Hiroshima City University
3-4-1 Ozuka-higashi, Asaminami-ku, Hiroshima 731-3194, Japan
Email: fujisaka@im.hiroshima-cu.ac.jp

Abstract—This paper presents a deterministic cellular array model of reaction-diffusion systems for parallel generation of pseudorandom binary i.i.d. sequences. As diffusion systems contain the Brownian particles, the cellular array contains virtual molecules which move like simple random walkers with their composition changed. Then, the direction which the virtual molecules move in will be i.i.d. Numerical experiments show that the pseudorandom i.i.d. sequences generated from the cellular array possess almost the same statistical properties as truly random binary i.i.d. sequences.

1. Introduction

Binary pseudorandom sequences which play important roles in communication and information processing fields are generated in various ways. Algebraic methods which employ linear feedback shift registers [1] are most widely applied in the fields. Chaotic methods using discretized piecewise linear maps [2] can generate not only independently and identically distributed (i.i.d.) sequences but also Markovian sequences. A method using cellular array models of probabilistic physical systems [3] is also proposed to generate Markovian sequences. In this paper, we will build a deterministic cellular array model of reaction-diffusion systems for parallel generation of pseudorandom binary i.i.d. sequences. As diffusion systems contain the Brownian particles, the cellular array contains virtual molecules which behave like simple random walkers. Then, the direction which the particles move in will be i.i.d. In Sections 2, we will introduce the cellular array. In Section 3, we will investigate the statistics of the sequences generated from the array.

2. Cellular Array

2.1. Diffusion Cellular Array

We first present a cellular array model of diffusion systems without reaction between their ingredients [4]. Figure 1 shows a one-dimensional cellular array model. We assume in the array pseudo-Brownian particles each of which carries a truth variable taking "1" or "0" and moves from a cell to one of its adjacent cells for one time step. The cells in the array are switches which take parallel or cross connection between two inputs a_l, a_r and two outputs u_l, u_r. Suppose that a particle which goes out from u_r of $Cell_{i-1}$ enters to a_l of $Cell_i$. When the internal connection of $Cell_i$ is parallel, the particle changes its direction and goes back to $Cell_{i-1}$. When the connection is cross, the particle keeps its direction and moves to $Cell_{i+1}$. The internal connection of each cell is determined by a logic function F,

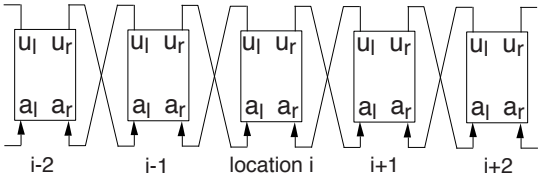

Figure 1: A diffusion cellular array.

$$\text{Parallel}/\overline{\text{Cross}} = F(a_l, a_r, q) \tag{1}$$

where a_l and a_r are the truth variables of two particles which enter the cell and $q \in \{1, 0\}$ is an internal state of the cell. A logic function F_q determines the state at each time step,

$$q \leftarrow F_q(a_l, a_r, q) \tag{2}$$

If the probabilities that the internal connection is parallel and cross are even, that is

$$\text{Prob}(F = 1) = \text{Prob}(F = 0) = 0.5 \tag{3}$$

a particle in a cell moves to its left and right adjacent cells at even probabilities. Then, we regard all the pseudo-Brownian particles in the array as simple random walkers.

The sequence of the direction of a simple random walker is ideally a binary i.i.d. sequence. We once expected that pseudorandom i.i.d. sequences of fine quality would be obtained by the cellular array model of diffusion systems. However, unfortunately, we saw a small difference between the statistical properties of the sequences obtained by the diffusion cellular array and truly random binary i.i.d. sequences.

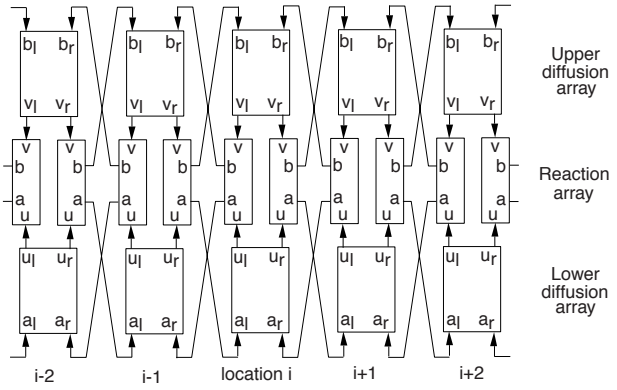

Figure 2: A reaction-diffusion cellular array.

2.2. Reaction-Diffusion Cellular Array

We introduce reaction cells and construct a cellular array model of reaction-diffusion systems. The reaction cells change the truth variables which the particles in the cellular array model of diffusion systems possess. Then, we expect to see very randomized motion of the particles in the cellular array model of reaction-diffusion systems.

We construct a three-layer cellular array as shown in Fig. 2. The cellular array executes simplified microscopic simulation of diffusion and the following chemical reaction.

$$A \rightleftharpoons B + C \tag{4}$$

The upper and the lower layers are the diffusion arrays introduced in the previous subsection. The inputs and the outputs of the cells in the upper array are denoted by b_l, b_r, v_l, and v_r. Cells for reaction (4) form the middle layer. The pseudo-Brownian particles possessing truth values "1"s and "0"s in the lower diffusion array represent molecules A and C. The pseudo-Brownian particles possessing truth values "1"s in the upper diffusion array represent molecules B. We assume in the upper diffusion array that there exists no molecule (which we call molecule ϕ) at the locations which particles possessing truth values "0"s occupy. The internal connections of the lower and the upper diffusion cells are always different. Then, the connections in the upper cells are determined by

$$\text{Parallel}/\overline{\text{Cross}} = \overline{F(a_l, a_r, q)} \tag{5}$$

Reaction cells simulate the chemical reaction given by Eq. (4). Each reaction cell has two inputs u,v, two outputs a,b and one internal state e. They all take truth values "1"s and "0"s. The cell operation rule is described by three logic functions G_a, G_b, and G_e,

$$a \leftarrow G_a(u, v, e) \tag{6}$$
$$b \leftarrow G_b(u, v, e) \tag{7}$$
$$e \leftarrow G_e(u, v, e) \tag{8}$$

The inputs and the outputs are connected to the outputs and the inputs of diffusion cells, as shown in Fig. 2. Input u takes the value that a particle at the output of the lower diffusion cell has, that is, u=1 if the particle is molecule A, u=0 if the particle is molecule C. Input v takes the value that a particle at the output of the upper diffusion cell has, that is, v=1 if the particle is molecule B, v=0 if the particle is molecule ϕ. If output a=G_a=1, a molecule at the output of the lower diffusion cell is changed to (or kept as) A. If a=0, the molecule is changed to (or kept as) C. Then, the molecule returns to the lower diffusion array. If output b=G_b=1, a molecule at the output of the upper diffusion cell is changed to (or kept as) molecule B. If b=0, the molecule is changed to (or kept as) molecule ϕ. Then, it returns to the upper diffusion array. The internal state e represents whether or not the molecules entered in the reaction cell have kinetic energy greater than activation energy. If e=1, reaction (4) occurs in the cell. Two reaction cells receive molecules from the same upper and lower diffusion cells. Let the internal states of the left and right reaction cells of the pair be e_l and e_r. Before the reaction cells operate according to Eqs. (6), (7) and (8), e_l and e_r may be exchanged. The exchange also depends on the logic function F which determines internal connections of the diffusion cells. The exchange rule is expressed by:

$$e_l \leftarrow Fe_l + \overline{F}e_r \tag{9}$$
$$e_r \leftarrow \overline{F}e_l + Fe_r \tag{10}$$

The reaction-diffusion system modeled by the three-layer cellular array is a materially closed system because the reaction cells conserve the total number of molecules A and B, and the total number of molecules A and C. Let the expectation of the number of molecules A in $Cell_i$ at time n be denoted by $w_i(n)$. From the operations of the diffusion and the reaction cells, we can derive the following equation:

$$\begin{aligned} &\frac{w_i(n+2) - w_i(n)}{2} \\ &= D\{(w_{i+1}(n) - w_i(n)) - (w_i(n) - w_{i-1}(n))\} \\ &+ kw_i(n) \end{aligned} \tag{11}$$

where D=1/32 and k=−3/8. Equation (11) corresponds to a difference equation obtained by the discretization of the following linear partial differential equation:

$$\frac{\partial w}{\partial t} = D\frac{\partial^2 w}{\partial x^2} - kw \tag{12}$$

The first and the second terms of the right hand side represent diffusion and reaction respectively. Diffusion coefficient D depends on the logic functions F and F_q. If Prob($F = 1$)≠1/2, coefficient D is smaller than 1/32 and an advection term is added to Eq. (12). Reaction speed k depends on the logic functions G_a, G_b, and G_e.

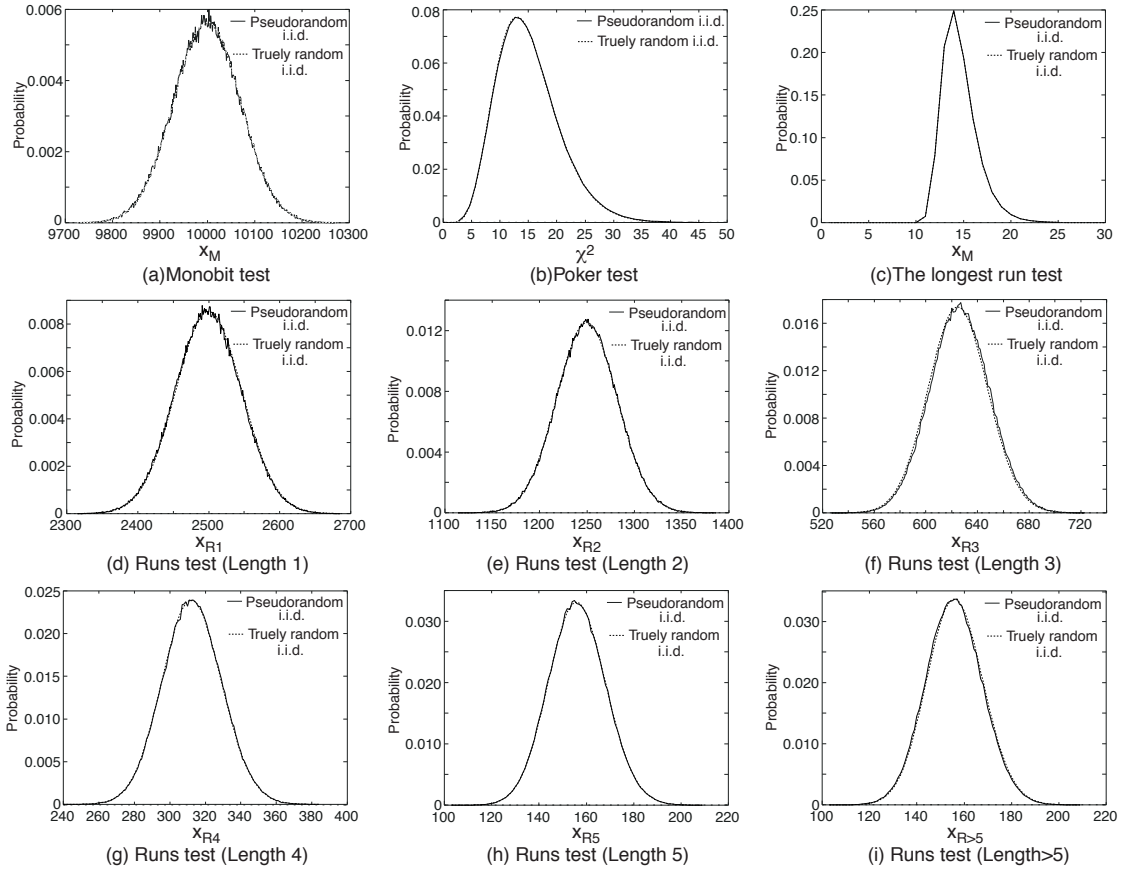

Figure 3: Probability distributions.

3. Numerical Experiments

In this section, we investigate the statistical properties of the sequences generated by a reaction-diffusion cellular array model. The specifications on the reaction-diffusion cellular array model are as follows: Both the upper and lower diffusion cellular arrays have (N=)19 diffusion cells and ($2N$=) 38 molecules. Then the number of the cells required to form the reaction layer is 38. Boundary conditions for the two diffusion cellular arrays are periodic, that is, the two arrays are circular. Logic functions which determine the operation of the diffusion cells are given by

$$F(a_l, a_r, q) = a_l \oplus a_r \oplus q \quad (13)$$

$$F_q(a_l, a_r, q) = \overline{a_l} \oplus q \quad (14)$$

Logic functions which determine the operation of the reaction cells are given by

$$G_a(u, v, e) = u\overline{e} + \overline{v}e \quad (15)$$

$$G_b(u, v, e) = \overline{u}e + v\overline{e} \quad (16)$$

$$G_e(u, v, e) = \overline{u \oplus v \oplus e} \quad (17)$$

Pseudorandom i.i.d. sequences to be examined are the sequences of the directions $d(n)$ which molecules in the lower diffusion cellular array move in. If the internal connection of $Cell_i$ is parallel at time n, a molecule which enters to $Cell_i$ from input a_l goes out from output u_l and moves to $Cell_{i-1}$. Then, $d(n)$=-1. If the connection is cross, the molecule moves to $Cell_{i+1}$. Then, $d(n)$=$+1$. From time n=n_0+1, n_0=10^7, we acquire sequences of length 2×10^6, $\{d(n_0+1), \cdots d(n_0+2\times10^6)\}$ by tracking the motion of molecules moving in the array which is given an initial condition at time n=0. (From time n=0 to n_0 we discard the sequences.) We can obtain ($2N$=)38 sequences in parallel for one initial condition. We acquire $100\times2N$ sequences for (M=)100 different initial conditions. We divide each sequence into (L=)100 subsequences of length 2×10^4. Then, we obtain totally ($L\times M\times 2N$=)380,000 subsequences. We use them for samples to investigate the statistical properties.

We also acquire sequences from cellular automata whose behavior is governed by the following iteration called $Rule30$ [5]:

$$c_i(n+1) \leftarrow c_{i-1}(n) \oplus c_i(n) \oplus c_{i+1}(n) \oplus c_i(n)c_{i+1}(n) \quad (18)$$

where $c_i(n)$ denotes the state of a cell at location i, i=0, 1, $\cdots$, 37, at time n. We compare the se-

Table 1: Probabilities that x_M, χ^2, x_Rj, x_L are out of the pass ranges.

Test	Pass range	Truly random binary i.i.d.	Reaction-diffusion cellular array	Cellular automata (Rule30)
Monobit test	$9725 < x_M < 10275$	10^{-4}	1.06×10^{-4}	1.97×10^{-4}
Poker test	$2.16 < \chi^2 < 46.17$	10^{-4}	9.21×10^{-5}	3.82×10^{-4}
Runs test				
Length 1	$2314 < x_{R1} < 2686$	7.36×10^{-5}	6.32×10^{-5}	5.00×10^{-5}
Length 2	$1113 < x_{R2} < 1387$	1.88×10^{-5}	1.58×10^{-5}	2.08×10^{-4}
Length 3	$526 < x_{R3} < 724$	1.87×10^{-5}	1.58×10^{-5}	8.16×10^{-5}
Length 4	$239 < x_{R4} < 385$	1.68×10^{-5}	1.84×10^{-5}	3.90×10^{-4}
Length 5	$102 < x_{R5} < 210$	1.30×10^{-5}	1.58×10^{-5}	1.05×10^{-5}
Length > 5	$102 < x_{R>5} < 210$	9.02×10^{-6}	2.63×10^{-6}	1.42×10^{-4}
The longest run test	$x_L < 26$	2.98×10^{-4}	2.95×10^{-4}	2.92×10^{-4}

quences generated from the reaction-diffusion cellular array model with the sequences generated from the cellular automata which operate according to *Rule*30.

Monobit Test

Figure 3(a) shows a probability distribution of the number x_M of "+1"s contained in a subsequence.

Poker Test

We obtain from a subsequence 5,000 four-bit words $\boldsymbol{d}_m$=($d(n_l+4m+1)$, $d(n_l+4m+2)$, $d(n_l+4m+3)$, $d(n_l+4m+4)$), m=0, $\cdots$, 4999, n_l=n_0+2×10^4×l, l=0, $\cdots$, 99. There exist 16 kinds of word, $\boldsymbol{w}_k$, k=0, $\cdots$, 15, in a set of 5,000 word elements. Let the number of words such that $\boldsymbol{d}_m$=$\boldsymbol{w}_k$ in the set be denoted by f_k. Figure 3(b) shows the probability distribution of χ^2 given by the following expression in terms of f_k:

$$\frac{16}{5000}\sum_{k=0}^{15} f_k^2 - 5000 \tag{19}$$

Runs Test

Figures 3(d) to (i) show probability distributions of the numbers x_{Rj} of "+1" runs of lenght (j=)1, 2, $\cdots$, 5 and longer than 5 contained in a subsequence.

The Longest Run Test

Figure 3(c) shows a probability distribution of the length x_L of the longest "+1" run contained in a subsequence.

Table 1 shows probabilities that x_M, χ^2, x_{Rj}, x_L are out of the ranges which were the *PASS RANGE* designated in FIPS 140-2 randomness tests. We see from Figs. 3 and Tab. 1 that the pseudorandom sequences generated from the reaction-diffusion cellular array have almost the same statistical properties as truly random binary i.i.d. sequences. We see from Tab. 1 that the sequence the cellular automata with *Rule*30 generate contains more runs whose length are longer than 5 than truly random binary i.i.d. sequences.

4. Conclusions

We have found that the pseudorandom i.i.d. sequences generated from the deterministic reaction-diffusion cellular array model have almost the same statistical properties as truly random i.i.d. sequences.

A diffusion cell permutes two molecules at each time step. Discretized chaotic maps [2] are also considered to permute small intervals of variable space. It is interesting that both discrete systems generate pseudorandom sequences by permutation. Permutation seems to be an origin of randomness.

References

[1] P. Fan and M. Darnell, "Sequence Design for Communication Applications," *Research Studies Press*, 1996.

[2] D. Yoshida, A. Tsuneda and T. Inoue, "An Algorithm for the Generation of Maximal-Period Sequences based on One-Dimensional Chaos Maps with Finite Bits," *IEICE Trans. on Fundamentals*, Vol.E87-A, No.6, pp.1371-1376, 2004.

[3] H. Fujisaka, K. Furuta, S. Soga, K. Haeiwa and T. Kamio, "A Parallel Method for Generating Pseudorandom Binary Markovian Sequences," *Proc. Int'l Symp. on Spread Spectrum Techniques and Applications*, pp.103-107, 2006.

[4] H. Fujisaka, D. Hamano, M Sakamoto and T. Kamio, "A Binary-Quantized Pseudo-Diffusion Systems," *Proc. Int'l Symp. on Circuits and Systems*, pp.720-723, 2004.

[5] A. Ilachinski, "Cellular Automata: A Discrete Universe," *World Scientific Publishing*, 2001.