Information Sciences 324 (2015) 23–31

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

Reversibility of general 1D linear cellular automata over the binary field $\mathbb{Z}_2$ under null boundary conditions

Bin Yang, Chao Wang*, Aiyun Xiang

College of Software, Nankai University, Tianjin 300071, China

A R T I C L E   I N F O

Article history:
Received 29 December 2014
Revised 6 May 2015
Accepted 28 June 2015
Available online 3 July 2015

Keywords:
Cellular automata
Reversibility
Linear rule
Null boundary
Deterministic finite automata

A B S T R A C T

The reversibility of cellular automata(CA) has long been studied but there are still many problems untouched. This paper tackles the reversibility problem of the general case concerning 1D CA under null boundary conditions defined by linear rules over the binary field $\mathbb{Z}_2$. Although transition matrix has been widely used for some special linear CA(LCA) rules, it has severe limitations: its complexity depends on the number of cells, and determining its reversibility becomes another unsolved tough problem for general rules. By constructing deterministic finite automata(DFA) of the de Bruijn graph presentation of CA, we conclude the reversibility problem of all 1D linear rules over $\mathbb{Z}_2$ under null boundary conditions. It turns out that any 1D LCA, except for some unilateral rules, over $\mathbb{Z}_2$ under null boundary conditions can be reversible once having a proper number of cells, and DFA provides an efficient way to find those numbers. Moreover, the complexity of the DFA solution is independent of the number of cells. In addition, the relative low complexity of DFA can be further significantly reduced by using only a small part of it.

1. Introduction

First introduced by John von Neumann and Stanislaw Marcin Ulam in the 1940s to study self-reproducing automata[38], cellular automaton (CA) is a kind of discrete mathematical dynamical system consisting of a regular network of finite state automata(cells) which change their states simultaneously according to the states of their neighbors under a local rule. The local rules are truly simple for CA, which, however, could lead to rich and complicated behaviours [23,39,41] – some CA are even capable of universal computation [40].

Driven by uniform local rules, CA have been widely applied to simulating or modelling complex systems in various areas, e.g. vehicular ad hoc networks modelling [37], skin disease pattern modelling [21], tumor growth modelling [20], pedestrian evacuation simulation [43]. Further, for their complexity, CA have been extensively used for image processing such as encryption [1] and image coding [5]. Applications of CA can also be seen in a variety of other fields [4,6,15,26].

As an important property of CA, reversibility has long been put efforts into, and a series of conditions were studied in the literature. The reversibility problem of 1D CA with no boundary condition considered was already solved [3], while for two or higher dimensional CA, it was proved to be generally undecidable whether a CA rule is invertible or not [18]. When restricted to linear rules, however, there exist some solutions to the reversibility problem of a two or higher dimensional CA [17], and the

* Corresponding author. Tel.: +86 13672001805.
E-mail addresses: yangbin1004@gmail.com (B. Yang), wangchao@nankai.edu.cn (C. Wang), xa-yun@mail.nankai.edu.cn (A. Xiang).

http://dx.doi.org/10.1016/j.ins.2015.06.048
0020-0255/

inverse CA can also be computed [22]. For more information about the reversibility problem of these conventional CA please refer to [19,24].

Since the number of cells is usually finite in practical applications, the reversibility problem of CA under various boundary conditions has also been broadly studied. Most commonly, people study periodic boundaries, null boundaries and reflective boundaries.

Under periodic boundary conditions, the reversibility problem of a 1D CA with any given rule and any number of cells was generally tackled [25]. There are also studies dealing with the reversibility problem of several kinds of particular rules, such as the hybrid elementary CA(ECA) 90/150 [29], ECA 150 [8,13] and the five-neighbor linear rule over finite state set $\mathbb{Z}_p$ [7,31].

For null boundary conditions, there are research results of both 1D CA and higher dimensional ones. In the 1D case, only a small group of rules were studied, including the hybrid ECA 90/150 [29], the ECA 150 [9], symmetric no-dummy-neighbor linear rules [10], the five-neighbor linear rule 11111 [11] and the ECA 150 over finite state set $\mathbb{Z}_p$ [12]. As for the higher dimensional case, there are results about the 2D linear rules group 2460 over the ternary field $\mathbb{Z}_3$ [32] and 3D linear rules over $\mathbb{Z}_p$ [28].

In addition, the 1D linear CA (LCA) with neighborhood radius 1 under the reflective boundary conditions was studied as well [2]. Moreover, studies about the reversibility problem of some kinds of modified CA, hexagonal 2D CA [33,36], CA with memory [30] and σ/σ^+-automata [35,42] for examples, can also be found in the literature.

Although we have a number of results in the literature about the invertibility problem of CA, most of them are specifically restricted ones such as ECA [8,9,12,13,29]. Transition matrix has been a useful tool for those special linear rules [2,7,9–12,29,32,33], because for any 1D linear rule (or some 2D ones) with any given number of cells, there is a transition matrix whose reversibility is equivalent to that of the CA. However, this method has fundamental limitations since the matrix size is dependent on the number of cells: it is obviously unwise to calculate the determinant of the transition matrix for each cell number, instead, we hope to find an algorithm which can tell the relationship between the reversibility of the transition matrix and its size. In [10,11] Martín del Rey et al. did find a solution to the reversibility problem of transition matrices of symmetric no-dummy-neighbor 1D linear rules over $\mathbb{Z}_2$ under null boundary conditions. But for general linear rules, one could hardly find such a universal solution to the reversibility problem of transition matrices since the form of such matrices would be too general. This is fully illustrated in Section 2.2.

In this paper, we set out to close the general reversibility problem of 1D LCA over the binary field $\mathbb{Z}_2$ under null boundary conditions, which has not been studied in the literature yet. Since transition matrix is only applicable for some special rules, we only use it to discuss unilateral rules. Then, for the general case, we introduce deterministic finite automata(DFA). Interestingly, the DFA graph, in this case, can be arranged into the form of a regular lattice, and it has a period equal to that of a corresponding linear feedback shift register (LFSR) which is known to be equal to that of a corresponding polynomial expression. This regular lattice form of DFA graph indicates that any given 1D linear rule over $\mathbb{Z}_2$ under null boundary conditions is reversible when having a proper number of cells — except for some unilateral rules dealt with in Section 3. Finally, a simplified graph is used to determine both the reversibility and the period in terms of the number of cells of any given 1D LCA over $\mathbb{Z}_2$ under null boundary conditions.

2. Mathematical description

2.1. Basic definitions

Adapted from J. Kari's paper [19], this section describes some basic definitions of CA involved in this paper.

CA is usually described by the use of a quadruple $A = \{d, S, N, f\}$:

- $d \in \mathbb{Z}_+$ is the dimension of the *cellular space*, then each point $\vec{n} \in \mathbb{Z}^d$ is called a *cell*.
- $S = \{0, 1, \ldots, p-1\}$ represents the *finite state set*, and the state of any cell at any time must be taken from S.
- $N = (\vec{n_1}, \vec{n_2}, \ldots, \vec{n_m})$ is the *neighbor vector*, where $\vec{n_i} \in \mathbb{Z}^d$, and $\vec{n_i} \neq \vec{n_j}$ when $i \neq j$ $(i, j = 1, 2, \ldots, m)$. Thus, the *neighbors* of the cell $\vec{n} \in \mathbb{Z}_2$ are the m cells $\vec{n} + \vec{n_i}$, $i = 1, 2, \ldots, m$.
- f: $S^m \to S$ is the *local rule*, which maps the current states of all neighbors of a cell to the next state of this cell.

A *configuration* is a mapping $c : \mathbb{Z}^d \to S$ which assigns each cell a state. Make c^t denote the configuration at time t, then the state of cell $\vec{n}$ at time t is $c^t(\vec{n})$, and its state at time $t+1$ goes like this:

$$c^{t+1}(\vec{n}) = f(c^t(\vec{n}+\vec{n_1}), c^t(\vec{n}+\vec{n_2}), \ldots, c^t(\vec{n}+\vec{n_m})).$$

Now we consider the case in which the local rule f is a linear function

$$\begin{aligned} c^{t+1}(\vec{n}) &= f(c^t(\vec{n}+\vec{n_1}), c^t(\vec{n}+\vec{n_2}), \ldots, c^t(\vec{n}+\vec{n_m})) \\ &= [\lambda_1 c^t(\vec{n}+\vec{n_1}) + \lambda_2 c^t(\vec{n}+\vec{n_2}) + \cdots + \lambda_m c^t(\vec{n}+\vec{n_m})] \mod |S|, \end{aligned} \tag{1}$$

where $\lambda_i \in S$ is the rule coefficient for neighbor $\vec{n} + \vec{n_i}$, $i = 1, 2, \ldots, m$.

Such CA are called *linear cellular automata*(LCA) [6]. Eq. (1) shows that for an LCA, the next state of a cell is a linear combination of current states of all its neighbors. Conventionally, a CA has infinite number of cells as its cellular space is the whole d-dimensional integer space $\mathbb{Z}^d$. However, usually the cellular space has to be finite when a CA is applied to a practical problem, thus the boundary conditions must be considered, and *null boundary* conditions are among the favourite ones. Null boundary