数理解析研究所講究録
1489 巻 2006 年 15-21

How does the neighborhood affect the global behavior of cellular automata? [1]

近傍系はセルオートマトンの大域行動にどう影響するか？

西尾英之助（元・京大理）
Hidenosuke Nishio (Kyoto)
Iwakura Miyake-cho 204-1, Sakyo-ku, 606-0022 Kyoto, Japan
Email: YRA05762@nifty.com

1 Introduction

A cellular automaton (CA for short) is a uniformly structured information processing system defined on a regular discrete space S, which is typically presented by a Cayley graph of a finitely generated group. The same finite automaton (cell) is placed at every point of the space. Every cell simultaneously changes its state following the local function defined on the neighboring cells. The neighborhood N is also spatially uniform. Most studies on CA assume the standard neighborhoods after John von Neumann and E. F. Moore.

Changing the view point, however, we posed an algebraic theory of neighborhoods of CA for clarifying the significance of the neighborhood itself, where the neighborhood N can be an arbitrary finite subset of S, see Nishio&Margenstern (2004) [9, 8].

Based on such a setting, we ask here a question "How does (or does not) the neighborhood affect the global behavior of a CA?" In this paper, two CAs are given such that the neighborhood *does not* affect the global behavior.

2 Cellular Automaton CA

A CA is defined by a 4-tuple $(\Gamma(S), N, Q, f)$.

- *Cellular space* $\Gamma(S)$ is a Cayley graph of a finitely generated group $S = \langle G|R\rangle$ with generators G and relators R. If $G = \{g_1, g_2, ..., g_r\}$, every element of S is presented by a word $x \in (G\cup G^{-1})^*$, where $G^{-1} = \{g^{-1} |\, g\cdot g^{-1} = 1,\ g \in G\}$. The set R of relators is written as

$$R = \{w_i = w_i' \mid w_i, w_i' \in (G \cup G^{-1})^*, i = 1, ..., n\}. \tag{1}$$

  For $x, y \in \Gamma(S)$, if $y = xg$, where $g \in G \cup G^{-1}$, then an edge labelled by g is drawn from vertex x to vertex y. In the sequel $\Gamma(S)$ and S are not distinguished.

- *Neighborhood* $N = \{n_1, n_2, ..., n_s\}$ is a finite subset of S. The set of all neighborhoods is denoted by $\mathcal{N}$. The cardinality $\#(N)$ is called the neighborhood size of CA. The set of the neighborhoods of size s is denoted by $\mathcal{N}_s$. For any cell $x \in S$, the information of cell xn_i reaches x in a unit of time.

- *Set of cell states* $Q = GF(q)$ where $q = p^n$ with prime p and positive integer n. $Q = \mathbb{Z}/m\mathbb{Z}$ is also considered.

[1] A preliminary version was presented at the 11th Workshop on Cellular Automata at Gdansk University, September 3-5, 2005

- *Local map* $f : Q^N \to Q$, where an element of Q^N is called a local configuration.

- *Global map* $F : C \to C$, where an element of $C = Q^S$ is called a global configuration. F is uniquely defined by f and N as follows.

$$F(c)(x) = f(c(xn_1), c(xn_2), \cdots, c(xn_s)), \tag{2}$$

where $c(x)$ is the state of cell $x \in S$ for any $c \in C$.

When starting with a configuration c, the behavior (trajectory) of CA is given by

$$F^{t+1}(c) = F(F^t(c)) \text{ for any } t \geq 0, \text{ where } F^0(c) = c. \tag{3}$$

3 Neighborhood and Neighbors

Given a *neighborhood* $N = \{n_1, n_2, ..., n_s\} \subset S$ for a cellular space $S = \langle G \mid R \rangle$, we recursively define the ***neighbors*** of CA. Let $p \in S$.

(1) The *1-neighbors* of p, denoted as pN^1, is the set

$$pN^1 = \{pn_1, pn_2, ..., pn_s\}. \tag{4}$$

(2) The *m-neighbors* of p, denoted as pN^m, are given as

$$pN^m = pN^{m-1} \cdot N, \; m \geq 1, \tag{5}$$

where $pN^0 = \{p\}$. *Note that the computation of pn_i has to comply with the relations R defining $S = \langle G|R \rangle$.*

We may say that the information contained in the cells of pN^m reaches the cell p after m time steps.
(3) ∞*-neighbors* of p, denoted as pN^∞, is defined by

$$pN^\infty = \bigcup_{m=0}^{\infty} pN^m. \tag{6}$$

Without loss of generality, we can concentrate on the *m-neighbors of the identity element* 1 *of S*, which is called m-neighbors of CA and denoted by N^m. Then

(4) ∞-neighbors of 1, denoted as N^∞ and called the *neighbors of CA*, is given by

$$N^\infty = \bigcup_{m=0}^{\infty} N^m. \tag{7}$$

The *intrinsic m-neighbors* $[N^m] = N^m \setminus N^{m-1}$ are the cells whose information can reach the origin in exactly m steps. Obviously, $N^\infty = \bigcup_{m=0}^{\infty}[N^m]$.

Now we have an algebraic result, which is proved by the fact that the procedure to generate a subsemigroup is the same as the above mentioned recursive definition of N^∞.

Proposition 1

$$N^\infty = \langle N \mid R\rangle_{sg}, \tag{8}$$

where $\langle N \mid R\rangle_{sg}$ means the semigroup obtained by concatenating the words from N with constraints of R.

We also have the following easily proved proposition.

Proposition 2

$$\langle N \mid R\rangle_g = \langle N \cup N^{-1} \mid R \rangle_{sg}, \tag{9}$$

where $\langle N \mid R\rangle_g$ is the smallest subgroup of S which contains N.

If $N = G$, then we have the following lemma as a corollary to Proposition 2.

Lemma 1

$$\langle g_1, g_2, ..., g_r | R\rangle_g = \langle g_1, g_2, ..., g_r, g_1^{-1}, g_2^{-1}, ..., g_r^{-1} | R\rangle_{sg}. \tag{10}$$

Example: $\mathbf{Z}^2 = \langle a, b | \ ab = ba\rangle_g = \langle a, b, a^{-1}, b^{-1} | \ ab = ba\rangle_{sg}$

4 Two CAs where the neighborhood does not affects the global behavior.

The neighborhood is usually crucial for the global behavior of a CA. For example, the Game of Life [?] has been formulated assuming binary states and the Moore neighborhood in $\mathbf{Z}^2$. The local rule is cleverly chosen and many interesting behaviors like construction- and computation-universality have been proved to emerge. It would not have been so successful, if it were defined assuming the von Neumann neighborhood.

Contrary to that, in this section, we give two cases where the neighborhood *does not* affect the global behavior of CA. A brief study on the growth function of groups/neighborhoods and the Garden of Eden theorem are also given.

(I) Parity function preserves the parity of configurations for any neighborhood.
(II) Surjectivity and injectivity of linear CAs are independent from the neighborhood.

4.1 Parity function

Let $Q = \{0, 1, ..., p-1, ...\} = GF(p^n)$ with prime p and positive integer n. Consider a CA (called a parity CA), which has an s-ary local function called a *(generalized) parity function* $f_{P,N}$ defined by

$$f_{P,N}(n_1, n_2, ..., n_s) = \sum_{i=1}^{s} c(n_i) \mod p, \tag{11}$$

where $c(n_i)$ is the state of cell n_i. Note that if $Q = \{0, 1\}$ then $f_{P,N}$ is the ordinary (binary) parity function.

The global map $F_{P,N}$ of a parity CA is defined as usual and also called a (global) parity function.

Since $f_{P,N}(0,,,,0) = 0$, $0 \in Q$ is a *quiescent state*. A configuration $c \in Q^S$ is called *finite* if $\#\{i \mid c(i) \neq 0, \ i \in S\} < \infty$. For a finite configuration c, a finite subset $\{i \mid c(i) \neq 0, \ i \in S\}$ of S is called a *support* of c and denoted by $supp(c)$.

Since the finiteness of configurations is preserved by $F_{P,N}$, in the sequel we treat only finite configurations.

The *(generalized) parity* $P(c)$ of a configuration c is defined by

$$P(c) = \sum_{x \in S} c(x) \mod p. \tag{12}$$

Then we have the following theorem.

Theorem 1

$$P(F_{P,N}(c)) = P(c),\ c \in Q^S, \tag{13}$$

if and only if $N \in \mathcal{N}_s$, *where* $s = kp + 1, k \geq 0$.

Proof.

$$\begin{aligned} P(F_{P,N}(c)) &= \sum_{x \in S} F_{P,N}(c)(x) = \sum_{x \in S} f_{P,N}(xn_1, ..., xn_s) && (14) \\ &= \sum_{x \in S} \sum_{i=1}^{s} c(xn_i) = \sum_{i=1}^{s} \sum_{x \in S} c(xn_i). && (15) \end{aligned}$$

We note here, since the neighborhood is spatially uniform,

$$\sum_{x \in S} c(xn_i) = \sum_{x \in S} c(x), \text{ for any } 1 \leq i \leq s. \tag{16}$$

Then, if $s = kp + 1$, from (15) we have

$$P(F_{P,N}(c)) = \sum_{i=1}^{s} \sum_{x \in S} c(xn_i) = \sum_{x \in S} c(x) = P(c). \tag{17}$$

For the necessity of condition $s = kp + 1$, we can consider a binary parity CA ($p = 2$) having a neighborhood of size $s = 2$. Such a CA maps all configurations into those of parity 0 and does not preserve the parity. ■

Note that a binary parity function is not number conserving.

Example 1 *Consider binary parity CAs in* $\mathbb{Z} = \langle a | \emptyset \rangle$ *with a neighborhood of size 3 such as* $N_3 = \{a^{-1}, 1, a\}$, $N_3' = \{a^{-2}, 1, a^2\}$ *and* $N_3'' = \{0, a, a^2\}$. *They preserves the parity, but a CA with a neighborhood of size 2* $N_2 = \{1, a\}$ *does not. The theorem holds for finite spaces like* $\mathbb{Z}_m = \langle a | a^m = 1 \rangle$.

4.2 Linear CA over $\mathbb{Z}_m$

We consider the linear local function f of arity s over $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$;

$$f(n_1, n_2, ..., n_s) = \sum_{i=1}^{s} a_i n_i,\ a_i \in \mathbb{Z}_m, \mod m. \tag{18}$$

Then we have the following theorem.

Theorem 2 *If the growth function of S is amenable*[2], *then the surjectivity and the injectivity of a linear CA are independent from the neighborhood.*

[2]A growth function is called *amenable* if it is less than exponential. Contrary, a CA could be called *amenable*, whenever the Garden of Eden theorem holds. See the following subsections.

Proof. For such a CA that the Garden of Eden theorem holds, the theorem is proved owing to the following two theorems given for $\mathbb{Z}^2(\mathbb{Z}^d)$ by Ito&Osato&Nasu (1983) [3], which completely characterize the surjectivity and the injectivity of a linear CA over $\mathbb{Z}_m$, respectively, in terms of the coefficients $a_1, a_2, \cdots, a_s$ and the prime factors of m. Note that their proofs assume the results of Richardson(1972) [11], which are based on the Garden of Eden theorem for $\mathbb{Z}^d$. Obviously, *the characterization is independent from the neighborhood.* For other spaces where the Garden of Eden theorem does not hold, see a discussion below. ∎

Theorem 3 (Theorem 1 of [3]) *A linear CA over $\mathbb{Z}_m$ is surjective if and only if any prime factor of m does not divide all of the coefficients $a_1, a_2, \cdots, a_s$.*

Theorem 4 (Theorem 2 of [3]) *A linear CA over $\mathbb{Z}_m$ is injective if and only if for each prime factor p of m there exists a unique coefficient a_j such that $p \nmid a_j$ and $p \mid a_i$ for $i \neq j$.*

4.3 Growth Function of Groups and Neighborhoods

The *growth function* γ_S of a finitely generated discrete group $S = \langle G|R\rangle$ is defined by means of the cardinality of the ball of radius n. That is

$$\gamma_S(n) = \#\{w \mid |w| \leq n,\ w \in S\}. \tag{19}$$

Similarly we define the *growth function* $\delta_{(N,S)}$ of neighborhood N in S of a CA by

$$\delta_{(N,S)}(m) = \#\{w \mid w \in N^m\}, \tag{20}$$

where N^m is the set of m-neighbors. Obviously, if N happens to be equal to $G \cup G^{-1}$, then $\delta_{(N,S)}(m) = \gamma_S(m)$.

The following definition of the growth rate of integer functions (groups) is due to L.Babai (1997) [1].

Two monotone non-decreasing functions $f_1, f_2 : \mathrm{N} \to \mathrm{N}$ are said to be *equivalent* ($f_1 \sim f_2$), if there exist constants $c_1, c_2, C_1, C_2, n_0 > 0$ such that for all $n \geq n_0$,

$$C_1 f_1(c_1 n) \leq f_2(n) \leq C_2 f_1(c_2 n). \tag{21}$$

The relation $\sim$ is an equivalence relation. An order $\precsim$ is introduced among the equivalence classes; Let $[f_1]$ and $[f_2]$ be the equivalence classes to which f_1 and f_2 belong, respectively. Then define $[f_1] \precsim [f_2]$ if $Cf_1(cn) \leq f_2(n)$ for constants $C, c, n_0 \geq 0$ and for all $n \geq n_0$.

Examples; $n^2 \nsim n^3$ ($[n^2] \precnsim [n^3]$), $n^a \nsim b^n$ ($[a^n] \precnsim [n^b]$) and $a^n \sim b^n$ for any $n,\ a,\ b \geq 1$.

The *growth rate* $[\gamma_S]$ of a group S is an equivalence class to which γ_S belongs. Note that in the literature the growth function often means the growth rate.

The *growth rate* $[\delta_{(N,S)}]$ of a neighborhood $N \subset S$ is similarly defined. Then we have the following theorem.

Theorem 5 *For a cellular space $S = \langle G|R\rangle_g$ and any neighborhood $N \subset S$,*

$$[\delta_{(N,S)}] \precsim [\gamma_S], \tag{22}$$

where the equivalence holds if and only if $\langle N \mid R\rangle_{sg} = S$.

4.4 Garden of Eden theorem

The *Garden of Eden (GOE) theorem* is originally proved for $\mathbb{Z}^2$ by E.Moore(1962) [6] and J.Myhill(1963)[7]. It is the earliest mathematical result proved about CA.

Definition 1 *A finite configuration (pattern) is called a Garden of Eden (GOE), if it is not in the image of F (A GOE has not an ancestor). Two distinct patterns p_1 and p_2 are called mutually erasable if two configurations c_1, c_2, which contain p_1 and p_2, respectively and coincide outside of the supports of p_1 and p_2, are mapped to the same configuration.*

Theorem 6 (Moore) *If there are mutually erasable patterns, then there are GOE patterns.*

Theorem 7 (Myhill) *If there are GOE patterns, then there are mutually erasable patterns.*

If there is no GOE patterns then F is *surjective* and if there is no mutually erasable patterns then F is *injective* when it is restricted to the finite configurations. Therefore these theorems together claim the following.

Theorem 8 (GOE theorem) *F is surjective if and only if F is injective when it is restricted to the finite configurations.*

Idea of proof of Theorem 6: Let $\#(c(N^m))$ be the cardinality of different patterns contained by cells in m-neighbors N^m. For $S = \mathbb{Z}^2$ and Moore neighborhood, if there are mutually erasable patterns, then $\#(c(N^{m-1}))$ becomes greater than $\#(c(N^m))$ when m becomes large enough, which implies the existence of GOE patterns. This proof is based on the fact that *the growth of the boundary (intrinsic neighbors)* is not too fast. On the other hand, in case of a Cayley graph of free group $\langle a, b \mid \emptyset \rangle$ the boundary grows exponentially.

Taking into account such an observation, group theorists reveal that the GOE theorem holds for groups of polynomial and subexponential growth[3], but does not for exponential growth, see Machi&Mignosi(1993) [5] and Gromov(1999) [2]. Note that group theorists usually discuss the GOE theorem assuming the generators of the group as the neighborhood. This fact is one of the reasons why we are interested in the growth function of neighborhoods in general.

The dual hyperbolic plane $\{4, 5\}$ of the pentagrid $\{5, 4\}$ allows a Cayley graph presentation of a group of exponential growth [10] and therefore the above discussion on linear CAs does not apply as it is. However, there could be another proof for Theorem 2 which does not assume the GOE theorem.

Many thanks are due to Maurice Margenstern and Friedrich von Haeseler for their discussion on the growth function of groups and the hyperbolic plane concerning the joint work [10] and to Thomas Worsch for his cooperation.

References

[1] Babai, L.: The growth rate of vertex-tansitive planer graphs, *8th Annual ACM-SIAM Symposium on Discrete Algorithm*, 1997.

[2] Gromov, M.: Endomorphisms of symbolic algebraic varieties, *J. Eur. Math. Soc.*, **1**, 1999, 109–197.

[3] Ito, M., Osato, N., Nasu, M.: Linear Cellular Automata over Z(m), *J. Comput. Syst. Sci.*, **27**(1), 1983, 125–140.

[3] A subexponential growth is faster than polynomial but slower than exponential growth.

[4] Knuth, D. E.: Big omicron and big omega and big theta, *SIGACT News*, **April-June 1976**, 1976, 18–24.

[5] Machi, A., Mignosi, F.: Garden of Eden Configurations for Cellular Automata on Cayley Graphs of Groups., *SIAM J. Discrete Math.*, **6**(1), 1993, 44–56.

[6] Moore, E. F.: Machine models of self-reproducution, *Proc. Symposium in Applied Mathematics*, 14, 1962.

[7] Myhill, J.: The converse to Moore's Garden-of-Eden theorem, *Proc. Amer. Math. Soc.*, **14**, 1963, 685–686.

[8] Nishio, H., Margenstern, M.: An algebraic Analysis of Neighborhoods of Cellular Automata, Submitted to JUCS, 2004.

[9] Nishio, H., Margenstern, M.: *An algebraic Analysis of Neighborhoods of Cellular Automata*, Technical Report (kokyuroku) vol. 1375, RIMS, Kyoto University, May 2004, Proceedings of LA Symposium, Feb. 2004.

[10] Nishio, H., Margenstern, M., von Haeseler, F.: On Algebraic Structure of Neighborhoods of Cellular Automata –Horse Power Problem–, Submitted to Fundamenta Informaticae, 2005.

[11] Richardson, D.: Tessellations with Local Transformations., *J. Comput. Syst. Sci.*, **6**(5), 1972, 373–388.