数理解析研究所講究録 1426 巻 2005 年 256-262

セルオートマトンの近傍系の代数的構造

On Algebraic Structure of Neighborhoods of Cellular Automata

—Decidability Results—

西尾英之助 (元・京大理学研究科)
Hidenosuke Nishio[1]
Iwakura Miyake-cho 204, Sakyo-ku,
606-0022, Kyoto, Japan
e-mail: YRA05762@nifty.ne.jp

モーリス・マルゲンシュテルン
Maurice Margenstern
LITA, EA 3097,
UFR MIM, University of Metz,
57045 Metz, France
e-mail: margens@sciences.univ-metz.fr

フリッツ・フォン・ヘーゼラー
Friedrich von Haeseler
KU Leuven, Dep. of Electrical Engineering,
Kasteelpark Arenberg 10,
3001 Leuven, Belgium
e-mail: friedrich.vonHaeseler@esat.kuleuven.ac.be

1 Introduction

A cellular automaton (CA for short) is a uniformly structured information processing system consisting of many identical finite state machines (cells) which are located at points of a discrete regular space. The essence of CA is that the *global* behavior of the whole system is determined *locally* : the state transition of every cell depends only on the states of its neighboring cells. The rule to specify the neighboring cells is called the *neighborhood (index)* of CA and common to every cell. The most famous neighborhood is von Neumann of size 5 defined for the 2-dimensional rectangular grid $\mathbb{Z}^2$. To investigate the nature of neighborhoods generally, we began an algebraic theory of neighborhoods [5] [6][7]. In this paper, after giving preliminaries and results obtained thus far, we report recent progress of our research especially for the space $\mathbb{Z}^2$ or $\mathbb{Z}^d$, including decidability results and problems for future research.

2 Preliminaries

A CA is defined by a 4 tuple (S, N, Q, f), where S is the cellular space, at each point of which the same cell is located. The structue of a cellular space is uniform and typically represented by a Cayley graph of a finitely generated group as discussed below.

N is the neighborhood (index) which consists of a finite number of neighborhood indices. The same neighborhood is applied to every point of S.

[1]Corresponding author

The set of states Q is a finite set of symbols. The local map $f : Q^N \to Q$ gives a local state transition function, which is common to every cell.

The global dynamics of CA is defined as the global map $F : C \to C$, where elements of $C = Q^S$ are called global configurations. F is uniquely induced from f by

$$F(c)(x) = f(c(xn_1), c(xn_2), \cdots, c(xn_s)),$$

for any $c \in C$ and $x \in S$. When starting from a configuration c, the behavior (trajectory) is given by $F^{t+1}(c) = F(F^t(c))$, for any $c \in C$ and $t \geq 0$, where $F^0(c) = c$.

2.1 Cellular space S and neighbors relative to S

2.1.1 Space

The cellular space S is assumed to be represented by a Cayley graph such that $S = \langle G \mid R \rangle$, where $G = \{g_1, g_2, ..., g_r\}$ is a finite set of generators (symbols) and R is a finite set of relations (equalities) of words over G and G^{-1}, where $G^{-1} = \{g^{-1} \mid g \in G\}$, $g \cdot g^{-1} = 1$ and 1 is the empty word or the identity if S happens to be a (semi)group.

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

Every element (point) of S is represented as a *word* $x \in (G \cup G^{-1})^*$. For $x, y \in S$, if $y = xg$, where $g \in G \cup G^{-1}$, then an edge labelled by g is drawn from point x to point y (definition of a Cayley graph). For a point x of S, there can be more than one words which represent x, but such a set of words constitutes an equivalence class closed under the group operation and therefore we are allowed to take any word as its representative. Particularly, in this paper we assume an *uncancellable* word, where no occurrences of subwords of the form gg^{-1} appear, see [1].

2.1.2 Neighborhood and neighbors

Let a space $S = \langle G \mid R \rangle$ be given. A neighborhood (index) for S is expressed by

$$N = \{n_1, n_2, ..., n_s\} \subset (G \cup G^{-1})^* \tag{2}$$

Now we recursively define the *neighbors* of CA as follows.

(1) Let $p \in S$, then the *1-neighbors* of p, denoted as pN^1, is the set

$$pN^1 = \{pn_1, pn_2, ..., pn_s\}. \tag{3}$$

(2) The $(m+1)$-*neighbors* of p, denoted as pN^{m+1}, are given as

$$pN^{m+1} = pN^m \cdot N, \ m \geq 0, \tag{4}$$

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. In the sequel, without loss of generality, we principally treat the m-neighbors $1N^m$ (N^m in short) of the origin 1 of S. The cardinality of N^m, denoted as $\#N^m$, is called the *neighborhood size.*

(3) ∞-*neighbors* of p, denoted as pN^∞, is defined by

$$pN^\infty = \bigcup_{m=0}^{\infty} pN^m. \tag{5}$$

(4) ∞-neighbors of 1, denoted as N^∞, is called *neighbors* (of CA).

Then we have an algebraic result, which is proved by the fact that the procedure to generate a subsemigroup and the above mentioned recursive definition of N^∞ are the same. For a recursive procedure to generate subalgebras, we refer to page 33 of [3].

Proposition 2.1

$$N^\infty = \langle N \mid R\rangle_{sg}, \tag{6}$$

where $\langle N \mid R\rangle_{sg}$ *means the semigroup generated by* N *with relation* R.

Remarks: A subalgebra $\langle A\rangle$ generated by a set A is the smallest subalgebra that contains A. A is called a set of generators. For a subalgebra there can be more than one set of generators. To avoid confusion, the group (res. subgroup) generated by G (res. G') is denoted by $\langle G \mid R\rangle_g$ (res. $\langle G' \mid R\rangle_{sg}$). When the defining relations are understood, we simply write as $\langle G\rangle_g$ (res.$\langle G'\rangle_{sg}$). We also use the terms of g-generate and sg-generate. A semigroup is an associative system. In addition we assume here that the cancellation rule holds.

In the sequel, for a group $S = \langle G|R\rangle_g$, a semigroup $\langle N|R\rangle_{sg}$ which is generated by words on R and complies with the same defining relations R is called a *semigroup relative to* S. Obviously, it is a subsemigroup of S. In the sg-generation, the *trivial defining relations* $\{g_i g_i^{-1} = 1, 1 \le i \le r\}$ have been assumed though not explicitly indicated.

Here we note the following lemma, which is easily proved.

Lemma 2.1

$$\langle g_1, g_2, ..., g_r|R\rangle_g = \langle g_1, g_2, ..., g_r, g_1^{-1}, g_2^{-1}, ..., g_r^{-1}|R\rangle_{sg}. \tag{7}$$

Example:

$$\mathbb{Z}^2 = \langle a, b|\ ab = ba\rangle_g = \langle a, a^{-1}, b, b^{-1}|\ ab = ba, aa^{-1} = 1, bb^{-1} = 1\rangle_{sg} \tag{8}$$

2.1.3 Set of neighborhoods

For a fixed space S, we consider the set of all finite neighborhoods relative to S and denote it as $\mathcal{N}^S$. If $N \subset N'$, where N and $N' \in \mathcal{N}^S$, N is called a *subneiborhood* of N'.

In $\mathcal{N}^S$, we define several special subclasses of neighborhoods which will be studied later.

Definition 2.1 (Symmetric) *If* $N = N^{-1}$, *then* N *is called a symmetric neighborhood.*

Von Neumann and Moore neighborhoods are symmetric.

Definition 2.2 (One-way) *If* $(N \cap N^{-1}) \setminus \{1\} = \emptyset$, *then* N *is called a one-way neighborhood.*

Remarks on the definition of one-way : The notion of *one-way* communication is clear for 1-dimensional CA, but not for higher dimensional CAs. Theorem 3.1 below shows that in case of the one-way neighborhood N_{3H} (3-horse), any pair of cells in $\mathbb{Z}^2$ can communicate with each other (the time is generally different depending on the direction). It is not true in the case of the ordinary definition of *one-way*, including that of Roka [8] and Terrier [9]. The neighborhood of a 3-horse could be said to be *locally one-way* but *globally* not. The plausibility of this definition of one-way is left for future discussion.

Definition 2.3 (Radius r) *When a metric γ happens to be defined on S, a neighborhood $N^{(r)} = \{n_1, n_2, ..., n_s | \gamma(1, n_i) \leq r, 1 \leq i \leq s\}$ is called radius r.*

Remarks on the metric : For a given S, there are several ways to define a metric. Firstly we can define a metric γ by the length of words, see [4] : for any $x \in S$, define a norm $|x|$ as the minimal length of the word representing x. By definition the length of the identity element 1 is 0. It is seen that $|x| = |x^{-1}|$ and $|xy| \leq |x| + |y|$ for any $x, y \in S$. Then the *metric by word length* is defined as $\gamma(x, y) = |xy^{-1}|$. When using the metric by word length, von Neumann neighborhood is radius 1 and Moore is radius 2.

For $\mathbb{Z}^2$ another metric γ_E called *Euclidean* can be defined : because of the commutativity between generators a and b, any point x is represented by a (shortest) unique word $x = a^i b^j$ where $i, j \in \mathbb{Z}$. Then we have $\gamma_E(x, 1) = \sqrt{i^2 + j^2}$. In the Euclidean metric, von Neumann neighborhood is radius 1 and Moore is radius $\sqrt{2}$. The Euclidean metric is defined similarly for $\mathbb{Z}^d, d > 2$.

2.1.4 Intrinsic neighbors

Define the *intrinsic* m-neighbors, denoted as $[N^m]$, as those cells that can reach the origin in exactly m steps. That is,

$$[N^m] = N^m \setminus N^{m-1}, \tag{9}$$

where $[N^0] = \{1\}$. Evidently we see,

$$N^\infty = \bigcup_{m=0}^{\infty} [N^m]. \tag{10}$$

2.2 Examples of spaces and neighborhoods

- Set of integers $\mathbb{Z} = \langle a \mid \emptyset \rangle$. Elementary CA has the neighborhood $\{a^{-1}, 1, a\}$.
- 2-dimensional rectangular grid: $\mathbb{Z}^2 = \langle a, b \mid ab = ba \rangle$.

  (1) Von Neumann neighborhood $N_V = \{1, a, a^{-1}, b, b^{-1})\}$.
  (2) Moore neighborhood $N_M = \{1, a, a^{-1}, b, b^{-1}, ab, (ab)^{-1}, ba, (ba)^{-1}\}$.
  (3) Horses (in additive group notation of $\mathbb{Z}^2$)
  (3-1) Horse $N_H = \{(\pm 2, \pm 1), (\pm 1, \pm 2)\} =$

  $$\{(2,1), (2,-1), (-2,-1), (-2,1), (1,2), (1,-2), (-1,-2), (-1,2)\}.$$

  (3-2) 3-horse $N_{3H} = \{(2,1), (-2,1), (1,-2)\} \subset N_H$.
  (3-3) Keima $N_K = \{(1,2), (-1,2)\} \subset N_H$.

- Torus $\mathbb{Z}_m \times \mathbb{Z}_n = \langle a, b \mid ab = ba, a^m = 1, b^n = 1 \rangle$ with $m, n \in \mathbb{N}$ the set of nonnegative integers.
- Hexagonal grid $\langle a, b, c \mid a^2 = 1, b^2 = 1, c^2 = 1, (abc)^2 = 1 \rangle$.
  Note that $ab \neq ba, ac \neq ca, bc \neq cb$. Since $a = a^{-1}$, any neighborhood is symmetric.
- Triangular grid $\langle a, b, c \mid abc = 1, acb = 1 \rangle$.
  The commutativity $ab = ba, ab = ba, bc = cb$ is derived from the relations.

3 Horse power problem

The problem of limited communication of CA is an interesting one and the one-way neighborhood is the most typical restriction as was discussed in Section 2. We observed various one-way neighborhoods for the space $\mathbb{Z}^2$, which do not sg-generate the whole space $\mathbb{Z}^2$. In this section, we present conditions for a neighborhood to *fill* the space.

Definition 3.1 *A neighborhood N is said to fill S if and only if $N^\infty = S$.*

Then, by Proposition 2.1, we have

Proposition 3.1 *N fills S if and only if $\langle N \rangle_{sg} = S$.*

As for a typical non-standard neighborhood, we studied the *horse power problem* and showed the following results [5][6]. When we treat the horse power problem, we use the notation of an additive group (vector space over $\mathbb{Z}$). That is, $\mathbb{Z}^2 = \{(i,j) | i,j \in \mathbb{Z}\}$ and the identity of the group is denoted as $\bar{0}$.

Theorem 3.1 *A 3-horse $N_{3H} = \{(2,1),(-2,1),(1,-2)\}$ fills $\mathbb{Z}^2$.*

Note that N_{3H} is not symmetric and *one-way.*

Theorem 3.2 *The generalized 3-horse $H_{G3H} = \{(a,b),(-a,b),(b,-a)\}$ fills $\mathbb{Z}^2$, if and only if the following conditions hold.*

condition 1: $gcd(a,b) = 1$.
condition 2: $a + b = 1 \ mod \ 2$, where $a > b > 0$.

We have generalized the problem to d-dimensional space and proved the following theorem using the theory of integral matrices.

Theorem 3.3 *Let $x_1, ..., x_s \in \mathbb{Z}^d$, where $s \geq d+1$. Then the neighborhood $\{x_1, ..., x_s\}$ fills the space or $\langle x_1, ..., x_s \rangle_{sg} = \mathbb{Z}^d$, if and only if the following two conditions hold.*

condition 1: $\gcd(\{det([x_{i_1}, ..., x_{i_d}]) | i_1, ..., i_d \in \{1, ..., s\}\}) = 1$.
condition 2: $\underline{0} \in int(conv(\{x_1, ..., x_s\}))$. (The zero of $\mathbb{R}^d$ should be in the interior of the convex hull of $\{x_1, ..., x_s\}$.)

Remarks: About the inequality $s \geq d+1$ in Theorem 3.3, it is clear that any smaller neighborhood than $d+1$ does not fill $\mathbb{Z}^d$. There is a neighborhood of size $d+1$ which fills $\mathbb{Z}^d$, that is, the inequality is tight.

Proposition 3.2

$$\langle \overline{-1}, e_1, ..., e_d \rangle_{sg} = \mathbb{Z}^d, \tag{11}$$

where e_i is the i-th unit vector and $\overline{-1} = (-1,-1,...,-1)$.

The theory of integer matrices also allows to state necessary and sufficient conditions for a horse to fill the torus.

Theorem 3.4 *If the horse moves on a d-dimensional torus $T = \mathbb{Z}_{m_1} \times ... \times \mathbb{Z}_{m_d}$, with $m_i \in \mathbb{N}$ and if the horse's move are $x_1, ..., x_s \in \mathbb{Z}^d$, then the horse fills the torus T if and only if*

$$\gcd(\{det([y_1, ..., y_d]) | y_i \in \{x_1, ..., x_s, m_1 e_1, ..., m_d e_d\}) = 1,$$

where e_i is the i-th unit vector.

4 Decidability results

In [5], we discussed some decision problems concerning the neighborhood, where some are decidable while others are not. Particularly we posed the problem whether a neighborhood fills S or not. Before entering our topics, we notice here the fundamental theorem that the word problem for semigroups is undecidable, which was posed in 1914 by Thue and proved in 1947 independently by Markov and Post, see [1]. We can show, however, some decidability results, if we assume a specific case of $S = \mathbb{Z}^2$ (or $\mathbb{Z}^d$).

4.1 Word problem

Assume $S = \mathbb{Z}^2 = \langle a, b | ab = ba \rangle_g$ and a subset $N \subset S$. The word problem for N relative to S is to decide, for any two words $x, y \in \langle N | ab = ba \rangle_{sg}$, whether or not $x = y$ in S.

Then we have,

Theorem 4.1 *For any neighborhood $N \subset S$, the word problem for N relative to S is decidable.*

Proof: Let $N = \{n_1, n_2, ..., n_s\}$, where $n_i \in \{a, b, a^{-1}, b^{-1}\}^*, 1 \leq i \leq s$. Since x and y are concatenations of words from N, we can uniquely obtain their *minimal presentations* $[x]$ and $[y]$ by rewriting words (reducing the lengths of words) using the commutative relation $ab = ba$ and the trivial defining relations $aa^{-1} = 1$ and bb^{-1} so that $[x] = a^i b^j$ and $[y] = a^{i'} b^{j'}$, where $i, i', j, j' \in \mathbb{Z}$. Since $x = y$ in S, if and only if $i = i'$ and $j = j'$, which are trivially decidable, we have proved the theorem. □

We have a corollary concerning the intrinsic neighbors.

Corollary 4.1 *For any word $x \in \langle N \rangle$ and m, it is decidable if $x \in [N^m]$ or not.*

Proof: Since $[N^m]$ is a finite set of effectively constructed words, there is a finite (effective) procedure to test if x is an element of $[N^m]$ or not. □

4.2 Decidability of infinity

In case of $S = \mathbb{Z}^2$, any nontrivial neighborhood generates an infinite neighbors(subsemigroup). That is,

Theorem 4.2 *For $S = \mathbb{Z}^2$ and a neighborhood $N \in \mathcal{N}^S$ such that $N \neq \{1\}$, $\#\langle N \rangle_{sg} = \infty$.*

Proof: If $N \ni x \neq 1$, then for $i \neq j \in \mathbb{N}$, $x^i \neq x^j$.

For the case of the hexagonal grid, however, there is a nontrivial neighborhood which generates a finite subsemigroup. For example, take $N = \{abc\}$, then we see $\langle N \rangle_{sg} = \{abc, (abc)^2 = 1\}$.

It is an algebraic problem to decide for an arbitrary space S and neighborhood N whether N generates an infinite neighbors (subsemigroup) or not. Even when a neighborhood generates an infinite subsemigroup, it does not necessarily generate (fill) the space. For example, in $\mathbb{Z}^2$, $N = \{1, a\}$ generates the infinite subspace $\{a^i | i \in \mathbb{Z}\}$.

4.3 Decidability of horse power problem

We show here decidability results (computational complexity) concerning the filling problem. As discussed earlier [6], we have a decidability result, which is proved using a result from the universal algebra [2].

Theorem 4.3 *The decision problem whether a neighborhood fills the space is* **P**-*complete.*

5 Problems for future research

As defined in Section 2.1.3, considering various neighborhoods for a space S will lead to a new interesting theory of CAs. For instance, assume a fixed space S and fix a local function f_s with s arguments, then observe what happens if the neighborhood is changed in N_s, the set of all neighborhoods consisting of s elements. Which neighborhood from N_s is the *best* one for f_s ? For a fixed local function, is its injectivity and/or subjectivity *neighborhood-sensitive* ? It is also interesting to investigate m-neighbors (informational distance) with respect to a duly defined metric γ (physical distance) as was discussed in Subsection 2.1.3.

References

[1] Adian, S. I., Durnev, V. G.: Decision Problems for groups and semigroups, *Russian Math. Surveys*, **55**, 2000, 207–296.

[2] Bergman, C., Slutzki, G.: Computational Complexity of Generators and Nongenerators in Algebra, *International Journal of Algebra and Computation*, **12**, 2002, 719–735.

[3] Burris, S., Sankappanavar, H. P.: *A Course in Universal Algebra*, The millennium edition, Open website, 2000.

[4] Gromov, M.: Groups of Polynomial Growth and Expanding Maps, *Publ. Math. I.H.E.S.*, **53**, 1981, 53–73.

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

[6] 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.

[7] Nishio, H., Margenstern, M., von Haeseler, F.: *On Algebraic Structure of Neighborhoods of Cellular Automata -full and one-way*, Technical Report 253, CDMTCS, University of Auckland, December 2004, Proceedings of the International Workshop on Tilings and Cellular Automata, 2004.

[8] Roka, Z.: One-way cellular automtata on Cayley graphs, *Theoretical Computer Science*, **132**, 1994, 259–290.

[9] Terrier, V.: *Cellular automata recognizer with restricted communication*, Technical Report 32, Turku Center for Computer Science, June 2004, Proceedings of DMCS'04.

March 22, 2005