数理解析研究所講究録 1375 巻 2004 年 1-7

An algebraic analysis of neighborhoods of cellular automata [1]

Hidenosuke Nishio[2]
西尾英之助 (元・京大理)
Iwakura Miyake-cho 204,
Sakyo-ku, Kyoto, 606-0022 Japan.
email: YRA05762@nifty.ne.jp

Maurice Margenstern
モーリス・マルゲンシュテルン (メッス大学)
LITA, EA 3097, Université de Metz
57045 METZ CEDEX, France
email: margens@sciences.univ-metz.fr

Abstract: From the point of view that the neighborhood plays a key role in information (signal) transmission of a cellular automaton, we define and analyze the neighborhood in terms of algebra and elementary number theory. Among others we treat the problem whether a neighborhood *fills* the cellular space or not. We distinguish the neighborhood from the generators of the group that defines a space. Definitions, analysis and results are given. Decision problems concerning the fullness are also investigated. As a very simple but instructive example of the neighborhood, we consider the horse of chess which can move to eight directions and *fills* the chess board, finite or infinite. We show that even when its move is limited to less, say three, directions, it fills the 2-dimensional Euclidean space, but a horse limited to any two directions does not. Also we define a generalized horse and discuss the condition in order that it fills the space.

1 Definitions

1.1 Cellular space

A cellular automaton (CA) is defined on a cellular space S, which is regularly structured. An element of S is called a *cell* or a *point*. A possible regular structure of S will be the Cayley graph of a finitely generated discrete group. Such a group is usually presented by finite generators and finite number of relations between words of them [4] [11] [9]. Generally, for a subset G of a group S, $\langle G \rangle$ means

[1] An extended abstract. The full paper will appear elsewhere.
[2] Corresponding author

the subgroup of S which is generated by G or the smallest subgroup of S that contains G. G is called a generator set of $\langle G \rangle$.

1.2 Neighborhood and neighbors

We define a ***neighborhood (index)*** N as an arbitrary nonempty subset of a cellular space S and consider that it specifies the extent where the information directly comes from. A CA is uniform also in the sense that N is applied to any point of S. Suppose that p is a cell in S. The cells $p+N$ are defined to be ***1-neighbors*** of p and denoted as pN^1. The information of a cell of 1-neighbor of p is considered to reach p in one unit of time (1 step). In other words the neighborhood N becomes 1-neighbor of p when applied to a cell p.

m-neighbors: The set of cells which directly send information to $p+N$ is defined to be $(p+N)+N$. Since their information reaches p in two steps, they are called 2-neighbors of p and denoted as pN^2. Inductively we define the ***m-neighbors*** of p as follows. By definition p is 0-neighbor of p or $pN^0 = p$. .

$$pN^{m+1} = pN^m + N, \; m \geq 0. \tag{1}$$

We interpret pN^m as a notation of the property that information of a cell in pN^m can reach p in m steps.

The following lemmas are trivial consequences of the definition of m-neighbor by Equation (1).

Lemma 1 transitivity. *If $q \in pN^m$ and $r \in qN^{m'}$ then $r \in pN^{m+m'}$.*

Lemma 2 additivity. *If $q \in pN^m$ then for any $a \in S$, $q + a \in (p+a)N^m$.*

Particularly, if $q \in pN^m$, then $q - p \in 0N^m$.

Definition 3 neighbors. We define the ***transitive closure*** of N by

$$pN^{\infty} = \bigcup_{m=0}^{\infty} pN^m. \tag{2}$$

If $q \in pN^{\infty}$, then q is called a ***neighbor*** of p. We interpret this relation as an indication that the information of cell q reaches cell p at some time. $0N^m$ and $0N^{\infty}$ will be shortly denoted by N^m and N^{∞}, respectively. We call N^m and N^{∞} the ***m-neighbors*** and the ***neighbors*** of (the origin of) a CA, respectively. We notice that N^{∞} is generally a semi-group $(N^{\infty}, +, 0)$ generated by N with relations.

Problems: (1) Estimate the size of N^m; It is not easy to estimate the size of N^m for general neighborhoods and spaces, since more than one semi-group words presents an identical element of N^∞.
(2) Define the *intrinsic* m-neighbors $[N^m]$ as such cells that can reach the origin in exactly m steps. Obviously, we see

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

and

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

The notion of intrinsic m-neighbors is particularly important when we consider the speed of information processing in CAs. Now we pose another problem: Find a simple algorithm to compute the intrinsic m-neighbors for any $m \geq 1$. Estimate the size of them.

1.3 Symmetric and one-way neighborhoods

If $N = -N$, then N is called *symmetric.* In a CA space with symmetric neighborhood, the information flow is bidirectional. If N is symmetric, then evidently N^∞ is a group. If $(N \cap -N) \setminus 0 = \emptyset$, then N is called *one-way,* since then the information flows in one direction. If N is not one-way and there is a $p \in N$ such that $-p \notin N$, then N is called *partially one-way.*

2 Analysis of neighborhoods

The first analysis of neighborhoods addresses the problem whether a neighbor *fills* a CA space or not. A neighborhood N is said to *fill* a CA space S if and only there is a nonnegative integer m such that $q \in pN^m$ for any $p, q \in S$. Formally, we define it by,

Definition 4 fill. Assume a CA space $S = (S, +, -, 0)$. $N \subseteq S$ is said to *fill* S, if and only if for any $p, q \in S$, $q \in pN^\infty$.

Note on the terminology: As is shown later our notion of *fill* is different from *generate* which is usually used in algebra. In order to avoid a confusion between the generators of the space and the neighborhood, we dare use the term *fill* for the neighborhood [3]. We also refrain from using the term *complete,* which has been used with different meanings for many theories of the computer science including our study of information dynamics of CA, see Section 5 of [7].

[3] As for the terminology we follow V.Terrier who uses the term *full* for a neighborhood when it *fills* the 2-dimensional cellular space [10], while V. Poupet uses the term *complet* in his French paper for the space $\mathbb{Z}^d$ [8].

Theorem 5. *N fills S, if and only if for any $p \in S$, $p \in N^\infty$.*

Theorem 6. *If N is a symmetric neighborhood, then for any $p, q \in S$ and non-negative integer m,*

$$p \in qN^m \Longleftrightarrow q \in pN^m. \tag{3}$$

Corollary 7. *If N is a symmetric neighborhood, then for any $p, q \in S$*

$$p \in qN^\infty \Longleftrightarrow q \in pN^\infty. \tag{4}$$

Theorem 8. $\langle N \rangle \supseteq N^\infty$.

Theorem 9. *There are Ns such that $\langle N \rangle \supsetneqq N^\infty$.*

Theorem 10. *If N is symmetric, then $\langle N \rangle = N^\infty$, but not vise versa.*

3 Horse power problem

The horse [4] of the chess can move to 8 directions (points) on the chess board, which is a finite 8×8 grid. Here we formulate and investigate the movement of a horse in an infinite cellular space $S = \mathbb{Z}^2$ with a neighborhood N_H as was shown in the previous section. The motion of a horse is interpreted as the information flow in the reverse direction; if it goes to a point q from point p in m-moves, then the information of cell q reaches cell p in m-time steps. Therefore, if a horse can go to every point of S from the origin, then the neighborhood N_H fills S. It will be shown that even when the horse's move is limited to properly selected 3 directions, it fills S, but if it is limited to any 2 directions, it does not. We shall call such a study the *horse power problem.*

3.1 3-horse

First we note the following proposition which has been known to every body.

Proposition 11. *A horse can reach any point of $\mathbb{Z}^2$ from its origin* $(0, 0)$.

A horse which is restricted to 3 moves $(2, 1), (-2, 1)$ and $(1, -2)$ is called a *3 horse* and its neighborhood is denoted by N_{3H}. Note that $N_{3H} = \{(2, 1), (-2, 1), (1, -2)\}$ is asymmetric.

Theorem 12. *A 3-horse can reach any point of $\mathbb{Z}^2$ from its origin* $(0, 0)$. *Formally,*

$$N_{3H}^\infty = \mathbb{Z}^2 = \langle N_{3H} \rangle.$$

[4] Usually it is called the *knight* in the chess terminology. But, we dare use the term horse here.

Proof. The point (X, Y) which the 3-horse reaches after x-steps of $(2,1)$ move, y-steps of $(1,-2)$ move and z-steps of $(-2,1)$ move is expressed by

$$\left.\begin{aligned} X &= 2x + y - 2z \\ Y &= x - 2y + z \end{aligned}\right\} \tag{5}$$

Note that x, y and z are the number of steps of 3-horse and therefore should be positive integers. It is necessary and sufficient to prove that the 3-horse can reach 5 points $(0,0), (1,0), (0,-1), (-1,0)$ and $(0,1)$, the von Neumann neighborhood, from the origin $(0,0)$.

By solving the above indeterminate system of equations (5) for each of those 5 points, we obtain the following solutions which give the smallest number of steps for the 3-horse to move.

- $(X, Y) = (0,0) : x = 3, y = 4, z = 5.$ total number of steps $= 12$.
- $(X, Y) = (1,0) : x = y = z = 1.$ total number of steps $= 3$.
- $(X, Y) = (0,-1) : x = 1, y = 2, z = 2.$ total number of steps $= 5$.
- $(X, Y) = (-1,0) : x = 2, y = 3, z = 4.$ total number of steps $=9$.
- $(X, Y) = (0,1) : x = 2, y = 2, z = 3.$ total number of steps $=7$.

Theorem 13. *Any horse which has no more than 2 moves does not fill nor generate $\mathbb{Z}^2$.*

3.2 Generalized horse

In this section, we consider the ***generalized horse*** which can move to 8 cells $(\pm a, \pm b)$ and $(\pm b, \pm a)$ and a generalized 3-horse $N_{G3H} = \{(a,b), (-a,b), (b,-a)\}$, where a and b are positive integers. Particularly, we shall prove two theorems showing that the generalized horse and a generalized 3-horse fill the space $\mathbb{Z}^2$, when a and b satisfy certain simple conditions.

Theorem 14. *A generalized horse fills $\mathbb{Z}^2$, if and only if $gcd(a,b) = 1$, where $a, b > 0$.*

Theorem 15. *The generalized 3-horse $H_{G3H} = \{(a,b), (-a,b), (b,-a)\}$ fills $\mathbb{Z}^2$, if and only if $gcd(a,b) = 1$ and $a + b = 1 \bmod 2$ (i.e. a and b have different parities), where $a > b > 0$.*

4 Decision problems

We pose some decision problems and solve them utilizing results which have been established about the computational algebra and the word problem of semi-groups.

Theorem 16 (Generation problem). *For an arbitrary neighborhood $N \subseteq S$, the decision problem whether $\langle N \rangle_G = \langle S, \cdot, ^{-1}, 0 \rangle$ or not is* **P***-complete.*

Proof. Since the group $\langle S, \cdot, ^{-1}, 1 \rangle$ is an algebra, we can apply the decidability result for the algebra generation established by Bergman and Slutzki, see [2]. It proves that the decision problem whether a subset of S generates the algebra is **P**-complete.

If N is symmetric, owing to Theorem (10), the following filling problem is equivalent to the generation problem of groups which was proved to be **P**-complete by Theorem 16. For asymmetric neighborhoods, however, we need a little device for applying the same result on the universal algebra.

Theorem 17 (Filling problem). *Assume that a cellular space S is defined by a finitely generated group $(G, R, \cdot, ^{-1}, 1)$ and an arbitrary (asymmetric) neighborhood is given as its subset $N \subseteq S$. Then, the decision problem whether $N^{\infty} = S$ or not is* **P***-complete and a fortiori decidable.*

Remarks: V. Poupet proved in the appendix to his thesis [8], without using the result of [2], that the filling problem is decidable for the case of $\mathbb{Z}^d$.

Theorem 18 (Membership problem). *Assume a space S. Then, for any $p \in S$, the decision problem whether $p \in \langle N \rangle_{SG}$ is* **P***-complete.*

Theorem 19 (Word problem). *For any $p, q \in S$ which are presented by words of generators (neighborhood), the decision problem whether $p = q$ or not is undecidable.*

Proof. This is because the word problem of semi-groups (associative systems) is undecidable, as is proved by A. A. Markov [6].

Remarks: We proved the word problem owing to a very general theorem which holds for an arbitrary semi-group. The decidability result could be different, however, if we consider a restricted class of spaces and neighborhoods. There are several classes of semi-groups where the word problem is computable in polynomial time. Such an algorithmic investigation of groups and semi-groups belongs to the computer algebra. Among others, we refer the reader to Adian and his school for very important results as Makanin's algorithm about equations in words [1]. See also a survey by Lothaire [5].

5 Concluding remarks

We formulated the neighbors relative to the space and analyzed its properties in terms of algebraic notions. In short, the space is a group and the set of neighbors is a semi-group relative to it. Once so formulated, many properties of cellular spaces and neighborhoods were made clear by using relevant results known to algebraists. However, we have left for further research to attack some problems like the horse power problem on finite spaces and the problem concerning the m-neighbors and the intrinsic m-neighbors.

The first author began this research during his stay at Faculty of Informatics, University of Karlsruhe, September-October, 2003. R. Vollmar and T. Worsch there had interest and made discussions with him on this topics. Véronique Terrier in Caen sent him the ps files of her own and Poupet's manuscripts [10] [8]. T. Saito in Osaka was helpful in drawing figures. Many thanks are due to them.

References

1. Adian, S. I. , Durnev, V. G. : Decision problems for groups and semigroups, *Russ. Math. Surv.* , **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. Coxter, H. S. M., Moser, W. O. J.: *Generators and Relations for Discrete Groups*, Fourth edition, Springer, 1980.
5. Lothaire, M. : *Algebraic Combinatorics on Words*, Cambridge University Press, 2002.
6. Markov, A. A.: On the impossibility of certain algorithms in the theory of associative systems, *Dokl. Acad. Nauk. USSR (English translation)*, **55**, 1947, 583–586.
7. Nishio, H., Saito, T.: Information Dynamics of Cellular Automata I: An Algebraic Study, *Fundamenta Informaticae*, **58**, 2003, 399–420.
8. Poupet, V.: *Accélération par une constante sur automates cellulaires*, Technical report, LIP ENS Lyon, Juillet 2003, Sous la direction de J. Mazoyer.
9. Roka, Z.: One-way cellular automata on Cayley graphs, *Theoretical Computer Science*, **132**, 1994, 259–290.
10. Terrier, V.: Two dimensional cellular automata and their neighborhoods, *TCS*, **312**, 2004, 203–222.
11. White, A. T.: *Graphs, Groups and Surfaces*, Second edition, North-Holland, 1984.