数理解析研究所講究録
第 1691 巻 2010 年 51-57

Automorphism Classification of Cellular Automata—a continuation

西尾英之助 (元・京大理)
Hidenosuke Nishio[1]
Kyoto University

Abstract

Following the previous studies on the automorphism classification of CA, we treat here a few new topics: (1) We prove first a lemma that the equivalence/automorphism of CA is conserved when changing the neighborhood. (2) We recollect the past studies on the enumeration of equivalence classes of Boolean functions in 1950-60s and generalize thereunder the automorphism classification of CA.

1 Preliminaries

The definitions and previous results are briefly restated, of which details will be found in [1, 2, 3].

1.1 CA and local structures

A cellular automaton is defined by a 4-tuple $(\mathbb{Z}^d, Q, f, \nu)$, where $\mathbb{Z}^d$ is a d-dimensional Euclidean space, Q is a finite set of *cell states*, $f : Q^n \to Q$ is a *local function* and ν is a *neighborhood*.

- **[neighborhood]** *A neighborhood* is an injective map $\nu : \mathbb{N}_n \to \mathbb{Z}^d$, where $\mathbb{N}_n = \{1, 2, \ldots, n\}$ and $n \in \mathbb{N}$. This can equivalently be seen as a list ν with n components $(\nu_1, \ldots, \nu_n)$, where $\nu_i = \nu(i), 1 \leq i \leq n$, is called the i-th *neighbor*. The i-th variable of f is connected to the i-th neighbor.

- **[local structure]** *A pair* (f, ν) is called a *local structure* of CA. We call n the *amity* of the local structure. When the space $\mathbb{Z}^d$ and the state set Q are understood, CA is often identified with its local structure.

- **[global function]** A local structure uniquely induces a *global function* $F : Q^{\mathbb{Z}^d} \to Q^{\mathbb{Z}^d}$, which is defined by
$$F(c)(p) = f(c(p + \nu_1), c(p + \nu_2), ..., c(p + \nu_n)), \tag{1}$$
for any *global configuration* $c \in Q^{\mathbb{Z}^d}$, where $c(p)$ is the state of cell $p \in \mathbb{Z}^d$ in c.

Remark 1 *In [2] the local structure is defined more generally, but in this paper we assume, without loss of generality, a restricted but most usual case of reduced local structures, see the following definition and Lemma 1.*

Definition 1 **[reduced local structure]** *A local structure is called reduced, if and only if*

- *ν is injective, i.e. $\nu_i \neq \nu_j$ for $i \neq j$ in the list of neighborhood ν and*
- *f depends on all arguments.*

Lemma 1 *For each local structure (f, ν) there is an equivalent reduced local structure (f', ν').*

---

[1] *email: YRA05762@nifty.com*

1.2 Permutation equivalence of local structures

Definition 2 [equivalence] *Two local structures (f, ν) and (f', ν') are called equivalent, if and only if they induce the same global function. In that case we write $(f, \nu) \approx (f', \nu')$.*

Definition 3 [permutation of local structures] *Let π denote a permutation of the numbers in $\mathbb{N}_n$. The set of all permutations πs of the numbers from $\mathbb{N}_n$ constitutes a symmetric group S_n of degree n.*

- *For a neighborhood ν, denote by ν^π the neighborhood defined by $\nu^\pi_{\pi(i)} = \nu_i$.*
- *For an n-tuple $\ell \in Q^n$, denote by ℓ^π the permutation of ℓ such that $\ell^\pi(i) = \ell(\pi(i))$ for $1 \le i \le n$.*

  For a local function $f : Q^n \to Q$, denote by f^π the local function $f^\pi : Q^n \to Q$ such that $f^\pi(\ell) = f(\ell^\pi)$ for all ℓ.

Remark 2 *As for the definition of the permutation of local functions, we have the following lemma.*

Lemma 2 *When a local function $f : Q^n \to Q$ is expressed by a polynomial $f(x_1, ..., x_n)$ over $GF(q), q = |Q|$, we have another equivalent definition for the permutation of local functions — permutation of the order of arguments.*

$$f^\pi(x_1, ..., x_n) = f(x_{\pi(1)}, ..., x_{\pi(n)}) \tag{2}$$

Example 1 *Permutations of 3 objects are usually expressed by a symmetric group $S_3 = \{\pi_i, 0 \le i \le 5\}$ as is shown below.*

$$\pi_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \pi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \pi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

$$\pi_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \pi_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \pi_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Neighborhood $(-1, 0, 1)$ is called the elementary neighborhood and denoted ENB. Then 6 permutations of ENB are seen isomorphic to S_3 as follows.

$$ENB^{\pi_0} = (-1, 0, 1), ENB^{\pi_1} = (-1, 1, 0), ENB^{\pi_2} = (0, -1, 1),$$

$$ENB^{\pi_3} = (0, 1, -1), ENB^{\pi_4} = (1, -1, 0), ENB^{\pi_5} = (1, 0, -1)$$

The local function of an ECA is called an elementary local function denoted ELF, which is expressed by a polynomial over $GF(2)$ or a Boolean function in 3 variables.

The local function of computation universal ECA rule 110 is expressed by $f_{110}(x_1, x_2, x_3) = x_1x_2x_3 + x_2x_3 + x_2 + x_3$. Then 6 permutations of f_{110} are shown as follows.

$$f_{110}^{\pi_0} = f_{110}^{\pi_1} = x_1x_2x_3 + x_2x_3 + x_2 + x_3. \tag{3}$$
$$f_{110}^{\pi_2} = f_{110}^{\pi_4} = x_1x_2x_3 + x_1x_3 + x_1 + x_3. \tag{4}$$
$$f_{110}^{\pi_3} = f_{110}^{\pi_5} = x_1x_2x_3 + x_1x_2 + x_1 + x_2. \tag{5}$$

1.3 Previous results

Here we extract from the previous papers some basic results on the equivalence of local structures.

Lemma 3 *(f, ν) and (f^π, ν^π) are equivalent for any permutation π.*

Lemma 4 *If (f, ν) and (f', ν') are two reduced local structures which are equivalent, then there is a permutation π such that $\nu^\pi = \nu'$.*

Theorem 1 [permutation-equivalence of local structures]
If (f, ν) and (f', ν') are two reduced local structures which are equivalent, then there is a permutation π such that $(f^\pi, \nu^\pi) = (f', \nu')$.

Automorphism classification of CA

Definition 4 *Two CA A and B are called automorphic, denoted $A \cong B$, if and only if there is a pair of permutations (π, φ) such that*

$$(f_B, \nu_B) = (\varphi^{-1} f_A^\pi \varphi, \nu_A^\pi). \tag{6}$$

The automorphism naturally induces a classification of local functions of CA, which will be called the automorphism classification. Every CA belonging to an automorphism class is said to have the same behavior up to permutations.

As a typical example of the automorphism classification, the set of 256 ELF is classified into 46 classes, see *kôkyûroku* of RIMS workshop (LA Symposium, Feb. 2009) [1].

2 Equivalence is conserved when changing neighborhoods

We prove here a lemma that *equivalence of local structures is conserved when changing the position of neighborhoods.* Owing to this lemma, the automorphism classification is not affected by changing the neighborhood. We notice that the mapping r introduced below conserves the equivalence, but generally not the global properties of CA like reversibility.

Consider an injective map $r : \mathbb{Z}^d \to \mathbb{Z}^{d'}$, $d, d' \geq 1$ which is used to change the positions of neighbors. Note that we are considering a mapping in possibly different dimensional spaces, see the example below. To neighborhood $\nu = (\nu_1, \dots, \nu_n)$, r is applied componentwise. For the resulting neighborhood we write $r\nu$. That is $(\forall i)(r\nu)_i = r(\nu_i)$. See Fig.1.

Lemma 5 *If $(f, \nu) \approx (f', \nu')$, then $(f, r\nu) \approx (f', r\nu')$.*

Proof. For a proof by contradiction assume, that $(f, r\nu) \not\approx (f', r\nu')$. Denote the corresponding global functions by F_r and F'_r. Then there is a configuration c_r, such that $F_r(c_r) \neq F'_r(c_r)$. Without loss of generality, we assume $F_r(c_r)(0) \neq F'_r(c_r)(0)$.

Define a configuration c as $c(x) = c_r(r(x))$ for all $x \in \mathbb{Z}^d$. We claim that $F(c_r)(0) \neq F'(c_r)(0)$, i.e.

$(f,\nu) \not\approx (f',\nu')$.

$$
\begin{aligned}
F(c)(0) &= f(c(\nu_1),\ldots,c(\nu_n)) \\
&= f(c_r(r(\nu_1)),\ldots,c_r(r(\nu_n))) \\
&= f(c_r((r\nu)_1),\ldots,c_r((r\nu)_n)) \\
&= F_r(c_r)(0) \\
&\neq F'_r(c_r)(0) \\
&= \ldots \\
&\vdots \\
&= F'(c)(0)
\end{aligned}
$$

□

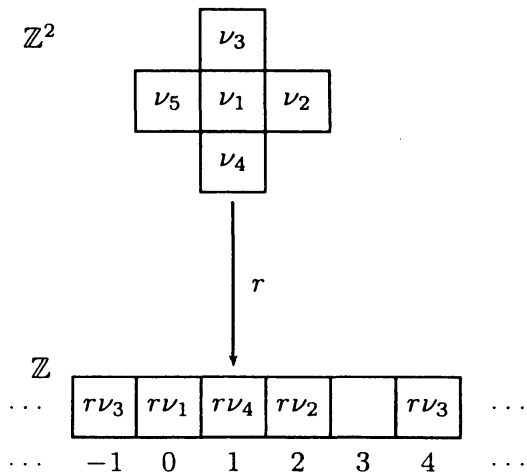

Figure 1: Mapping of von Neumann neighborhood $r : \mathbb{Z}^2 \longrightarrow \mathbb{Z}$.

Example 2 *Consider an injective map r from $\mathbb{Z}^2$ to $\mathbb{Z}$. r is defined by 4 partial maps r_I, r_{II}, r_{III} and r_{IV} as given below, each of which maps (I) the first quarter ($x \geq 0, y \geq 0$), (II) the second quarter ($x \geq 0, y < 0$), (III) the 3rd quarter ($x < 0, y < 0$) and (IV) the 4th quarter ($x < 0, y \geq 0$) into (I) nonnegative even, (II) positive odd, (III) negative even and (IV) negative odd integers, respectively. Note that $r_I(0,0) = 0$. It is also seen that r is surjective and therefore bijective.*

$$
\begin{aligned}
r_I(x,y) &= (x+y)(x+y+1)+2y, \text{ where } x \geq 0, y \geq 0. &(7)\\
r_{II}(x,y) &= (x-y)(x-y-1)-2y-1, \text{ where } x \geq 0, y < 0. &(8)\\
r_{III}(x,y) &= -\{(x+y+1)(x+y+2)-2y\}, \text{ where } x < 0, y < 0. &(9)\\
r_{IV}(x,y) &= -\{(x-y)(x-y+1)+2y+1\}, \text{ where } x < 0, y \geq 0. &(10)
\end{aligned}
$$

By this r, for instance the 2-dimensional von Neumann neighborhood $((0,0),(1,0),(0,1),(0,-1),(-1,0))$ is mapped to 1-dimensional neighborhood $(0,2,4,1,-1)$ as illustrated in Fig.1.

Of course, as noticed above this example of $r : \mathbb{Z}^2 \longrightarrow \mathbb{Z}$ is independent from the decidability issue of reversibility: reversibility is decidable in $\mathbb{Z}$ but not in $\mathbb{Z}^2$.

3 Enumeration of symmetry types of Boolean functions

The equivalence class of Boolean functions defined below is called a symmetry type and the enumeration problem of the number of symmetry types (equivalence classes) was generally solved (for arbitrary n) by D. Slepian (1953)[4] and M. Harrison (1963) [5] by use of Pólya's enumeration theorem (1937)[6]. One of their motivations for such a classification study is the *cost* of logical designs at the early stage of digital computers. The two circuits in Fig.2 are considered to be of the same cost and the corresponding Boolean functions are classified into one class.

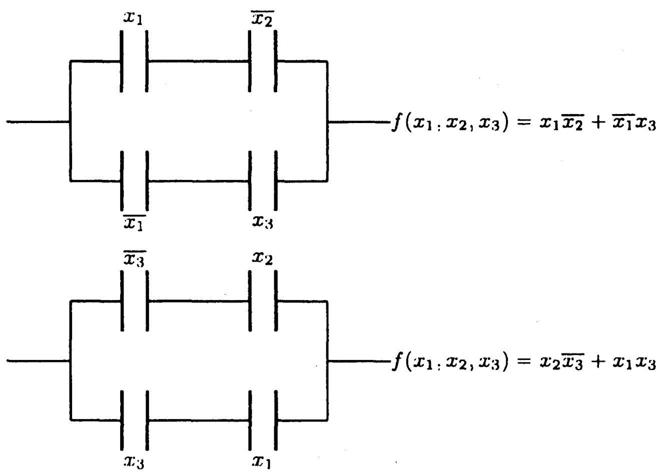

Figure 2: Logical circuits obtained by replacing x_2 by $\overline{x_2}$ and x_1 by $\overline{x_3}$. Remake of Fig.2 of M. Harrison(1963)

3.1 Basics

- Boolean logic: $B = (\{0,1\}, \vee, \wedge, \overline{a})$ with well known derivation rules.
- Boolean function in n variables: $f(x_1, ..., x_n)$.
- Boolean vs polynomial: $a \vee b = a + b + ab, a \wedge b = ab, \overline{a} = 1 + a$.
- Conjugation $\varphi^{-1} f \varphi = 1 + f(1 + x_1, ..., 1 + x_n) = \overline{f(\overline{x_1}\,\overline{x_2} ... \overline{x_n})}$.
- Any n variable Boolean function f_u, $u = 0, ..., 2^{2^n} - 1$ is expressed by a disjunctive normal form:

$$f_u(x_1, ..., x_n) = \sum_{v=0}^{2^n-1} \epsilon_{uv} s_v, \tag{11}$$

where $\epsilon_{uv} \in \{0,1\}$ and $s_0 = x_1x_2...x_n, s_1 = x_1x_2...\overline{x_n}, ..., s_{2^n-1} = \overline{x_1}\,\overline{x_2}...\overline{x_n}$.

3.2 Permutation and negation of Boolean functions

- Permutation of (variables of) a Boolean function is defined in the same way as Definition 3: $f^\pi(x_1, ..., x_n) = f(x_{\pi(1)}, ..., x_{\pi(n)})$. The set of permutations is isomorphic with S_n.
- For expressing a negation of x_i, we use a superfix $x_i^{\alpha_i}$; for $\overline{x_i}$ let $\alpha_i = 1$ and for x_i, let $\alpha_i = 0$.

- A list $\alpha = (\alpha_1, ..., \alpha_n)$ expresses a combined negation of variables of Boolean function $f(x_1, ..., x_n)$: $\alpha f(x_1, ..., x_n) = f(x_1^{\alpha_1}, ..., x_n^{\alpha_n})$.
- The set S_2^n of all αs is a permutation group of order 2^n.

3.3 Equivalence relation defined by (S_n, S_2^n)

The pair $G^n = (S_n, S_2^n)$ of permutation groups S_n and S_2^n naturally defines an equivalence relation $\approx_{G^n}$ among the set of Boolean functions in n variables;

$$f \approx_{G^n} f' \Longleftrightarrow f' = \alpha f^{\pi}, \text{for } \exists \pi \in S_n, \exists \alpha \in S_2^n. \tag{12}$$

Utilizing this relation, we can classify Boolean functions. D. Slepian (1953) uses Pólya's enumeration theorem for getting the number of equivalence classes for any Boolean functions in n variables [4].

Example 3 *Case of $n = 2$: $2^{2^2} = 16$ Boolean functions $f(x, y)$ are classified into 6 equivalence classes:*

$$[0], [1], [x, \overline{x}, y, \overline{y}], [xy, x\overline{y}, \overline{x}y, \overline{x}\,\overline{y}], [x \vee y, \overline{x} \vee y, x \vee \overline{y}, \overline{x} \vee \overline{y}], [x \oplus y, x \equiv y]$$

Case of $n = 3$: 256 Boolean functions are classified into 22 classes, which is compared with 46 in our automorphism classification of ECA.

4 Generalization of the automorphism of CA

Inspired by the above equivalence classes of Boolean functions, we generalize the definition of automorphisms of CA; The states of neighbors ν_i $(i = 1, ..., n)$ of a cell are *permuted independently* and then the function value is computed. The positions of the arguments (the neighbors) are also permuted as before. Formally, we have

Definition 5 *Let $S_q^n = S_q \times \cdots \times S_q$ and $\varphi^{(n)} \in S_q^n$. Denote $G^n = (S_n, S_q^n)$. Then two CA A and B are defined to be automorphic, denoted $A \cong_{G^n} B$, if and only if there are permutations $\pi \in S_n$ and $\varphi^{(n)} \in S_q^n$ such that*

$$(f_B, \nu_B) = (f_A^{\pi} \varphi^{(n)}, \nu_A^{\pi}), \tag{13}$$

where $f_A^{\pi}\varphi^{(n)}$ stands for $f_A^{\pi}(x_1^{\varphi_1}, ..., x_n^{\varphi_n})$, where $x_i^{\varphi_i}$ is a permutation $\varphi_i \in S_q$ of the i-th argument x_i for $1 \leq i \leq n$. In this case we write $\varphi^{(n)} = (\varphi_1, ..., \varphi_n) \in S_q^n$. The case of $q = 2$ is nothing other than the equivalence of Boolean functions.

Another definition will be possible; An additional permutation of states $\varphi' \in S_q$ is applied to the function value.

$$(f_B, \nu_B) = (\varphi' f_A^{\pi} \varphi^{(n)}, \nu_A^{\pi}). \tag{14}$$

If every permutation of the states is equal, i.e. $\varphi_i = \varphi$, $1 \leq i \leq n$, for some $\varphi \in S_q$, the automorphism is same as the original automorphism.

This generalized automorphism is an equivalence relation and induces a classification of CA like the original one. Any two local functions in a class have the same global behavior *up to permutations.* The classification is considered to be a group action of G^n on the set of polynomials $\mathcal{P}_{n,q}$ over $GF(q)$ in n-variables, where the action of a larger group generally gives a smaller number of classes, see [3].

5 Concluding remarks and acknowledgements

In this paper we discussed a generalization of the automorphism classification of CA following the past studies on the symmetry classes of Boolean functions. A motivation for that is to extract the symmetric structure of local functions by *disregarding* the effects of neighborhoods. The number of the generalized automorphism classes will be obtained using the orbit counting lemma and/or Pólya's enumeration theorem as was done for classifying Boolean functions. The computation itself, however, has been left for future work.

The author thanks to Thomas Worsch from the University of Karlsruhe for valuable discussions, particularly for establishing Lemma 5 and to Mitsuhiko Fujio from the Kyushu Institute of Technology for commenting on the résume presented at the RIMS workshop (LA Symposium) held in Kyoto University on February 2, 2010.

References

[1] Nishio, H., Worsch, T.: A note on automorphisms of cellular automata. *kôkyûroku* vol. 1649 (2009) 121-128, RIMS, Kyoto University.

[2] Nishio, H., Worsch, T.: Changing the neighborhood of cellular automata : local structure, equivalence and isomorphism. to appear in J. Cellular Automata.

[3] Nishio, H.: AUTOMORPHISM CLASSIFICATION OF CELLULAR AUTOMATA. In: Proceedings of Workshop on Non-Classical Models for Automata and Applications(NCMA), books@ocg.at. (2009) 195–208

[4] Slepian, D.: On the number of symmetry types of boolean functions of n variables. Canadian J. Math. **5** (1953) 185–193

[5] Harrison, M.A.: The number of transitivity sets of boolean functions. J. Soc. Indust. Appl. Math. **11** (1963) 806–828

[6] Pólya, G., Read, R.C.: Combinatorial Enumeration of Groups, Graphs and Chemical Compounds (English translation). Springer-Verlag (1987)

March 3, 2010