Propositional Logic and Cellular Automata

Shuichi Inokuchi * Toshikazu Ishida † Yasuo Kawahara

1 Introduction

The notion of cellular automata was introduced by von Neumann [8] and Ulam [12] as theoretical model to demonstrate a system capable of self-reproduction and universal computation. In the 1980s Wolfram [13] engaged in a study of elementary cellular automata and classified them into four classes. He claimed that the fourth class are thought to be computationally universal and in 2004 Cook proved that CA-110 is Turing-complete, and the importance of analysis of one dimensional we re-recognized. One dimensional cellular automata have been investigated by many researchers and one of important properties which should be studied is reversibility(surjectivity). Moore [6] and Myhill [7] proved the Garden-of-Eden theorem which states that a cellular automaton is locally injective if and only if it is surjective. Richardson [10] showed that the inverse dynamics of deterministic cellular automata can be described by another cellular automata if and only if it is reversible. Nobe and Yura [9], Inokuchi et. al. [4] showed the reversibility of one dimensional cellular automta with finite cell array. Hagiya et. al. [3] proposed the analyzing method of cellular automata using abstraction by temporal logic. And also researches on cellular automata on groups have been published. Sato [11] introduced group structured linear cellular automata and the star operation of local transition rules. Yukita [14] investigated the surjectivity of cellular automata on groups. Fujio [2] and Inokuchi et. al. [5] studied the composition of cellular automata on groups, and Ceccherini-Silberstein and Coornaert [1] summerized cellular automata and groups.

In the paper we mention an analogy of propositional logic and 2-state cellular automata on groups. The following analogy between them mentioned in the paper must be recognized by quit a lot of readers.

Many researchers on cellular automata so far understood that local rules are equivalent to formulae, because local rules are boolean functions of finite variables. However they might not make use of formulae to define transition functions. The main idea of the paper is to redefine transition functions with formulae and their truth values.

In section 2 and 3 we recall propositional logic and the usual definition of cellular automata on groups. In section 4 we deal with formulae and define multiplication of formulae, and we redefine the transition function wing formulae on groups in section 5. In section 6 we introduce some examples of reversible formulae.

2 Propositional logic

First we recall the fundamentals on propositional logic to emerge analogy of propositional logic and CA theory.

^{*}Faculty of Mathematics, Kyushu University, Japan.

[†]Center for Fundamental Education, Kyushu Sangyo University, Japan.

Let Φ be a set of propositional variables (or atomic propositions), and \bot and \to logical symbols. Formulae on Φ are inductively defined by BNF:

$$A ::= v \mid \bot \mid A \to A \quad (v \in \Phi)$$

Other logical symbols are introduced by the usual abbreviations.

Negation: $\neg A = A \rightarrow \bot$ Verum: $\top = \neg \bot$

Disjunction: $A \lor B = \neg A \to B$ Conjunction: $A \land B = \neg (A \to \neg B)$

Equivalence: $A \leftrightarrow B = (A \rightarrow B) \land (B \rightarrow A)$

Exclusive or: $A + B = \neg (A \leftrightarrow B)$.

The set of all formulae on Φ will be denoted by F_{Φ} .

Let $Q = \{0, 1\}$ be the set of truth values. The implication operator \Rightarrow on Q is defined as follows.

$$0 \Rightarrow 0 = 1$$
, $0 \Rightarrow 1 = 1$, $1 \Rightarrow 1 = 1$, $1 \Rightarrow 0 = 0$.

Operations \neg , \lor , \land , \Leftrightarrow , + (XOR, addition modulo 2) on Q are defined by the same way as the above abbreviations.

Definition 2.1 A valuation (interpretation) m of a set Φ is a function $m: \Phi \to Q$. The truth value $m[\![A]\!] \in Q$ of a formula A for m is inductively defined as follows.

- (a) m[v] = m(v) for all $v \in \Phi$.
- (b) $m[\![\bot]\!] = 0$
- (c) $m[A \to B] = m[A] \Rightarrow m[B]$.

For two formulae A and B we write as A = B, if m[A] = m[B] for all valuations $m : \Phi \to Q$.

Proposition 2.2 Let A, B, C be formulae on Φ . Then

- (a) $A \vee B = B \vee A$, $(A \vee B) \vee C = A \vee (B \vee C)$, $A \vee A = A$
- (b) $A \wedge B = B \wedge A$, $(A \wedge B) \wedge C = A \wedge (B \wedge C)$, $A \wedge A = A$
- (c) A + B = B + A, (A + B) + C = A + (B + C),
- (d) $\neg(\neg A) = A$, $\neg(A \lor B) = \neg A \land \neg B$, $\neg(A \land B) = \neg A \lor \neg B$
- (e) $A + A = \bot$, $A + \bot = A$, $\neg A = A + \top$

3 CA on groups

In this section we review the usual definition of 2-state CA on groups.

Let G be a group with a unit element e and $Q = \{0, 1\}$ the set of states. A function $m : G \to Q$ is called a configuration on G. We denote by Q^G the set of all configurations $m : G \to Q$.

Definition 3.1 For a configuration $m \in Q^G$ and $a \in G$ the *shifted* configurations $am, ma \in Q^G$ are defined as follows:

$$(am)(x) = m(a^{-1}x)$$
 and $(ma)(x) = m(xa^{-1})$

for all $x \in G$.

The following states the basic properties of shifted configurations.

Proposition 3.2 Let $m \in Q^G$ and $a, b \in G$. Then

- (a) em = m, me = m
- (b) $(ab)m = a(bm), \quad m(ab) = (ma)b.$

For a configuration $m \in Q^G$ and a subset V of G the restricted configuration $m|_V \in Q^V$ is defined by $\forall x \in V$. $(m|_V)(x) = m(x)$. Let N be a finite subset of G. A function $f: Q^N \to Q$ is called a local rule on a neighborhood N.

Definition 3.3 For a local rule $f: Q^N \to Q$ a function $T_f: Q^G \to Q^G$ is defined by

$$T_f(m)(x) = f(x^{-1}m|_N)$$

for all $m \in G^G$ and $x \in G$. The function T_f is called the transition function defined by f.

The transition function T_f is often called a *cellular automaton* (CA) on a group G.

4 Formulae on groups

4.1 Shifted formulae

To redefine transition functions of CA using formulae on groups, shifted formulae will be introduced by making use of multiplication of groups.

Let G be a group with a unit element e. The set of all formulae on G will be denoted by F_G .

Definition 4.1 For $A \in F_G$ and $a \in G$, the shifted formula $aA \in F_G$ is inductively defined as follows:

- (a) $av \in G$
- (b) $a \perp = \perp$
- (c) $a(A \to B) = aA \to aB$.

The following states the basic properties of shifted formulae.

Proposition 4.2 Let A, B be a formula on a group G, and $a, b \in G$. Then

- (a) eA = A
- (b) (ab)A = a(bA)
- (c) $a(\neg A) = \neg(aA)$
- (d) $a(A \lor B) = aA \lor aB$
- (e) $a(A \wedge B) = aA \wedge aB$
- (f) a(A+B) = aA + aB.

The following proposition is for valuation of a formula A for shifted configuration ma and am.

Proposition 4.3 Let $a \in G$, $m \in Q^G$ and $A \in F_G$. Then

- (a) $(am)[A] = m[a^{-1}A]$
- (b) $(ma)[A] = m[Aa^{-1}]$

4.2 Multiplication of formulae

Using the group action the multiplication of formulae can be defined as well as shifted formulae. In the next section it turns out that the multiplication of formulae dominates the composition of transition functions of CA on groups.

Definition 4.4 Let A and C be formulae on a group G. The multiplication AC of A and C is inductively defined as follows.

- (a) vC (shifted formula) is already defined.
- (b) $\perp C = \perp$
- (c) $(A \rightarrow B)C = AC \rightarrow BC$.

The following states the basic properties of the multiplication of formulae.

Proposition 4.5 Let A, B, C be formulae on a group G and $a, b \in G$. Then

- (a) Ae = A, A(ab) = (Aa)b
- (b) Either $A \perp = \perp$ or $A \perp = \top$.
- (c) $(\neg A)B = \neg (AB)$
- (d) $(A \lor B)C = AC \lor BC$
- (e) $(A \wedge B)C = AC \wedge BC$
- (f) (A+B)C = AC + BC
- (g) (AB)C = A(BC).

Remark. The following eqations need not hold.

- $A(B \to C) = AB \to AC$
- $A(B \lor C) = AB \lor AC$
- $A(B \wedge C) = AB \wedge AC$
- \bullet A(B+C)=AB+AC

Applying multiplication of formulae Fujio's example [2] is simply described as follows. Let $x \in G$.

$$(e+x)(x^{-1}+e) = e(x^{-1}+e) + x(x^{-1}+e) \{ 4.5 (f) \}$$

$$= (x^{-1}+e) + (e+x) \{ 4.2 (f) \}$$

$$= x^{-1} + x. \{ 2.2 (b) A + A = \bot \}$$

Let A be a formula A on a group. The power A^n $(n \ge 0)$ of A is defined as follows:

$$A^0 = e, \qquad A^{n+1} = A^n A.$$

For example we have

- $(e \wedge x)^n = e \wedge x \wedge x^2 \wedge \cdots \wedge x^{n-1} \wedge x^n$
- $\bullet \ (e \lor x)^n = e \lor x \lor x^2 \lor \dots \lor x^{n-1} \lor x^n$
- \bullet $(e \to x)^n = x^{n-1} \to x^n$
- $(e \wedge \neg x)^2 = e \wedge \neg x$.

If G is commutative, then Ax = xA holds for all $x \in G$.

5 New definition of transition functions

Following the analogy of propositional logic and CA we redefine the transition functions of CA using valuation of formulae.

Definition 5.1 For a formula $A \in F_G$ define a function $T_A : Q^G \to Q^G$ by

$$T_A(m)(x) = m[xA]$$

for all $m \in G^G$ and $x \in G$. The function T_A is called the transition function defined by A.

For $q \in Q$ the constant configuration $m \in Q^G$ such that m(v) = q for all atomic propositions $v \in G$ will be denoted by \hat{q} .

Proposition 5.2 Let $v, x, a \in G$, $m \in Q^G$ and $A, B \in F_G$. Then

- (a) $T_v(m) = mv^{-1}$
- (b) $T_{\perp}(m) = \hat{0}$
- (c) If $T_A = T_B$, then A = B.
- (d) $T_A(am) = a(T_A(m))$
- (e) $T_A(ma) = T_{Aa^{-1}}(m)$.
- (f) $T_{A\to B}(m)(x) = T_A(m)(x) \Rightarrow T_B(m)(x)$
- (g) $T_{\neg A}(m)(x) = \neg (T_A(m)(x))$
- (h) $T_{A \lor B}(m)(x) = T_A(m)(x) \lor T_B(m)(x)$
- (i) $T_{A \wedge B}(m)(x) = T_A(m)(x) \wedge T_B(m)(x)$
- (j) $T_{A+B}(m)(x) = T_A(m)(x) + T_B(m)(x)$.

The composition $S \circ T$ of a function $T: Q^G \to Q^G$ followed by a function $S: Q^G \to Q^G$ is defined as usual:

$$\forall m \in Q^G. \ (S \circ T)(m) = S(T(m)).$$

Although the composition of transition functions of CA is intractable to describe with the traditional definition using local rules $f: Q^N \to Q$. However, the multiplication of formulae directly corresponds to the composition of transition functions. The next theorem is a main result of the paper.

Theorem 5.3 For all formulae $A, B \in F_G$ the identity $T_A \circ T_B = T_{AB}$ holds.

Proof. We need to show the following.

- (a) $T_v \circ T_C = T_{vC}$
- (b) $T_{\perp} \circ T_C = T_{\perp C}$
- (c) $T_{A\to B} \circ T_C = T_{(A\to B)C}$.

(a)
$$T_{v} \circ T_{C} = T_{vC}$$
:
$$(T_{v} \circ T_{C})(m)(x) = T_{v}(T_{C}(m))(x)$$

$$= (T_{C}(m)v^{-1})(x) \{ 5.2 \text{ (a) } \}$$

$$= T_{C}(m)(xv) \{ 3.1 \}$$

$$= m[(xv)C] \{ 5.1 \}$$

$$= m[x(vC)] \{ 4.5 \text{ (b) } \}$$

$$= T_{vC}(m)(x). \{ 5.1 \}$$
(b) $T_{\perp} \circ T_{C} = T_{\perp}$:
$$(T_{\perp} \circ T_{C})(m) = T_{\perp}(T_{C}(m))$$

$$= \hat{0} \{ 5.2 \text{ (b) } \}$$

$$= T_{\perp}(m).$$
(c) $T_{A \to B} \circ T_{C} = T_{(A \to B)C}$:
$$(T_{A \to B} \circ T_{C})(m)(x)$$

$$= T_{A \to B}(T_{C}(m))(x)$$

 $= T_{A\to B}(T_C(m))(x)$ $= T_A(T_C(m))(x) \Rightarrow T_B(T_C(m))(x) \qquad \{ 5.2 \text{ (f) } \}$ $= (T_A \circ T_C)(m)(x) \Rightarrow (T_B \circ T_C)(m)(x)$ $= T_{AC}(m)(x) \Rightarrow T_{BC}(m)(x) \qquad \{ \text{ IH } \}$ $= T_{AC\to BC}(m)(x) \qquad \{ 5.2 \text{ (f) } \}$ $= T_{AC\to BC}(m)(x) \qquad \{ 4.4 \text{ (c) } \}$

This completes the proof.

6 Reversibility

6.1 Reversibility of formulae

By the virtue of the last theorem 5.3 the reversibility of transition functions can be converted to a condition for formulae. A formula A on a group G is reversible if there exists a formula B such that AB = e and BA = e.

Corollary 6.1 Let A, B and C be formulae on a group G. Then

- (a) If A is reversible, then $T_A: Q^G \to Q^G$ is reversible.
- (b) If AB = e and CA = e, then B = C.
- (c) A and B are reversible iff so are AB and BA.
- (d) If $AC = \bot$, $C \neq \bot$ and $C \neq \top$, then A is not reversible.

Proof. (a) It is trivial by proposition 5.2 and the last theorem 5.3.

(b) Assume AB = e and CA = e. Then

$$B = eB$$

= $(CA)B$ { $CA = e$ }
= $C(AB)$ { $4.5(g)$ }
= Ce { $AB = e$ }
= C . { $4.5(a)$ }

- (c) Assume that AB and BA are reversible. Then ABD = e and EBA = e hold for some formulae D and E. By (a) we have BD = EB, which implies that A is reversible.
- (d) Assume DA = e for some formula D. Then we have $C = eC = (DA)C = D(AC) = D\bot$. Hence $C = \bot$ or $C = \top$ by 4.5 (b). This contradicts the assumption.

Remark. The single condition $AC = \bot$ does not always imply that A is not reversible. $(e\bot = \bot)$

6.2 Examples of reversible formulae

In this section we give several examples of formulae which induce reversible transition functions.

Proposition 6.2 For $x \in G$ both x and $\neg x$ are reversible.

Proof.
$$xx^{-1} = x^{-1}x = e$$
 and $(\neg x)(\neg x^{-1}) = \neg (x \neg x^{-1}) = \neg \neg (xx^{-1}) = e$.

A polynomial is a formula constructed by powers of an element of G and exclusive or +. Formally polynomials of $x \in G$ are defined as follows.

- (a) Every power x^n is a polynomial (monomial) of x for all integers n.
- (b) If A and B are polynomials of x, then A + B is a polynomial of x.

For example, $e + x^2$, $x + x^2 + x^{-2}$ and $e + e = \bot$ are polynomials of x. But \top is not a polynomial.

Polynomials satisfy the following useful properties.

Proposition 6.3 Let A, B, C be formulae on a group G and $x \in G$. Then

- (a) If A is a polynomial of x, then $A \perp = \perp$.
- (b) If A, B and C are polynomials of x, then A(B+C) = AB + AC.
- (c) If A and B are polynomials of x, then AB is a polynomial of x.
- (d) If A and B are polynomials of x, then AB = BA.
- (e) If A is a polynomial of x and $x^n = e$ for some integer $n \ge 1$, then A(e + x) is not reversible.
- (f) If $x^n = e$ for some integer $n \ge 1$, then $e + x + \cdots + x^{2k} + x^{2k+1}$ is not reversible for all natural numbers k.

Proposition 6.4 Let $x \in G$. If $x^n = e$ for a positive integer $n \neq 0 \pmod{3}$, then the polynomial $A = e + x + x^2$ is reversible.

Proof. In the case of n = 3k - 1. First note that $(e + x)A = e + x^3$. Set $B = e + \sum_{j=1}^{k-1} x^{3j-1}(e + x)$. Then

$$\begin{array}{lll} BA & = & A + \sum_{j=1}^{k-1} x^{3j-1}(e+x)A \\ & = & A + \sum_{j=1}^{k-1} x^{3j-1}(e+x^3) \\ & = & A + x^2 + x^{3k-1} \\ & = & e + x + x^2 + x^2 + x^{3k-1} \\ & = & x. \end{array} \qquad \left\{ \begin{array}{ll} (e+x)A = e + x^3 \end{array} \right\}$$

In the case of n = 3k - 2. Set $B = x^{3k} + \sum_{j=1}^{k-1} x^{3j-3}(e+x)$. Then

$$BA = x^{3k}A + \sum_{j=1}^{k-1} x^{3j-3}(e+x)A$$

$$= x^{3k}A + \sum_{j=1}^{j-1} x^{3j-3}(e+x^3) \qquad \{ (e+x)A = e+x^3 \}$$

$$= x^{3k-3}A + e + x^{3k-3}$$

$$= x^{3k-3} + x^{3k-2} + x^{3k-1} + e + x^{3k-3}$$

$$= x. \qquad \{ x^{3k-2} = e \}$$

This completes the proof.

The polynomial $A=e+x+x^2$ extends the local rule with Wolfram number 150 for 3-neighborhood local rules.

Rule No.	111	110	101	100	011	010	001	000
Tule No.	111	110	101	100	011	010	001	000
150	1	0	0	1	0	1	1	0

Remark. If $x^{3k} = e$, then the polynomial $A = e + x + x^2$ is not reversible. Set $B = \sum_{j=1}^k x^{3j-2}(e+x)$. Then

$$BA = \sum_{j=1}^{k} x^{3j-2} (e+x) A$$

$$= \sum_{j=1}^{k} x^{3j-2} (e+x^3) \quad \{ (e+x) A = e+x^3 \}$$

$$= x + x^{3k+1}$$

$$= \bot, \qquad \{ x^{3k+1} = x \}$$

which shows that $AB = \bot$ and $A = e + x + x^2$ is not reversible.

Proposition 6.5 Let $x \in G$. If $x^{15k-1} = e$ for a positive integer k > 0, then the polynomial $A = e + x + x^2 + x^3 + x^4$ is reversible.

Proof. Assume that $x^{5k'-1} = e$ for a positive integer k' and set $C = e + \sum_{j=1}^{k'-1} x^{5j-1} (e+x)$. Then

$$CA = A + \sum_{j=1}^{k'-1} x^{5j-1} (e+x) A$$

$$= A + \sum_{j=1}^{k'-1} x^{5j-1} (e+x^5) \qquad \{ (e+x) A = e+x^5 \}$$

$$= A + x^4 + x^{5k'-1}$$

$$= e + x + x^2 + x^3 + x^4 + x^4 + x^{5k'-1}$$

$$= x + x^2 + x^3$$

$$= (e+x+x^2)x.$$

$$\{ x^{5k'-1} = e \}$$

From Prop. 6.4 if $x^{3h-1} = e$ for some positive integer h then the polynomial $(e + x + x^2)$ is reversible. Hence if $x^{15k-1} = e$ then the polynomial A is reversible.

Finally we show a reversible formula that is not a polynomial.

Lemma 6.6 Let $A = (\neg e \land x) + x^2$ be a formula on a group. Then the identity

$$A^{2^k} = (\neg e \land B_k) + x^{2^{k+1}}$$

holds for all natural numbers k, where $B_k = x \wedge x^3 \wedge x^5 \wedge \cdots \wedge x^{2^{k+1}-1}$.

Corollary 6.7 If $x^{2n-1} = e$ for an integer $n \ge 2$, then the formula $A = (\neg e \land x) + x^2$ is reversible.

Proof. In the previous lemma 6.6 we have seen that the identity

$$A^{2^{k-1}} = (\neg e \land B_{k-1}) + x^{2^k}$$

holds for all integers $k \ge 1$. Take a unique integer k such that $2^{k-1} < 2n-1 < 2^k$. Then $2 \le n \le 2^{k-1}$ and so $\neg e \wedge x^{2n-1} = \neg e \wedge e = \bot$. Hence we have

$$\begin{array}{rcl} A^{2^{k-1}} & = & (\neg e \wedge B_{k-1}) + x^{2^k} \\ & = & x^{2^k}, & \{ \neg e \wedge x^{2n-1} = \bot \} \end{array}$$

which proves the statement.

The formula $A = (\neg e \land x) + x^2$ extends the local rule with Wolfram number 166 (or 154, 180, 210) for 3-neighborhood local rules.

Rule No.	111	110	101	100	011	010	001	000
166	1	0	1	0	0	1	1	0

7 Conclusion

We mentioned the analogy of cellular automata and propositional logic, and defined the multipication of formulae and the transition function of cellular automata using valuation of formulae. And we showed that a formula on a group represents a local rule of CA and that the multiplication of formulae on a group determines the composition of transition functions. Also we defined the reversibility of a formula and proved that if a formula is reversible then the transition function for it is reversible.

References

- [1] T. Ceccherini-Silberstein and M. Coornaert, Cellular automata and groups, Springer, 2010.
- [2] M. Fujio, XOR²=90: Graded algebra structure of the Boolean algebra of local transition rules, 数 理解析研究所講究録、1599: 97 102, 2008.
- [3] M. Hagiya, K. Takahashi, M. Yamamoto and T. Sato, Analysis of Synchronous and Asynchronous Cellular Automata Using Abstraction by Temporal Logic, Functional and Logic Programming, LNCS 2998, 7–21, 2004.
- [4] S. Inokuchi, K. Honda, H. Lee, T. Sato, Y. Mizoguchi, Y. Kawahara, On reversible cellular automata with finite cell array, Proc. of Fourth International Conference on Unconventional Computation, LNCS 3699, 2005.
- [5] S. Inokuchi, T. Ito, M. Fujio and Y. Mizoguchi, A Formulation of Composition for Cellular Automata on Groups, accepted in IEICE transactions on Information and Systems.
- [6] E. F. Moore, Machine models of self-reproduction, Proc. Sympos. Appl. Math. AMS 14, 17 33, 1962.
- [7] J. Myhill, The converse of Moore's GOE theorem, Proc. AMS 14, 685 686, 1963.
- [8] J. von Neumann, The Theory of Self-Reproducing Automata (A. Burks ed.), University of Illinois Press, 1996.
- [9] A. Nobe and F. Yura, On reversibility of cellular automata with periodic boundary conditions, Journal of Physics A: Mathematical and General 37, 5789 5804, 2004.
- [10] D. Richardson, Tessellations with local transformations, J. Computer and System Sciences 6, 373 - 388, 1972.
- [11] T. Sato, Group structured linear cellular automata over \mathbf{Z}_m , Journal of Computer and System Sciences, 49, 18–23, 1994.
- [12] S. Ulam, Processes and Transformations, Proc. Int. Cong. Mathem. 2, 264–275, 1952.
- [13] S. Wolfram, A new kind of science, Wolfram Media, 2002.
- [14] S. Yukita, Dynamics of Cellular Automata on Groups, IEICE transactions on information and systems E82-D(10), 1316-1323, 1999.