数理解析研究所講究録
1166 巻 2000 年 200-206

Global Dynamics of 1-D Extended Cellular Automata

Hidenosuke Nishio 西尾英之助
Iwakura Miyake-cho 204, Sakyo-ku, Kyoto, Japan
E-mail: YRA05762@nifty.ne.jp

Abstract

Following our algebraic method for investigating information transmission in CA, the global dynamics of the extended CA[X] is studied in relation to that of CA. Computer simulations of 1-D finite cyclic CAs are also presented.

1 Preliminaries

The 1-D CA is defined as usual with the space Z (the set of integers), the neighborhood index N, the state set Q and the local function f and denoted as CA=(Z,N,Q,f). Throughout this paper we assume the 1-D CA with N=(−1,0,+1) and denote simply as CA=(Q,f).

State Set
Q is assumed to be a finite field. Thus Q=GF(q), where $q = p^n$ with prime p and positive integer n. Denote the cardinality of Q as $|Q|$. So $|Q| = q = p^n$.

Local Function
The local function $f : Q \times Q \times Q \to Q$ can be expressed as follows:

$$f(x,y,z) = u_1x^{q-1}y^{q-1}z^{q-1} + u_2x^{q-1}y^{q-1}z^{q-2} + u_3x^{q-1}y^{q-2}z^{q-1} + \cdots + u_{q^3-1}z + u_{q^3}, \ \mathit{where}\ u_i \in Q\ (1 \le i \le q^3). \quad (1)$$

x, y and z assume the state values of the neighboring cells −1(left), 0(center) and +1(right), respectively.

Global Map
The configuration set $C = Q^Z$ and the global map $F : C \to C$ are defined as usual. When a CA is 1-D finite CA of length $n \ge 1$, its configuration is a

word $w \in Q^n$. We confuse the terminologies *word* and *configuration* for the finite and the infinite CAs.

2 Extension of CA

2.1 Information Expressed by X

Let X be a symbol different from those used in equation (1). It stands for an unknown state or the *information* of the cell in CA. We explain first the role of X in the information transmission of the local function using an example.

Example 1.
The binary set $Q = \{0, 1\}$=GF(2) and the function $f(x, y, z) = yz + x$.

From the fact that $f(0, 0, 0) = 0$ and $f(1, 0, 0) = 1$, we may write as $f(X, 0, 0) = X$ (i). Similarly we write $f(X, 1, 1) = X + 1 \pmod 2$ (ii), which comes from the fact that $f(0, 1, 1) = 1$ and $f(1, 1, 1) = 0$. Also we have $f(X, 1, 0) = 1$ from $f(0, 1, 0) = 1$ and $f(1, 1, 0) = 1$ (iii). From the information related point of view, we claim: in cases (i) and (ii) the information X is transmitted to the right, but in case (iii), it vanishes. Note that from the function $X + 1$(a permutation of Q) we can restore the value of X without any loss of information.

In generalizing the above argument, we consider another polynomial form, which will be called the *information function.*

$$g(X) = a_1 X^{q-1} + a_2 X^{q-2} + \cdots + a_q, \text{ where } a_i \in Q \ (1 \leq i \leq q). \quad (2)$$

g defines a function $Q \to Q$ and the set of such functions is denoted by $Q[X]$. Evidently $|Q[X]|$=q^q. Note that $Q[X] \supset Q$. The element of $Q[X] \setminus Q$ is called *informative*, while that of Q *constant.*

The polynomial $g(X) \in Q[X]$ is uniquely expressed in the form of *coefficent vector* $(a_1, a_2, ..., a_q)$, which is particularly useful for the computer simulation.

When g is a permutaion function of Q, its function value, say a, has a unique preimage $g^{-1}(a)$ in the domain Q. Thus a permutation function completely conserves the information of the domain. When g is a constant, however, we can not obatin any information about preimages from the function value. There are intermediate stages of information amount contained by the information function g. The greater the cardinality of the value set $g(Q)$ is, the greater the information amount is.

2.2 Ring $Q[X]$

The set of information functions $Q[X]$ is characterized as follows. Let $P[X]$ be the polynomial ring over a finite field Q with an indeterminate X. $Q[X]$ be its factor ring by $X^q - X$, i.e. $Q[X] = P[X]/(X^q - X)$. Note that $X^q - X = X(X^{q-1} - 1)$ is a reducible polynomial in $P[X]$. Therefore $Q[X]$ is not a field but a commutaitive ring with identity[Lidle,et.al.97].

2.3 Extended CA

We define an extended CA[X]=$(Q[X], f)$, where $Q[X]$ is the set of cell states. The local function f is expressed by the same polynomial form f as in (Q, f). The variables x,y and z, however, move in $Q[X]$ instead of Q. That is, $f : Q[X]^3 \to Q[X]$. The global map is $F : Q[X]^Z \to Q[X]^Z$. A configuration is called *informative* if a cell state of the configuration is informative. Otherwise it is *constant.* When a CA[X] starts with a constant configuration, its trajectory always behaves in Q^Z.

3 Global Dynamics of CA[X]

3.1 Generalities

We investigate the dynamics of a CA[X] in relation to that of CA. Such notions as *injectivity, surjectivity, reversibility, limit sets* and so on are defined and analysed in CA[X] as well.

Substitution
Let a configuration of CA[X] be $w \in Q[X]^Z$. For any $a \in Q$, the word obtained from w by substituting a for the variable X of each cell state $g(X)$ is denoted by w_a. If w is a constant configuration, then by definition $w_a = w$. Substitution is expressed by the (many to one) mapping ψ_a: $w \mapsto w_a$ or $\psi_a(w) = w_a$ for any $a \in Q$.

Example 2. $q = 3$. GF(3)={0,1,2}. $n = 5$.
If $w = X, 1, X^2 + 1, 0, 0$, then $w_0 = 0, 1, 1, 0, 0, w_1 = 1, 1, 2, 0, 0$ and $w_2 = 2, 1, 2, 0, 0$.

Proposition 1.
(1) CA$[X]$ is injective, if and only if CA is injective.
(2) CA$[X]$ is surjective, if and only if CA is surjective.

Proof.
(1) If CA is injective, then for any $a \in Q$ and any pair of distinct configurations w and v, we have $F(w_a) \neq F(v_a)$. Therefore we have $F(w) \neq F(v)$, i.e. CA[X] is injective. The only if part is obvious.
(2) Let c_X be an arbitrary configuration of $Q[X]^Z$. Since CA is surjective, for any $a \in Q$, there is a constant configuration w such that $F(w) = c_a$. Therefore there is an informative configuration $c'_X \in Q[X]^Z$ such that $\psi_a(c'_X) = w$ and $F(c'_X) = c_X$. So we have the if part of (2). □

In addition to the above *mathematical* properties pertaining to the global map F, we consider the *informational* properties of CA dynamics. Among others we are interested in the information transmission ability of CAs. When a CA$[X]$ starts with an initial configuration vXw where v and w are constants, the information of X is generally transmitted to the right and left or to the *space direction.* If the trajectory of a CA$[X]$ contains informative configurations forever, then the information is called to be transmitted to the *time direction* without end.

The following proposition is a consequence of Kari's results[Kari94].

Propositon 2.
It is not decidable, whether or not a CA[X] enters a limit set consisting of constant configurations after starting with an initial configuration wXv, where w and v are constant.

The proposition means that as for an arbitrary 1-D CA the ultimate ability of information transmission to the time direction is undecidable[see Nishio99].

A local function f is called *permutive in x*, if $f(Q, y, z) = Q$ for any values of y and z. Similarly permutativity in y (and z) is defined[Hedlund70][Fagnani,et.al.98]. Then we have the following simple result. .

Proposition 3.
If a CA is permutive in x or z, then the information is transmitted without end to the space direction.

Proposition 4.
It is undecidable, whether or not a CA$[X]$ transmits the information X to the space direction without end.

Proof.
It was proved undecidable for finite fixed boundary CAs[see Nishio99]. Modification of the proof to fit with infinite CAs is easy.

3.2 Finite CA

Consider a finite CA=(Q, f, n, B) where $n \geq 1$ is the number of cells and B is the boundary condition, *cyclic, fixed* and others. Note that the following discussion is not sensitive to the boundary condition.

Cycle and Transient
When a CA starts with a configuration w, its trajectory consists of the finite transient $t(w)$ and the cycle $p(w)$, which follows the transient and repeates itself forever. The lengths of the cycle and the transient are denoted by $\phi(w)$ and $\tau(w)$, respectively.

Computer simulations are shown in **Appendix** for a three state cyclic CA$[X]$. The system starts with an informative configuration $w = X11111$ in (A) and enters the cycle of length 12 after the tansient of lenght 2. In (B),(C) and (D) it starts with constants $\psi_0(w), \psi_1(w)$ and $\psi_2(w)$, respectively. Note that $\phi(w) = 12 = LCM\{4, 1, 3\}$.

Proposition 5.
(1) $\phi(w) = LCM\{\phi(w_a) \mid a \in Q\}$.
(2) $\tau(w) = MAX\{\tau(w_a) \mid a \in Q\}$.

Proof.
The information function $g(X)$ can be represented by a *q-tuple* of constant vectors $(0, 0, 0, ..., 0, b_i), b_i \in Q, 1 \leq i \leq q$. In fact $b_i = g(a_i)$ and conversely from a set of q values b_i, $1 \leq i \leq q$, one can uniquly compute the set of coefficients a_is which gives $g(X)$. Consequently the dynamics of CA$[X]$ is faithfully simulated by computing separately each dynamics of CA and considering their *q-tuples*.
(1) If the trajectory of CA starting with w_a has the cycle length $\phi(w_a)$, then the trajectory of *q-tuples* of the coefficent vectors has the cycle length of a multiple of each $\phi(w_a)$. It is in fact equal to $LCM\{\phi(w_a)|a \in Q\}$.
(2) When every trajectoy of CAs enter the cycle, the *q-tuples* also become cyclic. Therefore we have (2) of the proposition. □

We state the following proposition without proof.

Proposition 6.
$\phi(w) = \phi(w_a)$ for any $a \in Q$, if and only if CA$[X]$ enters a cycle consiting

of constant configurations.

Concluding Remarks

The idea has been presented for the basic 1-D CA, though it works for general CAs. The decision problems we treated above asks if or not *any* information is transmitted. The problem asking *how much* information is transmitted is left for further reseach. Thanks are due to Takashi Saito for writing the simulation program of 1-D finite CA[X]s with the language DrScheme.

References

[Fagnani, et.al.98] F.Fagnani and L.Margara, Expansivility, Permutivity, and Chaos for Cellular Automata. *Theory of Computing Systems*, Vol.31, 663-677 (1998)

[Garzon95] M.Garzon,*Models of Massive Parallelism, Analysis of Cellular Automata and Neural Networks*,Springer, 1995.

[Hedlund70] G.A.Hedlund, Endomorphism and Automorphism of the Shift Dynamical System. *Mathematical System Theory*, Vol.3,No.4, 320-375(1970).

[Kari94] J.Kari, Rice's theorem for the limit sets of cellular automata. *Theoretical Computer Science*, vol.127, 229-254 (1994)

[Lidle,et.al,97] R.Lidle and H.Niederreiter,*Finte Fields*, 2nd ed. Cambridge University Press, 1997.

[Nishio99] H.Nishio, Algebraic Studies of Information in Cellular Automata, *RIMS, Kyoto University, Kokyuroku*, vol.1106,186-195(1999).
(Erratum:Proposition 2 has been proved false by a counter example.)

Appendix: Simulation of CA[X]
Q=GF(3), cyclic boundary, $n = 6$, $f = xz + y$.

(A) $w = X11111$
time: cell 1 to 6.
0 : ((0 1 0) (0 0 1) (0 0 1) (0 0 1) (0 0 1) (0 0 1))
1 : ((0 1 1) (0 1 1) (0 0 2) (0 0 2) (0 0 2) (0 1 1))
2 : ((1 0 2) (0 0 0) (0 2 1) (0 0 0) (0 2 1) (0 0 0))
3 : ((1 0 2) (1 0 2) (0 2 1) (1 1 1) (0 2 1) (1 0 2))
4 : ((0 0 0) (2 0 1) (1 2 0) (2 2 2) (1 2 0) (2 0 1))
5 : ((2 0 1) (2 0 1) (2 2 2) (1 0 2) (2 2 2) (2 0 1))
6 : ((1 0 2) (0 0 0) (0 2 1) (2 1 0) (0 2 1) (0 0 0))
7 : ((1 0 2) (1 0 2) (0 2 1) (0 2 1) (0 2 1) (1 0 2))
8 : ((0 0 0) (2 0 1) (1 2 0) (1 0 2) (1 2 0) (2 0 1))
9 : ((2 0 1) (2 0 1) (2 2 2) (0 1 2) (2 2 2) (2 0 1))
10 : ((1 0 2) (0 0 0) (0 2 1) (1 2 0) (0 2 1) (0 0 0))
11 : ((1 0 2) (1 0 2) (0 2 1) (2 0 1) (0 2 1) (1 0 2))
12 : ((0 0 0) (2 0 1) (1 2 0) (0 1 2) (1 2 0) (2 0 1))
13 : ((2 0 1) (2 0 1) (2 2 2) (2 2 2) (2 2 2) (2 0 1))
14 : ((1 0 2) (0 0 0) (0 2 1) (0 0 0) (0 2 1) (0 0 0)) $\tau = 2, \phi = 12$

(B) w_0=011111
0 : ((0 0 0) (0 0 1) (0 0 1) (0 0 1) (0 0 1) (0 0 1))
1 : ((0 0 1) (0 0 1) (0 0 2) (0 0 2) (0 0 2) (0 0 1))
2 : ((0 0 2) (0 0 0) (0 0 1) (0 0 0) (0 0 1) (0 0 0))
3 : ((0 0 2) (0 0 2) (0 0 1) (0 0 1) (0 0 1) (0 0 2))
4 : ((0 0 0) (0 0 1) (0 0 0) (0 0 2) (0 0 0) (0 0 1))
5 : ((0 0 1) (0 0 1) (0 0 2) (0 0 2) (0 0 2) (0 0 1)) $\tau = 1, \phi = 4$

(C) w_1=111111
0 : ((0 0 1) (0 0 1) (0 0 1) (0 0 1) (0 0 1) (0 0 1))
1 : ((0 0 2) (0 0 2) (0 0 2) (0 0 2) (0 0 2) (0 0 2))
2 : ((0 0 0) (0 0 0) (0 0 0) (0 0 0) (0 0 0) (0 0 0))
3 : ((0 0 0) (0 0 0) (0 0 0) (0 0 0) (0 0 0) (0 0 0)) $\tau = 2, \phi = 1$

(D) w_2=211111
0 : ((0 0 2) (0 0 1) (0 0 1) (0 0 1) (0 0 1) (0 0 1))
1 : ((0 0 0) (0 0 0) (0 0 2) (0 0 2) (0 0 2) (0 0 0))
2 : ((0 0 0) (0 0 0) (0 0 2) (0 0 0) (0 0 2) (0 0 0))
3 : ((0 0 0) (0 0 0) (0 0 2) (0 0 1) (0 0 2) (0 0 0))
4 : ((0 0 0) (0 0 0) (0 0 2) (0 0 2) (0 0 2) (0 0 0)) $\tau = 1, \phi = 3$

For example coefficient vector (2,0,1) means $2X^2 + 1$.