数理解析研究所講究録
1106巻 1999年 186-195

Algebraic Studies of Information in Cellular Automata

Presented at RIMS, Kyoto University, on March 9,1999
by Hidenosuke NISHIO (formerly with Department of Biophysics, Kyoto Univ.)
西尾　英之助　（元・京大理学研究科）

ABSTRACT
The algebraic study of information transmission in cellular automata (CA) is revisited, after its earlier expositions by this author in 1970s. The state set of each cell is thought to be a finite field and the information is expressed by an unknown variable like in the polynomial. The idea is presented for the basic CA (1-D with neighborhood index $\{-1,0,+1\}$), although it works for the general regular CA. The notion relevant to the information transmission in CA is discussed algebraically, or using polynomials over finite fields and finite commutative rings with identity. The decision problems arising from our motivation are briefly restated in our way, which have been solved or unsolved by colleagues. We also present the preliminary study of a new measure of the information amount using the algebraic tool.

1. INTRODUCTION

"What is the information ?" and "How to study the information ?" are fundamental questions in informatics. In the study of cellular automata too, it has been investigated from various points of view.

The problem of information transmission or propagation in cellular automata or cellular spaces has been investigated by many authors, since von Neumann constructed his self-reproducing automaton using 2-D CA with 29 state cells [vN]. In his design the information is transmitted by means of many *signals*. The firing squad synchronization problem and other real time computations have been solved by utilizing many signals, which travel though CA with various *speeds* [W],[F],[Ma]. In those works, the information is transmitted generally in the form of the signals, which have their own *meanings*.

On the other hand, the *macroscopic phenomena* in CA is another important research topic, where the notion of *entropy* or the like is exploited [Mi]. Here the *numerical measure* of information quantity is defined and analyzed.

Another relation of CA to the information will be the classic research topics of injectivity and surjuctivity of the global map [R]. The reversible CA is also relevant to thinking about what the information is [I-M].

In this paper we are going to discuss another way of viewing the information in CA [N1],[N2]. Our approach will be called *algebraic*.

2. DEFINITIONS

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. That is CA=(Z, N,Q,f). We assume in this paper 1-D CA and N to be $\{-1,0,1\}$, so simply denote as CA=(Q,f).

2.1. State set

Q is generally a finite set but is thought to be a finite field in our study. It may be possible Q to be an integral domain or even a ring, but we assume first the structure of the field for the sake of simplicity. Thus Q=GF(q), where $q = p^n$ with prime number p and positive integer n. We note pa=0 and $a^q = a$, for any element a of Q.

2.2. Local function

Various ways in expressing the local function f have been made use by CA researchers. Since Q is a field, we can express it in terms of the polynomial over the coefficients from Q. Note that the local function of a linear CA is expressed in the form of linear combination. When Q is an arbitrary finite set, f is usually expressed as a table, or by listing up the function values for every combinations of neighboring cell states.
Denote the number of elements of Q as $|Q|$.

Let $|Q|=q=p^n$. Then $f : Q\times Q\times Q \rightarrow Q$ can be expressed as follows.

$$(1) \quad f(x,y,z)= u_1 x^{q-1} y^{q-1} z^{q-1} +u_2 x^{q-1} y^{q-1} z^{q-2} +u_3 x^{q-1} y^{q-2} z^{q-1} +...+u_{q3-1} z+u_{q3}$$

where $u_i \in Q$ and x, y and z takes the state value of the neighboring cells $-1,0$ and 1, respectively.

There are q^{q3} local functions in all and it will be seen that (1) is a due form for expressing them. In fact, as for the unique polynomial representation of a mapping from $GF(q)^m$ to GF(q), the reader is referred to [L-N], Notes to Chapter 7.

Example 1. Q={0,1}. f(x,y,z)=yz+x.
It is expressed also as the Boolean function $x\neg y \vee (x \text{ .EOR. } z)y$.

2.3. Information function

Let X be a symbol different from those used above. It stands for an unknown state of the cell in CA. Take Example 1. Then f(0,0,0)=0 and f(1,0,0)=1. So we may claim f(X,0,0)=X. In this case X can be interpreted as a symbol expressing the information (0 or 1) of the left neighbor. Furthermore we see f(X,1,1)=X+1 (mod.2), which comes from the fact that f(0,1,1)=1 and f(1,1,1)=0. Since f(0,1,0)=0 and f(0,1.1)=1, we obtain f(0,1,X)=X. So X might be said to represent the information transmitted from the right neighbor. But since f(0,X,0)=0, the information of the center cell does not propagate anywhere, if both neighbors are 0.

Generalizing this observation we formulate the notion of *information function*, which is useful for investigating the phenomena of information transmission in CA.

We consider the following polynomial in X over Q and call it the *information function*.

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

g is a function from Q to Q and the set of such functions is denoted by Q[X]. Note that g is a polynomial form, which uniquely expresses a mapping from Q into itself. Thus $|Q[X]|=q^q$. Note that $Q[X] \supset Q$. The element of $Q[X] - Q$ is called *informative*, while that of Q *constant*.

We introduce two operations in Q[X], addition and multiplication, following the ring operations in Q. Particularly $pX=0$ and $X^q=X$. Thus Q[X] becomes a (commutative) ring with identity, but generally not a field nor an integral domain.

Example 2. Q={0,1}. Q[X]={0,1,X,X+1}.
The multiplication table is shown below. Addition is naturally mod.2 sum.

Note that this ring is not a field and different from $GF(2^2)$={0,1,k,k+1} whose multiplication table is also shown.

Q[X]	0	1	X	X+1
0	0	0	0	0
1	0	1	X	X+1
X	0	X	X	0
X+1	0	X+1	0	X+1

GF(4)	0	1	k	k+1
0	0	0	0	0
1	0	1	k	K+1
k	0	k	k+1	1
k+1	0	k+1	1	K

It is seen that Q[X] is isomorphic to the direct sum of two GF(2)s, which is different from GF(4).

2.4. Extended CA

CA=(Q,f) is extended to a cellular automaton CA[X]=(Q[X],f) in the obvious way. The state set is Q[X]. The local function f is expressed as the same polynomial as in (Q,f), provided the variables x, y and z move in Q[X] instead of Q. As is shown in Example 2, the domain and the range of f are not necessarily finite fields (their tuples) and the discussion in Section 2.2 can not be applicable directly.

3. DYNAMICAL PHNOMENA IN CA[X]

We can now discuss the dynamics of CA[X]. The global map $F : C \rightarrow C$ is defined as usual, where $C = Q[X]^Z$ is the set of all state configurations. When discussing the information transmission, we usually assume an initial configuration having one X in

it, the rests being the constants.

Simulations

For the sake of illustration, let us show some computational results of the *finite* 1-D CA with the cell of Example 1, consisting of n cells and the fixed boundary condition. See Fig.1 (a),(b) and (c). In those space-time developments of CA[X] from the initial configuration having X at the right most cell, we find many interesting behaviors of X, which propagates in space and time. Case (a) shows that the information represented by X and X+1 reaches the left most end and remains forever in CA. Case (b) shows the contrary phenomenon, i.e. the information disappears at time 12 and does not reach the left end. In case (c), X or X+1 does not go to the left end, but remains forever in the system. A simulation with two variables X and Y, which will be discussed in Section 6.1, is also shown in Fig.1 (d). Four polynomials appear and disappear during the dynamics of CA.

4. INFORMATION FUNCTION

How is the information function useful in investigating CA? Fig.1 illustrates various phenomena observed in the development of CA[X]. The unknown state X at time 0 goes through CA, keeping its information in the form of X or X+1 or loosing it. Since we can restore X from X or X+1 completely, they are considered to be most informative. Since X and X+1 are permutations of {0,1}, we first investigate permutations below in more detail.

Note: It should be discussed how much computation is required in order to restore the value of X from the function X or X+1. It seems related to the problem of computational algorithm in solving the polynomial equation. The former requires no step of computation but the latter does one subtraction X=(X+1) –1. We do not enter this problem any more in this paper.

4.1 Permutation

Generalizing this observation we obtain the following statements about the information function. In the following we denote the cell i at time t as (i,t).

Proposition 1. Suppose that g(X) appears at a space-time point (i,t) in the development of CA[X]. If g(X) is a permutation of Q, then we say there is no loss of information during cellular development until (i,t).

This proposition will be obviously admitted, because permutation is a one to one mapping and the original state value can be restored from the state g(X) of cell (i,t).

Example 3. Q=GF(3)={0,1,2}. $g(X)=a_1X^2+a_2X+a_3$

Six permutations are : X, X+1, X+2, 2X, 2X+1, 2X+2

Example 4. We consider Q[X] over Q=GF(4)={0,1,k,k+1}. See *Example 2,* Section

2.3, for the multiplication table of Q. There are 4!=24 permutations among 256 functions.

For example, X+1 and X^2 are permutations, but X^3 is not. In fact,

$$X+1=\begin{pmatrix}0 & 1 & k & k+1\\ 1 & 0 & k+1 & k\end{pmatrix} \quad X^2=\begin{pmatrix}0 & 1 & k & k+1\\ 0 & 1 & k+1 & k\end{pmatrix} \quad X^3=\begin{pmatrix}0 & 1 & k & k+1\\ 0 & 1 & 1 & 1\end{pmatrix}$$

Proposition 2. g(X)=aX+b, where a is not a zero divisor, is a permutation.

Problem. Characterize the permutation in terms of the coefficients of g(X).
See [L-N] Chapter 7 and other literatures for detailed discussions on permutation polynomials. But what we want here is a simple new characterization.

4.2 Measure of information quantity

Since Shannon's pioneering work on defining, utilizing and analyzing the numerical information measure, there have been made several efforts in studying the information quantity, using probability, computational algorithm (Turing Machine), combinatorics and other mathematical notions. It will be clear that such efforts have greatly contributed to informatics. We present below a preliminary study of information measure in terms of the analytic property of information functions.

For every g(X) we want to define its *information quantity*, which will be denoted by I(g). I(g) should be a measure of ambiguity, when restoring the input X from the output g(X). Therefore the permutation or injective map should be given the maximum value, because X is uniquely restored from g(X). When g is a permutation, its range g(Q) equals its domain Q. The function g, which maps Q to a single element of Q, carries no information of X, so it should be given 0 as its information amount. In short I(g) should be closely related to the *cardinality* $|g(Q)|$ of the value set of g.

Now the ***requirements to I(g)*** are listed, where g and g' are polynomials over Q.

(I) I(g) is a nonnegative real number.
(II) I(g) is a monotone function in $|g(Q)|$. That is,
$I(g) \le I(g')$, if $|g(Q)| \le |g'(Q)|$.
(III) I(g) takes the maximum, denoted by Imax, when g is a permutation of Q.
(IV) I(g)=0, if g is a constant. So $0 \le I(g) \le Imax$.

Those requirements are not sufficient for determining the functional form of I(g) uniquely. But we leave fixing the definite form of I(g) for future study, and only present the preliminary results obtained from those requirements. Note that the set of information functions is closed under the operations of sum and product of polynomials (Section 2.3). In the following, g and g' are functions defined on the domain Q, which is not explicitly written where it is clear.

Example 5. Consider polynomials belonging to Q[X] of Example 4, Section 2.3, with

coefficients from Q=GF(4).

Let g=g'=X. Then $|g+g'|=1$. As another example, we take $g=X^2$ with $|g|=4$ and $g'=X^3$ with $|g'|=2$. Since $g+g'=X^2+X^3=\begin{pmatrix}0 & 1 & k & k+1\\ 0 & 0 & k & 1\end{pmatrix}$, we have $|g+g'|=3$.

Generalizing this exercise, we obtain the following proposition.

Proposition 2.
(a) $|g+g'| \leq \max\{|g|,|g'|\}$.
(b) $|gg'| \leq \min\{|g|,|g'|\}$.

During cellular operation in CA[Q], each cell gets its new state by computing addition and multiplication of polynomials.

Definition. Information quantity I(c) of a state configuration c is defined to be $\max\{I(c(i)) \mid i\in Z\}$. I(c(i)) stands for I(g) provided g is the state polynomial of cell i.

If we adopt the cardinality of the value set of g as a candidate, denote as $I_{\#}$, of I(g), we have the following proposition 3, which suggests the *information degradation principle* of CA or any dynamical system. Notice that $I_{\#}$ satisfies the above listed requirements to I(g) except for (IV). Let c(t) be the state configuration of CA at time t.

Proposition 3. $I_{\#}(c(t+1)) \leq I_{\#}(c(t))$.

Note: For determining the final functional form of I(g), we might better add one more requirement like Proposition 3, which was proved for $I_{\#}$.

5. DECISION PROBLEMS

We present again the decision problems studied before [1][2], using our terminology. Assume first a CA=(Q,f) be the basic *finite* CA with fixed boundaries. A finite CA consists of n cells, simply written as 1,2,...,n. The left and the right boundaries are fixed to be the elements of Q denoted by b_l and b_r, respectively. CA is naturally extended to CA[X]. The state of the point (i,t) is denoted by c(i,t).

Now take a word $w \in Q^*$ of length n –1 and the variable X, and give to CA the word wX as its initial configuration. So c(n,0)=X and w=c(1,0)c(2,0)...c(n−1,0).
We are interested in the behavior of cell 1, denoted by P(wX). P(wX)=c(1,0)c(1,1)c(1,2)...c(1,t)..... It is an infinite string and consists of the finite 'transient part' and the 'cyclic part' which repeats indefinitely, since CA[X] is a finite dynamical system. A finite or infinite string of symbols from Q[X] is called *constant*,

when it does not contain any informative element.

5.1 Decision problem "D space"

Our decision problem asks if the information of the state c(n,0) reaches the cell 1 or not. If P(wX) is constant, then it does not reach the cell 1. In the converse, if it is informative, then this n-cell CA is said to transmit the information of the right most cell to the left most cell. Note that we do not concern with how much information is transmitted.

Consider all CA(Q,f)s. There are infinitely many such CAs. They are classified into three mutually disjoint sets. This classification reflects the easiness or ability of information transmission of a given CA.

(CAI) There is a positive integer k such that P(wX) is constant for any w longer than or equal to k.
(CAII) Set of all CAs minus CAI and CAII.
(CAIII) For evey w, P(wX) is informative.

It is shown that each class is not vacant and the classification is meaningful [2]. The shift register belongs to CAIII. Example 1 is CAI with k=7. Note that this classification heavily depends on the boundary condition.

Decision problem "D space" is stated as follows : *Given an arbitrary CA, decide to which class it belongs.*

Proposition. Problem "D space" is undecidable [T].

A similar decision problem can be stated for the 1-D CA with *cyclic boundary* : Decide whether the information X reaches the farthest cell or not. The farthest cell from 1 is cell n/2. This cyclic version is also supposed to be undecidable.

5.2 Decision problem "D time"

Let's state another decision problem concerning the information transmission in the direction of time [K-S]. We assume the cyclic boundary and the CA starts with the initial configuration wX. The configuration at time t is denoted by R(w,t), i.e. R(w,t)=c(1,t)c(2,t)...c(n,t).

Classification of CA[X]s into three mutually disjoint sets :

(CAI') There is a positive integer h such that R(w,t) is constant for any w and $t \leq h$.
(CAII') Set of all CAs minus CAI' and CAIII'.
(CAIII') For every w and h, R(w,h) is informative.

This classification according to the information transmission in the time direction reflects an aspect of information conservation in CA.

Decision problem "D time" is stated as follows : *Given an arbitrary CA, decide to*

which set it belongs.

Problem "D time" is left unsolved but suspected to be undecidable.

5.3 Infinite CA

When CA is infinite, we assume an finite initial configuration embedded in Z ...000wXw'000..., where 0 is a quiescent state. One problem to study is to investigate how far X propagates. Similar classification of CA is possible and the decision problem is conjectured to be undecidable.

6. GENERAL CASES

We can discuss more general formulation of our idea mentioned for the basic 1-D CA in the preceding chapters.

6.1 More than one variables

We present the formulation for the two variables X and Y. The information function is expressed as follows.

$$(3) \qquad g(X,Y)=a_1 X^{q-1}Y^{q-1} +a_2 X^{q-1} Y^{q-2} +...+a_{q2-2} X+a_{q2-1}Y+a_{q2}$$

The set of all information functions is denoted by Q[X,Y] and the local function f is extended to $f : Q[X,Y]^3 \rightarrow Q[X,Y]$. A computer simulation of this case is shown in Fig. 1(d), where 4 informative functions appear and disappear at time 79. The notion of permutation of the pair $Q \times Q$ is not so clear, contrary to the self-evident one of Q. It has been not settled how to define the permutation polynomial in Q[X,Y]. See [L-N], Chapter 7.

6.2 Larger neighborhood

The local function is written in the form of (1) with more terms in |N| variables.
The information function can be considered likely.

6.3 Higher dimensional CA and general regular CA

We can discuss the problems about information in the general CA, say 2-D CA and CA on the Cayley graph. But it is not clear what kind of research topics should be most interesting.

7. CONCLUDING REMARKS

We discussed an algebraic approach to the study of CA, which might be useful in understanding *what the information is*. There are many points left for further research. Among others we mention the following:
1) Algebraic analysis of the extension Q[X] (and Q[X,Y,..]) and its related polynomials. See Sections 2.3, 2.4 and 6.1. 2) More elegant formulation and solution of the decision problems stated in Section 5, which have been investigated in terms of

the formal language or automata theory. 3) More definite definition and usage of I(g).

Thanks are due to Masami Ito (Kyoto), who organized this meeting at RIMS and suggested me to talk there, Ryuki Matsuda (Mito), Yuji Kobayashi (Funabashi) and Masashi Katsura (Kyoto), who discussed with me and made comments on finite rings/fields.

REFERENCES

[F] P.C.Fisher,"Generation of primes by a one-dimensional iterative array", *J.A.C.M.* March 12 (1965) 388-394

[G] See for example the tutorial book by M.Garzon, 'Models of Massive Parallelism, Analysis of Cellular Automata and Neural Networks', Springer, 1995

[I-M] K.Imai and K.Morita, "Firing squad synchronization problem in reversible cellular automata", *Theoret. Comput. Sci.* 165 (1996) 457-482

[K-S] This decision problem was proposed and its classification for the case Q={0,1} was finished by Y.Kobuchi and T.Sakaguchi. The complete classification was published in Sakaguchi's MS thesis to Kyoto University, "Information Maintaining Capability in One-Dimensional Cyclic Cellular Automata" (1971).

[L-N] R.Lidl and H.Niederreiter, 'Finite Fields', Encyclopedia of Mathematics and Its Applications vol.20, 2nd ed. Cambridge University Press, 1997,

[Ma] J.Mazoyer, "Signals in one-dimensional cellular automata", *Theoret.Comput. Sci.* 217, No.1 (1999) 53-80

[Mi] J.Milnor, "On the Entropy Geometry of Cellular Automta", *Complex Systems* 2 (1988) 357-386

[N1] H.Nishio, "Heuristic use of image processing technique for theoretical studies of automata", in 'Frontiers of Pattern Recognition', ed.S.Watanabe, Academic Press (1972) 373-389.

[N2] 西尾英之助、岩波講座「現代物理学の基礎」９、生命の物理、第Ⅳ部、１９７２

[R] D.Richardson, "Tessellation with local transformations", *J.C.S.S* 6 (1972) 373-388

[T] H.Takahashi, "Information Transmission in One-Dimensional Cellular Space and the Maximum Invariant set", *Inf.and Control* 33 (1977) 35-55

[vN] J.von Neumann, 'Theory of self-reproducing automata', Univ.of Illinios Press 1966

[W] A.Waksman, "An optimal solution to the firing squad synchronization problem", *Inf.and Control*, 8 (1966) 66-78

Fig.1 Simulations of CA[X] and CA[X,Y]

Q={0,1}, f=yz+x, with fixed baudary conditions $b_l=b_r=1$.

In (a), (b) and (c), which are dynamics of CA(Q[X],f), the symbol + means X and − does X+1.

In (d), which is a simulaton of CA(Q[X,Y],f), four polynomials in X and Y are expressed as Greek alphabet: α =XY, β =X+Y, γ =XY+X+Y, δ =XY+X+Y+1

n is the length of CA. r is the length of transient part and p is the cycle length of dynamics of finite CA.

(a) n=5, r=4, p=30 (b) n=9, r=14, p=10 (c) n=9, r=14, p=10 (d) n=15, r=79, p=10