数理解析研究所講究録 1437 巻 2005 年 155-162

Commentary on Fritz von Haeseler's paper : "On a Problem in Information Dynamics of Cellular Automata"

Hidenosuke Nishio
Iwakura Miyake-cho 204-1
Sakyo-ku, 606-0022, Kyoto, Japan
Email: YRA05762@nifty.ne.jp

1 Introduction

This report is a commentary on the paper "On a problem in information dynamics of cellular automata" written and submitted by Friedrich von Haeseler (KU Leuven) [1]. He has developed a general setting for studying a problem posed by H.Nishio and T.Saito in connection with information dynamics of cellular automata (CA for short) [6]. Particularly he shows that the lattice introduced by them is anti-isomorphic to a certain partition lattice.

First, we shall give an introduction to information dynamics of CA and then present von Haeseler's results utilizing (the LaTeX source of) his manuscript. The references are very limited. For the general of algebra and polynomials over a finite field, we refer to [2] and [3], respectively.

2 Information Dynamics of Cellular Automata

2.1 Cellular automaton on a finite field

One-dimensional CA on a finite field is defined by a 4-tuple $(Q, \mathbb{Z}, N, f)$, where Q is the finite set of cell states, $\mathbb{Z}$ is the set of integers, N is the neighborhood and f is the local function.

State Set Q is assumed to be a finite field $\mathrm{GF}(q)$, where $q = p^n$ with prime p and positive integer n.

N is the neighborhood (index) which is assumed here to be the elementary neighborhood $N = \{-1, 0, +1\}$.

The local function $f : Q \times Q \times Q \to Q$ is uniquely expressed by the polynomial form:

$$f(x,y,z) = u_0 + u_1 x + u_2 y + \cdots + u_i x^h y^j z^k + \cdots + u_{q^3-2} x^{q-1} y^{q-1} z^{q-2} + u_{q^3-1} x^{q-1} y^{q-1} z^{q-1}, \quad \text{where } u_i \in Q \ (0 \le i \le q^3 - 1). \quad (1)$$

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

The global map $F : C \to C$ is defined on the set of configurations $C = Q^{\mathbb{Z}}$: For any $i \in \mathbb{Z}$, $F(c)(i) = f(c(i-1), c(i), c(i+1))$, where $c(i)$ is the state of cell $i \in \mathbb{Z}$ of $c \in C$. For a configuration $c \in C$, the dynamics of CA is defined by $F^{t+1}(c) = F(F^t(c))$, where $F^0(c) = c$.

2.2 Information X and polynomial states

Let X be a symbol different from those used in the polynomial form (1). It stands for an unknown state or the *information* of the cell in CA and will be called the *information variable*. In order to investigate the dynamics of information X in CA space, we consider another polynomial form, which generally defines the cell state of the extended CA.

$$g(X) = a_0 + a_1X + \cdots + a_iX^i + \cdots + a_{q-1}X^{q-1}, \text{ where } a_i \in Q \ (0 \leq i \leq q-1). \quad (2)$$

The polynomial form g uniquely defines a function $Q \to Q$ and the set of such functions is denoted by $Q[X]$. $Q[X]$ is a polynomial ring with identity. Note that $pX = 0$ and $X^q - X = 0$ in $Q[X]$.

2.3 Extended CA$[X]$ or Polynomial State CA

Based upon CA$=(Q, f)$ we define its extension CA$[X]=(Q[X], f_X)$, where the set of cell states is $Q[X]$. CA$[X]$ will be called the *polynomial state CA over GF(q)*. The local function f_X is defined on the same neighborhood and 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, $f_X : Q[X] \times Q[X] \times Q[X] \to Q[X]$.

2.4 Information dynamics of CA$[X]$

$F_X : C_X \to C_X$, where $C_X = Q[X]^{\mathbb{Z}}$. For any $i \in \mathbb{Z}$, $F_X(c_X)(i) = f(c_X(i-1), c_X(i), c_X(i+1))$, where $c_X(i)$ is the state of cell $i \in \mathbb{Z}$ of $c_X \in C_X$. For a configuration $c_X \in C_X$, the dynamics of CA$[X]$ is defined by $F_X^{t+1}(c_X) = F_X(F_X^t(c_X))$, where $F_X^0(c_X) = c_X$.

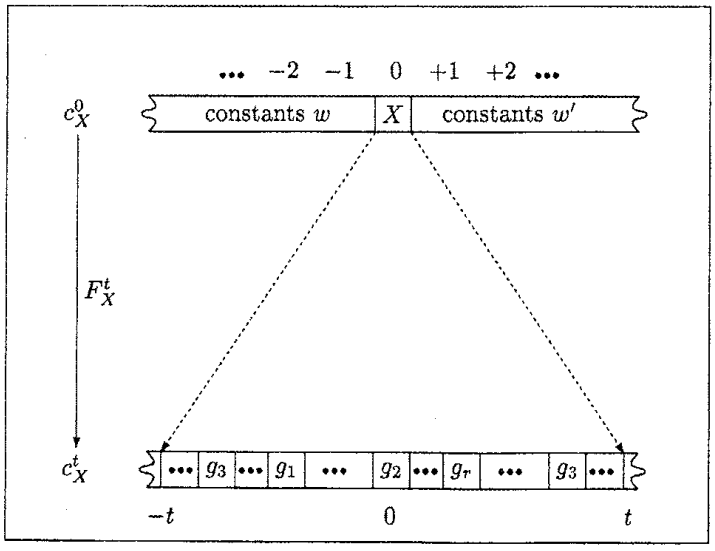


Fig.1. Information dynamics of CA$[X]$

Fig.1. illustrates an elementary information dynamics, which begins with the initial configuration $c_X^0 = wXw'$, where $c_X^0(0) = X$ and w and w' are semi infinite strings of constant polynomial functions. Obviously w and w' do not contain any information about X. Then, by repeated application of F_X, the information X spreads in time t among cells $-t, -t+1, ..., 0, ..., t-1, t$ and at time t we observe a configuration c_X^t, which might contain some polynomials in X. Note

that a same polynomial may appear at several cells. Such a set of polynomials is generally expressed by $G_{c^t_X} = \{g_1, g_2, ..., g_r\}$. $G_{c^t_X}$ is considered to preserve some amount of information of X contained by the initial configuration c^0_X.

2.5 Completeness and Degeneracy

Among several notions pertinent to information dynamics, we concentrate here on the *completeness* and the *degeneracy*.

The paper [6] contains the following definitions and a basic result.

Definition 1 (complete configuration) *A subset $G \subseteq Q[X]$ is called complete, if G generates $Q[X]$. Any constant is allowed to be used at the computation. For any configuration $c_X \in C_X$, define the set of polynomials $G_{c_X} = \{c_X(i) | i \in \mathbb{Z}\} \subseteq Q[X]$. A configuration c_X is called complete, if G_{c_X} is complete.*

Definition 2 (Degeneracy) *For a configuration $c_X \in Q[X]^{\mathbb{Z}}$, let $\psi_a(c_X)$ be a substitution of a in c. Then, c_X is called m-degenerate, if*

$$|\{\psi_a(c_X) \mid a \in Q\}| = |Q| - m.$$

It is easily seen that $0 \leq m \leq |Q| - 1$. Such m will be called the degree of degeneracy of c_X and denoted as $m(c_X)$. A configuration c_X is simply called degenerate if $m(c_X) \neq 0$.

Theorem 3 *A configuration is complete if and only if it is not degenerate.*

2.6 Generation of subrings and value size

In [5], the notion of the completeness is generalized and the degree of completeness is defined and related to the degree of degeneracy.

For a subset $G \subseteq Q[X]$, by $\langle G \rangle$ we mean the subring of $Q[X]$ which is generated by G and constant polynomial functions. Note that $\langle G \rangle$ is expressed as $\langle G \rangle_N$ in von Haeseler's formulation below.

For any subset $G \subseteq Q[X]$, the *log-ring size or degree of completeness* $\lambda(G)$ is defined by the following equation.

$$\lambda(G) = \log_q |\langle G \rangle| \tag{3}$$

Note that $1 \leq \lambda(G) \leq q$.

Suppose that a subset $G \subseteq Q[X]$ consists of r polynomials: $G = \{g_1, g_2, ..., g_r \mid g_i \in Q[X], 1 \leq i \leq r\}$. Then an r-tuple of values $(g_1(a), g_2(a), ..., g_r(a))$ for $a \in Q$ is called *the value vector* of G for a and denoted by $G(a)$. Note that $G(a) \in Q^r$. The *value set* $V(G)$ of G is defined by

$$V(G) = \{G(a) \mid a \in Q\}. \tag{4}$$

Finally we define the *value size* of G by $|V(G)|$. Note that $1 \leq |V(G)| \leq q$. Then, we have the following theorems which relate the degree of completeness to that of degeneracy.

Theorem 4

$$\lambda(G) = \log_q |\langle G \rangle| = |V(G)|. \tag{5}$$

Proof: See [5]. In [4] is given a new proof based on the partition of value set $V(G)$, which has been inspired by von Haeseler's results.

The following theorem, which is equivalent to the above theorem, has been given without proof in the concluding remarks of [6]. Note that the case of $m = 0$ corresponds to Theorem 3, i.e. G_{c_X} generates $Q[X]$.

Theorem 5

$$\lambda(G_{c_X}) + m(c_X) = q, \text{ for any } c_X \in C_X, \tag{6}$$

2.7 Problem posed by H.Nisho and T.Saito

The following problem arises from the above considerations on the degrees of completeness and degeneracy and has attracted von Haeseler.

Characterize the lattice (by set inclusion) of subrings of $Q[X]$ generated by arbitrary subsets G of $Q[X]$.

Besides Theorem 4, [5] contains several computational examples concerning the lattice structure of subrings of $Q[X]$, but H.Nishio has not succeeded in obtaining a complete solution.

3 F. von Haeseler's results

3.1 Formulation

From now on $\mathbb{F}$ denotes a finite field with q elements. The set of all maps $g : \mathbb{F} \to \mathbb{F}$ is denoted as $\mathbb{F}^{\mathbb{F}}$. It is a ring with pointwise addition and multiplication, i.e.,

$$(f+g)(x) = f(x) + g(x) \text{ and } (fg)(x) = f(x)g(x).$$

Now let $G \subseteq \mathbb{F}^{\mathbb{F}}$ and let $\langle G \rangle_N$ be the set of all finite sums of finite products of elements in G together with the constant maps, i.e., an element f of $\langle G \rangle_N$ is given as

$$f = \sum_{i=0}^{n} \prod_{j_i=0}^{m_i} g_{j_i},$$

where g_{j_i} in G or a constant function.

Then H. Nishio and T. Saito ask for a description of the lattice consisting of all sets $\langle G \rangle_N$, $G \subseteq \mathbb{F}^{\mathbb{F}}$. Moreover, they are interested in criteria for $\langle G \rangle_N = \mathbb{F}^{\mathbb{F}}$.

We consider the above problem in a slightly more general setting, which can be described as follows.
Let X be a finite set. The set of maps $g : X \to \mathbb{F}$ is denoted as $\mathbb{F}^X$. Note that $\mathbb{F}^X$ is a ring with pointwise addition and multiplication. For a subset G of $\mathbb{F}^X$ the set $\langle G \rangle$ denotes the set of all finite linear combinations of finite products of elements in G, i.e., an element f of $\langle G \rangle$ is given as

$$f = \sum_{i=0}^{n} c_i \prod_{j_i=0}^{m_i} g_{j_i},$$

where $c_i \in \mathbb{F}$ and g_{j_i} in G. Note that $\langle G \rangle_N = \langle G \cup \mathbf{C} \rangle$, where $\mathbf{C}$ is the set of constant functions.

The extended problem is now: Describe the lattice given by this construction and the relation with the lattice generated by H. Nishio and T. Saito.

It is clear that the following holds:

- $\langle G \rangle$ is the smallest (w.r.t. inclusion) subring R of $\mathbb{F}^X$ that contains G and that is an $\mathbb{F}$-vectorspace, i.e., $f \in R$ implies $\alpha f \in R$ for all $\alpha \in \mathbb{F}$.
- $\langle G \rangle_N$ is the smallest (w.r.t. inclusion) subring R of $\mathbb{F}^X$ that contains G and the constant functions, and R is an $\mathbb{F}$-vectorspace.

Thus one has : $\mathcal{L}(X,\mathbb{F}) = \{\langle G\rangle \mid G \subseteq \mathbb{F}^X\}$ is the set of all subrings of $\mathbb{F}^X$ which are also $\mathbb{F}$-vectorspaces, and $\mathcal{L}_N(X,\mathbb{F}) = \{\langle G\rangle_N \mid G \subseteq \mathbb{F}^X\}$ is the set of all subrings of $\mathbb{F}^X$ which contain the constant functions and are $\mathbb{F}$-vectorspaces. Moreover,

$$\mathcal{L}_N(X,\mathbb{F}) \subset \mathcal{L}(X,\mathbb{F}).$$

3.2 Characterization of generating sets

A generating set G is *minimal* if its cardinality $|G|$ is smallest among all generating sets. A generating set G is *properly generating* if no proper subset $G' \subset G$ is a generating set. Later we shall see that a properly generating set is not necessarily a minimal generating set. If $\langle G\rangle_N = \mathbb{F}^X$, then G is called *N-generating.*
In order to characterize generating sets we introduce some notions. For $G \subseteq \mathbb{F}^X$ the *support* of G is the set

$$\mathrm{supp}(G) = \{x \in X \mid \text{there is } g \in G \text{ with } g(x) \neq 0\}.$$

Two points $x, y \in X$ are called *G-equivalent*, denoted as $x \sim_G y$, if

$$g(x) = g(y) \text{ for all } g \in G.$$

$X/\sim_G$ denotes the set of equivalence classes and $\pi : X \to X/\sim G$ is the canonical projection.

Then one has

Lemma 6 *[L1]*

1. $\mathrm{supp}(G) = \mathrm{supp}(\langle G\rangle)$.
2. $x \sim_G y$ *if and only if* $x \sim_{\langle G\rangle} y$.

The set G *separates* if for every pair $x, y \in X$ with $x \neq y$ there exists a $g \in G$ such that

$$g(x) \neq g(y).$$

Theorem 7 *[T1] The set* $G \subseteq \mathbb{F}^X$ *is generating if and only if*

1. G *is separating and*
2. $\mathrm{supp}(G) = X$.

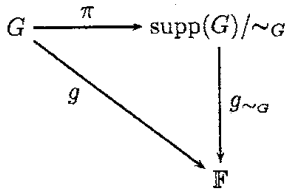
Corollary 8 *[C1]* $\langle G\rangle_N = \mathbb{F}^X$ *if and only if* G *separates.*

Theorem 7 also allows a description of $\langle G\rangle$ if $\mathrm{supp}(G) \neq X$.

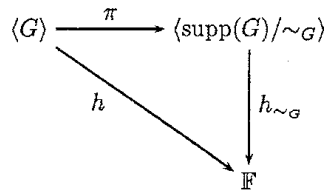
Theorem 9 *[T2]*

1. *The ring* $\langle G\rangle$ *is isomorphic to the ring* $\mathbb{F}^{\mathrm{supp}(G)/\sim_G}$.
2. *The ring* $\langle G\rangle_N$ *is isomorphic to the ring* $\mathbb{F}^{X/\sim_G}$.

Proof: Ad *1.* For every $g \in G$ there exists a unique and well defined map $g_{\sim_G}$ such that the diagram commutes.



Moreover, $(\alpha g + \beta h)_{\sim_G} = \alpha(g)_{\sim_G} + \beta(h)_{\sim_G}$ and $(gh)_{\sim_G} = (g)_{\sim_G}(h)_{\sim_G}$ for all $\alpha, \beta \in \mathbb{F}$ and all $g, h \in G$. This implies that for every $h \in \langle G \rangle$ there exists a unique $h_{\sim_G} \in \langle \mathrm{supp}(G)/{\sim_G} \rangle$ such that the diagram commutes



Let $G_{\sim_G} = \{g_{\sim_G} \mid g \in G\}$, then $G_{\sim_G} \subseteq \mathbb{F}^{\mathrm{supp}(G)/{\sim_G}}$. The above considerations show that the rings $\langle G \rangle$ and $\langle G_{\sim_G} \rangle$ are isomorphic. Since $G_{\sim_G}$ satisfies the conditions of Theorem 7 for $X = \mathrm{supp}(G)/{\sim_G}$, this proves the first assertion.
The second assertion follows from $\langle G \rangle_N = \langle G \cup \mathbf{C} \rangle$ and the fact that $\mathrm{supp}(G \cup \mathbf{C}) = X$ combined with the first assertion.

■

This also gives

Corollary 10 *1.* $|\langle G \rangle| = q^{|\mathrm{supp}(G)/{\sim_G}|}$.

2. $|\langle G \rangle_N| = q^{|X/{\sim_G}|}$.

Remarks by Nishio: We notice that the second equation of this corollary is equivalent to Equation (5) of Theorem 4 given in the previous section.

3.3 The lattice $\mathcal{L}(X, \mathbb{F})$

In this section we introduce the lattice $(\mathcal{L}(X, \mathbb{F}), \wedge, \vee)$ and show that it is anti-isomorphic to a partition lattice.

A *lattice* is any nonempty partially ordered set in which any two elements a and b have a least upper bound, $a \vee b$, and a greatest lower bound, $a \wedge b$. The operation $\vee$ is called *join*, and the operation $\wedge$ is called *meet*.

The set $\mathcal{L}(X, \mathbb{F})$ is via inclusion a partially ordered set; meet and join are given as

$$R_1 \wedge R_2 = R_1 \cap R_2$$
$$R_1 \vee R_2 = \langle R_1 \cup R_2 \rangle$$

i.e., $(\mathcal{L}(X, \mathbb{F}), \wedge, \vee)$ is a lattice.

Of particular importance is the *partition lattice* of a finite nonempty set Y. A partition of Y is given as $P = \{p_1, \ldots, p_s\}$, where p_i are mutually disjoint, nonempty subsets of Y such that

$$Y = \bigcup_{i=1}^{s} p_i.$$

The set of all partitions is denoted as $\mathcal{P}(Y)$. If $P = \{p_1, \ldots, p_s\}$ and $Q = \{1, \ldots, t\}$ are partitions of Y, then $P \leq Q$ if every $p \in P$ is contained in a $q \in Q$, i.e., P *is finer than* Q. This defines a partial order on $\mathcal{P}(Y)$. Then meet, $\sqcap$, and join, $\sqcup$, are defined, i.e., $(\mathcal{P}(Y), \sqcap, \sqcup)$ is a lattice.
We also need the concept of (anti)-isomorphic lattices. Two lattices $(L_i, \wedge_i, \vee_i)$, $i = 1, 2$, are *isomorphic*, if there exists a bijection $\xi : L_1 \to L_2$ such that

$$\xi(x \wedge_1 y) = \xi(x) \wedge_2 \xi(y)$$
$$\xi(x \vee_1 y) = \xi(x) \vee_2 \xi(y)$$

holds for all $x, y \in L_1$. They are *anti-isomorphic* if

$$\xi(x \wedge_1 y) = \xi(x) \vee_2 \xi(y)$$
$$\xi(x \vee_1 y) = \xi(x) \wedge_2 \xi(y)$$

We can now state the characterization of the lattice in question. Suppose 0 does not belong to X, then $X_0 = \{0\} \cup X$.

Theorem 11 *[T3] The lattices $(\mathcal{L}(X,\mathbb{F}), \wedge, \vee)$ and $(\mathcal{P}(X_0), \sqcap, \sqcup)$ are anti-isomorphic.*

Proof: Definition of a bijective map from $\mathcal{L}(X,\mathbb{F})$ to $\mathcal{P}(X_0)$. Let $R \in \mathcal{L}(X,\mathbb{F})$. Then one has $X = \mathrm{supp}(R) \cup \ker(R)$, where $\ker(R) = X \setminus \mathrm{supp}(R)$. The projection $\pi : \mathrm{supp}(R) \to \mathrm{supp}(R)/\sim_R$ defines a partition of $\mathrm{supp}(R)$, namely $P = \{\pi^{-1}(u) | u \in \mathrm{supp}(R)/\sim_R\}$.
This induces a partition of X_0 as

$$\xi(R) = \{\{0\} \cup \ker(R)\} \cup \{\pi^{-1}(u) \mid u \in \mathrm{supp}(R)/\sim_R\}.$$

For the inverse consider $\eta : \mathcal{P}(X_0) \to \mathcal{L}(X,\mathbb{F})$ is defined as follows. Let $Q = \{q_0, \ldots, q_s\}$ be a partition of X_0 such that $0 \in q_0$, then

$$\eta(Q) = \left\{ \sum_{i=1}^{s} \alpha_i \chi_{q_i} \mid \alpha_i \in \mathbb{F},\ i = 1, \ldots, s \right\}$$

is in $\mathcal{L}(X,\mathbb{F})$. It is easy to see that $\xi(\eta(Q)) = Q$ and $\eta(\xi(R)) = R$. This proves the bijectivity of ξ. It remains to show that ξ reverses the order, i.e., if $R_1 \subseteq R_2$ for $R_1, R_2 \in \mathcal{L}(X,\mathbb{F})$, then $\xi(R_1) \geq \xi(R_2)$. If $q \in \xi(R_2)$, then the characteristic map χ_q is in R_2. Since $R_1 \subset R_2$, it follows that every $p \in \Xi(R_1)$ either has empty intersection with q, or q is contained in p. In other words every $q \in \xi(R_2)$ is contained in a $p \in \xi(R_1)$. This shows that $\xi(R_2) \leq \xi(R_1)$ and that ξ is anti-isomorphic.

■

Corollary 12 *[C2] The lattice $(\mathcal{L}_N(X,\mathbb{F}), \wedge, \vee)$ is a sublattice of $(\mathcal{L}(X,\mathbb{F}), \wedge, \vee)$ and it is anti-isomorphic to the partition lattice $(\mathcal{P}(X), \sqcap, \sqcup)$.*

The proof is as the proof of Theorem 11 using $\xi_N : \mathcal{L}_N(X,\mathbb{F}) \to \mathcal{P}(X)$ defined as

$$\xi_N(R) = \{\pi^{-1}(u) \mid u \in X/\sim_G\}$$

Examples

- Consider $\mathbb{F}_5 = \{0, \ldots, 4\}$ and $X = \mathbb{F}_5$ and let $p(x) = x + x^3 + x^4$, $q(x) = 4x + 4x^2 + 2x^3 + x^4 \in \mathbb{F}_5^{\mathbb{F}_5}$ regarded as maps. Then $\langle p \rangle_N$ and $\langle q \rangle_N$ are different set. This follows from

	0	1	2	3	4
p	0	3	1	1	4
q	0	1	1	3	4

  i.e., the partitions $\xi(\langle p \rangle_N) = \{\{0\}, \{1\}, \{2,3\}, \{4\}\}$ and $\xi(\langle q \rangle_N) = \{\{0\}, \{1,2\}, \{3\}, \{4\}\}$ are different. Note also that $|\langle p \rangle_N| = |\langle q \rangle_N| = 5^4$, i.e., $\{p\}$ and $\{q\}$ are not generating, since $\left|\mathbb{F}_5^{\mathbb{F}_5}\right| = 5^5$.

- If $g \in \mathbb{F}^{\mathbb{F}}$, then $\langle g \rangle_N = \mathbb{F}^{\mathbb{F}}$ if and only if g is bijective. More general: Let $g \in \mathbb{F}^X$, then $\langle g \rangle_N = \mathbb{F}^X$ if and only if g is injective; and $\langle g \rangle = \mathbb{F}^X$ if and only if g is injective and $0 \notin \{g(x) \mid x \in X\}$.

Remarks: von Haeseler notes on the number of elements of $\mathcal{L}(X,\mathbb{F})$:

$$|\mathcal{L}(X,\mathbb{F})| = B_{|X|+1} \text{ and } |\mathcal{L}_N(X,\mathbb{F})| = B_{|X|},$$

where B_n is the n-th Bell number or the number of partitions of a set having n elements.

4 Concluding remarks

von Haeseler's paper consists of 17 pages with 5 references and includes more results like *properties of generating sets* and *the case of a ring* $\mathbb{Z}/m\mathbb{Z}$, which we have had to omit here. Many thanks are due to him for his cooperation, especially for a LaTeX source of his manuscript. ! !

References

[1] von Haeseler, F.: On a Problem in Information Dynamics of Cellular Automata, Int. Journal of Unconventional Computing, submitted 2004.

[2] Lang, S.: *Algebra*, Revised third edition, Springer, 2002.

[3] Lidl, R., Niederreiter, H.: *Finite Fields*, Second edition, Cambridge University Press, 1997.

[4] Nishio, H.: Completeness and Degeneracy in Information Dynamics of Cellular Automata, MFCS2005, submitted.

[5] Nishio, H.: *Log-ring size and value size of generators of subrings of polynomials over a finite field*, Technical Report kokyuroku 1375, RIMS, Kyoto University, 2004.

[6] Nishio, H., Saito, T.: Information Dynamics of Cellular Automata I : An Algebraic Study, *Fundamenta Informaticae*, **58**, 2003, 399–420.

(May 7, 2005)