On Polynomial Rings in Information Dynamics of Linear CA

Fritz v. Haeseler and Hidenosuke Nishio

Gießen, September 18th 2013

Introduction

Generally, information dynamics is concerned with CA whose states are in a finite (commutative) ring. However, we will concentrate on polynomial rings in X over a finite field.

Let R be a finite ring (the states) and $R^{\mathbb{Z}}$ be the set of all maps from $\mathbb{Z}$ to R (the configurations).

A one-dimensional three-neighbor cellular automaton (CA) $F : R^{\mathbb{Z}} \to R^{\mathbb{Z}}$ with values (states) in R is given by a map $f : R^3 \to R$ (the local rule) such that for a configuration $\underline{c} \in R^{\mathbb{Z}}$ one defines a new configuration $F(\underline{c})$ by setting

$$F(\underline{c})(j) = f(\underline{c}(j-1), \underline{c}(j), \underline{c}(j+1))$$

for all $j \in \mathbb{Z}$. Iterating this global map F leads to a sequence of configurations $\underline{c}^t = F^t(\underline{c}), t \geq 0$.

Information dynamics

Consider the initial configuration $\underline{c}^0$ defined as

$$\underline{c}^0(j) = \begin{cases} a_j & \text{if } j < 0 \\ X & \text{if } j = 0 \\ b_j & \text{if } j > 0, \end{cases}$$

where a_j and b_j are constants in R and X is considered as a variable (information variable). Then for $t \geq 1$ and $j \in \mathbb{Z}$ the value $F^t(\underline{c})(j)$ either depends on X or not. E.g., for values of j far to the left and right $F^t(\underline{c})(j)$ does not depend on X.

The study of information dynamics is concerned with the sets $M^t = \{F^t(\underline{c})(j) \mid j \in \mathbb{Z}\} \subset R^R$ for $t \geq 0$. E.g. it ignores the places (cells) where the information variable appears.

Problem I

The first problem considered by [N&S] is to ask if M^t contains complete information about X or not, and if not, how much information it contains.

A configuration $\underline{c}^t$ is said to contain the information of X completely and called a complete configuration, if X can be obtained by finite sums and finite products of maps and together with multiplication with constants (elements of R). This situation can be restated in terms of ring generation. That is, let

$$\mathcal{P}(t) = \langle M^t \rangle$$

denote the smallest subring of R^R which is also an R-module and contains M^t.

Then c^t is complete if and only if $\mathcal{P}(t) = R^R$.

Problem II

It was shown [N&S] that $|\langle M^t \rangle| \geq |\langle M^{t+1} \rangle|,\ t \geq 0$.
Note that it does not imply $\langle M^t \rangle \supseteq \langle M^{t+1} \rangle,\ t \geq 0$.

Another problem is the description of the lattice structure of $\langle M^t \rangle$. [vH] showed that the lattice is anti-isomorphic to a certain partition lattice.

Now the research interest goes to elucidating the dynamical properties of $\mathcal{P}(t) = \langle M^t \rangle, t \geq 1$. But unfortunately it seems very difficult to generally solve the problem for arbitrary CA.

In this talk we will confine ourselves to linear CA by use of formal Laurent series and polynomials.

Linear CA with states in R

We assume that R is a commutative ring. An R-linear scope k CA has a local rule $f : R^k \to R$ of the form

$$f(\xi_1, \ldots, \xi_k) = \sum_{j=1}^{k} r_j \xi_j$$

with $r_j \in R$ for $j = 1, \ldots, k$.

A configuration $\underline{c} \in R^{\mathbb{Z}}$ can be written as a formal Laurent series $\underline{c}(Y) = \sum_{j \in \mathbb{Z}} \underline{c}(j) Y^j$ and a linear local rule f can be written as a polynomial $P(Y)$with coefficients in R. Then $F(\underline{c})$ is the Laurent series obtained by the multiplication of $\underline{c}(Y)$ with $P(Y)$, i.e.

$$F(\underline{c})(Y) = P(Y)\underline{c}(Y) \text{ and } F^t(\underline{c})(Y) = P(Y)^t \underline{c}(Y)$$

Residue class ring

With $\mathbb{F}$ we denote the finite field $\mathbf{GF}(q)$ with $q = p^s$ elements where p is a prime and s is a positive integer.

The set of all maps from $\mathbb{F}$ to $\mathbb{F}$ is denoted as $\overline{\mathbb{F}}[X]$ which can be thought of as residue class ring $\mathbb{F}[X]/(X^q - X)$. In other words, there is a one to one relation of maps from $\mathbb{F}$ to $\mathbb{F}$ and the polynomials of degree less than q with coefficients in $\mathbb{F}$.

The set $\overline{\mathbb{F}}[X]$ becomes a ring with point wise addition and multiplication, i.e.

$$(f + g)(\xi) = f(\xi) + g(\xi)$$

$$(fg)(\xi) = f(\xi)g(\xi)$$

for f, $g \in \overline{\mathbb{F}}[X]$ and $\xi \in \mathbb{F}$.

Linear CA with states in $\overline{\mathbb{F}}[X]$

Let R be the commutative ring $\overline{\mathbb{F}}[X]$. A linear cellular automaton has a local rule given by a polynomial $P(Y)$ in $\overline{\mathbb{F}}[X][Y]$, i.e.,

$$P(Y) = \sum_{i=0}^{k-1} g_i Y^i, \text{ where } g_i \in \overline{\mathbb{F}}[X],\ i = 0, \ldots, k-1.$$

Here we are considering a special initial condition

$$\underline{c}(j) = \begin{cases} 0 & \text{if } j \neq 0 \\ 1 & \text{if } j = 0 \end{cases}$$

Note that 0 and 1 denote the constant maps 0 and 1, respectively.

In this setting, the set $\mathcal{P}(t)$ is generated by the non-zero coefficients of the polynomial $P(Y)^t$. Note that the coefficients of $P(Y)^t$ form a subset of $\overline{\mathbb{F}}[X]$, and therefore the old result is used to describe $\mathcal{P}(t)$.

A first result

The first result is based on

$$\xi^q = \xi \text{ and } p\xi = 0 \text{ for all } \xi \in \mathbb{F}$$

and

$$P(Y)^{qt} = (\sum_{i=0}^{k-1} g_i Y^i)^{qt} = (\sum_{i=0}^{k-1} g_i^q Y^{iq})^t$$

for all $P(Y) \in \overline{\mathbb{F}}[X][Y]$. This leads to

Lemma (Lemma 4). $\mathcal{P}(t) = \mathcal{P}(qt)$

An old result on $\langle M \rangle$

Let R be a finite field $\mathbb{F}$ and let $M \subseteq \overline{\mathbb{F}}[X]$ Then the description of $\langle M \rangle$ is related to the support of M

$$\text{supp}(M) = \{\xi \in \mathbb{F} \mid \text{there is } g \in M \text{ with } g(\xi) \neq 0\}$$

and separability properties of M. If ξ, $\zeta \in \mathbb{F}$, then

$$M \text{ separates } \xi, \zeta, \text{ if there is } g \in M \text{ with } g(\xi) \neq g(\zeta)$$

If ξ and ζ are not separable by M, then they are M-equivalent.

Theorem. *Let M_1, M_2 be subsets of $\overline{\mathbb{F}}[X]$. Then $\langle M_1 \rangle = \langle M_2 \rangle$ if and only if supp(M_1) = supp(M_2) and the M_1-equivalence classes and M_2-equivalence classes coincide.*

On supp($\mathcal{P}(t)$)

For $\xi \in \mathbb{F}$ we denote the ring homomorphism (evaluation map) $\phi_\xi : \overline{\mathbb{F}}[X][Y] \to \mathbb{F}[Y]$ defined as

$$\phi_\xi\left(\sum_{i=0}^{k-1} g_i Y^i\right) = \sum_{i=0}^{k-1} g_i(\xi) Y^i$$

Theorem (Lemma 5)**.**

supp($\mathcal{P}(t)$) = supp($\mathcal{P}(1)$) for all $t \geq 1$.

Proof: The result follows from

$$\phi_\xi(P(Y)^t) = \phi_\xi(P(Y))^t$$

and the fact that $\xi \in \text{supp}(M_t)$ if and only if

$$\phi_\xi(P(Y)^t) \neq 0.$$

Divisibility Properties I

Theorem (Theorem 1)**.**

$$\mathcal{P}(t) = \mathcal{P}(1) \textit{ for all } t \textit{ with } \gcd(t, q-1) = 1.$$

Proof: Apply the old result. By Lemma 5, $\mathcal{P}(t)$ and $\mathcal{P}(1)$ have equal support. It remains to show that the equivalence classes are the same. Note that ξ and ζ are separated by $P(Y)^t$ if and only if

$$\phi_\xi(P(Y)^t) \neq \phi_\zeta(P(Y)^t).$$

If ξ, ζ are $P(Y)$-equivalent, then $\phi_\xi(P(Y)) = \phi_\zeta(P(Y))$ and therefore $\phi_\xi(P(Y))^t = \phi_\zeta(P(Y))^t$, i.e., they are $P(Y)^t$ equivalent. On the other hand, i.e., ξ and ζ are $P(Y)^t$-equivalent, then the useful result implies that ξ and ζ are $P(Y)$-equivalent.

Divisibility Properties II

Theorem (Theorem 3). *Let ξ and ζ be $P(Y)$-separable and let δ be a divisor of $q-1$. ξ and ζ are $P(Y)^{\delta}$-equivalent if and only if there exists a ρ such that $\rho^{\delta} = 1$ and $\phi_{\xi}(P(Y)) = \rho\,\phi_{\zeta}(P(Y))$.*

Proof: The proof relies on the useful result shown in the next slide. Using some properties of the multiplicative group $(\mathbb{F} \setminus \{0\}, \cdot)$ one obtains

Lemma (Lemma 6). *Let $t \in \mathbb{N}$ such that* $\gcd(t, q-1) = \delta$. *Then ξ and ζ are $P(Y)^{t}$-equivalent if and only if they are $P(Y)^{\delta}$-equivalent.*

A Useful Result

Theorem (Lemma 9, Theorem 5). *Let $P(Y)$, $Q(Y)$ be non-zero polynomials with coefficients in $\overline{\mathbb{F}}[X]$ and let $n \in \mathbb{N}$ greater than 1. Then one has:*

$P(Y)^n = Q(Y)^n$ if and only if there exists $\rho \in \mathbb{F}$ such that $P(Y) = \rho\, Q(Y)$.

Consequences:

- $\rho^n = 1$.

- If $\gcd(n, q-1) = 1$, then $\rho = 1$

General Results

Theorem (Lemma 7). *The number $D(q)$ of different $\mathcal{P}(t)$ is bounded by the number of divisors of $q-1$.*

Thus we have the following upper bounds

q	2	3	4	5	7	8	9	11	13	16	17	19	23	25	27
$D(q)$	1	2	2	3	4	2	4	4	6	4	5	6	4	8	4

Lemma (Lemma 8). *If $P(Y)$ and $Q(Y)$ have the same non-zero coefficients in $\overline{\mathbb{F}}[X]$, then $\mathcal{P}(t) = \mathcal{Q}(t)$ for all $t \in \mathbb{N}$.*

This follows from the above considerations. At no place the order of the coefficients is important.

Finally: Example (number 7)

Let $\mathbb{F} = \mathbb{Z}_7 = \{0, 1, \ldots, 6\}$ with addition and multiplication modulo 7. Let $P(Y) = g_0 + g_1 Y + g_2 Y^2 + g_3 Y^3$, where the maps $g_j : \mathbb{F} \to \mathbb{F}$ are given as

$\mathbb{F}$	0	1	2	3	4	5	6
g_0	1	2	6	5	4	1	2
g_1	2	4	5	6	2	4	5
g_2	3	6	4	0	0	0	1
g_3	4	1	3	2	3	6	0

The columns correspond to the evaluation of polynomials $\phi_\xi(P(Y))$.

Since $\mathrm{supp}(\mathcal{P}(1)) = \mathbb{F}$, we have $\mathrm{supp}(\mathcal{P}(t)) = \mathbb{F}$ for all t. Now one has

$$\begin{array}{rcl} \phi_1(P(Y)) & = & 2\,\phi_0(P(Y)) \\ \phi_2(P(Y)) & = & 6\,\phi_0(P(Y)) \\ \phi_4(P(Y)) & = & 5\,\phi_3(P(Y)) \\ \phi_5(P(Y)) & = & 3\,\phi_3(P(Y)) \\ \phi_5(P(Y)) & = & 2\,\phi_4(P(Y)) \end{array}$$

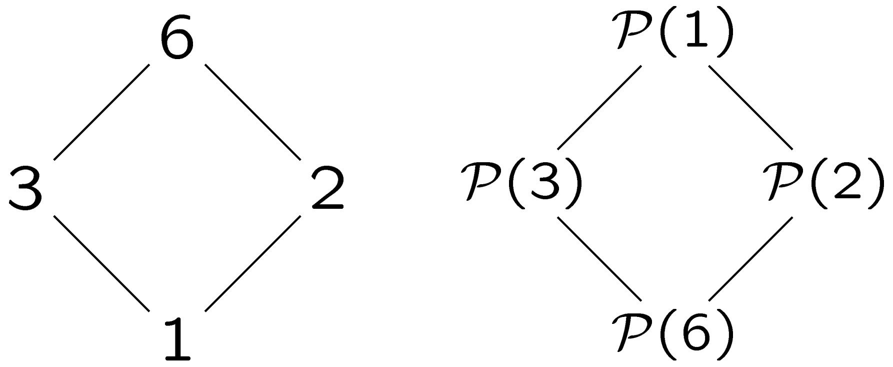
We thus obtain

factor	order	partition
1	1	$\{0\} \cup \{1\} \cup \{2\} \cup \{3\} \cup \{4\} \cup \{5\} \cup \{6\}$
6	2	$\{0,2\} \cup \{1\} \cup \{3\} \cup \{4\} \cup \{5\} \cup \{6\}$
2, 4	3	$\{0,1\} \cup \{4,5\} \cup \{2\} \cup \{3\} \cup \{6\}$
3, 5	6	$\{0,1,2\} \cup \{3,4,5\} \cup \{6\}$

$$\mathcal{P}(t) = \mathcal{P}(\mathrm{gcd}(t,6)) \text{ for any } t$$

Lattice Structure

Comparing the lattices of the divisors of $q-1$ and of the subrings one obtains the following picture



This figure suggests that the lattices are isomorphic.

Future Work

1: Study the relation of the divisor lattice and the lattice of subvectorspace-rings generated by a polynomial $P(Y) \in \overline{\mathbb{F}}[X][Y]$.

2: Consider local rules which are "less linear", e.g.,

$$f(g_1, g_2, g_3) = \lambda_1(g_1) + \lambda_2(g_2) + \lambda_3(g_3),$$

where $\lambda_i : \overline{\mathbb{F}}[X] \to \overline{\mathbb{F}}[X]$ are $\mathbb{F}$-linear maps.

3: Analyse the information dynamics by taking the initial condition $\underline{c} = (\ldots, u, \mathbf{x}, v, \ldots)$, where $\mathbf{x}$ is a variable with values in $\overline{\mathbb{F}}[X]$.

References

1. von Haeseler, Fritz; Nishio, Hidenosuke *On Polynomial Rings in Information Dynamics of linear CA*, Proceedings of Automata 2013, pp 171-186, LNCS 8155, Springer, Berlin (2013).

2. von Haeseler, Fritz *On a problem in information dynamics of cellular automata.* J. Cell. Autom. 1 (2006), no. 4, 377–393.

3. Nishio, Hidenosuke; Saito, Takashi *Information dynamics of cellular automata. I. An algebraic study*. Fund. Inform. 58 (2003), no. 3-4, 399–420.

4. Nishio, Hidenosuke *Completeness and degeneracy in information dynamics of cellular automata*. Mathematical foundations of computer science 2005, 699–707, LNCS 3618, Springer, Berlin (2005).

Thank you for your attention!