ON A POLYNOMIAL REPRESENTATION OF FINITE LINEAR CELLULAR AUTOMATA

Nohmi, Masaya
Department of Artificial Intelligence, Kyushu Institute of Technology

https://doi.org/10.5109/13414

出版情報：Bulletin of informatics and cybernetics. 24 (3/4), pp.137-145, 1991-03. Research Association of Statistical Sciences
バージョン：
権利関係：

Bulletin of Informatics and Cybernetics, Vol. 24, No. 3~4, 1991

ON A POLYNOMIAL REPRESENTATION OF FINITE LINEAR CELLULAR AUTOMATA

By

Masaya NOHMI*

Abstract

This paper decides the behaviour of cellular automata, including the existence of fixed points and the order of configurations, using the polynomial representation of configurations with respect to a basis derived from a series of state transition. We are mainly concerned with cellular automata with local transition rule 90 since the method described here can be used for any finite cellular automata with a little alternations [7].

1. Introduction

In this paper, we are concerned with cellular automata that have linearly-sited cells, and each cell of them has value 0 or 1. S. Wolfram gave a standard numbering to transition rules of this kind of cellular automata [8]. We are mainly concerned with local transition rule 90, that is decided so that the value of a cell is the sum of the values of its two nearest neighbourhoods at the previous time step, where the sum is computed modulo 2. We assume the boundary condition to be null, that is, for the left-most cell, the value of the left-hand neighbourhood is regarded as 0, and for the right-most cell, it is treated similarly.

Figure 1 gives an example of state transition of eight cells. The first column denotes the initial configuration. It can be selected arbitrarily. In this case, we choose the first vector of the standard basis. The second column denotes the configuration at the next time step and so on. We see the state transition to be periodic, and its order is fourteen.

* Department of Artificial Intelligence, Kyushu Institute of Technology, Iizuka 820, Japan

```
10100010000000101000100000001010001000000010100010000000
01000100000000101000100000001010001000000010100010000001
00101010000010001010100000100010101000001000101010000010
00010000000101000100000001010001000000010100010000000101
00001010001000000010100010000000101000100000001010001000
00000100010101000001000101010000010001010100000100010101
00000010100010000000101000100000001010001000000010100010
00000001010001000000010100010000000101000100000001010001
```

Fig. 1. An example of the state transition.

We treat the automaton in more mathematical manner. Let $F_2 = \{0, 1\}$ be the finite field of order 2, and let V_m be the vector space F_2^{m-1}. V_m is the set of all configurations of $m - 1$ cells. For convenience we use m instead of $m - 1$. The transition rule is a linear transformation on V_m and its representative matrix A_m of degree $m - 1$ is

$$A_m = \begin{pmatrix} 0 & 1 & & & & & \\ 1 & 0 & 1 & & & & \\ & 1 & 0 & 1 & & & \\ & & \ddots & \ddots & \ddots & & \\ & & & \ddots & \ddots & \ddots & \\ & & & & \ddots & \ddots & 1 \\ & & & & & 1 & 0 \end{pmatrix}.$$

For convenience, we denote it as follows:

$$ca - 90(m) = (V_m, A_m).$$

2. The Polynomial Representation of Configurations

Let $e_1, e_2, \ldots, e_{m-1}$ be the standard basis of V_m. We choose $m - 1$ vectors

$$f_i = A_m^{i-1} e_1 \ (i = 1, \ldots, m - 1)$$

from V_m. Since the matrix $(f_1, f_2, \ldots, f_{m-1})$ is regular, $f_1, f_2, \ldots, f_{m-1}$ is a basis of V_m. We call it *the transition basis*. We defined V_m as a vector space over F_2, but we can regard it as an $F_2[t]$-module by defining the polynomial multiplication of a vector $v \in V_m$ and a polynomial $f(t) \in F_2[t]$ as follows:

$$f(t) \cdot v = f(A_m)v.$$

Of course, substituting another matrix for $f(t)$, we get another $F_2[t]$-module, and in fact, we use another one later. But if e ($= e_1$) is taken as the vector v, we always substitute A_m for $f(t)$. Since the vectors $f_1, f_2, \ldots, f_{m-1}$ are a basis of V_m, any vector $v \in F_2$ can be uniquely represented as follows:

$$v = a_1 f_1 + a_2 f_2 + \ldots + a_{m-1} f_{m-1} \ (a_i \in F_2).$$

By the definition of the polynomial multiplication, we can rewrite the above equation as

$$v = (a_1 + a_2 t + \ldots + a_{m-1} t^{m-2}) \cdot e_1.$$

Therefore we can uniquely choose a polynomial $f(t) \in F_2[t]$ satisfying the equation $v = f(t) \cdot f_1$ under the condition $\deg(f(t)) \leq m - 2$. We call the polynomial $f(t)$ *the polynomial representation* of v, and emphasizing the configuration v, we often denote it by $f_v(t)$.

We define another square matrix B_m of degree $m - 1$ by

$$B_m = \begin{pmatrix} 0 & & & & & \\ 1 & 0 & & & & \\ & 1 & 0 & & & \\ & & \ddots & \ddots & & \\ & & & \ddots & \ddots & \\ & & & & 0 & \\ & & & & 1 & 0 \end{pmatrix}.$$

Similarly to the case of A_m, we get $F_2[t]$-module by defining the polynomial multiplication on V_m as follows:

$$f(t) \cdot v = f(B_m)v.$$

If $f\,(= f_1)$ is taken as the vector v, we always use the matrix B_m. If a polynomial $f(t) \in F_2[t]$ is written as

$$f(t) = a_1 + a_2 t + \ldots + a_{m-1} t^{m-2} \ (a_i \in F_2),$$

we have

$$f(t) \cdot f = {}^t(a_1, a_2, \ldots, a_{m-1}).$$

3. The Polynomial $\varphi_m(t)$

In describing the behavior of $ca - 90(m)$, we often use the polynomial $\varphi_m(t)$. We recall the definition of it and some formulas from Matsumoto [6]. The polynomial $\varphi_m(t) \in F_2[t]$ is defined by the equations $\varphi_0(t) = 0$, $\varphi_1(t) = 1$ and

$$\varphi_m(t) = t\varphi_{m-1}(t) + \varphi_{m-2}(t) \ (m \geq 2). \tag{1}$$

From the definition, we have some fundamental formulas. For any $m \geq 1$,

$$\deg(\varphi_m(t)) = m - 1, \tag{2}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & t \end{pmatrix}^m = \begin{pmatrix} \varphi_{m-1}(t) & \varphi_m(t) \\ \varphi_m(t) & \varphi_{m+1}(t) \end{pmatrix}, \tag{3}$$

$$\varphi_{m+1}(t)\varphi_{m-1}(t) + \varphi_m(t)^2 = 1. \tag{4}$$

Next, we see the factorization of $\varphi_m(t)$ in $\overline{F}_2$, where $\overline{F}_2$ is the algebraic closure of F_2. Now, we set

$$m = 2^s m' \ ((m', 2) = 1),$$

$$m_1 = \frac{m' - 1}{2},$$

and we denote the primitive m'-th root of unity by ζ, and set $\eta_i = \zeta^i + \zeta^{-i}$. We have the factorization of $\varphi_m(t)$ as follows:

$$\varphi_m(t) = t^{2^s-1} \prod_{i=1}^{m_1} (t - \eta_i)^{2^s+1}. \tag{5}$$

4. Lemmas

In this section, we give a few lemmas, and decide the Jordan normal form of A_m.

PROPOSITION 4.1. *If $m \geq 2$ and $e \in V_m (= F_2^{m-1})$, then*

$$\phi_m(t)e = 0.$$

PROOF. The proof is by induction on m. For $m = 2, 3$, it is trivial. Now, assume the theorem to be true in the case of $m - 2$; $\varphi_{m-2}(t)e = 0$ on V_{m-2}. Correcting errors derived from the difference between V_{m-2} and V_m, we have $\varphi_{m-2}(t)e = e_{m-2}$ on V_m. Similarly, $\varphi_{m-1}(t)e = e_{m-1}$ holds on V_m. Therefore, we have

$$\varphi_m(t)e = (t\varphi_{m-1}(t) + \varphi_{m-2}(t))e = A_m e_{m-1} + e_{m-2} = 0,$$

as required. ∎

PROPOSITION 4.2. *If $\varphi_m(t)$ is written as*

$$\varphi_m(t) = t^{m-1} + a_{m-2}t^{m-2} + \ldots + a_1 t + a_0,$$

then

$$A_m f_{m-1} = \sum_{i=1}^{m-1} a_{i-1} f_i.$$

PROOF. From Proposition 4.1, we have

$$\begin{aligned} 0 &= \varphi_m(t)e \\ &= (A_m^{m-1} + a_m{-}2\, A_m^{m-2} + \ldots + a_1 A_m + a_0)e \\ &= A_m^{m-1}e + a_{m-2}f_{m-1} + \ldots + a_1 f_2 + a_0 f_1 \\ &= A_m f_{m-1} + \sum_{i=1}^{m-1} a_{i-1} f_i. \end{aligned}$$

Transposing the term $A_m f_{m-1}$ to the left-hand side, we get the result. ∎

Let ${}^t\widetilde{A}_m$ be the representative matrix of the transition rule of a $ca - 90(m)$ with respect to the basis $f_1, f_2, \ldots, f_{m-1}$. It is transposed for convenience. The index m is

often omitted. By the Proposition 4.2, setting

$$\varphi_m(t) = t^{m-1} + a_{m-2}t^{m-2} + \ldots + a_1 + a_0,$$

we have,

$$^t\widetilde{A} = \begin{pmatrix} 0 & 1 & & & & \\ & 0 & 1 & & & \\ & & 0 & 1 & & \\ & & & \ddots & \ddots & \\ & & & & 0 & 1 \\ a_0 & a_1 & & \ldots & a_{m-3} & a_{m-2} \end{pmatrix}. \tag{6}$$

It is easy to confirm the characteristic polynomial of the matrix (6) is $\varphi_m(t)$. Let $H_{m'}$ be the set of non-zero roots of the polynomial $\varphi_m(t)$. From factorization (5), we have $H_{m'} = \{\eta_i = \zeta^i + \zeta^{-i} | i = 1, \ldots, m_1\}$. Denoting the $n \times n$ Jordan block corresponding to the eigenvalue $\alpha \in \overline{F_2}$ by $J_n(\alpha)$, we have the Jordan normal form J of $\widetilde{A}$ as follows:

$$J = \bigoplus_{i=1}^{m_1} J_{2^{s+1}}(\eta_i) \oplus J_{2^s-1}(0). \tag{7}$$

Next we give the matrix P satisfying the equation

$$\widetilde{A} = PJP^{-1}. \tag{8}$$

For $\alpha \in \overline{F_2}$, we define an $(m-1) \times n$ matrix $P_n(\alpha)$ by

$$P_n(\alpha) = \begin{pmatrix} 1 & & & & \\ \alpha & 1 & & & \\ \alpha^2 & \binom{2}{1}\alpha & 1 & & \\ \vdots & \vdots & \vdots & \ddots & \\ \vdots & \vdots & \vdots & & 1 \\ \vdots & \vdots & \vdots & & \vdots \\ \alpha^{m-2} & \binom{m-2}{1}\alpha^{m-3} & \binom{m-2}{2}\alpha^{m-4} & \ldots & \binom{m-2}{n-1}\alpha^{m-n-1} \end{pmatrix}, \tag{9}$$

that is, the (i, j)-element of $P_n(\alpha)$ is

$$\binom{i-1}{j-1}\alpha^{i-j} \quad (1 \leq i \leq m-1,\ 1 \leq j \leq n).$$

The matrix P satisfying the equation (8) is as follows:

$$P = (P_{2^{s+1}}(\eta_1), \ldots, P_{2^{s+1}}(\eta_{m_1}), P_{2^s-1}(0)).$$

PROPOSITION 4.3. *If a polynomial* $f(t) \in F_2[t]$ *satisfies* $\deg(f(t)) \leq m-2$, *then for any* $\alpha \in F_2$,

$$ {}^tP_n(\alpha)\, f\,(t) \cdot f_1 = \begin{pmatrix} f(\alpha) \\ f'(\alpha) \\ \frac{1}{2}f''(\alpha) \\ \vdots \\ \frac{1}{(n-1)!} f^{(n-1)}(\alpha) \end{pmatrix} . $$

5. Applications to Transition Diagrams

Vector space V_m is a direct sum of the set of infinite images and the set of infinite kernels; $V_m = \mathrm{Im}A^\infty \oplus \mathrm{Ker}A^\infty$. First, we decide the construction of *the kernel tree* that is the transition diagram whose verteces are restricted to the infinite kernel and the edge from 0 to 0 is removed. It is a binary tree, except the root has only one edge, and each leaf has the same depth. So, we can decide the construction of the kernel tree only by the depth of it. A vertex corresponding to infinite image appears as a node on a loop, and each node is connected to a tree isomorphic to the kernel tree. So, we can decide the global constitution of transition diagram by the order of each loop.

THEOREM 5.1. *We can select bases of* $\mathrm{Im}A^\infty$ and $\mathrm{Ker}A^\infty$ *as follows*:

$$ \mathrm{Im}A^\infty = \left\langle t^{2^s}, t^{2^s+1}, \ldots, t^{m-1} \right\rangle_{F_2}, $$

$$ \mathrm{Ker}A^\infty = \left\langle \frac{\varphi_m(t)}{t}, \frac{\varphi_m(t)}{t^2}, \ldots, \frac{\varphi_m(t)}{t^{2^s-1}} \right\rangle_{F_2} . $$

For any configuration, we can decide whether it is an element of $\mathrm{Im}A^\infty$ or not, by the next theorem.

THEOREM 5.2. *For any configuration* $x \in V_m$,

$$ x \in \mathrm{Im}A^\infty \Leftrightarrow f_x(t) \equiv 0 \pmod{\deg 2^s}. $$

Next, we decide the order of each configuration, using the polynomial representation. Let A be the set of all orders. It is easily seen that $\Lambda = \{1, 2, \ldots, 2^{s+1}\} \times \{\mathrm{ord}\,(\eta_i)\} \cup \{1\}$. For each $\lambda = 2^i\lambda' \in \Lambda$ (λ' : odd), we define the discriminant as follows:

$$ \Phi_\lambda(t) = \prod_{\mathrm{ord}(\eta_i)|\lambda'} t^{2^s-1}(t-\eta_i)^{2^i}. \tag{10} $$

We often use the quotient polynomial $\psi_\lambda(t)$ of $\Phi_\lambda(t)$ defined as follows in stead of $\Phi_\lambda(t)$:

$$ \varphi(m) = \psi_\lambda(t)\Phi_\lambda(t). \tag{11} $$

Figure 2 gives an example of the quotient polynomials in the case of $m = 60$.

THEOREM 5.3. *For any infinite image* x,

$$ord(x) \mid \lambda \quad \Leftrightarrow \quad \Phi\lambda(t) \mid f_x(t).$$

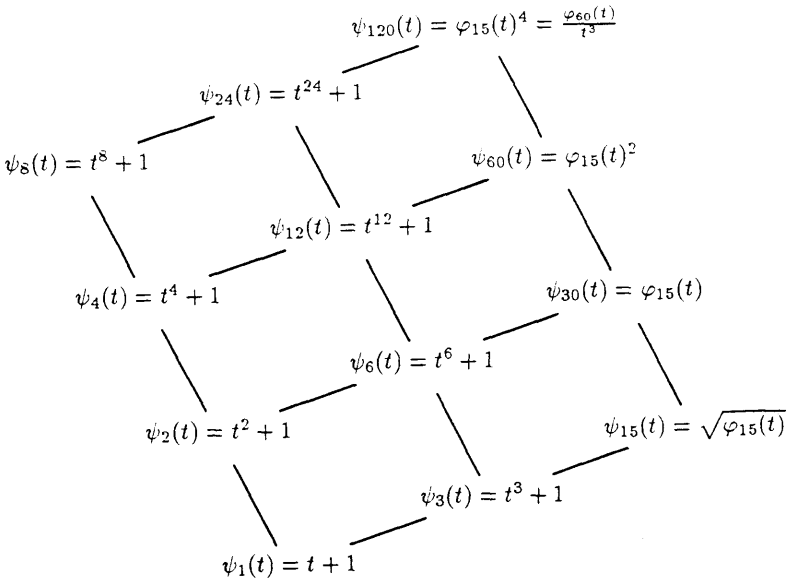

Fig. 2. An example of quotient polynomials.

6. Local Properties of $ca - 90(m)$

If the configuration $e_1 + e_{m-1} \in V_m$ is included in $\mathrm{Im}A^\infty$, we denote the order of it by $K(m)$. First, we discuss the existence of $K(m)$.

THEOREM 6.1. *$K(m)$ exists if and only if $4 \nmid m$.*

PROOF. In the case m is odd, the linear transformation A is regular, so the result is trivial. In the case m is even, we apply Proposition 5.2 to the polynomial $1 + \varphi_{m-1}(t)$ which is the polynomial representation of $e_1 + e_{m-1}$. If $m = 2m'(m'$: *odd*$)$, we have

$$\varphi_m(t) + 1 \equiv 0 \ (\mathrm{mod\ deg}\ 2),$$

so $e_1 + e_{m-1} \in \mathrm{Im}A\infty$. If $m = 2^s m'(s \geq 2,\ m'$: odd), then

$$\varphi_m(t) \equiv t^{2^{s-1}} \ (\mathrm{mod\ deg}\ 2^s)$$

$$\varphi_{m-2}(t) \equiv t \ (\mathrm{mod\ deg}\ 2)$$

so,

$$\varphi_{m-1}(t)^2 + 1 \equiv t^{2^s} \ (\mathrm{mod\ deg}\ 2^s + 2).$$

Hence,

$$\varphi_{m-1}(t) + 1 \not\equiv 0 \ (\mathrm{mod\ deg}\ 2^s).$$

Therefore, $K(m)$ doesn't exist in this case. ∎

PROPOSITION 6.2. *For all* $\eta_i \in H_m'$,

$$\varphi_m(\eta_i) = 0, \tag{12}$$

$$\varphi_{m-1}(\eta_i) = 1, \tag{13}$$

and if m is odd, then

$$\varphi_{m-1}(\eta_i)' = \eta_i^{-1}. \tag{14}$$

PROOF. (12) is trivial. (13) is easily seen by substituting η_i for (4). From the differentiation of (2), we have

$$\varphi_m(t) = \varphi_{m-1}(t) + t\varphi_{m-1}(t)' + \varphi_{m-2}(t)'.$$

Substituting η_i for it, we have (14). ∎

PROPOSITION 6.3. *If* $\eta_i \in H_{m'}$, *then*

$${}^t J(\eta_i)^n = \begin{pmatrix} \eta_i^n & & & \\ \binom{n}{1}\eta_i^{n-1} & \eta_i^n & & \\ \vdots & \vdots & \ddots & \\ \binom{n}{m-2}\eta_i^{n-m+2} & \binom{n}{m-3}\eta_i^{n-m+3} & \cdots & \eta_i^n \end{pmatrix}, \tag{15}$$

$${}^t J_2(\eta_i)^{2^{\mathrm{subord}_m(2)}-1} = \begin{pmatrix} 1 & \\ \eta_i^{-1} & 1 \end{pmatrix}. \tag{16}$$

PROOF. The proof is by induction on n. (16) directly follows from (15). ∎

THEOREM 6.4. *If m is odd, then*

$$K(m) | 2^{\mathrm{subord}_m(2)} - 1.$$

PROOF. By the matrix ${}^tP$, the configuration vector $(\varphi_{m-1}(t) + 1) \cdot f$ is mapped on the vector

$${}^tP(\varphi_{m-1}(t) + 1) \cdot f = \begin{pmatrix} \varphi_{m-1}(\eta_1) + 1 \\ \varphi_{m-1}(\eta_1)' \\ \varphi_{m-1}(\eta_2) + 1 \\ \varphi_{m-1}(\eta_2)' \\ \vdots \\ \varphi_{m-1}(\eta_{m_1}) + 1 \\ \varphi_{m-1}(\eta_{m_1})' \end{pmatrix} = \begin{pmatrix} 0 \\ \eta_1^{-1} \\ 0 \\ \eta_2^{-1} \\ \vdots \\ 0 \\ \eta_{m_1}^{-1} \end{pmatrix}.$$

Denoting this vector by x, we have

$$
\begin{aligned}
&{}^tJ^{2^{\mathrm{subord}_m(2)}-1}x \\
&= ({}^tJ_2(\eta_1)^{2^{\mathrm{subord}_m(2)}-1} \oplus \cdots \oplus {}^tJ_2(\eta_{m_1})^{2^{\mathrm{subord}_m(2)}-1})x \\
&= x,
\end{aligned}
$$

by Proposition 6.3. ∎

At last, we discuss the existence of fixed points.

THEOREM 6.5. *There exist non-trivial fixed points if and only if* $3|m$. *In this case, the subspace of fixed points is given as follows:*

$$\left\langle \frac{\varphi_m(t)}{t-1} \right\rangle_{F_2}.$$

PROOF. First, we search fixed points in the algebraic closure $\overline{F_2}^{m-1}$, and then we confirm they are included in F_2^{m-1}. Assume that J has a non-trivial fixed point in $\overline{F_2}^{m-1}$, that is, there exists one Jordan block of J such that

$$ {}^tJ_{2^{s+1}}(\eta_i) - I_{2^{s+1}} \tag{17}$$

is degenerate. It is equivalent to $\eta_i = 1$ and $\zeta^{2i} + \zeta^i + 1 = 0$. It means ζ^i is a third root of unity, so we have $3|m$. It is easily seen that the dimension of the kernel of (17) is 1. By

$$P_{2^{s+1}}(\eta_i)\frac{\varphi_t(t)}{t-1} = \begin{cases} 0 & (\eta_i \neq 1) \\ {}^t(0, \ldots, 0, 1) & (\eta_i = 1) \end{cases}$$

we see the polynomial representation

$$\frac{\varphi_m(t)}{t-1}$$

gives a unique non-trivial fixed point.

References

[1] GUAN, P., HE, Y.: *Exact results for deterministic cellular automata with additive rules*, J. of Statist. Phys, **43**, ¾ (1986).

[2] JEN, E.: *Cylindrical cellular automata*, Commun. Math. Phys. **118** (1988), 569–590.

[3] JEN, E.: *Global properties of cellular automata*, J. of Statist. Phys, **43**, ½ (1986).

[4] LI, W.: *Power spectra of regular languages and cellular automata*, Complex Systems, **1** (1987), 107–130.

[5] MARTIN, O., ODLYZKO M., WOLFRAM, S.: *Algebraic properties of cellular automata*, Commun. Math. Phys, **93** (1984), 219–258.

[6] MATSUMOTO, M.: *On cellular automaton CA − 90(m)*, Note, (1988).

[7] NOHMI, M.: *On transition diagrams of finite cellular automata*, in preparation.

[8] WOLFRAM, S.: *Statistical mechanics of cellular automata*, Rev. Mod. Phys. **55** (1982).

Received September 7, 1990
Communicated by Y. Kawahara