(Non)-Automaticity of Orbits of Linear Cellular Automata

Fritz v. Haeseler[1]

Center for Complex Systems and Visualization

University of Bremen

D-28334 Bremen

This is an abridged version of a joint paper, see [3], on the automaticty of orbits of linear cellular automata. We present an extension of results in [2, 6].

1 Preliminaries

Let us quickly recall what k-automatic sequences and double sequences are. For more details on automatic sequences the reader is referred to e.g. [1].

Definition 1 *Let $p \geq 2$ be an integer. A sequence $\{x(n)\}_{n\in\mathbb{N}}$ with values in a finite set is called p-automatic if its p-kernel, i.e., the set of subsequences*

$$\{n \mapsto x(p^i n + j) \mid i \geq 0, 0 \leq j \leq p^i - 1\},$$

is finite.

The double sequence $\{u(n,k)\}_{n,k\in\mathbb{N}}$ with values in a finite set is called p-automatic if the p-kernel, i.e., the set

$$\{n \mapsto u(p^i n + j, p^i k + l) \mid i \geq 0, 0 \leq j, l \leq p^i - 1\},$$

is finite.

Most important for our considerations is the following version of Cobham's Theorem, see [4].

Theorem 2 (Cobham)

- *Let p_1, p_2 be different prime numbers. A sequence $\{x(n)\}$ is p_1-automatic and p_2-automatic if and only if $\{x(n)\}$ is eventually periodic.*
- *Let p be a prime number. If $\{x(n)\}$ is not eventually periodic and p-automatic, then $\{x(n)\}$ is k-automatic if and only if $k = p^a$ for some $a \in \mathbb{N}$.*

Let m be a natural number. We denote the set of residue classes of $\mathbb{Z}$ modulo m by $\mathbb{Z}_m$. Furthermore, we consider the set $\mathbb{Z}_m$ as a ring with ring structure induced

[1]supported by the Deutsche Forschungsgemeinschaft Forschungsgruppe "Dynamische Systeme"

by the ring structure of $\mathbb{Z}$. Any polynomial $R(x) \in \mathbb{Z}_m[x]$ induces a linear cellular automaton on the configuration space

$$\Sigma(\mathbb{Z}_m) = \left\{ f(x) = \sum_{j \in \mathbb{Z}} a_j x^j \mid a_j \in \mathbb{Z}_m \right\}$$

by $f(x) \mapsto f(x)R(x)$. Given an initial condition $a(x) \in \mathbb{Z}_m[x]$, we are concerned with the orbit description of $a(x)$ under the cellular automaton induced by a polynomial $R(x) \in \mathbb{Z}_m[x]$. We write the orbit as a formal power series in two variables, i.e.,

$$F(X,Y) = \sum_{t=0}^{\infty} a(X)R(X)^t Y^t = \sum_{n,t=0}^{\infty} f(n,t) X^n Y^t.$$

We thus obtain a double sequence $(f(n,t))$, and we are interested under what conditions is the double sequence automatic. Some first results in that regard are:

Theorem 3 ([2, 6]) *Let m be a natural number, $m \geq 2$, and let $R(x) = 1 + x \in \mathbb{Z}_m[x]$ and $a(x) = 1$, then $(f(n,t))$ is p-automatic (p a prime number) if and only if $m = p^\alpha$ for some $\alpha \in \mathbb{N}$.*

More generally, we have

Theorem 4 ([2]) *Let p be a prime number and let $R(x), a(x) \in \mathbb{Z}_{p^\beta}[x], \beta \in \mathbb{N}$. Then $F(X,Y)$ is p-automatic.*

The proof of the above theorem relies on the little Fermat Theorem. It states that $R(x)^p = R(x^p)$ for all $R(x) \in \mathbb{Z}_p[x]$ and p a prime number. This observation yields the following

Theorem 5 ([3]) *Let $R(x) \in \mathbb{Z}_m[x]$ such that $R(x)^k = R(x^k)$ for a $k \geq 2$, then $(f(n,t))$ is k-automatic.*

2 The main result

In this section, we state the main result together with a sketch of the proof. For details we refer the reader to [3].

Theorem 6 ([3]) *Let $r(x), a(x) \in \mathbb{Z}[x]$ and let $m \geq 2$ be a natural number. Let*

$$F(X,Y) = \sum_{n,t=0}^{\infty} f(n,t) X^n Y^t = \sum_{t=0}^{\infty} a(x) r(x)^t Y^t$$

denote the orbit of $a(x)$ under the cellular automaton $r(x)$ in $\mathbb{Z}$. Furthermore, let χ be the number of different prime divisors p of m for which $r(x)$ mod p is not a monomial. Then the following holds

- *If $\chi \geq 2$, there is no value of $k \geq 2$ for which $(f(n,t)$ mod $m)$ is k-automatic.*
- *If $\chi = 1$, then $(f(n,t)$ mod $m)$ is k-automatic if and only if $k = p^\alpha$, where $\alpha \geq 2$ and p is the prime divisor for which $r(x)$ mod m is not a monomial.*
- *If $\chi = 0$, then $(f(n,t)$ mod $m)$ is k-automatic for all $k \geq 2$.*

The main ingredient of the proof of the above theorem is the following lemma

Lemma 7 (Slice Lemma) *Let p be a prime number and let $r(x)$ mod p be not a monomial, let $a(x) \in \mathbb{Z}_p[x]$. Then there exist $\alpha, \beta \in \mathbb{N}$ such that the sequence $u_p(n) = \{f(\alpha n, \beta n) \text{ mod } p\}_{n \in \mathbb{N}}$ is not eventually periodic.*

The proof of the lemma makes use of the geometrical description, cf.[5], of the orbit. We are now able to sketch the proof of the main theorem.

- Let p, q be different prime numbers such that $r(x)$ mod $p, r(x)$ mod q are not monomials, respectively. Now suppose $(f(n,m)$ mod $m)$ to be k-automatic, then, by the Slice Lemma, there exists a sequence $u_p(n)$ which is k-automatic and p-automatic. By Cobham's Theorem, it follows that $k = p^a$. On the other hand, there exists a sequence $u_q(n)$ which is k-automatic and q-automatic, therefore $k = q^b$; which is a contradiction.
- Let p be the only prime divisor of m such that $r(x)$ mod p is not a monomial, let $m = p^a q_1^{a_1} \cdots q_w^{a_w}$ be the prime factorisation of m. Then there exist $\alpha_j, j = 1, \ldots, w$, such that $g_j(x) = r(x)^{\alpha_j}$ has the property $g_j(x)^k = g_j(x^k)$ mod $q_i^{a_i}$. Moreover, there exists an α such that $g(x) = r(x)^\alpha$ has the property $g(x)^p = g(x^p)$ mod p^a. Then $G(x) = r(x)^{\alpha\alpha_1\cdots\alpha_w}$ has the property $G(x)^p = G(x^p)$ mod p. Hence $(f(n,t)$ mod $m)$ is p-automatic. By the Slice Lemma, we obtain that $(f(n,t)$ mod $m)$ is k-automatic if an only if k is of the form $k = p^\alpha$.
- A similar reasoning as for the second case shows that there exists a natural number M such that $G(x) = r(x)^M$ has the property $G(x)^k = G(x^k)$ mod m. Therefore the sequence $(f(n,t)$ mod $m)$ is k-automatic for all $k \geq 2$

References

[1] J.-P. Allouche, Automates finis en théorie des nombres, Expo. Math. 5 (1986), 239-266

[2] J.-P. Allouche, F. v.Haeseler, H.-O. Peitgen, G. Skordev, Linear cellular automata, finite automata, and Pascal's triangle, Discrete Appl. Math. (to appear)

[3] J.-P. Allouche, F. v.Haeseler, H.-O. Peitgen, A. Petersen, G. Skordev, Automaticity of double sequences generated by one-dimensional linear cellular automata, submitted

[4] A. Cobham, On the base-dependence of sets of numbers recognizable by finite automata, Math. Systems Theory 3 (1969), 186-192

[5] F. v.Haeseler, H.-O. Peitgen, G. Skordev, On the fractal structure of rescaled evolution sets of cellular automat and attractors of dynamical systems, Inst. Dyn. Syst., University of Bremen, Report 278, 1992

[6] I. Korec, Pascal's triangles modulo n and modular trellises, Computers and Artificial Intelligence 9 (1990), 105-113