Automaticity of double sequences generated by one-dimensional linear cellular automata

J.-P. Allouche, F. von Haeseler*, H.-O. Peitgen, A. Petersen§, G. Skordev

Abstract We give a complete answer to the question whether a double sequence that is generated by a one-dimensional linear cellular automaton, and whose states are integers modulo m, is k-automatic or not.

1 Introduction

Can the infinite double sequence generated by a linear one-dimensional cellular automaton whose values are integers modulo m be produced by a two-dimensional finite automaton? Recall that a linear one-dimensional cellular automaton can be defined by a polynomial $R(X)$. The configuration at time t is given by the coefficients of the polynomial $R(X)^t$. The double sequence generated by the cellular automaton is the sequence $(r(n,t))_{n,t\geq 0}$ defined by

$$R(X)^t = \sum_{n\geq 0} r(n,t)X^n.$$

In [12], [13], and [3] this question was addressed for k-Fermat cellular automata, i.e., cellular automata defined by k-Fermat polynomials. A polynomial $R(X)$ with coefficients in a given ring is called k-Fermat if $R(X^k) = R(X)^k$. The definition of k-Fermat polynomials is clearly inspired by the little Fermat theorem ([14] p. 65) which can be reformulated as follows: let p be a prime number and let $\mathbb{F}_p$ be the Galois field with p elements. Let $R(X) \in \mathbb{F}_p[X]$, then $R(X)$ is p-Fermat.

In [12], [13], and [3] it is shown that a linear one-dimensional cellular automaton defined by a polynomial $R(X)$ with coefficients in a finite commutative ring with unit generates a k-automatic double sequence if some power of $R(X)$ is k-Fermat. Furthermore, in [3] and [16] it is shown that the Pascal triangle modulo m, obtained by taking $R(X) = 1 + X$, is k-automatic if and only if m and k are nonzero powers of a same prime number. A similar result holds for the Lucas numbers and the signless Stirling numbers of the first kind, see [3].

In this paper, we address the general question. Namely, let $R(X), A(X) \in \mathbb{Z}[X]$ be two polynomials with integer coefficients, and let $m \in \mathbb{N}$, $m \geq 2$, be a natural number. Then, the linear cellular automaton defined by $R(X)$ modulo m, and a non-trivial initial condition $A(X)$ modulo m, generates a double sequence which is the orbit of $A(X)$ modulo m under the action of the linear cellular automaton. We provide a necessary and sufficient condition for the automaticity of this double sequence. The main result is:

let χ be the number of prime divisors p of m for which the polynomial $R(X)$ reduced modulo p is not a monomial. Then,

*Supported by the DFG-Forschergruppe "Dynamische Systeme".
§Supported by the DFG-Graduiertenkolleg "Komplexe Dynamische Systeme".

- *if $\chi \geq 2$, there is no value of $k \geq 2$ for which the double sequence is k-automatic,*
- *if $\chi = 1$, the double sequence is p^a-automatic, where p is the prime reduction for which $R(X)$ is not a monomial and a is any integer ≥ 1, and this sequence is not k-automatic for any $k \geq 2$ that is not a power of p.*
- *if $\chi = 0$ the double sequence is k-automatic for every $k \geq 2$.*

As a consequence of the previous result we obtain: *the double sequence generated by a one-dimensional linear cellular automaton modulo m, with a non-trivial initial condition, is k-automatic for some $k \geq 2$ if and only if a power of the polynomial defining the cellular automaton is k-Fermat.* Furthermore, we have the surprising result: *if the double sequence generated by a one-dimensional linear cellular automaton modulo m, with a non-trivial initial condition, is k-automatic for some $k \geq 2$, where k is not a power of a prime number, then it is k-automatic for every $k \geq 2$.* As an application of the above mentioned result we show a similar result for *the (signless) Stirling numbers of the first kind modulo m and for the Gaussian q-binomials modulo m, when m and q are coprime.*

Note that, from the Cobham-Semenov theorem, a b-dimensional sequence $u : \mathbb{N}^b \to A$ is k-automatic for all k if and only if it is definable in $\langle \mathbb{N}, + \rangle$ which is equivalent to saying that for every $a \in A$ the set $u^{-1}(a)$ is a rational subset of the monoid $\mathbb{N}^b$, or, equivalently, a semilinear subset of the monoid $\mathbb{N}^b$, [11]. For these questions the reader should read the beautiful survey [5].

2 The general framework

We study one-dimensional linear cellular automata on the ring $\mathbb{Z}/m\mathbb{Z}$. We have a local transition rule: $\varphi : \{0, 1, \cdots, m-1\}^{d+1} \to \{0, 1, \cdots, m-1\}$ that is linear, i.e., there exist r_i's such that, for $x_i \in \{0, 1, \cdots, m-1\}$, one has

$$\varphi(x_0, \cdots, x_d) = \sum_{i=0}^{d} r_{d-i} x_i.$$

The linear cellular automaton is the map $\mathcal{C} : \{0, 1, \cdots, m-1\}^{\mathbb{Z}} \to \{0, 1, \cdots, m-1\}^{\mathbb{Z}}$, defined on the set of all "configurations", by:

$$\mathcal{C}(\mathbf{a})(n) = \varphi(a_{n-d+1}, \cdots, a_n),$$

for $\mathbf{a} \in \{0, 1, \cdots, m-1\}^{\mathbb{Z}}$. The polynomial $R(X) = \sum_{i=0}^{d} r_i X^i$ is associated with the linear cellular automaton $\mathcal{C}$ and called its generating polynomial. Furthermore, any polynomial defines a linear cellular automaton in this way. We call also $R(X)$ the cellular automaton itself. For these notions one can read [15] for example.

The cellular automaton generates, starting from an initial condition $\mathbf{a} \in \{0, 1, \cdots, m-1\}^{\mathbb{Z}}$, a double sequence $(\mathcal{C}^t(\mathbf{a})(n))_{n,t \geq 0} = (r(n,t))_{n,t \geq 0}$. An initial condition $\mathbf{a}$ is represented by a formal Laurent series $\sum_{n \in \mathbb{Z}} \mathbf{a}(n) X^n$. We only consider initial conditions corresponding to polynomials $A(X)$. Then:

$$A(X) R(X)^t = \sum_{n \geq 0} r(n,t) X^n.$$

We say that $(r(n,t))_{n,t \geq 0}$ is the double sequence generated by the linear cellular automaton $R(X)$, with initial condition $A(X)$. For example, if $R(X) = 1 + X$ modulo m, and if $A(X) = 1$ modulo m, then, the double sequence $(r(n,t))_{n,t \geq 0}$ is the Pascal triangle modulo m.

Note that we could also consider the case where the initial condition is a Laurent polynomial, using the generalization of automaticity to sequences with indices in $\mathbb{Z}$ or $\mathbb{Z}^2$ studied in [2].

Let us recall quickly what k-automatic sequences and double sequences are. For more details the reader can read for example [8], [9], [10], [6], [1], [18], [19]. We only give the "combinatorial" definition.

Definition 1 *Let $k \geq 2$ be an integer. A sequence $(u(n))_{n\geq 0}$ with values in a finite set is called k-automatic if its k-kernel is finite, where the k-kernel is the set of subsequences*

$$\{n \longrightarrow u(k^i n + j);\ i \geq 0,\ 0 \leq j \leq k^i - 1\}.$$

The double sequence $(v(n,t))_{n,t\geq 0}$ with values in a finite set is called k-automatic if its k-kernel is finite, where the k-kernel is the set

$$\{(n,t) \longrightarrow v(k^i n + j, k^i t + \ell);\ i \geq 0,\ 0 \leq j, \ell \leq k^i - 1\}.$$

3 The slice lemma

Our main tool in [3] to prove the non-automaticity of Pascal's triangle modulo a number m that is not a prime power, is the existence of non-ultimately periodic one-dimensional subsequences. More precisely, the following formula holds over $\mathbb{Q}$,

$$F(X) = \sum_{n\geq 0} \binom{2n}{n} X^n = \frac{1}{\sqrt{1-4X}}.$$

Hence, in any field $\mathbb{F}_p$, with $p \neq 2$, the formal power series $F(X)$ satisfies the non-trivial algebraic equation

$$(1-4X)F(X)^2 = 1.$$

For $\mathbb{F}_2$, we characterized the power series

$$G(X) = \sum_{n\geq 0} \binom{3n}{n} X^n \bmod 2$$

as a solution of the cubic algebraic equation

$$XG(X)^3 + G(X) + 1 = 0 \bmod 2.$$

Using these algebraic equations we were able to show that the subsequences $(\binom{2n}{n} \bmod p)_{n\geq 0}$, $p \geq 3$, and $(\binom{3n}{n} \bmod 2)_{n\geq 0}$, are not ultimately periodic, respectively.

In this section, we will show that slices (i.e., one-dimensional subsequences) of the double sequences we study, are not ultimately periodic. In contrast to our procedure in [3], we will prove directly that some slices are not ultimately periodic. The task of finding an algebraic equation for the slices we study seems to be hopeless for the general situation.

Lemma 1 (Slice lemma)

Let p be a prime number. Let $R(X) = 1 + aX^\alpha + \cdots + bX^\beta$ be a polynomial in $\mathbb{F}_p[X]$ with $a \neq 0$ and $\alpha \geq 1$. The linear cellular automaton generated by $R(X)$, with initial condition equal to

1, *induces a double sequence* $(r(n,t))_{n,t\geq 0}$ *defined by* $R(X)^t = \sum_{n,t\geq 0} r(n,t)X^n$. *Let* ℓ *be an integer such that* $\alpha p^\ell > \beta p^{-\ell} + \beta$ *and define the unidimensional sequence* $u = (u(n))_{n\geq 0}$ *by*

$$u(n) = r(\alpha p^\ell n, (p^\ell + 1)n).$$

Then the sequence u *is not ultimately periodic.*

Proof

Firstly, we will prove that there are infinitely many integers $n \in \mathbb{N}$ such that $u(n) \neq 0$. Secondly, we will show that, for every k, there exists an n_0 such that $u(n_0) = u(n_0+1) = \ldots = u(n_0+k) = 0$. Therefore, the sequence $(u(n))_{n\geq 0}$ is not ultimately periodic.

1) Since $R(X)$ is a p-Fermat polynomial we have

$$\sum_{n\geq 0} r(n,pt)X^n = R(X)^{pt} = R(X^p)^t = \sum_{n\geq 0} r(n,t)X^{pn}.$$

Hence, $r(pn,pt) = r(n,t)$ holds for all n and t. This yields, for all n,

$$u(pn) = u(n).$$

Now one has

$$\begin{aligned}
\sum_{n\geq 0} r(n,p^\ell+1)X^n = R(X)^{p^\ell+1} &= R(X)^{p^\ell}R(X) = R(X^{p^\ell})R(X) \\
&= (1 + aX^{\alpha p^\ell} + \ldots + bX^{\beta p^\ell})(1 + aX^\alpha + \ldots + bX^\beta) \\
&= (1 + aX^\alpha + \ldots + bX^\beta) + aX^{\alpha p^\ell}(1 + aX^\alpha + \cdots + bX^\beta) \\
&\quad + \ldots + bX^{\beta p^\ell}(1 + aX^\alpha + \ldots + bX^\beta).
\end{aligned}$$

As $\alpha p^\ell > \beta p^{-\ell} + \beta > \beta$, then

$$u(1) = r(\alpha p^\ell, p^\ell + 1) = a$$

and, for all $k \in \mathbb{N}$,

$$u(p^k) = u(1) = a \neq 0.$$

2) We will prove that, if $k \geq \ell$, and if n is such that

$$\frac{p^k}{p^\ell + 1} < n < p^{k-\ell},$$

then $u(n) = 0$. Note that the length of this interval goes to infinity as k goes to infinity. Let n be as above, then, for $k \geq \ell$,

$$p^k < (p^\ell + 1)n < p^k + p^{k-\ell}.$$

Hence there exists a j_n such that

$$0 < j_n < p^{k-\ell} \text{ and } (p^\ell + 1)n = p^k + j_n.$$

Now

$$\begin{aligned} R(X)^{p^k+j_n} &= \sum_{m\geq 0} r(m,p^k+j_n)X^m = \sum_{m\geq 0} r(m,(p^\ell+1)n)X^m \\ &= R(X)^{p^k}R(X)^{j_n} = R(X^{p^k})R(X)^{j_n} \\ &= (1+aX^{\alpha p^k}+\cdots+bX^{\beta p^k})(1+aX^{\alpha}+\cdots+bX^{\beta})^{j_n}. \end{aligned}$$

For X^m such that

$$(*) \qquad \beta j_n < m < \alpha p^k,$$

we obtain $r(m,p^k+j_n)=0$, indeed $\beta j_n < \beta p^{k-\ell} < \alpha p^\ell p^{k-\ell} = \alpha p^k$. Now it suffices to prove that the integers $m=\alpha p^\ell n$ satisfy $(*)$, where

$$\frac{p^k}{p^\ell+1} < n < p^{k-\ell}.$$

We obtain

$$\frac{\alpha p^{k+\ell}}{p^\ell+1} < \alpha p^\ell n < \alpha p^k$$

and

$$\beta j_n < \beta p^{k-\ell} < \frac{\alpha p^{k+\ell}}{p^\ell+1}$$

from the choice of ℓ, which ends the proof.

Remark 1 In the case where $R(X)=1+X\in \mathbb{F}_p[X]$, the slice studied in the above theorem is the sequence $u(n)=\binom{(p+1)n}{pn}=\binom{(p+1)n}{n}$ modulo p, as we can take $\ell=1$. This is precisely the sequence studied for the case $p=2$ in [3], where the non-periodicity was deduced from the observation that the formal power series $\sum_{n\geq 0} u(n)X^n$ is cubic on $\mathbb{F}_2(X)$.

Remark 2 The proof of the slice lemma could be generalized to d-dimensional linear cellular automata with states in $\mathbb{F}_p$.

The following lemma provides a criterion for the automaticity of a double sequence generated by a linear cellular automaton with initial condition in $\mathbb{F}_p$.

Lemma 2 *Let $R(X)$ be a polynomial in $\mathbb{F}_p[X]$ that is not a monomial, and let $A(X)$ be a nonzero polynomial in $\mathbb{F}_p[X]$. Then the double sequence generated by the linear cellular automaton associated to the polynomial $R(X)$, with initial condition $A(X)$, is k-automatic for some $k\geq 2$ if and only if k is a non-trivial power of p.*

Proof

Suppose now we have a polynomial $R(X)$ in $\mathbb{F}_p[X]$ that is not a monomial, and a polynomial $A(X)$ that is not zero. The double sequence $r=(r(n,t))_{n,t\geq 0}$ generated by the cellular automaton $R(X)$ with initial condition $A(X)$ is defined by

$$A(X)R(X)^t = \sum_{n\geq 0} r(n,t)X^n.$$

If the sequence $r = (r(n,t))_{n,t\geq 0}$ is k-automatic for some $k \geq 2$, then the sequence $u = (u(n,t))_{n,t\geq 0}$ defined by

$$R(X)^t = \sum_{n\geq 0} u(n,t)X^n$$

is also k-automatic. Indeed, its general term is the Cauchy product of the k-automatic double sequence r with the double sequence $v = (v(n,t))_{n,t\geq 0}$ defined by $\sum v(n,t)X^nY^t = \frac{1}{A(X)}$. As $\frac{1}{A(X)}$ is a rational function with coefficients in $\mathbb{F}_p$, the sequence $(v(n,0))_{n\geq 0}$ is ultimately periodic. On the other hand, $v(n,t) = 0$ if $t \neq 0$. Hence v is k-automatic. A slight modification of the proof of Theorem 3.1 in [4] shows that the Cauchy product of two k-automatic double sequences is again k-automatic.

Now suppose that $R(X)$ is not a monomial, hence $R(X) = \lambda X^e S(X)$, where $\lambda \neq 0$, $S(X) = 1 + \ldots$, and $S(X) \neq 1$. If the sequence $u = (u(n,t))_{n,t\geq 0}$ is k-automatic for some $k \geq 2$, then the sequence u_1 defined by

$$R(X)^{(p-1)t} = \sum_{n\geq 0} u(n,(p-1)t)X^n = \sum_{n\geq 0} u_1(n,t)X^n$$

is also k-automatic, [18] and [19]. As

$$S(X)^{(p-1)t} = \sum_{n\geq 0} u_1(n,t)X^{n-(p-1)et} = \sum_{n\geq 0} u_1(n+(p-1)et,t)X^n,$$

the double sequence $w = (w(n,t))_{n,t\geq 0}$ generated by the polynomial $S(X)^{p-1}$, with initial condition 1, is k-automatic since $w(n,t) = u_1(n+(p-1)et,t)$. In fact, since the sequence $(u_1(n,t))_{n,t\geq 0}$ is k-automatic, it follows from a generalization of a result in [18] that any sequence $(u_1(\alpha n+\beta t+\gamma, \delta n+\varepsilon t+\zeta))_{n,t\geq 0}$ is also k-automatic.

On the other hand, the sequence w is p-automatic, since any polynomial in $\mathbb{F}_p[X]$ is p-Fermat. We thus obtain that the double sequence $(w(n,t))_{n,t\geq 0}$ is k-automatic as well as p-automatic. By the slice lemma, there exists a non-ultimately periodic slice $(z(n))_{n\geq 0}$, with $z(n) = w(\alpha n, \beta n)$. But this sequence is also both p- and k-automatic. By Cobham's theorem [7], k is a power of p.

4 Not ultimately periodic slices – another approach

Here we will present a method for checking that a unidimensional slice $u = (u(n))_{n\geq 0}$, where $u(n) = r(\alpha n, \beta n)$, and $\alpha, \beta \in \mathbb{N}$, of the double sequence $(r(n,t))_{n,t\geq 0}$ generated by a polynomial $R(X) \in \mathbb{F}_p[X]$, is not ultimately periodic. For this purpose we construct a one-dimensional p-automaton generating the sequence $u = (u(n))_{n\geq 0}$. The two-dimensional sequence $(r(n,t))_{n,t\geq 0}$ is automatic, i.e., there exists a p-automaton that generates this sequence in the sense that

$$r(n,t) = \tau((n_s,t_s)\ldots(n_0,t_0).a)$$

with $n = n_s p^s + \cdots + n_0$, $t = t_s p^s + \cdots + t_0$, $n_j, t_j \in \{0,1,\ldots,p-1\}$, where a is the initial state of the automaton and τ is an output function.

To construct a finite one-dimensional p-automaton that generates the subsequence $u = (r(\alpha n, \beta n))_{n\geq 0}$, we combine the transducers for multiplication in base p by α and β, respectively, and obtain a new transducer, that we call α-β-transducer, which relates each n with $(\alpha n, \beta n)$. For a definition and general properties of transducers, see [10]. Combining the α-β-transducer with the

two-dimensional p-automaton generating $(r(n,t))_{n,t\geq 0}$, since we only need to consider the arrows labelled by $(\alpha n, \beta n)$, we obtain a one-dimensional p-automaton that generates the subsequence $u = (r(\alpha n, \beta n))_{n\geq 0}$.

Example 1 Let $R(X) = 1 + X + X^2 \in \mathbb{F}_3[X]$, and $A(X) = 1$. Figure 1 (left) represents a two-dimensional 3-automaton that generates the double sequence $(r(n,t))_{n,t\geq 0}$ defined by $R^t(X) = \sum_{n\geq 0} r(n,t)X^n$. Consider the unidimensional sequence $u = (r(n,n))_{n\geq 0}$. It is generated by the 3-automaton shown in Figure 1 (right), which is a reduction of the two-dimensional 3-automaton. The sequence $u = (r(n,n))_{n\geq 0}$ has values 1 and 0. Furthermore, if the triadic expansion of n contains the digit 2, then $u(n) = 0$. Therefore, the sequence u is not ultimately periodic.

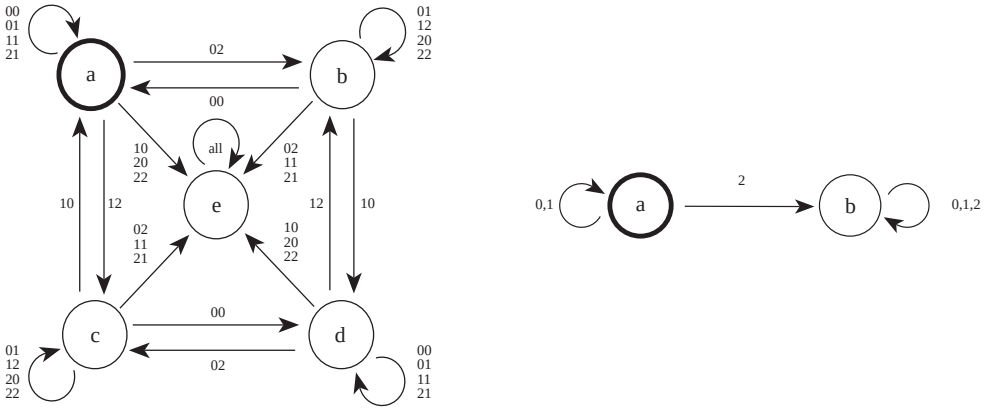

Figure 1: A 3-automaton associated with $1+X+X^2 \in \mathbb{F}_3[X]$ with output function $\tau(a) = \tau(b) = 1,\ \tau(c) = \tau(d) = 2,\ \tau(e) = 0$ (left), and a 3-automaton that generates the slice $u = (r(n,n))_{n\geq 0}$ of the double sequence $(r(n,t))_{n,t\geq 0}$ generated by $1 + X + X^2 \in \mathbb{F}_3[X]$ with output function $\tau(a) = 1$ and $\tau(b) = 0$ (right).

Example 2 Let $R(X) = 1 + X + X^2 \in \mathbb{F}_2[X]$, $A(X) = 1$, and consider the unidimensional slice $u = (r(n,3n))_{n\geq 0}$.

A two-dimensional 2-automaton that generates the double sequence $(r(n,t))_{n,t\geq 0}$ is shown in Figure 2 (left). Combining it with the transducer for binary multiplication by 3 (see Figure 2 (right)), we get a one-dimensional 2-automaton that generates the unidimensional sequence $u = (r(n,3n))_{n\geq 0}$ (see Figure 3). Careful observation yields that there are growing blocks of zeros, starting with the entries for $n = 11$ and $n = 12$, and growing like a power of 2: all entries n with $2^k \cdot 11 \leq n \leq 2^k \cdot 12 + 2^k - 1$ give zero. Again, this means that the unidimensional sequence we consider is not ultimately periodic.

Example 3 Let $R(X) = 1 + X + X^2 \in \mathbb{F}_2[X]$, $A(X) = 1$, and consider the unidimensional subsequence $u = (r(2n,3n))_{n\geq 0}$.

In order to construct a one-dimensional 2-automaton that generates this sequence, we first combine the transducers for binary multiplication by 2 and 3 (Figures 4 (left) and 2 (right)). The next step consists in combining the thus obtained transducer (Figure 4 (right)) with the two-dimensional 2-automaton corresponding to $R(X)$ (Figure 2 (left)). The one-dimensional 2-automaton is shown in Figure 5. By a careful analysis of the automaton we see that $u(n) \neq 0$ for those numbers n whose binary expansion consists of blocks 00101 or 010101 and an arbitrary

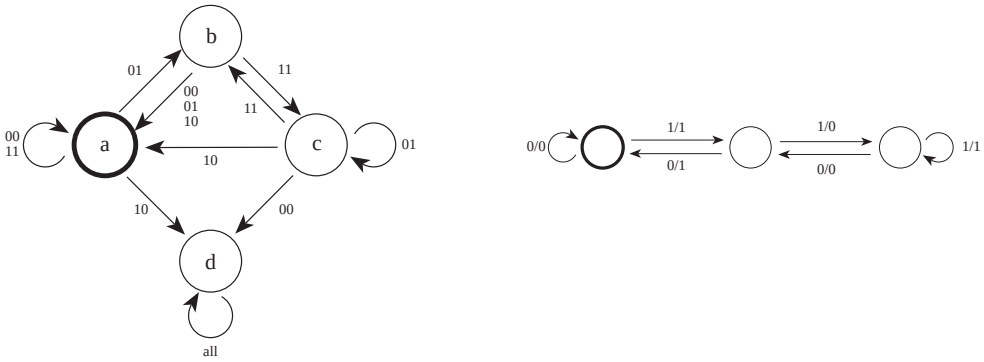

Figure 2: A 2-automaton associated with $1+X+X^2 \in \mathbb{F}_2[X]$ with output function $\tau(a) = \tau(b) = 1,\ \tau(c) = \tau(d) = 0$ (left) and a binary 3-transducer (right).

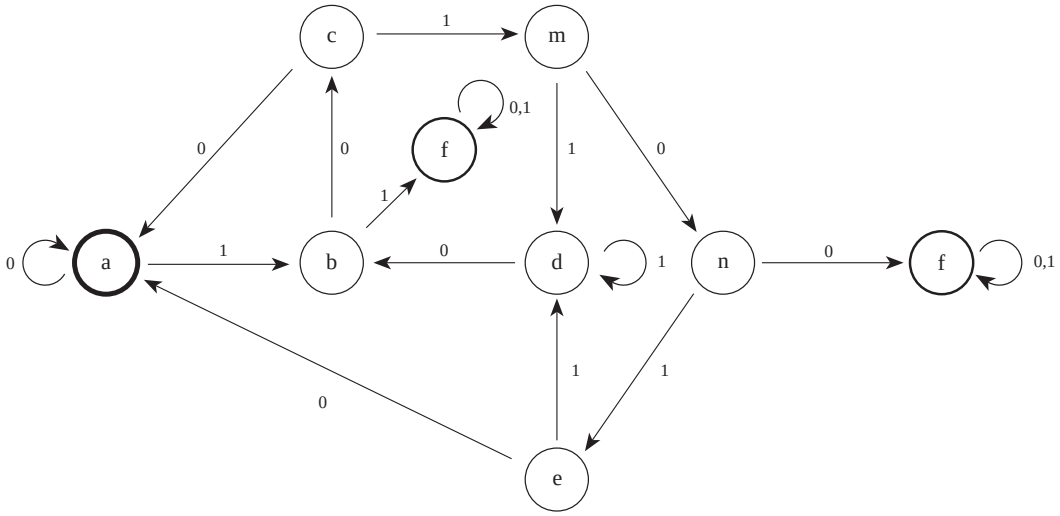

Figure 3: A 2-automaton that generates the subsequence $u = (r(n, 3n))_{n\geq 0}$ of the double sequence generated by $1 + X + X^2 \in \mathbb{F}_2[X]$ with output function $\tau(a) = \tau(b) = \tau(c) = \tau(d) = \tau(e) = 1$ and $\tau(m) = \tau(n) = \tau(o) = 0$.

number of zeros between the blocks. This shows that there are growing blocks of zeros, which implies that the sequence is not ultimately periodic.

Another way of proving that this sequence u is not ultimately periodic is to figure out the algebraic equation for the "generating" function $a(x)$ of u, which is $a(x) = \sum_{n=0}^{\infty} u(n)x^n \in \mathbb{F}_2[[x]]$. The 2-automaton generating the sequence u provides us with a system of equations for the unknown formal power series $a(x), \ldots, g(x)$ corresponding to the states of the 2-automaton.

$$\begin{aligned}
a(x) &= a(x)^2 + xf(x)^2 \\
b(x) &= a(x)^2 + xd(x)^2 \\
c(x) &= b(x)^2 + xg(x)^2 \\
d(x) &= a(x)^2 + xg(x)^2 \\
e(x) &= g(x)^2 + xc(x)^2 \\
f(x) &= e(x)^2 + xg(x)^2 \\
g(x) &= g(x)^2 + xg(x)^2
\end{aligned}$$

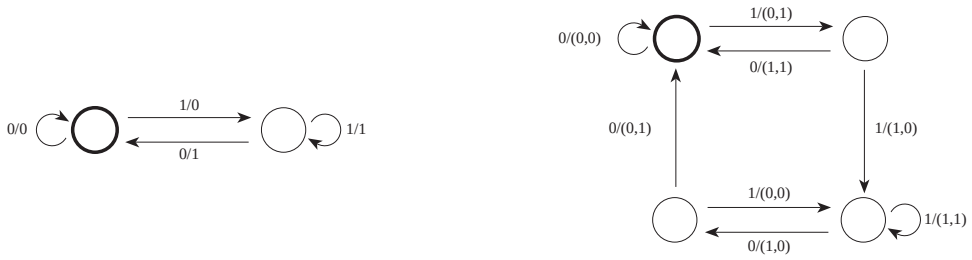

Figure 4: A binary 2-transducer (left) and a binary 2-3-transducer (right).

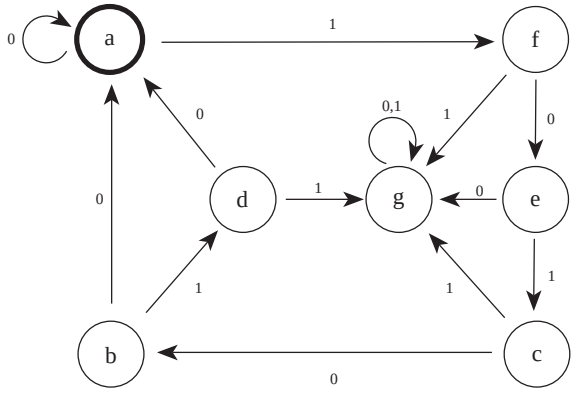

Figure 5: A 2-automaton generating the slice $u = (r(2n, 3n))_{n\geq 0}$ of the double sequence $(r(n,t))_{n,t\geq 0}$ generated by $1 + X + X^2 \in \mathbb{F}_2[X]$ with output function $\tau(a) = \tau(b) = \tau(c) = \tau(d) = 1$ and $\tau(e) = \tau(f) = \tau(g) = 0$.

Since $g(x) = g(x)^2 + xg(x)^2$ we see that g is either $g(x) = 0$ or $g(x) = \frac{1}{1+x}$. Since $\tau(g) = 0$ we obtain $g(x) = 0$. Using this fact we get the following equations

$$\begin{aligned} f(x) &= e(x)^2 \\ e(x) &= xc(x)^2 \\ d(x) &= a(x)^2 \\ c(x) &= b(x)^2 \\ b(x) &= a(x)^2 + xd(x)^2 \\ a(x) &= a(x)^2 + xf(x)^2. \end{aligned}$$

Hence,

$$a(x) = a(x)^2 + x^5 a(x)^{32} + x^{21} a(x)^{64}.$$

It is easy to see that this equation does not have a rational solution for $a(x)$, therefore the sequence u is not ultimately periodic.

5 An automaticity and non-automaticity theorem

In this section, we prove the main theorem. First we recall the definition of the k-Fermat property.

Definition 2 *Let $k \geq 2$ be an integer. A polynomial $P(X)$ with coefficients in the ring $\mathcal{R}$ (com-*

mutative and with unit) is called k-Fermat if

$$P(X^k) = P(X)^k.$$

The next lemma is a consequence of Theorem 78, in [14] p. 65.

Lemma 3 *Let $P(X)$ and $Q(X)$ be two polynomials in $\mathbb{Z}[X]$ and let p be a prime number. If*

$$P(X) \equiv Q(X) \bmod p,$$

then, for all $i \geq 1$,

$$P(X)^{p^i} \equiv Q(X)^{p^i} \bmod p^{i+1}.$$

The following lemma shows that, under certain conditions, a power of a polynomial $P(X) \in \mathbb{Z}[X]$ is k-Fermat in $\mathbb{Z}/p^i\mathbb{Z}$ for all k, where p is any prime number.

Lemma 4 *Let p be a prime number, and let $P(X)$ be a polynomial in $\mathbb{Z}[X]$. If $P(X)$ modulo p is a monomial, then, for all $i \geq 1$, there exists an integer $\alpha_i \geq 1$ such that $P(X)^{\alpha_i}$ modulo p^i is k-Fermat for all $k \geq 1$.*

Proof

We first notice that, if $P(X) = \lambda X^j$ modulo p, with λ different from zero modulo p, then $P(X)^{p-1} = X^{(p-1)j}$ modulo p. Hence, using Lemma 3 above, one has: $P(X)^{(p-1)p^{i-1}} = X^{(p-1)p^{i-1}j}$ modulo p^i. This implies that $P(X)^{(p-1)p^{i-1}}$ modulo p^i is k-Fermat for all $k \geq 1$.

Definition 3 *Let $A(X)$ be a polynomial in $\mathbb{Z}[X]$ and let m be an integer ≥ 2. We say that $A(X)$ is not m-trivial if there does not exist a prime number p that divides m such that $A(X) = 0$ modulo p.*

Theorem 1 *Let $R(X)$ and $A(X)$ be two polynomials in $\mathbb{Z}[X]$, and let m be an integer ≥ 2. Suppose $A(X)$ is not m-trivial, and consider the linear cellular automaton defined on $\mathbb{Z}/m\mathbb{Z}$ by the polynomial $R(X)$ modulo m. Then the following three cases are the only possible ones.*

- *There exist two different prime numbers p and q dividing m, such that the two polynomials $R(X)$ modulo p and $R(X)$ modulo q are not monomials. Then, the double sequence generated by the linear cellular automaton, with initial condition $A(X)$ modulo m, is not k-automatic, for any $k \geq 2$.*
- *There exists one prime number p dividing m for which $R(X)$ modulo p is not a monomial, and for every other prime divisor q of m (if any), the polynomial $R(X)$ modulo q is a monomial. Then, the double sequence generated by the linear cellular automaton, with initial condition $A(X)$ modulo m, is p^a-automatic, for every $a \geq 1$, and this sequence is not k-automatic for any $k \notin \{p^a;\ a \geq 1\}$.*
- *For every prime number p dividing m, the polynomial $R(X)$ modulo p is a monomial. Then, the double sequence generated by the linear cellular automaton, with initial condition $A(X)$ modulo m, is k-automatic for every $k \geq 2$.*

Proof

- It suffices to consider the case $A(X) = 1$. Suppose there exist two different prime numbers p and q dividing m such that the two polynomials $R(X)$ modulo p and $R(X)$ modulo q are not monomials. Let $(r(n,t))_{n,t\geq 0}$ modulo m be the sequence generated by the linear cellular automaton $R(X)$ modulo m with initial condition equal to 1. Then, the two canonical projections, $\pi_p : \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{F}_p$ and $\pi_q : \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{F}_q$, yield respectively the double sequences $(\pi_p(r(n,t)))_{n,t\geq 0}$ and $(\pi_q(r(n,t)))_{n,t\geq 0}$. These sequences are generated respectively by the cellular automata $R(X)$ modulo p and $R(X)$ modulo q with initial condition 1. Furthermore, $(\pi_p(r(n,t)))_{n,t\geq 0}$ is p-automatic and $(\pi_q(r(n,t)))_{n,t\geq 0}$ is q-automatic. By the slice lemma (Lemma 1) there exist non-ultimately periodic slices (one-dimensional subsequences) $(u_p(n))_{n\geq 0}$ with $u_p(n) = \pi_p(r(an, bn)),\ a, b \in \mathbb{N}$ and $(u_q(n))_{n\geq 0}$ with $u_q(n) = \pi_q(r(cn, dn)),\ c, d \in \mathbb{N}$, which are p-automatic and q-automatic, respectively.

  Now suppose that the double sequence $(r(n,t))_{n,t\geq 0}$ modulo m is k-automatic. Then the sequence $(\pi_p(r(n,t)))_{n,t\geq 0}$ is also k-automatic. This implies that the slice sequence $(u_p(n))_{n\geq 0}$ is k-automatic. On the other hand, the sequence $(u_p(n))_{n\geq 0}$ is p-automatic. Since it is not ultimately periodic, it follows, by Cobham's theorem [7], that k is a power of the prime number p. The same reasoning for the slice $(u_q(n))_{n\geq 0}$ implies that k is a power of the prime number q. This is a contradiction, since p and q are different prime numbers.

- Suppose now there exists one prime number p dividing m, such that the polynomial $R(X)$ modulo p is not a monomial, and that for every other prime divisor q of m (if any), the polynomial $R(X)$ modulo q is a monomial. If our double sequence modulo m is k-automatic for some $k \geq 2$, the same reasoning as above shows that k must be a power of p. Now let $m = p^a q_1^{a_1} q_2^{a_2} \cdots q_w^{a_w}$. For every prime number q_i (if any), the polynomial $R(X)$ modulo q_i is a monomial. From Lemma 4 there exists an integer α_i such that the polynomial $R(X)^{\alpha_i}$ modulo $q_i^{a_i}$ is k-Fermat for all $k \geq 1$, hence in particular p-Fermat. On the other hand, we know that there exists an integer α $(= p^{a-1})$ such that $R(X)^{\alpha}$ modulo p^a is p-Fermat (see [3]). From the Chinese Remainder theorem, the polynomial $R(X)^{\alpha\alpha_1\alpha_2\cdots\alpha_w}$ is p-Fermat, and hence the double sequence $(r(n,t))_{n,t\geq 0}$ modulo m is p-automatic (and also p^j-automatic for all $j \geq 1$).

- Finally, we suppose that the polynomial $R(X)$ modulo p is a monomial, for every prime number p dividing m. Let $m = q_1^{a_1} q_2^{a_2} \cdots q_w^{a_w}$. Using Lemma 4 we know that there exists an integer $\alpha_i \geq 1$ such that $R(X)^{\alpha_i}$ modulo $q_i^{a_i}$ is k-Fermat for every $k \geq 1$. Using the Chinese Remainder theorem again we deduce that $R(X)^{\alpha_1\alpha_2\cdots\alpha_w}$ modulo m is also k-Fermat for all $k \geq 1$. Hence from [3] the double sequence $(r(n,t))_{n,t\geq 0}$ modulo m is k-automatic for every $k \geq 2$.

Remark 3 The same assertion as in Theorem 1 follows for $(d+1)$-dimensional sequences generated by d-dimensional linear cellular automata modulo m.

6 Some applications

The following corollaries are immediate consequences of Theorem 1.

Corollary 1 *The double sequence generated by a one-dimensional linear cellular automaton on $\mathbb{Z}/m\mathbb{Z}$, with generating polynomial $R(X)$, and a polynomial initial condition $A(X)$ which is not m-trivial, is k-automatic for some $k \geq 2$ if and only if there exists a nonzero power of the generating polynomial $R(X)$ that is k-Fermat.*

Corollary 2 *If the double sequence generated by a one-dimensional linear cellular automaton on $\mathbb{Z}/m\mathbb{Z}$, with a non-m-trivial polynomial initial condition, is k-automatic for some $k \geq 2$ which is not a prime power, then, it is k-automatic for all $k \geq 2$.*

Example 4 Let $R(X) = 4 + 9X^2$ modulo 12. Then $R(X)$ is k-Fermat for every $k \geq 2$.

Let us now address the case of the (signless) Stirling numbers of the first kind and of the Gaussian q-binomial coefficents. We use again an idea of [17] and [3] and consider sequences generated by "several polynomials".

Definition 4 *Let K be a ring (commutative with unit). Let $R_0(X), \cdots, R_{\alpha-1}(X) \in K[X]$, $\mathcal{R} = (R_0(X), \cdots, R_{\alpha-1}(X))$. The sequence $(u_{\mathcal{R},A}(n,t))_{n,t\geq 0}$ is generated by the polynomials $\mathcal{R}$ with initial polynomial condition $A(X) \in K[X]$ if*

$$(R_0(X)\cdots R_{\alpha-1}(X))^{t_\alpha} R_0(X)\cdots R_{s_\alpha-1}(X)A(X) = \sum_{n\geq 0} u_{\mathcal{R}}(n,t)X^n$$

where $t = \alpha t_\alpha + s_\alpha$, $t_\alpha \in \mathbb{N}$, $0 \leq s_\alpha \leq \alpha - 1$.

Theorem 2 *Let $A(X), R_0(X), \cdots, R_{\alpha-1}(X) \in \mathbb{Z}[X]$, let $\mathcal{R} = (R_0(X), \cdots, R_{\alpha-1}(X))$. Let $m \geq 2$ be an integer, and consider the sequence $(u_{\mathcal{R},A}(n,t))_{n,t\geq 0}$ modulo m. Let $R(X) = R_0(X)R_1(X)\cdots R_{\alpha-1}(X)$. Let $A(X)$ be a non-m-trivial polynomial. Then, the following three cases are the only possible ones.*

- *There exist two different prime numbers p and q dividing m, such that the two polynomials $R(X)$ modulo p and $R(X)$ modulo q are not monomials. Then, the double sequence $(u_{\mathcal{R},A}(n,t))_{n,t\geq 0}$ modulo m, generated by the polynomials $\mathcal{R} = (R_0(X), \cdots, R_{\alpha-1}(X))$ and the initial condition $A(X)$, is not k-automatic, for any $k \geq 2$.*
- *There exists one prime number p dividing m for which $R(X)$ modulo p is not a monomial, and for every other prime divisor q of m (if any), the polynomial $R(X)$ modulo q is a monomial. Then, the double sequence $(u_{\mathcal{R},A}(n,t))_{n,t\geq 0}$ modulo m, generated by the polynomials $\mathcal{R} = (R_0(X), \cdots, R_{\alpha-1}(X))$ and the initial condition $A(X)$, is p^a-automatic, for every $a \geq 1$, and this sequence is not k-automatic for any $k \notin \{p^a;\ a \geq 1\}$.*
- *For every prime number p dividing m, the polynomial $R(X)$ modulo p is a monomial. Then, the double sequence $(u_{\mathcal{R},A}(n,t))_{n,t\geq 0}$ modulo m, generated by the polynomials $\mathcal{R} = (R_0(X), \cdots, R_{\alpha-1}(X))$ and the initial condition $A(X)$, is k-automatic for every $k \geq 2$.*

Proof

This theorem is an easy consequence of Theorem 1, once one has noticed that the sequence $(u_{\mathcal{R},A}(n,t))_{n,t\geq 0}$ modulo m is k-automatic if and only if all the sequences generated by the linear cellular automaton modulo m with generating polynomial $R(X) = R_0(X)R_1(X)\cdots R_{\alpha-1}(X)$ modulo m, and initial conditions $A(X)$ modulo m, $A(X)R_0(X)$ modulo m, $A(X)R_0(X)R_1(X)$ modulo m, $\ldots$, $A(X)R_0(X)\cdots R_{\alpha-2}(X)$ modulo m, are k-automatic. This follows from [3], Corollary 2.

Before applying this theorem to the (signless) Stirling numbers of the first kind and to the Gaussian q-binomials, we recall the following.

The (signless) Stirling numbers of the first kind $S(n,t)$ are defined by

$$\prod_{k=0}^{t-1}(X+k)=\sum_{n=0}^{t}S(n,t)X^n.$$

Note that we interchanged n and t in the classical definition of the signless Stirling numbers, see [20] p. 18.

The Gaussian q-binomial coefficients $G(n,t;q)$, q, n, $t\in\mathbb{N}$, $k\geq 2$, ([20] p. 26) are defined by

$$\prod_{k=1}^{t}(1+q^{k-1}X)=\sum_{n=0}^{t}G(t,n;q)q^{n(n-1)/2}X^n.$$

Corollary 3 *Let $m\geq 2$ be an integer. Suppose that $q\geq 1$ is an integer.*

(1) The sequence $(S(n,t))_{n,t\geq 0}$ modulo m of the (signless) Stirling numbers of the first kind taken modulo m is k-automatic for some $k\geq 2$ if and only if m and k are non-trivial powers of a same prime number.

(2) If q and m are coprime, then the sequence $(G(n,t;q))_{n,t\geq 0}$ modulo m of the Gaussian q-binomial coefficients taken modulo m is k-automatic for some $k\geq 2$ if and only if m and k are non-trivial powers of a same prime number.

Proof

(1) For the (signless) Stirling numbers of the first kind modulo m, the assertion follows from Theorem 2 with $R_i(X)=X+i$, $i=0,\cdots,m-1$, and $A(X)=1$.

(2) In [3] we proved that the sequences $(G(n,t;q))_{n,t\geq 0}$ modulo m and $(q^{n(n-1)/2}G(n,t;q))_{n,t\geq 0}$ modulo m are simultaneously k-automatic or non-k-automatic. The sequence $(q^{n(n-1)/2}G(n,t;q))_{n,t\geq 0}$ modulo m is generated by the polynomials $R_i(X)=1+q^{i-1}X$, $i=1,\cdots,\alpha-1$, where α is the smallest strictly positive integer for which $q^\alpha=1$ modulo m. The assertion follows from Theorem 2 since the polynomial $R(X)=R_0(X)\cdots R_{\alpha-1}(X)$ is not a monomial modulo p for any prime number p.

References

[1] J.-P. Allouche, *Automates finis en théorie des nombres*, Expo. Math. **5** (1987), 239–266.

[2] J.-P. Allouche, E. Cateland, H.-O. Peitgen, J. Shallit, G. Skordev, *Automatic maps on a semiring with digits*, Fractals, **3** (1995), 663–677.

[3] J.-P. Allouche, F. von Haeseler, H.-O. Peitgen, G. Skordev, *Linear cellular automata, finite automata and Pascal's triangle*, Discrete Appl. Math. **66** (1996), 1–22.

[4] J.-P. Allouche, J. Shallit, *The ring of k-regular sequences*, Theoret. Comput. Sci. **98** (1992), 163–187.

[5] V. Bruyère, G. Hansel, C. Michaux, R. Villemaire, *Logic and p-recognizable sets of integers*, Bull. Belg. Math. Soc. **1** (1994), 191–238; 577.

[6] G. Christol, T. Kamae, M. Mendès France, G. Rauzy, *Suites algébriques, automates et substitutions*, Bull. Soc. math. France **108** (1980), 401–419.

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

[8] A. Cobham, *Uniform tag sequences*, Math. Systems Theory **6** (1972) 164–192.

[9] M. Dekking, M. Mendès France, A. J. van der Poorten, *FOLDS!*, Math. Intelligencer **4** (1982), 130–138; 173–181; 190–195.

[10] S. Eilenberg, *Automata, Languages and Machines*, vol. A, (Acad. Press, New York, 1985).

[11] S. Ginsburg, E. Spanier, *Semigroups, Presburger formulas and languages*, Pacific J. Math. **16** (1966), 285–296.

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

[13] F. von Haeseler, H.-O. Peitgen, G. Skordev, *Cellular automata, matrix substitutions and fractals*, Ann. Math. and Art. Intell. **8** (1993), 345–362.

[14] G. Hardy, E. Wright, *Introduction to the theory of numbers*, (Clarendon Press, Oxford, 1979).

[15] G. A. Hedlund, *Endomorphisms and automorphisms of the shift dynamical systems*, Math. Systems Theory **3** (1969), 320–375.

[16] I. Korec, *Pascal triangles modulo n and modular trellises*, Computers and Artificial Intelligence **9** (1990), 105–113.

[17] E. Lange, H.-O. Peitgen, G. Skordev, *Fractal patterns in Gaussian and Stirling number tables*, Ars Combinatoria (to appear).

[18] O. Salon, *Suites automatiques à multi-indices*, Séminaire de Théorie des Nombres de Bordeaux, Exposé 4, (1986-1987), 4-01–4-27; followed by an Appendix by J. Shallit, 4-29A–4-36A.

[19] O. Salon, *Suites automatiques à multi-indices et algébricité*, C. R. Acad. Sci. Paris, Série I **305** (1987), 501–504.

[20] R. Stanley, *Enumerative Combinatorics*, I (Wadsworth & Brooks/Cole, Advanced Books & Software, Monterey, California, 1986).

J.-P. Allouche,
C. N. R. S., L. R. I., Bâtiment 490,
F-91405 Orsay Cedex (France),
allouche@lri.fr

F. von Haeseler, H.-O. Peitgen, G. Skordev,
Center for Complex Systems and Visualization, University of Bremen,
Universitätsallee 29
D-28359 Bremen (Germany),

fritz@mathematik.uni-bremen.de
peitgen@mathematik.uni-bremen.de
skordev@mathematik.uni-bremen.de

A. Petersen,
Institute for Dynamical Systems, University of Bremen
Postfach 330440
D-28334 Bremen (Germany)
antje@mathematik.uni-bremen.de