Linear cellular automata, finite automata and Pascal's triangle

J.-P. Allouche, F. v. Haeseler[1], H.-O. Peitgen, G. Skordev

Abstract We address the question of automaticity of double sequences of states produced by linear cellular automata. A complete solution for binomial coefficients and Lucas' numbers is given and some partial results for the general case are presented.

1 Introduction

A cellular automaton is - roughly speaking - a device acting on values given to the nodes of a lattice, with local transition rules and parallel updating: a more precise definition will be given below. For a one-dimensional cellular automaton, one can draw a two-dimensional lattice consisting of the initial configuration of the lattice and of its successive transforms computed by iteration of the transition rules, thus obtaining global state evolution patterns for this cellular automaton. A cellular automaton is called linear if the values of the nodes are taken in a ring (usually $\mathbb{Z}/d\mathbb{Z}$) and if the transform of the sum of two initial configurations is the sum of the transforms of the individual initial configurations. It has been observed for many cellular automata, for example all $\mathbb{Z}/p\mathbb{Z}$-state linear cellular automata (where p is a prime number), that the global state evolution patterns have a fractal (self-similar) structure: see for instance the papers of Wolfram [42], [43], [44], of Willson [37], of Takahashi [35], see also the paper of Culik II and Dube [11].

A special case of such patterns is given by the Pascal triangle modulo d. Note that analogous fractal sets are obtained for other classical double sequences reduced modulo d, like the Gaussian binomial coefficients, the Stirling numbers (of first and second kind) and the Lucas numbers: one can read the papers of M. Sved [32], [34], [33], and the book of Bondarenko [6].

S. Willson proposed ([37]) a rescaling procedure for investigating the fractal properties of state evolution patterns of linear cellular automata. This procedure yields a compact set which is associated with the evolution pattern of the linear cellular automaton. The fractal properties of this set are encoded properties of the state evolution patterns of the cellular automaton. The problem of describing the self-similarity properties of rescaled evolution

[1]Supported by DFG "Forschungsgruppe Dynamische Systeme"

patterns of linear cellular automata has been studied by Willson [38], [39], [40], [41] and Culik II and Dube [11]. It has been solved in some particular cases by Takahashi [35] and by von Haeseler, Peitgen and Skordev [14]. The general solution has been given by these three authors in [15], [16], [17], (see also [18] for some illustrating examples), using special hierarchical iterated function systems, which come from matrix substitution systems or, equivalently, from finite automata.

The considerations from [16] were applied in a paper of Lange, Peitgen and Skordev [23] for deciphering the self-similar structure of the patterns generated by the Gaussian binomial coefficients and the Stirling numbers. The same problem has been addressed by M. Sved [32], [33]; for the case of the binomial coefficients see the paper of M. Sved [34], the work of Holte [19], [20] and the paper of von Haeseler, Peitgen and Skordev [14]. The finite automata constructed by these three authors in [15], [16] for the deciphering of the self-similarity structure of a given linear cellular automaton also produce the state evolution of a finite initial configuration for the linear cellular automaton provided that the values of the nodes of the lattice belong to $\mathbb{Z}/p\mathbb{Z}$ where p is a prime number. This means that the (double) sequence of states produced by a $\mathbb{Z}/p\mathbb{Z}$-state linear cellular automaton and a finite initial configuration is p-automatic: a precise definition will be given below, let us just say here that this means essentially that the values of node i after j iterations of the transition rules can be computed using only the p-ary digits of the integers i and j in time $O(\log \sup(i,j))$. Note also that a general cellular automaton has a computational power strictly greater than the computational power of a finite automaton as the former is equivalent to a Turing machine. For general results on p-automaticity of double sequences one can read the papers of Salon [28], [29], and for the one-dimensional case the papers of Cobham [9], [10], Christol, Kamae, Mendès France and Rauzy [8] and Allouche [2], [3].

In this paper we shall address the question of automaticity of (double) sequences of states produced by the evolution of finite initial configurations with respect to a linear $\mathbb{Z}/m\mathbb{Z}$-state cellular automaton. *These sequences are m-automatic if m is a power of a prime number. In general they are not automatic. For example, the binomial coefficients* mod m *are not automatic if m is not a prime power.*

2 Preliminaries

2.1 Two dimensional automata and double automatic sequences

Let $m \in \mathbb{N}$, $m \geq 2$. A two dimensional m-automaton $\mathcal{A} = (A, a_0, \varphi, T, \tau)$ consists of five objects:

- *state alphabet*, a finite set A,
- *initial state*, an element $a_0 \in A$,
- *input map*, $\varphi : [m]^2 \times A \to A$, where $[m] = \{0, 1, \ldots, m-1\}$,
- *output alphabet*, a finite set T,
- *output map*, $\tau : A \to T$.

See [2], [3], [29], [28] or, for the equivalent notion of matrix (two dimensional) substitutions, [30], [16], [17], [18]. See also [5], [4]. The general notions are defined in [12].

Instead of the input map $\varphi : [m]^2 \times A \to A$ we shall consider the maps $(i, j) : A \to A$, $i, j \in [m]$, defined by $(i, j).a = \varphi((i, j), a)$ for $a \in A$.
For $(n, t) \in \mathbb{N}^2$ we define the maps $(n, t) : A \to A$ recursively. Write $n = n'm + n_0, t = t'm + t_0$ with $n_0, t_0 \in [m]$, then $(n, t) : A \to A$ is defined as

$$(n, t).a = (n_0, t_0).(n', t').a = \varphi((n_0, t_0), (n', t').a).$$

If the initial state a_0 is a fixed point of the map $(0, 0) : A \to A$ then the (two dimensional) m-automaton $\mathcal{A}$ produces a double sequence

$$(u(n, t))_{n,t\geq 0} = (\tau((n, t).a_0))_{n,t\geq 0}$$

in the output set T. The sequence $(u(n, t))_{n,t\geq 0}$ is called automatic (or m-automatic), [28], [29].

2.2 Linear cellular automata

Let R be a finite commutative ring with unit $1 \neq 0$. Usually we deal with the ring $\mathbb{Z}/m\mathbb{Z}$, i.e. the residues of the integers modulo m where m is a natural number greater then 1. With $R((X))$ we denote the set of all formal Laurent series with coefficients in R. An element of $R((X))$ is denoted by

$$r(X) = \sum_{i=n_0}^{\infty} r_i X^i$$

where $r_i \in R$. A Laurent polynomial is a Laurent series r such that there exist integers $d_1, d_2 \geq 0$, with $d = d_1 + d_2$ and $r_i = 0$ for all $i \geq d_1 + 1$ or $i \leq -d_2 - 1$ and $r_{d_1} \neq 0 \neq r_{-d_2}$. We say that d is the degree of this Laurent polynomial.

A Laurent polynomial $r(X)$ of degree d induces a linear cellular automaton (for a more general definition see [42]), denoted by A_r, which is defined as

$$\begin{aligned} A_r : R((X)) &\to R((X)) \\ g(X) &\mapsto r(X)g(X), \end{aligned}$$

i.e. multiplication with $r(X)$. The orbit of the Laurent series g w.r.t. the linear cellular automaton A_r is the set

$$O(g) = \{A^t(g) \,:\, t = 0, 1, 2, \ldots\} = \{r(X)^t g(X) \,:\, t = 0, 1, 2, \ldots\}.$$

The Laurent series $g(X) = \sum g_i X^i$ is represented on the one-dimensional lattice $\mathbb{Z}$. The point $i \in \mathbb{Z}$ indicates the location of a cell and $g(X)$ specifies the state g_i of the lattice point or cell i.

The orbit $O(g)$ of the Laurent series g w.r.t. the cellular automaton A_r is represented in the two dimensional lattice $\mathbb{Z}^2$ of the plane $\mathbb{R}^2$. The points $(i, t) \in \mathbb{Z}^2$ are referred to as cells. Then

$$A^t g(x) = r(x)^t g(x) = \sum_{i=-\infty}^{\infty} g(i, t) x^i$$

specifies the state of the cell at position i at time t. We shall consider the orbit representation as a formal Laurent series with coefficients in R, i.e.

$$O(g)(X, Y) = \sum_{i,t \in \mathbb{Z}} g(i, t) X^i Y^t.$$

We call $O(g)(X, Y)$ the state evolution of g w.r.t. r. For the sake of simplicity, we shall speak of the cellular automaton $r(x)$ instead of the cellular automaton induced by the polynomial r.

3 Main results

We start with a formulation of the problem. Consider two polynomials $g(X)$, $r(X) \in \mathbb{Z}[X]$. Let $m \in \mathbb{N}$, $m \geq 2$ and define the double sequence

$$g_m(n, t) = g(n, t) \bmod m, \tag{1}$$

where

$$g(X)r(X)^t = \sum_n g(n,t)X^n. \tag{2}$$

Question - Is the sequence $(g_m(n,t))_{n,t\geq 0}$ automatic? In particular, is the sequence of the binomial coefficients modulo m an automatic sequence?

Remarks
1. If $r(X) = 1 + X$ and $g(X) = 1$ the corresponding sequence (1) is the (double) sequence of the binomial coefficients $(\binom{t}{n})_{n,t}$ mod m.
2. For $r(X) = 1 + X$ and $g(X) = 1 + 2X$ we obtain the Lucas numbers modulo m, ([6] p. 22).

If $m = p$ is a prime number then there is an affirmative answer which follows for instance from a theorem of Salon, [28], [29] Theorem 5.1, (a generalization of the corresponding theorem of Christol, Kamae, Mendès France and Rauzy, [8]). The key idea is to consider the power series

$$F(X,Y) = \sum_{n,t\geq 0} g_p(n,t)X^nY^t$$

with coefficients in $\mathbb{Z}/p\mathbb{Z}$. The definition of $g_p(n,t)$ yields

$$F(X,Y) = \sum_{t\geq 0} g(X)r(X)^tY^t = \frac{g(X)}{1 - r(X)Y} \mod p.$$

Therefore $F(X,Y)$ is a rational function over the field $\mathbb{Z}/p\mathbb{Z}$. In particular, $F(X,Y)$ is algebraic over the field of rational functions $\mathbb{Z}/p\mathbb{Z}(X,Y)$ which yields the automaticity of the sequence $(g_p(n,t))_{n,t}$.
For composite numbers m we have to apply different arguments. We shall prove the following assertions.

Theorem 1 *Let $m \geq 2$ be a natural number. Then:*

- *the (double) sequence of binomial coefficients modulo m is automatic if and only if $m = p^l$, for some prime number p,*
- *the (double) sequence of Lucas' numbers modulo m is automatic if and only if $m = p^l$, for some prime number p,*

If $m = p^l$ for some prime number p, both sequences are p-automatic (or p^l-automatic which is equivalent).

The "if" conditions are consequences of the more general

Theorem 2 *Let $g(X)$, $r(X) \in \mathbb{Z}[X]$ and let p be a prime number. The sequence $(g_{p^l}(n,t))_{n,t\geq 0}$ (defined by (1)) is p-automatic for every natural number l.*

Remark
The assertion of Theorem 2 still holds for polynomials $g(X_1,\ldots,X_k)$, $r(X_1,\ldots,X_k)$ in $\mathbb{Z}[X_1,\ldots,X_k]$. This implies that the (n-dimensional) multinomial coefficients mod p^l are (n-dimensional) p-automatic sequences. In the next section we shall define a class of polynomials over a finite commutative ring with a 1 for which Theorem 2 holds.

4 Polynomials with the m-Fermat property

In what follows we consider a commutative ring R (with a 1).

Definition
Let $r(X) \in \mathrm{R}[X]$, $m \in \mathbb{N}, m \geq 2$. The polynomial $r(X)$ has the m-Fermat property if

$$r(X)^m = r(X^m).$$

Remark
In [27] the polynomials in $\mathbb{Z}/m\mathbb{Z}[X]$ having this property are called self-similar polynomials with scaling exponent m.

In this section we shall present some examples of polynomials with the m-Fermat property.

Lemma 1 *Let $k \in \mathbb{N}\backslash\{0\}$, p be a prime number and $r_i \in \mathrm{R}$, for $i = 0,\ldots,d$. If $p\mathrm{R} = 0$ and $r_i^{p^k} = r_i$, $i = 0,\ldots,d$, then the polynomial*

$$r(X) = r_0 + r_1 X + \cdots + r_d X^d \in \mathrm{R}[X]$$

has the p^k-Fermat property

Proof.

Induction with respect to d.
Let $d = 1$. Using the assumption, the property $\binom{p^k}{i} \equiv 0 \bmod p$ for

$1 \leq i \leq p^k - 1$ (Lucas' lemma, [25], [31] p. 53), and the binomial formula we obtain the assertion.
The induction step follows from the same arguments.

Examples
1. All polynomials with coefficients in the Galois field $GF(p^k)$ (see [7]) have the p^k-Fermat property.
2. Let p, q be two different prime numbers. Then the polynomial $r(X) = 1 + pX$ in $\mathbb{Z}/pq\mathbb{Z}[X]$ has the q-Fermat property. The polynomial $ps(X)$ has the q-Fermat property for every polynomial $s(X) \in \mathbb{Z}/pq\mathbb{Z}[X]$.

Lemma 2 *Let $k \in \mathbb{N}$, let p be a prime number, let R be a commutative ring and let*

$$r(X) = r_0 + r_1 X + \cdots + r_d X^d \in \mathrm{R}[X]$$

be a polynomial. If $p^k \mathrm{R} = 0$ and $r_i^p \equiv r_i \bmod p\mathrm{R}$, $i = 0, \ldots, d$, then the polynomial $q(X) = r(X)^{p^{k-1}}$ has the p-Fermat property.

Proof.

Let $a \in \mathbb{N}$, and let p be a prime number. We shall denote by $v_p(a)$ the largest power k, such that p^k divides a. It follows from Kummer's lemma ([22] p. $115 - 116$) that

$$v_p(\binom{n}{t}) \geq v_p(n) - v_p(t), \quad \text{and} \quad r_i^{p^k} = r_i^{p^{k-1}}. \tag{3}$$

Now, we proceed by induction with respect to the degree d of the polynomial $r(X)$.
Let $d = 1$, and $r(X) = r_0 + r_1 X$.
Then

$$q(X)^p = ((r_0 + r_1 X)^p)^{p^{k-1}} = (r_0^p + r_1^p X^p + p\tilde{r}(X))^{p^{k-1}}.$$

Applying the binomial formula one deduces from (3) that

$$q(X)^p = q(X^p).$$

The induction step follows from the same arguments.

Example ([27], [41]) Let p be a prime number and $r(X) \in \mathbb{Z}/p^k\mathbb{Z}[X]$. Then the polynomial $r(X)^{p^{k-1}}$ has the p-Fermat property.

5 Two dimensional m-automaton corresponding to a given polynomial

Let R be a finite commutative ring with 1, $r(X) \in \mathrm{R}[X]$ be a polynomial, k, $m \in \mathbb{N}$, $m \geq 2$.
Here we shall define a two dimensional m-automaton $\mathcal{A}_k(r)$, corresponding to the polynomial $r(X)$. The m-automaton $\mathcal{A}_k(r)$ has

- state alphabet $A = \mathrm{R}^k$,
- initial state $e_0 = (0, \ldots, 0, 1)$,
- output alphabet $T = \mathrm{R}$.

The output map $\tau_1 : \mathrm{R}^k \to \mathrm{R}$ is defined by

$$\tau_1(\alpha_{-k+1}, \ldots, \alpha_0) = \alpha_0$$

for $(\alpha_{-k+1}, \ldots, \alpha_0) \in \mathrm{R}^k$.
For the definition of the input maps

$$(i, j) : \mathrm{R}^k \to \mathrm{R}^k, \quad i, j \in [m],$$

we need some notations.
The map

$$b_k : \mathrm{R}((X^{-1})) \to \mathrm{R}^k$$

defined by

$$b_k(l(X)) = (l_{-k+1}, \ldots, l_0), \quad \text{where} \quad l(X) \in \mathrm{R}((X^{-1})),$$

and

$$l(X) = \sum_{n=-\infty}^{+\infty} l_n X^n$$

is called a k-block map. The map b_k is a R-module homomorphism.
By e_i, $i = 0, \ldots, k-1$, we shall denote the i-th basis vector of the free R-module R^k defined by:

$$e_i = b_k(x^{-i}).$$

The input map $(i, j) : \mathrm{R}^k \to \mathrm{R}^k$ shall be a R-module homomorphism. Since R^k is a free R-module with generators $\{e_0, \ldots, e_{k-1}\}$ we need to define the map (i, j) only on the elements e_l, $l = 0, \ldots, k-1$:

$$(i, j).e_l = b_k(X^{-lm-i} r(X)^j),$$

for $i, j \in \{0, 1, \ldots, m-1\}$, $0 \leq l \leq k-1$.
Observe that e_0 is a fixed point of the map $(0,0)$.
We shall use the m-automaton $\mathcal{A}_k(r)$ to produce the sequence $(g(n,t))_{n,t}$ defined by (2) for $g(X) = 1$, and a given polynomial $r(X) \in \mathrm{R}[X]$. In the next section we shall consider the case of a polynomial $r(X)$ which has the m-Fermat property for an integer $m \geq 2$.

6 m-automaticity of a double sequence produced by a polynomial with the m-Fermat property

Let R be a finite commutative ring (with a 1) and $r(X) \in \mathrm{R}[X]$. The polynomial $r(X)$ produces a double sequence $(r(n,t))_{n,t\geq 0}$ of elements in R defined by

$$r(X)^t = \sum r(n,t)X^n.$$

Theorem 3 *If $r(X)$ has the m-Fermat property then the double sequence $(r(n,t))_{n,t\geq 0}$ is m-automatic and for $k \geq \deg r(X)$ the m-automaton $\mathcal{A}_k(r)$ produces it.*

Proof.

The assertion of the theorem follows from

$$(n,t).e_0 = b_k(X^{-n}r(X)^t) \tag{4}$$

since

$$\tau_1(b_k(X^{-n}r(X)^t) = r(n,t),$$

for $n, t \in \mathbb{N}$. Let

$$n = n_0 + n_1 m + \cdots + n_s m^s, \quad t = t_0 + t_1 m + \cdots + t_s m^s$$
$$n_q, t_q \in [m],\ q = 0, \ldots, s.$$

Assume that at least one of the digits n_s, t_s is different from zero.
We shall prove (4) by induction with respect to s.
Step 1: $s = 0$.
In this case (4) coincides with the definition of the input maps (i, j).
Step 2:
Assume that (4) is proved for all numbers of the set $\{0, \ldots, m^{s-1} - 1\}$ and

that n, t are given by their m-expansions above. Then

$$\begin{aligned}
(n,t).e_0 &= (n_0+n'm, t_0+t'm).e_0 = (n_0,t_0).(n',t').e_0 \\
&= (n_0,t_0).b_k(X^{-n'}r(X)^{t'}), \\
&\quad \text{by the induction hypothesis,} \\
&= \sum_{u=0}^{k-1} r(n'-u,t')(n_0,t_0).e_u \\
&= \sum_{u=0}^{k-1} r(n'-u,t')b_k(X^{-um-n_0}r(X)^{t_0}) \\
&= \sum_{u=0}^{k-1} r(n'm-um,t'm)b_k(X^{-um-n_0}r(X)^{t_0}) \\
&\quad \text{from the } m\text{-Fermat property,} \\
&= \left(\sum_{u=0}^{k-1} r(n'm-um,t'm)r(um+n_0-k+1,t_0),\cdots,\right. \\
&\qquad \left.\sum_{u=0}^{k-1} r(n'm-um,t'm)r(um+n_0,t_0)\right) \\
&= (r(n-k+1,t),\cdots,r(n,t)), \\
&\quad \text{as } k \geq \deg r(X).
\end{aligned}$$

Remark
Theorem 3 is proved in a more general setting for n-dimensional strong Fermat cellular automata in [17]. The proof presented here is simpler. Another proof based upon the notion of *m-kernel*, (see [29]), will be presented in the next section.

Theorem 3 implies

Corollary 1 *Let $r(X)$, $g(X) \in \mathrm{R}[X]$ where* R *is a finite commutative ring and $r(X)$ has the m-Fermat property. Then the sequence $(g(n,t))_{n,t\geq 0}$ defined by* (2) *is m-automatic.*

Proof.
Let $k = \max(\deg r(X),\ 1+\deg g(X))$. We consider the m-automaton $\mathcal{A}_k(r)$ with a new output map $\tau_g : \mathrm{R}^k \to \mathrm{R}$ defined by

$$\tau_g(\alpha_{-k+1},\ldots,\alpha_0) = \sum_{i=0}^{k-1} \alpha_{-i} g(i,0).$$

Then the double sequence $(g(n,t))_{n,t\geq 0}$ is produced by the m-automaton $\mathcal{A}_k(r)$ with output map τ_g. Indeed, from (4) follows

$$\tau_g((n,t).e_0) = \tau_g(b_k(X^{-n}r(X)^t)) = \sum_{i=0}^{k-1} r(n-i,t)g(i,0) = g(n,t).$$

As a next step we consider double sequences generated by a polynomial $r(X) \in \mathrm{R}[X]$ which satisfies $r(X)^{km} = r(X^m)^k$, i.e. $r(X)^k$ has the m-Fermat property. In order to prove the automaticity of the sequence $(g(n,t))_{n,t}$ we need a "shuffling" property of automatic sequences.

Proposition 1 *Let $(u(n,t))_{n,t\geq 0}$ be a sequence with values in a finite set such that there exist two integers $a \geq 1$ and $b \geq 1$ for which all the sequences $((u(an+c,bt+d))_{n,t\geq 0}$ with $c \in [0,a-1]$, $d \in [0,b-1]$ are m-automatic for some integer $m \geq 2$. Then the sequence $(u(n,t))_{n,t\geq 0}$ itself is m-automatic.*

Proof.

Our proof will mimic the proof of the analogous claim for the one-dimensional case. First note that it suffices to prove the following assertions.

(A1) If $(w(an+c,t))_{n,t}$ is m-automatic for every $c \in [0,a-1]$ then $(w(n,t))_{n,t}$ is m-automatic.

(A2) If $(w(n,bt+d))_{n,t}$ is m-automatic for every $d \in [0,b-1]$ then $(w(n,t))_{n,t}$ is m-automatic.

Assume that (A1) and (A2) are proved and $(u(n,t))_{n,t}$ has the property of the proposition. Then for every fixed $d \in [0,b-1]$ the sequence $(u(an+c,bt+d))_{n,t}$ is m-automatic for any $c \in [0,a-1]$. By (A1), the sequence $(u(n,bt+d))_{n,t}$ is m-automatic for all $d \in [0,b-1]$. Now, (A2) implies that $(u(n,t))_{n,t}$ is m-automatic.

We conclude the proof by showing the validity of (A1) and (A2): to prove (A1), (same proof for (A2)), suppose that for some integer $m \geq 2$, for some integer $a \geq 2$, and for every $c \in [0,a-1]$ the sequence $(u(an+c,t))_{n,t}$ is m-automatic. To prove that the sequence u itself is m-automatic, one has to prove that the m-kernel of u, i.e. the set of subsequences

$$\{(u(m^\alpha n+\beta, m^\alpha t+\gamma))_{n,t} :\ \alpha \geq 0,\ 0 \leq \beta,\gamma \leq m^\alpha - 1\},$$

is finite, see [29], [10], [8]. Therefore it suffices to prove that there are only finitely many sequences of the type:

$$(u(m^\alpha(an+c)+\beta, m^\alpha t+\gamma))_{n,t},\ c \in [0,a-1],\ \alpha \geq 0,\ 0 \leq \beta,\gamma \leq m^\alpha - 1.$$

Now write $m^\alpha c + \beta = ax + y$, with $0 \leq y \leq a-1$.
One has: $ax \leq ax + y = m^\alpha c + \beta < m^\alpha(c+1) \leq am^\alpha$. Hence $x < m^\alpha$, i.e. $x \leq m^\alpha - 1$.
Then: $(u(m^\alpha(an+c)+\beta, m^\alpha t + \gamma)) = u(am^\alpha(n+x)+y, m^\alpha t + \gamma)$. The numbers x and y do not depend on (n,t), but only on α, β and c. Moreover, $y \leq a-1$ and $x \leq m^\alpha - 1$.
Hence the sequence $(u(a(m^\alpha n + x) + y, m^\alpha t + \gamma))_{n,t}$ is in the m-kernel of the sequence $(u(an+y,t))_{n,t}$ which ensures it can take only finitely many values. Indeed, there are finitely many sequences $(u(an+y,t))_{n,t}$, $(0 \leq y \leq a-1)$, each of which is m-automatic, ([29]).

Corollary 2 *Let g and r be two polynomials in $\mathrm{R}[X]$ such that there exists an integer $k \geq 2$ for which the polynomial $r(X)^k$ has the m-Fermat property. Then the double sequence $(g(n,t))_{n,t\geq 0}$ (defined by (2)) is m-automatic.*

Proof.

From Corollary 1, the sequences $u_s(n,t)_{n,t}$, $s = 0, \ldots, k-1$ defined by

$$r(X)^{kt+s} g(X) = \sum_n u_s(n,t) X^n$$

are m-automatic. Then the assertion follows from Proposition 1 applied to the sequence $(g(n,t))_{n,t}$ (defined by (2)) and $a = 1$, $b = k$.

Corollary 3 *Let $r(X) \in \mathrm{GF}(p^l)[X]$, $a, b, c, d \in \mathbb{N}$. Then the power series*

$$\sum_{n.t} r(an+b, ct+d) X^n Y^t$$

is algebraic over the field of rational functions $\mathrm{GF}(p^l)(X,Y)$.

Proof.

From Corollary 1 we know that the double sequence $(r(n,t))_{n,t}$ induced by the polynomial $r(X)$ with the initial polynomial $g(X) = 1$ (see (2)) is p-automatic since the polynomial $r(X)$ has the p^l-Fermat property. From [29], Proposition 7.6 follows that the sequence $(r(an+b, cd+d))_{n,t}$ is p-automatic. Then the assertion follows from [29], Theorem 5.1.

Remark
The case $a = 0$, $c = 1$, $d = 0$ has been proved in [24] with a theorem of Furstenberg, [13].

7 Another proof of the m-automaticity of a sequence produced by a polynomial with the m-Fermat property

We now give another proof of Theorem 3, which actually also proves directly Corollary 1. This proof is based upon the notion of *m-kernel* of a sequence, [29].

The m-kernel of a sequence $(r(n,t))_{n,t}$ is by definition the set of subsequences

$$\{(r(m^\alpha n+u, m^\alpha t+v)_{n,t},\ \alpha\geq 0,\ 0\leq u,\ v\leq m^\alpha-1\}\,.$$

The sequence $(r(n,t))$ is m-automatic if and only if its m-kernel is finite, (see [28], [29]). Clearly, this is equivalent to the existence of a set of sequences $\mathcal{S}$ such that:

- the set $\mathcal{S}$ is finite,
- the sequence r belongs to $\mathcal{S}$,
- the set $\mathcal{S}$ is invariant under the maps $\varphi_{u,v}$ defined for $0\leq u,\ v\leq m-1$ and any sequence a by:

$$\varphi_{u,v}\left((a(n,t))_{n,t}\right)=\left((a(mn+u,mt+v))_{n,t}\right).$$

Now, if h is a polynomial in $\mathrm{R}(X)$, say $h(X)=\sum b(n)X^n$, define $\Phi_u(h)$, for $0\leq u\leq m-1$, to be the polynomial $\Phi_u(h)(X)=\sum b(mn+u)X^n$. Note that $\deg\Phi_u(h)\leq\frac{\deg h}{m}$, and that for two polynomials A and B one has $\Phi_u(A(X)B(X^m))=B(X)\Phi_u(A(X))$, [8].
Let g and r be two polynomials in $\mathrm{R}(X)$ and define the sequence $(g(n,t))_{n,t}$ by (2).
Let $M=\deg g+(m-1)\deg r$, and let $\mathcal{S}$ be the set:

$$\mathcal{S}=\left\{(a(n,t))_{n,t};\ \exists h,\ \deg h\leq M;\ h(X)r(X)^t=\sum a(n,t)X^n\right\}.$$

As h belongs to a finite set of polynomials (R is finite), the set $\mathcal{S}$ is finite. This set contains the sequence r, (take $h=g$). Let us show that $\mathcal{S}$ is stable under the maps $\varphi_{u,v}$.
Let a be a sequence in $\mathcal{S}$ and h be such that $h(X)r(X)^t=\sum_n a(n,t)X^n$, $\forall t$. Then for all $v\leq m-1$ and for all integers t we have that

$$h(X)r(X)^{mt+v}=\sum_n a(n,mt+v)X^n=\sum_{u=0}^{m-1}X^u\sum_n a(mn+u,mt+v)X^{mn}.$$

On the other hand, $h(X)r(X)^{mt+v} = (h(X)r(X)^v)(r(X^m))^t$. Hence

$$\Phi_u(hr^v)r^t = \sum_n a(mn+u, mt+v)X^n.$$

As $\deg \Phi_u(hr^v) \leq \frac{M+(m-1)\deg r}{m} \leq M$, $(m \geq 2)$ one deduces that the sequence $(a(mn+u, mt+v))_{n,t}$ belongs to $\mathcal{S}$.

8 Proofs of Theorem 1 and of Theorem 2

Theorem 2 follows from Lemma 2 and Corollary 2. Theorem 2 implies the assertions on automaticity in Theorem 1.

Proof of the non-automaticity assertion in Theorem 1.

We begin with the binomial coefficients. Curiously enough the proof we have found breaks into two cases:

- The integer m admits two different odd prime divisors.

  We first note the formula (valid on the rational numbers, see for example [31] p. 52):

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

  Hence, defining the formal power series $F(X) = \sum_{t\geq 0} \binom{2t}{t} X^t$, one has:

  $$(1-4X)F(X)^2 - 1 = 0.$$

  As this relation holds in $\mathbb{Z}[[X]]$ it also holds in $\mathbb{Z}/p\mathbb{Z}[[X]]$

  for every prime number p. This proves that the series F is algebraic over the field of rational functions $\mathbb{Z}/p\mathbb{Z}(X)$. Moreover, if $p \neq 2$ this series is not rational. If one had $F = \frac{P}{Q}$ for two polynomials P and Q in $\mathbb{Z}/p\mathbb{Z}[X]$, P and Q coprime, then $(1-4X)P^2 = Q^2$, hence Q^2 would divide $(1-4X)$. This would imply that Q is a constant polynomial, and give the desired contradiction, (note that a different proof of the non-periodicity has just been given in [36]).
  Hence, from the theorem of Christol, Kamae, Mendès France and Rauzy ([8]) the sequence $(\binom{2t}{t})_t$ mod p is p-automatic and not ultimately periodic if p is an odd prime number.

Now suppose that the sequence $(\binom{t}{n})_{n,t\geq 0}$ mod m is k-automatic for some integer $k \geq 2$, and let p_1 and p_2 be two different odd prime numbers divisors of m. Therefore the one-dimensional sequence $(\binom{2t}{t})_t$ mod m is k-automatic (see for instance [29]). By "projection", (i.e. using the canonical map from $\mathbb{Z}/m\mathbb{Z}$ to $\mathbb{Z}/p_1\mathbb{Z}$), the sequence $(\binom{2t}{t})_t$ mod p_1 is k-automatic. From what precedes we know that this sequence is p_1-automatic and not ultimately periodic. Hence from Cobham's theorem ([9]), k is necessarily a power of p_1.

In the same way k must be a power of p_2, which is a contradiction.

- The integer m is equal to $2^a p^b$, where p is a prime odd number and $a, b \geq 0$.

  Here we shall study the coefficients $\binom{3t}{t}$ mod 2. The previous method does not work as the sequence $(\binom{2t}{t})_t$ mod 2 is ultimately periodic.

  Remember that Lucas' theorem asserts that if n and t have a binary expansions given by: $n = \sum_{q\geq 0} e_q(n)2^q$ and $t = \sum_{q\geq 0} e_q(t)2^q$, respectively, then:

$$\binom{t}{n} \equiv \prod_{q\geq 0} \binom{e_q(t)}{e_q(n)} \bmod 2.$$

  Using this theorem and defining the sequence u by

$$u(t) = \binom{3t}{t} \bmod 2,$$

  the reader can check that the following relations hold:

$$\forall t,\ u(2t) = u(t),\ u(4t+1) = u(t),\ u(4t+3) = 0.$$

  Hence the sequence is 2-automatic as its 2-kernel is equal to

$$\{(u(t))_t,\ (u(2t+1))_t,\ 0\}.$$

  Moreover, defining the formal power series G in $\mathbb{Z}/2\mathbb{Z}[[X]]$ by

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

  the previous relations imply that

$$XG^3 + G + 1 = 0.$$

This proves that the formal power series G is algebraic over the field of rational functions $\mathbb{Z}/2\mathbb{Z}(X)$ which is not a surprise ([8]). We can use this relation to prove that G is not a rational function (i.e. the sequence u is not ultimately periodic). If one has $G = \frac{P}{Q}$ for two polynomials in $\mathbb{Z}/2\mathbb{Z}[X]$, P and Q coprime then

$$XP^3 + PQ^2 + Q^3 = 0.$$

Hence Q divides X. If Q is constant we obtain

$$XP^3 + P + 1 = 0$$

which is not possible (compute the degrees). If $Q = X$ we get

$$XP^3 + X^2P + X^3 = 0,$$

hence

$$P^3 + XP + X^2 = 0.$$

That would imply that X divides P which is not possible as P and Q are coprime.

Now suppose that the sequence $(\binom{t}{n})_{n,t\geq 0}$ mod m is k-automatic for some integer $k \geq 2$, and remember that $m = 2^a p^b$. By the same reasoning as in the first case, k must be a power of p. On the other hand, the hypothesis implies that the one-dimensional sequence $(\binom{3t}{t})_t$ mod m is k-automatic, ([29]). Hence, by projection, the sequence $(\binom{3t}{t})_t$ mod 2 is k-automatic. As it is 2-automatic and not ultimately periodic, Cobham's theorem again implies that k must be a power of 2 which is impossible.

Now let us consider the Lucas numbers. They are defined by:

$$(1 + 2X)(1 + X)^t = \sum_n L(n, t)X^n.$$

Hence:

$$L(n, t) = \binom{t}{n} + 2\binom{t}{n-1} = \frac{t!(t + n + 1)}{n!(t - n + 1)!},$$

which implies easily:

$$(n + 1)L(n + 1, t) - (t - n + 1)L(n, t) = \binom{t}{n}.$$

Hence if $(L(n,t))_{n,t} \bmod m$ is automatic, then $(\binom{t}{n})_{n,t} \bmod m$ is automatic, too. Therefore $m = p^l$ for some prime number p.

Remarks
1. The sequence $(r(n,t))_{n,t}$ generated by the polynomial $r(X) \in GF(p^k)[X]$ is p^k-automatic (or equivalently p-automatic) as r has the p^k-Fermat property.
2. The sequence $(r(n,t))_{n,t}$ generated by the polynomial $r(X) = 1 + pX \in \mathbb{Z}/pq\mathbb{Z}[X]$ is q-automatic (for p and q two prime numbers) since the polynomial $r(X)$ has the q-Fermat property.

9 m-automaticity of sequences generated by several polynomials

In this section we consider sequences which are slightly more general than the sequences studied above:

Definition *Let* $r_0(X), \ldots, r_{\alpha-1}(X) \in \mathrm{R}[X], \mathcal{R} = \{r_0(X), \ldots, r_{\alpha-1}(X)\}$. *The sequence* $(u_{\mathcal{R},g}(n,t))_{n,t}$ *is generated by the polynomials* $\mathcal{R}$ *with initial polynomial* $g(X) \in \mathrm{R}[X]$ *if*

$$(r_0(X) \ldots r_{\alpha-1}(X))^{t_\alpha} r_0(X) \ldots r_{s_\alpha-1}(X) g(X) = \sum_n u_{\mathcal{R}}(n,t) X^n$$

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

Examples
1. The Gaussian binomial coefficients $G(n,t;q)$, q, n, $t \in \mathbb{N}$, $k \ge 2$, ([6] p. 14, [26], [31] p. 26) are defined by

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

Let $m \in \mathbb{N}$, and $(q,m) = 1$. Let α be the smallest natural number with $q^\alpha \equiv 1 \bmod m$.
The sequence $(G(n,t;q)q^{n(n-1)/2})_{n,t} \bmod m$ is generated by the polynomials

$$r_0(X) = 1 + X, \ \ldots, \ r_{\alpha-1}(X) = 1 + q^{\alpha-1}X \in \mathbb{Z}/m\mathbb{Z}[X],$$

and the initial polynomial $g(X) = 1$.
Defining $w(n) = q^{(\alpha-1)\frac{n(n-1)}{2}} \bmod m$, one notices that $w(n+2\alpha) = w(n) \bmod m$, i.e. this sequence is periodic. As

$$G(n,t;q) = G(n,t;q) q^{n(n-1)/2} . q^{(\alpha-1)n(n-1)/2} \bmod m$$

one sees that $(G_m(n,t;q))_{n,t} = (G(n,t;q))_{n,t} \bmod m$ is the product of a periodic one-dimensional sequence and of the sequence $(G(n,t;q)q^{n(n-1)/2}) \bmod m$ generated by the polynomials $r_0, \ldots, r_{\alpha-1}$ and the initial polynomial $g = 1$.
2. The Stirling numbers of first kind $S(t,n)$, ([31] p. 18, [21]), are defined by

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

Let $m \in \mathbb{N}$, $m \geq 2$. Then the sequence $(S_m(n,t))_{n,t}$ (Stirling numbers mod m):

$$S_m(n,t) = S(t,n) \bmod m$$

is generated by the polynomials $r_i(X) = X + i, \quad 0 \leq i \leq m-1$, and the initial polynomial $g(X) = 1$.

From Corollary 2 and Proposition 1 follows

Corollary 4 *Let $r_0(X), \ldots, r_{\alpha-1}(X) \in \mathrm{R}[X]$, $r(X) = r_0(X) \ldots r_{\alpha-1}(X)$. If $r(X)^k$ has the m-Fermat property for some $k \in \mathbb{N}$, $k \geq 2$, then the sequence $(u_{\mathcal{R},g}(n,t))_{n,t}$ is m-automatic for every polynomial $g(X) \in \mathrm{R}[X]$.*

From Corollary 2 and Lemma 2 follows, (remember that p-automaticity and p^k-automaticity are equivalent):

Corollary 5 *Let p be a prime number and k, $q \in \mathbb{N}$.*
1. If $(q,p) = 1$ then the sequence $(G_{p^k}(n,t;q))_{n,t}$ of the Gaussian binomial coefficients mod p^k is p-automatic.
2. The sequence $(S_{p^k}(n,t))_{n,t}$ of the Stirling numbers of first kind mod p^k is p-automatic.

Acknowledgments This work was done while the first author was visiting the University of Bremen. The first author wants to thank very warmly his colleagues for their hospitality. We thank the two referees for their remarks.

References

[1] J.-P. Allouche, Somme des chiffres et transcendance, Bull. Soc. math. France **110** (1982) 279–285.

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

[3] J.-P. Allouche, Finite automata in 1-dimensional and 2-dimensional physics, in: J.-M. Luck, P. Moussa, M. Waldschmidt, eds., Number Theory and Physics, Proceedings in Physics **47**, (Springer, 1990) 177–184.

[4] J. Berstel and M. Morcrette, Compact representation of patterns by finite automata, Pixim' 89 (proceedings) (Hermes, 1989) 387–402.

[5] J. Berstel and A. Nait Abdallah, Tétrarbres engendrés par des automates finis, Publications du L. I. T. P. **89–7** (1989), et Bigre + Globule, **61–62** (1989) 167–175.

[6] B. Bondarenko, Generalized Triangles and Pyramids of Pascal, Their Fractals, Graphs and Applications (Fan, Tashkent, 1990), (in Russian).

[7] L. Childs, A Concrete Introduction to Higher Algebra (Springer, 1979).

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

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

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

[11] K. Culik II and S. Dube, Fractal and recurrent behavior of cellular automata, Complex Systems **3** (1989) 253–267.

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

[13] H. Furstenberg, Algebraic functions over finite fields, J. Algebra **7** (1967) 271–277.

[14] F. von Haeseler, H.-O. Peitgen, G. Skordev, Pascal's triangle, dynamical systems and attractors, Ergod. Th. & Dynam. Sys. **12** (1992) 479–486.

[15] F. von Haeseler, H.-O. Peitgen, G. Skordev, Linear cellular automata, substitutions, hierarchical iterated systems, in: J. L. Encarnasao et al. eds., Fractal Geometry and Computer Graphics (Springer, 1992).

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

[17] 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.

[18] F. von Haeseler, H.-O. Peitgen, G. Skordev, Global analysis of self-similarity features of cellular automata: selected examples, (in preparation).

[19] J. Holte, A recurrence relation approach to fractal dimension in Pascal's triangle, ICM-90, Kyoto.

[20] J. Holte, *The dimension set of multinomial coefficients divisible by n*, Amer. Math. Soc. Ann. Meeting, Jan. 18, 1991.

[21] D. Knuth, Two notes on notations, Amer. Math. Monthly **99** (1992) 403–422.

[22] E. Kummer, Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen, J. reine angew. Math. **44** (1852) 93–146.

[23] E. Lange, H.-O. Peitgen, G. Skordev, Fractal patterns in Gaussian and Stirling number tables, Inst. Dyn. Syst., University of Bremen, Report 292, 1992..

[24] B. Litow, P. Dumas, Additive cellular automata and algebraic series, Theoret. Comput. Sci. **119** (1993), 345–354.

[25] E. Lucas, Sur les congruences des nombres eulériens et des coefficients différentiels des fonctions trigonométriques, Bull. Soc. math. France **6** (1878) 49–54.

[26] G. Polya, G. Alexanderson, Gaussian binomial coefficients, Elem. Math. **26** (1971) 102–109.

[27] A. Robison, Fast computation of additive cellular automata, Complex Systems **1** (1987) 211–216.

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

[29] O. Salon, Suites automatiques à multi-indices, Séminaire de Théorie des Nombres de Bordeaux, Exp. 4, 1986–1987.

[30] J. Shallit, J. Stolfi, Two methods for generating fractals, Comp. and Graphics **13** (1989) 185–191.

[31] R. Stanley, Enumerative Combinatorics, I (Wadsworth, Brooks/Cole, Advances Books, Software, Monterey, California, 1986).

[32] M. Sved, Geometry of combinatorial arithmetic, Ars Combinatoria **21** (1986) A, 271–298.

[33] M. Sved, Divisibility - with visibility, Math. Intell. **10** (1988) 56–64.

[34] M. Sved, J. Pitman, Divisibility of binomials by prime powers, a geometrical approach, Ars Combinatoria **26** (1988) A, 197–222.

[35] S. Takahashi, Self-similarity of linear cellular automata, J. Comp. Sci. **44** (1992) 114–140.

[36] H. S. Wilf, An aperiodic sequence, Problem E 3457, solution by J. R. Griggs, Amer. Math. Monthly **100** (1993) 502–503.

[37] S. Willson, Cellular automata can generate fractals, Discrete Appl. Math. **8** (1984) 91–99.

[38] S. Willson, Growth rates and fractional dimensions in cellular automata, Physica D **10** (1984) 69–74.

[39] S. Willson, The equality of fractional dimensions for certain cellular automata, Physica D **24** (1987) 179–189.

[40] S. Willson, Computing fractal dimensions for additive cellular automata, Physica D **24** (1987)190–206.

[41] S. Willson, Calculating growth rates and moments for additive cellular automata, Discrete Appl. Math. **35** (1992) 47–65.

[42] S. Wolfram, Statistical mechanics and cellular automata, Rev. Modern Phys. **55** (1983) 601–644.

[43] S. Wolfram, Some recent results and questions about cellular automata, in: J. Demongeot, E. Goles, M. Tchuente eds, Dynamical systems and cellular automata (Acad. Press, 1985) 153–167.

[44] S. Wolfram, Geometry of binomial coefficients, Amer. Math. Monthly **91** (1984) 566–571.

J.-P. Allouche,
C. N. R. S., L. M. D.
Luminy, Case 930
F-13288 Marseille Cedex 9
France

F. von Haeseler, H.-O. Peitgen, G. Skordev,
Center for Complex Systems and Visualization,
University of Bremen,
D-28334 Bremen, FRG
Germany