ELSEVIER

Discrete Applied Mathematics 66 (1996) 1–22

DISCRETE APPLIED MATHEMATICS

# Linear cellular automata, finite automata and Pascal's triangle

J.-P. Allouche[a], F. von Haeseler[b,*,1], H.-O. Peitgen[b], G. Skordev[b]

[a] *CNRS, LMD, Luminy, Case 930, F-13288 Marseille Cedex 9, France*

[b] *Centre for Complex Systems and Visualization, Universität Bremen, Postfach 330440, D-28334 Bremen, Germany*

Received 23 July 1993; revised 31 May 1994

**Abstract**

We address the question whether double sequences produced by one-dimensional linear cellular automata can also be generated by finite automata. A complete solution for binomial coefficients and Lucas' numbers is given and some partial results for the general case are presented.

## 1. Introduction

The properties of binomial coefficients have attracted the attention of a large number of mathematicians and amateur mathematicians over the last centuries, cf. [6]. Two results are fundamental: Lucas' lemma [21] and Kummer's lemma [19, p. 115]. Lucas' lemma gives an explicit formula for the residues of binomial coefficients $\binom{t}{n}$ modulo a prime number $p$ in terms of the $p$-adic expansions of $t$ and $n$:

$$\binom{t}{n} \equiv \binom{t_0}{n_0} \cdots \binom{t_s}{n_s} \bmod p,$$

where

$$t = t_s p^s + \cdots + t_1 p + t_0,\ n = n_s p^s + \cdots + n_1 p + n_0, \quad t_i, n_i \in \{0, 1, \ldots, p-1\}.$$

Kummer's lemma answers the question of the largest power $k$ of a prime number $p$ which divides the binomial coefficient $\binom{t}{n}$: $k$ is obtained as the number of carries generated in the $p$-adic subtraction of $t - n$. Thus, the explicit value of the residues

* Corresponding author.

[1] Supported by DFG "Forschungsgruppe Dynamische Systeme".


*SSDI* 0166-218X(94)00132-4

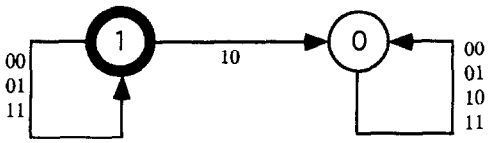


Fig. 1. A two-dimensional 2-automaton corresponding to the Lucas formula for binomial coefficients, $p = 2$.

$\binom{t}{n} \bmod p^k$ is not given; however, Kummer's lemma tells us whether it is zero or not zero. For our considerations it is interesting to note that Lucas' lemma can be interpreted as a two-dimensional $p$-automaton (a formal definition will be given later). Let us look at the example where $p = 2$. Here the 2-automaton has two states 0 and 1 and two input maps $(i, j): \{0, 1\} \to \{0, 1\}$, $i, j \in \{0, 1\}$, defined by $(0, 0).1 = (0, 1).1 = (1, 1).1 = 1$, $(1, 0).1 = 0$ and $(i, j).0 = 0$ for all $i, j = 0, 1$. Using this notation Lucas' formula can be written as

$$\binom{t}{n} \bmod 2 = (n_0, t_0) \cdots (n_s, t_s).1.$$

More conveniently the input maps are represented as arrows of a directed graph with nodes given by the states and a distinguished initial state 1, see Fig. 1.

This graph is called the transition graph of the finite automaton. For the computation of the residue of the binomial coefficient $\binom{t}{n}$ we simply follow the arrows starting from the initial node (state) $(n_s, t_s), (n_{s-1}, t_{s-1}), \ldots, (n_0, t_0)$ and arriving to some final node which gives the residue of the binomial coefficient. Thus we see that the sequence $(\binom{t}{n} \bmod 2)_{t,n \geqslant 0}$ can be generated by a (two-dimensional) 2-automaton. Observe that here we have read the dyadic representation from left to right and followed the corresponding arrows. We call such an automaton a $p$-automaton of the L–R kind. We could also read the dyadic representations from right to left. In this case we speak of a $p$-automaton of the R–L kind. For the 2-automaton corresponding to Lucas' lemma the direction of reading is in fact irrelevant. Two-dimensional automata of the L–R kind are also known as matrix substitutions systems and are sometimes called two-dimensional substitutions [24–26]. A (double) sequence generated by a two-dimensional $p$-automaton (of the L–R or the R–L kind, which is known to be equivalent) is called $p$-automatic [25]. Hence, the binomial coefficients modulo a prime number $p$ form a $p$-automatic (double) sequence. Explicit $p$-automata of the R–L kind corresponding to Kummer's lemma were given in [14]. However the presentation there was in a geometrical setting and was technically given in the language of hierarchical iterated function systems [22], see Fig. 2, where (two-dimensional) 2-automata $\mathscr{A}_l$ of the R–L kind for $p = 2$ and $l = 2$, $l = 3$ are presented. Now we shall explain how these automata work. For every natural number $l$ the sequence $(a_l(n, t))_{n,t \geqslant 0}$ defined by

$$a_l(n, t) = \begin{cases} 1 & \text{if } 2^l \text{ does not divide } \binom{t}{n}, \\ 0 & \text{otherwise} \end{cases}$$

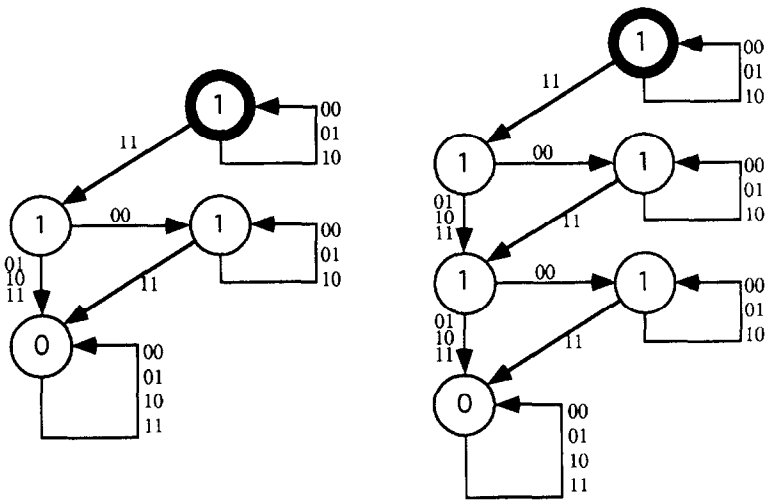


Fig. 2. A two-dimensional 2-automaton corresponding to the Kummer lemma for binomial coefficients, with $p = 2$ and $l = 2, 3$.

is produced by the automaton $\mathscr{A}_l$ as follows:

$$a_l(n, t) = (k_s, t_s)(k_{s-1}, t_{s-1}) \cdots (k_0, t_0).(\text{initial state}),$$

where $t = t_s 2^s + \cdots + t_1 2 + t_0$, $t - n = k_s 2^s + \cdots + k_1 2 + k_0$ and $t_i, k_i \in \{0, 1\}$.

Therefore the sequence $(a_l(n, t))_{n,t \geq 0}$ is 2-automatic. In this paper we will discuss several questions regarding automaticity of double sequences. The first question is whether the sequence $(\binom{t}{n} \bmod m)_{t,n \geq 0}$ is $k$-automatic (for some $k$ and $m$). In fact, if it would be produced by some $k$-automaton then we would have some Lucas-like formulae for the binomial coefficients modulo $m$. The main result of this paper is that the sequence of binomial coefficients modulo $m$ is $k$-automatic for some $k$ if and only if $m$ is the power of some prime number $p$. In fact, then it is $p$-automatic. The same question can be asked in a more general setting, i.e. for the double sequences which are generated by some (one-dimensional) linear cellular automaton (LCA). Recall that the binomial coefficients modulo $m$ can be generated by the LCA corresponding to the polynomial $1 + X$ considered as a polynomial with coefficients in the ring of residues of the integers modulo $m$. A precise definition of a LCA will be given below. But before stating the general question we shall offer some explanations. An $m$-state LCA is basically a map $A$ on the space of all sequences (called configurations) $\underline{a} = (a(n))_{-\infty}^{\infty}$, with $a(n) \in \{0, 1, \ldots, m-1\}$ for every integer $n$ defined by a local transition rule $\varphi : \{0, \ldots, m-1\}^{d+1} \to \{0, \ldots, m-1\}$ as follows:

$$A(\underline{a})(n) = \varphi(a(n-d+1), \ldots, a(n))$$

and the map $\varphi$ is linear, i.e.

$$\varphi\ (x_0, \ldots, x_d) = \sum_0^d r_{d-i} x_i,\ r_i \in \{0, \ldots, m-1\}.$$

The polynomial $r(X) = r_0 + r_1 X + \cdots + r_d X^d$ is called the generating polynomial of the LCA $A$ (for the binomial coefficients the generating polynomial is $r(X) = 1 + X$). An LCA $A$ produces a (double sequence $(r(n, t))_{n,t \geq 0}$ as follows:

$$r(n, t) = A^t(\underline{\delta})(n),$$

where $\underline{\delta}$ is the configuration $\underline{\delta}(0) = 1$, $\underline{\delta}(n) = 0$ for $n \neq 0$ and $A^t$ is the $t$th iteration of the map $A$. The main problem discussed in this paper is the question whether and when a sequence $(r(n, t))_{n,t \geq 0}$ is $k$-automatic. It should be understood and noted that this question is connected with the question of deciphering the self-similarity properties of the evolution patterns generated by a LCA starting with the simplest initial configuration $\underline{\delta}$. To study the evolution and pattern formation of (one-dimensional) cellular automaton $A$ one usually represents the initial configuration $\underline{a} = (a(n))_n$ as the 0th (in the $Y$-direction) row in a two-dimensional lattice and records state $a(n)$ in site $(n, 0)$. The successive transforms obtained by the iteration of the cellular automaton $A$ are then recorded in the successive rows (in the positive $Y$-direction), i.e. configuration $A^t(\underline{a})$ is represented in the $t$th row. Considering only the set of sites in the lattice which have nonzero states we obtain an evolution pattern. It has been observed that for many cellular automata (all LCA with a few trivial exceptions) the evolution patterns starting from initial configurations with a finite number of nonzero states have a fractal structure with an often very convoluted self-similarity structure, cf. [31–34, 10]. To study the evolution pattern, which is an unbounded set for $t \to \infty$, one has to apply a rescaling. Willson proposed in [31] the following scaling procedure for $p^k$-state LCA, where $p$ is a prime number. Consider the evolution pattern of the automaton up to the time $p^n$, $n \in \mathbb{N}$, and rescale it by the factor $1/p^n$. One thus obtains a sequence of compact sets which converges towards a limit (called rescaled evolution set in [17]). For that reason we call the sequence a scaling sequence for the LCA. It turns out that the rescaled evolution set in fact does not depend on the particular initial configuration, as long as we start with initial configurations which have a finite number of nonzero states [31]. In Figs. 3 and 4 we provide rescaled evolution sets for two examples of LCA.

The self-similarity structure of the rescaled evolution set of the binomial coefficients modulo a power of a prime number $p$ is deciphered by the geometrical interpretation (hierarchical iterated function system) of a (two-dimensional) $p$-automaton of the R–L kind corresponding to Kummer's lemma [14]. The patterns of those of the binomial coefficients which are not zero modulo a prime power are considered also in [28, 18].

The problem of deciphering the geometrical self-similarity properties of LCA has been solved in some special cases by [29, 14] and in the general case in [15]. The general solution in [16, 17] uses special hierarchical iterated function systems which are generated by two-dimensional substitutions (matrix substitution systems), or as mentioned earlier by (two-dimensional) $p$-automata of the L–R kind. In the case of a $p$-state LCA this $p$-automaton produces the sequence $(r(n, t))_{n,t}$ generated by the LCA, i.e. this sequence is $p$-automatic. But in the case of $p^k$-state LCA, $k \geq 2$, this $p$-automaton generates only the sequence $(r(n, p^{k-1}l))_{n,l}$.

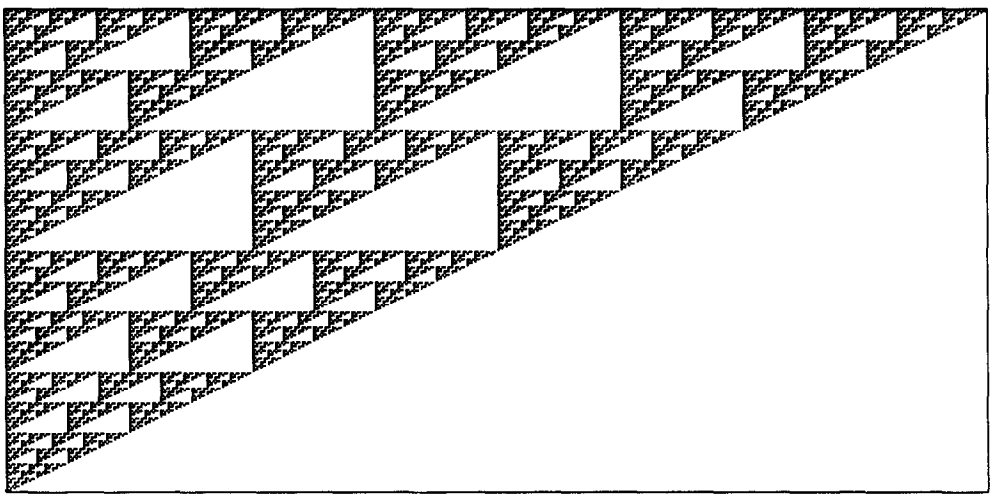

Fig. 3. Rescaled evolution sets for the LCA with generating polynomial $1 + X + X^2 \bmod 2$.

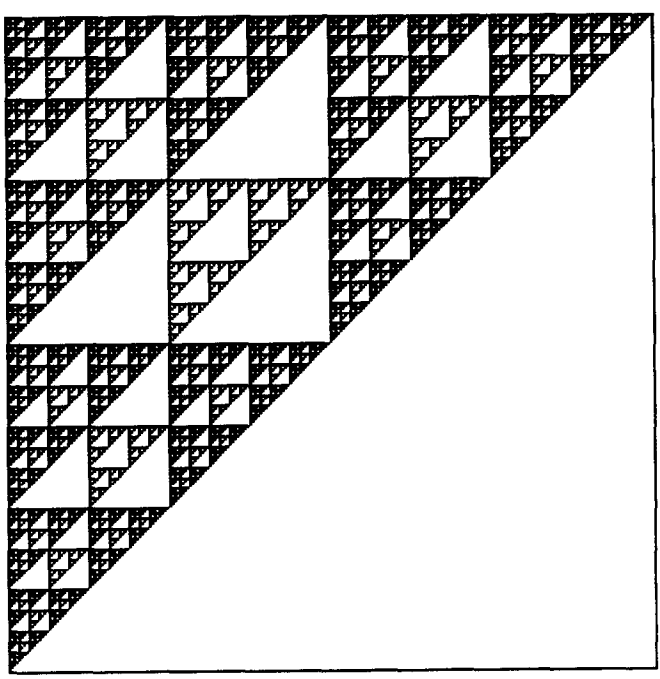

Fig. 4. Rescaled evolution set for the LCA with generating polynomial $1 + X \bmod 4$.

Before presenting the 2-automaton constructed in [16, 17] for the deciphering of the self-similarity properties of the binomial coefficients modulo 4, as an example, we make one remark.

It is common knowledge that the self-similarity properties of the evolution patterns of $m$-state LCA for $m$ not a prime power are very complicated and there is no simple and natural way to define a rescaled evolution set in this case. In Fig. 5 the evolution of the automaton with generating polynomial $1 + X \bmod 6$ is shown. One observes easily that it is the superposition of the evolution sets of $1 + X \bmod 2$ and $1 + X \bmod 3$, respectively.

Following Willson's idea, we know that a rescaling with $1/2^n$, respectively $1/3^n$ gives a limit set for the evolution set of $1 + X \bmod 2$, respectively $1 + X \bmod 3$. Therefore, the key idea to obtain a limit set for the evolution set is the following, find a sequence $(t_n)_{n\in\mathbb{N}}$ such that $t_n$ is "close" both to a power of 2 and to a power of 3. But a theorem of

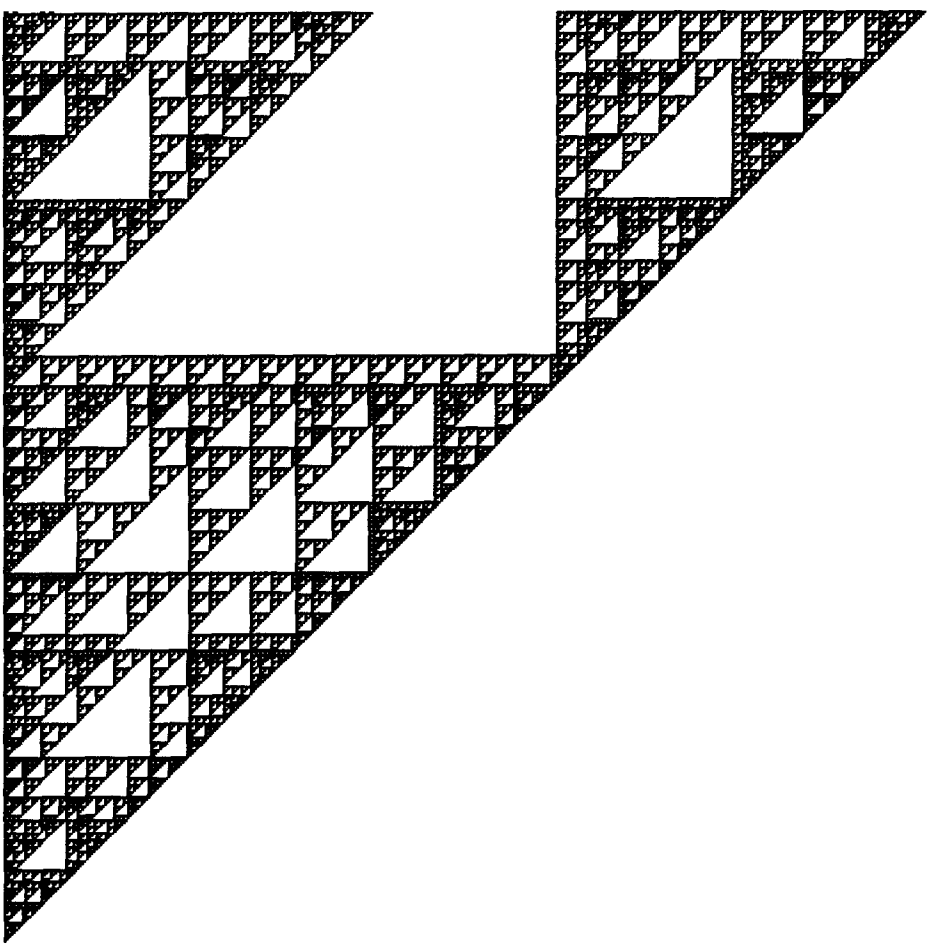

Fig. 5. The evolution set for the LCA with generating polynomial $1 + X \bmod 6$ is the union of the evolution sets of the LCA with generating polynomial $1 + X \bmod 2$ and the LCA with generating polynomial $1 + X \bmod 3$.

number theory (more precisely in Diophantine approximation theory) asserts that the equation

$$\left|\frac{\log 2}{\log 3} - \frac{p}{q}\right| < \frac{1}{q^2},$$

with $p, q \in \mathbb{Z}$, $p$ and $q$ coprime, has infinitely many solutions. This equation yields $|\log(2^q/3^p)| < C/q$. It is shown in [16], in a more general setting, that the sequence $(2^q)_q$ is a scaling sequence for $1 + X \bmod 6$. Moreover, the rescaled evolution set is the union of the evolution sets of $1 + X \bmod 2$ and $1 + X \bmod 3$. This is shown in Fig. 6.

In the last example we present a (two-dimensional) 2-automaton of the L–R kind which produces only the even rows of the binomial coefficients modulo 4. Its

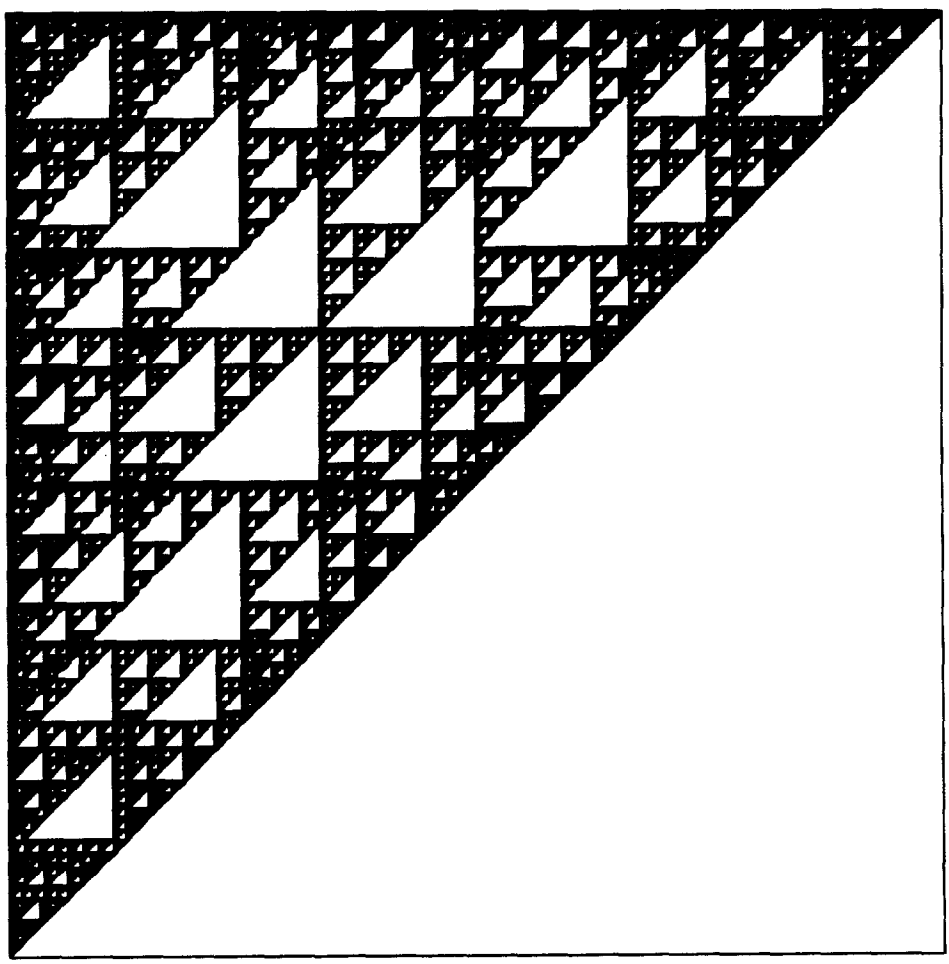

Fig. 6. Rescaled evolution set for the LCA with generating polynomial $1 + X \bmod 6$.

geometrical interpretation as hierarchical iterated function system generates the corresponding rescaled evolution set and thus deciphers, the self-similarity properties of this set. For more examples and details see [15–17]. The state set of the 2-automaton deciphering the self-similarity properties of the binomial coefficients modulo 4 is $Q = \{0,1,2,3\}^2$ with initial state 01. The input maps $(i,j): Q \to Q, i,j \in \{0,1\}$, are defined by

$$(i,j).(\alpha,\beta) = \alpha(i,j).10 + \beta(i,j).01$$

and

$$(0,0).01 = 01, \quad (1,0).01 = 10, \quad (0,1).01 = 01, \quad (1,1).01 = 12,$$

$$(0,0).10 = 00, \quad (1,0).10 = 00, \quad (0,1).10 = 21, \quad (0,1).10 = 10.$$

Then

$$\binom{2t}{n} \bmod 4 = \tau((n_0,t_0)\cdots(n_s,t_s).01),$$

where

$$t = t_s p^s + \cdots + t_1 p + t_0, \quad n = n_s p^s + \cdots + n_1 p + n_0, \qquad t_i, n_i \in \{0,1,\ldots,p-1\},$$

are the $p$-adic representations of the numbers $t, n$ and the output map $\tau$ is simply the projection onto the right coordinate, $\tau(\alpha,\beta) = \beta$. One of the general consequences of the results of this paper is that *the sequences generated by any $p^k$-state LCA are all $p$-automatic.*

Note that relations between one-dimensional cellular automata and one-dimensional transducers have also been studied; one can read for example [34, pp. 189–231].

## 2. Preliminaries

### 2.1. Two-dimensional automata and double automatic sequences

Let $m \in \mathbb{N}$, $m \geqslant 2$. A two-dimensional $m$-automaton $\mathscr{A} = (A, a_0, \varphi, T, \tau)$ 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 [1, 2, 25, 24] or, for the equivalent notion of matrix (two-dimensional) substitutions, [26, 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 $\mathscr{A}$ 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) [24, 25].

### 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. We denote by $R((X^{-1}))$ the set of all formal Laurent series with coefficients in $R$. An element of $R((X))$ is denoted by

$$g(X) = \sum_{i=-\infty}^{\infty} g_i X^i,$$

where $g_i \in R$.

Here we shall recall only the definition of a linear cellular automaton induced by a given polynomial $r(X) \in R[X]$ (for a more general definition see [34]). A polynomial $r(X)$ of degree $d$ induces a linear cellular automaton, denoted by $A_r$, which is defined as

$$A_r: R((X^{-1})) \to R((X^{-1})),$$

$$g(X) \mapsto r(X)g(X),$$

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

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

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

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

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

specifies the state of the cell at position $i$ and 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 polynomial $r(x)$ 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 $m\in\mathbb{N}$, $m\geqslant 2$ and define the double sequence

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

where

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

**Remarks.** (1) If $r(X) = 1 + X$ and $g(X) = 1$, the corresponding sequence given by Eq. (1) is the (double) sequence of the binomial coefficients $(\binom{t}{n})_{n,t} \bmod m$.

(2) For $r(X) = 1 + X$ and $g(X) = 1 + 2X$, we obtain the Lucas numbers modulo $m$, [6, p. 22].

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

If $m = p$ is a prime number, then there is an affirmative answer which follows for instance from a theorem of Salon [24, 25, Theorem 5.1] (a generalization of the corresponding theorem of Christol et al. [7, Theorem 1]). The key idea is to consider the power series

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

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

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

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 $(g_p(n, t))_{n,t}$.

But for composite numbers $m$ we have to apply different arguments. We shall prove the following assertions.

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

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

(b) *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. Then the sequence $(g_{p^l}(n,t))_{n,t \geqslant 0}$ (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 $1 \neq 0$).

**Definition.** Let $r(X) \in \mathbb{N}, m \geqslant 2$. The polynomial $r(X)$ has the *$m$-Fermat property* if

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

**Remark.** In [23] 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 samples of polynomials with the $m$-Fermat property.

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

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

*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 $1 \leqslant i \leqslant p^k - 1$ (Lucas' lemma, [27, p. 53, Ex. 6a]), 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 $\mathrm{GF}(p^k)$ 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*

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

*be a polynomial. If $p^k R = 0$ and $r_i^p \equiv r_i \bmod pR$, $i = 0, \ldots, d$, 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 [19, pp. 115–116] that

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

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** (Robison [23]). 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 $1 \neq 0$, $r(X) \in R[X]$ be a polynomial, $k, m \in \mathbb{N}$, $m \geqslant 2$.

Here we shall define a two-dimensional $m$-automaton $\mathscr{A}_k(r)$, corresponding to the polynomial $r(X)$. The $m$-automaton $\mathscr{A}_k(r)$ has

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

The output map $\tau_1 : R^k \to R$ is defined, for $(\alpha_{-k+1}, \ldots, \alpha_0) \in R^k$, by

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

For the definition of the input maps

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

we need some notations.

The map

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

$$b_k(l(X)) = (l_{-k+1}, \ldots, l_0), \ \forall l = l(X) = \sum_{n=-\infty}^{+\infty} l_n X^n \in R((X^{-1})),$$

is called a $k$-block map. The map $b_k$ is an $R$-module homomorphism. By $e_i = 0, \ldots, k-1$, 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 $(i, j) : R^k \to R^k$ will be an $R$-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 $e_l$, $l = 0, \ldots, k-1$:

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

for $i, j \in \{0, 1, \ldots, m-1\}$, $0 \leqslant l \leqslant k-1$. Observe that $e_0$ is a fixed point of the map $(0, 0)$.

We shall use the $m$-automaton $\mathscr{A}_k(r)$ to produce the sequence $(g(n, t))_{n,t}$ defined by Eq. (2) for $g(X) = 1$, and a given polynomial $r(X) \in R[X]$. In the next section we shall consider the case of a polynomial $r(X)$ which has the $m$-Fermat property for some integer $m \geqslant 2$.

## 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 $1 \neq 0$) and $r(X) \in R[X]$. The polynomial $r(X)$ produces a double sequence $(r(n, t))_{n,t \geqslant 0}$ 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 $(r(n,t))_{n,t\geqslant 0}$ is $m$-automatic and the $m$-automaton $\mathscr{A}_k(r)$ produces this sequence for any $k \geqslant \deg r(X)$.*

**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

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

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

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

**Remark.** Theorem 3 is proved in a more general setting, for $n$-dimensional $m$-Fermat (called strong Fermat) cellular automata in [16]. The proof presented here is simpler. Another proof based upon the notion of $m$-kernel (see [25]) will be presented in the next section.

Theorem 3 implies

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

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

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

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

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

As a next step we consider double sequences generated by a polynomial $r(X) \in R[X]$ 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 $(u(n,t))_{n,t\geqslant 0}$ be a sequence with values in a finite set such that there exist two integers $a \geqslant 1$ and $b \geqslant 1$ for which all the sequences $(u(an+c, bt+d))_{n,t\geqslant 0}$ with $c \in [0, a-1]$, $d \in [0, b-1]$ are $m$-automatic for some integer $m \geqslant 2$. Then the sequence $(u(n,t))_{n,t\geqslant 0}$ itself is $m$-automatic.*

**Proof.** Our proof will mimic the proof of the analogous claim for the one-dimensional case (see for example the related proof for $k$-regular one-dimensional sequences in [3, Theorem 2.7]). 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 $m \geqslant 2$, for some integer $a \geqslant 2$, and for every $c \in [0, a-1]$ the sequence $(w(an+c,t))_{n,t}$ is $m$-automatic. Then from the theorem of Salon [25] the kernels of all these sequences are finite.

To prove that the sequence $w$ itself is $m$-automatic, one has to prove that the $m$-kernel of $w$, i.e. the set of subsequences

$$\{(w(m^\alpha n + \beta, m^\alpha t + \gamma))_{n,t} : \alpha \geqslant 0,\ 0 \leqslant \beta, \gamma \leqslant m^\alpha - 1\},$$

is finite, see [25, 9, 7]. Therefore it suffices to prove that there are only finitely many sequences of the type

$$(w(m^\alpha(an + c) + \beta, m^\alpha t + \gamma))_{n,t}, \quad c \in [0, a-1],\ \alpha \geqslant 0,\ 0 \leqslant \beta,\ \gamma \leqslant m^\alpha - 1.$$

Now write $m^\alpha c + \beta = ax + y$, with $0 \leqslant y \leqslant a - 1$. One has $ax \leqslant ax + y = m^\alpha c + \beta < m^\alpha(c+1) \leqslant am^\alpha$. Hence $x < m^\alpha$, i.e. $x \leqslant m^\alpha - 1$. Then $(w(m^\alpha(an + c) + \beta, m^\alpha t + \gamma)) = w(a(m^\alpha n + x) + y, m^\alpha t + \gamma)$. The numbers $x$ and $y$ do not depend on $(n, t)$, but only on $\alpha$, $\beta$ and $c$. Moreover, $y \leqslant a - 1$ and $x \leqslant m^\alpha - 1$.

Hence the sequence $(w(a(m^\alpha n + x) + y, m^\alpha t + \gamma))_{n,t}$ is in the $m$-kernel of the sequence $(w(an + y, t))_{n,t}$, i.e. the kernel of the sequence $w$ is contained in the union (w.r.t. $y$) of the kernels of the sequences $w(an + y, t)$ and since all of them are finite (see for instance [25]), the assertion follows. □

**Corollary 2.** *Let $g$ and $r$ be two polynomials in $R[X]$ such that there exists an integer $k \geqslant 2$ for which the polynomial $r(X)^k$ has the $m$-Fermat property. Then the double sequence $(g(n, t))_{n,t \geqslant 0}$ (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 [25, Proposition 7.6] it follows that the sequence $(r(an + b, cd + d))_{n,t}$ is $p$-automatic. Then the assertion follows from Theorem 5.1 of [25]. □

**Remark.** The case $a = 0$, $c = 1$, $d = 0$ has been proved in [20] 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 [25]: the $m$-kernel of a sequence $(g(n,t))_{n,t}$ is by definition the set of subsequences

$$\{g(m^\alpha n + u, m^\alpha t + v)_{n,t},\ \alpha \geqslant 0,\ 0 \leqslant u, v \leqslant m^\alpha - 1\}.$$

The sequence $(r(n,t))_{n,t}$ is $m$-automatic if and only if its $m$-kernel is finite (see [24, 25]). Clearly, this is equivalent to the existence of a set of sequences $\mathscr{S}$ such that

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

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

Now, if $h$ is a polynomial in $R[X]$, say $h(X) = \sum b(n)X^n$, define $\Phi_u(h)$, for $0 \leqslant u \leqslant m-1$, to be the polynomial $\Phi_u(h)(X) = \sum b(mn+u)X^n$. Note that $\deg \Phi_u(h) \leqslant (\deg h)/m$, and that for two polynomials $A$ and $B$ one has $\Phi_u(A(X)B(X^m)) = B(X)\Phi_u(A(X))$ [7].

Let $g$ and $r$ be two polynomials in $R[X]$ and define the sequence $(g(n,t))_{n,t}$ by Eq. (2). Let $M = \deg g + (m-1)\deg r$, and let $\mathscr{S}$ be the set

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

As $h$ belongs to a finite set of polynomials ($R$ is finite), the set $\mathscr{S}$ is finite. This set contains the sequence $(g(n,t))_{n,t}$ (take $h = g$). Let us show that $\mathscr{S}$ is stable under the maps $\varphi_{u,v}$.

Let $a$ be a sequence in $\mathscr{S}$ and $h$ be such that $h(X)r(X)^t = \sum_n a(n,t)X^n$, $\forall t$. Then for all $v \leqslant m-1$ 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 $\deg \Phi_u(hr^v) \leqslant (M + (m-1)\deg r)/m \leqslant M$ ($m \geqslant 2$) one deduces that the sequence $(a(mn+u, mt+v))_{n,t}$ belongs to $\mathscr{S}$.

## 8. Proofs of Theorems 1 and 2

Theorem 2 follows from Lemma 2 and Corollary 2. Theorem 2 implies the assertions on automaticity in Theorem 1. Note that a different proof of Theorem 2 could also be deduced from [11].

*Proof of the nonautomaticity assertion in Theorem* 1

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

(a) The integer m admits two different odd prime divisors. We first note the formula (valid on the rational numbers, see for example [27, p. 52]

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

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

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

As this relation holds in $\mathbb{Z}[[X]]$, the ring of power series with integer coefficients, it also holds in $\mathbb{Z}/p\mathbb{Z}[[X]]$, the ring of power series with coefficients in $\mathbb{Z}/p\mathbb{Z}$, 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 $F = P/Q$ 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 nonperiodicity has just been given in [30]).

Hence, from the theorem of Christol et al. [7] the sequence $(\binom{2t}{t})_t \bmod p$ is $p$-automatic and not ultimately periodic if $p$ is an odd prime number.

Now suppose that the sequence $(\binom{t}{n})_{n,t \geqslant 0} \bmod m$ is $k$-automatic for some integer $k \geqslant 2$, and let $p_1$ and $p_2$ be two different odd prime divisors of $m$. Therefore the one-dimensional sequence $(\binom{2t}{n})_t \bmod m$ is $k$-automatic (see for instance [25]). By "projection" (i.e. using the canonical map from $\mathbb{Z}/m\mathbb{Z}$ to $\mathbb{Z}/p_1\mathbb{Z}$), the sequence $(\binom{2t}{t})_t \bmod p_1$ is $k$-automatic. From what precedes we know that this sequence is $p_1$-automatic and not ultimately periodic. Hence from Cobham's theorem [8], $k$ is necessarily a power of $p_1$.

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

(b) The integer $m$ is equal to $2^a p^b$, where $p$ is a prime odd number and $a, b \geqslant 1$. Here we shall study the coefficients $\binom{3t}{t} \bmod 2$. The previous method does not work as the sequence $(\binom{2t}{t})_t \bmod 2$ is ultimately periodic. Remember that Lucas' lemma asserts that if $n$ and $t$ have binary expansions given respectively by $n = \sum_{q \geqslant 0} e_q(n) 2^q$ and $t = \sum_{q \geqslant 0} e_q(t) 2^q$, then

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

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:

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

Hence [9, 7], the sequence $u$ 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

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

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 surprising [7]. 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 $G = P/Q$ 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 $(\binom{t}{n})_{n,t \geqslant 0} \bmod m$ is $k$-automatic for some integer $k \geqslant 2$, and remember that $m = 2^a p^b$, $a, b \geqslant 1$. 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 $(\binom{3t}{t})_t \bmod m$ is $k$-automatic [25]. Hence, by projection, the sequence $(\binom{3t}{t})_t \bmod 2$ is $k$-automatic. As it is 2-automatic and not ultimately periodic, Cobham's theorem [8] 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 $m=p^t$ for some prime number $p$.

## 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 $r_0(X),\dots,r_{\alpha-1}(X)\in R[X]$, $\mathscr{R}=\{r_0(X),\dots,r_{\alpha-1}(X)\}$. The sequence $(u_{\mathscr{R},g}(n,t))_{n,t}$ is generated by the polynomials $\mathscr{R}$ with initial polynomial $g(X)\in R[X]$ if

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

where $t=\alpha t_\alpha+s_\alpha$, $t_\alpha\in\mathbb{N}$, $0\leqslant s_\alpha\leqslant\alpha-1$ (we take $r_{-1}=0$).

**Examples.** (1) The Gaussian binomial coefficients $G(n,t;q)$, $q,n,t\in\mathbb{N}$, $k\geqslant 2$ [27, 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 $\alpha$ 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

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

and the initial polynomial $g(X)=1$. Defining $w(n)=q^{(\alpha-1)(n(n-1)/2)} \bmod m$, 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 $r_0,\dots,r_{\alpha-1}$ and the initial polynomial $g=1$.

(2) The Stirling numbers of first kind $S(t, n)$ [27, p. 18] are defined by

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

Let $m \in \mathbb{N}$, $m \geqslant 2$. 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 $r_i(X) = X + i$, $0 \leqslant i \leqslant m - 1$, and the initial polynomial $g(X) = 1$.

From Corollary 2 and Proposition 1 follows

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

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.*

## Acknowledgements

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, Automates finis en théorie des nombres, Expo. Math. 5 (1986) 239–266.
[2] J.-P. Allouche, Finite automata in 1-dimensional and 2-dimensional physics, in: J.-M. Luck, P. Moussa and M. Waldschmidt, eds., Number Theory and Physics, Proceedings in Physics, Vol. 47 (Springer, Berlin, 1990) 177–184.
[3] J.-P. Allouche and J. Shallit, The ring of $k$-regular sequences, Theoret. Comput. Sci. 98 (1992) 163–197.
[4] J. Berstel and M. Morcrette, Compact representation of patterns by finite automata, Proc. Pixim '89 (Hermes, 1989) 387–402.
[5] J. Berstel and A. Nait Abdallah, Tétrarbres engendrés par des automates finis, Publications du LITP 89-7 (1989) and: 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] G. Christol, T. Kamae, M. Mendès France and G. Rauzy, Suites algébriques, automates et substitutions, Bull. Soc. Math. France 108 (1980) 401–419.
[8] A. Cobham, On the base-dependence of sets of numbers recognizable by finite automata, Math. Systems Theory 3 (1969) 186–192.
[9] A. Cobham, Uniform tag sequences, Math. Systems Theory 6 (1972) 164–192.
[10] K. Culik II and S. Dube, Fractal and recurrent behavior of cellular automata, Complex Systems 3 (1989) 253–267.
[11] J. Denef and L. Lipschitz, Algebraic power series and diagonals, J. Number Theory 26 (1987) 46–67.
[12] S. Eilenberg, Automata, Languages and Machines, Vol. A (Academic 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 and G. Skordev, Pascal's triangle, dynamical systems and attractors, Ergodic Theory Dynamical Systems 12 (1992) 479–486.
[15] F. von Haeseler, H.-O. Peitgen and G. Skordev, Linear cellular automata, substitutions, hierarchical iterated systems, in: J.L. Encarnasao et al., eds., Fractal Geometry and Computer Graphics (Springer, Berlin, 1992).
[16] F. von Haeseler, H.-O. Peitgen and G. Skordev, On the fractal structure of rescaled evolution sets of cellular automata and attractors of dynamical systems, Report 278, Inst. Dyn. Syst., University of Bremen (1992).
[17] F. von Haeseler, H.-O. Peitgen and G. Skordev, Cellular automata, matrix substitutions and fractals, Ann. Math. Art. Intel. 8 (1993) 345–362.
[18] J. Holte, The dimension of the set of multinomial coefficients not divisible by $n$, AMS Annual Meeting (1991).
[19] E. Kummer, Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen, J. Reine Angew. Math. 44 (1852) 93–146.
[20] B. Litow and P. Dumas, Additive cellular automata and algebraic series, Theoret. Comput. Sci. 119 (1993) 345–354.
[21] E. Lucas, Sur les congruences des nombres eulériens et des coefficients différentiels des fonctions trigonométriques, Bull. Soc. Math. France 6 (1878) 49–54.
[22] H.-O. Peitgen, H. Jürgens and D. Saupe, Chaos and Fractals (Springer, Berlin, 1992).
[23] A.D. Robinson, Fast computation of additive cellular automata, Complex Systems 1 (1987) 211–216.
[24] O. Salon, Suites automatiques à multi-indices et algébraicité, C.R. Acad. Sci. Paris 305 (Sér. I) (1987) 501–504.
[25] 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.
[26] J. Shallit and J. Stolfi, Two methods for generating fractals, Comput. Graphics 13 (1989) 185–191.
[27] R. Stanley, Enumerative Combinatorics, I (Wadsworth and Brooks/Cole, Advanced Books and Software, Monterey, CA, 1986).
[28] M. Sved and J. Pitman, Divisibility of binomials by prime powers, a geometrical approach, Ars Combin. 26 (1988) 197–222.
[29] S. Takahashi, Self-similarity of linear cellular automata, J. Comput. Sci. 44 (1992) 14–140.
[30] H.S. Wilf, An aperiodic sequence, Problem E 3457, solution by J.R. Griggs, Amer. Math. Monthly 100 (1993) 502–503.
[31] S. Willson, Cellular automata can generate fractals, Discrete Appl. Math. 8 (1984) 91–99.
[32] S. Willson, A use of cellular automata to obtain families of fractals, in: M. Barnsley and S. Demko, eds., Chaotic Dynamics and Fractals (Academic Press, New York, 1986).
[33] S. Willson, Calculating growth rates and moments for additive cellular automata, Discrete Appl. Math. 35 (1992) 47–65.
[34] S. Wolfram, Theory and Application of Cellular Automata (World Scientific, Singapore, 1986).