Available online at www.sciencedirect.com
SCIENCE DIRECT®
Discrete Mathematics 297 (2005) 91–103
DISCRETE MATHEMATICS
www.elsevier.com/locate/disc

The distribution of elements in automatic double sequences

Yossi Moshe[1]
Ben-Gurion University, Beer-Sheva, Israel

Received 4 December 2003; received in revised form 23 February 2005; accepted 24 March 2005
Available online 11 July 2005

Abstract

Let $A=(A(i,j))_{i,j=0}^{\infty}$ be a q-automatic double sequence over a finite set Ω. Let $g\in\Omega$ and assume that the number $\mathcal{N}_g(A,n)$ of g's in the nth row of A is finite for each n. We provide a formula for $\mathcal{N}_g(A,n)$ as a product of matrices according to the digits in the base q expansion of n. This formula generalizes several results on Pascal's triangle modulo a prime and on recurrence double sequences. It allows us to relate the asymptotic typical behavior of $\mathcal{N}_g(A,n)$ to a certain Lyapunov exponent. In some cases we determine this exponent exactly.

Keywords: Pascal's triangle modulo primes; Recurrence sequences; Asymptotic frequency; Random matrix products; Automatic sequences

1. Introduction

The distribution of the elements in Pascal's triangle modulo a prime p has been extensively studied (cf. [1,6,14,19]). Hexel and Sachs [15] obtained a general (complicated) formula for the number $N(n,g,p)$ of the elements in the nth row which are congruent to g modulo p. (See [5] for another formula which involves characters, and [8,16,17] for similar formulas modulo some prime powers.) Garfield and Wilf [11] defined the polynomial $R_n(x)=\sum_{i=0}^{p-2}N(n,g^i,p)x^i$, where g is a primitive root modulo p. They showed

[1] Current address: Erwin Schrödinger Institute, Boltzmanngasse 9, A-1090, Vienna, Austria.

0012-365X/$ - see front matter
doi:10.1016/j.disc.2005.03.022

how $R_n(x)$ can be obtained from the p polynomials $R_0(x), \ldots, R_{p-1}(x)$. (See Theorem 10 below for the precise formulation.)

Other researchers considered the number $F(n, g, p)$ of g's in the first n rows of the triangle modulo p. Fine [9] proved that the number of nonzero elements in the first p^k rows is $(p(p+1)/2)^k$ and concluded that the density of 0's in the triangle is 1. Barbolosi and Grabner [5] related the behavior of $F(n, g, p)$ to a certain continuous real function (see also [22]) and proved that the asymptotic frequency of each $g \in (\mathbb{Z}/p\mathbb{Z})^{\times}$ among the nonzero elements of Pascal's triangle modulo p is $1/(p-1)$.

Similar questions have been asked in [13] on Pascal's rhombus. Pascal's rhombus is a variation of Pascal's triangle in which values are computed as the sum of four terms, rather than two. More precisely, it is defined by the recurrence relation

$$a_{i,j} = a_{i-1,j-1} + a_{i-1,j} + a_{i-1,j+1} + a_{i-2,j}, \quad 2 \leqslant i \in \mathbb{N}, \quad j \in \mathbb{Z},$$

with the initial conditions

$$\begin{aligned} &a_{1,0} = 1, \\ &a_{i,j} = 0, \quad (i, j) \in \{0, 1\} \times \mathbb{Z} \backslash \{(1, 0)\}. \end{aligned}$$

In [13], an explicit formula for the number of 1's in the first 2^n rows of Pascal's rhombus (mod 2) was obtained, which enables proving that the density of 0's is 1. Also, the number of 1's in the nth row is calculated for some special values of n.

Pascal's triangle and Pascal's rhombus, when viewed modulo a prime, are particular instances of the following general family of (double) sequences. A double array $(A(i, j))_{i=0, j=-\infty}^{\infty, \infty}$ over a finite field $\mathbb{F}$ is a *double linear recurrence sequence of order d with finite rows* (henceforward DLR) if:

(1) $(A(i, j))_{i,j}$ satisfies a recurrence of the form

$$A(i, j) = \sum_{k=1}^{t} c_k A(i - i_k, j - j_k), \quad i \geqslant d, \quad j \in \mathbb{Z}.$$

Here $c_k \in \mathbb{F} \backslash \{0\}$, $j_k \in \mathbb{Z}$, $i_k \in \mathbb{N} \backslash \{0\}$, $t \geqslant 1$ are constants, and $d = \max_{1 \leqslant k \leqslant t} i_k$.

(2) for every $i < d$ there are only finitely many elements $j \in \mathbb{Z}$ such that $A(i, j) \neq 0$.

In view of the above-mentioned results concerning Pascal's triangle and rhombus, it is natural to investigate the distribution of the elements in other DLR's as well. In [21] we obtained a general formula for the number $\#_g(A, n)$ of g's in the first q^n rows of a given DLR, where g is an arbitrary fixed element in the multiplicative group $\mathbb{F}^{\times}$ and $q = |\mathbb{F}|$. We used this formula to characterize the DLR's in which the density of 0's is 1.

In this paper we give a formula for the number $\mathcal{N}(A, n) = \mathcal{N}_g(A, n)$ of g's in the nth row of a DLR A. In fact, we consider even a larger family of double arrays A which contains the *q-automatic double sequences* with finitely many g's in each row. (See for example [2,3] for a background on automatic sequences.) Given such a double array A we construct q square matrices $D_0, \ldots, D_{q-1}$ and vectors $\vec{v}, \vec{e}_0$ such that

$$\mathcal{N}(A, n) = \vec{v}^T D_{n_{k-1}} \ldots D_{n_1} D_{n_0} \vec{e}_0, \quad n = 0, 1, \ldots, \tag{1}$$

where $n = \sum_{r=0}^{k-1} n_r q^r$ is the base q expansion of n.

We use this formula to study the "typical" behavior of $\mathscr{N}(A, n)$, namely its behavior for most n's. It turns out that, in many examples, $\mathscr{N}(A, n)$ behaves typically (approximately) as $e^{\lambda k}$, where k is the length of the base q expansion of n and λ is the so-called *upper Lyapunov exponent*. (See [4] for various Lyapunov exponents.)

2. Notations and main results

Let $A_0(i, j)$ be a DLR over a finite field $\mathbb{F}$. Due to the nature of our questions we may assume, by an appropriate shift of the rows, that $j_k \geqslant 0$ for each k and that $A_0(i, j) = 0$ for every $j < 0$. Hence we may consider A_0 as a double array of the form $A_0 = (A_0(i, j))_{i=0, j=0}^{\infty,\infty}$.

It is convenient to view the initial conditions as determined by an infinite matrix of the form $(B(i, j))_{i=0, j=0}^{d-1,\infty}$, with $B(i, j) \neq 0$ for at most finitely many pairs (i, j), by the requirement

$$A_0(i, j) = B(i, j), \quad i < d, \quad j \in \mathbb{N}.$$

Let Ω be a finite set and $A = (A(i, j))_{i,j=0}^{\infty}$ be a double array over Ω. Let $q \geqslant 2$ be an integer and consider the decomposition of A into q^2 double arrays $(A^{s,t})_{s,t=0}^{q-1}$ according to the values of the two indices modulo q: for each (s, t) with $0 \leqslant s, t < q$, let $A^{s,t} : \mathbb{N} \times \mathbb{N} \to \mathbb{F}$ be given by

$$A^{s,t}(i, j) = A(iq + s, jq + t), \quad i \geqslant 0, \quad j \geqslant 0.$$

Define a sequence $(X_i)_{i=0}^{\infty}$ of finite sets of double arrays by

$$X_0 = \{A\},$$
$$X_{i+1} = \{C^{s,t} : C \in X_i, \ 0 \leqslant s, t < q\}, \quad i \geqslant 0.$$

Put

$$X = \bigcup_{i \in \mathbb{N}} X_i.$$

A is a *q-automatic double sequence* if $X \ (=X(A))$ is a finite set (cf. [2]). Propositions 3, 4 of [21] imply that every DLR over a finite field $\mathbb{F} = \mathrm{GF}(q)$ is q-automatic. (In fact, a similar proof shows that if p^e is a prime power, then every DLR over $\mathbb{Z}/p^e\mathbb{Z}$ is p-automatic.)

Assume from now on that A is a q-automatic double sequence over Ω and that the number, $\mathscr{N}(A, n)$, of g's in each row n of A is finite. For every $C \in X(A)$, let $j_C = \min\{j \mid \exists i; C(i, j) \neq 0\}$, and consider the double array $\overline{C}$ given by

$$\overline{C}(i, j) = C(i, j + j_C), \quad i \geqslant 0, \quad j \geqslant 0.$$

(if $C = 0$ we put $\overline{C} = 0$). Obviously, $\mathscr{N}(\overline{C}, n) = \mathscr{N}(C, n)$ for every n. A double array $(C(i, j))$ over Ω is g-trivial if it contains no g's. Let $T \ (=T_g)$ denote the set of g-trivial double arrays over Ω and let $X' = X'(A)$ be given by

$$X'(A) = \{\overline{C} : C \in X(A) \backslash T\}.$$

Remark. The only reason for introducing the double arrays $\overline{C}$ is to minimize $|X'|$ in our examples. The removal of the g-trivial arrays from X serves also in that we work with X', which is smaller then X. Moreover, we use it in the proof of Theorem 4. However, it has no effect on our main result—Theorem 1.

To avoid triviality we will assume $X' \neq \emptyset$ (otherwise, $\mathcal{N}(A, n) = 0$ identically). Let us enumerate the elements of X', say $X' = \{A_0, \dots, A_{m-1}\}$, where $A_0 = \overline{A}$. If A is a DLR over $\mathrm{GF}(q)$, then so are $A_0, \dots, A_{m-1}$ [21, Proposition 3]. Moreover, each A_i satisfies exactly the same recurrence as A. In such case we denote the initial conditions of A_i by B_i for $i \leqslant m-1$.

For each $s < q$ and $i, j \leqslant m-1$, let $d^s_{i,j}$ be the number of elements $t < q$ such that $\overline{A^{s,t}_j} = A_i$. The $m \times m$-matrices $D_s = (d^s_{i,j})^{m-1}_{i,j=0}$, $0 \leqslant s < q$, will play an important role in the sequel. Let $\{\vec{e}_i : 0 \leqslant i \leqslant m-1\}$ be the standard basis of $\mathbb{Z}^m$, the vectors being considered as column vectors. Let $\vec{v} = (v_i)^{m-1}_{i=0}$ be the column vector defined by $v_i = \mathcal{N}(A_i, 0)$.

Theorem 1. *Let n be a non-negative integer. Write* $n = \sum_{r=0}^{k-1} n_r q^r$ *with* $0 \leqslant n_r < q$ (*where some of the leading digits may vanish*). *Then*

$$\mathcal{N}(A_i, n) = \vec{v}^T D_{n_{k-1}} \dots D_{n_1} D_{n_0} \vec{e}_i .$$

The following theorem generalizes the formula given in [21] for $\#_g(A_i, n)$. (Here E_{q-1} plays the role of the matrix D from [21].)

Theorem 2. *Let* $\mathcal{F}(A_i, n)$ *denote the number of g's in the first n rows of* A_i *and*

$$E_s = D_0 + \cdots + D_s, \quad 0 \leqslant s < q,$$
$$E_{-1} = 0.$$

Then

$$\mathcal{F}(A_i, n) = \vec{v}^T \left(\sum_{r=0}^{k-1} D_{n_{k-1}} D_{n_{k-2}} \dots D_{n_{r+1}} E_{n_r - 1} E^r_{q-1} \right) \vec{e}_i, \tag{2}$$

and in particular,

$$\#_g(A_i, j) = \mathcal{F}(A_i, q^j) = \vec{v}^T E^j_{q-1} \vec{e}_i .$$

Note that the above formula enables us to compute $f(n) = \mathcal{F}(A_i, n)$ in polynomial time (the input being the list of digits in the base q expansion of n).

Example 3. Let A be a 2-automatic double sequence with finitely many g's in each row, then

$$\mathcal{N}(A_i, 10) = \vec{v}^T D_1 D_0 D_1 D_0 \vec{e}_i ,$$

and

$$\begin{aligned}\mathscr{F}(A_i, 10) &= \vec{v}^T(D_1D_0D_1E_{-1} + D_1D_0E_0E_1 + D_1E_{-1}E_1^2 + E_0E_1^3)\vec{e}_i \\ &= \vec{v}^T D_1D_0^2E_1\vec{e}_i + \vec{v}^T D_0E_1^3\vec{e}_i.\end{aligned}$$

Using Theorem 2 one can prove that the number of g's in the first N rows of A is "approximately" $N^{\log_q R}$, where $R = R(E_{q-1})$ is the spectral radius of E_{q-1}. More precisely, there are constants $C, r > 0$ such that for large enough N,

$$CN^{\log_q R} < \mathscr{F}(A, N) < (\log_q N)^r N^{\log_q R}.$$

In particular, the average number of g's in those rows is "approximately" $N^{\log_q R-1}$. It is interesting to compare this average with the number of g's in a *typical row n*. Here, taking a typical n with (up to) k digits means that the digits n_r in the expansion $n = \sum_{r=0}^{k-1} n_r q^r$ are chosen at random independently uniformly from $\{0, \ldots, q-1\}$. The question is how $\mathscr{N}(A, n)$ behaves for most n's as $k \to \infty$. Since choosing the digits n_r randomly means that the matrices appearing in (1) are random, we are naturally led to study certain random matrix products.

Thus, we assume that the matrices (D_{n_r}) are chosen at random independently uniformly from $\{D_0, \ldots, D_{q-1}\}$. By the theorem of Furstenberg and Kesten [10] on product of random matrices, the limit

$$\lambda = \lim_{k\to\infty} \frac{1}{k} \ln \| D_{n_{k-1}} \ldots D_{n_1} D_{n_0} \|$$

exists with probability 1. That is the norm of a typical product $D_{n_{k-1}} \ldots D_{n_0}$ is approximately $e^{\lambda k}$. The limit λ is the *upper Lyapunov exponent* of $D_0, \ldots, D_{q-1}$. (For more on random matrix products see, for example, [7].)

Since the formula for $\mathscr{N}(A, n)$ involves also product by the vectors $\vec{v}^T$, $\vec{e}_0$, it may happen that $\mathscr{N}(A, n)$ behaves differently than the above norm. However, in many cases (for example, when each row of A contain g's and there exists a word $n_{k-1} \ldots n_1 n_0$ such that $D_{n_{k-1}} \ldots D_{n_1} D_{n_0}$ is a strictly positive matrix), we have

$$\lim_{k\to\infty} \frac{\#(n \in [0, q^k) : e^\lambda - \varepsilon < \sqrt[k]{\mathscr{N}(A, n)} < e^\lambda + \varepsilon)}{q^k} = 1$$

for every $\varepsilon > 0$. This implies that,

$$(e^\lambda - \varepsilon)^{\log_q n} < \mathscr{N}(A, n) < (e^\lambda + \varepsilon)^{\log_q n}$$

for almost every n (i.e., for a set of density 1).

It turns out that in many examples $e^\lambda < R/q$ and thus $\lambda/\ln(q) < \log_q R - 1$. (See Examples 5, 7, 8.) Since the number of g's in a typical row $n < N$ is approximately $e^{\lambda \log_q N} = N^{\lambda/\ln(q)}$, this implies that the average number of g's in a row $n < N$ is much bigger than the number of g's in a typical row. The explanation for this difference is that most of the g's are concentrated in a relatively small number of rows ("most of the money belongs to the rich people").

Unfortunately, it is only rarely possible to compute the upper Lyapunov exponent. For example, in [20] Lima and Rahibe computed the upper Lyapunov exponent of 2×2 matrices A, B, where $\det(A) = 0$ (see also [18]). In our case, the sum of entries in any column of the matrices D_s is $\leqslant q$, and thus the upper Lyapunov exponent is $\leqslant \ln q$. The following theorem characterizes the cases where $\lambda = \ln q$. (See Examples 6, 9.)

Theorem 4. *The following properties are equivalent*:

(1) $\lambda = \ln q$.
(2) *The matrices* $D_0, \ldots, D_{q-1}$ *have a common* (*row*) *eigenvector corresponding to the eigenvalue* q.
(3) *There exists a set* $I \subseteq \{0, \ldots, m-1\}$ *of indices such that the sum of entries in each column of each sub-matrix* $((D_0)_{i,j})_{i,j \in I}, \ldots, ((D_{q-1})_{i,j})_{i,j \in I}$ *is* q.
(4)

$$\overline{\lim_{N\to\infty}} \frac{\#((i,j) \in [0,N) \times [0,N) : A(i,j) = g)}{N^2} > 0.$$

(5) $R = q^2$

Remark. There are interesting examples where the matrices $D_0, \ldots, D_{q-1}$ commute (for example, when A is Pascal's triangle modulo a prime). In those cases the number $\mathcal{N}(A,n)$ depends only on the number $s_i(n) = s_{i,q}(n)$ of occurrences of each nonzero digit i in the base q expansion of n, and not on the locations of those digits. For example, if $q = 3$ then $\mathcal{N}(A,5) = \mathcal{N}(A,7) = \mathcal{N}(A,33)$. Actually, using the Jordan form of $D_0, \ldots, D_{q-1}$, one can obtain a much simpler formula for $\mathcal{N}(A,n)$. (See Examples 5, 8.) In those examples it is possible to compute the upper Lyapunov exponent explicitly. This can be done by triangulating $D_0, \ldots, D_{q-1}$ simultaneously. If $\vec{d_i} = (d_i(j))_{j=0}^{m-1}$ is the diagonal in the triangular form of D_i, then

$$\lambda = \max_{0 \leqslant j \leqslant m-1} \frac{1}{q} \ln(d_0(j) \cdot d_1(j) \ldots d_{q-1}(j)).$$

Example 5. Let us use Theorem 1 to obtain the classical formula for the number of 1's in the nth row of Pascal's triangle modulo 2 (cf. [12]). Take A as Pascal's triangle modulo 2 (Fig. 1), and $g = 1$, and calculate $\mathcal{N}(A,n)$.

It can be easily observed that

$$A^{0,0} = A^{1,0} = A^{1,1} = A, \quad A^{0,1} = 0.$$

(Recall that $A^{s,t}$ satisfies the same recurrence as A and thus it is enough to consider the first row of $A^{s,t}$ in order to determine the whole array.) Thus $X' = \{A\}$, and the matrices involved in Theorem 1 are the following 1×1 matrices:

$$D_0 = (1), \quad D_1 = (2), \quad \vec{v} = (1), \quad \vec{e}_0 = (1).$$

By Theorem 1, the number of 1's in the nth row is $2^{s_1(n)}$.

$$\begin{array}{l} 1 \\ 1\ 1 \\ 1\ 0\ 1 \\ 1\ 1\ 1\ 1 \\ 1\ 0\ 0\ 0\ 1 \\ 1\ 1\ 0\ 0\ 1\ 1 \\ 1\ 0\ 1\ 0\ 1\ 0\ 1 \\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1 \\ \vdots \qquad\qquad\qquad \ddots \end{array}$$

Fig. 1. Pascal's triangle modulo 2.

$$\begin{array}{lcl} 1 & \qquad & 2 \\ 1\ 1 & & 2\ 2 \\ 1\ 2\ 1 & & 2\ 1\ 2 \\ 1\ 0\ 0\ 1 & & 2\ 0\ 0\ 2 \\ 1\ 1\ 0\ 1\ 1 & & 2\ 2\ 0\ 2\ 2 \\ 1\ 2\ 1\ 1\ 2\ 1 & & 2\ 1\ 2\ 2\ 1\ 2 \\ \vdots \qquad\qquad \ddots & & \vdots \qquad\qquad \ddots \end{array}$$

Fig. 2. The first rows of A_0 and A_1.

In this example $\lambda = \frac{1}{2}\ln 2$. This implies that in most rows n the number of 1's is "approximately" $\sqrt{n}$. Employing Theorem 2 we check easily that the average number of 1's in the first n rows is, as is well known (cf. [5]), "approximately" $n^{\log_2 3-1}$.

In a similar way, taking A_0 as Pascal's triangle modulo 3, we have $X' = \{A_0, A_1\}$, where $A_1 = 2 \cdot A_0$ (Fig. 2).

It can be easily checked that

$$A_0^{0,0} = A_0^{1,0} = A_0^{1,1} = A_0^{2,0} = A_0^{2,2} = A_0, \quad A_0^{2,1} = A_1, \quad A_0^{s,t} = 0, \quad s < t,$$

$$A_1^{0,0} = A_1^{1,0} = A_1^{1,1} = A_1^{2,0} = A_1^{2,2} = A_1, \quad A_1^{2,1} = A_0, \quad A_1^{s,t} = 0, \quad s < t,$$

and thus

$$D_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad D_1 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \quad D_2 = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}, \quad \vec{v} = \begin{cases} \vec{e}_0, & g = 1 \\ \vec{e}_1, & g = 2 \end{cases}.$$

Using Theorem 1, one can show routinely that the number of 1's in the nth row is $2^{s_1(n)-1}(3^{s_2(n)} + 1)$, and similarly the number of 2's is $2^{s_1(n)-1}(3^{s_2(n)} - 1)$ (cf. [5]).

We refer the reader to the proof of Theorem 10 *infra* for the matrices D_s in the case of Pascal's triangle modulo other primes.

Example 6. Let $A_0(i, j)$ be the second-order DLR over $\mathbb{Z}/2\mathbb{Z}$ generated by the recurrence

$$A_0(i, j) = A_0(i-1, j) + A_0(i-1, j-1) + A_0(i-2, j-1), \quad i \geqslant 2, \quad j \in \mathbb{Z},$$

and the initial conditions given by

$$B_0 = \begin{matrix} 0, 0, 0, 0, \ldots, \\ 1, 0, 0, 0, \ldots \ . \end{matrix}$$

It can be observed directly that the nth row of A_0 consists of n consecutive 1's and thus $\mathcal{N}(A_0, n) = n$.

In this example $X' = \{A_0, A_1\}$, where A_1 is the double array generated by the same recurrence as A_0 and the matrix B_1 of initial conditions given by

$$B_1 = \begin{matrix} 1, 0, 0, 0, \ldots, \\ 1, 1, 0, 0, \ldots \ . \end{matrix}$$

The matrices involved in Theorem 1 are

$$D_0 = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}, \quad D_1 = \begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix}, \quad \vec{v} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad \vec{e}_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

An easy calculation yields

$$\vec{v}^T D_{n_{k-1}} \ldots D_{n_1} D_{n_0} \vec{e}_i = \sum_{r=0}^{k-1} n_r 2^r, \tag{3}$$

so that Theorem 1 gives again the result $\mathcal{N}(A_0, n) = n$. We note that (3) provides an amusing way of calculating a number by means of matrix products, by giving the base 2 expansion of the number.

In this example $\lambda = \ln\ 2$, $R = 4$ and so $e^{\lambda} = R/q$.

Example 7. Let $A_0(i, j)$ be the first-order DLR over $\mathbb{Z}/2\mathbb{Z}$ generated by the recurrence

$$A_0(i, j) = A_0(i-1, j) + A_0(i-1, j-1) + A_0(i-1, j-2), \quad i \geqslant 1, \quad j \in \mathbb{Z},$$

and the initial conditions given by

$$B_0 = 1, 0, 0, \ldots \ .$$

Thus, the nth row of A_0 consists of the coefficients in $(1 + x + x^2)^n$ (mod 2).

A routine calculation shows that $X' = \{A_0, A_1\}$, where the initial conditions of A_1 are given by

$$B_1 = 1,\ 1,\ 0,\ 0,\ \ldots \ .$$

The matrices D_0, D_1 and the vectors $\vec{v}$ and $\vec{e}_0$ are

$$D_0 = \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix}, \quad D_1 = \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix}, \quad \vec{v} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \quad \vec{e}_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Here, $\mathcal{N}(A, n)$ is equal to the number of odd coefficients in $(1+x+x^2)^n$. Theorem 1 shows that this number is $\vec{v}^T D_{n_k} \ldots D_{n_1} D_{n_0} \vec{e}_0$. Thus, for example, there are $\vec{v}^T D_1 D_0 D_1 D_1 \vec{e}_0 = 15$ odd coefficients in $(1 + x + x^2)^{11}$.

The matrices D_0, D_1 satisfy the condition in [20]. Hence we can express the upper Lyapunov exponent as an infinite sum:

$$\lambda = \sum_{i=1}^{\infty} \frac{\ln(\frac{1}{3}(2^{i+2} - (-1)^i))}{2^{i+2}}.$$

In this case the spectral radius of

$$E_1 = \begin{pmatrix} 2 & 4 \\ 1 & 0 \end{pmatrix}$$

is $R = 1 + \sqrt{5}$. One can check that $e^{\lambda} \approx 1.537 < R/2$.

Example 8. Let $A_0(i, j)$ be the second-order DLR over $\mathbb{Z}/2\mathbb{Z}$ generated by the recurrence

$$\begin{aligned} A_0(i, j) = {} & A_0(i-1, j) + A_0(i-1, j-1) + A_0(i-2, j) \\ & + A_0(i-2, j-1) + A_0(i-2, j-2), \quad i \geqslant 2, \ j \in \mathbb{Z}, \end{aligned}$$

and the initial conditions which are given by

$$B_0 = \begin{matrix} 0, \ 0, \ 0, \ 0, \ \ldots, \\ 1, \ 1, \ 0, \ 0, \ \ldots \ . \end{matrix}$$

Here, $X' = \{A_0, A_1, A_2\}$ and

$$B_1 = \begin{matrix} 1, \ 0, \ 0, \ 0, \ \ldots, \\ 0, \ 1, \ 0, \ 0, \ \ldots, \end{matrix} \qquad B_2 = \begin{matrix} 1, \ 0, \ 0, 0, \ \ldots, \\ 1, \ 0, \ 0, \ 0, \ \ldots \ . \end{matrix}$$

The matrices D_0, D_1 and the vectors $\vec{v}$ and $\vec{e}_0$ are

$$D_0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad D_1 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \quad \vec{v} = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}, \quad \vec{e}_0 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}.$$

Note that $D_0 D_1 = D_1 D_0$, which enables us (as in Example 5) to obtain the following simple formula for the number of 1's in the nth row:

$$\mathcal{N}(A_0, n) = \tfrac{2}{3}(2^{s_1(n)} - (-1)^{s_1(n)}).$$

Here $\lambda = \frac{1}{2} \ln 2$, $R = 3$.

Example 9. Let A_0' be the DLR generated by the same recurrence relation as in Example 8, but this time let the initial conditions be given by

$$B_0' = \begin{matrix} 0, \ 0, \ 0, \ 0, \ \ldots, \\ 1, \ 0, \ 0, \ 0, \ \ldots \ . \end{matrix}$$

A simple calculation shows that $X' = \{A_0', A_1', A_2'\}$ where A_1', A_2' satisfy the initial conditions

$$B_1' = \begin{matrix} 1, \ 0, \ 0, \ 0, \ \ldots, \\ 0, \ 0, \ 0, \ 0, \ \ldots \ . \end{matrix} \qquad B_2' = \begin{matrix} 1, \ 0, \ 0, \ 0, \ \ldots, \\ 1, \ 1, \ 0, \ 0, \ \ldots, \end{matrix}$$

respectively, and

$$D_0 = \begin{pmatrix} 2 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad D_1 = \begin{pmatrix} 1 & 2 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 2 \end{pmatrix}, \quad \vec{v} = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}, \quad \vec{e}_0 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}.$$

Using Theorem 4 we have $\lambda = \ln 2$, which is bigger than the Lyapunov exponent of the previous example. Thus, the asymptotic behavior of $\mathcal{N}(A, n)$ may depend on the initial conditions. (In fact, according to several examples we investigated, this phenomenon seems to occur frequently.)

Finally, as an application of Theorem 1, we give a new proof for the following result of Garfield and Wilf.

Theorem 10 (*Garfield and Wilf [11]*). *Let p be a prime and g a primitive root modulo p. Denote by $N(n, g, p)$ the number of g's in the nth row of Pascal's triangle modulo p. Define a polynomial sequence $(R_n(x))_{n=0}^{\infty}$ by $R_n(x) = \sum_{i=0}^{p-2} N(n, g^i, p)x^i$. Let $n = \sum_{r=0}^{k-1} n_r p^r$ be an integer expanded in base p. Then $R_n(x)$ is the remainder of the Euclidean division of the polynomial $P(x) = R_{n_0}(x)R_{n_1}(x)\ldots R_{n_{k-1}}(x)$ by $x^{p-1} - 1$.*

3. Proofs

Lemma 11. *For all $n \geqslant 0$ and $s \in \{0, \ldots, q-1\}$*:

$$\mathcal{N}(A, qn + s) = \sum_{t=0}^{q-1} \mathcal{N}(A^{s,t}, n).$$

Proof. The lemma follows straightforwardly from the definition of $A^{s,t}$. $\square$

Proof of Theorem 1. For every $n \geqslant 0$ define a row *m*-vector, $\vec{v}^n = (v_i^n)_{i=0}^{m-1}$, by $v_i^n = \mathcal{N}(A_i, n)$ (thus we have $\vec{v}^0 = \vec{v}^T$). Let us prove that $\vec{v}^{qn+s} = \vec{v}^n D_s$ for every $n \geqslant 0$, $s < q$.

Using Lemma 11, the *i*th entry of $\vec{v}^{qn+s}$ is

$$v_i^{qn+s} = \mathcal{N}(A_i, qn + s) = \sum_{t=0}^{q-1} \mathcal{N}(A_i^{s,t}, n) = \sum_{t=0}^{q-1} \mathcal{N}(\overline{A_i^{s,t}}, n).$$

Thus, by the definition of the numbers $(d_{i,j}^s)$ we obtain

$$v_i^{qn+s} = \sum_{r=0}^{m-1} d_{r,i}^s \cdot \mathcal{N}(A_r, n).$$

This sum is exactly the *i*th entry in the product $\vec{v}^n D_s$ and hence we have $\vec{v}^{qn+s} = \vec{v}^n D_s$.

Using induction on the length k of the expansion $n = \sum_{r=0}^{k-1} n_r q^r$, we conclude that $\vec{v}^n = \vec{v}^0 D_{n_{k-1}} \ldots D_{n_1} D_{n_0}$. In particular,

$$\mathcal{N}(A_i, n) = v_i^n = \vec{v}^n \vec{e}_i = \vec{v}^T D_{n_{k-1}} \ldots D_{n_1} D_{n_0} \vec{e}_i. \qquad \square$$

Proof of Theorem 2. Let $n \geqslant 0$ and assume that $n = \sum_{r=0}^{k-1} n_r q^r$ where $k > 0$ and $0 \leqslant n_i < q$ for $i \leqslant k-1$ (if $n = 0$ then $n_i = 0$ for each i). Define

$$N(n) = D_{n_{k-1}} \ldots D_{n_0},$$

$$F(n) = \sum \left\{ D_{m_{k-1}} \ldots D_{m_0} \,\middle|\, \sum_{r=0}^{k-1} m_r q^r < \sum_{r=0}^{k-1} n_r q^r \right\}.$$

It can be easily observed that for any $n' > 0$ and $n'' \in \{0, \ldots, q-1\}$ we have

$$F(qn' + n'') = F(n') \cdot E_{q-1} + N(n') \cdot E_{n''-1}. \tag{4}$$

Repeatedly using (4) (and noting that $F(n_{k-1}) = E_{n_{k-1}-1}$) we have

$$\begin{aligned} F(n) &= F\left(\sum_{r=0}^{k-1} n_r q^r\right) = F\left(\sum_{r=0}^{k-2} n_{r+1} q^r\right) \cdot E_{q-1} + D_{n_{k-1}} \ldots D_{n_1} E_{n_0-1} \\ &= \cdots = E_{n_{k-1}-1} E_{q-1}^{k-1} + D_{n_{k-1}} E_{n_{k-2}-1} E_{q-1}^{k-2} + \cdots + D_{n_{k-1}} \ldots D_{n_1} E_{n_0-1}. \end{aligned}$$

The formula for $\mathcal{F}(A_i, n)$ is obtained from the last equation, observing that $\mathcal{F}(A_i, n) = \vec{v}^T F(n) \vec{e}_i$.

Take $n = q^j$. Since $E_{-1} = 0$, there is only one nonzero summand in Eq. (2). Thus,

$$\mathcal{F}(A_i, q^j) = \vec{v}^T E_0 E_{q-1}^j \vec{e}_i = \vec{v}^T D_0 E_{q-1}^j \vec{e}_i.$$

Theorem 1 implies that $\vec{v}^T D_0 N(n') \vec{e}_i = \vec{v}^T N(n') \vec{e}_i$ for every n'. Hence, $\mathcal{F}(A_i, q^j) = \vec{v}^T E_{q-1}^j \vec{e}_i$. $\square$

Proof of Theorem 4. (5) $\Rightarrow$ (4): the proof is similar to the proof that (1)$\Rightarrow$(2) in [21, Theorem 10]. (Observing that the opposite of property (4) is that the limit converges to 0.)

(4) $\Rightarrow$ (3): exactly as in [21, Theorem 4], we obtain that there exists a set $I \subseteq \{0, \ldots, m-1\}$ such that the sum of entries in each column of the matrix $((E_{q-1})_{i,j})_{i,j \in I}$ is q^2. Since the sum of entries in any column of the matrices $D_0, \ldots, D_{q-1}$ is at most q, this set I satisfies the required property.

(3) $\Rightarrow$ (2): let $\vec{w} = (w_i)_{i=0}^{m-1}$ where, $w_i = 1$ if $i \in I$ and $w_i = 0$ otherwise. Then $\vec{w}^T$ is a common eigenvector as required.

(2) $\Rightarrow$ (1): denote the common eigenvector by $\vec{w}^T$. Then $\vec{w}^T D_{n_{k-1}} \ldots D_{n_0} = q^k \vec{w}^T$ for any $n_0, \ldots, n_{k-1} \in \{0, \ldots, q-1\}$, and thus $\|D_{n_{k-1}} \ldots D_{n_0}\| \geqslant q^k$, which implies that $\lambda \geqslant \ln q$.

(1) $\Rightarrow$ (5): since $\lambda = \ln q$, we obtain that for every $\mu < q$,

$$\lim_{k \to \infty} \frac{\#((n_{k-1}, \ldots, n_0) \in \{0, \ldots, q-1\}^k \; : \; \|D_{n_{k-1}} \ldots D_{n_0}\| \geqslant \mu^k)}{q^k} = 1.$$

Noting that

$$E_{q-1}^{k}=\sum\{D_{n_{k-1}}\ldots D_{n_0}\mid 0\leqslant n_0,n_1,\ldots,n_{k-1}<q\},$$

we conclude that $\|E_{q-1}^{k}\|=\Omega(q^k\cdot\mu^k)$. On the other hand, using the Jordan form of E_{q-1}, we have $\|E_{q-1}^{k}\|=\mathrm{O}(k^{m-1}\cdot R^k)$. Thus we must have $R\geqslant q\cdot\mu$, and since $\mu<q$ has been chosen arbitrarily, we have $R\geqslant q^2$. Observing that the sum of entries in any column of E_{q-1} is at most q^2, we conclude that $R\leqslant q^2$. Thus, $R=q^2$. □

Proof of Theorem 10. Let A denote the DLR corresponding to Pascal's triangle modulo p. It can be observed that in this case $X'=\{aA\mid 0<a<p\}$. Enumerate the elements of X' by $X'=\{A_0,\ldots,A_{p-2}\}$ where $A_i=g^iA$. One can easily observe that $A_j^{s,t}=A_i$ if and only if $A_{j+1}^{s,t}=A_{i+1}$, where the indices are taken modulo $p-1$, and thus $d_{i,j}^s=d_{i+1,j+1}^s$. Moreover, using the definition of D_s, we conclude that $d_{i,0}^s=N(s,g^i,p)$. Those two facts imply that $D_s=\sum_{i=0}^{p-2}N(s,g^i,p)C^i$, where $C=(C_{i,j})_{i,j=0}^{p-2}$ is the permutation matrix given by

$$C_{i,j}=\begin{cases}1 & i\equiv j+1\ (\mathrm{mod}\ p-1),\\ 0 & \text{otherwise.}\end{cases}$$

In other words, $D_s=R_s(C)$ for each $s<p$.

By Theorem 1, we have

$$N(n,g^i,p)=\mathcal{N}_{g^i}(A_0,n)=\vec{e}_i^{\,T}R_{n_{k-1}}(C)\ldots R_{n_1}(C)R_{n_0}(C)\vec{e}_0=\vec{e}_i^{\,T}P(C)\vec{e}_0.$$

Note that the definition of $R_n(x)$ implies that $\vec{e}_i^{\,T}R_n(C)\vec{e}_0=N(n,g^i,p)$ as well, and thus we must have $P(C)=R_n(C)$. Since the minimal polynomial of the matrix C is $x^{p-1}-1$, we obtain

$$P(x)\equiv R_n(x)\quad(\mathrm{mod}\ x^{p-1}-1).$$

Observing that $\mathrm{Deg}(R_n(x))<p-1$, we conclude that $R_n(x)$ is the remainder of $P(x)$ upon division by $x^{p-1}-1$. □

Acknowledgements

The manuscript was completed during the author's postdoctoral fellowship at the Erwin Schrödinger Institute, Vienna, supported by the FWF Project P16004-N05. The author is very thankful to Daniel Berend for introduction to the subject and valuable discussions, to Avinoam Braverman for a significant contribution in the proof of Theorem 1 and to Yuval Peres, Jean-Paul Allouche and the anonymous referees for their very useful suggestions and comments on the paper.

References

[1] J.-P. Allouche, V. Berthé, Triangle de Pascal, complexité et automates, Bull. Belg. Math. Soc. 4 (1997) 1–23.

[2] J.-P. Allouche, F.v. Haeseler, H.-O. Peitgen, A. Petersen, G. Skordev, Automaticity of double sequences generated by one-dimensional linear cellular automata, Theoret. Comput. Sci. 188 (1997) 195–209.

[3] J.-P. Allouche, J. Shallit, Automatic Sequences: Theory, Applications, Generalizations, Cambridge University Press, Cambridge, 2003.

[4] L. Arnold, V. Wihstutz, Lyapunov exponents: a survey, Lyapunov exponents (Bremen, 1984), pp. 1–26, Lecture Notes in Mathematics, vol. 1186, Springer, Berlin, 1986.

[5] D. Barbolosi, P.J. Grabner, Distribution des coefficients multinomiaux et q-binomiaux modulo p, Indag. Math. (N.S.) 7 (1996) 129–135.

[6] D. Berend, J.E. Harmse, On some arithmetical properties of middle binomial coefficients, Acta Arith. 84 (1998) 31–41.

[7] P. Bougerol, J. Lacroix, Products of Random Matrices with Applications to Schrödinger Operators, Birkhäuser, Boston, 1985.

[8] K.S. Davis, W.A. Webb, Pascal's triangle modulo 4, Fibonacci Quart. 29 (1991) 79–83.

[9] N.J. Fine, Binomial coefficients modulo a prime, Amer. Math. Monthly 54 (1947) 589–592.

[10] H. Furstenberg, H. Kesten, Products of random matrices, Ann. Math. Statist. 31 (1960) 457–469.

[11] R. Garfield, H.S. Wilf, The distribution of the binomial coefficients modulo p, J. Number Theory 41 (1992) 1–5.

[12] J.W.L. Glaisher, On the residue of a binomial-theorem coefficient with respect to a prime modulus, Quart. J. Math. 30 (1899) 150–156.

[13] J. Goldwasser, W. Klostermeyer, M. Mays, G. Trapp, The density of ones in Pascal's rhombus, Discrete Math. 204 (1999) 231–236.

[14] A. Granville, Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers. Organic mathematics (Burnaby, BC, 1995) pp. 253–276, CMS Conference Proceedings, 20, American Mathematical Society, Providence, RI, 1997.

[15] E. Hexel, H. Sachs, Counting residues modulo a prime in Pascal's triangle, Indian J. Math. 20 (1978) 91–105.

[16] J.G. Huard, B.K. Spearman, K.S. Williams, Pascal's triangle $(\bmod 9)$, Acta Arith. 78 (1997) 331–349.

[17] J.G. Huard, B.K. Spearman, K.S. Williams, Pascal's triangle (mod 8), European J. Combin. 19 (1998) 45–62.

[18] R. Kenyon, Y. Peres, Intersecting random translates of invariant Cantor sets, Invent. Math. 104 (1991) 601–629.

[19] N. Kriger, Arithmetical properties of some sequences of binomial coefficients, M. Sc. Thesis, Ben-Gurion University, 2001.

[20] R. Lima, M. Rahibe, Exact Lyapunov exponent for infinite products of random matrices, J. Phys. A: Math. Gen. 27 (1994) 3427–3437.

[21] Y. Moshe, The density of 0's in recurrence double sequences, J. Number Theory 103 (2003) 109–121.

[22] A.H. Stein, Binomial coefficients not divisible by a prime, Number Theory (New York, 1985/1988), pp. 170–177, Lecture Notes in Mathematics, vol. 1383, Springer, Berlin, 1989.