Discrete Mathematics 214 (2000) 21–49

DISCRETE MATHEMATICS

Schur congruences, Carlitz sequences of polynomials and automaticity

J.-P. Allouche[a,*], G. Skordev[b]

[a] *CNRS, Lab de Recherche en Informatique, Université Paris-Sud, Centre d'Orsay, UMR 8623, Bâtiment 490, F-91405 Orsay, Cedex, France*

[b] *CEVIS, Universität Bremen, Universitätsallee 29, D-28359 Bremen, Germany*

Received 4 June 1997; revised 10 June 1998; accepted 26 April 1999

Abstract

We first generalize the Schur congruence for Legendre polynomials to sequences of polynomials that we call 'd-Carlitz'. This notion is more general than a similar notion introduced by Carlitz. Then, we study automaticity properties of double sequences generated by these sequences of polynomials, thus generalizing previous results on the double sequences produced by one-dimensional linear cellular automata. © 2000 Elsevier Science B.V. All rights reserved.

Keywords: Schur congruence; Legendre and classical polynomials; Automatic sequences

1. Introduction

The classical Schur congruence for Legendre polynomials modulo an odd prime p (see [38]) reads: for all $n \geqslant 0$ and all $v \in [0, p-1]$,

$$P_{pn+v} \equiv P_n(X^p)P_v(X) \bmod p.$$

This property is similar to the well-known theorem of Lucas for the binomial coefficients modulo a prime number. We recall Lucas property: for p prime, u and v in $[0, p-1]$, and any integers $m, n \geqslant 0$,

$$\binom{pm+u}{pn+v} \equiv \binom{m}{n}\binom{u}{v} \bmod p.$$

This property can also be written as

$$(1+X)^{pn+v} \equiv (1+X^p)^n(1+X)^v \bmod p.$$

A similar congruence holds for the sequence of powers of a given polynomial modulo p. For the case $v=0$ it was called the p-Fermat property in [5,4], and was one of the

---

* Corresponding author.

E-mail addresses: allouche@lri.fr (J.-P. Allouche), skordev@cevis.uni-bremen.de (G. Skordev)

PII: S0012-365X(99)00195-8

tools we used to study automaticity properties of two-dimensional sequences generated by one-dimensional linear cellular automata.

This congruence property has been generalized by Carlitz [10], and the definition we give below of what we call 'd-Carlitz sequences of polynomials' is a generalization of his notion. (The definition of Carlitz essentially corresponds to what we call 'simple d-Carlitz sequences of polynomials'.) If, for all prime numbers p, a sequence of polynomials is p-Carlitz when reduced modulo p, then, the coefficients of these polynomials form a double sequence, that has under some conditions the Lucas property: one or two-dimensional sequences having the Lucas property have been introduced by McIntosh [29]. The simplest example is precisely given by the sequence of binomial coefficients $(\binom{m}{n})_{m,n\geqslant 0}$.

In what follows we investigate more closely the notion of d-Carlitz sequences of polynomials. In particular we study classical polynomials such as Legendre, Gegenbauer, Jacobi, Chebishev, Hermite, and modified Laguerre polynomials. We recall known results for *simple* d-Carlitz sequences of polynomials. We also prove results for the more general notion of d-Carlitz sequences of polynomials.

We furthermore address the question whether the double sequence generated by a d-Carlitz sequence of polynomials is automatic, i.e., is generated by a finite automaton. (For definitions and properties of automatic sequences, see [15,11,12,36,37].) Our tools are a 'slice lemma' (generalizing the one we gave in [4]), and Cobham's theorem [13] on sequences that are both a and b-automatic. Our results are related to, but different from those in [27,5,4]. In particular, a sequence of polynomials $(P_n(X))_{n\geqslant 0}$ that has the p-Carlitz property can be seen as a generalization of the time evolution of a one-dimensional linear cellular automaton over $\mathbb{Z}/p\mathbb{Z}$: this case namely corresponds to $P_n(X) = R^n(X)$ for some fixed polynomial $R(X)$.

Are these notions closely related to combinatorial properties of orthogonal polynomials, or to the hypergeometric function? We think the answer to this question is no, and we give other sequences of polynomials (Meixner, Charlier, continuous dual Hahn) that are not simple d-Carlitz sequences of polynomials, although they have a combinatorial background and are related to the hypergeometric function. For these sequences of polynomials we also give automaticity and non-automaticity results.

Note that some of our results have been announced in the survey [3].

2. d-Carlitz sequences of polynomials: definition and first properties

We give here a definition, the second part of which is essentially the definition given by Carlitz in [9]. Our definition is thus a generalization of Carlitz. We then make some observations on the properties of these sequences of polynomials. Most are straightforward. We also state a proposition (Proposition 2.2) that will prove useful in what follows.

Definition 2.1. Let R be a finite commutative ring with unit. Let d be an integer $\geqslant 2$. A sequence of polynomials $(P_n(X))_{n\geqslant 0}$ with coefficients in R is called a *d-Carlitz sequence of polynomials* if there exists a finite set of sequences of polynomials $\{(P_n^{(k)}(X))_{n\geqslant 0},\ 1\leqslant k\leqslant r\}$ such that

* the sequence $(P_n^{(1)}(X))_{n\geqslant 0}$ is equal to the sequence $(P_n(X))_{n\geqslant 0}$,
* $\forall k \in [1,r]$, $\exists \ell = \ell(k) \in [1,r]$, $\forall (k,j) \in [1,r]\times[0,d-1]$, $\exists m = m(k,j) \in [1,r]$, such that

$$(\#) \quad \forall k \in [1,r],\ \forall n > 0,\ \forall j \in [0,d-1], \quad P_{dn+j}^{(k)}(X) = P_n^{(\ell(k))}(X^d)P_j^{(m(k,j))}(X).$$

If the number r above is equal to 1, i.e., if the sequence $(P_n(X))_{n\geqslant 0}$ satisfies

$$\forall n > 0,\ \forall j \in [0,d-1], \quad P_{dn+j}(X) = P_n(X^d)P_j(X),$$

then, the sequence $(P_n(X))_{n\geqslant 0}$ is called a *simple d-Carlitz sequence of polynomials.*

Observations. 1. Let $(P_n(X))_{n\geqslant 0}$ be a simple d-Carlitz sequence of polynomials. If $n = \sum_{j=0}^{s} n_j d^j$, with $0\leqslant n_j \leqslant d-1$ and $n_s \neq 0$, is the base-d expansion of the integer n, then

$$P_n(X) = \prod_{j=0}^{s} P_{n_j}(X^{d^j}).$$

In particular, this sequence is uniquely determined by the d polynomials $P_0(X),\ldots,P_{d-1}(X)$. Conversely, any d polynomials $P_0(X),\ldots,P_{d-1}(X)$ determine a unique simple d-Carlitz sequence of polynomials.

Note that, to avoid problems with possible leading zeroes in the base-d expansion of n, we only consider the shortest expansion of n. We could also have restricted ourselves to sequences of polynomials such that $P_0(X) = 1$. In this case the condition for simple d-Carlitz sequences reads: $\forall j \in [0,d-1]$, $\forall n\geqslant 0$, $P_{dn+j}(X) = P_n(X^d)P_j(X)$. For the general definition, the examples below furthermore satisfy: $P_0^{(k)}(X) = 1$ for each $k \in [1,r]$, and $m(k,j) = k$ for all (k,j). Hence, these polynomials satisfy Equality (#) with $n\geqslant 0$ instead of $n > 0$ (and k instead of $m(k,j)$).

If $(P_n(X))_{n\geqslant 0}$ is a d-Carlitz sequence of polynomials, then, there exists a sequence of positive integers $(m_k)_k \in [1,r]^{\mathbb{N}}$ such that, if $n = \sum_{j=0}^{s} n_j d^j$, with $0\leqslant n_j\leqslant d-1$ and $n_s \neq 0$, then

$$P_n(X) = \prod_{j=0}^{s} P_{n_j}^{(m_j)}(X^{d^j}).$$

2. We recall that a polynomial $P(X)$ is called d-Fermat if $P(X^d) = P(X)^d$, (see [5]). Then, it is easy to check that *the sequence* $(P(X)^n)_{n\geqslant 0}$ *is a simple d-Carlitz sequence of polynomials if and only if the polynomial* $P(X)$ *is d-Fermat*. In particular, if $q = p^a$ is a nonzero power of a prime number, and if $R = \mathbb{F}_q$, the Galois field with q elements, then, for any polynomial $P(X) \in \mathbb{F}_q[X]$, the sequence $(P(X)^n)_{n\geqslant 0}$ is a simple q-Carlitz sequence of polynomials. Note that, for any ring R, and any polynomial $P \in R[X]$, the

sequence $(P(X)^n)_{n\geqslant 0}$ is the orbit of a linear cellular automaton with initial condition equal to 1, see [5,4] and the references quoted there. We also say that a sequence of polynomials $(P_n(X))_{n\geqslant 0}$ is a *generalized d-Fermat sequence of polynomials* if $\forall n > 0$, $P_{nd}(X)=P_n(X^d)$. Of course a simple d-Carlitz sequence of polynomials is a generalized d-Fermat sequence of polynomials. Note that this notion resembles (but is different from) the notion of *Honda sequence of polynomials*: a sequence $(H_n(X))_{n\geqslant 0}$ of p-adic polynomials, i.e., of polynomials with coefficients in $\mathbb{Z}_p$, is called a Honda sequence (see [6,43] for example) if for all $n\geqslant 0$, $H_{np}(X) \equiv H_n(X^p) \bmod np\mathbb{Z}_p[X]$. (For related works see [19,32–34,40–42].)

3. We recall that a sequence $(u_n)_{n\geqslant 0}$ of elements in a ring R is called strongly d-multiplicative (see for example [30]) if

$$\forall n\geqslant 0,\ \forall j \in [0, d-1], \quad u_{dn+j} = u_n u_j.$$

It is easy to see that *if a sequence of polynomials* $(P_n(X))_{n\geqslant 0}$ *is a simple d-Carlitz sequence of polynomials, such that* $P_0(X) = 1$, *then, the sequences* $(P_n(0))_{n\geqslant 0}$ *and* $(P_n(1))_{n\geqslant 0}$ *(in* $R^{\mathbb{N}}$*) are strongly d-multiplicative.*

4. If $(P_n(X))_{n\geqslant 0}$ is a d-Carlitz sequence of polynomials, then, there exists a constant $C > 0$ such that, for every n, the inequality $\deg P_n(X) \leqslant Cn$ holds.

Define indeed

$$C' = \max_{1\leqslant k\leqslant r}\ \max_{0\leqslant i\leqslant d-1}\ \deg P_i^{(k)}(X).$$

If $n = \sum_{j=0}^{s} n_j d^j$, with $0\leqslant n_j \leqslant d-1$ and $n_s \neq 0$, then, from Observation 1 above,

$$\deg P_n(X) \leqslant C' \sum_{j=0}^{s} d^j = C' \frac{d^{s+1}-1}{d-1} \leqslant C' d^{s+1} \leqslant C' dn = Cn,$$

where $C = C'd$.

5. A (simple) d-Carlitz sequence of polynomials is also a (simple) d^k-Carlitz sequence of polynomials, for every $k \geqslant 1$.

6. If $(P_n(X))_{n\geqslant 0}$ and $(Q_n(X))_{n\geqslant 0}$ are two simple d-Carlitz sequences of polynomials, their product $(P_n(X)Q_n(X))_{n\geqslant 0}$ is also a simple d-Carlitz sequence of polynomials.

7. The notion of (simple) d-Carlitz sequence of polynomials can be easily extended to polynomials in several variables. A straightforward property reads: if $(P_n(X))_{n\geqslant 0}$ and $(Q_n(Y))_{n\geqslant 0}$ are two (simple) d-Carlitz sequences of polynomials, then, the product $(P_n(X)Q_n(Y))_{n\geqslant 0}$ is a (simple) d-Carlitz sequence of polynomials of two variables.

8. Let $(P_n(X))_{n\geqslant 0}$ be a (simple) d-Carlitz sequence of polynomials with coefficients in a commutative ring R with a 1. Let $r(X) \in R[X]$ be a polynomial with the d-Fermat property. Then, the sequence of polynomials $(Q_n(X))_{n\geqslant 0}$ defined by

$$\forall n\geqslant 0, \quad Q_n(X) = P_n(r(X))$$

is a (simple) d-Carlitz sequence of polynomials.

9. Several generalizations of the notion of d-Carlitz sequences of polynomials are possible. We restrict ourselves to generalizations of simple d-Carlitz sequences of polynomials. Let R_1 be a (D,d)-semiring in the sense of Allouche et al. [2], let R_2 be a

commutative ring with 1, and let $\alpha : R_2 \to R_2$ be a homomorphism. A map $f : R_1 \to R_2$ is called a $((D,d),\alpha)$-Carlitz map if, for all $u \in D$ and all $r \in R_1 \backslash \{0\}$,

$$f(rd+u) = \alpha(f(r))f(u).$$

Then, for $r = r_s d^s + \cdots + r_1 d + r_0$, $r_j \in D$ for $j = 0,1,\ldots,s$, and $r_s \neq 0$,

$$f(r) = \alpha^s(f(r_s))\ldots\alpha(f(r_1))f(r_0).$$

Here are some examples.

(a) Let $R_1 = \mathbb{N}$, $d \in \mathbb{N}$, $d \geqslant 2$, $D = \{0,1,\ldots,d-1\}$, and let α be the identity map. A sequence $(u_n)_{n\geqslant 0} \in R_2^{\mathbb{N}}$ is strongly d-multiplicative if and only if the map $f : \mathbb{N} \to R_2$ defined by $f(n) = u_n$ is a $((D,d),\alpha)$-Carlitz map.
(b) Let $R_1 = \mathbb{N}$, $d \in \mathbb{N}$, $d \geqslant 2$, and $D = \{0,1,\ldots,d-1\}$. Let R be a finite commutative ring with 1, let $R_2 = R[X]$, let $\alpha : R_2 \to R_2$ be defined by $\alpha(r(X)) = r(X^d)$, for every $r(X) \in R_2$. Let $(r_n(X))_{n\geqslant 0}$ be a sequence of elements in R_2. Define the function $f : \mathbb{N} \to R[X]$ by $f(n) = r_n(X)$. Then, the sequence $(r_n(X))_{n\geqslant 0}$ is a simple d-Carlitz sequence of polynomials if and only if the map f is a $((D,d),\alpha)$-Carlitz map.
(c) Take $R_1 = \mathbb{N} \times \mathbb{N}$, $d \in \mathbb{N}$, $d \geqslant 2$, $D = \{0,1,\ldots,d-1\}$, $\underline{D} = D \times D$, and $\underline{d} = (d,d)$. Then, R_1 is a $(\underline{D},\underline{d})$-ring. Let R be a finite commutative ring with 1, let $R_2 = R[X]$, let $\alpha : R_2 \to R_2$ be defined by $\alpha(r(X)) = r(X^d)$, for every $r(X) \in R_2$. Then, a sequence $(r_{m,n}(X))_{m,n\geqslant 0})$ of polynomials in R_2 is a simple d-Carlitz sequence of polynomials if and only if the map $f : \mathbb{N} \times \mathbb{N} \to R_2$, defined by $f(m,n) = r_{m,n}(X)$, is a $((\underline{D},\underline{d}),\alpha)$-Carlitz map, i.e., for all $u,v \in D$, for all $m,n \in \mathbb{N}$

$$r_{md+u,nd+v}(X) = r_{m,n}(X^d)r_{u,v}(X).$$

(d) In b and c above, one can replace $R[X]$ by $R[[X]]$, or by $R[X_1,\ldots,X_t]$, or by $R[[X_1,\ldots,X_t]]$.
(e) If R_2 has characteristic p, a natural notion is the notion of $((D,p),\alpha)$-Carlitz map, where $\alpha : R_2 \to R_2$ is given by $\alpha(a) = a^p$, for every a in R_2.

We end this section with a proposition giving a characterization of the simple d-Carlitz sequences of polynomials.

Proposition 2.2. *Let d be an integer $\geqslant 2$ Let $(P_n(X))_{n\geqslant 0}$ be a sequence of polynomials over the ring R, such that $P_0(X) = 1$. Define the generating function $F(X,Y) \in R[[X,Y]]$ by*

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

Then, the sequence $(P_n(X))_{n\geqslant 0}$ is a simple d-Carlitz sequence of polynomials if and only if there exists a polynomial $A(X,Y)$ in $R[X,Y]$, such that $\deg_Y A(X,Y) \leqslant d-1$ and $F(X,Y) = A(X,Y)F(X^d,Y^d)$.

Proof. If $(P_n(X))_{n\geqslant 0}$ is a simple d-Carlitz sequence of polynomials, then

$$\begin{aligned}
F(X,Y) &= \sum_{n\geqslant 0} P_n(X)Y^n \\
&= \sum_{j=0}^{d-1}\sum_{n\geqslant 0} P_{dn+j}(X)Y^{dn+j} \\
&= \sum_{j=0}^{d-1}\sum_{n\geqslant 1} P_{dn+j}(X)Y^{dn+j} + \sum_{j=0}^{d-1} P_j(X)Y^j \\
&= \sum_{j=0}^{d-1} Y^j \sum_{n\geqslant 1} P_n(X^d)P_j(X)Y^{dn} + \sum_{j=0}^{d-1} P_j(X)Y^j \\
&= \left(\sum_{j=0}^{d-1} P_j(X)Y^j\right) F(X^d, Y^d).
\end{aligned}$$

Hence, defining $A(X,Y) = \sum_{j=0}^{d-1} P_j(X)Y^j$, we have $F(X,Y) = A(X,Y)F(X^d, Y^d)$.

Suppose now that

$$F(X,Y) = A(X,Y)F(X^d, Y^d),$$

where $A(X,Y)$ is a polynomial in X and Y with partial degree in Y smaller than or equal to $d-1$. Then, there exist d polynomials $A_0(X), A_2(X), \ldots, A_{d-1}(X)$ such that

$$A(X,Y) = \sum_{j=0}^{d-1} A_j(X)Y^j.$$

Hence we have

$$\begin{aligned}
\sum_{n\geqslant 0} P_n(X)Y^n &= \left(\sum_{j=0}^{d-1} A_j(X)Y^j\right)\left(\sum_{n\geqslant 0} P_n(X^d)Y^{dn}\right) \\
&= \sum_{j=0}^{d-1}\sum_{n\geqslant 0} A_j(X)P_n(X^d)Y^{dn+j}.
\end{aligned}$$

But

$$\sum_{n\geqslant 0} P_n(X)Y^n = \sum_{j=0}^{d-1}\sum_{n\geqslant 0} P_{dn+j}(X)Y^{dn+j}.$$

Hence, comparing the coefficients of Y^j for $j\in[0,d-1]$, we obtain

$$\forall j\in[0,d-1],\quad P_j(X) = A_j(X).$$

Then, comparing the coefficients of Y^{dn+j}, we have, for every $n>0$ and every $j\in[0,d-1]$,

$$P_{dn+j}(X) = A_j(X)P_n(X^d).$$

Hence, we finally have

$$\forall n > 0, \ \forall j \in [0, d-1], \quad P_{dn+j}(X) = P_j(X)P_n(X^d)$$

and the sequence $(P_n(X))_{n\geqslant 0}$ is a simple d-Carlitz sequence of polynomials. □

Remark 2.3. A similar assertion holds if we replace $R[X]$ by $R[[X]]$ both for $P_n(X)$ and for the $A_j(X)$'s. The sequence $(P_n(X))_{n\geqslant 0}$ (with $P_0(X)=1$) is a simple d-Carlitz sequence of power series if and only if its generating function $F(X,Y)$ satisfies the equation above.

3. Simple p-Carlitz sequences of polynomials and sequences having the Lucas property

In [29] McIntosh studies sequences that behave like the binomial coefficients modulo prime numbers: a double sequence $(a(m,n))_{m,n\geqslant 0}$ with values in $\mathbb{Z}$ is said to have the (double) Lucas property if $a(m,n)=0$ for $m > n$, if $a(0,0)=1$, and if, *for each prime p*,

$$a(m,n) \equiv \prod_{i=0}^{\max(s,t)} a(m_i, n_i) \bmod p,$$

where $m = \sum_{i=0}^{s} m_i p^i$, with $0 \leqslant m_i \leqslant p-1$ and $m_s \neq 0$, and $n = \sum_{i=0}^{t} n_i p^i$, with $0 \leqslant n_i \leqslant p-1$ and $n_t \neq 0$. As usual $a(0,0)=1$, since this is an empty product.

With a sequence $(a(m,n))_{m,n\geqslant 0}$ such that, for any fixed n, we have $a(m,n)=0$ if m is large enough, we associate a sequence of polynomials $(P_n(X))_{n\geqslant 0}$ defined by

$$P_n(X) = \sum_{m\geqslant 0} a(m,n)X^m.$$

We prove in this paragraph that, for every prime p, the reduction modulo p of a sequence of polynomials associated to a double sequence having the double Lucas property is a simple p-Carlitz sequence of polynomials.

Proposition 3.1. *Let $(P_n(X))_{n\geqslant 0}$ be a sequence of polynomials with coefficients in the ring R, such that $P_0(X)=1$. Define the double sequence $(a(m,n))_{m,n\geqslant 0}$ by*

$$P_n(X) = \sum_{m\geqslant 0} a(m,n)X^m$$

(this implies that $a(m,n)=0$ for $m \geqslant m_0(n)$). Then, the sequence $(P_n(X))_{n\geqslant 0}$ is a simple d-Carlitz sequence of polynomials if and only if

$$\forall m,n \geqslant 0, \ \forall i,j \in [0,d-1], \quad a(dm+i, dn+j) = \sum_{u+v=m} a(u,n)a(dv+i, j).$$

In particular, if $\deg P_n(X) \leqslant n$, *i.e., if $a(m,n)=0$ for $m > n$, then, the sequence $(P_n(X))_{n\geqslant 0}$ is a simple d-Carlitz sequence of polynomials if and only if*

$$\forall m,n \geqslant 0, \ \forall i,j \in [0,d-1], \quad a(dm+i, dn+j) = a(m,n)a(i,j),$$

which implies, if $m=\sum_{i=0}^{s} m_i d^i$ *and* $n=\sum_{i=0}^{t} n_i d^i$, *with* $0 \leqslant m_i,\ n_i \leqslant d-1$ *and* $m_s n_t \neq 0$,

$$a(m,n)=\prod_{i=0}^{\max(s,t)} a(m_i,n_i).$$

Proof. By definition of the sequence $(a(m,n))_{m,n\geqslant 0}$,

$$P_n(X)=\sum_{m\geqslant 0} a(m,n)X^m.$$

Hence, for $j \in [0,d-1]$,

$$\begin{aligned} P_{dn+j}(X) &= \sum_{m\geqslant 0} a(m,dn+j)X^m \\ &= \sum_{i=0}^{d-1} X^i \sum_{m\geqslant 0} a(dm+i,dn+j)X^{dm}. \end{aligned}$$

But

$$\begin{aligned} P_n(X^d)P_j(X) &= \sum_{u\geqslant 0} a(u,n)X^{du} \sum_{k\geqslant 0} a(k,j)X^k \\ &= \sum_{u\geqslant 0} a(u,n)X^{du} \sum_{v\geqslant 0} \sum_{i=0}^{d-1} a(dv+i,j)X^{dv+i} \\ &= \sum_{i=0}^{d-1} X^i \sum_{u,v\geqslant 0} a(u,n)a(dv+i,j)X^{du+dv} \\ &= \sum_{i=0}^{d-1} X^i \sum_{m\geqslant 0} X^{dm} \sum_{u+v=m} a(u,n)a(dv+i,j). \end{aligned}$$

Hence, looking at the coefficient of X^{dm+i}, we obtain

$$\forall n\geqslant 0,\ \forall j \in [0,d-1], \quad P_{dn+j}(X)=P_n(X^d)P_j(X),$$

if and only if

$$\forall m,n\geqslant 0,\ \forall i,j \in [0,d-1], \quad a(dm+i,dn+j)=\sum_{u+v=m} a(u,n)a(dv+i,j)$$

which is the first claim in the proposition above.

Suppose now that $\deg P_n(X)\leqslant n$, i.e., that $a(m,n)=0$ for $m>n$. Then, if i and j belong to $[0,d-1]$, and if $v\geqslant 1$, then,

$$a(dv+i,j)=0.$$

Hence, the sum $\sum_{u+v=m} a(u,n)a(dv+i,j)$ above boils down to $a(m,n)a(i,j)$, and we are done.

Remark 3.2. McIntosh considered also double sequences $(a(m,n))_{m,n\geqslant 0}$ having the generalized Lucas property, by removing from the above definition the condition

$a(m,n)=0$ for $m > n$. For such sequences $A_n(X)=\sum_{m\geqslant 0} a(m,n)X^m$ is not a polynomial in general, and the sequence $(A_n(X) \bmod p)_{n\geqslant 0}$ does not have in general the p-Carlitz property as a sequence of power series. One example is the sequence

$$a(m,n) = \binom{n+m}{m}\binom{n+2m}{m}.$$

Other interesting examples are given in [29]. Note that our Proposition 2.2 can be used to prove Lucas lemma, and to prove that the orbit of 1 with respect to a one-dimensional linear cellular automaton given by a polynomial with integer coefficients and reduced modulo, the successive prime numbers has the double Lucas property. It can also be used to prove Theorems 3 and 4 (Reflection Principle) of McIntosh in [29].

4. Examples

In this paragraph we give examples of sequences of polynomials related to classical orthogonal polynomials and that have the Carlitz property. The essential tool will be Proposition 2.2. For an integer $m\geqslant 2$, we denote here by $\mathbb{Q}_{(m)}$ the set of rational numbers defined by

$$\mathbb{Q}_{(m)} = \left\{\frac{a}{b};\ a \in \mathbb{Z},\ b \in \mathbb{N}\backslash\{0\},\ \gcd(m,b) = 1\right\}$$

4.1. Legendre polynomials

The sequence of Legendre polynomials $\mathscr{P} = (P_n(X))_{n\geqslant 0}$ can be defined [17, p. 179] by the recurrence relations

$$P_0(X) = 1, \qquad P_1(X) = X,$$

$$\forall n\geqslant 1, \quad (n+1)P_{n+1}(X) = (2n+1)XP_n(X) - nP_{n-1}(X).$$

The sequence $(P_n(X))_{n\geqslant 0}$ can also be defined explicitly [17, p. 180] as

$$P_n(X) = \frac{1}{2^n}\sum_{v=0}^{\lfloor n/2\rfloor}(-1)^v\binom{n}{v}\binom{2n-2v}{n-2v}X^{n-2v}.$$

Each polynomial $P_n(X)$ belongs to $\mathbb{Q}_{(p)}(X)$ for any odd prime number p. The following, known as the Schur congruence (see [38,9]), holds: *the sequence* $(P_n(X) \bmod p)_{n\geqslant 0}$ *is a simple* p*-Carlitz sequence of polynomials over the ring* $\mathbb{Z}/p\mathbb{Z}$, for each odd prime number p.

We give here a quick proof of this result, using Proposition 2.2. The generating function $F(X,Y) = \sum_{n\geqslant 0} P_n(X)Y^n$ has the explicit expression (see [17, p. 182] for example)

$$F(X,Y) = \frac{1}{\sqrt{1-2XY+Y^2}}.$$

Hence

$$F(X,Y)^2 = \frac{1}{1-2XY+Y^2}.$$

This can be viewed as an equality between the formal power series or the rational functions over $\mathbb{Q}$, hence over $\mathbb{Q}_{(p)}$ for every odd prime number p. Let p be such an odd prime number, then, over $\mathbb{F}_p$

$$\frac{F(X,Y)}{F(X^p,Y^p)} = \frac{F(X,Y)}{F(X,Y)^p} = \frac{1}{F(X,Y)^{p-1}}$$
$$= \frac{1}{(F(X,Y)^2)^{(p-1)/2}} = (1-2XY+Y^2)^{(p-1)/2}.$$

We can now apply Proposition 2.2 with

$$A(X,Y) = (1-2XY+Y^2)^{(p-1)/2}.$$

Remark 4.1. (a) For other proofs of the above congruence the reader can look at the papers of Wahab, Brylinski and Landweber, [38,8,28]. The property of Legendre's polynomials is called the Schur congruence. Landweber [28] preceded his proof by noting that these congruences were mentioned in the Ph.D. Thesis of Ille [24], a student of I. Schur, and proved by Wahab [38]. Honda [23] and Yui [39] derived new congruences modulo p^k (p being an odd prime) for special indices of Legendre polynomials, that are close to generalizations of the p-Fermat property modulo p^k.

(b) McIntosh [29] proved that the double sequence

$$\left(\binom{n}{k}\binom{n+k}{k}\right)_{n,k\geqslant 0}$$

has the double p-Lucas property. This can also be proved by noting that

$$\sum_{k=0}^{n}\binom{n}{k}\binom{n+k}{k}X^k = P_n(2X+1)$$

where $P_n(X)$ is the nth Legendre polynomial, and using the Schur congruence for Legendre polynomials together with Observation 8 with $R=\mathbb{F}_p$.

4.2. Gegenbauer polynomials

The same reasoning as above implies the following assertion.

Theorem 4.2. *Let $a,b \in \mathbb{N}\backslash\{0\}$, with $a<b$, $\gcd(a,b)=1$. Let p be a prime number such that $b\,|\,p-1$. Let $Q(X,Y)\in\mathbb{Z}[X,Y]$, with $\deg_Y Q(X,Y)=d$. Suppose $Q(X,0)=1$ and $d\leqslant b/a$. Define a sequence of polynomials $(Q_n(X))_{n\geqslant 0}$ by*

$$\frac{1}{Q(X,Y)^{a/b}} = \sum_{n\geqslant 0} Q_n(X)Y^n.$$

Then, $(Q_n(X) \bmod p)_{n\geqslant 0}$ is a simple p-Carlitz sequence of polynomials.

Proof. It is not hard to see that the coefficients of $Q_n(X)$ are integers modulo p. (This can also be seen as a consequence of Heine's proof [22] of the Eisenstein theorem, announced by Eisenstein in [16].) This theorem is then a consequence of Proposition 2.2.

A special case is given by the Gegenbauer polynomials $(C_n^{\lambda}(X))_{n\geqslant 0}$ (see [17, p. 177]) defined by

$$(1-2XY+Y^2)^{-\lambda} = \sum_{n\geqslant 0} C_n^{\lambda}(X)Y^n.$$

Corollary 4.3. *For a, b, p satisfying the above conditions, $d=2$, and $\lambda = a/b$, the sequence of Gegenbauer polynomials $(C_n^{\lambda}(X))_{n\geqslant 0}$, reduced modulo p, is a simple p-Carlitz sequence of polynomials.*

Remark 4.4. For other congruence properties of Gegenbauer's polynomials, see [8].

4.3. Hermite polynomials

The sequence of Hermite polynomials $\mathscr{H} = (H_n(X))_{n\geqslant 0}$ can be defined [17, p. 193] by the recurrence relations

$$H_0(X) = 1, \qquad H_1(X) = 2X,$$

$$\forall n\geqslant 1, \quad H_{n+1}(X) = 2XH_n(X) - 2nH_{n-1}(X).$$

Then (see [17, p. 193])

$$H_n(X) = n! \sum_{k=0}^{\lfloor n/2 \rfloor} \frac{(-1)^k (2X)^{n-2k}}{k!(n-2k)!}.$$

Carlitz proved [9, Theorem 2] that, for every $j\geqslant 0$ and every $d\geqslant 2$,

$$H_{d+j}(X) \equiv (2X)^d H_j(X) \bmod d.$$

Hence, for every $j\geqslant 0$, every $d\geqslant 2$, and every $n\geqslant 0$,

$$(*)\ H_{dn+j}(X) \equiv (2X)^{nd} H_j(X) \bmod d.$$

Defining d sequences of polynomials $(Q_n^{(k)}(X))_{n\geqslant 0}$, for $k \in [0, d-1]$, by

$$Q_n^{(k)}(X) \equiv (kX)^n \bmod d,$$

Equality $(*)$ can be rewritten as

$$H_{dn+j}(X) \equiv Q_n^{(2^d \bmod d)}(X^d) H_j(X) \bmod d.$$

Furthermore, for all $n\geqslant 0$ and $j \in [0, d-1]$,

$$Q_{dn+j}^{(k)}(X) \equiv Q_n^{(k^d \bmod d)}(X^d) Q_j^{(k)}(X) \bmod d.$$

Hence we have the following result.

Theorem 4.5. *The sequence of Hermite polynomials $(H_n(X))_{n\geqslant 0}$, reduced modulo d, is a d-Carlitz sequence of polynomials* (*and the number r in the definition can be taken equal to $d+1$*).

4.4. Modified Laguerre polynomials

The sequence of Laguerre polynomials $\mathscr{L}^{(\alpha)} = (L_n^{(\alpha)}(X))_{n\geqslant 0}$ can be defined [17, p. 189] by the recurrence relations

$$L_0^{(\alpha)}(X) = 1, \qquad L_1^{(\alpha)}(X) = -X + \alpha + 1,$$

$$\forall n \geqslant 1, \quad (n+1)L_{n+1}^{(\alpha)}(X) = (-X + 2n + \alpha + 1)L_n^{(\alpha)}(X) - (n+\alpha)L_{n-1}^{(\alpha)}(X).$$

Then (see [17, p. 188])

$$L_n^{(\alpha)}(X) = \sum_{k=0}^{n} \binom{n+\alpha}{n-k} \frac{(-X)^k}{k!}.$$

Following Carlitz [9], define

$$\Lambda_n^{(\alpha)}(X) = n! L_n^{(\alpha)}(X).$$

Then

$$\Lambda_n^{(\alpha)}(X) = n! \sum_{k=0}^{n} \binom{n+\alpha}{n-k} \frac{(-X)^k}{k!}.$$

We will assume that α is an integer $\bmod m$. Then, the coefficients of $\Lambda_n^{(\alpha)}(X)$ are integers $\bmod m$.

Carlitz proved [9, Theorem 3] that, for every integer $d \geqslant 2$ and every $j \geqslant 0$,

$$\Lambda_{d+j}^{(\alpha)}(X) \equiv (-X)^d \Lambda_j^{(\alpha)}(X) \bmod d.$$

This implies, for $d \geqslant 2$, $n \geqslant 0$, and $j \in [0, d-1]$,

$$\Lambda_{dn+j}^{(\alpha)}(X) \equiv (-X)^{dn} \Lambda_j^{(\alpha)}(X) \bmod d.$$

Hence, if we mimic the proof given for the Hermite polynomials, we obtain the following result.

Theorem 4.6. *The sequence of modified Laguerre polynomials* $(\Lambda_n^{(\alpha)}(X))_{n\geqslant 0}$, *reduced modulo d, is a d-Carlitz sequence of polynomials* (*and the number r in the definition can be taken equal to* 3).

4.5. A property of $J_0(X)$

Carlitz defined in [10] a sequence of polynomials $(\omega_n(X))_{n\geqslant 0}$ obtained from the Bessel function $J_0(X)$ (see for example [17, p. 6]) by

$$\frac{J_0(2\sqrt{XZ})}{J_0(2\sqrt{Z})} = \sum_{n\geqslant 0} \frac{\omega_n(X) Z^n}{(n!)^2}.$$

Carlitz then proved that, for any prime number p, the sequence $(\omega_n(X) \bmod p)_{n\geqslant 0}$ is a simple p-Carlitz sequence of polynomials. He also noted that the sequence $(\omega_n \bmod p)_{n\geqslant 0}$, where $\omega_n = \omega_n(0)$, is strongly p-multiplicative (see also Observation 3 above).

5. Examples of sequences of orthogonal polynomials that are not simple p-Carlitz

We gave above examples of sequences having the d-Carlitz property, that come from polynomials with a combinatorial background. One of the referees, after reading a previous version of this paper, asked whether a general combinatorial property could be hidden behind these results. We think the answer is no, and will give in this section examples of sequences of polynomials from the Askey scheme of hypergeometric orthogonal polynomials that are not simple p-Carlitz sequences, for any prime p.

5.1. Chebishev polynomials

The sequences of Chebishev polynomials of the first kind $\mathscr{T}=(T_n(X))_{n\geqslant 0}$ and of the second kind $\mathscr{U}=(U_n(X))_{n\geqslant 0}$ satisfy the recurrence equation

$$\forall n\geqslant 1, \quad F_{n+1}(X)=2XF_n(X)-F_{n-1}(X)$$

with the initial conditions $T_0(X)=1$, $T_1(X)=X$, and $U_0(X)=1$, $U_1(X)=2X$ (see for example [17, p. 185]). Hence, they have the generating functions

$$\mathscr{T}(X,Y)=\sum_{n=0}^{\infty} T_n(X)Y^n=\frac{1-XY}{1-2XY+Y^2},$$

$$\mathscr{U}(X,Y)=\sum_{n=0}^{\infty} U_n(X)Y^n=\frac{1}{1-2XY+Y^2}.$$

If p is a prime number, it is clear that neither $(\mathscr{T}(X,Y)/\mathscr{T}(X^p,Y^p) \bmod p)$ nor $(\mathscr{U}(X,Y)/\mathscr{U}(X^p,Y^p) \bmod p)$ are polynomials of degree in Y at most $p-1$ (take $X=0$). Hence, using Proposition 2.2, we see that the sequences of Chebishev polynomials of the first and of the second kind reduced modulo p are not simple p-Carlitz sequences of polynomials (for any prime p). Note nevertheless that, the sequence of Chebishev polynomials of the first kind modulo any odd prime number p has the generalized p-Fermat property: this last result is due to Askey (quoted in [8]).

5.2. Jacobi polynomials

Define, for $a_3 \notin -\mathbb{N}$,

$${}_2F_1(a_1,a_2;a_3;a_4)=\sum_{k\geqslant 0}\frac{(a_1)_k(a_2)_k}{(a_3)_k}\frac{a_4^k}{k!},$$

where

$$(a)_k=a(a+1)\cdots(a+k-1).$$

The Jacobi polynomials are defined [17, p. 170] by

$$P_n^{(\alpha,\beta)}=\frac{(\alpha+1)_n}{n!}\,{}_2F_1\left(-n,n+\alpha+\beta+1;\alpha+1;\frac{1-x}{2}\right).$$

Proposition 2.2 implies that, for α and β in $\mathbb{N}\backslash\{0\}$, the sequence of Jacobi polynomials, reduced modulo any odd prime number p, is not a simple p-Carlitz sequence of polynomials. Namely the generating function is given [17, p. 172] by

$$F(X,Y) = \sum_{n \geqslant 0} P_n^{(\alpha,\beta)}(X)Y^n = \frac{2^{\alpha+\beta}}{r(X,Y)(1-Y+r(X,Y))^{\alpha}(1+Y+r(X,Y))^{\beta}},$$

where $r(X,Y) = (1-2XY+Y^2)^{1/2}$. In particular for $X=1$, and Y small enough, all the series converge as real power series, and we have: $r(1,Y) = (1-2Y+Y^2)^{1/2} = 1-Y$. Hence

$$F(1,Y) = (1-Y)^{-\alpha-1}.$$

This also holds as an equality between formal power series with rational coefficients. Now, if p is an odd prime number, and if $(F(X,Y)/F(X^p,Y^p) \bmod p)$ were a polynomial in X and Y, of degree in Y at most $(p-1)$, then, $(F(1,Y)/F(1,Y^p) \bmod p)$ would be a polynomial in Y of degree at most $(p-1)$. But this not the case, since $F(1,Y)/F(1,Y^p) = (1+Y+Y^2+\cdots+Y^{p-1})^{\alpha+1}$, and $\alpha \in \mathbb{N}\backslash\{0\}$.

5.3. Meixner polynomials

This sequence is defined [17, p. 225] with the notations above (for $\beta \notin -\mathbb{N}$ and $c \neq 0$) by

$$\tilde{M}_n(X,\beta,c) = (\beta)_n \, {}_2F_1(-n,-X;\beta;1-c^{-1}).$$

These polynomials satisfy the recurrence (see [26, p. 38] for example)

$$\tilde{M}_{n+1}(X,\beta,c) = \left(\frac{c-1}{c}X + \frac{n+(n+\beta)c}{c}\right)\tilde{M}_n(X,\beta,c) - \frac{n(\beta+n-1)}{c}\tilde{M}_{n-1}(X,\beta,c).$$

We will suppose that $\beta \in \mathbb{N}\backslash\{0\}$ and $1/c \in \mathbb{Z}\backslash\{1\}$. Then, from a result of Carlitz [9, Theorem 1], we have for any prime $p \geqslant 2$ (actually this is true even if p is not prime)

$$\forall n \geqslant 0, \quad \tilde{M}_{pn}(X,\beta,c) \equiv \tilde{M}_p(X,\beta,c)^n \bmod p.$$

This implies that, for $\beta \in \mathbb{N}\backslash\{0\}$ and $1/c \in \mathbb{Z}\backslash\{1\}$, the sequence of Meixner polynomials, reduced modulo any prime number p, is not a simple p-Carlitz sequence of polynomials. Namely, if this sequence were a simple p-Carlitz sequence of polynomials, we would have

$$\forall n \geqslant 0, \quad \tilde{M}_{pn}(X,\beta,c) \equiv \tilde{M}_n(X^p,\beta,c) \equiv \tilde{M}_n(X,\beta,c)^p \bmod p.$$

Hence

$$\tilde{M}_n(X,\beta,c)^p \equiv \tilde{M}_p(X,\beta,c)^n \bmod p.$$

Taking n prime to p, and differentiating with respect to X, this would imply that $\tilde{M}'_p(X,\beta,c)$ is zero modulo p. This is not the case, since it is easy to compute from the above definition $\tilde{M}_p(X,\beta,c) \equiv (1-c^{-1})(X^p - X) \bmod p$.

5.4. Charlier polynomials

The Charlier polynomials can be defined [26, p. 40, 17, p. 226] (for $a \neq 0$) by

$$C_n(X,a) = {}_2F_0(-n,-X;\ ;-1/a) = \sum_{k\geqslant 0} \frac{(-n)_k(-X)_k}{k!}\left(\frac{-1}{a}\right)^k.$$

Hence

$$C_n(X,a) = \sum_{k=0}^{n}(-1)^k\binom{n}{k}X(X-1)\cdots(X-k+1)\frac{1}{a^k}.$$

They satisfy the recurrence [17, p. 227]

$$aC_{n+1}(X,a) = (n+a-X)C_n(X,a) - nC_{n-1}(X,a).$$

In particular if we take $1/a \in \mathbb{N}$, we can apply the result [9, Theorem 1] of Carlitz and the remark that $C_p(X,a) \equiv 1-(1/a)(X^p - X) \bmod p$, to conclude, as for the Meixner polynomials in Section 5.3 above: for $1/a \in \mathbb{N}$, the sequence of Charlier polynomials, reduced modulo any prime number p, is not a simple p-Carlitz sequence of polynomials.

5.5. Continuous dual Hahn polynomials

The continuous dual Hahn polynomials $S_n(X,a,b,c)$ are defined (see [26, p. 27] for example) by $S_n(X^2,a,b,c) = (a+b)_n(a+c)_n\, {}_3F_2(-n, a+\mathrm{i}X, a-\mathrm{i}X; a+b, a+c; 1)$, i.e.,

$$S_n(X^2,a,b,c) = (a+b)_n(a+c)_n \sum_{k=0}^{\infty} \frac{(-n)_k(a+\mathrm{i}X)_k(a-\mathrm{i}X)_k}{(a+b)_k(a+c)_k\, k!}.$$

Hence

$$S_n(X,a,b,c) = \sum_{k=0}^{n}(-1)^k\binom{n}{k}\prod_{j=0}^{k-1}((a+j)^2+X)\prod_{\ell=k}^{n-1}((a+b+\ell)(a+c+\ell)).$$

Let us take $a,b,c \in \mathbb{N}\setminus\{0\}$. It is not difficult, using the three-term recurrence relation satisfied by these polynomials (see [26, pp. 27–28] for example), the result [9, Theorem 1] of Carlitz again, and the expression $S_p(X) \equiv (-1)^p\prod_{j=0}^{p-1}((a+j)^2+X)$, which implies $S_p(X)S_p(-X) \equiv (X^p - X)^2 \bmod p$, to prove that: the sequence of continuous dual Hahn polynomials, reduced modulo any odd prime p, is not a simple p-Carlitz sequence of polynomials.

6. An automaticity theorem

Theorem 6.1. *Let R be a finite commutative ring with unit. Let $d \geqslant 2$. If $(P_n(X))_{n\geqslant 0}$ is a d-Carlitz sequence of polynomials with coefficients in R, such that all polynomials*

$P_0^{(k)}(X)$ of Definition 2.1 are equal to 1, and if

$$P_n(X) = \sum_{m \geqslant 0} a(m,n) X^m,$$

then, the sequence $(a(m,n))_{m,n \geqslant 0}$ is d-automatic.

Proof. To prove that the sequence $(a(m,n))_{m,n \geqslant 0}$ is d-automatic, we have to prove (see [36,37]) that the set

$$\mathscr{N} = \{(a(d^u m + v, d^u n + w))_{m,n},\ u \geqslant 0,\ 0 \leqslant v, w \leqslant d^u - 1\}$$

is finite. Instead of working with subsequences of double sequences of elements of R, we will work with subsequences of sequences of polynomials of $R[X]$. For $i \in [0, d-1]$, the operators Φ_i (sometimes called d-decimation operators) are defined on $R[[X]]$ (hence on $R[X]$) by

$$\Phi_i\left(\sum_{m \geqslant 0} c_m X^m\right) = \sum_{m \geqslant 0} c_{dm+i} X^m.$$

To prove that $\mathscr{N}$ is finite, it suffices to find a set of sequences of polynomials $\mathscr{N}'$ that is finite, that contains the sequence $(P_n(X))_{n \geqslant 0}$, and such that, for any sequence of polynomials $(Q_n(X))_{n \geqslant 0}$ in $\mathscr{N}'$, for every i, j in $[0, d-1]$, the sequence $(\Phi_i(Q_{dn+j}(X)))_{n \geqslant 0}$ is also in $\mathscr{N}'$.

Consider the set $\{(P_n^{(k)}(X))_{n \geqslant 0},\ k \in [1, r]\}$ in the definition of the d-Carlitz property for the sequence $(P_n(X))_{n \geqslant 0}$. Take also a number C such that, for every sequence $(P_n^{(k)}(X))_{n \geqslant 0}$, $k \in [1, r]$, we have

$$\deg P_n^{(k)}(X) \leqslant Cn.$$

Such a number exists as we have seen in Observation 4 above. Define now the set of sequences of polynomials $\mathscr{N}'$ by

$$\mathscr{N}' = \{(H(X) P_n^{(k)}(X))_{n \geqslant 0},\ k \in [1, r],\ H(X) \in R[X],\ \deg H(X) \leqslant C\}.$$

This set is finite, as the ring R is finite. It contains the sequence $(P_n(X))_{n \geqslant 0} = (1.P_n^{(1)}(X))_{n \geqslant 0}$. Finally, if $(H(X) P_n^{(k)}(X))_{n \geqslant 0}$ is a sequence in $\mathscr{N}'$, then

$$\Phi_i(H(X) P_{dn+j}^{(k)}(X)) = \Phi_i(H(X) P_n^{(\ell(k))}(X^d) P_j^{(k)}(X)) = P_n^{(\ell(k))}(X) \Phi_i(H(X) P_j^{(k)}(X)).$$

But

$$\begin{aligned} \deg \Phi_i(H(X) P_j^{(k)}(X)) &\leqslant \frac{1}{d}(\deg H(X) + \deg P_j^{(k)}(X)) \\ &\leqslant \frac{1}{d}(C + Cj) \leqslant \frac{1}{d}(C + C(d-1)) \leqslant C. \end{aligned}$$

Hence, the sequence $(\Phi_i(H(X) P_{dn+j}^{(k)}(X)))_{n \geqslant 0}$ belongs to $\mathscr{N}'$, and our theorem is proved. $\square$

Remark 6.2. If $R = \mathbb{F}_p$, and if $(P_n(X))_{n \geqslant 0}$ is a simple p-Carlitz sequence of polynomials with $P_0(X) = 1$, then, Theorem 6.1 follows from the theorem of Salon [36,37], since the generating function $F(X,Y)=\sum_{n\geqslant 0} P_n(X)Y^n$ is algebraic over the field of rational functions $\mathbb{F}_p(X,Y)$ (see Proposition 2.2).

7. A non-automaticity theorem

Lemma 7.1 (Generalized slice lemma). *Let $d\geqslant 2$, and let $(R_n(X))_{n\geqslant 0}$ be a simple d-Carlitz sequence of polynomials of $\mathbb{Z}/d\mathbb{Z}[X]$ with $R_0(X)=1$. We make the assumption that there exists $i_0\in[1,d-1]$ such that $R_{i_0}(X)$ is not a monomial. Let $R_{i_0}(X)=aX^\alpha+bX^\beta+\cdots$, with $ab\neq 0 \bmod d$, and $\alpha<\beta$. We define the double sequence $(r(n,t))_{n,t\geqslant 0} \bmod d$ by $R_t(X)=\sum_{n,t\geqslant 0} r(n,t)X^n$.*

Let C be a constant such that $\deg R_n(X)\leqslant Cn$ (see Observation 4 above). Let ℓ be an integer such that $(\alpha+Ci_0d^{-\ell})/(\alpha+\beta d^\ell)<1/(d^\ell+1)$ and such that $d^\ell>i_0$. Define the unidimensional sequence $u=(u(n))_{n\geqslant 0}$ by

$$u(n)=r((\alpha+\beta d^\ell)n,\, i_0(d^\ell+1)n).$$

Then, the sequence u is not ultimately periodic.

Proof. We will first prove that there are infinitely many integers $n\in\mathbb{N}$ such that $u(n)\neq 0$. Then, we will prove that for any t there exists an n_t such that $u(n_t)=u(n_t+1)=\cdots=u(n_t+t)=0$. This will imply that the sequence $(u(n))_{n\geqslant 0}$ is not ultimately periodic.

(a) Since $(R_n(X))_{n\geqslant 0}$ is a simple d-Carlitz sequence of polynomials with $R_0(X)=1$, we have, for every $n\geqslant 0$ and for every $j\in[0,d-1]$,

$$R_{dn+j}(X)=R_n(X^d)R_j(X).$$

In particular, for every $n\geqslant 0$,

$$\sum_{m\geqslant 0} r(m,dn)X^m=R_{dn}(X)=R_n(X^d)=\sum_{m\geqslant 0} r(m,n)X^{dm}.$$

Hence, $r(dm,dn)=r(m,n)$ holds for all $m,n\geqslant 0$. (Of course we also have $r(dm+u,dn)=0$ for $0<u\leqslant d-1$.) This yields for all n

$$u(dn)=u(n).$$

Take now $i_0\in[0,d-1]$ given by the hypothesis, such that $R_{i_0}(X)$ is not a monomial. Let $R_{i_0}(X)=aX^\alpha+bX^\beta+\cdots$ (this is of course a finite sum) with $ab\neq 0 \bmod d$ and $\beta>\alpha$. Then, for ℓ such that $d^\ell>i_0$, we have

$$\begin{aligned}\sum_{m\geqslant 0} r(m,i_0(d^\ell+1))X^m &= R_{i_0d^\ell+i_0}(X)\\ &= R_{i_0d^\ell}(X)R_{i_0}(X)\\ &= R_{i_0}(X^{d^\ell})R_{i_0}(X)\\ &= (aX^{\alpha d^\ell}+bX^{\beta d^\ell}+\cdots)(aX^\alpha+bX^\beta+\cdots)\end{aligned}$$

$$= aX^{\alpha d^\ell}(aX^\alpha + bX^\beta + \cdots)$$
$$+bX^{\beta d^\ell}(aX^\alpha + bX^\beta + \cdots) + \cdots .$$

As $(\alpha + \beta d^\ell) > (\alpha + Ci_0 d^{-\ell})(d^\ell + 1) > \alpha d^\ell + Ci_0 \geqslant \alpha d^\ell + \deg R_{i_0}(X)$, then

$$u(1) = r((\alpha + \beta d^\ell), i_0(d^\ell + 1)) = ab \neq 0$$

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

$$u(d^k) = u(1) = ab \neq 0.$$

(b) We will prove that, if $k \geqslant \ell$, and if n is such that

$$\frac{d^k}{d^\ell + 1} < n < \frac{\beta d^k}{\alpha + \beta d^\ell},$$

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

$$d^k < (d^\ell + 1)n < \frac{\beta d^k (d^\ell + 1)}{\alpha + \beta d^\ell} < d^k + d^{k-\ell}$$

for $k \geqslant \ell$. Hence, there exists j_n such that

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

Now (remember that $d^\ell > i_0$, hence $i_0 j_n < d^k$)

$$\begin{aligned}\sum_{m \geqslant 0} r(m, i_0(d^\ell + 1)n) X^m &= \sum_{m \geqslant 0} r(m, i_0 d^k + i_0 j_n) X^m = R_{i_0 d^k + i_0 j_n}(X)\\ &= R_{i_0 d^k}(X) R_{i_0 j_n}(X) = R_{i_0}(X^{d^k}) R_{i_0 j_n}(X)\\ &= (aX^{\alpha d^k} + bX^{\beta d^k} + \cdots) R_{i_0 j_n}(X)\\ &= aX^{\alpha d^k} R_{i_0 j_n}(X) + bX^{\beta d^k} R_{i_0 j_n}(X) + \cdots .\end{aligned}$$

Hence, if $m = (\alpha + \beta d^\ell)n$, with $d^k/(d^\ell + 1) < n < \beta d^k/(\alpha + \beta d^\ell)$, we have on one hand,

$$m < \beta d^k$$

and on the other hand,

$$\begin{aligned}m &> \frac{(\alpha + \beta d^\ell) d^k}{d^\ell + 1} > (\alpha + Ci_0 d^{-\ell}) d^k = \alpha d^k + Ci_0 d^{k-\ell} > \alpha d^k + Ci_0 j_n\\ &\geqslant \alpha d^k + \deg R_{i_0 j_n}(X).\end{aligned}$$

It is now clear that, for such an m, we have $r(m, d^k + j_n) = 0$. This can also be written

$$\forall n \in \left] \frac{d^k}{d^\ell + 1}, \frac{\beta d^k}{\alpha + \beta d^\ell} \right[, \qquad u(n) = r((\alpha + \beta d^\ell)n, (d^k + 1)n) = 0$$

which ends the proof. $\square$

Lemma 7.2 (Monomial slice lemma). *Let p be a prime number, and let $\mathscr{R} = (R_n(X))_{n\geqslant 0}$ be a simple p-Carlitz sequence of polynomials of $\mathbb{F}_p[X]$. Let*

$$R_n(X) = \sum_m r(m,n)X^m.$$

Assume

- $R_0(X) = 1$,
- $R_j(X) = \alpha_j X^{s(j)}$, *where, for* $1 \leqslant j \leqslant p-1$, $\alpha_j \neq 0 \bmod p$,
- $\min_{1\leqslant j\leqslant p-1}(s(j)/j) < \max_{1\leqslant j\leqslant p-1}(s(j)/j) = K$.

Let $\bar{j} = \min\{j \in [1, p-1],\ s(j) = jK\}$ and $\bar{s} = s(\bar{j})$. Then, the sequence $(a(n))_{n\geqslant 0}$ defined by $a(n) = r(\bar{j}n, \bar{s}n)$ is not ultimately periodic.

Proof. Let

$$\mathscr{M} = \left\{ j \in [1, p-1];\ \frac{s(j)}{j} = K \right\} \cup \{0\}.$$

(Note that $\mathscr{M}$ is strictly included in $[1, p-1]$.)

Assume that the sequence $(a(n))_{n\geqslant 0}$ is ultimately periodic, i.e., that there exist $n_0 \in \mathbb{N}$ and $T \in \mathbb{N}\backslash\{0\}$, such that

$$\forall n \geqslant n_0, \quad a(n+T) = a(n).$$

Let $\mathscr{N} = \{n,\ a(n) \neq 0\}$. We first claim that

$$\mathscr{N} = \{n;\ \bar{j}n = n_k p^k + \cdots + n_1 p + n_0,\ n_j \in \mathscr{M} \text{ for all } j \in [0,k]\}.$$

Namely, if $\bar{j}n = n_k p^k + \cdots + n_1 p + n_0$ with the n_j's in $[0, p-1]$, then

$$R_{\bar{j}n}(X) = \prod_{i=0}^{k} (\alpha_{n_i} X^{s(i)})^{p^i} = \prod_{i=0}^{k} (\alpha_{n_i}^{p^i}) X^{\sum_{i=0}^{k} s(n_i)p^i}.$$

Since $R_{\bar{j}n}(X) = \sum_m r(m, \bar{j}n)X^m$, we see that $a(n) = r(\bar{j}n, \bar{s}n) \neq 0$ if and only if $\bar{s}n = \sum_{i=0}^k s(n_i)p^i$. But $\bar{s} = s(\bar{j})$, and $s(\bar{j}) = \bar{j}K$. Hence, the condition $\bar{s}n = \sum_{i=0}^k s(n_i)p^i$ is equivalent to the condition $K(\bar{j}n) = \sum_{i=0}^k s(n_i)p^i$. Since $\mathscr{M}$ is precisely the set of j's such that either $j=0$ or $s(j)=Kj$, and its complement the set of j's such that $s(j) < Kj$, we deduce that the condition holds if and only if $s(n_i) = Kn_i$ for all $i \in [0,k]$, which is exactly saying that $n_i \in \mathscr{M}$ for all $i \in [0,k]$.

In other words n is in $\mathscr{N}$ if and only if the p-ary digits of $\bar{j}n$ belong to the restricted set of digits $\mathscr{M}$.

Now, the characteristic function χ of the set $\mathscr{N}$, defined by

$$\chi(n) = \begin{cases} 1 & \text{if } a(n) \neq 0, \\ 0 & \text{otherwise} \end{cases}$$

is also ultimately periodic (we can take the same T and n_0). Hence $n \in \mathscr{N}$ and $n \geqslant n_0$ implies $n + T \in \mathscr{N}$.

Let now $\bar{j}T = t_l p_l + \cdots + t_1 p + t_0$, with $t_j \in [0, p-1]$ for $j \in [0, l]$, be the p-ary expansion of $\bar{j}T$. Let $n' \in \mathcal{N}$ such that $n' \geqslant n_0/p^{l+2}$. Looking at the p-ary digits of $\bar{j}n'$ proves that the number $n = p^{l+2}n'$ is also an element of $\mathcal{N}$, and it is $\geqslant n_0$. Still looking at the p-ary digits of the product by $\bar{j}$, we see that $n + T$ belongs to $\mathcal{N}$, and hence T belongs to $\mathcal{N}$. Of course this holds for any period, hence for any integer multiple of T. This last condition is impossible, using the following straightforward lemma.

Lemma 7.3. *Let $\mathcal{M}$ be a restricted set of p-ary digits containing* 0, *where p is prime. If a non-zero integer has all its digits in $\mathcal{M}$, then, there exists a multiple of this integer, such that its less significant non-zero digit is not in $\mathcal{M}$.*

Theorem 7.4. *Let p be a prime number, and let $\mathcal{R}=(R_n(X))_{n\geqslant 0}$ be a simple p-Carlitz sequence of polynomials of $\mathbb{F}_p[X]$, with $R_0(X) = 1$. Let $\mathcal{R}(X,Y) = \sum_{n\geqslant 0} R_n(X)Y^n = \sum_{m,n\geqslant 0} r(m,n)X^m Y^n$.*

(1) *The double sequence $(r(m,n))_{m,n\geqslant 0} \in (\mathbb{F}_p)^{\mathbb{N}\times\mathbb{N}}$ has been proved p-automatic (and hence is p^l-automatic, for every $l \geqslant 1$).*

(2) *If at least one of the polynomials $R_u(X)$, $1 \leqslant u \leqslant p-1$ is not a monomial, and if the double sequence $(r(m,n))_{m,n\geqslant 0}$ is k-automatic, then $k = p^l$ for some $l \geqslant 1$.*

(3) *If the conditions of the monomial slice lemma are satisfied, and if the double sequence $(r(m,n))_{m,n\geqslant 0}$ is k-automatic, then $k = p^l$ for some $l \geqslant 1$.*

Proof. 1. This follows from Observation 5 and Theorem 6.1.

2. Suppose now that the sequence $(r(m,n))_{m,n\geqslant 0}$ is k-automatic and the assumptions of (2) are satisfied. Then, from the slice lemma, there exists a non-ultimately periodic sequence $u = (u(n))_{n\geqslant 0}$, where $u(n) = r((\alpha + \beta p^l)n, i_0(p^l + 1)n)$. The sequence u is k-automatic, in the sense of [11,12], since the double sequence $(r(n,t))_{n,t\geqslant 0}$ is k-automatic (see [36,37]). But the sequence u is also p-automatic from (1). Since it is not ultimately periodic, Cobham's theorem [13] implies that k is a non-trivial power of p.

3. The proof follows the proof of (2), using the monomial slice lemma instead of the slice lemma.

8. Automaticity of sequences generated by classical orthogonal polynomials

8.1. Legendre polynomials

We consider the sequence $\mathcal{P} = (P_n(X))_{n\geqslant 0}$ of Legendre polynomials and its generating function $\mathcal{P}(X,Y) = \sum_{n\geqslant 0} P_n(X)Y^n = \sum_{m,n\geqslant 0} b(m,n)X^m Y^n$. As we already noted, this generating function has the explicit expression (see [17, p. 182] for example)

$$\mathcal{P}(X,Y) = \frac{1}{\sqrt{1 - 2XY + Y^2}}.$$

This formula can be either considered as an equality for real functions with Y small enough, or as an equality of formal power series with rational coefficients. Note that it implies

$$\mathscr{P}(X,Y)^2 = \frac{1}{1-2XY+Y^2},$$

that can be considered as an equality of formal power series with coefficients in $\mathbb{Q}_{(p)}$ for any odd prime number p.

Lemma 8.1. *Let p be an odd prime number. The sequence $(b(n,n) \bmod p)_{n\geqslant 0}$ is not ultimately periodic.*

Proof. Let $a(n)=b(n,n) \bmod p$. We have seen that an explicit expression for $P_n(X)$ is

$$P_n(X) = \frac{1}{2^n}\sum_{v=0}^{\lfloor n/2 \rfloor}(-1)^v \binom{n}{v}\binom{2n-2v}{n-2v} X^{n-2v}.$$

Hence, $a(n)=b(n,n)=2^{-n}\binom{2n}{n}$. This implies

$$A(X) = \sum_{n\geqslant 0} a(n)X^n = \sum_{n\geqslant 0}\binom{2n}{n}\left(\frac{X}{2}\right)^n = \frac{1}{\sqrt{1-2X}}.$$

This equality holds between the formal power series with coefficients in $\mathbb{Q}$. But the coefficients are also in $\mathbb{Q}_{(p)}$ for every odd prime number p. Hence, for any odd prime number p,

$$(1-2X)A(X)^2 \equiv 1 \bmod p.$$

It is straightforward to see that this equation cannot be satisfied by a rational function. Hence, $(A(X) \bmod p)$ is not a rational function, which is equivalent to saying that the sequence $(a(n) \bmod p)_{n\geqslant 0}$ is not ultimately periodic.

Remark 8.2. We could have given several other non-ultimately periodic subsequences of the sequence $(b(m,n) \bmod p)_{m,n}$. We just give another example here. Let $z(n) = b(0,n) = P_n(0)$. We easily have $z(n)=0$ if n is odd, and $z(n) = 2^{-2t}(-1)^t\binom{2t}{t}$ if $n=2t$. As previously the formal power series

$$\sum_{n\geqslant 0} z(n)X^n = \frac{1}{\sqrt{1+X^2}}$$

does not reduce modulo any odd prime number p to a rational function. In the case $p=3$, the sequence $(z(n) \bmod 3)_{n\geqslant 0}$ can take only the values 0 and 1. This sequence is actually the characteristic function of those integers that have no digit 1 in their base-3 expansion.

Note that the sequence $(a_n)_{n\geqslant 0}$ above, when reduced modulo 3, can be encountered in various other contexts:

* *Integers with missing digits*. The sequence $(a(n) \bmod 3)_{n\geqslant 0}$ is the characteristic function of those integers that have no digit 2 in their base-3 expansion;
* *Infinite sequences without arithmetic progressions*. Consider the minimal (for the lexicographical order) sequence of integers that does not contain three terms in arithmetic progression. This sequence begins with

$$0\ 1\ 3\ 4\ 9\ 10\ 12\ 13\ 27\ \ldots$$

The characteristic sequence of these integers is precisely $(a(n) \bmod 3)_{n\geqslant 0}$. For the general problem see [18,35,20], see also the survey [25]. For a Toeplitz-transform framework, see [1];
* *Geometric constructions*. A curious geometric construction involving this sequence occurs in [31].

Theorem 8.3. *Let $(P_n(X))_{n\geqslant 0}$ be the sequence of Legendre polynomials. Let $b(m,n)$ be defined by $\mathscr{P}(X,Y)=\sum_{n\geqslant 0} P_n(X)Y^n=\sum_{m,n\geqslant 0} b_{m,n}X^mY^n$. Let d be an odd natural number $d\geqslant 3$. Then, the double sequence $(b(m,n) \bmod d)_{m,n\geqslant 0}$ is k-automatic if and only if there exists a prime number p and two integers $l_1,l_2\geqslant 1$ such that $d=p^{l_1}$* and $k=p^{l_2}$.

Proof. 1. We first prove that, if the sequence $(b(m,n) \bmod d)_{m,n\geqslant 0}$ is k-automatic, with $d,k\geqslant 2$, then, d and k must be powers of a same prime number p. Let p be a prime divisor of d. The sequence $(b(m,n) \bmod d)_{m,n\geqslant 0}$ is k-automatic, hence its re-reduction modulo p, i.e., the sequence $(b(m,n) \bmod p)_{m,n\geqslant 0}$, is also k-automatic. We then deduce from Lemma 7.1, Theorem 7.4, and Lemma 8.1 that k must be a power of p. Now, if p_1 were another prime divisor of d, the number k should also be a power of p_1, which is not possible.

2. We now prove that if $d=p^l$ for some odd prime number p, and some $l\geqslant 1$, then, the sequence $(b(m,n) \bmod d)_{m,n\geqslant 0}$ is p-automatic (and hence p^k-automatic for any $k\geqslant 1$). If $l=1$, this is a consequence of Theorem 6.1 and of the p-Carlitz property of the sequence of Legendre polynomials modulo p that we recalled in Section 4. But we need a proof for the general case. Remember that we have

$$\mathscr{P}(X,Y)^2=\sum_{m\geqslant 0} b(m,n)X^mY^n=\frac{1}{1-2XY+Y^2}.$$

This equality is a priori true over $\mathbb{Q}$, but it is actually true over $\mathbb{Q}_{(p)}$, and hence over $\mathbb{Z}_p$, the p-adic numbers. Then, considered as an element of $\mathbb{Z}_p[[X,Y]]$, the formal power series $\mathscr{P}(X,Y)$ is algebraic over $\mathbb{Z}_p(X,Y)$. Hence, from a theorem of Denef and Lipshitz [14, Theorem 3.1], the sequence $(b(m,n) \bmod p^l)_{m,n\geqslant 0}$ is p-automatic, and hence p^k-automatic for any $k\geqslant 1$.

8.2. Hermite and Laguerre polynomials

8.2.1. Hermite polynomials

We consider here the sequence of coefficients for the generating function of the Hermite polynomials. We have the following theorem.

Theorem 8.4. *Let* $\mathscr{H} = (H_n(X))_{n\geqslant 0}$ *be the sequence of Hermite polynomials. Let* $h(m,n)$ *be defined by* $\mathscr{H}(X,Y) = \sum_{n\geqslant 0} H_n(X)Y^n = \sum_{m,n\geqslant 0} h(m,n)X^m Y^n$. *Let* d *be an integer* $\geqslant 2$. *Then, the sequence* $(h(m,n) \bmod d)_{m,n\geqslant 0}$ *is* k*-automatic for every integer* $k\geqslant 2$.

Proof. We proved in Section 4 that, for every $d\geqslant 2$, the sequence of Hermite polynomials modulo d is a d-Carlitz sequence of polynomials. Hence, from Theorem 6.1, for every $d\geqslant 2$, the sequence $(h(m,n) \bmod d)_{m,n\geqslant 0}$ is d-automatic.

Fix now $d\geqslant 2$, and let a and b be two different prime numbers that do not divide d. The sequence $(h(m,n) \bmod ad)_{m,n\geqslant 0}$ is ad-automatic. Hence, its projection obtained by re-reducing modulo d, i.e., the sequence $(h(m,n) \bmod d)_{m,n\geqslant 0}$ is also ad-automatic. For the same reason this sequence is bd-automatic. Now, ad and bd are clearly multiplicatively independent (in other words the equation $(ad)^x = (bd)^y$ has no solution in nonzero integers x and y). Hence, by the Cobham–Semenov theorem (see the survey [7] for example), the sequence $(h(m,n) \bmod d)_{m,n\geqslant 0}$ is recognizable, and therefore it is k-automatic for all $k\geqslant 2$.

8.2.2. Modified Laguerre polynomials

Let us consider as previously the sequence of modified Laguerre polynomials $(\Lambda_n^{(\alpha)}(X))_{n\geqslant 0}$. Following the same lines as above we can easily prove the following theorem.

Theorem 8.5. *Let* $(L_n^{(\alpha)}(X))_{n\geqslant 0}$ *be the sequence of Laguerre polynomials, with* α *integer. Let* $(\Lambda_n^{(\alpha)}(X))_{n\geqslant 0} = (n!L_n^{(\alpha)}(X))_{n\geqslant 0}$ *be the corresponding sequence of modified Laguerre polynomials. Define* $\ell(m,n)$ *by* $\sum_{n\geqslant 0} \Lambda_n^{(\alpha)}(X)Y^n = \sum_{m,n\geqslant 0} \ell(m,n)X^m Y^n$. *Let* d *be an integer* $\geqslant 2$. *Then, the sequence* $(\ell(m,n) \bmod d)_{m,n\geqslant 0}$ is k*-automatic for every* $k\geqslant 2$.

8.3. Chebishev polynomials

As recalled in Section 5.1, the sequences of Chebishev polynomials of the first kind $\mathscr{T} = (T_n(X))_{n\geqslant 0}$ and of the second kind $\mathscr{U} = (U_n(X))_{n\geqslant 0}$ have the generating functions

$$\mathscr{T}(X,Y) = \sum_{n=0}^{\infty} T_n(X)Y^n = \frac{1-XY}{1-2XY+Y^2},$$

$$\mathscr{U}(X,Y) = \sum_{n=0}^{\infty} U_n(X)Y^n = \frac{1}{1-2XY+Y^2}.$$

Define the double sequences $(t(m,n))_{m,n\geqslant 0}$ and $(u(m,n))_{m,n\geqslant 0}$ by

$$\mathcal{T}(X,Y)=\sum_{n=0}^{\infty}T_n(X)Y^n=\sum_{m,n=0}^{\infty}t(m,n)X^mY^n,$$

$$\mathcal{U}(X,Y)=\sum_{n=0}^{\infty}U_n(X)Y^n=\sum_{m,n=0}^{\infty}u(m,n)X^mY^n.$$

Using the equality $(\sum_{n\geqslant 0}X^nY^n)\mathcal{T}(X,Y)=\mathcal{U}(X,Y)$, it is not hard to prove that, for a given $k\geqslant 2$, the sequences $(t(m,n) \bmod d)_{m,n\geqslant 0}$ and $(u(m,n) \bmod d)_{m,n\geqslant 0}$ are simultaneously k-automatic or not k-automatic. We will consider the sequence generated by the Chebishev polynomials of the second kind.

We can, as previously, use the generating function to deduce that

$$u(m,n)=\begin{cases} 2^m\binom{\frac{m+n}{2}}{m} & \text{if } m+n \text{ is even and } m\leqslant n,\\ 0 & \text{otherwise.}\end{cases}$$

We can then make the same reasoning as done previously, using the theorem of Denef and Lipschitz [14], the theorem of Cobham [13], and the property that the sequence $(u(n,3n) \bmod p)_n$ is not ultimately periodic, for any odd prime p, since

$$\sum_{n\geqslant 0}u(n,3n)X^n=\sum_{n\geqslant 0}\binom{2^n}{n}X^n=\frac{1}{\sqrt{1-8X}},$$

cannot be a rational function mod p if p is an odd prime. This leads us to the following theorem, for which we will give a different proof that directly works for both sequences of Chebishev polynomials.

Theorem 8.6. *Let $(W_n(X))_{n\geqslant 0}$ be the sequence of Chebishev polynomials of the first or of the second kind. Define $w(m,n)$ by $\mathcal{W}(X,Y)=\sum_{n\geqslant 0}W_n(X)Y^n=\sum_{m,n\geqslant 0}w(m,n)X^mY^n$. Then, the following automaticity properties hold.*

- *If $d=2^kp^l$, where p is an odd prime number, $k\geqslant 0$, and $l\geqslant 1$, then, the sequence $(w(m,n) \bmod d)_{m,n\geqslant 0}$ is p^a-automatic for any $a\geqslant 1$ and not r-automatic for $r\notin\{p^a,\ a\geqslant 1\}$.*
- *If d has two different odd prime divisors, then, the sequence $(w(m,n) \bmod d)_{m,n\geqslant 0}$ is not k-automatic for any k.*
- *If $d=2^l$, with $l\geqslant 1$, then, the sequence $(w(m,n) \bmod d)_{m,n\geqslant 0}$ is k-automatic for all k.*

Our proof will make use of a recent result of von Haeseler and Petersen [21].

Theorem 8.7 (Haeseler and Petersen [21]). *Let $P(X,Y)/Q(X,Y)=\sum_{m,n}a(m,n)X^mY^n$ be a formal power series over $\mathbb{Z}/d\mathbb{Z}$ that is equal to the quotient of two polynomials in $\mathbb{Z}/d\mathbb{Z}[X]$, with $Q(0,0)$ invertible in $\mathbb{Z}/d\mathbb{Z}$. Let Δ be the set of prime divisors p*

of d for which there does not exist a polynomial $S(X,Y)$ in $\mathbb{Z}/d\mathbb{Z}[X,Y]$ and finitely many monomials $a_jX^{\alpha_j}Y^{\beta_j}$, $j=1,2,\ldots,s$ such that

$$S(X,Y)Q(X,Y)=\prod_{j=1}^{s}(1-a_jX^{\alpha_j}Y^{\beta_j}) \bmod p,$$

and let χ be the cardinality of Δ.

- *If $\chi \geqslant 2$, then, the sequence $(a(m,n))_{m,n\geqslant 0}$ is not k-automatic for any $k\geqslant 2$.*
- *If $\chi=1$, then, the sequence $(a(m,n))_{m,n\geqslant 0}$ is p^a-automatic, where p is the only element of Δ, and a any integer $\geqslant 1$, and this sequence is not k-automatic for any $k\notin\{p^a; a\geqslant 1\}$.*
- *If $\chi=0$, then, the sequence $(a(m,n))_{m,n\geqslant 0}$ is k-automatic for any $k\geqslant 2$.*

Proof of Theorem 8.6. In view of Theorem 8.7 we consider the denominators of the generating functions for the Chebishev sequences of polynomials, $Q(X,Y)=1-2XY+Y^2$. For $p=2$, we clearly have $Q(X,Y)=1+Y^2 \bmod 2$, hence $2\notin\Delta$. In order to prove our theorem it suffices to prove that, for every odd prime number p, there does not exist a polynomial $S(X,Y)$ and finitely many monomials $a_jX^{\alpha_j}Y^{\beta_j}$, $j=1,2,\ldots,s$, such that

$$S(X,Y)Q(X,Y)=\prod_{j=1}^{s}(1-a_jX^{\alpha_j}Y^{\beta_j}) \bmod p.$$

Suppose it were the case. Define $K=\mathbb{F}_p(X)$ (K is the field of rational functions with coefficients in $\mathbb{F}_p$). Let g be an element such that $g^2=X^2-1$. We know that there exists a quadratic extension of K containing such a g: the fact that g cannot belong to K immediately follows from the fact that $p\neq 2$ and hence $+1\neq -1 \bmod p$.

Now, the element $X+g$ is a root of the polynomial $Q(X,Y)$ over $K(g)$. Hence, this is a root of the polynomial $\prod_{j=1}^{s}(1-a_jX^{\alpha_j}Y^{\beta_j})$ over $K(g)$. Hence, there exist an a in $\mathbb{F}_p\backslash\{0\}$, and two integers α and β, not both equal to 0, such that

$$(X+g)^\beta=\frac{1}{aX^\alpha}(\text{in } K(g)).$$

We then expand the left-hand term

$$\begin{aligned}\frac{1}{aX^\alpha}&=(X+g)^\beta=\sum_{j=0}^{\beta}\binom{\beta}{j}X^{\beta-j}g^j\\&=\sum_{j\leqslant\beta/2}\binom{\beta}{2j}X^{\beta-2j}g^{2j}+g\sum_{j\leqslant(\beta-1)/2}\binom{\beta}{2j+1}X^{\beta-2j-1}g^{2j}\\&=\sum_{j\leqslant\beta/2}\binom{\beta}{2j}X^{\beta-2j}(X^2-1)^j+g\sum_{j\leqslant(\beta-1)/2}\binom{\beta}{2j+1}X^{\beta-2j-1}(X^2-1)^j.\end{aligned}$$

Since g does not belong to $K=\mathbb{F}_p(X)$, we have

$$\sum_{j\leqslant\beta/2}\binom{\beta}{2j}X^{\beta-2j}(X^2-1)^j=\frac{1}{aX^\alpha}$$

and

$$\sum_{j\leqslant(\beta-1)/2}\binom{\beta}{2j+1}X^{\beta-2j-1}(X^2-1)^j=0.$$

Looking at the degrees in the first equality proves that $\alpha=0$, hence

$$(X+g)^{\beta}=\frac{1}{a}.$$

Putting $X=1$ in the second equality gives $\beta=0 \bmod p$. Hence $\beta=p\beta'$, and

$$\left((X+g)^{\beta'}-\frac{1}{a}\right)^p=(X+g)^{\beta}-\frac{1}{a^p}=(X+g)^{\beta}-\frac{1}{a}=0.$$

This implies

$$(X+g)^{\beta'}=\frac{1}{a},$$

Iterating the process, we obtain that $\beta=0$ and the desired contradiction. □

8.4. Other examples

Automaticity of sequences associated to some of the sequences of orthogonal polynomials given in Section 5 that are not simple p-Carlitz can be addressed using the following proposition. This proposition is an easy consequence of a result of Carlitz [9, Theorem 1] and of the theorem of von Haeseler and Petersen quoted above (Theorem 8.7, see also [21]).

Proposition 8.8. *Let $(U_n(X))_{n\geqslant 0}$, $(f_n(X))_{n\geqslant 0}$, and $(g_n(X))_{n\geqslant 0}$ be three sequences of polynomials with integer coefficients, such that*

- $U_0(X)=1$;
- $U_1(X)=f_0(X)$;
- $g_0(X)=0$;
- *the following relation holds for all $n\geqslant 1$:*

$$U_{n+1}(X)=f_n(X)U_n(X)+g_n(X)U_{n-1}(X).$$

Suppose that for each prime number p, the polynomial $(U_p(X) \bmod p)$ is not a monomial. Define the double sequence of integers $(z(m,n))_{m,n\geqslant 0}$ by $\sum_{n\geqslant 0}U_n(X)Y^n=\sum_{m,n\geqslant 0}z(m,n)X^mY^n$. Let $d\geqslant 2$ be an integer. Then,

- *if $d=p^a$ for some prime number p and some integer $a\geqslant 1$, then, the sequence $(z(m,n) \bmod d)_{m,n\geqslant 0}$ is p^b-automatic, for any integer $b\geqslant 1$, and not r-automatic for any $r\notin\{p^b,\ b\geqslant 1\}$;*
- *if d has two different prime divisors, then, the sequence $(z(m,n) \bmod d)_{m,n\geqslant 0}$ is not k-automatic for any $k\geqslant 2$.*

Proof. Using [9, Theorem 1] we first see that

$$\forall j\in[0,d-1],\quad \forall n\geqslant 0,\quad U_{dn+j}(X)\equiv U_d(X)^nU_j(X) \bmod d.$$

Hence

$$\sum_{n\geqslant 0} U_n(X)Y^n \equiv \frac{\sum_{j=0}^{d-1} U_j(X)Y^j}{1-U_d(X)Y^d} \bmod d.$$

Now, to obtain the conclusion of our Theorem we only need, using Theorem 8.7, to prove that, for any prime number p dividing d, there does not exist a polynomial $S(X,Y) \in \mathbb{Z}/d\mathbb{Z}[X]$ and finitely many monomials $a_j X^{\alpha_j} Y^{\beta_j}$, $j = 1,2,\ldots,s$ such that

$$(*) \quad S(X,Y)(1-U_d(X)Y^d) = \prod_{j=1}^{s}(1-a_j X^{\alpha_j} Y^{\beta_j}) \bmod p.$$

If such an equality were satisfied, let $K = \mathbb{F}_p(X)$ and let g be a root of $T^d = U_d(X)$ in an extension K' of K. Considering equality $(*)$ as an equality between polynomials in $K'(X)[Y]$, we see that the left-hand side cancels out for $Y = 1/g$. Hence, the right-hand side also cancels out. In other words, there exist a, α, β, such that

$$1 - \frac{aX^\alpha}{g^\beta} = 0,$$

i.e.,

$$g^\beta = aX^\alpha.$$

Take now the dth power, and remember that p divides d, say $d = pd'$. Then, using [9, Theorem 1] again, but modulo p, we have

$$U_p(X)^{d'\beta} = U_{pd'}(X)^\beta = U_d(X)^\beta = g^{d\beta} = a^d X^{d\alpha} \quad (\text{in } K').$$

But this equality also holds in K, hence $(U_p(X) \bmod p)$ should be a monomial, which is not the case. □

Corollary 8.9. *The above result applies*

- *to the Meixner polynomials, with the conditions* $\beta \in \mathbb{N}\backslash\{0\}$, $c \neq 0$ *and* $1/c \in \mathbb{Z} \setminus \{1\}$;
- *to the Charlier polynomials, with the conditions* $a \neq 0$ *and* $1/a \in \mathbb{N}$;
- *to the continuous dual Hahn polynomials, with the conditions* $a,b,c \in \mathbb{N}\backslash\{0\}$.

It suffices to use the results given in Sections 5.3–5.5 to see that Proposition 8.8 above can be applied to the sequence of Meixner polynomials, to the sequence of Charlier polynomials, and to the sequence of continuous dual Hahn polynomials, with the restrictions on parameters given in the statement of the corollary.

Acknowledgements

This paper was written when the first author visited the Cevis at Bremen Universität. The first author wants to thank his friends from Bremen for their hospitality and enthusiasm. Both authors acknowledge with thanks very interesting discussions with H.-O. Peitgen and F. von Haeseler. They also thank the referees for their remarks.

References

[1] J.-P. Allouche, R. Bacher, Toeplitz sequences, paperfolding, Hanoi towers and progression-free sequences of integers, Enseign. Math. 38 (1992) 315–327.
[2] J.-P. Allouche, E. Cateland, W. J. Gilbert, H.-O. Peitgen, J. Shallit, G. Skordev, Automatic maps on semiring with digits, Theory Comput. Systems (Math. Systems Theory) 30 (1997) 285–331.
[3] J.-P. Allouche, F. von Haeseler, E. Lange, A. Petersen, G. Skordev, Linear cellular automata and automatic sequences, Parallel Comput. 23 (1997) 1577–1592.
[4] J.-P. Allouche, F. von 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.
[5] J.-P. Allouche, F. von Haeseler, H.-O. Peitgen, G. Skordev, Linear cellular automata, finite automata and Pascal's triangle, Discrete Appl. Math. 66 (1996) 1–22.
[6] D. Barsky, Analyse p-adique et suites classiques de nombres, Sém. Lotharingien Combin. B05b (1981) 24 pages [http://cartan.u-strasbg.fr:80/opapers/s05barsky.ps].
[7] V. Bruyère, G. Hansel, C. Michaux, R. Villemaire, Logic and p-recognizable sets of integers, Bull. Belg. Math. Soc. 1 (1994) 191–238; 577.
[8] J.-L. Brylinski, Legendre polynomials and the elliptic genus, J. Algebra 145 (1992) 83–93.
[9] L. Carlitz, Congruence properties of polynomials of Hermite, Laguerre and Legendre, Math. Z. 59 (1954) 474–483.
[10] L. Carlitz, The coefficients of the reciprocal of $J_0(X)$, Arch. Math. 6 (1955) 121–127.
[11] G. Christol, Ensembles presque périodiques k-reconnaissables, Theoret. Comput. Sci. 9 (1979) 141–145.
[12] G. Christol, T. Kamae, M. Mendès France, G. Rauzy, Suites algébriques, automates et substitutions, Bull. Soc. Math. France 108 (1980) 401–419.
[13] A. Cobham, On the base-dependence of sets of numbers recognizable by finite automata, Math. Systems Theory 3 (1969) 186–192.
[14] J. Denef, L. Lipshitz, Algebraic power series and diagonals, J. Number Theory 26 (1987) 46–67.
[15] S. Eilenberg, Automata, Languages and Machines, Vol. A, Academic Press, New York, 1985.
[16] G. Eisenstein, Über eine allgemeine Eigenschaft der Reihenentwicklungen aller algebraischen Funktionen, Berlin. Sitzber. (1852) 441–443.
[17] A. Erdélyi (Ed.), Higher Transcendental Functions, Vol. II, Mc Graw Hill Book Company Inc., New York, 1953.
[18] P. Erdös, P. Turan, On some sequences of integers, J. Lond. Math. Soc. 11 (1936) 261–264.
[19] A. Gertsch, A.M. Robert, Some congruences concerning the Bell numbers, Bull. Belg. Math. Soc. 3 (1996) 467–475.
[20] J.L. Gerver, L.T. Ramsey, Sets of integers with no long arithmetic progressions generated by the greedy algorithm, Math. Comput. 33 (1979) 1353–1359.
[21] F. von Haeseler, A. Petersen, Automaticity of rational functions, Beiträge zur Algebra und Geometrie (Contributions to Algebra and Geometry) 39 (1998) 219–229.
[22] E. Heine, Der Eisensteinsche Satz über Reihen-Entwicklung algebraischer Functionen, J. Reine Angew. Math. 45 (1853) 285–302.
[23] T. Honda, Two congruence properties of Legendre polynomials, Osaka J. Math. 13 (1976) 131–133.
[24] H. Ille, Zur Irreduzibilität der Kugelfunktionen, Jahrbuch der Dissertationen der Universität Berlin, 1924.
[25] K. Jacobs, Ergodic theory and combinatorics, Contemp. Math. 26 (1984) 171–184. (Conference in modern analysis and probability, R. Beals, A. Beck, A. Bellow, A. Hajian (Eds.), AMS, Providence, RI.)
[26] R. Koekoek, R.F. Swarttouw, The Askey-scheme of hypergeometrical polynomials and its q-analogue, Report 94-05, TU Delft, Faculty of Technical Mathematics and Informatics, 1994. [http://www.wins.uva.nl/pub/mathematics/reports/Analysis/aboutothers/AskeyWilson.ps.gz] [ftp://ftp.fwi.uva.nl/pub/mathematics/reports/Analysis/aboutothers/AskeyWilson.ps.gz]
[27] I. Korec, Pascal triangle modulo n and modular trellises, Comput. Artif. Intell. 9 (1990) 105–113.
[28] P.S. Landweber, Supersingular elliptic curves and congruences for Legendre polynomials, in: P.S. Landweber (Ed.), Elliptic Curves and Modular Forms in algebraic Topology, Lecture Notes in Math. Vol. 1326, 1988, Springer, New York, pp. 69–83.

[29] R. McIntosh, A generalization of a congruential property of Lucas, Amer. Math. Monthly 99 (1992) 231–238.
[30] M. Mendès France, Les suites à spectre vide et la répartition modulo 1, J. Number Theory 5 (1973) 1–15.
[31] M. Mendès France, A.J. van der Poorten, From geometry to Euler identities, Theoret. Comput. Sci. 65 (1989) 213–220.
[32] A. Robert, Polynômes de Legendre mod p, Séminaire d'Analyse, Université Blaise Pascal 6 (1990 –1991) 19.01–19.12.
[33] A. Robert, Polynômes de Legendre modulo 4, C. R. Acad. Sci. Paris, Sér. I 316 (1993) 1235–1240.
[34] A. Robert, M. Zuber, The Kazandzidis supercongruences. A simple proof and an application, Rend. Sem. Mat. Univ. Padova 94 (1995) 235–243.
[35] R. Salem, D.C. Spencer, On sets of integers which contain no three terms in arithmetical progression, Proc. Nat. Acad. Sci. 28 (1942) 561–563.
[36] O. Salon, Suites automatiques à multi-indices, Sém. Théor. Nombres Bordeaux, Exposé 4 (1986–1987), 4-01–4-27; followed by an Appendix by J. Shallit, 4-29A–4-36A.
[37] O. Salon, Suites automatiques à multi-indices et algébricité, C. R. Acad. Sci. Paris, Sér. I 305 (1987) 501–504.
[38] J. Wahab, New cases of irreducibility for Legendre polynomials, Duke Math. J. 19 (1952) 165–176.
[39] N. Yui, Jacobi quartics, Legendre polynomials and formal groups, in: P.S. Landweber (Ed.), Elliptic Curves and Modular Forms in Algebraic Topology, Lecture Notes in Math., Vol. 1326, 1988, Springer, New York, pp. 182–215.
[40] M. Zuber, Propriétés p-adiques de polynômes classiques, Thèse, Université de Neuchâtel, 1992.
[41] M. Zuber, Propriétés de congruence de certaines familles classiques de polynômes, C. R. Acad. Sci. Paris, Sér. I 315 (1992) 869–872.
[42] M. Zuber, Une suite récurrente remarquable, C. R. Acad. Sci. Paris, Sér. I 318 (1994) 205–208.
[43] M. Zuber, Suites de Honda, Ann. Math. Blaise Pascal 2 (1995) 307–314.