On vanishing coefficients of algebraic power series over fields of positive characteristic

Boris Adamczewski · Jason P. Bell

Abstract Let K be a field of characteristic $p > 0$ and let $f(t_1, \ldots, t_d)$ be a power series in d variables with coefficients in K that is algebraic over the field of multivariate rational functions $K(t_1, \ldots, t_d)$. We prove a generalization of both Derksen's recent analogue of the Skolem–Mahler–Lech theorem in positive characteristic and a classical theorem of Christol, by showing that the set of indices $(n_1, \ldots, n_d) \in \mathbb{N}^d$ for which the coefficient of $t_1^{n_1} \cdots t_d^{n_d}$ in $f(t_1, \ldots, t_d)$ is zero is a p-automatic set. Applying this result to multivariate rational functions leads to interesting effective results concerning some Diophantine equations related to S-unit equations and more generally to the Mordell–Lang Theorem over fields of positive characteristic.

Contents

B. Adamczewski (✉)
Institut Camille Jordan, CNRS, Université de Lyon, Université Lyon 1, 43 boulevard du 11 novembre 1918, 69622 Villeurbanne Cedex, France
e-mail: Boris.Adamczewski@math.univ-lyon1.fr

J.P. Bell
Department of Mathematics, Simon Fraser University, Burnaby, BC V5A 1S6, Canada
e-mail: jpb@math.sfu.ca

1 Introduction

The Skolem–Mahler–Lech theorem is a celebrated result which describes the
set of solutions in n to the equation $a(n) = 0$, where $a(n)$ is a sequence satis-
fying a linear recurrence over a field of characteristic 0. We recall that if K is
a field and a is a K-valued sequence, then a satisfies a linear recurrence over
K if there exist a natural number m and values $c_1, \ldots, c_m \in K$ such that

$$a(n) = \sum_{i=1}^{m} c_i a(n - i)$$

for all sufficiently large values of n. The zero set of the linear recurrence a is
defined by

$$\mathcal{Z}(a) := \{n \in \mathbb{N} \mid f(n) = 0\}.$$

The Skolem–Mahler–Lech theorem can then be stated as follows.

Theorem 1.1 (Skolem–Mahler–Lech) *Let a be a linear recurrence over a
field of characteristic* 0. *Then the set $\mathcal{Z}(a)$ is a union of a finite set and a
finite number of infinite arithmetic progressions.*

   This result was first proved for linear recurrences over the rational numbers
by Skolem [39]. It was next extended to linear recurrences over the algebraic
numbers by Mahler [28]. The version above was proven first by Lech [26]
and later by Mahler [29, 30]. More details about the history of this theorem
can be found in the book by Everest et al. [13].
   Though the conclusion of the Skolem–Mahler–Lech theorem obviously
holds for linear recurrences defined over finite fields, this is not the case for

infinite fields K of positive characteristic. The simplest counter-example was given by Lech [26]. Throughout this paper, p will denote a prime number. Let $K = \mathbb{F}_p(t)$ be the field of rational functions in one variable over $\mathbb{F}_p$. Let

$$a(n) := (1+t)^n - t^n - 1.$$

We can observe that the sequence a satisfies the recurrence

$$a(n) = (2 + 2t)a(n-1) - (1 + 3t + t^2)a(n-2) + (t + t^2)a(n-3)$$

for $n > 3$, while

$$\mathcal{Z}(a) = \{1, p, p^2, p^3, \ldots\}.$$

More recently, Derksen [10] gave more pathological examples, which show that the correct analogue of the Skolem–Mahler–Lech theorem in positive characteristic is much more subtle. For example, one has

$$\mathcal{Z}(a) = \{p^n \mid n \in \mathbb{N}\} \cup \{p^n + p^m \mid n, m \in \mathbb{N}\},$$

for the linear recurrence a defined over the field $\mathbb{F}_p(x, y, z)$ by

$$a(n) := (x + y + z)^n - (x + y)^n - (x + z)^n - (y + z)^n + x^n + y^n + z^n.$$

Derksen noted that while pathological examples of zero sets of linear recurrences do exist in characteristic p, the base-p expansions of the natural numbers in the zero set are still well behaved. In fact, he proved the remarkable result that the zero set of a linear recurrence can always be described in terms of finite automata [10].

Theorem 1.2 (Derksen) *Let a be a linear recurrence over a field K of characteristic p. Then the set $\mathcal{Z}(a)$ is p-automatic.*

We recall that an infinite sequence a with values in a finite set is said to be p-automatic if $a(n)$ is a finite-state function of the base-p representation of n. Roughly, this means that there exists a finite automaton taking the base-p expansion of n as input and producing the term $a(n)$ as output. A set $\mathcal{E} \subset \mathbb{N}$ is said to be p-automatic if there exists a finite automaton that reads as input the base-p expansion of n and accepts this integer (producing as output the symbol 1) if n belongs to $\mathcal{E}$, otherwise this automaton rejects the integer n, producing as output the symbol 0.

Let us give a formal definition of both notions. Let $k \geq 2$ be a natural number. We let Σ_k denote the alphabet $\{0, 1, \ldots, k-1\}$. A k-automaton is a 6-tuple

$$\mathcal{A} = (Q, \Sigma_k, \delta, q_0, \Delta, \tau),$$

where Q is a finite set of states, $\delta : Q \times \Sigma_k \to Q$ is the transition function, q_0 is the initial state, Δ is the output alphabet and $\tau : Q \to \Delta$ is the output function. For a state q in Q and for a finite word $w = w_1 w_2 \cdots w_n$ on the alphabet Σ_k, we define $\delta(q, w)$ recursively by $\delta(q, w) = \delta(\delta(q, w_1 w_2 \cdots w_{n-1}), w_n)$. Let $n \geq 0$ be an integer and let $w_r w_{r-1} \cdots w_1 w_0$ in $(\Sigma_k)^{r+1}$ be the base-k expansion of n. Thus $n = \sum_{i=0}^{r} w_i k^i := [w_r w_{r-1} \cdots w_0]_k$. We denote by $w(n)$ the word $w_0 w_1 \cdots w_r$.

Definition 1.1 A sequence $(a_n)_{n \geq 0}$ is said to be k-automatic if there exists a k-automaton $\mathcal{A}$ such that $a_n = \tau(\delta(q_0, w(n)))$ for all $n \geq 0$.

Definition 1.2 A set $\mathcal{E} \subset \mathbb{N}$ is said to be recognizable by a finite k-automaton, or for short k-automatic, if the characteristic sequence of $\mathcal{E}$, defined by $a_n = 1$ if $n \in \mathcal{E}$ and $a_n = 0$ otherwise, is a k-automatic sequence.

More generally, feeding a finite automaton with d-tuples of nonnegative integers leads to the notion of p-automatic subsets of $\mathbb{N}^d$. Some background on automata theory, including examples, formal definitions of multidimensional automatic sequences and sets, and their extension to arbitrary finitely generated abelian groups, are given in Sect. 5.

Remark 1.1 Let us make few important remarks.

- In the previous definitions, we chose the convention that the base-k expansion of n is scanned from left to right. Our automata thus read the input starting with the most significant digit. We recall that it is well-known that the class of k-automatic sets or sequences remains unchanged when choosing to read the input starting from the least significant digit (see for instance Chap. V of [12] or Chap. 5 of [2]).
- One could also ask whether the base k plays an important role here. As proved in a fundamental paper of Cobham [7], this is actually the case. Periodic sets, that are sets obtained as a union of a finite set and a finite number of infinite arithmetic progressions, are exactly those that are k-automatic for every integer $k \geq 2$. In addition, an infinite aperiodic k-automatic set is also k^n-automatic for every positive integer n, while it cannot be ℓ-automatic if k and ℓ are two multiplicatively independent integers.
- The class of k-automatic sets is closed under various natural operations such as intersection, union and complement (see for instance Chap. V of [12] or Chap. 5 of [2]).

On the other hand, it is well known that if K is a field and a is a K-valued sequence, then a satisfies a linear recurrence over K if and only if the power

series

$$f(t) = \sum_{n=0}^{\infty} a(n)t^n$$

is the power series expansion of a rational function. For instance, Mahler [28–30] worked with rational power series rather than linear recurrences when proving what we now call the Skolem–Mahler–Lech theorem. Let

$$\mathcal{Z}(f) := \{n \mid a(n) = 0\}.$$

Then Derksen's theorem can be restated as follows: let K be a field of characteristic p and let $f(t) \in K[[t]]$ be a rational function, then the set $\mathcal{Z}(f)$ is p-automatic.

This formulation of Derksen's theorem is in the same spirit as another famous result involving automata theory and known as Christol's theorem [5, 6].

Theorem 1.3 (Christol) *Let q be a positive integer power of p. Then $f(t) = \sum_{n=0}^{\infty} a(n)t^n \in \mathbb{F}_q[[t]]$ is algebraic over $\mathbb{F}_q(t)$ if and only if the sequence a is p-automatic.*

The main aim of this paper is to produce a simultaneous multivariate generalization of both the theorem of Derksen and the theorem of Christol.

Given a multivariate power series

$$f(t_1, \ldots, t_d) = \sum_{(n_1, \ldots, n_d) \in \mathbb{N}^d} a(n_1, \ldots, n_d)t_1^{n_1} \cdots t_d^{n_d} \in K[[t_1, \ldots, t_d]],$$

we define the set of vanishing coefficients of f by

$$\mathcal{Z}(f) = \{(n_1, \ldots, n_d) \in \mathbb{N}^d \mid a(n_1, \ldots, n_d) = 0\}.$$

Our main result reads as follows.

Theorem 1.4 *Let K be a field of characteristic p and let $f(t_1, \ldots, t_d) \in K[[t_1, \ldots, t_d]]$ be a power series that is algebraic over the field of multivariate rational functions $K(t_1, \ldots, t_d)$. Then the set $\mathcal{Z}(f)$ is p-automatic.*

Let us make few comments on this result.

- In the case that $d = 1$ and $f(t)$ is chosen to be the power series expansion of a rational function in Theorem 1.4, we immediately obtain Derksen's theorem (Theorem 1.2). We do not obtain his finer characterization, but, as explained in Sect. 9, it is not possible to obtain a significantly improved characterization of zero sets even for multivariate rational power series.

- In the case that $d = 1$ and K is chosen to be a finite field in Theorem 1.4, we cover the more difficult direction of Christol's theorem (Theorem 1.3). Indeed, if $f(t) = \sum_{n=0}^{\infty} a(n)t^n \in K[[t]]$ is an algebraic power series, then for each $x \in K$ the function $f(t) - x/(1-t)$ is algebraic. Theorem 1.4 thus implies that the set $\{n \in \mathbb{N} \mid a(n) = x\}$ is p-automatic for all $x \in K$. This immediately implies that the sequence a is p-automatic.
- Theorem 1.4 can actually take a stronger form. Let $\mathcal{E} \subset \mathbb{N}^d$. The following conditions are equivalent.

  (i) The set $\mathcal{E}$ is p-automatic.
  (ii) $\mathcal{E} = \mathcal{Z}(f)$ for some algebraic power series with coefficients over a field of characteristic p.

  Indeed, it is known [35] that given a p-automatic set $\mathcal{E} \subset \mathbb{N}^d$, the formal power series

  $$f(t_1, \ldots, t_d) = \sum_{(n_1, \ldots, n_d) \in \mathcal{E}} t_1^{n_1} \cdots t_d^{n_d}$$

  is algebraic over $\mathbb{F}_p(t_1, \ldots, t_d)$. From the latter property and Theorem 1.4, we also deduce the following result. Let K be a field of characteristic p and let

  $$f(t_1, \ldots, t_d) = \sum_{(n_1, \ldots, n_d) \in \mathbb{N}^d} a(n_1, \ldots, n_d) t_1^{n_1} \cdots t_d^{n_d} \in K[[t_1, \ldots, t_d]]$$

  be a power series that is algebraic over the field of multivariate rational functions $K(t_1, \ldots, t_d)$. For $x \in K$, let

  $$a^{-1}(x) := \{(n_1, \ldots, n_d) \in \mathbb{N}^d \mid a(n_1, \ldots, n_d) = x\}.$$

  Then for every $x \in K$ the formal power series

  $$f_x(t_1, \ldots, t_d) := \sum_{(n_1, \ldots, n_d) \in a^{-1}(x)} t_1^{n_1} \cdots t_d^{n_d}$$

  is also algebraic. In the particular case where K is a finite field, this result was first proved by Furstenberg [18] (see also the more recent result of Kedlaya [24] for a generalization to Hahn's power series with coefficients in a finite field).
- No such multivariate generalization of the Skolem–Mahler–Lech theorem exists in characteristic 0. For example, if one takes the rational bivariate power series

  $$f(x, y) = \sum_{n,m} (n^3 - 2^m) x^n y^m \in \mathbb{Q}[[x, y]],$$

then $\mathcal{Z}(f) = \{(n, m) \mid m \equiv 0 \pmod{3}, n = 2^{m/3}\}$. This shows that there is no natural way to express the set of vanishing coefficients of f in terms of more general arithmetic progressions or in terms of automatic sets. In fact, finding zero sets of coefficients of multivariate rational power series with integer coefficients is often equivalent to very difficult classes of Diophantine problems which cannot be solved at this moment, such as for instance finding an effective procedure to solve all S-unit equations (see Sect. 3 for more details). In Sect. 2, we also give a Diophantine problem related to linear recurrences which is conjectured in [4] to be undecidable and, as shown in the proof of Theorem 2.1, which is equivalent to describe the zero sets of coefficients of a class of simple mutivariate rational power series with integer coefficients.

Our proof of Theorem 1.4 involves using methods of Derksen as well as more advanced techniques from automata theory reminiscent of works of Christol [5, 6], Denef and Lipshitz [9], Harase [21], Sharif and Woodcock [38] among others. We first consider the action of a certain infinite semigroup on the ring of power series over a field of characteristic p. We use the fact that algebraic power series have a finite orbit under the action of this semigroup to apply Derksen's "Frobenius splitting" technique which allows us to show that the set of vanishing coefficients is necessarily p-automatic. An especially important aspect of the proof of Theorem 1.2 is that each step can be made effective. We prove that this is also the case with Theorem 1.4.

Theorem 1.5 *Let K be a field of positive characteristic and let $f(t_1, \ldots, t_d) \in K[[t_1, \ldots, t_d]]$ be a power series that is algebraic over the field of multivariate rational functions $K(t_1, \ldots, t_d)$. Then the set $\mathcal{Z}(f)$ can be effectively determined. Furthermore, the following properties are decidable.*

(i) *The set $\mathcal{Z}(f)$ is empty.*
(ii) *The set $\mathcal{Z}(f)$ is finite.*
(iii) *The set $\mathcal{Z}(f)$ is periodic, that is, formed by the union of a finite set and of a finite number of (d-dimensional) arithmetic progressions.*

In particular, when $\mathcal{Z}(f)$ is finite, one can determine (in a finite amount of time) all its elements.

Remark 1.2 When we say that the set $\mathcal{Z}(f)$ can be effectively determined, this means that there is an algorithm that produces a p-automaton that generates $\mathcal{Z}(f)$ in a finite amount of time. Furthermore, there exists an algorithm that allows one to determine in a finite amount of time whether or not $\mathcal{Z}(f)$ is empty, finite, or periodic.

As we will illustrate in Sects. 2, 3 and 4, applying Theorem 1.5 to multivariate rational functions actually leads to interesting effective results con-

cerning some Diophantine equations related to *S*-unit equations and more generally to the Mordell–Lang Theorem over fields of positive characteristic.

The outline of this paper is as follows. Our Diophantine applications are discussed in Sects. 2, 3 and 4. In Sect. 5, we recall some basic background on automata theory. We define in particular the notion of automatic sets of $\mathbb{N}^d$ and more generally of automatic subsets of finitely generated abelian groups. The latter notion does not appear to have been introduced earlier and may be of independent interest. In Sect. 6, we prove Theorem 1.4. In Sects. 7 and 8, we make the proof of Theorem 1.4 effective, proving Theorem 1.5. Finally, we conclude our paper with some comments in Sect. 9.

2 Linear recurrences and decidability

There are many different proofs and extensions of the Skolem–Mahler–Lech theorem in the literature (see for instance [3, 13, 20, 33]). These proofs all use *p*-adic methods in some way, although the result is valid in any field of characteristic 0. This seems to be responsible for a well-known deficiency of the Skolem–Mahler–Lech theorem: all known proofs are ineffective. This means that we do not know any algorithm that allows us to determine the set $\mathcal{Z}(a)$ for a given linear recurrence $a(n)$ defined over a field of characteristic 0. We refer the reader to [13] and to the recent discussion in [40] for more details. It is actually still unknown whether the fact that $\mathcal{Z}(a)$ is empty or not is decidable. In fact, it seems unclear that one should even expect it to be decidable. In this direction, let us recall the following conjecture from [4]. Given linear recurrences $a_1(n), \ldots, a_d(n)$ over a field K, we let

$$\mathcal{Z}(a_1, \ldots, a_d) := \left\{ (n_1, \ldots, n_d) \in \mathbb{N}^d \mid a_1(n_1) + \cdots + a_d(n_d) = 0 \right\}.$$

It was conjectured in [4] that, if $K = \mathbb{Q}$, the property

$$\mathcal{Z}(a_1, \ldots, a_d) \neq \emptyset$$

is undecidable for every positive integer *d* large enough.

As mentioned in the introduction, the situation is drastically different for fields of positive characteristic. Indeed, Derksen [10] proved that each step of the proof of Theorem 1.2 can be made effective. In particular, there exists an algorithm that allows one to decide whether the set $\mathcal{Z}(a)$ is empty or not in a finite amount of time. We give below a generalization of Derksen's theorem to an arbitrary number of linear recurrences. It well illustrates the relevance of Theorem 1.5.

Theorem 2.1 *Let K be a field of characteristic p, d a positive integer, and let $a_1(n), \ldots, a_d(n)$ be linear recurrences over K. Then $\mathcal{Z}(a_1, \ldots, a_d)$ is a*

p-automatic set that can be effectively determined. In particular, the property

$$\mathcal{Z}(a_1, \ldots, a_d) \neq \emptyset$$

is decidable.

Note that, in addition, we can decide whether such a set $\mathcal{Z}(a_1, \ldots, a_d)$ is finite or periodic.

Proof In view of Theorem 1.5, it suffices to prove that there exists an explicit multivariate rational function $f(t_1, \ldots, t_d) \in K(t_1, \ldots, t_d)$ such that $\mathcal{Z}(f) = \mathcal{Z}(a_1, \ldots, a_d)$.

Let $i \in \{1, \ldots, d\}$. Since a_i is a linear recurrence over K, we have that $f_i(t) := \sum_{n \geq 0} a_i(n) t^n$ is a rational function. Thus,

$$f(t_1, \ldots, t_d) := \sum_{i=1}^{d} \left(f_i(t_i) \cdot \prod_{j \neq i} \frac{1}{1 - t_j} \right)$$

is a multivariate rational function in $K(t_1, \ldots, t_d)$. Furthermore, this definition implies that

$$f(t_1, \ldots, t_d) = \sum_{(n_1, \ldots, n_d) \in \mathbb{N}^d} \left(a_1(n_1) + \cdots + a_d(n_d) \right) t_1^{n_1} \cdots t_d^{n_d}.$$

We thus deduce that $\mathcal{Z}(f) = \mathcal{Z}(a_1, \ldots, a_d)$. This ends the proof. $\square$

3 Linear equations over multiplicative groups

In this section, we discuss some Diophantine equations that generalize the famous S-unit equations (see for instance the survey [15]). More precisely, given a field K and a finitely generated subgroup Γ of K^*, we consider linear equations of the form

$$c_1 X_1 + \cdots + c_d X_d = 1, \tag{3.1}$$

where $c_1, \ldots, c_d$ belong to K and where we look for solutions in Γ^d.

These equations have a long history. Let S be a finite number of prime numbers and $\Gamma \subseteq \mathbb{Q}^*$ the multiplicative group generated by the elements of S. In 1933, Mahler [27] proved that for all nonzero rational numbers a and b the equation

$$aX + bY = 1 \tag{3.2}$$

has only a finite number of solutions in Γ^2. Lang [25] later generalized this result by proving that for all a and b belonging to $\mathbb{C}^*$ and all subgroups of finite rank Γ of $\mathbb{C}^*$, (3.2) has only a finite number of solutions in Γ^2. Furthermore, in the case where Γ is a subgroup of $\mathbb{Q}^*$, there exists an effective method based on the theory of linear forms of logarithms to determine all solutions of (3.2).

When the number of variables d is larger than 2, one can no longer expect that (3.1) necessarily has only a finite number of solutions. However, the subspace theorem can be used to prove that such an equation has only a finite number of nondegenerate solutions; that is, solutions with the property that no proper subsum vanishes [14, 34]. Furthermore, it is possible to use some quantitative version of the subspace theorem to bound the number of nondegenerate solutions. In this direction, the following general and very strong result was obtained by Evertse, Schlickewei and W.M. Schmidt [16]: given K a field of characteristic 0 and Γ a multiplicative subgroup of rank r of K^*, (3.1) has at most $\exp((6d)^{3d}(r+1))$ nondegenerate solutions. However, all general known results concerning more than two variables are ineffective.

The situation in characteristic p is similar to the one encountered with the Skolem–Mahler–Lech theorem. The Frobenius endomorphism may be responsible for the existence of "pathological solutions". Indeed, it is easy to check that, for every positive integer q that is a power of p, the pair $(t^q, (1-t)^q)$ is a solution of the equation

$$X + Y = 1$$

in Γ^2, where Γ is the multiplicative subgroup of $\mathbb{F}_p(t)^*$ generated by t and $1-t$. In fact, if we take $K = \mathbb{F}_p(t)$ and $\Gamma = \langle t, (1-t) \rangle$, we can find more sophisticated examples. As observed in [31], the equation

$$X + Y - Z = 1$$

has for every pair of positive integer (n, m) the nondegenerated solution

$$X = t^{(p^n-1)p^m}, \qquad Y = (1-t)^{p^{n+m}}, \qquad Z = t^{(p^n-1)p^m}(1-t)^{p^m}.$$

Thus, there is no hope to obtain in this framework results similar to those mentioned previously. Concerning (3.2), Voloch [41] gave interesting results. He obtained, in particular, conditions that ensure the finiteness of the number of solutions (with explicit bounds for the number of solutions). Masser [31] obtained a result concerning the structure of the solutions of the general equation (3.1). His aim was actually to prove a conjecture of K. Schmidt concerning mixing properties of algebraic $\mathbb{Z}^d$-actions (see [31, 36, 37] for more details on this problem).

As a consequence of Theorem 1.5, we are able to give a satisfactory effective solution to the general equation (3.1) over fields of positive characteristic, proving that the set of solutions is p-automatic in a natural sense. We note that the notion of an automatic subset of a finitely generated abelian group is given in Sect. 5 (see Definition 5.9 and Proposition 5.4).

Theorem 3.1 *Let K be a field of characteristic p, let $c_1, \ldots, c_d \in K^*$, and let Γ be a finitely generated multiplicative subgroup of K^*. Then the set of solutions in Γ^d of the equation*

$$c_1 X_1 + \cdots + c_d X_d = 1$$

is a p-automatic subset of Γ^d that can be effectively determined.

Proof Let

$$S := \left\{ (x_1, \ldots, x_d) \in \Gamma^d \mid c_1 x_1 + \cdots + c_d x_d = 1 \right\}.$$

Our aim is to prove that S is p-automatic and can be effectively determined.

We first fix some notation. Let $g_1, \ldots, g_m$ be a set of generators of Γ and let us consider a surjective group homomorphism $\Phi : \mathbb{Z}^m \to \Gamma$. This allows us to define a surjective group homomorphism $\tilde{\Phi} : (\mathbb{Z}^m)^d \to \Gamma^d$ by $\tilde{\Phi}(\mathbf{x}_1, \ldots, \mathbf{x}_d) = (\Phi(\mathbf{x}_1), \ldots, \Phi(\mathbf{x}_d))$. By Proposition 5.3, it is enough to show that $\tilde{\Phi}^{-1}(S)$ is a p-automatic subset of $(\mathbb{Z}^m)^d \simeq \mathbb{Z}^{m \times d}$. Let $\mathcal{E} := \{\pm 1\}^m$. Given $\mathbf{n} := (n_1, \ldots, n_m) \in \mathbb{N}^m$ and $\mathbf{a} := (a_1, \ldots, a_m) \in \mathcal{E}$, we let $\mathbf{a} \cdot \mathbf{n} := (a_1 n_1, \ldots, a_m n_m)$ denote the ordinary coordinate-wise multiplication. Given $A \subseteq \mathbb{N}^m$, we also set $\mathbf{a} \cdot A := \{\mathbf{a} \cdot \mathbf{n} \mid \mathbf{n} \in A\}$. For every $\mathbf{a} := (\mathbf{a}_1, \ldots, \mathbf{a}_d) \in \mathcal{E}^d$, we set

$$S_{\mathbf{a}} := \left\{ (\mathbf{n}_1, \ldots, \mathbf{n}_d) \in \mathbb{N}^{m \times d} \mid c_1 \Phi(\mathbf{a}_1 \cdot \mathbf{n}_1) + \cdots + c_d \Phi(\mathbf{a}_d \cdot \mathbf{n}_d) = 1 \right\}.$$

Thus

$$\tilde{\Phi}^{-1}(S) = \bigcup_{\mathbf{a} \in \mathcal{E}^d} \mathbf{a} \cdot S_{\mathbf{a}}. \tag{3.3}$$

Note that by Proposition 5.1, S is p-automatic subset of Γ^d if and only if $S_{\mathbf{a}}$ is a p-automatic subset of $\mathbb{N}^d$ for every $\mathbf{a} \in \mathcal{E}^d$.

We let $t_{i,j}$ be indeterminates for $1 \leq i \leq d$ and $1 \leq j \leq m$. We define $\mathbf{t}_i = (t_{i,1}, \ldots, t_{i,m})$ for $1 \leq i \leq d$. Given $\mathbf{n} \in \mathbb{N}^m$ and $i \in \{1, 2, \ldots, d\}$, we define $\mathbf{t}_i^{\mathbf{n}}$ to be the product $t_{i,1}^{n_1} \cdots t_{i,m}^{n_m}$. Given $\mathbf{a} := (\mathbf{a}_1, \ldots, \mathbf{a}_d) \in \mathcal{E}^d$, we define the function

$$f_{\mathbf{a}}(\mathbf{t}_1, \ldots, \mathbf{t}_d) := \sum_{\mathbf{n}_1, \ldots, \mathbf{n}_d \in \mathbb{N}^m} \left(-1 + \sum_{i=1}^{d} c_i \Phi(\mathbf{a}_i \cdot \mathbf{n}_i) \right) \mathbf{t}_1^{\mathbf{n}_1} \cdots \mathbf{t}_d^{\mathbf{n}_d}.$$

This definition ensures that

$$S_{\mathbf{a}} = \mathcal{Z}(f_{\mathbf{a}}). \tag{3.4}$$

For every $i \in \{1, 2, \ldots, d\}$, we also set $\mathbf{n}_i = (n_{i,1}, \ldots, n_{i,m})$ and $\mathbf{a}_i := (a_{i,1}, \ldots, a_{i,m})$. Let $\mathbf{e}_j = (0, 0, \ldots, 0, 1, 0, \ldots, 0) \in \mathbb{Z}^m$ denote the element whose jth coordinate is 1 and whose other coordinates are 0. Then for every $i \in \{1, \ldots, d\}$, we have

$$\sum_{\mathbf{n}_i \in \mathbb{N}^m} c_i \Phi(\mathbf{a}_i \cdot \mathbf{n}_i) \mathbf{t}_i^{\mathbf{n}_i} = \sum_{n_{i,1}=0}^{\infty} \cdots \sum_{n_{i,m}=0}^{\infty} \prod_{j=1}^{m} \Phi(\mathbf{e}_j)^{a_{i,j} n_{i,j}} t_{i,j}^{n_{i,j}}$$

$$= \prod_{j=1}^{m} \left(1 - \Phi(\mathbf{e}_j)^{a_{i,j}} t_{i,j}\right)^{-1}$$

is a rational function. Hence

$$f_{\mathbf{a}}(\mathbf{t}_1, \ldots, \mathbf{t}_d) = \prod_{i=1}^{d} \prod_{j=1}^{m} (1 - t_{i,j})^{-1} \left(-1 + \sum_{i=1}^{d} c_i \prod_{j=1}^{m} \frac{(1 - t_{i,j})}{(1 - \Phi(\mathbf{e}_j)^{a_{i,j}} t_{i,j})}\right)$$

is a rational function for each $\mathbf{a} \in \mathcal{E}^d$. Since we get an explicit expression for the function $f_{\mathbf{a}}$ (assuming that we explicitly know a set of generators $g_1, \ldots, g_m$ of Γ), we infer from Theorem 1.5 that the set $\mathcal{Z}(f_{\mathbf{a}})$ is a p-automatic subset of $\mathbb{N}^d$ which can be effectively determined. By (3.3) and (3.4), this ends the proof.   □

4 An effective result related to the Mordell–Lang theorem

The expression "Mordell–Lang theorem" or "Mordell–Lang conjecture" serves as a generic appellation which denotes results describing the structure of intersections of the form

$$X \cap \Gamma,$$

where X is a subvariety (Zariski closed subset) of a (affine, abelian, or semi-abelian) variety A and Γ is a finitely generated subgroup (or even a subgroup of finite rank) of A. The case where the variety A is defined over a field of characteristic 0 has many interesting Diophantine consequences, including the famous Faltings' theorem [17].

On the other hand, simple examples constructed using the Frobenius endomorphism (as in Sect. 3) show that such intersections may behave differently when the variety A is defined over a field of positive characteristic.

Hrushovski [23] proved a relative version of the Mordell–Lang conjecture for semi-abelian varieties defined over a field K of positive characteristic. His approach, which makes use of model theory, has then been pursued by several authors (see for instance [19, 32]).

All general results known up to now in this direction seem to be ineffective. The aim of this section is to prove the two following effective statements. We recall that the notion of an automatic subset of a finitely generated abelian group is given in Sect. 5 (see Definition 5.9 and Proposition 5.4).

Theorem 4.1 *Let K be a field of characteristic p and let d be a positive integer. Let X be a Zariski closed subset of $\mathrm{GL}_d(K)$ and Γ a finitely generated abelian subgroup of $\mathrm{GL}_d(K)$. Then the set $X \cap \Gamma$ is a p-automatic subset of Γ that can be effectively determined.*

Note more generally that, given positive integers $d_1, \ldots, d_n$, the same result holds for Zariski closed subsets of $\prod_{i=1}^n \mathrm{GL}_{d_i}(K)$. Indeed, we have a natural embedding β of $\prod_{i=1}^n \mathrm{GL}_{d_i}(K)$ as a Zariski closed subset of $\mathrm{GL}_{d_1+\cdots+d_n}(K)$, where β sends an n-tuple of invertible matrices in which the ith matrix has size $d_i \times d_i$ to the block diagonal matrix with n blocks whose ith block is the ith coordinate of our n-tuple. Indeed, under this identification, $\prod_{i=1}^n \mathrm{GL}_{d_i}(K)$ is the zero set of the linear polynomials $x_{i,j}$ for which i and j have the property that there does not exist a positive integer k, $k \leq n$, such that

$$d_0 + \cdots + d_{k-1} < i, j \leq d_1 + \cdots + d_k,$$

where we take d_0 to be zero. Given a Zariski closed subset X of $\prod_{i=1}^n \mathrm{GL}_{d_i}(K)$, we thus may regard X as a Zariski closed subset of $\mathrm{GL}_{d_1+\cdots+d_n}(K)$. We note that the additive torus embeds in $\mathrm{GL}_2(K)$ by identifying the torus with unipotent upper-triangular matrices. Moreover, this is easily seen to be a Zariski closed subset of $\mathrm{GL}_2(K)$. Applying these remarks with $d_1, \ldots, d_n \in \{1, 2\}$, we deduce the following corollary.

Corollary 4.1 *Let K be a field of characteristic p and let s and t be non-negative integers. Let X be a subvariety of $\mathrm{G}_a^s(K) \times \mathrm{G}_m^t(K)$ and Γ a finitely generated subgroup of $\mathrm{G}_a^s(K) \times \mathrm{G}_m^t(K)$. Then the set $X \cap \Gamma$ is a p-automatic subset of Γ that can be effectively determined.*

We note that one can actually obtain an ineffective version of Theorem 4.1 from Corollary 4.1. In fact, one only needs to consider multiplicative tori. To see this, we observe that if Γ is a finitely generated abelian subgroup of $\mathrm{GL}_d(K)$, then by considering Jordan forms, there is some natural number n such that g^{p^n} is diagonalizable for every $g \in \Gamma$. As commuting diagonalizable operators are simultaneously diagonalizable, we may replace K by

a finite extension K' that contains the eigenvalues of g^{p^n} as g ranges over a generating set, and assume that Γ^{p^n} is a subgroup of $T \cong G_m^d(K')$, the invertible diagonal matrices in $GL_d(K')$. As $X \cap T$ is Zariski closed in T and $X \cap \Gamma^{p^n} = (X \cap T) \cap \Gamma^{p^n}$, Corollary 4.1 applies and so $\Gamma^{p^n} \cap X$ is p-automatic. By applying a suitable translate, it follows that the intersection of X with each coset of Γ / Γ^{p^n} is p-automatic. As there are only finitely many cosets, using basic properties of automaticity, we deduce that $\Gamma \cap X$ is p-automatic.

It is however less clear whether an effective version of Theorem 4.1 can be obtained from Corollary 4.1. Indeed, to determine the intersection using the method described above in practice, one must be able to explicitly find eigenvectors in order to diagonalize elements of Γ^{p^n}. A necessary step in doing this is to find roots of characteristic polynomials in the algebraic closure of K, which seems uneasy to be done explicitly in general.

It is also natural to ask whether a similar version of Theorem 4.1 might hold for abelian varieties. We believe this to be the case, but it is not clear whether the result follows from our approach: if P is a point on an abelian variety X over a field of positive characteristic then the points $n \cdot P$ do not appear, in general, to be sufficiently well-behaved to allow one to associate an algebraic generating function, which is necessary to apply our methods.

Proof of Theorem 4.1 We first make a few reductions. We let $\Phi : GL_d(K) \to \mathbb{A}^{d^2}(K)$ be the injective morphism whose image, Y, consists of all points at which the determinant does not vanish. Note that the affine variety $GL_d(K)$ is a Zariski open subset of $\mathbb{A}^{d^2}(K)$ and that the Zariski closed subsets of $GL_d(K)$ are precisely those obtained by intersecting Zariski closed subsets of $\mathbb{A}^{d^2}(K)$ with $GL_d(K)$. By the Hilbert Basis Theorem, a Zariski closed subset of $\mathbb{A}^{d^2}(K)$ is given by the vanishing set of a finite set of polynomials. Thus there are polynomials $P_1, \ldots, P_r \in K[x_{1,1}, \ldots, x_{d,d}]$ such that for $M \in GL_d(K)$,

$$M \in X \quad \Longleftrightarrow \quad P_1\big(\Phi(M)\big) = \cdots = P_r\big(\Phi(M)\big) = 0.$$

It is then enough to consider the case that $\Phi(X) = Z(P) \cap Y$, where P is a single polynomial in the indeterminates $x_{i,j}$ with $1 \le i, j \le d$ and $Z(P)$ denotes the set of zeros of P.

Let Γ be a finitely generated abelian subgroup of $GL_d(K)$ and let X be a Zariski closed subset of $GL_d(K)$ such that $\Phi(X) = Z(P) \cap Y$, where $P \in K[x_{1,1}, \ldots, x_{d,d}]$. Our aim is to prove that $X \cap \Gamma$ is a p-automatic subset of Γ. Let $C_1, \ldots, C_m \in GL_d(K)$ be generators of Γ and suppose that $\Psi : \mathbb{Z}^m \to \Gamma$ is the surjective group homomorphism defined by $\Psi(e_i) = C_i$ for $1 \le i \le m$, where e_i stands for the vector whose ith coordinate is 1 and all

other coordinates are 0. We let $\mathbf{n}$ denote an m-tuple $(n_1, \ldots, n_m) \in \mathbb{N}^m$. By Proposition 5.3, $X \cap \Gamma$ is p-automatic if

$$S := \left\{ \mathbf{n} \in \mathbb{Z}^m \mid P\big(\Phi \circ \Psi(\mathbf{n})\big) = 0 \right\}$$

is a p-automatic subset of $\mathbb{Z}^m$. Let $\mathcal{E} := \{\pm 1\}^m$. Given $\mathbf{n} := (n_1, \ldots, n_m) \in \mathbb{N}^m$ and $\mathbf{a} := (a_1, \ldots, a_m) \in \mathcal{E}$, we denote by $\mathbf{a} \cdot \mathbf{n} := (a_1 n_1, \ldots, a_m n_m)$ the ordinary coordinate-wise multiplication. Given $A \subseteq \mathbb{N}^m$, we also set $\mathbf{a} \cdot A := \{\mathbf{a} \cdot \mathbf{n} \mid \mathbf{n} \in A\}$. For every $\mathbf{a} \in \mathcal{E}$, we set

$$S_{\mathbf{a}} := \left\{ \mathbf{n} \in \mathbb{N}^m \mid P\big(\Phi \circ \Psi(\mathbf{a} \cdot \mathbf{n})\big) = 0 \right\}.$$

Note that by Proposition 5.1, S is a p-automatic subset of $\mathbb{Z}^m$ if and only if $S_{\mathbf{a}}$ is a p-automatic subset of $\mathbb{N}^m$ for every $\mathbf{a} \in \mathcal{E}$.

To see this, let t_j be indeterminates for $1 \leq j \leq m$. Given $\mathbf{n} \in \mathbb{N}^m$, we define $\mathbf{t}^{\mathbf{n}}$ to be the product $t_1^{n_1} \cdots t_m^{n_m}$. Let $\mathbf{a} = (a_1, \ldots, a_m) \in \mathcal{E}$. We set

$$f_{\mathbf{a}}(\mathbf{t}) := \sum_{\mathbf{n} \in \mathbb{N}^m} \Psi(\mathbf{a} \cdot \mathbf{n}) \mathbf{t}^{\mathbf{n}} \in \mathrm{GL}_d(K)[[\mathbf{t}]].$$

We claim that for $1 \leq i, j \leq d$, the (i, j) entry of $\Psi(\mathbf{a} \cdot \mathbf{n})\mathbf{t}^{\mathbf{n}}$ is a rational function in $\mathbf{t}$. To see this, first note that since $C_1, \ldots, C_m$ commute, we have

$$f_{\mathbf{a}}(\mathbf{t}) = \sum_{(n_1, \ldots, n_m) \in \mathbb{N}^m} C_1^{a_1 n_1} \cdots C_m^{a_m n_m} t_1^{n_1} \cdots t_m^{n_m}$$

$$= \prod_{i=1}^{m} \sum_{n_i \in \mathbb{N}} C_i^{a_i n_i} t_i^{n_i}.$$

On the other hand, for every $i \in \{1, \ldots, m\}$, the sum

$$\sum_{n_i \in \mathbb{N}} C_i^{a_i n_i} t_i^{n_i}$$

is a $d \times d$ matrix whose entries are rational functions that belong to $K(t_i)$. This follows for instance from Proposition 1.1 in [20]. Since rational functions are closed under Hadamard product and taking linear combinations, we obtain that $f_{\mathbf{a}}(\mathbf{t})$ is a $d \times d$ matrix whose entries are all multivariate rational functions in $\mathbf{t}$. For all $1 \leq i, j \leq d$, let us denote by $f_{i,j,\mathbf{a}}(\mathbf{t})$ the (i, j) entry of $f_{\mathbf{a}}(\mathbf{t})$. Note that the power series

$$\tilde{f}_{\mathbf{a}}(\mathbf{t}) := \sum_{\mathbf{n} \in \mathbb{N}^m} P(\Phi \circ \Psi(\mathbf{a} \cdot \mathbf{n})) \mathbf{t}^{\mathbf{n}}$$

can be obtained by taking Hadamard product and linear combinations of the rational functions $f_{i,j,\mathbf{a}}(\mathbf{t})$. We thus deduce that $\tilde{f}_{\mathbf{a}}(\mathbf{t})$ belongs to the field of multivariate rational functions $K(\mathbf{t})$. On the other hand, the definition of $\tilde{f}_{\mathbf{a}}$ implies that

$$S_{\mathbf{a}} = \mathcal{Z}(\tilde{f}_{\mathbf{a}}).$$

By Theorem 1.5, we have that the set $S_{\mathbf{a}}$ is a p-automatic set that can be effectively determined. Since this holds true for every $\mathbf{a} \in \mathcal{E}$, this ends the proof. □

5 Background from automata theory

We start this section with few examples of automatic sequences and automatic subsets of the natural numbers, as well as a useful characterization of them (Theorem 5.1). Then we describe Salon's [35] extension of the notion of automatic sets to subsets of $\mathbb{N}^d$ and show how to generalize it to subsets of $\mathbb{Z}^d$. Finally, we introduce a natural notion of automaticity for subsets of arbitrary finitely generated abelian groups. It seems that the latter notion has not been considered before and that it could be of independent interest.

Let $k \geq 2$ be a natural number. We let Σ_k denote the alphabet $\{0, 1, \ldots, k-1\}$.

5.1 Automatic sequences and one-dimensional automatic sets

For reader's convenience we choose to recall here the definitions of a k-automatic sequence and a k-automatic subset of the natural numbers.

A k-automaton is a 6-tuple

$$\mathcal{A} = (Q, \Sigma_k, \delta, q_0, \Delta, \tau),$$

where Q is a finite set of states, $\delta : Q \times \Sigma_k \to Q$ is the transition function, q_0 is the initial state, Δ is the output alphabet and $\tau : Q \to \Delta$ is the output function. For a state q in Q and for a finite word $w = w_1 w_2 \cdots w_n$ on the alphabet Σ_k, we define $\delta(q, w)$ recursively by $\delta(q, w) = \delta(\delta(q, w_1 w_2 \cdots w_{n-1}), w_n)$. Let $n \geq 0$ be an integer and let $w_r w_{r-1} \cdots w_1 w_0$ in $(\Sigma_k)^{r+1}$ be the base-k expansion of n. Thus $n = \sum_{i=0}^{r} w_i k^i :=$ $[w_r w_{r-1} \cdots w_0]_k$. We denote by $w(n)$ the word $w_0 w_1 \cdots w_r$. A sequence $(a_n)_{n \geq 0}$ is said to be k-automatic if there exists a k-automaton $\mathcal{A}$ such that $a_n = \tau(\delta(q_0, w(n)))$ for all $n \geq 0$. A set $\mathcal{E} \subset \mathbb{N}$ is said to be recognizable by a finite k-automaton, or for short k-automatic, if the characteristic sequence of $\mathcal{E}$, defined by $a_n = 1$ if $n \in \mathcal{E}$ and $a_n = 0$ otherwise, is a k-automatic sequence.

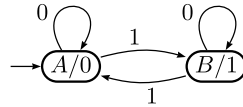**Fig. 1** A 2-automaton generating the Thue–Morse sequence

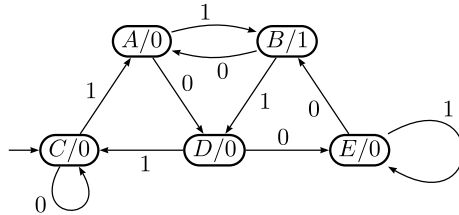**Fig. 2** A 2-automaton recognizing the arithmetic progression $5\mathbb{N} + 3$

Fig. 3 A 2-automaton recognizing the powers of 2
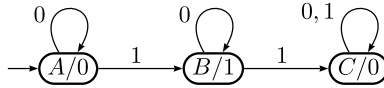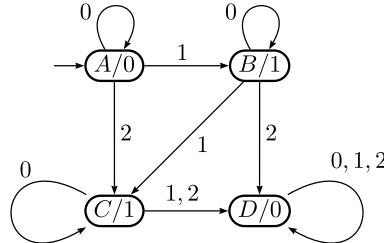
Fig. 4 A 3-automaton recognizing those integers that are the sum of at most two powers of 3

Example 5.1 The Thue–Morse sequence $t := (t_n)_{n \geq 0}$ is probably the famous example of automatic sequences. It is defined as follows: $t_n = 0$ if the sum of the binary digits of n is even, and $t_n = 1$ otherwise. The Thue–Morse sequence can be generated by the following finite 2-automaton (see Fig. 1): $\mathcal{A} = (\{A, B\}, \{0, 1\}, \delta, A, \{0, 1\}, \tau)$, where $\delta(A, 0) = \delta(B, 1) = A$, $\delta(A, 1) = \delta(B, 0) = B$, $\tau(A) = 0$ and $\tau(B) = 1$.

Example 5.2 The simplest automatic sets are arithmetic progressions (see Fig. 2).

Example 5.3 The set $\{1, 2, 4, 8, 16, \ldots\}$ formed by the powers of 2 is also a typical example of a 2-automatic set (see Fig. 3).

Example 5.4 In the same spirit, the set formed by taking all integers that can be expressed as the sum of at most two powers of 3 is 3-automatic (see Fig. 4).

There are also much stranger automatic sets. The fact that the class of k-automatic sets is closed under various natural operations such as intersection, union and complement, can actually be used to easily construct rather

sophisticated automatic sets. For instance, the set of integers whose binary expansion has an odd number of digits, does not contain three consecutive 1's, and contains an even number of two consecutive 0's is a 2-automatic set.

An important notion in the study of k-automatic sequences is the notion of k-kernel.

Definition 5.1 The k-kernel of a sequence $a = (a_n)_{n \geq 0}$ is defined as the set

$$\left\{ (a_{k^i n + j})_{n \geq 0} \mid i \geq 0, \, 0 \leq j < k^i \right\}.$$

Example 5.5 The 2-kernel of the Thue–Morse sequence t has only two elements t and the sequence $\bar{t}$ obtained by exchanging the symbols 0 and 1 in t.

This notion gives rise to a useful characterization of k-automatic sequences which was first proved by Eilenberg in [12].

Theorem 5.1 (Eilenberg) *A sequence is k-automatic if and only if its k-kernel is finite.*

5.2 Automatic subsets of $\mathbb{N}^d$ and multidimensional automatic sequences

Salon [35] extended the notion of automatic sets to include subsets of $\mathbb{N}^d$, where $d \geq 1$. To do this, we consider an automaton

$$\mathcal{A} = \left(Q, \Sigma_k^d, \delta, q_0, \Delta, \tau \right),$$

where Q is a finite set of states, $\delta : Q \times \Sigma_k^d \to Q$ is the transition function, q_0 is the initial state, Δ is the output alphabet and $\tau : Q \to \Delta$ is the output function. Just as in the one-dimensional case, for a state q in Q and for a finite word $w = w_1 w_2 \cdots w_n$ on the alphabet Σ_k^d, we recursively define $\delta(q, w)$ by $\delta(q, w) = \delta(\delta(q, w_1 w_2 \cdots w_{n-1}), w_n)$. We call such an automaton a d-dimensional k-automaton.

We identify $(\Sigma_k^d)^*$ with the subset of $(\Sigma_k^*)^d$ consisting of all d-tuples $(u_1, \ldots, u_d)$ such that $u_1, \ldots, u_d$ all have the same length. Each nonnegative integer n can be written uniquely as

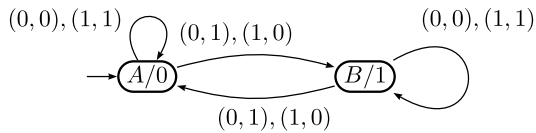$$n = \sum_{j=0}^{\infty} e_j(n) k^j,$$

in which $e_j(n) \in \{0, \ldots, k-1\}$ and $e_j(n) = 0$ for all sufficiently large j. Given a nonzero d-tuple of nonnegative integers $(n_1, \ldots, n_d)$, we set

$h := \max\{ j \geq 0 \mid \text{there exists some } i, \, 1 \leq i \leq d, \text{ such that } e_j(n_i) \neq 0 \}.$

Furthermore, if $(n_1, \ldots, n_d) = (0, \ldots, 0)$, we set $h := 0$.

Fig. 5 A 2-dimensional 2-automaton generating the map f defined in Example 5.7

We can then produce an element

$$w_k(n_1, \ldots, n_d) := (w_1, \ldots, w_d) \in \left(\Sigma_k^d\right)^*$$

corresponding to $(n_1, \ldots, n_d)$ by defining

$$w_i := e_h(n_i)e_{h-1}(n_i) \cdots e_0(n_i).$$

In other words, we are taking the base-k expansions of $n_1, \ldots, n_r$ and then "padding" the expansions of each n_i at the beginning with 0's if necessary to ensure that each expansion has the same length.

Example 5.6 If $d = 3$ and $k = 2$, then we have $w_2(3, 5, 0) = (011, 101, 000)$.

Definition 5.2 A map $f : \mathbb{N}^d \to \Delta$ is k-automatic if there is a d-dimensional k-automaton $\mathcal{A} = (Q, \Sigma_k^d, \delta, q_0, \Delta, \tau)$ such that

$$f(n_1, \ldots, n_d) = \tau(\delta(q_0, w_k(n_1, \ldots, n_d))).$$

Similarly, a subset S of $\mathbb{N}^d$ is k-automatic if its characteristic function, $f : \mathbb{N}^d \to \{0, 1\}$, defined by $f(n_1, \ldots, n_d) = 1$ if $(n_1, \ldots, n_d) \in S$; and $f(n_1, \ldots, n_d) = 0$, otherwise, is k-automatic.

Example 5.7 Let $f : \mathbb{N}^2 \to \{0, 1\}$ be defined by $f(n, m) = 1$ if the sum of the binary digits of n added to the sum of the binary digits of m is even, and $f(n, m) = 0$ otherwise. Then $f(m, n)$ is a 2-automatic map. One can check that f can be generated by the following 2-dimensional 2-automaton (see Fig. 5): $\mathcal{A} = (\{A, B\}, \{0, 1\}^2, \delta, A, \{0, 1\}, \tau)$, where $\delta(A, (0, 0)) = \delta(A, (1, 1)) = \delta(B, (1, 0)) = \delta(B, (0, 1)) = A$, $\delta(A, (1, 0)) = \delta(A, (0, 1)) = \delta(B, (0, 0)) = \delta(B, (1, 1)) = B$, $\tau(A) = 0$ and $\tau(B) = 1$.

Just as k-automatic sequences can be characterized by the finiteness of the k-kernel, multidimensional k-automatic sequences have a similar characterization.

Definition 5.3 Let d be a positive integer and let Δ be a finite set. We define the k-*kernel* of a map $f : \mathbb{N}^d \to \Delta$ to be the collection of all maps of the form

$$g(n_1, \ldots, n_d) := f(k^a n_1 + b_1, \ldots, k^a n_d + b_d)$$

where $a \geq 0$ and $0 \leq b_1, \ldots, b_d < k^a$.

Example 5.8 The 2-kernel of the map $f : \mathbb{N}^2 \to \{0, 1\}$ defined in Example 5.7 consists of the 2 maps $f_1(m, n) := f(m, n)$, $f_2(m, n) = f(2m + 1, 2n)$.

Just as Eilenberg [12] showed that being k-automatic is equivalent to having a finite k-kernel for k-automatic sequences, Salon [35, théorème 1] observed that a similar characterization of multidimensional k-automatic maps holds.

Theorem 5.2 (Salon) *Let d be a positive integer and let Δ be a finite set. A map $f : \mathbb{N}^d \to \Delta$ is k-automatic if and only if its k-kernel is finite.*

5.3 Automatic subsets of $\mathbb{Z}^d$

We show now how to naturally extend Salon's construction to k-automatic subsets of $\mathbb{Z}^d$ by simply adding symbols $+$ and $-$ to our alphabet Σ_k.

Given a natural number n, we let $[n]_k$ denote the base-k expansion of n. We set

$$\Sigma_k' = \{0, 1, \ldots, k - 1, -, +\}$$

and we let $\mathcal{L}_k$ denote the language over the alphabet Σ_k' consisting of the empty word and all words over Σ_k' whose length is at least 2 such that the initial letter is either $+$ or $-$, the remaining letters are all in Σ_k, and the last letter is not equal to zero. This is easily seen to be a regular language.

There is a bijection $[\cdot]_k : \mathcal{L}(k) \to \mathbb{Z}$ in which the empty word is sent to zero,

$$+s_0 \cdots s_n \in \mathcal{L}(k) \mapsto \sum_{j=0}^{n} s_j k^j$$

and

$$-s_0 \cdots s_n \in \mathcal{L}(k) \mapsto -\sum_{j=0}^{n} s_j k^j,$$

where $s_0, \ldots, s_n \in \{0, 1, \ldots, k - 1\}$.

Definition 5.4 We say that a subset S of $\mathbb{Z}$ is k-*automatic* if there is a finite-state automaton that takes words over Σ_k' as input, and has the property that a word $W \in \mathcal{L}_k$ is accepted by the automaton if and only if $[W]_k \in S$.

More generally, we can define automatic subsets of $\mathbb{Z}^d$, mimicking the construction of Salon [35]. For a natural number $d \geq 1$, we create the alphabet $\Sigma_k'(d)$ to be the alphabet $(\Sigma_k')^d$ consisting of all d-tuples of elements of

Σ'_k. With this in mind, we construct a regular language $\mathcal{L}_k(d) \subseteq (\Sigma'_k(d))^*$ as follows. Given a nonzero integer n, we can write it uniquely as

$$n = \epsilon \sum_{j=0}^{\infty} e_j(n) k^j,$$

in which $\epsilon \in \{\pm 1\}$, $e_j(n) \in \{0, \ldots, k-1\}$ and there is some natural number N, depending on n, such that $e_j(n) = 0$ whenever $j > N$. We also set

$$0 = + \sum_{j=0}^{\infty} e_j(0) k^j,$$

where $e_j(0) = 0$ for all $j \geq 0$. Given a nonzero d-tuple of integers $(n_1, \ldots, n_d)$, we set

$$h := \max\{j \mid \text{there exists some } i \text{ such that } e_j(n_i) \neq 0\}.$$

If $(n_1, \ldots, n_d) = (0, \ldots, 0)$, we set $h := 0$.

We can then produce an element

$$w_k(n_1, \ldots, n_d) := (w_1, \ldots, w_d) \in (\Sigma'_k(d))^*$$

corresponding to $(n_1, \ldots, n_d)$ by defining

$$w_i := \epsilon_i e_h(n_i) e_{h-1}(n_i) \cdots e_0(n_i),$$

where ϵ_i is $+$ if n_i is nonnegative and is $-$ if $n_i < 0$. In other words, we are taking the base k-expansions of $n_1, \ldots, n_d$ and then "padding" the expansions of each n_i at the beginning to ensure that each expansion has the same length.

Example 5.9 If $d = 3$ and $k = 2$, then we have $w_3(14, -3, 0) = (+1110, -0011, +0000)$.

We then take $\mathcal{L}_k(d)$ to be the collection of words of the form

$$w_k(n_1, \ldots, n_d)$$

where $(n_1, \ldots, n_d) \in \mathbb{Z}^d$. Then there is an obvious way to extend the map $[\cdot]_k$ to a bijection $[\cdot]_k : \mathcal{L}_k(d) \to \mathbb{Z}^d$; namely,

$$[w_k(n_1, \ldots, n_d)]_k := (n_1, \ldots, n_d).$$

We also denote by $[\cdot]_k^{-1}$ the reciprocal map.

We can now define the notion of a k-automatic function from $\mathbb{Z}^d$ to a finite set as follows.

Definition 5.5 Let Δ be a finite set. A function $f : \mathbb{Z}^d \to \Delta$ is *k-automatic* if there is a finite automaton that takes words over $\mathcal{L}_k(d)$ as input and has the property that reading a word $W \in \mathcal{L}_k(d)$, the automaton outputs $f([W]_k)$.

Similarly, a subset S of $\mathbb{Z}^d$ is *k-automatic* if its characteristic function, $f : \mathbb{Z}^d \to \{0, 1\}$, defined by $f(n_1, \ldots, n_d) = 1$ if $(n_1, \ldots, n_d) \in S$; and $f(n_1, \ldots, n_d) = 0$, otherwise, is *k-automatic*.

In fact, much as in the classical situation, automaticity of subsets of $\mathbb{Z}^d$ can be characterized using the kernel.

Definition 5.6 Let $d \geq 1$ be an integer and Δ a finite set. Given a map $f : \mathbb{Z}^d \to \Delta$, we define the *k-kernel* of f to be the collection of all maps of the form

$$g(n_1, \ldots, n_d) := f(k^a n_1 + b_1, \ldots, k^a n_d + b_d)$$

where $a \geq 0$ and $0 \leq b_1, \ldots, b_d < k^a$.

Proposition 5.1 *Let $d \geq 1$ be an integer and Δ a finite set. Given a map $f : \mathbb{Z}^d \to \Delta$, the following are equivalent.*

(i) *The map f is k-automatic.*
(ii) *The k-kernel of f is finite.*
(iii) *For each $\epsilon = (\epsilon_1, \ldots, \epsilon_d) \in \{\pm 1\}^d$, the function $f_\epsilon : \mathbb{N}^d \to \Delta$ defined by $(n_1, \ldots, n_d) \mapsto f(\epsilon_1 n_1, \ldots, \epsilon_d n_d)$ is k-automatic in the usual sense.*

Proof We note that by definition of automatic maps on $\mathbb{Z}^d$, each of the f_ϵ is *k*-automatic in the usual sense and hence (i) implies (iii). Similarly, (iii) implies (i). Next assume that (iii) holds. Let $h(n_1, \ldots, n_d) = f(k^a n_1 + b_1, \ldots, k^a n_d + b_d)$ be a map in the kernel of f. Then for $\epsilon = (\epsilon_1, \ldots, \epsilon_d) \in \{\pm 1\}^d$, the map $h_\epsilon : \mathbb{N}^d \to \Delta$ defined by $(n_1, \ldots, n_d) \mapsto h(\epsilon_1 n_1, \ldots \epsilon_d n_d)$ is of the form

$$f\bigl(\epsilon_1 k^a n_1 + b_1, \ldots, \epsilon_d k^a n_d + b_d\bigr),$$

which is in the *k*-kernel of f_ϵ. Since there are only finitely many $\epsilon = (\epsilon_1, \ldots, \epsilon_d) \in \{\pm 1\}^d$ and only finitely many elements in the kernel of f_ϵ, we see that the kernel of f is finite and hence (iii) implies (ii). Similarly, (ii) implies (iii). $\qquad\square$

5.4 Automatic subsets of finitely generated abelian groups

We introduce here a relevant notion of automaticity for subsets of arbitrary finitely generated abelian groups. In this area, we quote [1] where the authors provide a general framework for the automaticity of maps from some semirings to finite sets. In particular, a similar notion of automaticity for subsets of $\mathbb{Z}^2$ was considered in that paper.

In this more general framework, it seems more natural to define first k-automatic maps in terms of some generalized k-kernels and then to prove that such maps can be characterized in terms of finite automata.

In the rest of this section, all finitely generated abelian groups are written additively. We thus first define the k-kernel of a map from a finitely generated abelian group to a finite set.

Definition 5.7 Let Γ be a finitely generated abelian group and $T = \{\gamma_1, \ldots, \gamma_d\}$ a set of generators of Γ. Let Δ be a finite set. Given a map $f : \Gamma \to \Delta$, we define the k-kernel of f with respect to the generating set T to be the collection of all maps from Γ to Δ of the form

$$g(x) := f(k^a x + b_1 \gamma_1 + \cdots + b_d \gamma_d)$$

such that $a \geq 0$ and $0 \leq b_1, \ldots, b_d < k^a$.

We can now define k-automatic maps as follows.

Definition 5.8 Let Γ be a finitely generated abelian group and Δ a finite set. A map $f : \Gamma \to \Delta$ is k-automatic if its k-kernel with respect to every finite generating set of Γ is finite.

As usual, we can use the previous definition to introduce the notion of a k-automatic subset of a finitely generated abelian group.

Definition 5.9 Let Γ be a finitely generated abelian group. A subset S of Γ is k-automatic if the map $\chi_S : \Gamma \to \{0, 1\}$, defined by $\chi_S(x) = 1$ if and only if $x \in S$, is k-automatic.

We note that our definition of k-automaticity appears to be somewhat difficult to verify, as we must check that the k-kernel is finite with respect to every finite generating set. As shown below, it actually suffices to check that the k-kernel is finite with respect to just anyone generating set.

Proposition 5.2 *Let Γ be a finitely generated abelian group and Δ a finite set. Let us assume that the map $f : \Gamma \to \Delta$ has a finite k-kernel with respect to some generating set of Γ. Then the map f is k-automatic.*

Proof Suppose that the k-kernel of f is finite with respect to the generating set $T := \{\gamma_1, \ldots, \gamma_d\}$ of Γ and let $f_1, \ldots, f_m$ denote the distinct maps in the k-kernel of f.

Given another generating set of Γ, say $T' := \{\delta_1, \ldots, \delta_e\}$, we have to show that the k-kernel of f with respect to T' is also finite.

There exist integers $c_{i,j}$ with $1 \le i \le d$ and $1 \le j \le e$ such that

$$\delta_j = \sum_{i=1}^{d} c_{i,j} \gamma_i$$

for $j \in \{1, \ldots, e\}$. Set $N := \sum_{i,j} |c_{i,j}|$. Given an integer i, $1 \le i \le m$, and a d-tuple of integers $\mathbf{j} = (j_1, \ldots, j_d)$, we define the map $g_{i,\mathbf{j}}$ from Γ to Δ by

$$g_{i,\mathbf{j}}(x) := f_i(x + j_1 \gamma_1 + \cdots + j_d \gamma_d)$$

for all $x \in \Gamma$. We claim that the k-kernel of f with respect to T' is contained in the finite set $\mathcal{S}$ defined by

$$\mathcal{S} := \{ g_{i,\mathbf{j}} : \Gamma \to \Delta \mid \mathbf{j} = (j_1, \ldots, j_d) \in \{-N, -N+1, \ldots, N\}^d,$$
$$i \in \{1, \ldots, m\} \}.$$

To see this, note that if $a \ge 0$ and $0 \le b_1, \ldots, b_d < k^a$, then

$$b_1 \delta_1 + \cdots + b_e \delta_e = b_1' \gamma_1 + \cdots + b_d' \gamma_d,$$

where $b_i' = \sum_{j=1}^{e} b_j c_{i,j}$. It follows that

$$|b_i'| \le N(k^a - 1)$$

for every i, $1 \le i \le d$. We can thus write $b_i' = k^a m_i + r_i$ with $|m_i| < N$ and $0 \le r_i < k^a$. This implies that

$$f(k^a x + b_1 \delta_1 + \cdots + b_e \delta_e)$$
$$= f(k^a x + b_1' \gamma_1 + \cdots + b_d' \gamma_d)$$
$$= f(k^a (x + m_1 \gamma_1 + \cdots + m_d \gamma_d) + r_1 \gamma_1 + \cdots + r_d \gamma_d)$$
$$= f_\ell(x + m_1 \gamma_1 + \cdots + m_d \gamma_d)$$

for some ℓ, $1 \le \ell \le m$. Thus we see that

$$f(k^a x + b_1 \delta_1 + \cdots + b_e \delta_e) = g_{\ell,\mathbf{m}}(x)$$

where $\mathbf{m} := (m_1, \ldots, m_d)$, which proves that the k-kernel of f with respect to the generating set T' is included in the finite set $\mathcal{S}$, as claimed. $\qquad \square$

Proposition 5.3 *Let Γ_1 and Γ_2 be two finitely generated abelian groups, and $\Phi : \Gamma_1 \to \Gamma_2$ a surjective group homomorphism. If S is a k-automatic subset of Γ_2 then $\Phi^{-1}(S)$ is a k-automatic subset of Γ_1.*

Proof Let f and g denote respectively the characteristic function of $\Phi^{-1}(S)$ and S. Let $\{\gamma_1, \ldots, \gamma_d\}$ be a set of generators of Γ_1. Then if $a \geq 0$ and $0 \leq b_1, \ldots, b_d < k^a$, we infer from the definition of f that

$$f\left(k^a x + b_1 \gamma_1 + \cdots + b_d \gamma_d\right) = 1 \quad \Longleftrightarrow \quad \Phi\left(k^a x + b_1 \gamma_1 + \cdots + b_d \gamma_d\right) \in S,$$

which occurs if and only if

$$g\left(k^a \Phi(x) + \sum_{i=1}^{d} b_i \Phi(\gamma_i)\right) = 1.$$

Note that

$$T := \left\{\Phi(\gamma_i) \ : \ 1 \leq i \leq d\right\}$$

is a set of generators of Γ_2 since Φ is surjective. Since, by assumption, g is k-automatic, the k-kernel of g is finite with respect to T. Thus the k-kernel of f is finite with respect to $T' := \{\gamma_1, \ldots, \gamma_d\}$. The result now follows from Proposition 5.2. □

We can now prove, as we may expect, that a k-automatic subset of a finitely generated abelian group can be described by a finite automaton.

Proposition 5.4 *Let Γ be a finitely generated group, $\{\gamma_1, \ldots, \gamma_d\}$ a set of generators of Γ, and S a subset of Γ. Then S is k-automatic if and only if there exists a finite automaton that takes words over $\mathcal{L}_k(d)$ as input and has the property that for every d-tuple of integers $(n_1, \ldots, n_d)$ the word $[(n_1, \ldots, n_d)]_k^{-1} \in \mathcal{L}_k(d)$ is accepted by the automaton if and only if $n_1 \gamma_1 + \cdots + n_d \gamma_d$ belongs to S.*

Proof For every integer i, $1 \leq i \leq d$, we denote by $e_i := (0, 0, \ldots, 0, 1, 0, \ldots, 0)$ the element of $\mathbb{Z}^d$ whose jth coordinate is 1 and whose other coordinates are 0. Let Φ be the surjective group homomorphism from $\mathbb{Z}^d$ to Γ defined by $\Phi(e_i) = \gamma_i$ for every integer i, $1 \leq i \leq d$.

If S is k-automatic then, by Proposition 5.3, $\Phi^{-1}(S)$ is a k-automatic subset of $\mathbb{Z}^d$. By Definition 5.5, there is a finite automaton that takes words over $\mathcal{L}_k(d)$ as input and has the property that the word $W \in \mathcal{L}_k(d)$ is accepted by the automaton if and only if $[W]_k$ belongs to $\Phi^{-1}(S)$. Thus for every d-tuple of integers $(n_1, \ldots, n_d)$ the word $[(n_1, \ldots, n_d)]_k^{-1} \in \mathcal{L}_k(d)$ is accepted by this automaton if and only if $n_1 \gamma_1 + \cdots + n_d \gamma_d$ belongs to S.

On the other hand, if there exists a finite automaton such that for every d-tuple of integers $(n_1, \ldots, n_d)$ the word $[(n_1, \ldots, n_d)]_k^{-1} \in \mathcal{L}_k(d)$ is accepted by this automaton if and only if $n_1 \gamma_1 + \cdots + n_d \gamma_d$ belongs to S. The same automaton can also be used to recognize $\Phi^{-1}(S)$. Thus $\Phi^{-1}(S)$ is a k-automatic

subset of $\mathbb{Z}^d$. By Proposition 5.1, the set $\Phi^{-1}(S)$ has a finite k-kernel and it follows that S has a finite k-kernel with respect to $\{\gamma_1, \ldots, \gamma_d\}$. By Proposition 5.2, S is thus a k-automatic subset of Γ. $\square$

6 Proof of our main result

Our aim is to prove Theorem 1.4. Throughout this section, we take d to be a natural number. We let $\mathbf{n}$ and $\mathbf{j}$ denote respectively the d-tuple of natural numbers $(n_1, \ldots, n_d)$ and $(j_1, \ldots, j_d)$. We will also let $\mathbf{t}^{\mathbf{n}}$ denote the monomial $t_1^{n_1} \cdots t_d^{n_d}$ in indeterminates $t_1, \ldots, t_d$. The degree of such a monomial is the nonnegative integer $n_1 + \cdots + n_d$. Given a polynomial P in $K[\mathbf{t}]$, we denote by $\deg P$ the maximum of the degrees of the monomials appearing in P with nonzero coefficient.

Definition 6.1 We say that a power series $f(\mathbf{t}) \in K[[\mathbf{t}]]$ is algebraic if it is algebraic over the field of rational functions $K(\mathbf{t})$, that is, if there exist polynomials $A_0, \ldots, A_m \in K[\mathbf{t}]$, not all zero, such that

$$\sum_{i=0}^{m} A_i(\mathbf{t}) f(\mathbf{t})^i = 0.$$

In order to prove Theorem 1.4 we need to introduce some notation. For each $\mathbf{j} = (j_1, \ldots, j_d) \in \{0, 1, \ldots, p-1\}^d$, we define $e_{\mathbf{j}} : \mathbb{N}^d \to \mathbb{N}^d$ by

$$e_{\mathbf{j}}(n_1, \ldots, n_d) := (pn_1 + j_1, \ldots, pn_d + j_d). \tag{6.1}$$

We let Σ denote the semigroup generated by the collection of all $e_{\mathbf{j}}$ under composition. In view of Definition 5.3, this semigroup is intimately related to the definition of the p-kernel of d-dimensional maps. As a direct consequence of Theorem 5.2, we make the following remark which underlines the important role that will be played by the semigroup Σ in the proof of Theorem 1.4.

Remark 6.1 Let Δ be a finite set. Then a map $a : \mathbb{N}^d \to \Delta$ is p-automatic if and only the set of functions $\{a \circ e \mid e \in \Sigma\}$ is a finite set.

We recall that a field K of characteristic $p > 0$ is perfect if the map $x \mapsto x^p$ is surjective on K. Let p be a prime number and let K be a perfect field of characteristic p. For every $\mathbf{j} \in \Sigma_p^d = \{0, 1, \ldots, p-1\}^d$, we define the so-called Cartier operator $E_{\mathbf{j}}$ from $K[[\mathbf{t}]]$ into itself by

$$E_{\mathbf{j}}(f(\mathbf{t})) := \sum_{\mathbf{n} \in \mathbb{N}^d} \left(a \circ e_{\mathbf{j}}(\mathbf{n})\right)^{1/p} \mathbf{t}^{\mathbf{n}} \tag{6.2}$$

where $f(\mathbf{t}) := \sum_{\mathbf{n} \in \mathbb{N}^d} a(\mathbf{n}) \mathbf{t}^{\mathbf{n}} \in K[[\mathbf{t}]]$. Then we have the following useful decomposition:

$$f = \sum_{\mathbf{j} \in \Sigma_p^d} \mathbf{t}^{\mathbf{j}} E_{\mathbf{j}}(f)^p. \tag{6.3}$$

We now recall the following simple classical result, usually known as Ore's lemma.

Lemma 6.1 *Let $f(\mathbf{t}) \in K[[\mathbf{t}]]$ be a nonzero algebraic power series. Then there exists a positive integer r and polynomials $P_0, \ldots, P_r$ in $K[\mathbf{t}]$ such that*

$$\sum_{i=0}^r P_i f^{p^i} = 0$$

and $P_0 \neq 0$.

Proof Since f is algebraic, $\{f, f^p, f^{p^2}, \ldots\}$ is linearly dependent over $K(\mathbf{t})$. There thus exists a natural number r and polynomials $P_0, \ldots, P_r$ in $K[\mathbf{t}]$ such that

$$\sum_{i=0}^r P_i f^{p^i} = 0.$$

It remains to prove that one can choose $P_0 \neq 0$. Let k be the smallest non-negative integer such that f satisfies a relation of this type with $P_k \neq 0$. We shall prove that $k = 0$ which will end the proof. We assume that $k > 0$ and we argue by contradiction. Since $P_k \neq 0$, we infer from Equality (6.3) that there exists a d-tuple $\mathbf{j} \in \Sigma_p^d$ such that $E_{\mathbf{j}}(P_k) \neq 0$. Since $\sum_{i=k}^r P_i f^{p^i} = 0$, we have

$$E_{\mathbf{j}}\left(\sum_{i=k}^r P_i f^{p^i} \right) = \sum_{i=k}^r E_{\mathbf{j}}\left(P_i f^{p^i} \right) = \sum_{i=k}^r E_{\mathbf{j}}(P_i) f^{p^{i-1}} = 0.$$

We thus obtain a new relation of the same type but for which the coefficient of $f^{p^{k-1}}$ is nonzero. This provides a contradiction with the definition of k. $\square$

We now let Ω denote the semigroup generated by the collection of the Cartier operators $E_{\mathbf{j}}$ and the identity operator under composition. We let $\Omega(f)$ denote the orbit of f under the action of Ω, that is,

$$\Omega(f) := \{ E(f) \mid E \in \Omega \}.$$

As in the work of Harase [21] and of Sharif and Woodcock [38], the K-vector space spanned by $\Omega(f)$ will play an important role. We will in particular need the following auxiliary result based on Ore's lemma.

Lemma 6.2 *Let K be a perfect field of characteristic p, and let*

$$f(\mathbf{t}) := \sum_{\mathbf{n} \in \mathbb{N}^d} a(\mathbf{n})\mathbf{x}^{\mathbf{n}} \in K[[\mathbf{t}]]$$

be a nonzero algebraic function over $K(\mathbf{t})$. Then there exists a natural number m and there exist maps $a_1, \ldots, a_m : \mathbb{N}^d \to K$ with the following properties.

(i) *The formal power series $f_i(\mathbf{t}) := \sum_{\mathbf{n} \in \mathbb{N}^d} a_i(\mathbf{n})\mathbf{t}^{\mathbf{n}}$, $1 \le i \le m$, form a basis of the K-vector space spanned by $\Omega(f)$.*
(ii) *One has $f_1 = f$.*
(iii) *Let $g(\mathbf{t}) := \sum_{\mathbf{n} \in \mathbb{N}^d} b(\mathbf{n})\mathbf{t}^{\mathbf{n}}$ be a power series that belongs to $\Omega(f)$. Then $b \circ e_{\mathbf{j}} \in K\,a_1^p + \cdots + K\,a_m^p$ for every $\mathbf{j} \in \{0, \ldots, p-1\}^d$.*

Proof Let $f(\mathbf{t}) \in K[[\mathbf{t}]]$ be a nonzero algebraic power series. By Lemma 6.1, there exist a positive integer r and polynomials $P_0, \ldots, P_r$ in $\mathbb{K}[\mathbf{t}]$ such that

$$\sum_{i=0}^{r} P_i f^{p^i} = 0$$

and $P_0 \ne 0$. Set $\tilde{f} := P_0^{-1} f$. Then

$$\tilde{f} = \sum_{i=1}^{r} Q_i \tilde{f}^{p^i}, \qquad (6.4)$$

where $Q_i = -P_i P_0^{p^i - 2}$. Set $M := \max\{\deg P_0, \deg Q_i \mid 1 \le i \le r\}$ and

$$\mathcal{H} := \left\{ h \in K((\mathbf{t})) \,\middle|\, h = \sum_{i=0}^{r} R_i \tilde{f}^{p^i} \text{ such that } R_i \in K[\mathbf{t}] \text{ and } \deg R_i \le M \right\}. \qquad (6.5)$$

We first note that f belongs to $\mathcal{H}$ since $f = P_0 \tilde{f}$ and $\deg P_0 \le M$. We also observe that $\mathcal{H}$ is closed under the action of Ω. Indeed, if $h := \sum_{i=0}^{r} R_i \tilde{f}^{p^i} \in \mathcal{H}$ and $\mathbf{j} \in \{0, \ldots, p-1\}^d$, then

$$E_{\mathbf{j}}(h) = E_{\mathbf{j}}\left(R_0 \tilde{f} + \sum_{i=1}^{r} R_i \tilde{f}^{p^i} \right) = E_{\mathbf{j}}\left(\sum_{i=1}^{r} (R_0 Q_i + R_i) \tilde{f}^{p^i} \right)$$

$$= \sum_{i=1}^{r} E_{\mathbf{j}}(R_0 \tilde{f} + R_i) \tilde{f}^{p^{i-1}},$$

and since $\deg(R_0 Q_i + R_i) \leq 2M$, we have $\deg E_{\mathbf{j}}(R_0 Q_i + R_i) \leq 2M/p \leq M$. It follows that the K-vector space spanned by $\Omega(f)$ is contained in $\mathcal{H}$ and thus has finite dimension, say m.

We can thus pick maps $a_1, \ldots, a_m : \mathbb{N}^d \to K$ such that the m power series $f_i(\mathbf{t}) := \sum_{\mathbf{n} \in \mathbb{N}^d} a_i(\mathbf{n}) \mathbf{t}^{\mathbf{n}}$ form a basis of $\Omega(f)$. Furthermore, since by assumption f is a nonzero power series, we can chose $f_1 = f$. Let $b : \mathbb{N}^d \to K$ be such that $g(\mathbf{t}) := \sum_{\mathbf{n} \in \mathbb{N}^d} b(\mathbf{n}) \mathbf{t}^{\mathbf{n}}$ belongs to $\Omega(f)$. Observe that the power series g can be decomposed as

$$g(\mathbf{t}) = \sum_{\mathbf{j} \in \{0, \ldots, p-1\}^d} \mathbf{t}^{\mathbf{j}} E_{\mathbf{j}}\big(g(\mathbf{t})\big)^p. \tag{6.6}$$

By assumption, $E_{\mathbf{j}}(g(\mathbf{t})) \in K f_1(\mathbf{t}) + \cdots + K f_m(\mathbf{t})$ and hence $E_{\mathbf{j}}(g(\mathbf{t}))^p \in K f_1(\mathbf{t})^p + \cdots + K f_m(\mathbf{t})^p$. Let $\mathbf{j} \in \{0, 1, \ldots, p-1\}^d$. Considering the coefficient of $\mathbf{t}^{p\mathbf{n}+\mathbf{j}}$ in (6.6), we see that $b \circ e_{\mathbf{j}}(\mathbf{n})$ is equal to the coefficient of $\mathbf{t}^{p\mathbf{n}}$ in $E_{\mathbf{j}}(g(\mathbf{t}))^p$, which belongs to $K a_1(\mathbf{n})^p + \cdots + K a_m(\mathbf{n})^p$. This concludes the proof. $\qquad\square$

We will also need the following lemma that says we will only have to work with finitely generated extensions of the prime field instead of general fields of characteristic p.

Lemma 6.3 *Let $f_1, \ldots, f_m$ be power series as in Lemma 6.2. Then there is a finitely generated field extension K_0 of $\mathbb{F}_p$ such that all coefficients of the power series $f_1, \ldots, f_m$ belong to K_0.*

Proof Let $\tilde{f} := \sum_{\mathbf{n} \in \mathbb{N}^d} \tilde{a}(\mathbf{n}) \mathbf{t}^{\mathbf{n}}$ be defined as in (6.4), that is,

$$\tilde{f} = \sum_{i=1}^{r} Q_i \tilde{f}^{p^i}, \tag{6.7}$$

Let also $\mathcal{H}$ be the K-vector space defined as in (6.5), that is,

$$\mathcal{H} = \left\{ h \in K\big((\mathbf{t})\big) \,\Big|\, h = \sum_{i=0}^{r} R_i \tilde{f}^{p^i} \text{ such that } R_i \in K[\mathbf{t}] \text{ and } \deg R_i \leq M \right\}. \tag{6.8}$$

Since $\mathcal{H}$ contains the K-vector space spanned by $\Omega(f)$, the power series $f_1, \ldots, f_m$ belong to $\mathcal{H}$. There thus exist a finite number of polynomials $R_{i,k}$ such that

$$f_k = \sum_{i=0}^{r} R_{i,k} \tilde{f}^{p^i}.$$

It thus remains to prove that there exists a finitely generated field extension K_0 of $\mathbb{F}_p$ such that all coefficients of $\tilde{f}$ belong to K_0. Indeed, by adding to K_0 all the coefficients of the polynomials $R_{i,k}$, we would obtain a finitely generated field extension K_1 of $\mathbb{F}_p$ such that all coefficients of the power series $f_1, \ldots, f_m$ belong to K_1.

Given a d-tuple $\mathbf{n} = (n_1, \ldots, n_d)$, we set $\|\mathbf{n}\| := \max(n_1, \ldots, n_d)$. Let N be a positive integer. We let K_0 be the finitely generated extension of $\mathbb{F}_p$ generated by the coefficients of $Q_1, \ldots, Q_r$ and the collection of coefficients of $\mathbf{t^n}$ in $\tilde{f}(\mathbf{t})$ with $\|\mathbf{n}\| \leq N$. We claim that the coefficients of $\tilde{f}$ all lie in K_0. We prove by induction on $\|\mathbf{n}\|$ that all coefficients $\tilde{a}(\mathbf{n})$ belongs to K_0. By construction, this holds whenever $\|\mathbf{n}\| \leq N$.

Suppose that the claim holds whenever $\|\mathbf{n}\| < M$ for some $M > N$ and let us assume that $\|\mathbf{n}\| = M$. Then if we consider the coefficient of $t_1^{n_1} \cdots t_d^{n_d}$ in both sides of (6.7), we get that

$$\tilde{a}(n_1, \ldots, n_d) \in \sum_{i=1}^{r} \sum_{(m_1, \ldots, m_d) \in S} K_0 \tilde{a}(m_1, \ldots, m_d)^{p^i},$$

where S is the (possibly empty) set of all d-tuples $\mathbf{m} := (m_1, \ldots, m_d) \in \mathbb{N}^d$ such that either $m_i = 0$ or $m_i < n_i$ for each $i \in \{1, \ldots, d\}$. Since $M > 0$, we get that $\|\mathbf{m}\| < M$ and the inductive hypothesis implies that

$$\sum_{i=1}^{r} \sum_{(m_1, \ldots, m_d) \in S} K_0 \tilde{a}(m_1, \ldots, m_d)^{p^i} \subseteq K_0,$$

and so $\tilde{a}(n_1, \ldots, n_d) \in K_0$. This completes the induction and shows that all coefficients of $\tilde{f}$ lie in K_0. □

Before proving Theorem 1.4, we first fix a few notions. Given a finitely generated field extension K_0 of $\mathbb{F}_p$, we let $K_0^{\langle p \rangle}$ denote the subfield consisting of all elements of the form x^p with $x \in K_0$. Given $\mathbb{F}_p$-vector subspaces U and V of K_0 we let VU denote the $\mathbb{F}_p$-subspace of K_0 spanned by all products of the form vu with $v \in V, u \in U$. We let $V^{\langle p \rangle}$ denote the $\mathbb{F}_p$-vector subspace consisting of all elements of the form v^p with $v \in V$. We note that since K_0 is a finitely generated field extension of $\mathbb{F}_p$, K_0 is a finite-dimensional $K_0^{\langle p \rangle}$-vector space. If we fix a basis

$$K_0 = \bigoplus_{i=1}^{r} K_0^{\langle p \rangle} h_i$$

then we have *projections* $\pi_1, \ldots, \pi_r : K_0 \to K_0$ defined by

$$x = \sum_{i=1}^{r} \pi_i(x)^p h_i. \tag{6.9}$$

Remark 6.2 For $1 \le i \le r$ and $x, y, z \in K_0$ we have

$$\pi_i(x^p y + z) = x \pi_i(y) + \pi_i(z).$$

The last ingredient we have to state before proving Theorem 1.4 is a rather technical result, but very useful, due to Derksen, which we state here without proof. It corresponds to Proposition 5.2 in [10]. Basically, we will prove an effective version of this result later in Sect. 8 (step 2 in the proof of Theorem 1.5).

Proposition 6.1 (Derksen) *Let K_0 be a finitely generated field extension of $\mathbb{F}_p$ and let $\pi_1, \ldots, \pi_r : K_0 \to K_0$ be as in* (6.9). *If U is a finite-dimensional $\mathbb{F}_p$-vector subspace of K_0. Then there exists a finite-dimensional $\mathbb{F}_p$-vector subspace V of K_0 containing U such that*

$$\pi_i(VU) \subseteq V$$

for all i such that $1 \le i \le r$.

We are now ready to prove Theorem 1.4.

Proof of Theorem 1.4 By enlarging K if necessary, we may assume that K is perfect. By Lemma 6.2 we can find maps $a_1, \ldots, a_m : \mathbb{N}^d \to K$ with the following properties.

(i) The power series $f_i(\mathbf{t}) := \sum_{\mathbf{n} \in \mathbb{N}^d} a_i(\mathbf{n})\mathbf{t}^{\mathbf{n}}$, $1 \le i \le m$, form a basis of the K-vector space spanned by $\Omega(f)$.
(ii) One has $f_1 = f$.
(iii) Let $g(\mathbf{t}) := \sum_{\mathbf{n} \in \mathbb{N}^d} b(\mathbf{n})\mathbf{t}^{\mathbf{n}}$ be a power series that belongs to $\Omega(f)$. Then $b \circ e_{\mathbf{j}} \in K a_1^p + \cdots + K a_m^p$ for every $\mathbf{j} \in \{0, \ldots, p-1\}^d$.

In particular, given $1 \le i \le m$ and $\mathbf{j} \in \{0, 1, \ldots, p-1\}^d$, there are elements $\lambda(i, \mathbf{j}, k)$, $1 \le k \le m$, such that

$$a_i \circ e_{\mathbf{j}} = \sum_{k=1}^{m} \lambda(i, \mathbf{j}, k) a_k^p. \tag{6.10}$$

Furthermore, by Lemma 6.3, there exists a finitely generated field extension of $\mathbb{F}_p$ such that all coefficients of $f_1, \ldots, f_m$ are contained in this field extension. It follows that the subfield K_0 of K generated by the coefficients

of $f_1(\mathbf{t}), \ldots, f_m(\mathbf{t})$ and all the elements $\lambda(i, \mathbf{j}, k)$ is a finitely generated field extension of $\mathbb{F}_p$.

Since K_0 is a finite-dimensional $K_0^{\langle p \rangle}$-vector space, we can fix a basis $\{h_1, \ldots, h_r\}$ of K_0, that is,

$$K_0 = \bigoplus_{i=1}^r K_0^{\langle p \rangle} h_i.$$

As already mentioned, we have projections $\pi_1, \ldots, \pi_r : K_0 \to K_0$ defined by

$$x = \sum_{i=1}^r \pi_i(x)^p h_i. \tag{6.11}$$

We let U denote the finite-dimensional $\mathbb{F}_p$-vector subspace of K_0 spanned by the elements $\lambda(i, \mathbf{j}, k)$, $1 \le i, k \le m$ and $\mathbf{j} \in \{0, 1, \ldots, p-1\}^d$, and by 1. By (6.10), we have

$$a_i \circ e_{\mathbf{j}} \in U a_1^p + \cdots + U a_m^p, \tag{6.12}$$

for $1 \le i \le m$ and $\mathbf{j} \in \{0, 1, \ldots, p-1\}^d$. By Proposition 6.1 there exists a finite-dimensional $\mathbb{F}_p$-vector subspace V of K_0 containing U such that $\pi_i(VU) \subseteq V$ for $1 \le i \le r$.

We now set

$$W := V a_1 + \cdots + V a_m \subseteq \{b \mid b : \mathbb{N}^d \to K_0\}.$$

We note that since V is a finite-dimensional $\mathbb{F}_p$-vector space, it is a finite set. It follows that W is also a finite set since $\operatorname{Card} W \le (\operatorname{Card} V)^d < \infty$. Note also that if $\ell \in \{1, \ldots, r\}$, $i \in \{1, \ldots, m\}$, and $j \in \{0, 1, \ldots, p-1\}^d$ then by (6.12) and Remark 6.2 we have

$$\begin{aligned}
\pi_\ell(V a_i \circ e_{\mathbf{j}}) &\subseteq \pi_\ell(V U a_1^p + \cdots + V U a_m^p) \\
&\subseteq \pi_\ell(VU) a_1 + \cdots + \pi_\ell(VU) a_m \\
&\subseteq V a_1 + \cdots + V a_m.
\end{aligned}$$

By Remark 6.2, we obtain that

$$b_\ell := \pi_\ell(b \circ e_{\mathbf{j}}) \in W \tag{6.13}$$

for all $b \in W$, $\mathbf{j} \in \{0, 1, \ldots, p-1\}^d$, and $1 \le \ell \le r$. Since $\{h_1, \ldots, h_r\}$ form a basis of K_0 as a $K_0^{\langle p \rangle}$-vector space, given x in K_0, we have

$$x = 0 \quad \Longleftrightarrow \quad \big(\pi_\ell(x) = 0 \text{ for all } 1 \le \ell \le r\big).$$

In particular,

$$b(p\mathbf{n} + \mathbf{j}) = 0 \quad \Longleftrightarrow \quad b_1(\mathbf{n}) = b_2(\mathbf{n}) = \cdots = b_r(\mathbf{n}) = 0. \qquad (6.14)$$

Given a map $b : \mathbb{N}^d \to K_0$, we define the map $\chi_b : \mathbb{N}^d \to \{0, 1\}$ by

$$\chi_b(\mathbf{n}) = \begin{cases} 0 & \text{if } b(\mathbf{n}) \neq 0 \\ 1 & \text{if } b(\mathbf{n}) = 0. \end{cases} \qquad (6.15)$$

Then we set

$$X := \{\chi_{b_1} \cdots \chi_{b_t} \mid t \geq 0, b_1, \ldots, b_t \in W\}.$$

We first get from (6.14) that

$$(\chi_b \circ e_{\mathbf{j}})(\mathbf{n}) = \prod_{\ell=1}^{r} \chi_{b_\ell}(\mathbf{n}).$$

Furthermore, we infer from (6.13) that $b_\ell \in W$ for all $b \in W$, $\mathbf{j} \in \{0, 1, \ldots, p-1\}^d$, and $1 \leq \ell \leq r$. The definition of X then implies that $\chi_b \circ e_{\mathbf{j}}$ belongs to X. More generally, it follows that

$$\forall \chi \in X, \forall e \in \Sigma, \quad \chi \circ e \in X. \qquad (6.16)$$

We note that by (6.15) we have $\chi_b^2 = \chi_b$ for all $b \in W$. Since W is a finite set, it follows that the set X is also finite. It thus follows from (6.16) and Remark 6.1 that all maps χ in X are p-automatic. In particular, since by assumption $a(\mathbf{n}) = a_1(\mathbf{n}) \in W$, we deduce that the map χ_a is p-automatic. It follows that the set

$$\mathcal{Z}(f) = \{\mathbf{n} \in \mathbb{N}^d \mid a(\mathbf{n}) = 0\}$$

is a p-automatic set, which ends the proof. $\qquad \square$

7 Finite automata and effectivity

In this section, we define a classical measure of complexity for p-automatic sets and we show how it can be used to prove effective results concerning such sets. We follow the presentation of [10].

Definition 7.1 Let $S \subset \mathbb{N}^d$ be a p-automatic set and let denote by K the p-kernel of S. We define the p-complexity of S by

$$\mathrm{comp}_{\mathrm{p}}(S) := \mathrm{Card}\, K.$$

The aim of this section is to state and prove the following result.

Proposition 7.1 *Let $S \subset \mathbb{N}^d$ be a p-automatic set and suppose that there exists an explicit integer $N(S)$ such that*

$$\mathrm{comp}_\mathrm{p}(S) \leq N(S).$$

Suppose also that for every positive integer n one can compute (in a finite amount of time) all the elements $\mathbf{s} \in S$ such that $\|\mathbf{s}\| \leq n$. Then the set S can be effectively determined. Furthermore, the following properties are decidable.

- (i) *The set S is empty.*
- (ii) *The set S is finite.*
- (iii) *The set S is periodic, that is, formed by the union of a finite set and of a finite number of (d-dimensional) arithmetic progressions.*

In particular, when S is finite, one can find (in a finite amount of time) all its elements.

Remark 7.1 When we say that the set S can be effectively determined, this means that there is an algorithm that produces in a finite amount of time a p-automaton that generates S. The format of the output is thus a 6-tuple $(Q, \Sigma_p^d, \delta, q_0, \{0, 1\}, \tau)$, where Q the set of states, $\delta : Q \times \Sigma_k^d \to Q$ is the transition function, q_0 is the initial state, and $\tau : Q \to \{0, 1\}$ is the output function. Furthermore, there exists an algorithm that allows one to determine in a finite amount of time whether S is empty, finite or whether S is formed by the union of a finite set and of a finite number of (d-dimensional) arithmetic progressions.

We first make the important observation that for every positive integer N there are only a finite number of p-automatic subsets of $\mathbb{N}^d$ whose p-complexity is at most N.

Lemma 7.1 *Let N be a positive integer. Then there at most $N2^N N^{pN}$ distinct p-automatic subsets of $\mathbb{N}^d$ whose p-complexity is at most N.*

Proof In the definition of p-automatic sets in Sect. 5, we used p-automata that read the input (d-tuples of integers) starting from the most significant digits (the input is scanned from the left to the right). It is well known that using p-automata that read the input starting from the least significant digits (the input is scanned from the right to the left) leads to the same notion of p-automatic sets. Furthermore, it is known that for every p-automatic set S, there exists such a p-automaton for which the number of states is equal to the cardinality of the p-kernel of S. Such an automaton has actually the minimal

number of states among all automata recognizing S and reading the input from the right to the left (see for instance [2] or [10]).

Thus a p-automatic set $S \subseteq \mathbb{N}^d$ with p-complexity at most N can be recognized by a p-automaton $\mathcal{A}$ (reading from the right to the left) with at most N states. Let $Q := \{Q_1, \ldots, Q_N\}$ denote the set of states of $\mathcal{A}$. To define $\mathcal{A}$, we must choose the initial state, the transition function from $Q \times \Sigma_p$ to Q, and the output function from Q to $\{0, 1\}$. We have at most N choices for the initial state, at most N^{pN} choices for the transition function, and at most 2^N choices for the output function. The result immediately follows. $\square$

Lemma 7.2 *Let $S_1, S_2 \subseteq \mathbb{N}^d$ be p-automatic sets. Then the following hold.*

- $\mathrm{comp}_p(S_1 \cap S_2) \leq \mathrm{comp}_p(S_1) \, \mathrm{comp}_p(S_2)$.
- $\mathrm{comp}_p(S_1 \cup S_2) \leq \mathrm{comp}_p(S_1) \, \mathrm{comp}_p(S_2)$.
- $\mathrm{comp}_p((S_1 \setminus S_2) \cup (S_2 \setminus S_1)) \leq \mathrm{comp}_p(S_1) \, \mathrm{comp}_p(S_2)$.
- $\mathrm{comp}_p(S_1 \setminus (S_1 \cap S_2)) \leq \mathrm{comp}_p(S_1) \, \mathrm{comp}_p(S_2)$.

Proof Given a set S let us denote by $\mathcal{I}_S$ its indicator function. The proof follows from the fact that $\mathcal{I}_{S_1 \cap S_2} = \mathcal{I}_{S_1} \cdot \mathcal{I}_{S_2}, \mathcal{I}_{S_1 \setminus S_2} = \mathcal{I}_{S_1} \cdot (1 - \mathcal{I}_{S_2}), \mathcal{I}_{S_1 \cup S_2} = \mathcal{I}_{S_1} + \mathcal{I}_{S_2} - \mathcal{I}_{S_1} \cdot \mathcal{I}_{S_2}, \mathcal{I}_{(S_1 \setminus S_2) \cup (S_2 \setminus S_1)} = \mathcal{I}_{S_1} \cdot (1 - \mathcal{I}_{S_2}) + \mathcal{I}_{S_2} \cdot (1 - \mathcal{I}_{S_1})$, and $\mathcal{I}_{S_1 \setminus (S_1 \cap S_2)} = \mathcal{I}_{S_1} \cdot (1 - \mathcal{I}_{S_1} \cdot \mathcal{I}_{S_2})$. $\square$

We will also use the following two results that can be easily proved as in [10].

Lemma 7.3 *Let $S \subseteq \mathbb{N}^d$ be a nonempty p-automatic set. Then*

$$\min\{\|\mathbf{s}\| \mid \mathbf{s} \in S\} \leq p^{\mathrm{comp}_p(S) - 2}.$$

Lemma 7.4 *Let $S \subseteq \mathbb{N}^d$ be a finite p-automatic set. If $\mathbf{s} \in S$, then*

$$\|\mathbf{s}\| \leq p^{\mathrm{comp}_p(S) - 2}.$$

We are now ready to prove Proposition 7.1.

Proof of Proposition 7.1 Let $S \subseteq \mathbb{N}^d$ be a p-automatic set. Let us assume that one knows an effective bound $N(S)$ for the p-complexity of S. Let us also assume that for every positive integer n one can compute (in a finite amount of time) all the elements $\mathbf{s} \in S$ such that $\|\mathbf{s}\| \leq n$.

We first note that by Lemma 7.1 there are only a finite number, say r, of p-automatic subsets of $\mathbb{N}^d$ with p-complexity at most $N(S)$. Going through the proof of Lemma 7.1, we can explicitly enumerate all these sets to get a collection $S_1, S_2, \ldots, S_r$.

Now for each S_i, we can check whether $S = S_i$ as follows. Since both S and S_i have p-complexity at most $N(S)$, we infer from Lemma 7.2 that

$$\mathrm{comp}_p\big((S \setminus S_i) \cup (S_i \setminus S)\big) \leq \mathrm{comp}_p(S)\mathrm{comp}_p(S_i) \leq N(S)^2.$$

Thus, by Lemma 7.3, the set $(S \setminus S_i) \cup (S_i \setminus S)$ is empty if and only if it has no element up to $p^{N(S)^2-2}$. This implies that $S = S_i$ if and only if

$$S \cap \big\{\mathbf{n} \in \mathbb{N}^d \mid \|\mathbf{n}\| \leq p^{N(S)^2-2}\big\} = S_i \cap \big\{\mathbf{n} \in \mathbb{N}^d \mid \|\mathbf{n}\| \leq p^{N(S)^2-2}\big\}.$$

By assumption, this can be verified in a finite amount of time.

(i) Since the p-complexity of S is at most $N(S)$, Lemma 7.3 implies that S is empty if and only if

$$S \cap \big\{\mathbf{n} \in \mathbb{N}^d \mid \|\mathbf{n}\| \leq p^{N(S)^2-2}\big\} = \emptyset.$$

By assumption, this can be verified in a finite amount of time.

(ii) Since the p-complexity of S is at most $N(S)$, Lemma 7.4 implies that S is finite if and only if

$$S = S \cap \big\{\mathbf{n} \in \mathbb{N}^d \mid \|\mathbf{n}\| \leq p^{N(S)^2-2}\big\}.$$

Set $S' := \{\mathbf{n} \in \mathbb{N}^d \mid \|\mathbf{n}\| \leq p^{N(S)^2-2}\}$. Thus S is finite if and only if the set

$$S \setminus (S \cap S') = \emptyset. \tag{7.1}$$

On the other hand, it is easy to see that S' is a p-automatic set with complexity at most $(p^{N(S)^2-2} + 1)^d$. By Lemma 7.2, we deduce that

$$\mathrm{comp}_p(S \setminus (S \cap S')) \leq \mathrm{comp}_p(S)\mathrm{comp}_p(S') \leq N(S)(p^{N(S)^2-2} + 1)^d.$$

This shows, using (i), that one can check whether equality (7.1) is satisfied in a finite amount of time.

(iii) We have already shown that we can explicitly determine a p-automaton that recognized S, since the p-complexity of S is at most $N(S)$. Then a classical result of Honkala [22] shows that one can check whether such set is periodic, that is, whether S is the union of a finite set and a finite number of (d-dimensional) arithmetic progressions.

Finally, to obtain all the elements of S when S is finite one can proceed as follows. First, one can check that S is finite as in (ii). Once this has been done, one knows that S is finite and thus Lemma 7.4 implies that

$$S = S \cap \big\{\mathbf{n} \in \mathbb{N}^d \mid \|\mathbf{n}\| \leq p^{N(S)^2-2}\big\}$$

since S has complexity at most $N(S)$. By assumption, all the elements of S can thus be determined in a finite amount of time. This ends the proof. $\qquad\square$

8 Proof of Theorem 1.5

The aim of this section is to show how each step of the proof of Theorem 1.4 can be made effective.

We first recall some notation. Given a polynomial $P(X) \in K[\mathbf{t}][X]$, we define the height of P as the maximum of the degrees of the coefficients of P. The (naive) height of an algebraic power series

$$f(\mathbf{t}) = \sum_{n \in \mathbb{N}} a(\mathbf{n})\mathbf{t}^{\mathbf{n}} \in K[[\mathbf{t}]]$$

is then defined as the height of the minimal polynomial of f, or equivalently, as the minimum of the heights of the nonzero polynomials $P(X) \in K[\mathbf{t}][X]$ that vanishes at f.

We first prove the following effective version of Ore's lemma.

Lemma 8.1 *Let s and H be two positive integers and let $f(\mathbf{t}) \in K[[\mathbf{t}]]$ be an algebraic power series of degree at most s and height at most H. Then there exist polynomials $Q_0, \ldots, Q_s \in K[\mathbf{t}]$ with degree at most Hsp^s such that*

$$\sum_{i=0}^{s} Q_i(\mathbf{t}) f(\mathbf{t})^{p^i} = 0$$

and $Q_0 \neq 0$.

In order to prove Lemma 8.1, we will need the following auxiliary result.

Lemma 8.2 *Let s be a natural number and let $V_0, \ldots, V_s$ be $s + 1$ vectors in $K[\mathbf{t}]^s$ such that each coordinate has degree at most r. Then there exist $Q_0(\mathbf{t}), \ldots, Q_s(\mathbf{t})$ in $K[\mathbf{t}]$ of degree at most rs, not all of which are zero, such that*

$$\sum_{i=0}^{s} Q_i V_i = 0.$$

Proof Let e denote the size of a maximally linearly independent subset of $V_0, \ldots, V_s$. By relabelling if necessary, we may assume that $V_0, \ldots, V_{e-1}$ are linearly independent. Let A denote the $s \times e$ matrix whose $(j+1)$th column is V_j. Then by reordering the coordinates of our vectors if necessary, we may assume that the $e \times e$ submatrix B of A obtained by deleting the bottom $d - e$

rows of A is invertible. Let V_s' denote the vector in $K[\mathbf{t}]^e$ obtained by deleting the bottom $d - e$ coordinates of V_s. Then there is a unique vector X that is a solution to the matrix equation

$$BX = V_s'.$$

Moreover, by Cramer's rule, the ith coordinate of X is the polynomial X_i defined by

$$X_i(\mathbf{t}) := \det(B_i)/\det(B),$$

where B_i is the $e \times e$ matrix obtained by replacing the ith column of B by V_s'. For $0 \leq i \leq e - 1$, we set

$$Q_i(\mathbf{t}) := -\det(B_i).$$

We also set

$$Q_s(\mathbf{t}) := \det(B).$$

Since the entries of B_i and B are all polynomials of degree at most r, we obtain that these polynomials have degree at most $re \leq rs$. Furthermore, by construction

$$\sum_{i=0}^{e-1} X_i V_i = V_s.$$

Letting $Q_i(\mathbf{t}) = 0$ for $e \leq i < s$, we obtain that

$$\sum_{i=0}^{s} Q_i V_i = 0$$

and each Q_i has degree at most rs, as required. □

We are now ready to prove Lemma 8.1.

Proof of Lemma 8.1 By assumption, there exist polynomials $P_0(\mathbf{t}), \ldots,$ $P_s(\mathbf{t}) \in K[\mathbf{t}]$ of degree at most H such that

$$\sum_{i=0}^{s} P_i(\mathbf{t}) f(\mathbf{t})^i = 0$$

and $P_s(\mathbf{t}) \neq 0$.

Let $\mathcal{V}$ denote the $K(\mathbf{t})$-vector space spanned by $1, f, \ldots, f^{s-1}$. For $1 \leq i \leq s$, let e_i denote the standard unit $d \times 1$ vector in $K(\mathbf{t})^s$ whose jth coordinate is equal to the Kronecker delta δ_{ij}. Then we have a surjective

linear map $T : K(\mathbf{t})^s \to \mathcal{V}$ in which we send the vector e_i to f^{i-1}. Let $V = \sum_{i=1}^{s} T(e_i)e_i \in K(\mathbf{t})^s$ and let

$$M := \begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & -X_0(\mathbf{t}) \\ 1 & 0 & 0 & \ldots & 0 & -X_1(\mathbf{t}) \\ 0 & 1 & 0 & \ldots & 0 & -X_2(\mathbf{t}) \\ \vdots & \vdots & \vdots & \ddots & \ldots & \vdots \\ 0 & \ldots & 0 & 1 & 0 & -X_{s-2}(\mathbf{t}) \\ 0 & 0 & \ldots & 0 & 1 & -X_{s-1}(\mathbf{t}) \end{pmatrix} \in M_s(K(\mathbf{t})),$$

where $X_i(\mathbf{t}) := P_i(\mathbf{t})/P_s(\mathbf{t})$ for $i = 0, 1, \ldots, s-1$. Then

$$T(M^n e_1) = f(\mathbf{t})^n.$$

Notice that $M^n = P_s(\mathbf{t})^{-n} C_n$ where C_n is a matrix in $M_s(K[\mathbf{t}])$ whose entries have degree at most nH. Then to find a relation of the form

$$\sum_{i=0}^{s} Q_i(\mathbf{t}) f(\mathbf{t})^{p^i} = 0,$$

it is enough to find a vector

$$[Q_0(\mathbf{t}), \ldots, Q_s(\mathbf{t})] \in K[\mathbf{t}]^{1 \times d}$$

such that

$$P_s(\mathbf{t})^{p^s} Q_0(\mathbf{t})e_1 + P_s(\mathbf{t})^{p^s - p} Q_1(\mathbf{t})C_p e_1 + \cdots + Q_s(\mathbf{t})C_{p^s} e_1 = 0. \quad (8.1)$$

For $0 \le j \le s$, we set

$$V_j := P_s(\mathbf{t})^{p^s - p^j} C_{p^j} e_1. \quad (8.2)$$

We note that V_j is a vector in $K[\mathbf{t}]^s$ such that each coordinate has degree at most Hp^s. Then Lemma 8.2 ensures the existence of polynomials $Q_0(\mathbf{t}), \ldots, Q_s(\mathbf{t})$ in $K[\mathbf{t}]$ of degree at most sHp^s, not all of which are 0, and such that

$$\sum_{j=0}^{s} Q_j V_j = 0.$$

We deduce from (8.1) and (8.2) that

$$\sum_{j=0}^{s} Q_j(\mathbf{t}) f^{p^j}(\mathbf{t}) = 0. \quad (8.3)$$

It thus remains to show that we can choose our polynomials $Q_0, \ldots, Q_s$ such that Q_0 is nonzero. To see this, we let k denote the smallest index such that we have a relation of the form given in (8.3) with the degrees of $Q_0, \ldots, Q_s$ all bounded above by sHp^s and such that Q_k is nonzero. If k is equal to zero, we are done.

We now assume that $k > 0$ and we argue by contradiction. Since $Q_k \neq 0$, we infer from equality (6.3) that there exists a d-tuple $\mathbf{j} \in \Sigma_p^d$ such that $E_{\mathbf{j}}(Q_k) \neq 0$. Since $\sum_{i=k}^{s} Q_i f^{p^i} = 0$, we have

$$E_{\mathbf{j}}\left(\sum_{i=k}^{s} Q_i f^{p^i}\right) = \sum_{i=k}^{s} E_{\mathbf{j}}\left(Q_i f^{p^i}\right) = \sum_{i=k}^{s} E_{\mathbf{j}}(Q_i) f^{p^{i-1}} = 0.$$

Furthermore, one can observe that, for $k \leq i \leq s$, the polynomial $E_{\mathbf{j}}(Q_i)$ has degree at most sHp^s. We thus obtain a new relation of the same type but for which the coefficient of $f^{p^{k-1}}$ is nonzero, which contradicts the minimality of k. This ends the proof. $\qquad\square$

We are now ready to prove Theorem 1.5.

Proof of Theorem 1.5 We first explain our strategy. We assume that $f(\mathbf{t}) \in K[[\mathbf{t}]]$ is an algebraic function and that we know an explicit polynomial $P(X) \in K[\mathbf{t}][X]$ that vanishes at f. Note that from the equation $P(f) = 0$, one can obviously derive explicit effective bounds of the degree and of the height of f. Then we will show how the proof of Theorem 1.4 allows us to derive an effective upper bound for $\mathrm{comp}_p(\mathcal{Z}(f))$. It will thus follows from the results of Sect. 7 that one can effectively determined the set $\mathcal{Z}(f)$ only by looking at the first coefficients of f (which can be computed in a finite amount of time by using the equation $P(f) = 0$).

Let us assume that the degree of f is bounded by s and that the height of f is bounded by H. In order to get an effective upper bound for $\mathrm{comp}_p(\mathcal{Z}(f))$, we have to give effective upper bounds for the cardinality of the sets U, V, W and X introduced all along the proof of Theorem 1.4.

Step 1. In this first step we show how to obtain an effective upper bound for the dimension m of the K-vector space spanned by $\Omega(f)$. We then deduce an effective upper bound for the cardinality of the $\mathbb{F}_p$-vector space U.

This can be deduced from our effective version of Ore's lemma. Indeed, by Lemma 6.1, one can find polynomials $Q_0, \ldots, Q_s \in K[\mathbf{t}]$ with degree at most Hsp^s such that

$$\sum_{i=0}^{s} Q_i(\mathbf{t}) f(\mathbf{t})^{p^i} = 0$$

and $Q_0 \neq 0$. We set $\tilde{f} := Q_0^{-1} f$. Then

$$\tilde{f} = \sum_{i=1}^{s} R_i \tilde{f}^{p^i}, \tag{8.4}$$

where $R_i = -Q_i Q_0^{p^i - 2}$. Then each R_i has degree at most $Hsp^s(p^i - 1)$. Set $M := Hsp^s(p^s - 1)$ and

$$\mathcal{H} := \left\{ h \in K((\mathbf{t})) \, \middle| \, h = \sum_{i=0}^{s} S_i \tilde{f}^{p^i} \text{ such that } S_i \in K[\mathbf{t}] \text{ and } \deg S_i \leq M \right\}. \tag{8.5}$$

Furthermore, $\mathcal{H}$ is a K-vector space of dimension at most

$$(s+1) \binom{M+d}{M}.$$

Just as in the proof of Lemma 6.2, one can check that f belongs to $\mathcal{H}$ and that $\mathcal{H}$ is closed under the action of Ω. It follows that the K-vector space spanned by $\Omega(f)$ is contained in $\mathcal{H}$. There thus exists an effective constant $N_0 := (s+1)\binom{M+d}{M}$ such that the K-vector space spanned by $\Omega(f)$ has dimension

$$m \leq N_0. \tag{8.6}$$

We recall that K_0 denotes the subfield of K generated by the coefficients of $f_1, \ldots, f_m$ and all the elements $\lambda(i, \mathbf{j}, k)$ $1 \leq i, k \leq m$ and $\mathbf{j} \in \{0, 1, \ldots, p-1\}^d$, and that U is defined as the finite-dimensional $\mathbb{F}_p$-vector subspace of K_0 spanned by the elements $\lambda(i, \mathbf{j}, k)$, $1 \leq i, k \leq m$ and $\mathbf{j} \in \{0, 1, \ldots, p-1\}^d$, and by 1. We thus deduce from (8.6) that there exist an effective upper bound $N_1 := p^{1+p^d N_0^2}$ such that

$$\text{Card}(U) \leq N_1. \tag{8.7}$$

Step 2. From Derksen's proposition (Proposition 6.1), we know that there exists a finite-dimensional $\mathbb{F}_p$-vector subspace V of K_0 containing U such that $\pi_i(VU) \subseteq V$ for $1 \leq i \leq r$. In this second step, we show how to obtain an effective upper bound for the cardinality of such a vector space V.

In the proof of Lemma 6.3, we have shown that K_0 is a finitely generated field extension of $\mathbb{F}_p$ that can be generated by the $\lambda(i, \mathbf{j}, k)$ and the coefficients of a finite number of some explicit polynomials. We write

$$K_0 = \mathbb{F}_p(X_1, \ldots, X_r)(a_1, \ldots, a_s),$$

where $X_1, \ldots, X_r$ are algebraically independent over $\mathbb{F}_p$ and $a_1, \ldots, a_s$ form a basis for K_0 as an $\mathbb{F}_p(X_1, \ldots, X_r)$-vector space; moreover, we may assume

that for each i and j, we have $a_i a_j$ is an $\mathbb{F}_p(X_1, \ldots, X_r)$-linear combination of $a_1, \ldots, a_s$ in which the numerators and denominators of the coefficients are polynomials in $\mathbb{F}_p[X_1, \ldots, X_r]$ whose degrees are uniformly bounded by some explicit constant N_2.

Let $T_1, \ldots, T_n$ denote such a set of generators of K_0 with the following properties.

   (i) $T_i = X_i$ for $i \leq r$.
   (ii) $T_{r+j} = a_j$ for $j \leq s$.
   (iii) $T_n = 1$.
   (iv) $\{T_1, \ldots, T_n\}$ contains all the $\lambda(i, \mathbf{j}, k)$.

Note that from Step 1 and the proof of Lemma 6.3 we can obtain an explicit upper bound for the integer n.

An easy induction shows that for $1 \leq j \leq s$, a_j^p is an $\mathbb{F}_p(X_1, \ldots, X_r)$-linear combination of $a_1, \ldots, a_s$ in which the coefficients are rational functions whose numerators and denominators have degrees uniformly bounded by

$$N_3 := N_2 \left(2s^{p-2} + \frac{s^{p-2} - s}{s-1} \right). \tag{8.8}$$

We now regard K_0 as an s-dimensional $\mathbb{F}_p(X_1, \ldots, X_r)$-vector space. Then we may regard the $\mathbb{F}_p(X_1, \ldots, X_r)$-span of $a_1^p, \ldots, a_s^p$ as a subspace of

$$\mathbb{F}_p(X_1, \ldots, X_r)^s$$

spanned by s vectors whose coordinates are rational functions whose numerators and denominators have degrees uniformly bounded by N_3. We can effectively compute the dimension of this space and a basis. We let t denote the dimension of this vector space and by relabelling if necessary, we may assume that $a_1^p, \ldots, a_t^p$ form a basis. Then there exist $\ell_1, \ldots, \ell_{s-t}$ such that $\{a_1^p, \ldots, a_t^p, a_{\ell_1}, \ldots, a_{\ell_{s-t}}\}$ forms a basis for K_0 as a $\mathbb{F}_p(X_1, \ldots, X_r)$-vector space. Moreover, using Cramer's rule, we can express each a_j as a $\mathbb{F}_p(X_1, \ldots, X_r)$-linear combination of $a_1^p, \ldots, a_t^p, a_{\ell_1}, \ldots, a_{\ell_{s-t}}$ in which the numerators and denominators have degrees uniformly bounded by

$$N_4 := 2N_3 st. \tag{8.9}$$

To see this, let $\phi : K_0 \to \mathbb{F}_p(X_1, \ldots, X_r)^s$ be the $\mathbb{F}_p(X_1, \ldots, X_r)$-linear isomorphism which sends a_i to the vector with a 1 in the ith coordinate and zeros in all other coordinates. Let A denote the $s \times s$ matrix whose ith row is equal to $\phi(a_i^p)$ for $i \leq t$ and is equal to $\phi(a_{\ell_{t-i}})$ for $i > t$. Then the entries of A are rational functions whose numerators and denominators have degrees that are uniformly bounded by N_3. Note that expressing a_j as a $\mathbb{F}_p(X_1, \ldots, X_r)$-linear combination of $a_1^p, \ldots, a_t^p, a_{\ell_1}, \ldots, a_{\ell_{t-s}}$ is the same as solving the

matrix equation

$$Ax = e_j,$$

where e_j is the vector whose jth coordinate is 1 and whose other coordinates are 0. By Cramer's rule, the ith coordinate of x is a ratio of two $s \times s$ determinants, each of which have entries which are rational functions in $\mathbb{F}_p(X_1, \ldots, X_r)$ whose numerators and denominators have degrees that are uniformly bounded by N_3, and such that the bottom $s - t$ rows consist of constants. Note that the determinant of an $s \times s$ matrix whose entries are rational functions is a rational function; moreover, we can take the denominator to be the product of the denominators of the entries. Since our matrices have a total of st entries which are not constant, we obtain a bound of N_3st for the degrees of the denominators of our determinants. It is easy to check that this bound applies to the degrees of the numerators as well. When we take a ratio of these determinants, this can at most double this bound on the degrees of the numerators and denominators. Thus we can express each a_j as a $\mathbb{F}_p(X_1, \ldots, X_r)$-linear combination of $a_1^p, \ldots, a_t^p, a_{\ell_1}, \ldots, a_{\ell_{t-s}}$ in which the degrees of the numerators and denominators are uniformly bounded by $2N_3st$, as claimed.

Notice that

$$S := \left\{ T_1^{i_1} \cdots T_n^{i_n} \mid 0 \le i_1, \ldots, i_n < p \right\}$$

spans K_0 as a $K_0^{\langle p \rangle}$-vector space. Observe also that every polynomial $Q \in \mathbb{F}_p[T_1, \ldots, T_n]$ can be decomposed as

$$Q = \sum_{f \in S} Q_f^p f, \tag{8.10}$$

where the Q_f are polynomials in $\mathbb{F}_p[T_1, \ldots, T_n]$ of degree at most $\lfloor \deg Q / p \rfloor$.

Let us choose S_0 to be the subset of S corresponding to the monomials from the set formed by the union of

$$\left\{ X_1^{i_1} \cdots X_r^{i_r} \mid 0 \le i_1, \ldots, i_r < p \right\}$$

and

$$\left\{ X_1^{i_1} \cdots X_r^{i_r} a_{\ell_j} \mid 0 \le i_1, \ldots, i_r < p, 1 \le j \le s - t \right\}.$$

Then S_0 is a basis for K_0 as a $K_0^{\langle p \rangle}$-vector space. Thus for $T_1^{i_1} \cdots T_n^{i_n} \in S$, we have

$$T_1^{i_1} \cdots T_n^{i_n} = \sum_{h \in S_0} \alpha_{h, i_1, \ldots, i_n}^p h$$

for some coefficients $\alpha_{h,i_1,\ldots,i_n} \in K_0$. We may pick some nonzero polynomial $H(T_1, \ldots, T_n)$ such that

$$H(T_1, \ldots, T_n)^p T_1^{i_1} \cdots T_n^{i_n} = \sum_{h \in S_0} A_{h,i_1,\ldots,i_n}^p h, \qquad (8.11)$$

where

$$A_{h,i_1,\ldots,i_n} \in \mathbb{F}_p[T_1, \ldots, T_n]$$

for all

$$(h, i_1, \ldots, i_n) \in S_0 \times \{0, 1, \ldots, p-1\}^n.$$

We let

$$M' := \max \{\deg H, \deg A_{h,i_1,\ldots,i_n}\} \qquad (8.12)$$

where the maximum is taken over all

$$(h, i_1, \ldots, i_n) \in S_0 \times \{0, 1, \ldots, p-1\}^n.$$

We claim that it is possible to obtain an effective upper bound for M', once the set of generators and the basis are known. To see this, note that we write $T_i = \sum_{j=1}^{s} \phi_{i,j}(X_1, \ldots, X_r) a_s$, where each $\phi_{i,j}$ is a rational function in $X_1, \ldots, X_r$, where we assume that the degrees of the numerators and denominators of the $\phi_{i,j}$ are uniformly bounded by some explicit constant N_5.

Note that by construction, a monomial $T_1^{i_1} \cdots T_n^{i_n}$ with $0 \le i_1, \ldots, i_n < p$ is an $\mathbb{F}_p(X_1, \ldots, X_r)$-linear combination of $a_1, \ldots, a_s$ in which the coefficients are rational functions whose numerators and denominators have degrees uniformly bounded by

$$N_6 := (N_2 + N_5)(p-1)ns^{2(p-1)n}. \qquad (8.13)$$

To see this, we claim more generally that a monomial $T_1^{j_1} \cdots T_n^{j_n}$ can be expressed as a $\mathbb{F}_p(X_1, \ldots, X_r)$-linear combination of $a_1, \ldots, a_s$ in which the coefficients are rational functions whose numerators and denominators have degrees uniformly bounded by

$$(N_2 + N_5)(j_1 + \cdots + j_n)s^{2(j_1 + \cdots + j_n)}.$$

We prove this by induction on $j_1 + \cdots + j_n$. When $j_1 + \cdots + j_n = 1$, the claim is trivially true. So we assume that the claim holds whenever $j_1 + \cdots + j_n < k$ and we consider the case that $j_1 + \cdots + j_n = k$. Then $j_i \ge 1$ for some i. Thus we may write

$$T_1^{j_1} \cdots T_n^{j_n} = T_i \cdot T_1^{j_1} \cdots T_i^{j_i-1} \cdots T_n^{j_n}.$$

By the inductive hypothesis,

$$T_1^{j_1} \cdots T_i^{j_i-1} \cdots T_n^{j_n} = \sum_{\ell=1}^{s} \psi_\ell a_\ell,$$

where each ψ_ℓ is a rational function whose numerator and denominator have degrees bounded by $(N_2 + N_5)(k-1)s^{2k-2}$. Thus

$$T_i \cdot T_1^{j_1} \cdots T_i^{j_i-1} \cdots T_n^{j_n} = \left(\sum_{j=1}^{s} \phi_{i,j} a_j \right) \left(\sum_{\ell=1}^{s} \psi_\ell a_\ell \right)$$

$$= \sum_{1 \le j, \ell \le s} (\phi_{i,j} \psi_\ell) a_j a_\ell.$$

Recall that by assumption each $a_j a_\ell$ is a $\mathbb{F}_p(X_1, \ldots, X_r)$-linear combination of $a_1, \ldots, a_s$ in which the degrees of the numerators and denominators are uniformly bounded by N_2. Thus the coefficient of each a_j is a linear combination consisting of s^2 terms whose numerators and denominators have degrees bounded by $N_5 + (N_2 + N_5)(k-1)s^{2k-2} + N_2$ and hence can be expressed as a rational function whose numerator and denominator have degrees bounded by $(N_2 + N_5)(1 + (k-1)s^{2k-2})s^2 \le (N_2 + N_5)ks^{2k}$. This gives the bound (8.13), as claimed.

Then we may write

$$T_1^{i_1} \cdots T_n^{i_n} = \sum_{j=1}^{s} \frac{C_j(X_1, \ldots, X_r)}{D(X_1, \ldots, X_r)^p} a_j,$$

where $C_1, \ldots, C_s, D$ are polynomials of degree at most $N_6 sp$. Furthermore, we showed in (8.9) that each a_j can be written as a $\mathbb{F}_p(X_1, \ldots, X_s)$-linear combination of $\{a_1^p, \ldots, a_t^p, a_{\ell_1}, \ldots, a_{\ell_{s-t}}\}$ in which the coefficients have numerators and denominators uniformly bounded by N_4. Thus we may write

$$T_1^{i_1} \cdots T_n^{i_n} = \sum_{j=1}^{t} \frac{\widehat{C}_j(X_1, \ldots, X_r)}{\widehat{D}(X_1, \ldots, X_r)^p} a_j^p + \sum_{j=1}^{s-t} \frac{\widehat{C}_j(X_1, \ldots, X_r)}{\widehat{D}(X_1, \ldots, X_r)^p} a_{\ell_j},$$

where $\widehat{C}_1, \ldots, \widehat{C}_s, \widehat{D}$ have degrees bounded by

$$(N_4 + N_6)sp.$$

Since S_0 forms a basis for $K_0^{\langle p \rangle}$, this ensures that

$$M' \le (N_4 + N_6)sp + p. \tag{8.14}$$

Now, we set

$$U_0 := \mathbb{F}_p H^{-1} + \sum_{j=1}^{n} \mathbb{F}_p T_j. \tag{8.15}$$

Since $\{1\} \cup \{\lambda_{i,\mathbf{j},k} \mid 1 \le i, k \le m, \mathbf{j} \in \{0, 1, \ldots, p-1\}^d\} \subseteq \{T_1, \ldots, T_n\}$, we have

$$U \subseteq U_0. \tag{8.16}$$

Let k be a positive integer. We infer from (8.15) that U_0^k is contained in the $\mathbb{F}_p$-vector space spanned by the set

$$\mathcal{K} := \left\{ H^{-j_0} T_1^{j_1} \cdots T_n^{j_n} \;\Big|\; \sum_{i=0}^{n} j_i \le k \right\}.$$

Then, every element L of $\mathcal{K}$ can be written as

$$L = H^{-p i_0} \big(H^{\ell} T_1^{j_1} \cdots T_n^{j_n} \big) =: H^{-p(i_0+1)} H^p Q \tag{8.17}$$

where $Q := H^{\ell} T_1^{j_1} \cdots T_n^{j_n}$, $0 \le \ell < p$, $0 \le i_0 \le \lfloor k/p \rfloor$ and $\sum_{i=1}^{n} j_i \le k - p i_0$. Thus Q is a polynomial in $\mathbb{F}_p[T_1, \ldots, T_n]$ of degree at most $(p \deg H + k - p i_0)$. By (8.10), Q can be decomposed as

$$Q = \sum_{f \in S} Q_f^p f,$$

where Q_f are polynomials in $\mathbb{F}_p[T_1, \ldots, T_n]$ of degree at most $\deg H + \lfloor k/p \rfloor - i_0$. We deduce that

$$H^{-(i_0+1)} Q_f \in U_0^{M' + \lfloor k/p \rfloor + 1}.$$

Thus we have

$$H^p Q = \sum_{f \in S} Q_f^p \big(H^p f \big). \tag{8.18}$$

Furthermore, by assumption, for $f \in S$

$$H^p f \in \bigoplus_{h \in S_0} \big(U_0^{M'} \big)^{\langle p \rangle} h. \tag{8.19}$$

We infer from (8.17), (8.18) and (8.19) that

$$L \in \bigoplus_{h \in S_0} \big(U_0^{2M' + \lfloor k/p \rfloor + 1} \big)^{\langle p \rangle} h$$

and thus

$$U_0^k \subseteq \bigoplus_{h \in S_0} \left(U_0^{2M' + \lfloor k/p \rfloor + 1} \right)^{\langle p \rangle} h.$$

Let $k_0 := \lfloor 2(M'+1)p/(p-1) \rfloor + 1$ and set $V := U_0^{k_0-1}$. This choice of k_0 implies that $\pi_i(VU) \subseteq V$. Furthermore, $U \subseteq V$ and the cardinality of V is bounded by Card $U_0^{k_0-1} \leq (\text{Card } U_0)^{k_0-1} \leq p^{(n+1)(k_0-1)}$. Since one could find an effective upper bound for n and since inequality (8.14) provides an effective upper bound for M' (and thus for k_0), we obtain that there exists an effective constant N_7 such that

$$\text{Card } V \leq N_7.$$

Step 3. In this last step, we show how to derive from Step 2 effective upper bounds for the cardinality of the sets W and X, from which we will finally deduce an effective upper bound for $\text{Comp}_p \mathcal{Z}(f)$.

We just show that it is possible to get an effective upper bound N_7 for the cardinality of the $\mathbb{F}_p$-vector space V. We now recall that the set W is defined by

$$W := V a_1 + \cdots + V a_m.$$

We thus have Card $W \leq (\text{Card } V)^m$, and we infer from (8.6) that there exists an effective constant $N_8 := N_7^{N_0}$ such that

$$\text{Card } W \leq N_8. \tag{8.20}$$

We recall that given a map $b : \mathbb{N}^d \to K_0$, the map $\chi_b : \mathbb{N}^d \to \{0, 1\}$ is defined by

$$\chi_b(\mathbf{n}) = \begin{cases} 0 & \text{if } b(\mathbf{n}) \neq 0 \\ 1 & \text{if } b(\mathbf{n}) = 0. \end{cases} \tag{8.21}$$

We recall that the set X is defined by

$$X := \{ \chi_{b_1} \cdots \chi_{b_t} \mid t \geq 0, b_1, \ldots, b_t \in W \}.$$

Since $\chi_b^2 = \chi_b$ for all $b \in W$ and since the product of maps χ_b is commutative, we get that

$$\text{Card } X \leq 2^{\text{Card } W}.$$

Thus we infer from (8.20) the existence of an effective constant $N_9 := 2^{N_8}$ such that

$$\text{Card } X \leq N_9.$$

On the other hand, the proof of Theorem 1.4 shows that the p-kernel of $\mathcal{Z}(f)$ is contained in X, which implies that

$$\mathrm{comp}_\mathrm{p}\big(\mathcal{Z}(f)\big) \leq N_9.$$

This ends the proof.   □

9 Concluding remarks

We end our paper with a few comments. We note that Derksen [10] also proved a refinement of his Theorem 1.2. Let us state his result. Let p be a prime number and let q be a power of p. Given $c_0, \ldots, c_d \in \mathbb{Q}^*$ with $(q - 1)c_i \in \mathbb{Z}$ for $i \in \{1, \ldots, d\}$ and $c_0 + \cdots + c_d \in \mathbb{Z}$, we define

$$\tilde{S}_q(c_0, \ldots, c_d) := \big\{ c_0 + c_1 q^{i_1} + \cdots + c_d q^{i_d} \mid i_1, \ldots, i_d \geq 0 \big\}$$

and we take

$$S_q(c_0, \ldots, c_d) := \mathbb{N} \cap \tilde{S}_q(c_0, \ldots, c_d).$$

If $c_i > 0$ for some $i \in \{1, \ldots, d\}$, we say that $S_q(c_0, \ldots, c_d)$ is an elementary p-nested set of order d. We say that a subset of the natural numbers is p-nested of order d if it is a finite union of elementary p-nested sets of order at most d with at least one set having order exactly d. We then say that a subset of the natural numbers is p-normal of order d if it is, up to a finite set, the union of a finite number of arithmetic progressions along with a p-nested set of order d. Derksen [10, Theorem 1.8] proved that the zero set of a linear recurrence of order d is a p-normal set of order at most equal to $d - 2$. Of course, this refines the fact that such a set is p-automatic.

We already observed in the introduction that Theorem 1.4 is in some sense best possible since any p-automatic subset of $\mathbb{N}^d$ can be obtained as the set of vanishing coefficients of an algebraic power series in $\mathbb{F}_p[[t_1, \ldots, t_d]]$. However, one might hope that a refinement, involving a reasonable version of multidimensional p-normal set, could hold if we restrict our attention to multivariate rational functions. This is actually not the case. Even for bivariate rational functions over finite fields, the set of vanishing coefficients can be rather pathological. Indeed, Furstenberg [18] showed that the diagonal of a multivariate rational power series with coefficients in a field of positive characteristic is an algebraic power series in one variable.[1] Moreover, the converse holds for any field: any one variable algebraic power series can be obtained

---

[1]Deligne [8] generalized this result to diagonals of algebraic power series with coefficients in a field of positive characteristic.

as the diagonal of a bivariate rational power series.[2] In light of Christol's theorem, this implies in particular that any p-automatic subset of $\mathbb{N}$ can be realized as the diagonal of the set of vanishing coefficients of a bivariate rational power series with coefficients in $\mathbb{F}_p$.

Nevertheless, we may imagine that a similar refinement of Theorem 1.4 does exist for the special rational functions that appear in the Diophantine applications given in Sects. 2, 3 and 4. Finally, since these applications only involve multivariate rational functions, it would be interesting to find natural Diophantine problems that would involve some sets of vanishing coefficients of algebraic irrational multivariate power series.

Addendum   During the last stage of the writing of this paper, the authors learned about a related work (though not written in terms of automata) of Derksen and Masser [11]. These authors obtain in particular strong effective results for the general S-unit equations over fields of positive characteristic and more generally for the Mordell–Lang theorem, in the special case of linear subvarieties of $G_m^n(K)$ for fields K of positive characteristic.

References

1. Allouche, J.-P., Cateland, E., Gilbert, W.J., Peitgen, H.-O., Shallit, J.O., Skordev, G.: Automatic maps in exotic numeration systems. Theory Comput. Syst. **30**, 285–331 (1997)
2. Allouche, J.-P., Shallit, J.: Automatic Sequences. Theory, Applications, Generalizations. Cambridge University Press, Cambridge (2003)
3. Bézivin, J.-P.: Une généralisation du théorème de Skolem–Mahler–Lech. Q. J. Math. Oxf. **40**, 133–138 (1989)
4. Cerlienco, L., Mignotte, M., Piras, F.: Suites récurrentes linéaires : propriétés algébriques et arithmétiques. Enseign. Math. **33**, 67–108 (1987)
5. Christol, G.: Ensembles presque périodiques k-reconnaissables. Theor. Comput. Sci. **9**, 141–145 (1979)
6. Christol, G., Kamae, T., Mendès France, M., Rauzy, G.: Suites algébriques, automates et substitutions. Bull. Soc. Math. Fr. **108**, 401–419 (1980)
7. Cobham, A.: On the base-dependence of sets of numbers recognizable by finite automata. Math. Syst. Theory **3**, 186–192 (1969)
8. Deligne, P.: Intégration sur un cycle évanescent. Invent. Math. **76**, 129–143 (1983)
9. Denef, J., Lipshitz, L.: Algebraic power series and diagonals. J. Number Theory **26**, 46–67 (1987)
10. Derksen, H.: A Skolem-Mahler-Lech theorem in positive characteristic and finite automata. Invent. Math. **168**, 175–224 (2007)

---

[2]This result is essentially proved in [18]. Denef and Lipshitz [9] actually obtained the following stronger result: any algebraic power series in n variables with coefficients in an arbitrary field can be obtained as the diagonal of a rational power series in $2n$ variables.

11. Derksen, H., Masser, D.: Linear equations over multiplicative groups, recurrences, and mixing I. Manuscript (2010)
12. Eilenberg, S.: Automata, Languages, and Machines, vol. A. Academic Press, San Diego (1974)
13. Everest, G., van der Poorten, A., Shparlinski, I., Ward, T.: Recurrence Sequences. Mathematical Surveys and Monographs, vol. 104. American Mathematical Society, Providence (2003)
14. Evertse, J.-H.: On sums of S-units and linear recurrences. Compos. Math. **53**, 225–244 (1984)
15. Evertse, J.-H., Györy, K., Stewart, C.L., Tijdeman, R.: S-unit equations and their applications. In: New Advances in Transcendence Theory, Durham, 1986, pp. 110–174. Cambridge Univ. Press, Cambridge (1988)
16. Evertse, J.-H., Schlickewei, H.P., Schmidt, W.M.: Linear equations in variables which lie in a multiplicative group. Ann. Math. **155**, 807–836 (2002)
17. Faltings, G.: Diophantine approximation on abelian varieties. Ann. Math. **133**, 549–576 (1991)
18. Furstenberg, H.: Algebraic functions over finite fields. J. Algebra **7**, 271–277 (1967)
19. Ghioca, D.: The isotrivial case in the Mordell–Lang Theorem. Trans. Am. Math. Soc. **360**, 3839–3856 (2008)
20. Hansel, G.: Une démonstration simple du théorème de Skolem–Mahler–Lech. Theor. Comput. Sci. **43**, 91–98 (1986)
21. Harase, T.: Algebraic elements in formal power series rings. Isr. J. Math. **63**, 281–288 (1988)
22. Honkala, J.: A decision method for the recognizability of sets defined by number systems. Theor. Inform. Appl. **20**, 395–403 (1986)
23. Hrushovski, E.: The Mordell-Lang conjecture for function fields. J. Am. Math. Soc. **9**, 667–690 (1996)
24. Kedlaya, K.: Finite automata and algebraic extensions of function fields. J. Théor. Nombres Bordeaux **18**, 379–420 (2006)
25. Lang, S.: Integral points on curves. Publ. Math. IHÉS **6**, 27–43 (1960)
26. Lech, C.: A note on recurring series. Ark. Mat. **2**, 417–421 (1953)
27. Mahler, K.: Zur Approximation algebraischer Zahlen, I. (Über den grössten Primteiler binärer Formen). Math. Ann. **107**, 691–730 (1933)
28. Mahler, K.: Eine arithmetische Eigenschaft der Taylor–Koeffizienten rationaler Funktionen. Proc. K. Ned. Akad. Wet. **38**, 50–60 (1935)
29. Mahler, K.: On the Taylor coefficients of rational functions. Proc. Camb. Philos. Soc. **52**, 39–48 (1956)
30. Mahler, K.: Addendum to the paper "On the Taylor coefficients of rational functions". Proc. Camb. Philos. Soc. **53**, 544 (1957)
31. Masser, D.: Mixing and linear equations over groups in positive characteristic. Isr. J. Math. **142**, 189–204 (2004)
32. Moosa, R., Scanlon, T.: F-structures and integral points on semiabelian varieties over finite fields. Am. J. Math. **126**, 473–522 (2004)
33. van der Poorten, A.J.: Some facts that should be better known, especially about rational functions. In: Number Theory and Applications, Banff, AB, 1988. NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., vol. 265, pp. 497–528. Kluwer Academic, Dordrecht (1989)
34. van der Poorten, A.J., Schlickewei, H.P.: Additive relations in fields. J. Aust. Math. Soc. **51**, 154–170 (1991)
35. Salon, O.: Suites automatiques à multi-indices et algébricité. C. R. Acad. Sci. Paris Sér. I Math. **305**, 501–504 (1987)
36. Schmidt, K.: The dynamics of algebraic Z^d-actions. In: European Congress of Mathematics, vol. I, Barcelona, 2000. Progress in Mathematics, vol. 201, pp. 543–553. Birkhäuser, Basel (2001)

37. Schmidt, K., Ward, T.: Mixing automorphisms of compact groups and a theorem of Schlickewei. Invent. Math. **111**, 69–76 (1993)
38. Sharif, H., Woodcock, C.F.: Algebraic functions over a field of positive characteristic and Hadamard products. J. Lond. Math. Soc. **37**, 395–403 (1988)
39. Skolem, T.: Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen und diophantischer Gleichungen. In: Comptes Rendus Congr. Math. Scand., Stockholm, pp. 163–188 (1934)
40. Tao, T.: Structure and Randomness, Pages from Year One of a Mathematical Blog. American Mathematical Society, Providence (2008)
41. Voloch, J.F.: The equation $ax + by = 1$ in characteristic p. J. Number Theory **73**, 195–200 (1998)