A SHARPER MULTIVARIATE CHRISTOL'S THEOREM WITH APPLICATIONS TO DIAGONALS AND HADAMARD PRODUCTS

BORIS ADAMCZEWSKI, ALIN BOSTAN, AND XAVIER CARUSO

ABSTRACT. We provide a new proof of the multivariate version of Christol's theorem about algebraic power series with coefficients in finite fields, as well as of its extension to perfect ground fields of positive characteristic obtained independently by Denef and Lipshitz, Sharif and Woodcock, and Harase. Our proof is elementary, effective, and allows for much sharper estimates. We discuss various applications of such estimates, in particular to a problem raised by Deligne concerning the algebraicity degree of reductions modulo p of diagonals of multivariate algebraic power series with integer coefficients.

1. INTRODUCTION

Rational and algebraic power series play an important role in various areas of mathematics, and especially in number theory and combinatorics. There are two fundamental results concerning rationality of power series in one variable. The first one is that, given an arbitrary field k, a power series $f(t) = \sum_{n=0}^{\infty} a(n)t^n \in k[[t]]$ is rational if and only if its coefficient sequence $a(n)$ satisfies a linear recurrence with coefficients in k. The second one is the famous Skolem-Mahler-Lech theorem stating that, when k is a field of characteristic zero, the zero set

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

of a rational power series $f \in k[[t]]$ is a *periodic* set, that is the union of a finite set and of finitely many arithmetic progressions. When k has characteristic zero, it seems difficult to obtain similar results for *algebraic* power series, *i.e.* power series $f \in k[[t]]$ for which there exists a nonzero bivariate polynomial $P \in k[t, y]$ such that $P(t, f) = 0$. Although it is known that the coefficient sequences of univariate algebraic power series do satisfy linear recurrences with polynomial coefficients, a characterization of such sequences is still lacking. On the other hand, proving that the corresponding zero sets are periodic remains a challenging open problem (cf. [Zan09, p. 176]). The situation in several variables is worse and not much is known or

Key words and phrases. Christol's theorem; automatic sequences; algebraic power series; diagonals; Hadamard products.

Partially supported by the French grant DeRerumNatura (ANR-19-CE40-0018), and by the French–Austrian project EAGLES (ANR-22-CE91-0007 & FWF I6130-N).

even conjectured about zero sets of multivariate rational power series; this is very unfortunate, as they encode interesting Diophantine problems.

In a short but influential paper, Furstenberg [Fur67] observed for the first time that algebraic power series over ground fields of positive characteristic have a very particular structure. For instance, when $k = \mathbb{F}_q$ is a finite field, he proved that the ring of algebraic power series is closed under the Hadamard product and that $\sum_{n=0}^{\infty} a(n)t^n \in \mathbb{F}_q[[t]]$ is algebraic over $\mathbb{F}_q(t)$ if and only if $\sum_{n:a(n)=a} t^n$ is algebraic for every $a \in \mathbb{F}_q$; these two properties do not hold in characteristic zero. Later, Christol [Chr79] elaborated on Furstenberg's approach and proved the following beautiful result.

Theorem A (Christol)**.** A power series $\sum_{n=0}^{\infty} a(n)t^n \in \mathbb{F}_q[[t]]$ is algebraic over $\mathbb{F}_q(t)$ if and only if its coefficient sequence $a(n)$ can be generated by a finite q-automaton.

We refer the reader to [AS03, Chapters 4 and 5] for the notions of finite automata and automatic sequences. A different proof of Christol's theorem was given in [CKMFR80], from which Salon [Sal87, Sal86] also derived a natural extension to multivariate power series. What makes Christol's theorem deep and fascinating is that it establishes an intimate connection between two important objects coming from seemingly unrelated areas.

When the ground field k is an arbitrary field of positive characteristic, the characterization of algebraic power series in terms of finite automata is somewhat lost but there are still important related results. Furstenberg [Fur67] proved that the diagonal of a multivariate rational power series remains algebraic; this result was generalized by Deligne [Del84] to diagonals of multivariate algebraic power series. A related result is that the ring of multivariate algebraic power series is closed under the Hadamard product (cf. [DL87, SW88, Har88]). More recently, Derksen [Der07] found an appropriate version of the Skolem-Mahler-Lech theorem involving finite automata. Derksen's theorem was then generalized to zero sets of arbitrary multivariate algebraic power series by Adamczewski and Bell [AB12].

It turns out that all the previously mentioned results (in positive characteristic) can be proved by using some splitting process associated with the Frobenius map (cf. Equality (1.1)). Let k be a perfect field of characteristic $p > 0$. Then the Frobenius endomorphism F, that maps x to x^p, is an automorphism of k. Let $\boldsymbol{t} = (t_1, \dots, t_n)$ be indeterminates, and let K denote the field of fractions of the ring of power series $k[[\boldsymbol{t}]] := k[[t_1, \dots, t_n]]$. The Frobenius map F extends naturally to K as an injective homomorphism. We let $K^{\langle p \rangle}$ denote the image of K by F, so that F defines an isomorphism between K and $K^{\langle p \rangle}$. Then K is a $K^{\langle p \rangle}$-vector space of dimension p^n, a basis being given by all the products of the form $\boldsymbol{t}^{\boldsymbol{r}} := t_1^{r_1} \cdots t_n^{r_n}$, with $\boldsymbol{r} := (r_1, \dots, r_n) \in \{0, \dots, p-1\}^n$. Thus, every $f \in K$ has a unique expansion of the form

$$f = \sum_{\boldsymbol{r} \in \{0,\dots,p-1\}^n} \boldsymbol{t}^{\boldsymbol{r}} f_{\boldsymbol{r}}\,. \tag{1.1}$$

For every $\boldsymbol{r} \in \{0, \dots, p-1\}^n$, the *section operator* $S_{\boldsymbol{r}}$ is defined by

$$S_{\boldsymbol{r}}(f) \coloneqq \mathsf{F}^{-1}(f_{\boldsymbol{r}})\,. \tag{1.2}$$

Section operators are semilinear maps from K into itself. For a power series $f \coloneqq \sum_{\boldsymbol{i}\in\mathbb{N}^n} a(\boldsymbol{i})\boldsymbol{t}^{\boldsymbol{i}} \in k[[\boldsymbol{t}]]$, we have

$$S_{\boldsymbol{r}}(f) = \sum_{\substack{\boldsymbol{i}\in\mathbb{N}^n \\ \boldsymbol{i}=(i_1,\dots,i_n)}} a(pi_1+r_1,\dots,pi_n+r_n)^{1/p}\boldsymbol{t}^{\boldsymbol{i}} \in k[[\boldsymbol{t}]]\,.$$

We let Ω_n denote the monoid generated by all section operators under composition.

At the end of the 1980s, Denef and Lipshitz [DL87], Sharif and Woodcock [SW88] and Harase [Har88] obtained independently the following nice characterization of multivariate algebraic power series in terms of section operators.

Theorem B. Let k be a perfect field of characteristic p. A power series $f \in k[[\boldsymbol{t}]]$ is algebraic over $k(\boldsymbol{t})$ if and only if there exists a finite-dimensional k-vector space $W \subset K$ containing f and invariant under the action of Ω_n.

Remark 1.1. When $k = \mathbb{F}_q$, the putative vector space W has to be finite and its existence is thus equivalent to the finiteness of the orbit of f under Ω_n. By a classical result of Eilenberg, the latter property is itself equivalent to the fact that the coefficient sequence of f is q-automatic, so one recovers the multivariate extension of Christol's theorem.

In this paper, we investigate the problem of finding a sharp quantitative version of Theorem B, *i.e.* finding a k-vector space W having the smallest possible dimension in terms of the "complexity" of the algebraic power series f.

The particular case of multivariate rational power series can be treated in a satisfactory way. Indeed, if $f(\boldsymbol{t}) = A(\boldsymbol{t})/B(\boldsymbol{t}) \in k[[\boldsymbol{t}]]$ for some $A, B \in k[\boldsymbol{t}]$, whose degree in t_i is at most h_i, then it is easy to prove that the k-vector space

$$W \coloneqq \left\{ \frac{P(\boldsymbol{t})}{B(\boldsymbol{t})} : P \in k[\boldsymbol{t}],\ \deg_{t_i} P \le h_i, 1 \le i \le n \right\}$$

contains f and is invariant under Ω_n. Similarly, if the total degree of both A and B is at most h, then the same conclusion applies to

$$W' \coloneqq \left\{ \frac{P(\boldsymbol{t})}{B(\boldsymbol{t})} : P \in k[\boldsymbol{t}],\ \deg_{\boldsymbol{t}} P \le h \right\}\,.$$

Furthermore, W and W' have dimensions $(h_1+1)\cdots(h_n+1)$ and $\binom{n+h}{n}$, respectively.

On the other hand, the case of algebraic irrational multivariate power series is known to be more difficult and the known estimates are much weaker. To summarize roughly, the main aim of this paper is to develop a unified method, which is able to deal with arbitrary multivariate algebraic

power series as if they were rational. In this direction, our main results are Theorem 1.2 and Corollary 1.4. The proof of Theorem 1.2 follows a new approach recently initiated in [BCCD19] for the case $n = 1$. Its main feature is that it combines all the advantages of the different methods used so far to study (part of) this problem (cf. [Chr79, CKMFR80, Sal86, Sal87, DL87, SW88, Har88, Har89, AB12, AB13, Bri17, AY19]). Indeed, our method is elementary, as general as possible in the sense that it applies to arbitrary multivariate algebraic power series over arbitrary fields of characteristic p, and it provides much sharper quantitative estimates. The methods used to date are briefly discussed in Section 1.3.

1.1. **Statement of our main result.** The "complexity" of an algebraic power series $f \in k[[\boldsymbol{t}]]$ is classically measured by its *degree* and its *height*. The degree of f is the minimal degree in y of a nonzero polynomial $A(\boldsymbol{t}, y) \in k[\boldsymbol{t}, y]$ such that $A(\boldsymbol{t}, f) = 0$. It is also equal to $[k(\boldsymbol{t})(f) : k(\boldsymbol{t})]$, the degree of the field extension $k(\boldsymbol{t})(f)$ of $k(\boldsymbol{t})$. For the height, we have two natural choices, since we can consider either the *partial height* or the *total height*. We say that f has partial height $\boldsymbol{h} = (h_1, \ldots, h_n)$ if, for all i, h_i is the minimal degree in t_i of a nonzero polynomial $A(\boldsymbol{t}, y) \in k[\boldsymbol{t}, y]$ such that $A(\boldsymbol{t}, f) = 0$, while the total height of f is the minimal total degree in $\boldsymbol{t}$ of such polynomials $A(\boldsymbol{t}, y)$. In fact, a finer way to measure the complexity of multivariate polynomials, and hence of algebraic power series, is to consider their Newton polytopes. We recall that the *Newton polytope* (or, *Newton polyhedron*) $\mathrm{NP}(A)$ of a multivariate polynomial

$$A \coloneqq \sum_{\substack{\boldsymbol{i} \in \mathbb{N}^n \\ j \in \mathbb{N}}} a_{\boldsymbol{i},j} \boldsymbol{t}^{\boldsymbol{i}} y^j \in k[\boldsymbol{t}, y]$$

is defined as the convex hull in $\mathbb{R}^{n+1}$ of the tuples $(\boldsymbol{i}, j)$ with $a_{\boldsymbol{i},j} \neq 0$. An important result is that, for a generic polynomial A, the number of integer points in the interior of $\mathrm{NP}(A)$ is equal to the (geometric) genus of the hypersurface associated with A. This has been proved by Baker for plane curves [Bak93], by Hodge for surfaces [Hod29] and by Khovanskii for arbitrary hypersurfaces [Hov78]. As a result, Theorem 1.2 has a geometric flavor, as does the result obtained by Bridy [Bri17] in the case where k is a finite field and $n = 1$ (cf. Section 4 for more details).

Keeping the previous notation, our main result reads as follows.

Theorem 1.2. *Let k be a perfect field of characteristic p. Let $A(\boldsymbol{t}, y)$ be a nonzero polynomial in $k[\boldsymbol{t}, y]$ and let $f \in k[[\boldsymbol{t}]]$ satisfy the algebraic relation $A(\boldsymbol{t}, f) = 0$. Set*

$$C \coloneqq \mathrm{NP}(A) + (-1, 0]^{n+1}\,.$$

Then there exists a k-vector space $W \subset K$ of dimension at most

$$\mathrm{Card}(C \cap \mathbb{N}^{n+1})$$

that contains f and that is closed under the action of Ω_n.

Remark 1.3. The plus sign in the definition of C refers to the Minkowski sum. In Theorems B and 1.2, the field k must be perfect for the section operators to be well-defined, but this is not a real limitation. Indeed, replacing an arbitrary field of characteristic p by its perfect closure does not affect our results (cf. Section 3).

When measuring complexity of algebraic power series in terms of degree and height, our main result can be translated as follows.

Corollary 1.4. *We keep the notation of Theorem 1.2. Let us further assume that* $\deg_y(A) \leq d$, $\deg_{\boldsymbol{t}}(A) \leq h$, *and* $\deg_{t_i}(A) \leq h_i$ *for all* $1 \leq i \leq n$. *Then, there exists a* k*-vector space* $W \subset K$ *of dimension at most*

$$N \coloneqq (d+1) \cdot \min\left\{ \prod_{i=1}^{n} (h_i + 1), \binom{n+h}{n} \right\}$$

that contains f *and that is closed under the action of* Ω_n.

Remark 1.5. In the rest of the paper, we express our results mostly in terms of degree and height rather than in terms of Newton polytopes, which leads to somewhat less precise bounds (compare, for instance, Theorem 1.2 and Corollary 1.4). This is the case for Theorems 4.1, 5.2, 6.1 and 6.3. The reason for this choice is that we think it could be more meaningful for some readers. However, there is no difficulty in deducing from our arguments and Theorem 1.2 more precise results involving Newton polytopes.

1.2. **Motivation.** Theorem 1.2 is motivated by various applications, in particular to the four following problems:

(i) Given an algebraic power series

$$f(\boldsymbol{t}) \coloneqq \sum_{\boldsymbol{i} \in \mathbb{N}^n} a(\boldsymbol{i}) \boldsymbol{t}^{\boldsymbol{i}} \in \mathbb{F}_q[[\boldsymbol{t}]]\,,$$

find upper bounds for the minimal number of states required for a q-automaton in order to generate the sequence $(a(\boldsymbol{i}))_{\boldsymbol{i} \in \mathbb{N}^n}$.

(ii) Given an algebraic power series

$$f(\boldsymbol{t}) \coloneqq \sum_{\boldsymbol{i} \in \mathbb{N}^n} a(\boldsymbol{i}) \boldsymbol{t}^{\boldsymbol{i}} \in \mathbb{Z}[[\boldsymbol{t}]]\,,$$

find upper bounds for the degree of algebraicity over $\mathbb{F}_p(t)$ of the reduction modulo p of the diagonal of f, that is

$$\Delta(f)_{|p} \coloneqq \sum_{i=0}^{\infty} (a(i, \ldots, i) \bmod p) t^i \in \mathbb{F}_p[[t]]\,.$$

(iii) Given two multivariate algebraic power series over an arbitrary field of characteristic p, find upper bounds for the degree of algebraicity of their Hadamard product.

(iv) Given an algebraic power series

$$f(\boldsymbol{t}) := \sum_{\boldsymbol{i}\in\mathbb{N}^n} a(\boldsymbol{i})\boldsymbol{t}^{\boldsymbol{i}} \in \mathbb{F}_q[[\boldsymbol{t}]]$$

(encoded by its minimal polynomial over $\mathbb{F}_q(\boldsymbol{t})$ and a large enough enclosure which guarantees uniqueness) and given a multi-index $\boldsymbol{i} \in \mathbb{N}^n$, find fast algorithms to compute the coefficient $a(\boldsymbol{i})$.

For each of them, our results strongly improve and/or generalize previously known results (cf. Sections 4–7). For example, in connection with Problem (ii), we significantly improve the main upper bound obtained by Adamczewski and Bell [AB13] for the algebraicity degree of reductions modulo p of diagonals of algebraic power series with integer coefficients, thus fully answering a question raised in 1984 by Deligne [Del84] (see Theorem 5.2).

1.3. **Comparison of previous methods.** There are essentially three different approaches to prove results in the vein of Theorems A and 1.2. We briefly recall them together with their main advantages and shortcomings.

(1) The most classical approach, initiated in [CKMFR80] and used in [Sal86, Sal87, DL87, SW88, Har88, Har89, AB12], is based on the fact that algebraic power series are roots of polynomials of a certain type called *Ore polynomials*, *i.e.* they satisfy algebraic equations of the form

$$a_0 f + a_1 f^p + \cdots + a_d f^{p^d} = 0\,,$$

where $a_0, \ldots, a_d \in k[\boldsymbol{t}]$, not all zero. The main advantage of this approach is that it is elementary and general in the sense that it applies to arbitrary multivariate algebraic power series over arbitrary fields of positive characteristic. Its main deficiency is that it provides poor bounds for the dimension of the k-vector space W, namely bounds of the form p^A, where A can be made explicit and depends polynomially on the parameters d and h (or d and $h_1, \ldots, h_n$), that is on the degree and the height of f.

(2) The second approach is based on the so-called *rationalization process*. This means that one expresses the algebraic power series f as the diagonal of a rational function with more variables. Its main advantage is that it provides bounds on the dimension of the k-vector space W that do not depend on p. It is based on Furstenberg's formula [Fur67, Proposition 2] which is elementary. The main drawback is that Furstenberg's formula only applies to algebraic power series satisfying some specific polynomial relations. For algebraic power series in one variable, one can overcome this difficulty by using resultant techniques (see, for example, [AY19]). For multivariate power series, one can use inductively these resultant methods as in [AB13], but the worst case scenario leads to really huge bounds. The same approach is also used in [DL87], where the rationalization process is ensured by a nonelementary and ineffective argument (cf. [AB13, Remark 3.1]).

(3) The last approach consists in using a geometric setting, considering the projective curve (or hypersurface) associated with the algebraic power series f. It was used by Deligne [Del84] in order to reprove Furstenberg's theorem on diagonals, and more recently by Bridy [Bri17] to prove a strong quantitative version of Christol's theorem in dimension one. The main advantage of the geometric approach is that it seems to provide tight bounds for the dimension of the k-vector space W, which is indeed the case in [Bri17]. The main shortcomings of this method are that it is not elementary, since it requires tools from algebraic geometry, and that it does not seem to work as well in the multivariate setting.

1.4. **Organization of the paper.** Section 2 is devoted to the proof of Theorem 1.2. In Section 3, we prove a result ensuring that one can consider, without any loss in our bounds, algebraic power series over arbitrary ground fields of positive characteristic (instead of perfect fields as assumed in Theorem 1.2). This result is used in Sections 5 and 6. In Section 4, we discuss Problem (i) and prove, in the multivariate setting, results similar to those obtained by Bridy [Bri17] for univariate algebraic power series. Section 5 is devoted to Problem (ii). We consider diagonals of algebraic power series in several variables over arbitrary fields of characteristic p, and obtain a general upper bound for their algebraicity degree, which significantly improves the main known result in this direction obtained by Adamczewski and Bell [AB13]. In Section 6, we discuss Problem (iii). We obtain the first simply exponential bound (with respect to the characteristic p of the ground field) for the degree of algebraicity of the Hadamard product of two multivariate algebraic power series. We also prove a similar result for the Hurwitz and the Lamperti products of two algebraic power series in one variable. This considerably improves the doubly exponential bounds which follow from [DL87, SW88, Har88] and that were made explicit by Harase [Har89]. Finally, in Section 7, we consider some algorithmic consequences of Theorem 1.2 to Problem (iv). In particular, we show that the M-th coefficient of the diagonal of an algebraic power series $f \in \mathbb{F}_p[[t_1, \ldots, t_n]]$ can be computed using a number of operations in $\mathbb{F}_p$ which is logarithmic in M and almost linear in p^{n+1}. Again, this improves significantly upon previously known results.

Throughout the paper, we let $\mathbb{N} \coloneqq \{0, 1, \ldots\}$ denote the set of nonnegative integers.

2. Proof of Theorem 1.2

This section is devoted to the proof of our main result.

2.1. **A variant of Furstenberg's formula.** Let K be a field and T be an indeterminate. The residue map res is defined from the field of Laurent series

$K((T))$ to K by setting

$$\mathsf{res}\left(\sum_{n\geq\nu} a_n T^n\right) \coloneqq a_{-1}\,.$$

Given a polynomial $A \in K[y]$, we let A_y denote its derivative with respect to y. The following key lemma is a slight reformulation of [BCCD19, Lemma 2.3], itself inspired by [Fur67, Proposition 2]. We provide a proof for the reader's convenience.

Lemma 2.1. *Let K be a field, $f \in K$ and $A(y) \in K[y]$. Assume that $A(f) = 0$ and $A_y(f) \neq 0$. Then*

$$\mathsf{res}\left(\frac{P(f+T)}{A(f+T)}\right) = \frac{P(f)}{A_y(f)}\,,$$

for all $P \in K[y]$.

Proof. By assumption, the polynomial $A(f+T) \in K[T]$ has a simple root at $T = 0$. There thus exists a polynomial $Q(T) \in K[T]$ such that

$$A(f+T) = T \cdot Q(T) \quad \text{and} \quad Q(0) \neq 0\,.$$

Taking the logarithmic derivative with respect to T yields the equality

$$\frac{A_y(f+T)}{A(f+T)} = \frac{1}{T} + \frac{Q'(T)}{Q(T)}\,.$$

Setting $g(T) \coloneqq P(f+T)/A_y(f+T)$, we find that g belongs to $K[[T]]$, as $A_y(f+T)$ does not vanish at $T = 0$. Furthermore, one has

$$\frac{P(f+T)}{A(f+T)} = \frac{g(T)}{T} + \frac{g(T)Q'(T)}{Q(T)}\,.$$

Similarly, $g(T)Q'(T)/Q(T)$ belongs to $K[[T]]$ since $Q(0) \neq 0$. It follows that

$$\mathsf{res}\left(\frac{P(f+T)}{A(f+T)}\right) = g(0) = \frac{P(f)}{A_y(f)}\,,$$

as claimed. □

2.2. **Frobenius and section operators.** Let k be a perfect field of characteristic p. We keep on with the notation introduced in Section 1. We let F be the Frobenius map. We consider indeterminates $t_1, \ldots, t_n$ and write $\boldsymbol{t} = (t_1, \ldots, t_n)$. We set $K_0 \coloneqq k(\boldsymbol{t})$, $R \coloneqq k[[\boldsymbol{t}]]$ and $K \coloneqq \mathrm{Frac}(R)$. For every $\boldsymbol{r} \in \{0, \ldots, p-1\}^n$, the section operator $S_{\boldsymbol{r}}$ is the semilinear operator from K into itself defined as in (1.2).

2.2.1. *Section operators on $K((T))$.* Let us consider a new indeterminate T. Then F extends to an injective homomorphism from $K((T))$ into itself. We let $K((T))^{\langle p\rangle}$ denote the image of $K((T))$ by F. As previously, $K((T))$ is a $K((T))^{\langle p\rangle}$-vector space of dimension p^{n+1}, a basis being given by all the products of the form $\boldsymbol{t}^{\boldsymbol{r}}T^s$ with $\boldsymbol{r} \in \{0,\dots,p-1\}^n$ and $0 \le s \le p-1$. However, it will be more convenient for our purpose to replace this standard basis by a more appropriate one (depending on a given $f \in R$). We proceed in the same way as in [BCCD19, Lemma 2.4].

Lemma 2.2. *For any $f \in R$, the family*

$$\mathcal{B}_f := \left\{\boldsymbol{t}^{\boldsymbol{r}}(f+T)^s : \boldsymbol{r}, s \in \{0,\dots,p-1\}^{n+1}\right\}$$

is a basis of $K((T))$ as a $K((T))^{\langle p\rangle}$-vector space.

Proof. First, we observe that $\mathcal{B}_f$ is a generating family. Indeed, we can obtain $\boldsymbol{t}^{\boldsymbol{r}}T^s$ as a linear combination of $\boldsymbol{t}^{\boldsymbol{r}}(f+T)^i$, $0 \le i \le s$. To see this, it is enough to invert the matrix

$$\begin{pmatrix} 1 & 0 & \cdots & \cdots & \cdots & 0 \\ f & 1 & 0 & \cdots & \cdots & 0 \\ f^2 & 2f & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ f^s & sf^{s-1} & \frac{s(s-1)}{2}f^{s-2} & \cdots & sf & 1 \end{pmatrix}.$$

Since $\mathcal{B}_f$ has the same cardinality as the basis $\{\boldsymbol{t}^{\boldsymbol{r}}T^s : \boldsymbol{r}, s \in \{0,\dots,p-1\}^{n+1}\}$, it is also a basis of $K((T))$. □

It follows that, given $f \in R$, every $x \in K((T))$ has a unique expansion of the form

$$x = \sum_{\boldsymbol{r}\in\{0,\dots,p-1\}^n} \boldsymbol{t}^{\boldsymbol{r}} \sum_{s=0}^{p-1} (f+T)^s x_{f,\boldsymbol{r},s}\,, \tag{2.1}$$

with $x_{f,\boldsymbol{r},s} \in K((T))^{\langle p\rangle}$. For every $\boldsymbol{r} \in \{0,\dots,p-1\}^n$ and $s \in \{0,\dots,p-1\}$, we define the *section operator* $S_{f,\boldsymbol{r},s}$, from $K((T))$ into itself, by

$$S_{f,\boldsymbol{r},s}(x) := \mathsf{F}^{-1}(x_{f,\boldsymbol{r},s})\,. \tag{2.2}$$

We observe that $S_{f,\boldsymbol{r},s}(xy^p) = S_{f,\boldsymbol{r},s}(x\mathsf{F}(y)) = S_{f,\boldsymbol{r},s}(x)y$, for all $x, y \in K((T))$, all $\boldsymbol{r} \in \{0,\dots,p-1\}^n$, and all $s \in \{0,\dots,p-1\}$.

2.2.2. *Section operators and residues.* The next result is the key observation of our proof. Roughly speaking, it shows some compatibility between taking residues at $f(t)$ and residues at 0. It corresponds to a multivariate extension of [BCCD19, Proposition 2.5].

Proposition 2.3. *For any $f \in R$ and $\boldsymbol{r} \in \{0,\dots,p-1\}^n$, the following commutation relation holds over $K((T))$:*

$$S_{\boldsymbol{r}} \circ \mathsf{res} = \mathsf{res} \circ S_{f,\boldsymbol{r},p-1}\,.$$

Proof. Let $x \in K((T))$. By (2.1), we have

$$x = \sum_{\boldsymbol{r}\in\{0,\dots,p-1\}^n} \boldsymbol{t}^{\boldsymbol{r}} \sum_{s=0}^{p-1} (f+T)^s\, \mathsf{F}(S_{f,\boldsymbol{r},s}(x))\,.$$

Hence

$$\begin{aligned}\mathsf{res}(x) &= \sum_{\boldsymbol{r}\in\{0,\dots,p-1\}^n} \boldsymbol{t}^{\boldsymbol{r}} \sum_{s=0}^{p-1} \mathsf{res}\Big((f+T)^s\, \mathsf{F}(S_{f,\boldsymbol{r},s}(x))\Big)\\ &= \sum_{\boldsymbol{r}\in\{0,\dots,p-1\}^n} \boldsymbol{t}^{\boldsymbol{r}}\, \mathsf{F}\big(\mathsf{res}\,\big(S_{f,\boldsymbol{r},p-1}(x)\big)\big)\ .\end{aligned}$$

By (1.1) and (1.2), we obtain

$$S_{\boldsymbol{r}} \circ \mathsf{res}(x) = \mathsf{res} \circ S_{f,\boldsymbol{r},p-1}(x)\,,$$

as wanted. □

2.3. **Proof of Theorem 1.2.** We keep on with the previous notation and the notation of Section 1. Let $E(\boldsymbol{t}, y) \in k[\boldsymbol{t}, y]$ denote the minimal polynomial of f over $k(t)$, normalized so that its coefficients are globally coprime.

Lemma 2.4. *The power series f is a simple root of $E(\boldsymbol{t}, y)$.*

Proof. It is enough to show that $E(\boldsymbol{t}, y)$ is separable with respect to the variable y. Since it is defined as a minimal polynomial, this further reduces to prove that $E(\boldsymbol{t}, y)$ is not of the form $F(\boldsymbol{t}, y^p)$ for some polynomial $F(\boldsymbol{t}, z) \in k[\boldsymbol{t}, z]$. We assume by contradiction that this occurs, and we write

$$F(\boldsymbol{t}, z) = a_0(\boldsymbol{t}) + a_1(\boldsymbol{t})z + \cdots + a_m(\boldsymbol{t})z^m$$

with $a_i(\boldsymbol{t}) \in k[\boldsymbol{t}]$ and $a_m(\boldsymbol{t}) \neq 0$. Let $\boldsymbol{r} \in \{0,\dots,p-1\}^n$. Applying the section operator $S_{\boldsymbol{r}}$ to the identity $F(\boldsymbol{t}, f^p) = 0$, we obtain

$$S_{\boldsymbol{r}}\big(a_0(\boldsymbol{t})\big) + S_{\boldsymbol{r}}\big(a_1(\boldsymbol{t})\big) f + \cdots + S_{\boldsymbol{r}}\big(a_m(\boldsymbol{t})\big) f^m = 0\,.$$

Moreover, since $a_m(\boldsymbol{t})$ is nonzero, there must exist $\boldsymbol{r}$ for which $S_{\boldsymbol{r}}(a_m(\boldsymbol{t}))$ does not vanish either. For this particular $\boldsymbol{r}$, we then get a polynomial annihilating f with y-degree less than the y-degree of E. This contradicts the minimality of E. □

Let E_y be the partial derivative of E with respect to y. Lemma 2.4 ensures that $E_y(\boldsymbol{t}, f) \neq 0$. Besides, given that A annihilates f, it must be a multiple of E, *i.e.* we can write $A = E \cdot F$ for some polynomial $F \in k[\boldsymbol{t}, y]$. Let J be the interval $(-1, 0]$ and set $C' := \mathrm{NP}(E) + J^{n+1}$.

We claim that the k-vector space

$$W \coloneqq \left\{ \frac{P(\boldsymbol{t}, f)}{E_y(\boldsymbol{t}, f)} : P \in k[\boldsymbol{t}, y],\ \mathrm{NP}(P) \subset C' \right\} \subset K$$

contains f and is invariant under the action of Ω_n. The fact that $f \in W$ follows from the observation that $\mathrm{NP}(yE_y) \subset \mathrm{NP}(E) \subset C'$. We now consider a tuple $\boldsymbol{r} \in \{0, 1, \ldots, p-1\}^n$ together with a polynomial $P \in k[\boldsymbol{t}, y]$ whose Newton polytope is a subset of C'. We set $R \coloneqq P \cdot E^{p-1}$ and let $Q \in k[\boldsymbol{t}, y]$ be defined by

$$Q(\boldsymbol{t}, f + T) \coloneqq S_{f,\boldsymbol{r},p-1}(R(\boldsymbol{t}, f + T)) \in K\,. \tag{2.3}$$

Combining Lemma 2.1 and Proposition 2.3, we obtain:

$$\begin{aligned} S_{\boldsymbol{r}} \left(\frac{P(\boldsymbol{t}, f)}{E_y(\boldsymbol{t}, f)} \right) &= S_{\boldsymbol{r}} \circ \mathsf{res} \left(\frac{P(\boldsymbol{t}, f + T)}{E(\boldsymbol{t}, f + T)} \right) \\ &= \mathsf{res} \circ S_{f,\boldsymbol{r},p-1} \left(\frac{P(\boldsymbol{t}, f + T)}{E(\boldsymbol{t}, f + T)} \right) \\ &= \mathsf{res} \left(\frac{Q(\boldsymbol{t}, f + T)}{E(\boldsymbol{t}, f + T)} \right) \\ &= \frac{Q(\boldsymbol{t}, f)}{E_y(\boldsymbol{t}, f)}\,. \end{aligned} \tag{2.4}$$

To establish our claim, it just remains to prove that $\mathrm{NP}(Q) \subset C'$. We recall the following standard fact about Newton polytopes. The formation of Newton polytopes is compatible with products: given $A, B \in k[\boldsymbol{t}, y]$, we have the relation

$$\mathrm{NP}(AB) = \mathrm{NP}(A) + \mathrm{NP}(B).$$

From this property, we derive that

$$\mathrm{NP}(R) \subset (p-1) \cdot \mathrm{NP}(E) + C' = p \cdot \mathrm{NP}(E) + J^{n+1}.$$

Let $(\boldsymbol{i}, j)$ be a tuple of exponents that belongs to the support of Q, *i.e.* for which the coefficient in Q in front of $\boldsymbol{t}^{\boldsymbol{i}} y^j$ is nonzero. It follows from the definition of $S_{f,\boldsymbol{r},p-1}$ that $(p\boldsymbol{i} + \boldsymbol{r}, pj + p - 1)$ must lie in $\mathrm{NP}(R)$. Dividing by p and writing $I \coloneqq (-\frac{1}{p}, 0]$, we obtain that

$$\left(\boldsymbol{i} + \tfrac{1}{p}\boldsymbol{r},\ j + \tfrac{p-1}{p} \right) \in \mathrm{NP}(E) + I^{n+1}\,,$$

so that

$$(\boldsymbol{i}, j) \in \mathrm{NP}(E) + I^{n+1} + \left\{ \left(-\tfrac{1}{p}\boldsymbol{r}, -\tfrac{p-1}{p} \right) \right\} \subset \mathrm{NP}(E) + J^{n+1} = C'\,.$$

Finally, we conclude that $\mathrm{NP}(Q) \subset C'$, as wanted.

Clearly W is spanned by the fractions of the form $\boldsymbol{t}^{\boldsymbol{i}} f^j / E_y(\boldsymbol{t}, f)$ with $(\boldsymbol{i}, j) \in C' \cap \mathbb{N}^{n+1}$. Hence its dimension is upper bounded by the cardinality of this set. We observe moreover that $C = \mathrm{NP}(F) + C'$. Since F is nonzero, its Newton polytope $\mathrm{NP}(F)$ meets $\mathbb{N}^{n+1}$. Hence C contains a translate of

C' by an element with nonnegative integral coefficients. Consequently the cardinality of $C \cap \mathbb{N}^{n+1}$ is at least that of $C' \cap \mathbb{N}^{n+1}$, and we conclude that

$$\dim_k W \leq \mathrm{Card}(C' \cap \mathbb{N}^{n+1}) \leq \mathrm{Card}(C \cap \mathbb{N}^{n+1}),$$

as wanted.

Remark 2.5. The proof above actually implies the following statement, which is a little more precise than Theorem 1.2 and can be useful is some cases. For a nonnegative integer m, let J_m be the interval $(-1,\, -1+p^{-m}]$ and define:

$$C'_m \coloneqq \mathrm{NP}(E) + (J_0^n \times J_m),$$
$$W_m \coloneqq \left\{ \frac{P(\boldsymbol{t}, f)}{E_y(\boldsymbol{t}, f)} : P \in k[\boldsymbol{t}, y],\ \mathrm{NP}(P) \subset C'_m \right\}.$$

The W_m's form a nonincreasing sequence of k-vector spaces and the action of Ω_n sends W_m to W_{m+1}. In particular, it stabilizes the intersection of the W_m's. However, it is not true that f belongs to W_m for all m: in full generality, it only lies in W_0.

If we set $\Omega_n^+ \cdot f \coloneqq \{S_{\boldsymbol{r}_1} \circ \cdots \circ S_{\boldsymbol{r}_t}(f) : t \geq 1\}$, we obtain that $\Omega_n \cdot f = \{f\} \cup \Omega_n^+ \cdot f$, while $\Omega_n^+ \cdot f$ is contained in W_1, which can be strictly smaller than W_0. For example, if we assume that $\deg_y(A) \leq d$, $\deg_{\boldsymbol{t}}(A) \leq h$, and $\deg_{t_i}(A) \leq h_i$ for all $1 \leq i \leq n$, then

$$\dim_k W_0 \leq (d+1) \cdot \min \left\{ \prod_{i=1}^{n} (h_i + 1), \binom{n+h}{n} \right\},$$

whereas

$$\dim_k W_1 \leq d \cdot \min \left\{ \prod_{i=1}^{n} (h_i + 1), \binom{n+h}{n} \right\}.$$

3. From perfect to arbitrary fields of positive characteristic

In Theorem 1.2, the ground field k must be perfect for the section operators to be well-defined. If k is not perfect, one can always replace k by its perfect closure and then apply Theorem 1.2. In this section, we prove a result which ensures that passing to the perfect closure does not affect the bounds we obtain in Sections 5 and 6.

Recall that if k is an arbitrary field of characteristic p, then adjoining to k all the p^r-th roots ($r \geq 1$) of all the elements of k yields a perfect field; it is called the perfect closure of k and we will denote it by k_p.

Proposition 3.1. *Let k be an arbitrary field of characteristic p and let k_p be its perfect closure. Let $f \in k[[\boldsymbol{t}]]$ be algebraic over $k(\boldsymbol{t})$. Then, $[k(\boldsymbol{t})(f) : k(\boldsymbol{t})] = [k_p(\boldsymbol{t})(f) : k_p(\boldsymbol{t})]$.*

Proposition 3.1 is a direct consequence of the following lemma.

Lemma 3.2. *Let k_0 be a field, k_1 be an extension of k_0, $\boldsymbol{t} = (t_1, \dots, t_n)$ be indeterminates, and $f_1(\boldsymbol{t}), \dots, f_r(\boldsymbol{t}) \in k_0[[\boldsymbol{t}]]$. If the power series $f_1, \dots, f_r$ are linearly dependent over the field $k_1(\boldsymbol{t})$, then they are linearly dependent over the field $k_0(\boldsymbol{t})$.*

Proof. By assumption, there exist polynomials $A_i(\boldsymbol{t}) \in k_1[\boldsymbol{t}]$, not all zero, such that

$$\sum_{i=1}^{r} A_i(\boldsymbol{t}) f_i(\boldsymbol{t}) = 0\,. \tag{3.1}$$

Set

$$A_i(\boldsymbol{t}) \coloneqq \sum_{\mathbf{j} \in \mathcal{S}_i} b_{i,\mathbf{j}} \mathbf{t}^{\mathbf{j}}$$

where we let $\mathcal{S}_i \subset \mathbb{N}^n$ denote the support of A_i, and

$$f_i(\boldsymbol{t}) \coloneqq \sum_{\boldsymbol{j} \in \mathbb{N}^n} a_{i,\mathbf{j}} \mathbf{t}^{\mathbf{j}} \in \mathbf{k}_0[[\boldsymbol{t}]]\,.$$

Let $(e_\ell)_{\ell \in L}$ be a basis of k_1, seen as a k_0-vector space. Thus, there exist some $c_{i,\mathbf{j},\ell} \in k_0$ such that

$$b_{i,\mathbf{j}} \coloneqq \sum_{\ell \in L} c_{i,\mathbf{j},\ell} e_\ell\,.$$

Then, Equality 3.1 implies that for all $\mathbf{k} \in \mathbb{N}^n$, one has

$$\sum_{i=1}^{r} \sum_{\mathbf{j} \in \mathcal{S}_i} b_{i,\mathbf{j}} a_{i,\mathbf{k}-\mathbf{j}} = 0\,,$$

and hence

$$\sum_{i=1}^{r} \sum_{\mathbf{j} \in \mathcal{S}_i} \sum_{\ell \in L} c_{i,\mathbf{j},\ell} e_\ell a_{i,\mathbf{k}-\mathbf{j}} = \sum_{\ell \in L} \left(\sum_{i=1}^{r} \sum_{\mathbf{j} \in \mathcal{S}_i} c_{i,\mathbf{j},\ell} a_{i,\mathbf{k}-\mathbf{j}} \right) e_\ell = 0\,.$$

Since the e_ℓ's are linearly independent over k_0, we obtain

$$\sum_{i=1}^{r} \sum_{\mathbf{j} \in \mathcal{S}_i} c_{i,\mathbf{j},\ell} a_{i,\mathbf{k}-\mathbf{j}} = 0 \tag{3.2}$$

for all $\ell \in L$ and all $\mathbf{k} \in \mathbb{N}^n$. Setting $A_{i,\ell}(\boldsymbol{t}) \coloneqq \sum_{\mathbf{j} \in \mathcal{S}_i} c_{i,\mathbf{j},\ell} \mathbf{t}^{\mathbf{j}} \in k_0[\boldsymbol{t}]$, Equality (3.2) implies that

$$\sum_{i=1}^{r} A_{i,\ell}(\boldsymbol{t}) f_i(\boldsymbol{t}) = 0, \quad \text{for all } \ell \in L\,. \tag{3.3}$$

Since the polynomials A_i are not all zero, the coefficients $b_{i,\mathbf{j}}$ are not all zero, and the same is also true for the coefficients $c_{i,\mathbf{j},\ell}$. Hence, there exists an index ℓ such that the polynomials $A_{i,\ell}$, $1 \le i \le r$, are not all zero. We thus deduce from (3.3) that $f_1, \dots, f_r$ are linearly dependent over $k_0(\boldsymbol{t})$, as wanted. □

4. State complexity in Christol's theorem

Given an integer $q \geq 2$, a multidimensional sequence $\mathbf{a} = (a(\boldsymbol{i}))_{\boldsymbol{i} \in \mathbb{N}^n}$ with values in a finite set is said to be *q-automatic* if $a(\boldsymbol{i})$ is a finite-state function of the base-q expansions of the entries of $\boldsymbol{i}$. This means that there exists a deterministic finite automaton taking the base-q expansion of each entry of $\boldsymbol{i}$ as input, and producing the symbol $a(\boldsymbol{i})$ as output. For a formal definition, we refer the reader to [AB21].

For the rest of this section, we let q denote a prime power. The multivariate extension of Christol's theorem can be stated as follows. It is usually proved by following the approach initiated in [CKMFR80] for the case $n = 1$ (cf. [Sal86, Sal87, DL87, SW88, Har88]).

Theorem C. Let $f(\boldsymbol{t}) \coloneqq \sum_{\boldsymbol{i} \in \mathbb{N}^n} a(\boldsymbol{i}) \boldsymbol{t}^{\boldsymbol{i}} \in \mathbb{F}_q[[\boldsymbol{t}]]$. Then f is algebraic over $\mathbb{F}_q(\boldsymbol{t})$ if and only if the sequence $\mathbf{a} \coloneqq (a(\boldsymbol{i}))_{\boldsymbol{i} \in \mathbb{N}^n}$ is q-automatic.

On each side, there is a natural way to measure the complexity of the corresponding objects, as described below. A natural problem is then to study the interplay between the complexity of the algebraic power series f and that of its sequence of coefficients $\mathbf{a}$.

4.1. Two notions of complexity.

As already mentioned in Section 1, the complexity of an algebraic power series $f \in \mathbb{F}_q[[\boldsymbol{t}]]$ can be measured by its degree d and either its partial height $\boldsymbol{h} \coloneqq (h_1, \ldots, h_n)$ or its total height h. We recall that $d \coloneqq [\mathbb{F}_q(\boldsymbol{t})(f) : \mathbb{F}_q(\boldsymbol{t})]$, and, for all i, $1 \leq i \leq n$, h_i (resp. h) is the minimal degree in the variable t_i (resp. the minimal total degree in $\boldsymbol{t}$) of a nonzero polynomial $A(\boldsymbol{t}, y)$ such that $A(\boldsymbol{t}, f) = 0$. These two notions of height are the same when $n = 1$.

The complexity of a q-automatic sequence $\mathbf{a}$ is measured by its *state complexity*. We let $\overleftarrow{\mathrm{comp}}_q(\mathbf{a})$ denote the number of states in a minimal finite automaton generating $\mathbf{a}$ in *reverse* reading, by which we mean that the input $\boldsymbol{i}$ is read starting from the least significant digits. In a similar way, we let $\overrightarrow{\mathrm{comp}}_q(\mathbf{a})$ denote the state complexity of $\mathbf{a}$ with respect to *direct* reading. In general, $\overleftarrow{\mathrm{comp}}_q(\mathbf{a})$ and $\overrightarrow{\mathrm{comp}}_q(\mathbf{a})$ behave quite differently and are only related by the inequalities $\overleftarrow{\mathrm{comp}}_q(\mathbf{a}) \leq q^{\overrightarrow{\mathrm{comp}}_q(\mathbf{a})}$ and $\overrightarrow{\mathrm{comp}}_q(\mathbf{a}) \leq q^{\overleftarrow{\mathrm{comp}}_q(\mathbf{a})}$. These estimates are derived from classical bounds for converting a nondeterministic finite automaton into a deterministic one (see, for example, [AS03, Chapter 4]).

4.2. Previous bounds on the state complexity.

Let us first recall that if $\mathbf{a}$ is generated by a q-automaton with at most m states in reverse reading, it is not difficult to show that the associated power series f has degree $d \leq q^m - 1$ and total height $h \leq mq^m$ (this follows, for instance, from the proofs of [AB13, Propositions 5.1 and 5.2]). Furthermore, it seems that these bounds cannot be significantly improved in general.

Bounds in the other direction are more challenging. The approach based on Ore's polynomials, initiated in [CKMFR80] and pursued in [Sal86, Sal87, DL87, SW88, Har88, Har89, AB12], leads to bounds of the form

$$\overleftarrow{\mathrm{comp}}_q\,(\mathbf{a}) \le q^{Aq^B}\,,$$

where A and B are polynomial functions of the parameters $d, h_1, \ldots, h_n$, that can be made explicit. The common feature of these bounds is that they have a doubly exponential nature (with respect to the size q of the ground field).

By contrast, when f is a rational function (*i.e.* $d = 1$), one can easily obtain the bound q^N, where $N \coloneqq \min\{(h_1+1)\cdots(h_n+1), \binom{n+h}{n}\}$, and thus get rid of the double exponential. This follows from Proposition 4.2 using the vector spaces W and W' introduced in Section 1, and suggests that the previous bounds are artificially large. In a more recent paper, Bridy [Bri17] drastically improved on these doubly exponential bounds in the case $n = 1$. More precisely, he proved that

$$\overleftarrow{\mathrm{comp}}_q\,(\mathbf{a}) \le (1+o(1))q^{h+d+g-1}\,, \tag{4.1}$$

where g is the genus of the projective curve associated with f, and where the $o(1)$ term tends to 0 for large values of any of q, h, d, or g. By Riemann's inequality, which gives $g \le (h-1)(d-1)$, he deduced that

$$\overleftarrow{\mathrm{comp}}_q\,(\mathbf{a}) \le (1+o(1))q^{hd}\,. \tag{4.2}$$

He also proved that

$$\overrightarrow{\mathrm{comp}}_q\,(\mathbf{a}) \le q^{(h+1)d}\,. \tag{4.3}$$

Bridy's approach is based on a new proof of Christol's theorem in the context of algebraic geometry, due to Speyer (see his blog post untitled *Christol's theorem and the Cartier operator*[1]). Speyer's argument is elegant, connecting finite automata with the geometry of curves. However, the price to pay to get (4.1) is that some classical but nonelementary background from algebraic geometry is needed: the Riemann-Roch theorem, the existence and the basic properties of the *Cartier* operator acting on the space of Kähler differentials of the function field associated with f, along with asymptotic bounds for the Landau function. Also, this geometric method does not seem to generalize easily to higher dimension. In an unpublished note, Adamczewski and Yassawi [AY19] showed how a slightly weaker bound can be obtained in an elementary way using diagonals, as in the original proof of Christol's theorem [Chr79], and resultant techniques. However, the use of resultants makes the proof somewhat tedious.

4.3. **A simply exponential bound in all dimensions.** As a consequence of Theorem 1.2, we obtain the following bound valid in any dimension.

[1]Available at https://sbseminar.wordpress.com/2010/02/11.

Theorem 4.1. *Let $f(\boldsymbol{t}) \coloneqq \sum_{\boldsymbol{i}\in\mathbb{N}^n} a(\boldsymbol{i})\boldsymbol{t}^{\boldsymbol{i}} \in \mathbb{F}_q[[\boldsymbol{t}]]$ be algebraic over $\mathbb{F}_q(\boldsymbol{t})$ with degree d, total height h, and partial height $\boldsymbol{h} \coloneqq (h_1, \ldots, h_n)$. Set*

$$N \coloneqq d \cdot \min\left\{\prod_{i=1}^{n}(h_i+1), \binom{n+h}{n}\right\}$$

and

$$N' \coloneqq (d+1) \cdot \min\left\{\prod_{i=1}^{n}(h_i+1), \binom{n+h}{n}\right\}.$$

Then

$$\overleftarrow{\mathrm{comp}}_q(\mathbf{a}) \le 1 + q^N \quad \text{and} \quad \overrightarrow{\mathrm{comp}}_q(\mathbf{a}) \le q^{N'}.$$

For $n = 1$ we obtain $\overleftarrow{\mathrm{comp}}_p(\mathbf{a}) \le 1 + p^{(h+1)d}$ and $\overrightarrow{\mathrm{comp}}_q(\mathbf{a}) \le q^{(h+1)(d+1)}$; these estimates are close to Bridy's bounds (4.2) and (4.3). Note that this could be pushed a little by considering separately the orbit of f under the section operator $S_{\mathbf{0}}$. In fact, this is precisely how Bridy proceeds to get (4.2). Let $C \coloneqq \mathrm{NP}(A) + (-1, 0]^2$ be defined as in Theorem 1.2 (in the case $n = 1$) and let g_A denote the number of integer points in the interior of $\mathrm{NP}(A)$. Generically, we have that $g = g_A$. To simplify the exposition, the bounds given in Theorem 4.1 are obtained by overapproximating $C \cap \mathbb{N}^2$ (for instance, by $(h_1 + 1)(d + 1)$ for the second one). Using g_A instead, we would obtain bounds with the same flavor as (4.1). Theorem 4.1 is new in dimension $n \ge 2$, where only doubly exponential bounds were available until now (cf. [Har89, FKdM00, AB12] and the discussion in [Bri17]).

The proof of Theorem 4.1 is derived from Theorem 1.2 and the following result.

Proposition 4.2. *Let $f(\boldsymbol{t}) \coloneqq \sum_{\boldsymbol{i}\in\mathbb{N}^n} a(\boldsymbol{i})\boldsymbol{t}^{\boldsymbol{i}} \in \mathbb{F}_q[[\boldsymbol{t}]]$. Assume that there exists a $\mathbb{F}_q$-vector space $W \subset \mathbb{F}_q((\boldsymbol{t}))$ of dimension m containing f and invariant under the action of Ω_n. Then*

$$\max\{\overrightarrow{\mathrm{comp}}_q(\mathbf{a}), \overleftarrow{\mathrm{comp}}_q(\mathbf{a})\} \le q^m. \tag{4.4}$$

Furthermore, we have

$$\overleftarrow{\mathrm{comp}}_q(\mathbf{a}) = |\Omega_n \cdot f|. \tag{4.5}$$

In the case $n = 1$, Inequality (4.4) is a rephrasing of [Bri17, Proposition 2.4], while Equality (4.5) is a rephrasing of a classical result of Eilenberg which asserts that $\overleftarrow{\mathrm{comp}}_q(\mathbf{a})$ is equal to the cardinality of the q-kernel of the sequence $\mathbf{a}$. Both results extend straightforwardly to arbitrary positive integers n.

Proof of Theorem 4.1. The upper bound for $\overleftarrow{\mathrm{comp}}_q(\mathbf{a})$ follows from Theorem 1.2 and Equation 4.4. The upper bound for $\overrightarrow{\mathrm{comp}}_q(\mathbf{a})$ is a direct consequence of Remark 2.5 and Equation (4.5). □

5. Diagonals

Given a field k and a multivariate power series

$$f(t_1,\dots,t_n) \coloneqq \sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} a(i_1,\dots,i_n)t_1^{i_1}\cdots t_n^{i_n} \in k[[t_1,\dots,t_n]]\,,$$

the *diagonal* of f is defined as the univariate power series

$$\Delta(f)(t) \coloneqq \sum_{i=0}^{+\infty} a(i,\dots,i)t^i \in k[[t]]\,.$$

When k is a number field, diagonals of algebraic functions form a remarkable class of power series: they satisfy linear differential equations of Picard-Fuchs type, they belong to the class of Siegel's G-functions, and they are constantly reoccurring in enumerative combinatorics. Furthermore, diagonalization is related to integration and, in general, the diagonal of an algebraic power series is transcendental over $k(t)$. For more details, we refer to the survey [Chr15].

By contrast, Furstenberg [Fur67] proved that if k has characteristic p and f is a rational power series, then $\Delta(f)$ is algebraic over $k(t)$. In [Del84], Deligne generalized this result to diagonals of algebraic power series. Then Harase [Har88], Sharif and Woodcock [SW88], Denef and Lipshitz [DL87], as well as Salon [Sal87, Sal86] (in some particular case) independently reproved Deligne's theorem.

Combining Theorem 1.2 with Propositions 5.1 and 5.2 of [AB13], we readily obtain an effective version of Deligne's theorem: given an algebraic power series $f \in k[[\boldsymbol{t}]]$ with degree d and total heights h, the diagonal $\Delta(f)$ has degree at most p^N and height at most Np^N, where N is explicitly given by

$$N \coloneqq (d+1)\cdot\binom{n+h}{n}\,.$$

In this section, we will prove a further refinement of this result, which can be formulated as follows.

Theorem 5.1. *Let k be an arbitrary field of characteristic p. Let $f \in k[[\boldsymbol{t}]]$ be an algebraic power series with degree d, total height h, and partial height $\boldsymbol{h} = (h_1,\dots,h_n)$. Set*

$$N \coloneqq (d+1)\cdot\min\left\{\prod_{i=1}^{n}(h_i+1) - \prod_{i=1}^{n} h_i, \binom{n+h}{n} - \binom{h}{n}\right\}\,.$$

Then, there exist $c_0, c_1, \dots, c_N \in k[t]$, not all zero, such that

$$c_0\cdot\Delta(f) + c_1\cdot\Delta(f)^p + \cdots + c_N\cdot\Delta(f)^{p^N} = 0\,.$$

In particular, $\Delta(f)$ has degree at most $p^N - 1$.

5.1. **Reduction of diagonals modulo primes.** Given a prime number p and a power series $f(\boldsymbol{t}) \coloneqq \sum_{\boldsymbol{i}\in\mathbb{N}^n} a(\boldsymbol{i})\boldsymbol{t}^{\boldsymbol{i}} \in \mathbb{Z}[[\boldsymbol{t}]]$, we let $f_{|p}$ denote the reduction of f modulo p, that is

$$f_{|p}(\boldsymbol{t}) \coloneqq \sum_{\boldsymbol{i}\in\mathbb{N}^n} (a(\boldsymbol{i}) \bmod p)\boldsymbol{t}^{\boldsymbol{i}} \in \mathbb{F}_p[[\boldsymbol{t}]]\,.$$

Deligne [Del84] made the following nice observation: since diagonalization and reduction modulo p commute, that is $\Delta(f)_{|p} = \Delta(f_{|p})$, if $f(\boldsymbol{t}) \in \mathbb{Z}[[\boldsymbol{t}]]$ is algebraic over $\mathbb{Q}(\boldsymbol{t})$, then $\Delta(f)_{|p}$ is algebraic over $\mathbb{F}_p(t)$ for almost all prime p. Hence, it is natural to ask how the "complexity" of the algebraic function $\Delta(f)_{|p}$ may increase when p runs along the primes. When $\Delta(f)$ is transcendental, van der Poorten [vdP93] conjectured that the degree of $\Delta(f)_{|p}$ cannot remain bounded independently of p. On the other hand, Deligne [Del84] suggested that the degree of $\Delta(f)_{|p}$ should grow at most polynomially in p.

Using the vector spaces W and W' introduced in Section 1, we can deduce the polynomial bound p^N, with $N \coloneqq \min\{(h_1+1)\cdots(h_n+1), \binom{n+h}{n}\}$, for f a multivariate rational power series with total height h and partial height $\boldsymbol{h} = (h_1, \ldots, h_n)$. The case where f is not rational is much more challenging. Deligne [Del84] obtained a first result in this direction by proving that if $f(t_1, t_2) \in \mathbb{Z}[[t_1, t_2]]$ is algebraic, then, for all but finitely many primes p, $\Delta(f)_{|p}$ is of degree at most Ap^B, where A and B do not depend on p but only on certain geometric quantities associated with f. On the other hand, the works of Harase [Har88, Har89], Sharif and Woodcock [SW88], and Adamczewski and Bell [AB12] lead to doubly exponential bounds (*i.e.* of the form p^{p^M}). The first general polynomial bound (*i.e.* of the form p^A) was obtained by Adamczewski and Bell in [AB13]. They provide an effective A that depends only on the degree and the total height of f. However, when f has degree $d > 1$, the value of A becomes huge due to a recursive procedure involving resultants. For instance, even for $n = 2$, the estimate for A is of the form

$$d^{4^{(h^2d^6)^{d^{4^{hd^2}}}}}$$

and the length of the exponential tower increases at least linearly with n. It is also possible to deduce from the work of Denef and Lipshitz [DL87] the existence of such a polynomial bound, but with an ineffective constant A.

Theorem 5.1 readily implies the following result, which quite significantly improves the previous known bounds.

Theorem 5.2. *Let $f \in \mathbb{Z}[[\boldsymbol{t}]]$ be an algebraic power series with degree d, total height h, and partial height $\boldsymbol{h} = (h_1, \ldots, h_n)$. Set*

$$N \coloneqq (d+1)\cdot \min\left\{\prod_{i=1}^{n}(h_i+1) - \prod_{i=1}^{n} h_i, \binom{n+h}{n} - \binom{h}{n}\right\}. \tag{5.1}$$

Then, for all prime numbers p, $\Delta(f)_{|p}$ has degree at most $p^N - 1$ over $\mathbb{F}_p(t)$.

Remark 5.3. Not only Theorem 5.1 gives a nice bound on the degree of $\Delta(f)_{|p}$, but it also shows that $\Delta(f)_{|p}$ is annihilated by an Ore polynomial of bounded p-degree. This additional feature implies that the Galois conjugates of $\Delta(f)_{|p}$ are all contained in an $\mathbb{F}_p$-vector space of dimension N and eventually that the Galois group of $\Delta(f)$ (*i.e.* the Galois group of the extension of $k(t)$ generated by $\Delta(f)$ and all its Galois conjugates) canonically embeds, up to conjugacy, into $\mathrm{GL}_N(\mathbb{F}_p)$. This observation allows for asking more precise questions about the uniformity with respect to p. For example, one may wonder if the Galois groups of $\Delta(f)_{|p}$ all come by reduction modulo p from a unique group (or maybe a finite number of groups) defined in characteristic zero.

Remark 5.4. Using the same arguments as in [AB13, p. 967], we could also prove a more general statement than Theorem 5.2 by replacing the ring $\mathbb{Z}$ with a number field and consider reductions modulo prime ideals. In fact, we could even consider the case where f has coefficients in an arbitrary field of characteristic zero (see [AB13, Theorem 1.4]). Note that, beyond diagonals of algebraic power series, there are other interesting families of G-functions in $\mathbb{Q}[[t]]$ whose reductions modulo p are algebraic (cf. [VM21]). Furthermore, algebraicity modulo p turns out to be useful to prove transcendence and algebraic independence results for power series in characteristic zero (cf. [WS89, AGBS98, AB13, ABD19, VM23]).

5.2. **Generalized diagonals.** In what follows, we consider a slight generalization of the diagonalization process. Let k be a perfect field of characteristic p and let $\boldsymbol{t} \coloneqq (t_1, \dots, t_n)$ be a tuple of indeterminates. We set $K_0 \coloneqq k(\boldsymbol{t})$, $R \coloneqq k[[\boldsymbol{t}]]$, and we let K denote the field of fractions of R. Let G be a subgroup of $\mathbb{Z}^n$ such that the quotient $\mathbb{Z}^n/G$ has no torsion. We let $K_{0,G}$ be the subfield of K_0 generated by k and by the monomials $\boldsymbol{t}^{\boldsymbol{i}}$ with $\boldsymbol{i} \in G$. Similarly, we define R_G as the k-subalgebra of R consisting of series of the form $\sum_{\boldsymbol{i}\in G} a(\boldsymbol{i})\boldsymbol{t}^{\boldsymbol{i}}$. Given that G is abstractly isomorphic to $\mathbb{Z}^m$ for some integer $m \leq n$, the rings K_G and R_G are respectively isomorphic to $k(x_1, \dots, x_m)$ and $k[[x_1, \dots, x_m]]$.

Definition 5.5. We keep the previous notation. The *G-diagonal* is the operator defined by

$$\begin{array}{rccc} \Delta_G : & R & \longrightarrow & R_G \\ & \displaystyle\sum_{\boldsymbol{i}\in\mathbb{N}^n} a(\boldsymbol{i})\boldsymbol{t}^{\boldsymbol{i}} & \mapsto & \displaystyle\sum_{\boldsymbol{i}\in G} a(\boldsymbol{i})\boldsymbol{t}^{\boldsymbol{i}} \end{array}$$

with the convention that $a(\boldsymbol{i}) = 0$ when $\boldsymbol{i} \notin \mathbb{N}^n$.

When G is the subgroup generated by $(1, \dots, 1)$, the ring R_G is isomorphic to $k[[t]]$ *via* the map $t_1 \cdots t_n \mapsto t$ and the diagonal operator Δ_G is the usual diagonal operator Δ. However the general construction Δ_G is more flexible and allows in particular for partial diagonals: letting G be the subgroup generated by $(1, \dots, 1)$ and by $e_i = (0, \dots, 0, 1, 0, \dots, 0)$ (with 1 in

i-th position) for $i \in \{1, \dots, m\}$, we obtain that $R_G \simeq k[[t_1, \dots, t_m, x]]$ and

$$\Delta_G\left(\sum_{i \in \mathbb{N}^n} a(\boldsymbol{i}) \boldsymbol{t}^{\boldsymbol{i}}\right) = \sum_{\substack{(i_1,\dots,i_m) \in \mathbb{N}^m \\ n \in \mathbb{N}}} a(i_1, \dots, i_m, n, \dots, n)\, t_1^{i_1} \cdots t_m^{i_m} x^n \,.$$

In general, one can check that Δ_G is $K_{0,G}$-linear.

Theorem 5.6. *Let k be an arbitrary field of characteristic p, G be a subgroup of $\mathbb{Z}^n$ such that $\mathbb{Z}^n/G$ has no torsion, let $G_{\mathbb{R}}$ be the subvector space of $\mathbb{R}^n$ generated by G, and let $\pi_G : \mathbb{R}^{n+1} \to (\mathbb{R}^n/G_{\mathbb{R}}) \times \mathbb{R}$ denote the canonical projection. Let $A(\boldsymbol{t}, y) \in k[\boldsymbol{t}, y]$ and let $f \in k[[\boldsymbol{t}]]$ satisfying the algebraic relation $A(\boldsymbol{t}, f) = 0$. Let C be the convex subset of $\mathbb{R}^{n+1}$ defined by*

$$C \coloneqq \mathrm{NP}(A) + \big(G_{\mathbb{R}} \times (-1, 0]\big) \,.$$

Then, there exist $c_0, c_1, \dots, c_N \in K_{0,G}$, not all zero, such that

$$c_0 \cdot \Delta_G(f) + c_1 \cdot \Delta_G(f)^p + \cdots + c_N \cdot \Delta_G(f)^{p^N} = 0 \,, \tag{5.2}$$

where $N \coloneqq \mathrm{Card}\big(\pi_G(C \cap \mathbb{N}^{n+1})\big)$.

Proof. We first observe that, by Proposition 3.1, we can replace without any loss of generality the field k by the perfect closure of the subfield of k generated over $\mathbb{F}_p$ by the coefficients of f. Hence, we can assume that k is perfect.

Let $E \in k(\boldsymbol{t}, y)$ be the minimal polynomial of f and E_y be the derivative of E with respect to y. Set $J \coloneqq (-1, 0]$ and

$$C' \coloneqq \mathrm{NP}(E) + \big(G_{\mathbb{R}} \times J\big) \,.$$

Repeating the proof of Theorem 1.2, we show that the k-vector space

$$W \coloneqq \left\{ \frac{P(\boldsymbol{t}, f)}{E_y(\boldsymbol{t}, f)} : P \in k[\boldsymbol{t}, y],\, \mathrm{NP}(P) \subset C' \right\}$$

contains f and is invariant under $S_{\boldsymbol{r}}$ for all $\boldsymbol{r} \in G$. Noticing that Δ_G commutes with $S_{\boldsymbol{r}}$ whenever $\boldsymbol{r} \in G$, we conclude that $\Delta_G(W)$ is invariant under $S_{\boldsymbol{r}}$ for all $\boldsymbol{r} \in G$ as well.

Let V be the $K_{0,G}$-span of $\Delta_G(W)$ in $K_G \coloneqq \mathrm{Frac}(R_G)$. By linearity, we find that V is spanned by the elements $\boldsymbol{t}^{\boldsymbol{i}} f^j / E_y(\boldsymbol{t}, f)$ for $(\boldsymbol{i}, j)$ running over $C' \cap \mathbb{N}^{n+1}$. Besides, two fractions $\boldsymbol{t}^{\boldsymbol{i}} f^j / E_y(\boldsymbol{t}, f)$ and $\boldsymbol{t}^{\boldsymbol{i}'} f^{j'} / E_y(\boldsymbol{t}, f)$ are $K_{0,G}$-collinear as soon as $\boldsymbol{i} \equiv \boldsymbol{i}' \bmod G$, which occurs if and only if $\pi_G(\boldsymbol{i}, j) = \pi_G(\boldsymbol{i}', j)$. The dimension of V over $K_{0,G}$ is then upper bounded by the cardinality of $\pi_G(C' \cap \mathbb{N}^{n+1})$, which is itself upper bounded by N (see the last paragraph of the proof of Theorem 1.2 for more details).

The Frobenius map F acts as an endomorphism of $K_{0,G}$. We consider the "relative" Frobenius map of K_G defined by

$$\begin{array}{rccc} \psi : & K_G \otimes_{K_{0,G},\mathsf{F}} K_{0,G} & \longrightarrow & K_G \\ & x \otimes y & \mapsto & x^p y \end{array}$$

where the notation $\otimes_{K_{0,G},\mathsf{F}}$ means that we view $K_{0,G}$ as an algebra over itself via F. Hence, in $K_G \otimes_{K_{0,G},\mathsf{F}} K_{0,G}$, we have $1 \otimes y = y^p \otimes 1$. This construction ensures that ψ is a $K_{0,G}$-linear isomorphism. Moreover, it is related to the section operators *via* the formula

$$\psi^{-1}(f) = \sum_{\boldsymbol{r} \in G_p} S_{\boldsymbol{r}}(f) \otimes \boldsymbol{t}^{\boldsymbol{r}}\,,$$

where we let $G_p \subset G$ denote a set of representatives of G/pG. Recall that we have proved earlier that V is closed under the action of $S_{\boldsymbol{r}}$ for all $\boldsymbol{r} \in G$. Therefore, we find that ψ^{-1} induces a $K_{0,G}$-linear morphism from V to $V \otimes_{K_{0,G},\mathsf{F}} K_{0,G}$. Being the restriction of an injective map, this morphism is clearly injective. Given that V is finite dimensional over $K_{0,G}$ and that $\dim_{K_{0,G}} V = \dim_{K_{0,G}}(V \otimes_{K_{0,G},\mathsf{F}} K_{0,G})$, we conclude that it is an isomorphism. Hence ψ takes $V \otimes_{K_{0,G},\mathsf{F}} K_{0,G}$ to V, which further implies that V is invariant under the Frobenius map.

In particular, $\Delta_G(f)^{p^s}$ lies in V for all nonnegative integers s. Since moreover $\dim_{K_{0,G}} V \leq N$, it follows that $\Delta_G(f), \Delta_G(f)^p, \ldots, \Delta_G(f)^{p^N}$ must be linearly dependent over $K_{0,G}$. Thus, there exist $c_0, c_1, \ldots, c_N \in K_{0,G}$, not all zero, such that

$$c_0 \cdot \Delta_G(f) + c_1 \cdot \Delta_G(f)^p + \cdots + c_N \cdot \Delta_G(f)^{p^N} = 0\,,$$

as desired. □

5.3. **Proof of Theorem 5.1.** We apply Theorem 5.6 with the group G generated by $(1, \ldots, 1)$. As already noticed, the diagonal Δ_G is then the usual diagonal Δ, up to the identification $t \coloneqq t_1 \cdots t_n$. Let $A(\boldsymbol{t}, y)$ be the minimal polynomial of f, so that A has degree d, total height h, and partial height $\boldsymbol{h} = (h_1, \ldots, h_n)$. Let π_G be the mapping and C be the convex set defined in the statement of Theorem 5.6. By Theorem 5.6, it remains to prove that $\mathrm{Card}\big(\pi_G(C \cap \mathbb{N}^{n+1})\big) \leq N$.

Let $c \coloneqq (a_1, \ldots, a_n, b) \in C \cap \mathbb{N}^{n+1}$. We have $-1 < b \leq d$ and, given that b is an integer, we conclude that $0 \leq b \leq d$. Moreover, up to translating c by an element of G, one may assume that $0 \leq a_i \leq h_i$ for all $i \in \{1, \ldots, n\}$ and that $\sum_{i=1}^n a_i \leq h$. Define $a \coloneqq \min\{a_1, \ldots, a_n\}$ and, for all i, set $\tilde{a}_i \coloneqq a_i - a$. Then one of the first n coordinates of $\tilde{c} \coloneqq (\tilde{a}_1, \ldots, \tilde{a}_n, b)$ vanishes. On the other hand, one has $0 \leq \tilde{a}_i \leq h_i$ and $\sum_{i=1}^n \tilde{a}_i \leq h$. Furthermore, $\pi_G(c) = \pi_G(\tilde{c})$. This ensures that any element of $\pi_G(C \cap \mathbb{N}^{n+1})$ has a preimage in each of the sets

$$\mathcal{E}_1 \coloneqq \big\{(a_1, \ldots, a_n, b) \in \mathbb{N}^{n+1} : b \leq d, \forall i, a_i \leq h_i, \exists i, a_i = 0\big\}$$

and

$$\mathcal{E}_2 \coloneqq \left\{(a_1, \ldots, a_n, b) \in \mathbb{N}^{n+1} : b \leq d, \sum_{i=1}^n a_i \leq h, \exists i, a_i = 0\right\}.$$

Since

$$\mathrm{Card}(\mathcal{E}_1) = (d+1)\cdot\left(\prod_{i=1}^{n}(h_i+1) - \prod_{i=1}^{n} h_i\right)$$

and

$$\mathrm{Card}(\mathcal{E}_2) = (d+1)\cdot\left(\binom{n+h}{n} - \binom{h}{n}\right),$$

we have that $\mathrm{Card}\big(\pi_G(C\cap\mathbb{N}^{n+1})\big) \le \min\{\mathrm{Card}(\mathcal{E}_1), \mathrm{Card}(\mathcal{E}_2)\} = N$, as wanted.

6. Hadamard product and other similar products

Let k be a field and $\boldsymbol{t} := (t_1,\dots,t_n)$ be a vector of indeterminates. Given two multivariate power series $f(\boldsymbol{t}) := \sum_{\boldsymbol{i}\in\mathbb{N}^n} a(\boldsymbol{i})\boldsymbol{t}^{\boldsymbol{i}}$ and $g(\boldsymbol{t}) := \sum_{\boldsymbol{i}\in\mathbb{N}^n} b(\boldsymbol{i})\boldsymbol{t}^{\boldsymbol{i}}$ in $k[[\boldsymbol{t}]]$, their Hadamard product is defined by

$$f\odot g := \sum_{\boldsymbol{i}\in\mathbb{N}^n} a(\boldsymbol{i})b(\boldsymbol{i})\boldsymbol{t}^{\boldsymbol{i}} \in k[[\boldsymbol{t}]]\,.$$

The Hadamard product is intimately connected to diagonalization. Indeed, we have

$$\Delta(f) = \varphi\left(f\odot\frac{1}{1-t_1\cdots t_n}\right),$$

where φ is the map defined by $t_1\cdots t_n \mapsto t$, while

$$f\odot g = \Delta_G(f(\boldsymbol{t})g(\boldsymbol{y}))\,,$$

where G is the subgroup of $\mathbb{Z}^{2n}$ generated by the vectors v_i, $1\le i\le n$, whose i-th and $(i+n)$-th entries are 1 and the other entries are 0.

As with diagonals, if k has characteristic zero, the Hadamard product of two algebraic power series in $k[[\boldsymbol{t}]]$ is in general transcendental. The situation is totally different if k has characteristic p. When k is a finite field and $n=1$, Furstenberg [Fur67] proved that the ring of algebraic power series is closed under Hadamard product. This was independently extended to arbitrary fields k of characteristic p and positive integers n, by Denef and Lipshitz [DL87], Sharif and Woodcock [SW88], and Harase [Har88]. Harase [Har89] also obtained a quantitative version of this result when k is a perfect field: the degree of algebraicity of $f\odot g$ over $k(\boldsymbol{t})$ is bounded by p^{Ap^B} for some A and B that are made explicit and depend polynomially on the degrees and the heights of f and g.

The following theorem improves considerably Harase's bound.

Theorem 6.1. *Let k be a field of characteristic p and let $f,g\in k[[\boldsymbol{t}]]$ be two algebraic power series of degree d and d', total height h and h', and partial height $\boldsymbol{h} := (h_1,\dots,h_n)$ and $\boldsymbol{h}' := (h'_1,\dots,h'_n)$, respectively. Set*

$$N_1 := (d+1)\cdot\min\left\{\prod_{i=1}^{n}(h_i+1), \binom{n+h}{n}\right\}$$

and

$$N_2 \coloneqq (d'+1)\cdot \min\left\{\prod_{i=1}^{n}(h_i'+1), \binom{n+h'}{n}\right\}.$$

Then $f \odot g$ is an algebraic power series of degree at most $p^{N_1 N_2}-1$ over $k(\boldsymbol{t})$.

We will prove this theorem in Section 6.2.

Remark 6.2. Again, we could also bound the total height h of $f \odot g$ following the argument in [AB13, Proposition 5.2].

6.1. **Hurwitz and Lamperti products.** All along this section, we only consider univariate power series, that is the case $n=1$. Given a field k and two power series $f(t) \coloneqq \sum_{i=0}^{\infty} a(i)t^i$ and $g(t) \coloneqq \sum_{i=0}^{\infty} b(i)t^i$ in $k[[t]]$, their Hurwitz product is defined by

$$f \circ_{\mathrm{H}} g \coloneqq \sum_{i=0}^{\infty}\left(\sum_{k=0}^{i}\binom{i}{k}a(k)b(i-k)\right)t^i \in k[[t]]\,,$$

and their Lamperti product by

$$f \circ_{\mathrm{L}} g \coloneqq \sum_{i=0}^{\infty}\left(\sum_{j+k+\ell=i}\frac{i!}{j!k!\ell!}\alpha^j\beta^k\gamma^\ell a(j+k)b(\ell+k)\right)t^i \in k[[t]]\,,$$

where the parameters α, β, and γ belong to k. The Lamperti product generalizes both the Hadamard product (taking $\alpha=\beta=0$ and $\gamma=1$) and the Hurwitz product (taking $\alpha=\beta=1$ and $\gamma=0$). When k has positive characteristic, Harase [Har88, Har89] proved that the Lamperti product of two algebraic power series f and g remains algebraic and he provided a doubly exponential bound (*i.e.* of the form p^{Ap^B}) for the degree of $f \circ_{\mathrm{L}} g$ (and thus for $f \circ_{\mathrm{H}} g$). Again, our approach leads to a simply exponential bound.

Theorem 6.3. *Let k be a field of characteristic p and let $f, g \in k[[t]]$ be two algebraic power series of degree d and d' and height h and h', respectively. Set*

$$N \coloneqq (d+1)(d'+1)(h+1)(h'+1)\,.$$

Then $f \circ_{\mathrm{L}} g$ is an algebraic power series of degree at most p^N-1 over $k(t)$. In particular, the same result holds for $f \odot g$ and $f \circ_H g$.

6.2. **Proof of Theorems 6.1 and 6.3.** As previously, we let K denote the field of fractions of $k[[\boldsymbol{t}]]$ and $S_{\boldsymbol{r}}$, $\boldsymbol{r} \in \{0,\dots,p-1\}^n$ be the section operators. We first deduce from Theorem 1.2 and Proposition 3.1 the following general result.

Proposition 6.4. *Let k be a field of characteristic p and let $\star$ be a bilinear product defined over $k[[\boldsymbol{t}]]$ such that for all $f, g \in k[[\boldsymbol{t}]]$ one has*

$$S_{\boldsymbol{r}}(f \star g) \in \operatorname{span}_k\left\{S_{\boldsymbol{i}}f \star S_{\boldsymbol{j}}g : \boldsymbol{i},\boldsymbol{j} \in \{0,\dots,p-1\}^n\right\}. \tag{6.1}$$

Let $f_1, f_2 \in k[[\boldsymbol{t}]]$ and let us assume that for all $i \in \{1,2\}$ there exists a k-vector space $W_i \subset K$ of dimension at most d_i containing f_i and invariant by Ω_n. Then $f_1 \star f_2$ is an algebraic power series of degree at most $p^{d_1 d_2} - 1$ over $k(\boldsymbol{t})$.

Proof. Let us first assume that k is a perfect field. Let $h_1, \dots, h_r$ be a basis of W_1 and $h'_1, \dots, h'_s$ be a basis of W_2. Set

$$W \coloneqq \operatorname{span}_k\{h_i \star h'_j : 1 \le i \le r,\ 1 \le j \le s\}\,.$$

Then W has dimension at most $d_1 d_2$ and the bilinearity of $\star$ implies that W contains $f_1 \star f_2$. On the other hand, since W_1 and W_2 are invariant under Ω_n, we infer from the bilinearity of $\star$, the semilinearity of the section operators, and (6.1) that W is also invariant under Ω_n. Then it follows classically that $f_1 \star f_2$ is algebraic over $k(\boldsymbol{t})$ with degree at most $p^{d_1 d_2} - 1$ (cf., for instance, [Har89] and [AB13, Proposition 5.1]).

Now, if k is an arbitrary field of characteristic p, one can pass to its perfect closure k_p and then apply the previous argument to obtain that $f_1 \star f_2$ as degree at most $p^{d_1 d_2} - 1$ over $k_p(\boldsymbol{t})$. By Proposition 3.1, we deduce that the degree of $f_1 \star f_2$ over $k(\boldsymbol{t})$ is also at most $p^{d_1 d_2} - 1$, as wanted. □

Proof of Theorem 6.1. After noticing that

$$S_{\boldsymbol{r}}(f \odot g) = S_{\boldsymbol{r}}(f) \odot S_{\boldsymbol{r}}(g)\,,$$

the proof follows directly from Proposition 6.4 and Corollary 1.4. □

Proof of Theorem 6.3. After noticing, as in [Har89], that

$$S_r(f \circ_{\mathrm{L}} g) = \sum_{\substack{0 \le s,r \\ s+t \le r}} \frac{r!}{s!t!(r-s-t)!} \alpha^{s/p} \beta^{t/p} \gamma^{(r-s-t)/p} S_{r-t}(f) \circ_{\mathrm{L}} S_{r-s}(g)\,,$$

the proof follows directly from Proposition 6.4 and Corollary 1.4 (with $n = 1$). □

7. Algorithmic consequences of Theorem 1.2

Throughout this section, we assume for simplicity that k is a finite field $\mathbb{F}_q$. We address the question of the efficient computation of *one* "faraway" coefficient of a power series $f(\boldsymbol{t}) \in k[[\boldsymbol{t}]]$ assumed to be algebraic over $k(\boldsymbol{t})$.

It was pointed out in [AS92, Corollary 4.5] that the M-th term of an automatic sequence (and more generally of a k-regular sequence) can be computed using $O(\log M)$ operations in k. By Christol's theorem (and its multivariate version) it follows that, given $\boldsymbol{i} \coloneqq (i_1, \dots, i_n)$, the coefficient of $\boldsymbol{t}^{\boldsymbol{i}} \coloneqq t_1^{i_1} \cdots t_n^{i_n}$ in the expansion of f can be computed in $O(\log M)$ operations in k, where $M \coloneqq \max(i_1, \dots, i_n)$. (For fields of characteristic zero, there is no algorithm achieving polynomial time in $\log M$ for the same task, even if $n = 1$.) However, this estimate is oversimplified in the sense that the $O(\cdot)$ hides dependencies in the other parameters, namely the characteristic p of the ground field k, the number of variables n and the various algebraicity degree and heights of f. The actual efficiency of any algorithm that computes

the coefficient of $\boldsymbol{t}^{\boldsymbol{i}}$ of f heavily depends on these parameters, especially given that before entering the $O(\log M)$-part, some of these algorithms may need to perform precomputations whose cost is so large with respect to the other parameters, that the algorithms are highly inefficient in practice. This is particularly true for the class of algorithms that start with building a q-automaton: the running time of this precomputation depends on number of states of the automaton, which can be huge. For these reasons, in the algorithmic design, it is important to care about the dependencies with respect to all the other parameters. This is the object of this section.

7.1. **The algorithm.** For algorithmic purposes, the starting point is always to find a suitable finite representation of the objects we want to compute with. In our setting, it is of course not possible to represent a power series $f(\boldsymbol{t})$ by its full sequence of coefficients in k, because this sequence is an infinite object. However, when $f(\boldsymbol{t})$ is algebraic, we can hope to come back to a finite representation by working with an annihilating polynomial of $f(\boldsymbol{t})$, together with sufficiently many initial coefficients in the expansion of $f(\boldsymbol{t})$. This indeed works but requires some caution, given that the aforementioned polynomial may in general have several roots. In what follows, we shall encode an algebraic power series $f(\boldsymbol{t}) \coloneqq \sum_{\boldsymbol{i}\in\mathbb{N}^n} a(\boldsymbol{i})\boldsymbol{t}^{\boldsymbol{i}}$ by the following data:

(a) its minimal polynomial $E(\boldsymbol{t}, y) \in k[\boldsymbol{t}, y]$ over $k(\boldsymbol{t})$, which we normalize (up to a unit in k) by requiring it to have polynomial coefficients in $k[t]$ that are globally coprime,
(b) a minimal element (for the product order on $\mathbb{N}^n$), denoted by $\boldsymbol{\rho} \coloneqq (\rho_1, \dots, \rho_n)$, of $\mathrm{NP}\big(E_y(\boldsymbol{t}, y)\big) \cap \mathbb{N}^n$ (which is nonempty thanks to Lemma 2.4),
(c) the coefficients $a(\boldsymbol{i})$ for all tuples $\boldsymbol{i} \coloneqq (i_1, \dots, i_n)$ with $0 \le i_j \le \rho_j$ for all $1 \le j \le n$.

Lemma 7.1. *The previous data uniquely determines the algebraic power series f.*

Proof. Let $\boldsymbol{i} \coloneqq (i_1, \dots, i_n) \in \mathbb{N}^n$ be a multiindex. For each $j \in \{1, \dots, n\}$, we write the decomposition in base p of i_j

$$i_j = \sum_{m=0}^{\ell-1} r_{j,m}\, p^m\,,$$

where ℓ is a positive integer and all the $r_{j,m}$'s are integers between 0 and $p-1$. For each m, we form the tuple $\boldsymbol{r}_m \coloneqq (r_{1,m}, \dots, r_{n,m})$ and consider the corresponding section operator $S_{\boldsymbol{r}_m}$. It follows from the definitions that the coefficient $a(\boldsymbol{i})$ is equal to the p^ℓ-th power of the constant coefficient of the power series

$$g(\boldsymbol{t}) \coloneqq S_{\boldsymbol{r}_{\ell-1}} \circ \cdots \circ S_{\boldsymbol{r}_1} \circ S_{\boldsymbol{r}_0}\big(f(\boldsymbol{t})\big)\,.$$

Input: A multiindex $\boldsymbol{i} = (i_1, \ldots, i_n)$ and an algebraic power series $f(\boldsymbol{t}) \in k[[\boldsymbol{t}]]$ encoded by $(E(\boldsymbol{t}, y), \boldsymbol{\rho}, f(\boldsymbol{t}) \bmod \boldsymbol{t}^{\boldsymbol{\rho}+1})$
Output: The $\boldsymbol{i}$-th coefficient of $f(\boldsymbol{t})$

1. For $j = 1, \ldots, n$,
   write the decomposition of i_j in base p: $i_j = \sum_{m=0}^{\ell-1} r_{j,m}\, p^m$
2. Set $Q_0(\boldsymbol{t}, y) \coloneqq y \cdot E_y(\boldsymbol{t}, y)$
3. For $i = 0, 1, \ldots, \ell - 1$,
   set $Q_{i+1}(\boldsymbol{t}, y) \coloneqq S_{f, r_{1,m}, \ldots, r_{n,m}, p-1}\big(Q_i(\boldsymbol{t}, y) \cdot E(\boldsymbol{t}, y)^{p-1}\big)$
4. Compute $Q_\ell(\boldsymbol{t}, f(\boldsymbol{t})) \bmod \boldsymbol{t}^{\boldsymbol{\rho}+1}$ and set $\alpha \coloneqq [\boldsymbol{t}^{\boldsymbol{\rho}}] Q_\ell(\boldsymbol{t}, f(\boldsymbol{t}))$
5. Compute $E_y(\boldsymbol{t}, f(\boldsymbol{t})) \bmod \boldsymbol{t}^{\boldsymbol{\rho}+1}$ and set $\beta \coloneqq [\boldsymbol{t}^{\boldsymbol{\rho}}] E_y(\boldsymbol{t}, f(\boldsymbol{t}))$
6. Return $(\alpha/\beta)^{p^\ell}$

Algorithm 1: $\boldsymbol{i}$-th coefficient of an algebraic power series.

Moreover, by Eq. (2.4), there exists a polynomial $Q \in k[\boldsymbol{t}, y]$ such that

$$g(\boldsymbol{t}) = \frac{Q(\boldsymbol{t}, f(\boldsymbol{t}))}{E_y(\boldsymbol{t}, f(\boldsymbol{t}))}\,, \quad \textit{i.e.} \quad Q(\boldsymbol{t}, f(\boldsymbol{t})) = g(\boldsymbol{t}) \cdot E_y(\boldsymbol{t}, f(\boldsymbol{t}))\,.$$

Identifying the coefficients in $\boldsymbol{t}^{\boldsymbol{\rho}}$ in the latter equality, we find

$$[\boldsymbol{t}^{\boldsymbol{\rho}}] Q(\boldsymbol{t}, f(\boldsymbol{t})) = \sum_{\boldsymbol{u}+\boldsymbol{v}=\boldsymbol{\rho}} [\boldsymbol{t}^{\boldsymbol{u}}] g(\boldsymbol{t}) \cdot [\boldsymbol{t}^{\boldsymbol{v}}] E_y(\boldsymbol{t}, f(\boldsymbol{t}))\,,$$

where the notation $[\boldsymbol{t}^{\boldsymbol{j}}]\varphi(\boldsymbol{t})$ refers to the coefficients in front of $\boldsymbol{t}^{\boldsymbol{j}}$ in the power series $\varphi(\boldsymbol{t})$. On the other hand, we derive from the definition of $\boldsymbol{\rho}$ (and especially from the minimality condition (b)) that the unique $\boldsymbol{v} \le \boldsymbol{\rho}$ for which the coefficient $[\boldsymbol{t}^{\boldsymbol{v}}] E_y(\boldsymbol{t}, f(\boldsymbol{t}))$ does not vanish is $\boldsymbol{\rho}$ itself. Therefore, we conclude that

$$[\boldsymbol{t}^{\boldsymbol{\rho}}] Q(\boldsymbol{t}, f(\boldsymbol{t})) = [\boldsymbol{t}^0] g(\boldsymbol{t}) \cdot [\boldsymbol{t}^{\boldsymbol{\rho}}] E_y(\boldsymbol{t}, f(\boldsymbol{t}))$$

which gives

$$a(\boldsymbol{i}) = \big([\boldsymbol{t}^0] g(\boldsymbol{t})\big)^{p^\ell} = \left(\frac{[\boldsymbol{t}^{\boldsymbol{\rho}}] Q(\boldsymbol{t}, f(\boldsymbol{t}))}{[\boldsymbol{t}^{\boldsymbol{\rho}}] E_y(\boldsymbol{t}, f(\boldsymbol{t}))}\right)^{p^\ell}\,.$$

Since $f(\boldsymbol{t})$ is given at precision $O(t_1^{\rho_1+1} \cdots t_n^{\rho_n+1})$, we can compute $Q(\boldsymbol{t}, f(\boldsymbol{t}))$ at the same precision; this ensures that the coefficient $[\boldsymbol{t}^{\boldsymbol{\rho}}] Q(\boldsymbol{t}, f(\boldsymbol{t}))$ can be recovered from the set of data that we have at our disposal. Hence the same holds for $a(\boldsymbol{i})$. Since $\boldsymbol{i}$ was chosen arbitrarily at the beginning of the proof, the lemma is proved. □

Importantly, we notice that the proof of Lemma 7.1 together with the explicit formula (2.3) translate immediately to Algorithm 1 which computes the coefficient $a(\boldsymbol{i})$ of the power series $f(\boldsymbol{t})$. Note that Algorithm 1 can be seen as a multivariate version of the algorithms in [BCCD19, Section 3].

We now study the (arithmetic) complexity of Algorithm 1. In what follows, we will express complexity of algorithms in terms of the number of operations

they perform in the ground field k. By "operation", we mean either a classical arithmetical (field) operation (addition, subtraction, multiplication, division) or an application of the Frobenius map F, or its inverse. We recall the soft-O notation $\tilde{O}$: by definition, $\tilde{O}(c)$ is the union of the $O(c\log^k(c))$ for k varying in $\mathbb{N}$. Using $\tilde{O}$ instead of the more customary O-notation makes it possible to "hide" logarithmic factors.

Theorem 7.2. *Let $f(\boldsymbol{t}) \in k[[\boldsymbol{t}]]$ be an algebraic power series encoded by the data*

$$(E(\boldsymbol{t}, y), \boldsymbol{\rho}, f(\boldsymbol{t}) \bmod \boldsymbol{t}^{\boldsymbol{\rho}+1}).$$

Let $\boldsymbol{h} := (h_1, \dots, h_n)$ be the vector of partial heights of $E(\boldsymbol{t}, y)$ and d be its degree. On input $f(\boldsymbol{t})$ and $\boldsymbol{i} := (i_1, \dots, i_n)$, Algorithm 1 performs at most

$$\tilde{O}\big(2^n dp^{n+1}(h_1+1)\cdots(h_n+1)\log M + 2^n(\rho_1+1)\cdots(\rho_n+1)\big)$$

operations in k, where $M := \max(i_1, \dots, i_n)$.

Proof. By construction, all intermediate polynomials $Q_i(\boldsymbol{t}, y)$ have partial heights at most $\boldsymbol{h}$ and degree at most d. Recall that polynomials in $k[\boldsymbol{t}, y]$ of degree at most d and partial heights at most $\boldsymbol{h} = (h_1, \dots, h_n)$ can be multiplied in $\tilde{O}\left(2^n d(h_1+1)\cdots(h_n+1)\right)$ operations in k, using Fast Fourier Transform (FFT) multiplication of univariate polynomials [CK91] and Kronecker's substitution [Pan94]. Therefore, each iteration of the loop in line 3 requires at most $\tilde{O}\big(2^n dp^{n+1}(h_1+1)\cdots(h_n+1)\big)$ operations in k. Besides, the number of times this loop is executed, namely ℓ, grows at most logarithmically with respect to M. The total cost of line 3 then stays within

$$\tilde{O}\big(2^n dp^{n+1}(h_1+1)\cdots(h_n+1)\log M\big)$$

operations in k. Similarly, the computations in lines 4 and 5 require at most $\tilde{O}\big(2^n(\rho_1+1)\cdots(\rho_n+1)\big)$ operations in k. Adding both contributions, we find the announced complexity. □

Remark 7.3. A small optimization can be applied to Algorithm 1. It consists in computing $Q_i^{\mathsf{F}^i}$ (that is the polynomial obtained from Q_i by applying F^i to each of its coefficients) instead of Q_i on line 3, thanks to the recurrence relation:

$$Q_{i+1}^{F^{i+1}}(\boldsymbol{t}, y) = S^{\mathsf{F}}_{f, r_{1,m}, \dots, r_{n,m}, p-1}\big(Q_i^{F^i}(\boldsymbol{t}, y) \cdot E^{\mathsf{F}^i}(\boldsymbol{t}, y)^{p-1}\big),$$

where $S^{\mathsf{F}}_{f,\boldsymbol{r},s}$ is the same operator as $S_{f,\boldsymbol{r},s}$ except that we do not take preimages of the coefficients by the Frobenius map F. Proceeding this way, we retrieve $\mathsf{F}^\ell(\alpha) = \alpha^{p^\ell}$ by selecting the coefficient of $\boldsymbol{t}^{\boldsymbol{\rho}}$ in $Q_\ell^{\mathsf{F}^\ell}(\boldsymbol{t}, f(\boldsymbol{t}))$ and can return $\mathsf{F}^\ell(\alpha)/\beta^{p^\ell}$ on line 6. With this optimization, it becomes unnecessary to apply inverses of F in Algorithm 1. This may be beneficial since, in practice, applying F^{-1} may be a more expensive operation than applying F.

Remark 7.4. It is possible to give *a priori* bounds on $\boldsymbol{\rho}$ in terms of $\boldsymbol{h}$ and d. Indeed, let $r(\boldsymbol{t})$ be the resultant in y of the polynomials $E(\boldsymbol{t}, y)$ and $E_y(\boldsymbol{t}, y)$. A calculation shows that the t_i-degree of $r(\boldsymbol{t})$ is upper bounded by $2dh_i$.

Besides, it follows from the standard properties of resultants that $E_y(\boldsymbol{t}, f(\boldsymbol{t}))$ divides $r(\boldsymbol{t})$ in the ring $k[[\boldsymbol{t}]]$. Hence the Newton polytope of $E_y(\boldsymbol{t}, f(\boldsymbol{t}))$ necessarily has one point in the box $[0, 2dh_1] \times \cdots \times [0, 2dh_n]$, from which we derive that one can always choose $\boldsymbol{\rho} \leq 2d \cdot \boldsymbol{h}$. The above discussion shows that the complexity of Algorithm 1 can be controlled in terms of $\boldsymbol{h}$, d and $\log M$ only: to simplify notation, setting

$$H := (h_1+1) \cdots (h_n+1)\,,$$

the number of operations used by Algorithm 1 is at most

$$\tilde{O}\big(2^n d p^{n+1} H \log M + 4^n d^n H\big)\,. \tag{7.1}$$

For $n = 1$ and $h_1 = h > 0$, the cost (7.1) reads $\tilde{O}\big(dhp^2 \log M\big)$. This is similar to the complexity estimate $\tilde{O}\big(h(d+h)p^2 + h^2(d+h)^2 \log M\big)$ of [BCD16, Algorithm 3]. Faster algorithms are available when $n = 1$, with quasi-linear complexity in p: $\tilde{O}\big(h^2(h+d)^2 \log M + h(h+d)^5 p\big)$ ([BCD16, Theorem 11]) and even $\tilde{O}\big(d^2h^2 \log M + d^2hp + d^3h\big)$ ([BCCD19, Theorem 3.4]).

For a general n, the complexity estimate (7.1) is exponentially better (with respect to p) than all estimates that could be deduced from known approaches. This important improvement is of course ultimately inherited from Theorem 1.2. It would be interesting to design faster variants of Algorithm 1, whose complexities improve the estimate (7.1), e.g. replacing the term p^{n+1} by p^n.

7.2. **Applications to diagonals.** Assume that $f(\boldsymbol{t}) \in \mathbb{F}_p[[\boldsymbol{t}]]$ is an algebraic power series in n variables of degree d and partial height $\boldsymbol{h} := (h_1, \ldots, h_n)$. We consider here the following algorithmic problem: given $M \in \mathbb{N}$, how fast can one compute the M-th coefficient in the expansion of the diagonal $\Delta(f)$?

When f is rational, Rowland and Yassawi proposed in [RY15, Section 2] two algorithms to compute finite automata that could be used to compute terms of the coefficient sequence of $\Delta(f)$. However, the number of states of the produced automata is prohibitively large: Remark 2.2 in [RY15] provides an upper bound of the form $p^{(h+1)^n}$, where h is the total height of f.

By Theorem 5.2 and the discussion above, $\Delta(f)$ is an algebraic power series in $\mathbb{F}_p[[t]]$ of degree $D_\Delta \leq p^N - 1$ and height $H_\Delta \leq N p^N$ where N is at most $(d+1)H$ and, as before, $H = (h_1+1) \cdots (h_n+1)$. Hence, a "naive" way of computing the coefficient $[t^M]\Delta(f)$ would be to first determine an annihilating polynomial $E \in \mathbb{F}_p[t, y]$ for $\Delta(f)$, and then to apply the algorithms of [BCD16] or [BCCD19] to this E. Starting from the first $2(D_\Delta+1)(H_\Delta+1)$ terms in the expansion of $\Delta(f)$, one can compute such an E, by (structured) linear algebra, using $\tilde{O}(D_\Delta^\omega H_\Delta) \subseteq \tilde{O}(N p^{(\omega+1)N})$ operations in $\mathbb{F}_p$, as explained in [BCCD19, p. 128]. Here $\omega \in [2, 3]$ is a feasible exponent for the matrix multiplication. Hence, using [BCCD19, Theorem 3.4], we conclude

that, for $M \gg 0$, the coefficient $[t^M]\Delta(f)$ can be computed in

$$\tilde{O}\big(H_\Delta^2(H_\Delta + D_\Delta)^2 \log M + D_\Delta^2 H_\Delta p + D_\Delta^3 H_\Delta\big) \subseteq \tilde{O}\big(d^4 H^4 p^{4(d+1)H} \log M\big)$$

operations in $\mathbb{F}_p$. This complexity estimate is quasi-optimal with respect to M, but its dependence in p is far from optimal.

A much better method is to apply Algorithm 1 with $\boldsymbol{i} = (M, \ldots, M)$ directly, without first precomputing an annihilating polynomial for $\Delta(f)$. The resulting complexity is then provided by Theorem 7.2, and is bounded in terms of $n, p, d, h_1, \ldots, h_n$ by the estimate in (7.1), namely

$$\tilde{O}\big(2^n d p^{n+1} H \log M + 4^n d^n H\big)\,.$$

This method then allows to compute the M-th coefficient of the diagonal of $f(t_1, \ldots, t_n)$ in arithmetic complexity linear in $\log M$ and quasi-linear in p^{n+1}. This result was previously known only in the bivariate case. For more than two variables, previous algorithms with complexity linear in $\log M$ required (at least) doubly exponential time in the arithmetic size of f.

Note finally that the truth of Christol's conjecture [Chr90, Conjecture 4] would imply that $\log(M)$-time algorithms for computing the M-th term modulo p might well exist for the whole class of integer sequences with geometric growth which are P-finite (i.e., which satisfy linear recurrence relations with polynomial coefficients in the index n).

7.3. **Examples.** We consider the Apéry numbers $A(n) := \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2$. Their generating function $\sum_{n=0}^{\infty} A(n) t^n$ is the diagonal of the rational function in $n = 4$ variables [Str14]

$$f(t_1, t_2, t_3, t_4) := \frac{1}{(1 - t_1 - t_2)(1 - t_3 - t_4) - t_1 t_2 t_3 t_4}\,.$$

Hence, by (7.1), $A(M) \bmod p$ can be computed in $O(p^5 \log M)$ operations in $\mathbb{F}_p$. This estimate can be lowered to $\tilde{O}(p^4 \log M)$ by using that $\sum_{n \geq 0} A(n) t^n$ is also the diagonal of the following algebraic function in $n = 3$ variables:

$$1/\sqrt{(t_1 t_2 t_3 + t_1 + t_2 - 1)^2 - 4(t_1 + t_2 - 1)^2 t_3}.$$

In this particular case, a better complexity bound can be obtained by exploiting nontrivial arithmetic properties of the Apéry numbers. Indeed, it turns out that the sequence $(A(n))_{n \geq 0}$ is p-Lucas [Ges82]: if $M = (i_{\ell-1} \ldots i_1 i_0)_p$ is the base-p expansion of M, then $A(M) = A(i_{\ell-1}) \cdots A(i_1) A(i_0) \bmod p$, hence it is sufficient to precompute $A(0) \bmod p, \ldots, A(p-1) \bmod p$. This can be done for a cost of $O(p)$ operations in $\mathbb{F}_p$ by unrolling the recurrence $(n+1)^3 A(n+1) = (2n+1)\big(17n^2 + 17n + 5\big) A(n) - n^3 A(n-1)$ satisfied by $(A(n))_{n \geq 0}$. After this, computing $A(M) \bmod p$ only requires $O(\log M)$ extra operations in $\mathbb{F}_p$.

However, beyond this example, many other interesting integer sequences are not p-Lucas, but are known to admit diagonals of algebraic functions as

generating functions. Most of the integer sequences from the combinatorial literature, which are P-finite and have a geometric growth, are known to fall into this class. For instance, the sequence $1, 6, 222, 9918, \ldots$ (A144045) counting diagonal rook paths on a 3D chessboard was proved in [BCvHP12] to satisfy the recurrence

$$\begin{aligned} &2n^2(n-1)a(n) - (n-1)(121n^2 - 91n - 6)a(n-1) \\ &-(n-2)(475n^2-2512n+2829)a(n-2)+18(n-3)(97n^2-519n+702)a(n-3) \\ &\qquad - 1152(n-3)(n-4)^2a(n-4) = 0\,, \qquad \text{for } n \geq 4\,, \end{aligned}$$

and to admit a generating function $F(t) := \sum_{n\geq 0} a(n)t^n$ equal to

$$F(t) = 1 + 6 \cdot \int_0^t \frac{{}_2F_1\left(\begin{matrix}1/3 & 2/3 \\ & 2\end{matrix}\middle|\, \frac{27w(2-3w)}{(1-4w)^3}\right)}{(1-4w)(1-64w)}\, dw\,.$$

Given a prime p, neither the recurrence, nor the closed form of $F(t)$ are well-suited to compute rapidly the value $a(M) \bmod p$ for high values of M. In exchange, $a(M)$ is the M-th coefficient of the diagonal of the rational function in 3 variables

$$f(t_1, t_2, t_3) := \frac{(1-t_1)(1-t_2)(1-t_3)}{1 - 2(t_1+t_2+t_3) + 3(t_1t_2 + t_2t_3 + t_1t_3) - 4t_1t_2t_3}\,.$$

Hence, by (7.1), $a(M) \bmod p$ can be computed using $\tilde{O}(p^4 \log M)$ operations in $\mathbb{F}_p$. This can be lowered to $\tilde{O}(p^3 \log M)$ by using a diagonal expression for $F(t)$ as the diagonal of an algebraic function in $n = 2$ variables, e.g. of

$$\frac{1}{2} + \frac{(1-t_1)^2}{2-3t_1} \cdot \sqrt{\frac{(1-t_2)}{(1-2t_1)^2 - (3-4t_1)^2\, t_2}}.$$

A similar example is given by the sequence $1, 2, 18, 255, 4522, \ldots$ (A151362) whose n-th term $q(n)$ counts walks in the quarter plane $\mathbb{N}^2$ of length $2n$ starting at the origin and using steps in the set {N, S, NE, SE, NW, SW}. The generating function $Q(t) := \sum_{n\geq 0} q(n)t^{2n}$ of this sequence is known to be transcendental over $\mathbb{Q}(t)$ and to admit the ${}_2F_1$ expression [BCvH+17]

$$Q(t) = \frac{2}{t^2} \int_0^t \int_0^y \frac{1}{(12\,z^2+1)^{3/2}} \cdot {}_2F_1\left(\begin{matrix}3/4 & 5/4 \\ & 2\end{matrix}\middle|\, \frac{64\,z^2}{(12\,z^2+1)^2}\right) \mathrm{d}z\, \mathrm{d}y$$

and also the diagonal expression [MM16]

$$Q(t) = \Delta\left(\frac{\left(t_2^2-1\right)\left(t_3^2-1\right)}{1 - t_1\left(t_2^2t_3^2 + t_2t_3^2 + t_2^2 + t_3^2 + t_2 + 1\right)}\right),$$

with $n = 3$ and $(h_1, h_2, h_3) = (1, 2, 2)$. Using the last expression, $q(M) \bmod p$ can be computed in $\tilde{O}(p^4 \log M)$ operations in $\mathbb{F}_p$. The same remark actually applies to all $19 \times 4 - 3$ transcendental generating functions of the form $Q(0,0), Q(1,0), Q(0,1)$ and $Q(1,1)$ from [BCvH+17, Theorem 2].

REFERENCES

[AB12] B. Adamczewski and J. Bell. On vanishing coefficients of algebraic power series over fields of positive characteristic. *Invent. Math.*, 187:343–393, 2012.

[AB13] B. Adamczewski and J. Bell. Diagonalization and rationalization of algebraic Laurent series. *Ann. Sci. Éc. Norm. Supér.*, 46:963–1004, 2013.

[AB21] B. Adamczewski and J. Bell. Automata in number theory. In *Handbook of automata theory. Vol. II. Automata in mathematics and selected applications*, pages 913–945. EMS Press, Berlin, 2021.

[ABD19] B. Adamczewski, J.. Bell, and E. Delaygue. Algebraic independence of G-functions and congruences "à la Lucas". *Ann. Sci. Éc. Norm. Supér.*, 52:515–559, 2019.

[AGBS98] J.-P. Allouche, D. Gouyou-Beauchamps, and G. Skordev. Transcendence of binomial and Lucas' formal power series. *J. Algebra*, 210:577–592, 1998.

[AS92] Jean-Paul Allouche and Jeffrey Shallit. The ring of k-regular sequences. *Theoret. Comput. Sci.*, 98(2):163–197, 1992.

[AS03] J.-P. Allouche and J. Shallit. *Automatic sequences*. Cambridge University Press, Cambridge, 2003.

[AY19] B. Adamczewski and R. Yassawi. A note on Christol's theorem. arXiv:1906.08703 [math.NT], https://arxiv.org/abs/1906.08703, 2019.

[Bak93] H. F. Baker. Examples of the application of Newton's polygon to the theory of singular points of algebraic functions. *Trans. Camb. Phil. Soc.*, XV(IV):403–450, 1893.

[BCCD19] A. Bostan, X. Caruso, G. Christol, and P. Dumas. Fast coefficient computation for algebraic power series in positive characteristic. In *Proceedings of the Thirteenth Algorithmic Number Theory Symposium*, volume 2 of *Open Book Ser.*, pages 119–135. Math. Sci. Publ., Berkeley, CA, 2019.

[BCD16] Alin Bostan, Gilles Christol, and Philippe Dumas. Fast computation of the Nth term of an algebraic series over a finite prime field. In *Proceedings of the 2016 ACM International Symposium on Symbolic and Algebraic Computation*, pages 119–126. ACM, New York, 2016.

[BCvH+17] A. Bostan, F. Chyzak, M. van Hoeij, M. Kauers, and L. Pech. Hypergeometric expressions for generating functions of walks with small steps in the quarter plane. *European J. Combin.*, 61:242–275, 2017.

[BCvHP12] A. Bostan, F. Chyzak, M. van Hoeij, and L. Pech. Explicit formula for the generating series of diagonal 3D rook paths. *Sém. Lothar. Combin.*, 66:Art. B66a, 27, 2011/12.

[Bri17] A. Bridy. Automatic sequences and curves over finite fields. *Algebra Number Theory*, 11:685–712, 2017.

[Chr79] G. Christol. Ensembles presque periodiques k-reconnaissables. *Theoret. Comput. Sci.*, 9:141–145, 1979.

[Chr90] G. Christol. Globally bounded solutions of differential equations. In *Analytic number theory (Tokyo, 1988)*, volume 1434 of *Lecture Notes in Math.*, pages 45–64. Springer, Berlin, 1990.

[Chr15] G. Christol. Diagonals of rational fractions. *Eur. Math. Soc. Newsl.*, 97:37–43, 2015.

[CK91] David G. Cantor and Erich Kaltofen. On fast multiplication of polynomials over arbitrary algebras. *Acta Inform.*, 28(7):693–701, 1991.

[CKMFR80] G. Christol, T. Kamae, M. Mendès France, and G. Rauzy. Suites algébriques, automates et substitutions. *Bull. Soc. Math. France*, 108:401–419, 1980.

[Del84] P. Deligne. Intégration sur un cycle évanescent. *Invent. Math.*, 76:129–143, 1984.

[Der07] H. Derksen. A Skolem-Mahler-Lech theorem in positive characteristic and finite automata. *Invent. Math.*, 168:175–224, 2007.

[DL87] J. Denef and L. Lipshitz. Algebraic power series and diagonals. *J. Number Theory*, 26:46–67, 1987.

[FKdM00] J. Fresnel, M. Koskas, and B. de Mathan. Automata and transcendence in positive characteristic. *J. Number Theory*, 80:1–24, 2000.

[Fur67] H. Furstenberg. Algebraic functions over finite fields. *J. Algebra*, 7:271–277, 1967.

[Ges82] I. Gessel. Some congruences for Apéry numbers. *J. Number Theory*, 14:362–368, 1982.

[Har88] T. Harase. Algebraic elements in formal power series rings. *Israel J. Math.*, 63:281–288, 1988.

[Har89] T. Harase. Algebraic elements in formal power series rings. II. *Israel J. Math.*, 67:62–66, 1989.

[Hod29] W. V. D. Hodge. The Isolated Singularities of an Algebraic Surface. *Proc. London Math. Soc. (2)*, 30(2):133–143, 1929.

[Hov78] A. G. Hovanskiĭ. Newton polyhedra, and the genus of complete intersections. *Funktsional. Anal. i Prilozhen.*, 12(1):51–61, 1978.

[MM16] S. Melczer and M. Mishna. Asymptotic lattice path enumeration using diagonals. *Algorithmica*, 75:782–811, 2016.

[Pan94] Victor Y. Pan. Simple multivariate polynomial multiplication. *J. Symbolic Comput.*, 18(3):183–186, 1994.

[RY15] E. Rowland and R. Yassawi. Automatic congruences for diagonals of rational functions. *J. Théor. Nombres Bordeaux*, 27:245–288, 2015.

[Sal86] O. Salon. Suites automatiques à multi-indices. *Sém. Théorie Nombres Bordeaux (1986-1987),*, Exposé 4:1–27, 1986.

[Sal87] O. Salon. Suites automatiques à multi-indices et algébricité. *C. R. Acad. Sci. Paris Sér. I Math.*, 305:501–504, 1987.

[Str14] A. Straub. Multivariate Apéry numbers and supercongruences of rational functions. *Algebra Number Theory*, 8:1985–2007, 2014.

[SW88] H. Sharif and C. F. Woodcock. Algebraic functions over a field of positive characteristic and Hadamard products. *J. London Math. Soc. (2)*, 37:395–403, 1988.

[vdP93] A. J. van der Poorten. Power series representing algebraic functions. In *Séminaire de Théorie des Nombres, Paris, 1990–91*, volume 108 of *Progr. Math.*, pages 241–262. Birkhäuser Boston, Boston, MA, 1993.

[VM21] D. Vargas-Montoya. Algébricité modulo p, séries hypergéométriques et structures de Frobenius fortes. *Bull. Soc. Math. France*, 149:439–477, 2021.

[VM23] D. Vargas-Montoya. Monodromie unipotente maximale, congruences “à la Lucas” et indépendance algébrique. arXiv:2103.15192 [math.NT], to appear in *Trans. Amer. Math. Soc.*, DOI: https://doi.org/10.1090/tran/8913, 2023.

[WS89] C. F. Woodcock and H. Sharif. On the transcendence of certain series. *J. Algebra*, 121:364–369, 1989.

[Zan09] U. Zannier. *Lecture notes on Diophantine analysis*, volume 8 of *Appunti. Scuola Normale Superiore di Pisa (Nuova Serie) [Lecture Notes. Scuola Normale Superiore di Pisa (New Series)]*. Edizioni della Normale, Pisa, 2009.

B. Adamczewski: Univ. Claude Bernard Lyon 1, CNRS UMR 5208, Institut Camille Jordan, 43 blvd. du 11 novembre 1918, F-69622 Villeurbanne cedex, France
Email address: boris.adamczewski@math.cnrs.fr

A. Bostan: Inria, Université Paris-Saclay, 1 rue Honoré d'Estienne d'Orves, 91120 Palaiseau, France
Email address: alin.bostan@inria.fr

X. Caruso: CNRS, IMB, Université de Bordeaux, 351 cours de la Libération, 33405 Talence, France
Email address: xavier@caruso.ovh