DIAGONALS AND ALGEBRAICITY MODULO p: A SHARPER DEGREE BOUND

by

Boris Adamczewski, Alin Bostan & Xavier Caruso

Résumé. — En 1984, Deligne a montré que pour tout nombre premier p, la réduction modulo p de la diagonale d'une série formelle algébrique de plusieurs variables à coefficients entiers est algébrique sur le corps des fonctions rationnelles à coefficients dans $\mathbb{F}_p$. De plus, il a suggéré que les degrés d'algébricité d_p de ces fonctions devaient croître au plus polynomialement en fonction de p. Dans cet article, nous présentons une nouvelle preuve du théorème de Deligne qui est élémentaire et permet d'établir la première borne générale polynomiale avec un degré raisonnable.

Abstract. — In 1984, Deligne proved that for any prime number p, the reduction modulo p of the diagonal of a multivariate algebraic power series with integer coefficients is algebraic over the field of rational functions with coefficients in $\mathbb{F}_p$. Moreover, he conjectured that the algebraic degrees d_p of these functions should grow at most polynomially in p. In this article, we provide a new and elementary proof of Deligne's theorem, which yields the first general polynomial bound on d_p with an explicit and reasonable degree.

1. Introduction

Given a ring R and a multivariate power series

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

Key words and phrases. — Diagonals of algebraic power series, algebraicity modulo p, Christol's theorem.

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).

where we write $\boldsymbol{i} = (i_1, \ldots, i_n)$, $a(\boldsymbol{i}) = a(i_1, \ldots, i_n)$, $\boldsymbol{t} = (t_1, \ldots, t_n)$, and $\boldsymbol{t}^{\boldsymbol{i}} = t_1^{i_1} \cdots t_n^{i_n}$, the *diagonal* of f is the univariate power series

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

When $\mathfrak{p}$ is an ideal of R, the *reduction modulo* $\mathfrak{p}$ of f is given by

$$f_{|\mathfrak{p}}(\boldsymbol{t}) \coloneqq \sum_{\boldsymbol{i} \in \mathbb{N}^n} (a(\boldsymbol{i}) \bmod \mathfrak{p}) \boldsymbol{t}^{\boldsymbol{i}} \in (R/\mathfrak{p})[\![\boldsymbol{t}]\!] .$$

A particularly interesting case arises when $R = \overline{\mathbb{Q}}$, the field of algebraic numbers, and the power series f is algebraic over $\overline{\mathbb{Q}}(\boldsymbol{t})$. In this setting, $\Delta(f)$ satisfies a linear differential equation of Picard-Fuchs type and belongs to the class of Siegel's G-functions. We refer the reader to [**AB13**, **Chr15**] and the references therein for further discussion of these connections. Moreover, such power series frequently appear in enumerative combinatorics (see [**Sta99**, Chap. 6], [**BMM10**] and [**Mel21**, Chap. 4]). Additionally, diagonalization is closely related to integration (see [**Del84**] and [**Chr15**, Sec. 3]), and in general, $\Delta(f)$ is transcendental over $\overline{\mathbb{Q}}(t)$ (see, for instance, [**AB13**]).

By contrast, when $R = k$ is a field of characteristic $p > 0$, and f is a multivariate rational power series, Furstenberg [**Fur67**] proved the following remarkable result: the diagonal $\Delta(f)$ is always algebraic over $k(t)$. Later, Deligne [**Del84**] provided a geometric proof of Furstenberg's theorem and extended it to the case where f is algebraic. He also noted an intriguing connection between these two seemingly opposite situations through reductions modulo p. Indeed, the relation $\Delta(f)_{|\mathfrak{p}} = \Delta(f_{|\mathfrak{p}})$ holds in general. It follows from Deligne's theorem that if $f \in \mathbb{Z}[\![\boldsymbol{t}]\!]$ is algebraic, then $\Delta(f)_{|p}$ remains algebraic over $\mathbb{F}_p(t)$ for all primes p. This naturally raises the question of how the algebraic degree d_p of $\Delta(f)_{|p}$ evolves as p varies. Deligne's proof relies on heavy arithmetic geometry machinery and proceeds inductively on the number n of variables. In [**Del84**], he suggested that a direct proof would be more satisfactory and could yield a polynomial bound of the form $d_p = O(p^N)$.

Deligne's work has been highly influential, inspiring several authors [**DL87**, **SW88**, **Har88**, **Sal87**, **Sal86**], who independently provided a direct and elementary proof of his theorem. However, this proof resulted in a very weak nonpolynomial bound on d_p. More recently, Bell and the first author [**AB13**] established the first general polynomial bound, but their proof relies on an inductive argument, leading to an excessively large value of N in the worst case. A brief discussion of these results is provided in Section 1.1.

Our main contribution is a new, direct, and elementary proof of Deligne's theorem, which yields the first polynomial bound $d_p < p^N$ with a reasonable

value for N, expressed in terms of the complexity of the underlying algebraic function.

The complexity of an algebraic power series $f \in k[\![\boldsymbol{t}]\!]$ is traditionally measured in terms of its *degree* and *height*. Since the ring $k[\boldsymbol{t}, y]$ is a unique factorization domain, there exists a polynomial $E(\boldsymbol{t}, y) \in k[\boldsymbol{t}, y]$ satisfying $E(\boldsymbol{t}, f) = 0$, which is minimal for divisibility. Moreover such a polynomial is unique up to multiplication by a nonzero constant in k. The *degree* of f is defined as the degree in y of $E(\boldsymbol{t}, y)$; equivalently, it is the degree of the field extension $k(\boldsymbol{t})(f)$ of $k(\boldsymbol{t})$. For the height, we consider two natural definitions: the *total height* of f is the total degree in $\boldsymbol{t}$ of $E(\boldsymbol{t}, y)$ (where the total degree of the monomial $\boldsymbol{t}^{\boldsymbol{i}}$ is $i_1 + \cdots + i_n$), while its *partial height* is the tuple $\boldsymbol{h} = (h_1, \dots, h_n)$ where, for each i, h_i is the degree in t_i of $E(\boldsymbol{t}, y)$.

We recall that any element f in the algebraic closure of $\mathbb{F}_p(t)$ is annihilated by a *linearized polynomial*, *i.e.*, a polynomial $P(X) \in \mathbb{F}_p(t)[X]$ of the form

$$c_0 X + c_1 X^p + \cdots + c_N X^{p^N}, \qquad c_N \neq 0.$$

The integer N is called the *p-degree* of P. It easily follows that the Galois conjugates of f are all contained in an $\mathbb{F}_p$-vector space of dimension N. Consequently, the Galois group of f (*i.e.*, the Galois group of the extension of $\mathbb{F}_p(t)$ generated by f and all its Galois conjugates) canonically embeds, up to conjugacy, into $\mathrm{GL}_N(\mathbb{F}_p)$.

Our main result is stated as follows.

Theorem 1.1. — *Let $f \in \mathbb{Z}[\![\boldsymbol{t}]\!]$ be an algebraic power series with degree d, total height h, and partial height $(h_1, \dots, h_n)$. Set*

$$N \coloneqq (d+1) \cdot \min\left\{ \prod_{i=1}^{n} (h_i + 1) - \prod_{i=1}^{n} h_i, \binom{n+h}{n} - \binom{h}{n} \right\}. \tag{1.1}$$

Then, for every prime number p, $\Delta(f)_{|p}$ is annihilated by a linearized polynomial of p-degree at most N. In particular, $\Delta(f)_{|p}$ has degree at most $p^N - 1$ over $\mathbb{F}_p(t)$.

Let us make a few comments about this result.

Remark 1.2. — It follows from Theorem 1.1 and the preceding remark, that, for every prime p, the Galois group of $\Delta(f)_{|p}$ embeds, up to conjugacy, into $\mathrm{GL}_N(\mathbb{F}_p)$. The key point here is that N does not depend on p. This observation naturally leads to more refined questions concerning uniformity with respect to p. In particular, one may ask whether the Galois groups of $\Delta(f)_{|p}$ arise by reduction modulo p from a unique group, or a finite number of groups, defined in characteristic zero. In a recent preprint [**CFVM25**], Caruso, Fürnsinn, and Vargas-Montoya investigate this problem.

Remark 1.3. — We will deduce Theorem 1.1 from a slightly more precise statement (see Theorem 3.3) in which the bound N is expressed in terms of the number of integer points in the Newton polytope of $E(\boldsymbol{t}, y)$. Beyond the significant improvements this refined version may induce in some cases, it also suggests a potential link between the optimal bound N and geometric invariants attached to the algebraic hypersurface of equation $E(\boldsymbol{t}, y) = 0$. Indeed, after the work of Baker [**Bak93**], Hodge [**Hod29**] and Khovanskii [**Kho78**], it is known that the geometric genus of the aforementioned hypersurface is bounded from above by the number of integer points in the Newton polytope of $E(\boldsymbol{t}, y)$ and that equality holds generically. A natural question is then whether the degree of the minimal polynomial of $\Delta(f)_{|p}$ is always at most $p^{g+O(1)}$ where g is the geometric genus of the underlying hypersurface. When $n = 1$, Bridy's approach [**Bri17**] provides a positive answer to this expectation; in full generality, however, the question remains open.

Let k be a field of characteristic zero, and let $f(\boldsymbol{t}) \in k[\![\boldsymbol{t}]\!]$ be algebraic over $k(\boldsymbol{t})$. Then there exists a finitely generated $\mathbb{Z}$-algebra Z such that $f(\boldsymbol{t}) \in Z[\![\boldsymbol{t}]\!]$, and, for any maximal ideal $\mathfrak{p}$ of Z, the quotient $Z/\mathfrak{p}$ is a finite field (see, e.g., [**AB13**, p. 967]). In this framework, we obtain, as a direct consequence of Theorem 3.1, the following generalization of Theorem 1.1, in the spirit of [**AB13**, Thm. 1.4]. A particularly interesting case occurs when k is a number field and $Z = \mathcal{O}_{k,\mathfrak{p}}$, the localization of the ring of integers $\mathcal{O}_k$ of k at $\mathfrak{p}$.

Theorem 1.4. — *Let k be a feld of characteristic zero, $Z \subset k$ be a finitely generated $\mathbb{Z}$-algebra, and $f \in Z[\![\boldsymbol{t}]\!]$ be algebraic over $k(\boldsymbol{t})$ with degree d, total height h, and partial height $(h_1, \dots, h_n)$. Then, for every maximal ideal $\mathfrak{p}$ of Z, $\Delta(f)_{|\mathfrak{p}}$ is annihilated by a linearized polynomial with coefficients in $(Z/\mathfrak{p})(t)$ of p-degree at most N, where p is the characteristic of $Z/\mathfrak{p}$ and N is defined as in (1.1). In particular, $\Delta(f)_{|\mathfrak{p}}$ has degree at most $p^N - 1$ over $(Z/\mathfrak{p})(t)$.*

1.1. Comparison with previous works. — The proof of Furstenberg's theorem presented in [**Fur67**] is direct and elementary, yielding a polynomial upper bound $d_p < p^N$ when $d = 1$ and n is arbitrary, with N having a value similar to that in Theorem 1.1 in this case. Deligne [**Del84**, p. 140] subsequently treated the case $n = 2$ and arbitrary d, obtaining the bound $d_p = O(p^N)$, where N is expressed in terms of geometric quantities associated with the underlying algebraic power series. Another approach, which traces its origin to [**CKMFR80**], relies on the fact that any algebraic power series is annihilated by a linearized polynomial. This method has been used independently by several authors [**DL87**, **SW88**, **Har88**] (and also [**Sal87**, **Sal86**]

in some special cases) to give an elementary proof of Deligne's theorem. Harase [**Har89**] (see also [**AB12**]) later showed that this approach yields a doubly exponential bound, namely $d_p = O(p^{p^N})$, for arbitrary d and n.

As noted earlier, the first general polynomial bound, *i.e.*, in $O(p^N)$, was established in [**AB13**], where the proof provides an effective N that depends only on the degree d and the total height h of f[(1)]. However, before this paper, the best upper bound for N was a *nonelementary* primitive recursive bound –precisely, a tower of exponentials with height (at least) linear in the number n of variables. The reason is that, when $d > 1$, the value of N becomes exceedingly large due to a recursive procedure involving resultants. For instance, even when the number of variables is $n = 2$, the estimate for $N = N(2, d, h)$ in [**AB13**, Theorem 6.1] takes the form

$$2^{2^{2^{4^{hd^2}}}}.$$

This can be seen by carefully analyzing the quantities appearing in the proof of Theorem 6.1, together with the estimates of Lemmas 6.1, 6.2 and 6.3 in [**AB13**]. Indeed, $N(2, d, h)$ grows like $N(1, d_1, h_1) \sim 4h_1d_1^3$, where d_1 grows like $d_0^{d_0M^2}$ and h_1 grows like $d_0^{d_0\cdot M^{2d_0^{M^2}}}$, where $M \sim 4hd^3$ and $d_0 \sim d^{4^{hd^2}}$, and these estimates altogether imply that $\log_2\log_2\log_2\log_2(h_1)$ grows like $2hd^2$.

The approach we adopt here is analogous to that in [**AB13**], but instead of expressing algebraic power series as diagonals of rational functions, we express them as formal residues of rational functions. This formulation, which was first employed in [**BCCD19**] for univariate algebraic power series, is a variant of Furstenberg's formula analogous to Lagrange's formula for the residues of rational functions with simple poles (see Lemma 2.6). The primary advantage of this method is that it avoids any inductive process.

Beyond diagonals of algebraic power series, other significant families of G-functions in $\mathbb{Q}[\![t]\!]$ have algebraic reductions modulo p (cf. [**ABD19**, **VM21**]). Moreover, the property of *algebraicity modulo p* provides a powerful tool for establishing results on the transcendence and algebraic independence of power series in characteristic zero (cf. [**WS89**, **AGBS98**, **AB13**, **ABD19**, **VM24**]).

1.2. Organization of the article. — This article is a condensed version of an unpublished preprint made available on arXiv in 2023 (cf. [**ABC23**]). In Section 2, we establish Theorem 2.3, which provides a sharp, quantitative multivariate extension of Christol's theorem (see [**Chr79**, **CKMFR80**]) concerning algebraic power series with coefficients in finite fields. Our result also

(1) Using the approach from [**AB13**], it is also possible to deduce the existence of such a polynomial bound from another result in [**DL87**], but with an ineffective constant N.

generalizes its extension to perfect ground fields of positive characteristic, obtained independently in [**DL87**, **SW88**, **Har88**]. In Section 3, we derive our quantitative version of Deligne's theorem as a consequence of Theorem 2.3, from which Theorem 1.1 follows directly. We emphasize that Theorem 2.3 is of independent interest and has several further applications, discussed in detail in [**ABC23**], including the following:

(i) For a multivariate algebraic power series with coefficients in a finite field $\mathbb{F}_q$, it provides an upper bound on the minimal number of states required for a q-automaton to generate its sequence of coefficients. This generalizes a result of Bridy [**Bri17**] to the multidimensional setting (see [**ABC23**, Sec. 4]).

(ii) For two multivariate algebraic power series over an arbitrary field of characteristic p, it establishes an upper bound on the algebraic degree of their Hadamard product and other related products. This significantly improves the doubly exponential bounds that follow from [**DL87**, **SW88**, **Har88**] and were made explicit by Harase [**Har89**] (see [**ABC23**, Sec. 6]).

(iii) It provides an efficient algorithm for computing the coefficient of a given multivariate algebraic power series in $\mathbb{F}_q[\![\boldsymbol{t}]\!]$ at a specified multi-index. The power series is encoded by its minimal polynomial over $\mathbb{F}_q(\boldsymbol{t})$ along with a sufficient number of initial coefficients to ensure uniqueness, Again, this improves significantly upon previously known results (see [**ABC23**, Sec. 7]).

2. A sharper multivariate Christol theorem

Let k be a perfect field of characteristic $p > 0$. Then the Frobenius endomorphism F, which maps x to x^p, is an automorphism of k. Let $\boldsymbol{t} = (t_1, \dots, t_n)$ be indeterminates, and define $K_0 := k(\boldsymbol{t})$, $R := k[\![\boldsymbol{t}]\!]$ and $K := \mathrm{Frac}(R)$, the field of fractions of R. The Frobenius map F extends naturally to K as a field homomorphism by setting $\mathsf{F}(t_i) = t_i^p$, for $1 \le i \le n$, so that for a power series $f := \sum_{\boldsymbol{i} \in \mathbb{N}^n} a(\boldsymbol{i}) \boldsymbol{t}^{\boldsymbol{i}} \in k[\![\boldsymbol{t}]\!]$, we have

$$\mathsf{F}(f) = \sum_{\substack{\boldsymbol{i} \in \mathbb{N}^n \\ \boldsymbol{i} = (i_1, \dots, i_n)}} a(\boldsymbol{i})^p \boldsymbol{t}^{p\boldsymbol{i}} \in k[\![\boldsymbol{t}]\!] \,.$$

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 monomials 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

$$f = \sum_{\boldsymbol{r}\in\{0,\dots,p-1\}^n} \boldsymbol{t}^{\boldsymbol{r}} f_{\boldsymbol{r}}\,, \qquad \text{where } f_{\boldsymbol{r}} \in K^{\langle p\rangle}. \tag{2.1}$$

Definition 2.1. — For every $\boldsymbol{r} \in \{0,\dots,p-1\}^n$, the *section operator* $S_{\boldsymbol{r}}$ is the map from K into itself defined by

$$S_{\boldsymbol{r}}(f) \coloneqq \mathsf{F}^{-1}(f_{\boldsymbol{r}})\,. \tag{2.2}$$

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.

The section operators are also sometimes referred to as *Cartier operators* (see, for instance, [**AB13**]). Recall that they are k-linear and satisfy, for all $f, g \in K$, the relation

$$S_{\boldsymbol{r}}(f\mathsf{F}(g)) = S_{\boldsymbol{r}}(f)g\,. \tag{2.3}$$

Moreover, Equality (2.1) can be equivalently written as

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

for all $f \in K$.

Definition 2.2. — 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 $(\boldsymbol{i}, j)$ such that $a_{\boldsymbol{i},j} \neq 0$.

The main result of this section is stated as follows.

Theorem 2.3. — *Let k be a perfect field of characteristic p and let $\boldsymbol{t} = (t_1,\dots,t_n)$. 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 $A(\boldsymbol{t}, f) = 0$. Define*

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

Then, there exists a k-vector space $W \subset k[\![\boldsymbol{t}]\!]$ of dimension at most

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

which contains f and is invariant under the action the monoid Ω_n of all section operators.

Remark 2.4. — The plus sign in the definition of C refers to the Minkowski sum. In Theorem 2.3, the field k must be perfect for the section operators to be well-defined; however, this does not present a real limitation. Indeed, replacing an arbitrary field of characteristic p by its perfect closure does not affect our results (cf. Proposition 3.4).

In the case where k is a finite field, it follows that the orbit of f under Ω_n is finite, which implies that the sequence of coefficients of f is generated by a finite p-automaton. Consequently, Theorem 2.3 extends and refines Christol's theorem. Furthermore, Theorem 2.3 carries a geometric flavor (cf. Remark 1.3), analogous to the more recent result established by Bridy [**Bri17**] in the case where k is a finite field and $n = 1$ (see [**ABC23**, Sec. 4] for a detailed discussion).

2.1. Preliminary results. — We begin by establishing three auxiliary results: Lemmas 2.5 and 2.6, and Proposition 2.7. These results correspond, respectively, to natural extensions in our framework of Lemma 2.4, Lemma 2.3, and Proposition 2.5 from [**BCCD19**].

2.1.1. Section operators on $K(\!(T)\!)$. — Consider a new indeterminate T. Then F extends to a field homomorphism from $K(\!(T)\!)$ into itself by setting $\mathsf{F}(T) = T^p$. We let $K(\!(T)\!)^{\langle p\rangle}$ denote the image of $K(\!(T)\!)$ under F. As before, $K(\!(T)\!)$ is a $K(\!(T)\!)^{\langle p\rangle}$-vector space of dimension p^{n+1}, with a basis given by all monomials of the form $\boldsymbol{t}^{\boldsymbol{r}}T^s$, where $\boldsymbol{r} \in \{0,\dots,p-1\}^n$ and $0 \le s \le p-1$. However, for our purposes, it will be more convenient to replace this standard basis with a more suitable one, adapted to a given $f \in R$.

Lemma 2.5. — *For any $f \in R$, the family*

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

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 $\boldsymbol{t}^{\boldsymbol{r}}(f+T)^i$, for $0 \le i \le s$. This follows from

$$T^s = (T+f-f)^s = \sum_{i=0}^{s} \binom{s}{i} (-f)^{s-i}(T+f)^i\,.$$

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

$$x = \sum_{\boldsymbol{r} \in \{0,\dots,p-1\}^n} \boldsymbol{t}^{\boldsymbol{r}} \sum_{s=0}^{p-1} (f+T)^s x_{f,\boldsymbol{r},s}\,, \qquad \text{where } x_{f,\boldsymbol{r},s} \in K(\!(T)\!)^{\langle p \rangle}. \tag{2.4}$$

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

$$S_{f,\boldsymbol{r},s}(x) \coloneqq \mathsf{F}^{-1}(x_{f,\boldsymbol{r},s})\,. \tag{2.5}$$

One readily verifies that, for all $x, y \in K(\!(T)\!)$,

$$S_{f,\boldsymbol{r},s}(xy^p) = S_{f,\boldsymbol{r},s}(x\mathsf{F}(y)) = S_{f,\boldsymbol{r},s}(x)y\,,$$

for every $\boldsymbol{r} \in \{0,\dots,p-1\}^n$ and $s \in \{0,\dots,p-1\}$. This definition and the above identity are analogous to Definition 2.1 and Equation (2.3).

2.1.2. A variant of Furstenberg's formula. — We define the residue map res from $K(\!(T)\!)$ 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 inspired by [**Fur67**, Prop. 2] and analogous to Lagrange's formula for the residues of rational functions with simple poles.

Lemma 2.6. — *Let $f \in K$ and $A(y) \in K[y]$. Assume that $A(f) = 0$ and $A_y(f) \neq 0$. Then, for all $P \in K[y]$, one has*

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

Proof. — Let $U, V \in K[y]$ such that $V(0) = 0$ and $V_y(0) \neq 0$. Thus, we can express V as $V = \sum_{n=1}^{r} a_n y^n$ with $a_1 \neq 0$. It follows that

$$\frac{U(T)}{V(T)} = \frac{1}{T} \cdot \left(\frac{U(T)}{a_1 + a_2 T + \cdots + a_r T^{r-1}}\right)$$

and consequently,

$$\mathsf{res}\left(\frac{U(T)}{V(T)}\right) = \frac{U(0)}{a_1} = \frac{U(0)}{V_y(0)}\,.$$

The result follows by applying the above equality to $U = P(f+T)$ and $V = A(f+T)$. □

2.1.3. Section operators and residues. — The next result establishes a fundamental commutation relation between taking residues and applying section operators. It is reminiscent of a result of Cartier involving the so-called Cartier operator [**Car57**, Th. 4] (see also [**Bri17**, Sec. 3]).

Proposition 2.7. — *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 Equations (2.4) and (2.5), 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, we obtain that

$$\mathsf{res}(x) = \sum_{\boldsymbol{r}\in\{0,\dots,p-1\}^n} \boldsymbol{t}^{\boldsymbol{r}} \sum_{s=0}^{p-1} \mathsf{res}\Big((f+T)^s\, \mathsf{F}(S_{f,\boldsymbol{r},s}(x))\Big)\,. \tag{2.6}$$

Since $\mathsf{F}(S_{f,\boldsymbol{r},s}(x)) \in K(\!(T)\!)^{\langle p\rangle}$, its support (that is, the set of indices corresponding to nonzero coefficients of $\mathsf{F}(S_{f,\boldsymbol{r},s}(x))$ viewed as a Laurent series in the variable T) is contained in $p\mathbb{Z}$. Therefore, we have

$$\mathsf{res}\Big((f+T)^s\, \mathsf{F}(S_{f,\boldsymbol{r},s}(x))\Big) = 0 \quad \text{for} \quad 0 \le s \le p-2\,,$$

while, for $s = p-1$,

$$\mathsf{res}\Big((f+T)^{p-1}\, \mathsf{F}(S_{f,\boldsymbol{r},s}(x))\Big) = \mathsf{res}\Big(T^{p-1}\, \mathsf{F}(S_{f,\boldsymbol{r},s}(x))\Big) = \mathsf{F}\big(\mathsf{res}\,\big(S_{f,\boldsymbol{r},p-1}(x)\big)\big)\,.$$

Substituting this into Equation (2.6), we obtain

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

Finally, applying (2.1) and (2.2) with $f = \mathsf{res}(x)$, we deduce that

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

as desired. □

2.2. Proof of Theorem 2.3. — Let $E(\boldsymbol{t}, y) \in k[\boldsymbol{t}, y]$ denote the minimal polynomial of f over $k(t)$, normalized such that its coefficients are globally coprime.

Lemma 2.8. — *The polynomial $E(\boldsymbol{t}, y)$ is separable with respect to y. In particular, f is a simple root of $E(\boldsymbol{t}, y)$ with respect to y.*

Proof. — Since $E(\boldsymbol{t}, y)$ is defined as the minimal polynomial, it suffices 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 proceed by contradiction, assuming that $E(\boldsymbol{t}, y) = F(\boldsymbol{t}, y^p)$ for some $F(\boldsymbol{t}, z) \in k[\boldsymbol{t}, z]$. We can 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 $\boldsymbol{r} \in \{0, \ldots, p-1\}^n$. Applying the section operator $S_{\boldsymbol{r}}$ to the identity $F(\boldsymbol{t}, f^p) = 0$, we obtain

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

Since $a_m(\boldsymbol{t})$ is nonzero, there must exist an index $\boldsymbol{r}$ for which $S_{\boldsymbol{r}}(a_m(\boldsymbol{t})) \neq 0$. For such an $\boldsymbol{r}$, we obtain a nonzero polynomial annihilating f with y-degree smaller than the y-degree of E. This contradicts the minimality of E. □

Proof of Theorem 2.3. — Let E_y denote the partial derivative of E with respect to y. By Lemma 2.8, we have $E_y(\boldsymbol{t}, f) \neq 0$. Furthermore, since A annihilates f, it must be a multiple of E; that is, we can write $A = E \cdot F$ for some $F \in k[\boldsymbol{t}, y]$. Let J be the interval $(-1, 0]$ and define $C' := \mathrm{NP}(E) + J^{n+1}$.

We claim that the k-vector space

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

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

$$Q(\boldsymbol{t}, f + T) := S_{f,\boldsymbol{r},p-1}(U(\boldsymbol{t}, f + T)) \in K\,. \tag{2.7}$$

By combining Lemma 2.6 and Proposition 2.7, we obtain:

$$\begin{aligned} S_{\boldsymbol{r}}\left(\frac{P(\boldsymbol{t}, f)}{E_y(\boldsymbol{t}, f)}\right) &= S_{\boldsymbol{r}} \circ \mathsf{res}\left(\frac{P(\boldsymbol{t}, f+T)}{E(\boldsymbol{t}, f+T)}\right) \\ &= \mathsf{res} \circ S_{f,\boldsymbol{r},p-1}\left(\frac{P(\boldsymbol{t}, f+T)}{E(\boldsymbol{t}, f+T)}\right) \\ &= \mathsf{res}\left(\frac{Q(\boldsymbol{t}, f+T)}{E(\boldsymbol{t}, f+T)}\right) \\ &= \frac{Q(\boldsymbol{t}, f)}{E_y(\boldsymbol{t}, f)}\,. \end{aligned} \tag{2.8}$$

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. Specifically, for $A, B \in k[\boldsymbol{t}, y]$, we have the relation

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

Using this property, we can derive the following:

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

Now, let $(\boldsymbol{i}, j)$ be a tuple of exponents belonging to the support of Q, *i.e.*, for which the coefficient in Q in front of $\boldsymbol{t}^{\boldsymbol{i}} y^j$ is nonzero. From the definition of $S_{f,\boldsymbol{r},p-1}$, it follows that $(p\boldsymbol{i} + \boldsymbol{r}, pj + p - 1)$ must lie in $\mathrm{NP}(U)$. Dividing by p and defining $I := (-\frac{1}{p}, 0]$, we obtain

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

Thus, we conclude that

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

Finally, we have shown that $\mathrm{NP}(Q) \subset C'$, as desired.

Clearly W is spanned by the fractions of the form $\boldsymbol{t}^{\boldsymbol{i}} f^j / E_y(\boldsymbol{t}, f)$, where $(\boldsymbol{i}, j) \in C' \cap \mathbb{N}^{n+1}$. Hence, the dimension of W is bounded from above by the cardinality of this set. Furthermore, we observe that $C = \mathrm{NP}(F) + C'$, where F is nonzero. Since $\mathrm{NP}(F)$ is the Newton polytope of a nonzero polynomial, it must intersect $\mathbb{N}^{n+1}$. Therefore, C contains a translate of C' by an element with nonnegative integer coefficients. As a result, the cardinality of $C \cap \mathbb{N}^{n+1}$ is at least that of $C' \cap \mathbb{N}^{n+1}$, and we conclude that

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

as desired. □

3. Diagonals

By combining Theorem 2.3 with Propositions 5.1 and 5.2 of [**AB13**], we immediately obtain an effective version of Deligne's theorem: given an algebraic power series $f \in k[\![\boldsymbol{t}]\!]$ of degree d and total height h, its diagonal $\Delta(f)$ has degree at most p^N (and height at most Np^N), where N is explicitly given by

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

3.1. An effective version of Deligne's theorem. — In this section, we establish a refinement of the result stated above, from which Theorem 1.1 follows directly.

Theorem 3.1. — *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*

$$N \coloneqq (d+1) \cdot \min\left\{ \prod_{i=1}^{n} (h_i + 1) - \prod_{i=1}^{n} h_i, \binom{n+h}{n} - \binom{h}{n} \right\}. \tag{3.1}$$

Then, $\Delta(f)$ is annihilated by a linearized polynomial with coefficients in $k(t)$ of p-degree at most N. In particular, $\Delta(f)$ has degree at most $p^N - 1$ over $k(t)$.

Theorem 3.1 will be deduced from Theorem 3.3, a slightly more general result stated in terms of generalized diagonals and Newton polytopes.

3.2. Generalized diagonals. — In what follows, we introduce a slight generalization of the diagonalization process. We continue with the previous notation: k is a perfect field of characteristic p and $K_0 = k(\boldsymbol{t})$, $R = k[\![\boldsymbol{t}]\!]$, and $K = \mathrm{Frac}(R)$ are defined as in Section 2. Let G be a subgroup of $\mathbb{Z}^n$ such that the quotient $\mathbb{Z}^n/G$ has no torsion. We define $K_{0,G}$ as 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 $\sum_{\boldsymbol{i} \in G} a(\boldsymbol{i}) \boldsymbol{t}^{\boldsymbol{i}}$. Since G is abstractly isomorphic to $\mathbb{Z}^m$ for some integer $m \leq n$, the rings $K_{0,G}$ and R_G are isomorphic to $k(x_1, \dots, x_m)$ and $k[\![x_1, \dots, x_m]\!]$, respectively.

Definition 3.2. — We keep the notation introduced above. 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 $a(\boldsymbol{i}) = 0$ for $\boldsymbol{i} \notin \mathbb{N}^n$.

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 reduces to the usual diagonal operator Δ. However, the more general construction of Δ_G offers greater flexibility and allows for partial diagonals, as considered in [**DL87**]. For instance, if G is the subgroup generated by $(1, \dots, 1)$ together with the standard basis vectors $e_i = (0, \dots, 0, 1, 0, \dots, 0)$ (where 1 is in i-th position) for $i \in \{1, \dots, m\}$, then

$$R_G \simeq k[\![t_1, \dots, t_m, x]\!]$$

and we have

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

More generally, one can verify that Δ_G is $K_{0,G}$-linear.

Theorem 3.3. — *Let k be an arbitrary field of characteristic p, and let G be a subgroup of $\mathbb{Z}^n$ such that $\mathbb{Z}^n/G$ has no torsion. Let $G_{\mathbb{R}}$ be the vector subspace 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 $f \in k[\![\boldsymbol{t}]\!]$ satisfy the algebraic relation $A(\boldsymbol{t}, f) = 0$. Define C as the convex subset of $\mathbb{R}^{n+1}$ given by*

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

Then, $\Delta_G(f)$ is annihilated by a linearized polynomial with coefficients in $K_{0,G}$ of p-degree at most N, where $N \coloneqq \mathrm{Card}\big(\pi_G(C \cap \mathbb{N}^{n+1})\big)$.

Recall that if k is a 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, called the perfect closure of k, which we denote by k_p. Before proving Theorem 3.3, we recall the following elementary result (see [**ABC23**, Prop. 3.1] for a proof).

Proposition 3.4. — *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, $[k(\boldsymbol{t})(f) : k(\boldsymbol{t})] = [k_p(\boldsymbol{t})(f) : k_p(\boldsymbol{t})]$.*

Proof of Theorem 3.3. — By Proposition 3.4, we may, without any loss of generality, replace the field k by the perfect closure of the subfield of k generated over $\mathbb{F}_p$ by the coefficients of f. Hence we may assume that k is perfect.

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

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

By following the proof of Theorem 2.3, we obtain 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 $\boldsymbol{r} \in G$, it follows that $\Delta_G(W)$ is also invariant under $S_{\boldsymbol{r}}$ for all $\boldsymbol{r} \in G$.

Let V denote the $K_{0,G}$-span of $\Delta_G(W)$ in $K_G \coloneqq \mathrm{Frac}(R_G)$. We first show that the dimension of V, viewed as a $K_{0,G}$-vector space, is bounded by N, and then prove that V is invariant under the action of the Frobenius map.

By linearity, we see that V is spanned by the elements $\frac{\boldsymbol{t}^{\boldsymbol{i}} f^j}{E_y(\boldsymbol{t},f)}$ for $(\boldsymbol{i},j)$ running over $C' \cap \mathbb{N}^{n+1}$. Moreover, two fractions

$$\frac{\boldsymbol{t}^{\boldsymbol{i}} f^j}{E_y(\boldsymbol{t},f)} \quad \text{and} \quad \frac{\boldsymbol{t}^{\boldsymbol{i}'} f^{j'}}{E_y(\boldsymbol{t},f)}$$

are $K_{0,G}$-collinear when $\boldsymbol{i} \equiv \boldsymbol{i}'$ mod 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 therefore bounded above by the cardinality of $\pi_G(C' \cap \mathbb{N}^{n+1})$, which is itself bounded by N (see the final paragraph of the proof of Theorem 2.3 for more details).

Let us now show that V is invariant under the Frobenius map F. The latter acts as an endomorphism of $K_{0,G}$. We now define the "relative" Frobenius map on K_G 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 $\otimes_{K_{0,G},\mathsf{F}}$ indicates 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. Furthermore, ψ 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 $G_p \subset G$ is a set of representatives of G/pG. As shown earlier, V is closed under the action of $S_{\boldsymbol{r}}$ for all $\boldsymbol{r} \in G$. Therefore, we conclude that ψ^{-1} induces a $K_{0,G}$-linear morphism from V to $V \otimes_{K_{0,G},\mathsf{F}} K_{0,G}$. Since ψ^{-1} is the restriction of an injective map, it is clearly injective. Furthermore, because V is finite dimensional over $K_{0,G}$ and $\dim_{K_{0,G}} V = \dim_{K_{0,G}}(V \otimes_{K_{0,G},\mathsf{F}} K_{0,G})$, we conclude that ψ^{-1} is an isomorphism. This implies that ψ takes $V \otimes_{K_{0,G},\mathsf{F}} K_{0,G}$ to V, which in turn shows that V is invariant under the Frobenius map.

In particular, for all nonnegative integers s, we have $\Delta_G(f)^{p^s} \in V$. Since $\dim_{K_{0,G}} V \leq N$, 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. □

3.3. Proof of Theorem 3.1. — We will now proceed with the proof of the main result of this section.

Proof of Theorem 3.1. — We apply Theorem 3.3 with the group G generated by $(1, \ldots, 1)$. As already noted, the diagonal Δ_G coincides with the usual diagonal Δ, under 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 and C be the mapping and convex set defined in the statement of Theorem 3.3. By Theorem 3.3, it remains to prove that $\mathrm{Card}\big(\pi_G(C \cap \mathbb{N}^{n+1})\big) \leq N$, where N is defined as in Equation (3.1).

Consider an element $c \coloneqq (a_1, \ldots, a_n, b) \in C \cap \mathbb{N}^{n+1}$. By definition of C, we have $-1 < b \leq d$, and since b is an integer, we conclude that $0 \leq b \leq d$. Moreover, by translating c by an element of G, we may assume that $0 \leq a_i \leq h_i$ for all $i \in \{1, \ldots, n\}$, and $\sum_{i=1}^{n} a_i \leq h$. Define $a \coloneqq \min\{a_1, \ldots, a_n\}$ and, for each i, set $\tilde{a}_i \coloneqq a_i - a$. Then at least one of the first n coordinates of $\tilde{c} \coloneqq (\tilde{a}_1, \ldots, \tilde{a}_n, b)$ is zero. Furthermore, we still have $0 \leq \tilde{a}_i \leq h_i$ and $\sum_{i=1}^{n} \tilde{a}_i \leq h$. Since $\pi_G(c) = \pi_G(\tilde{c})$, it follows that every element of $\pi_G(C \cap \mathbb{N}^{n+1})$ has a preimage in both of the following sets:

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

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

The cardinalities of these sets are given by

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

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

Thus, we obtain that $\mathrm{Card}\big(\pi_G(C \cap \mathbb{N}^{n+1})\big) \leq \min\{\mathrm{Card}(\mathcal{E}_1), \mathrm{Card}(\mathcal{E}_2)\} = N$, as required. □

Acknowledgements. — The authors would like to thank the anonymous referees for their careful reading of an earlier version of this paper and for their valuable comments.

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.

[ABC23] B. Adamczewski, A. Bostan, and X. Caruso. A sharper multivariate Christol theorem with applications to diagonals and Hadamard products. arXiv:2306.02640 [math.NT], https://arxiv.org/abs/2306.02640, 2023.

[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.

[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.

[BMM10] M. Bousquet-Mélou and M. Mishna. Walks with small steps in the quarter plane. In *Algorithmic probability and combinatorics*, volume 520 of *Contemp. Math.*, pages 1–39. Amer. Math. Soc., Providence, RI, 2010.

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

[Car57] P. Cartier. Une nouvelle opération sur les formes différentielles. *C. R. Acad. Sci. Paris*, 244:426–428, 1957.

[CFVM25] X. Caruso, F. Fürnsinn, and D. Vargas-Montoya. Galois groups of reductions modulo p of D-finite series. arXiv:2504.09429 [math.NT], https://arxiv.org/abs/2504.09429, 2025.

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

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

[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.

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

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

[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.

[Kho78] A. G. Khovanskiĭ. Newton polyhedra, and the genus of complete intersections. *Funktsional. Anal. i Prilozhen.*, 12(1):51–61, 1978.

[Mel21] S. Melczer. *An invitation to analytic combinatorics—from one to several variables*. Texts and Monographs in Symbolic Computation. Springer, Cham, [2021] ©2021. With a foreword by Robin Pemantle and Mark Wilson.

[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.

[Sta99] s R. P. Stanley. *Enumerative combinatorics. Vol. 2*, volume 62 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1999.

[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.

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

[VM24] D. Vargas-Montoya. Monodromie unipotente maximale, congruences "à la Lucas" et indépendance algébrique. *Trans. Amer. Math. Soc.*, 377:167–202, 2024.

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

Boris Adamczewski, Univ. Claude Bernard Lyon 1, CNRS UMR 5208, Institut Camille Jordan, 43 blvd. du 11 novembre 1918, F-69622 Villeurbanne Cedex, France, and Centre International de Rencontres Mathématiques (CIRM), 163 Av. de Luminy, 13009 Marseille, France • *E-mail :* boris.adamczewski@math.cnrs.fr

Alin Bostan, Inria, Sorbonne Université, LIP6, 4 place Jussieu, 75252 Paris, France *E-mail :* alin.bostan@inria.fr

Xavier Caruso, CNRS, IMB, Université de Bordeaux, 351 cours de la Libération, 33405 Talence, France • *E-mail :* xavier@caruso.ovh