

quatrième série - tome 59 fascicule 3 mai-juin 2026

*ANNALES
SCIENTIFIQUES
de
L'ÉCOLE
NORMALE
SUPÉRIEURE*

Boris ADAMCZEWSKI, Alin BOSTAN & Xavier CARUSO

Diagonals and algebraicity modulo p : a sharper degree bound

SOCIÉTÉ MATHÉMATIQUE DE FRANCE

Annales Scientifiques de l'École Normale Supérieure

Publiées avec le concours du Centre National de la Recherche Scientifique

Responsable du comité de rédaction / *Editor-in-chief*

Jean-François QUINT

Publication fondée en 1864 par Louis Pasteur

Continuée de 1872 à 1882 par H. SAINTE-CLAIRE DEVILLE
de 1883 à 1888 par H. DEBRAY
de 1889 à 1900 par C. HERMITE
de 1901 à 1917 par G. DARBOUX
de 1918 à 1941 par É. PICARD
de 1942 à 1967 par P. MONTEL

Comité de rédaction au 27 mars 2026

T. ALAZARD	S. GOUËZEL
S. CANTAT	Y. HARPAZ
K. CESNAVICIUS	A. KEATING
Y. DE CORNULIER	G. MIERMONT
C. FERMANIAN KAMMERER	S. RICHEL
J. FRESÁN	A. SONG

Rédaction / *Editor*

Annales Scientifiques de l'École Normale Supérieure,
45, rue d'Ulm, 75230 Paris Cedex 05, France.

Tél. : (33) 1 44 32 20 88.

Email : annales@ens.fr

Édition et abonnements / *Publication and subscriptions*

Société Mathématique de France

Case 916 - Luminy

13288 Marseille Cedex 09

Tél. : (33) 04 91 26 74 64

Email : abonnements@smf.emath.fr

Tarifs

Abonnement électronique : 514 euros.

Abonnement avec supplément papier :

Europe : 722 €. Hors Europe : 813 € (\$ 985). Vente au numéro : 77 €.

© 2026 Société Mathématique de France, Paris

En application de la loi du 1^{er} juillet 1992, il est interdit de reproduire, même partiellement, la présente publication sans l'autorisation de l'éditeur ou du Centre français d'exploitation du droit de copie (20, rue des Grands-Augustins, 75006 Paris).

All rights reserved. No part of this publication may be translated, reproduced, stored in a retrieval system or transmitted in any form or by any other means, electronic, mechanical, photocopying, recording or otherwise, without prior permission of the publisher.

ISSN 0012-9593 (print) 1873-2151 (electronic)

Directrice de la publication : Isabelle Gallagher

Périodicité : 6 n^{os} / an

DIAGONALS AND ALGEBRAICITY MODULO p : A SHARPER DEGREE BOUND

BY BORIS ADAMCZEWSKI, ALIN BOSTAN AND XAVIER CARUSO

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.

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 fractions rationnelles à coefficients dans $\mathbb{F}_p$. De plus, il a suggéré que les degrés d’algébricité d_p de ces fonctions ne devraient croître qu’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 explicite et raisonnable.

1. Introduction

Given a ring R and a multivariate power series

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

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

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

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).

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

$$f|_{\mathfrak{p}}(\mathbf{t}) := \sum_{\mathbf{i} \in \mathbb{N}^n} (a(\mathbf{i}) \bmod \mathfrak{p}) \mathbf{t}^{\mathbf{i}} \in (R/\mathfrak{p})[[\mathbf{t}]].$$

A particularly interesting case arises when R is $\mathbb{Z}$, or more generally the ring of integers of a number field, and the power series f is algebraic over $\overline{\mathbb{Q}}(\mathbf{t})$. 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 [2, 13] and the references therein for further discussion of these connections. Moreover, such power series frequently appear in enumerative combinatorics (see [26, Chap. 6], [8] and [22, Chap. 4]). Additionally, diagonalization is closely related to integration (see [15] and [13, Sec. 3]), and in general, $\Delta(f)$ is transcendental over $\overline{\mathbb{Q}}(\mathbf{t})$ (see, for instance, [2]).

By contrast, when $R = k$ is a field of characteristic $p > 0$, and f is a multivariate rational power series, Furstenberg [17] proved the following remarkable result: the diagonal $\Delta(f)$ is always algebraic over $k(\mathbf{t})$. Later, Deligne [15] 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 $f \in \mathbb{Z}[[\mathbf{t}]]$ is algebraic, then $\Delta(f)|_p$ remains algebraic over $\mathbb{F}_p(\mathbf{t})$ 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 [15], 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 [16, 25, 18, 24, 23], 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 [2] 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.

Given a field k , the complexity of an algebraic power series $f \in k[[\mathbf{t}]]$ is traditionally measured in terms of its *degree* and *height*. Since the ring $k[\mathbf{t}, y]$ is a unique factorization domain, there exists a polynomial $E(\mathbf{t}, y) \in k[\mathbf{t}, y]$ satisfying $E(\mathbf{t}, f) = 0$, 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 $E(\mathbf{t}, y)$; equivalently, it is the degree of the field extension $k(\mathbf{t})(f)$ of $k(\mathbf{t})$. For the height, we consider two natural definitions: the *total height* of f is the total degree in $\mathbf{t}$ of $E(\mathbf{t}, y)$ (where the total degree of the monomial $\mathbf{t}^{\mathbf{i}}$ is $i_1 + \dots + i_n$), while its *partial height* is the tuple $\mathbf{h} = (h_1, \dots, h_n)$ where, for each i , h_i is the degree in t_i of $E(\mathbf{t}, y)$.

We recall that, when k has characteristic $p > 0$, every element f in the algebraic closure of $k(\mathbf{t})$ is annihilated by a *linearized polynomial*, i.e., a polynomial $P(X) \in k(\mathbf{t})[X]$ of the

form

$$c_0X + c_1X^p + \cdots + c_NX^{p^N}, \quad c_N \neq 0.$$

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

Our main result is stated as follows.

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

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

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

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. This problem is investigated in a recent preprint by Caruso, Fürnsinn, and Vargas-Montoya ([11]).

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 $E(t, y)$. 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 $E(t, y) = 0$. Indeed, after the work of Baker [6], Hodge [20] and Khovanskii [21], 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 $E(t, y)$ 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 [9] 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 $f(t) \in k[[t]]$ be algebraic over $k(t)$. Then there exists a finitely generated $\mathbb{Z}$ -algebra Z such that $f(t) \in Z[[t]]$, and, for any maximal ideal $\mathfrak{p}$ of Z , the quotient $Z/\mathfrak{p}$ is a finite field (see, e.g., [2, 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 [2, 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 $\mathfrak{p}$.