ISSN 0012-9593

quatrième série - tome 52 *fascicule 3* *mai-juin 2019*

ANNALES SCIENTIFIQUES de L'ÉCOLE NORMALE SUPÉRIEURE

SOCIÉTÉ MATHÉMATIQUE DE FRANCE

Annales Scientifiques de l'École Normale Supérieure

Publiées avec le concours du Centre National de la Recherche Scientifique

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. Fax : (33) 1 44 32 20 80.
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
Fax : (33) 04 91 41 17 51
email : abonnements@smf.emath.fr

Tarifs

Abonnement électronique : 420 euros.
Abonnement avec supplément papier :
Europe : 551 €. Hors Europe : 620 € ($ 930). Vente au numéro : 77 €.

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

Directeur de la publication : Stéphane Seuret
Périodicité : 6 nos / an

Ann. Scient. Éc. Norm. Sup.
4ᵉ série, t. 52, 2019, p. 515 à 559

ALGEBRAIC INDEPENDENCE OF G-FUNCTIONS AND CONGRUENCES "À LA LUCAS"

BY BORIS ADAMCZEWSKI, JASON P. BELL AND ÉRIC DELAYGUE

ABSTRACT. – We develop a new method for proving algebraic independence of G-functions. Our approach rests on the following observation: G-functions do not always come with a single linear differential equation, but also sometimes with an infinite family of linear difference equations associated with the Frobenius that are obtained by reduction modulo prime ideals. When these linear difference equations have order one, the coefficients of the corresponding G-functions satisfy congruences reminiscent of a classical theorem of Lucas on binomial coefficients. We use this to derive a Kolchin-like criterion for algebraic independence. We show the relevance of this criterion by proving that many classical families of G-functions turn out to satisfy congruences "à la Lucas".

RÉSUMÉ. – Nous développons une nouvelle méthode pour démontrer l'indépendance algébrique de G-fonctions. Notre approche repose sur l'observation suivante : une G-fonction est toujours solution d'une équation différentielle linéaire mais elle est aussi parfois solution d'une infinité d'équations aux différences linéaires associées au Frobenius que l'on obtient par réduction modulo des idéaux premiers. Lorsque ces équations aux différences linéaires sont d'ordre un, les coefficients de la G-fonction correspondante satisfont des congruences rappelant un théorème classique de Lucas sur les coefficients binomiaux. Nous utilisons cette propriété pour en déduire un critère d'indépendance algébrique "à la Kolchin". Nous montrons que ce critère est pertinent en démontrant que de nombreuses familles classiques de G-fonctions satisfont des congruences "à la Lucas".

1. Introduction

This paper is the fourth of a series started by the first two authors [1, 2, 3] concerning several number theoretical problems involving linear difference equations, called Mahler's equations, as well as underlying structures associated with automata theory. We investigate here a class of analytic functions introduced by Siegel [45] in his landmark 1929 paper under the name of G-functions. Let us recall that $f(z) := \sum_{n=0}^{\infty} a(n)z^n$ is a G-function if it satisfies

This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No 648132.

doi:10.24033/asens.2392

the following conditions. Its coefficients $a(n)$ are algebraic numbers and there exists a positive real number C such that for every non-negative integer n:

(i) The absolute values of all Galois conjugates of $a(n)$ are at most C^n.

(ii) There exists a sequence of positive integers $d_n < C^n$ such that $d_n a_m$ is an algebraic integer for all m, $0 \leq m \leq n$.

(iii) The function f satisfies a linear differential equation with coefficients in $\overline{\mathbb{Q}}(z)$.

Their study leads to a remarkable interplay between number theory, algebraic geometry, combinatorics, and the study of linear differential equations (see [7, 24, 25, 33, 48]).

In this paper, we focus on the algebraic relations over $\overline{\mathbb{Q}}(z)$ that may or may not exist between G-functions. In this respect, our main aim is to develop a new method for proving algebraic independence of such functions. Our first motivation is related to transcendence theory of values of G-functions. A large part of the theory is actually devoted to the study of algebraic relations over $\overline{\mathbb{Q}}$ between periods [(1)]. Unfortunately, this essentially remains *terra incognita*. At least conjecturally, G-functions may be thought of as their functional counterpart (smooth algebraic deformations of periods). Understanding algebraic relations among G-functions thus appears to be a first step in this direction and, first of all, a much more tractable problem. For instance, a conjecture of Kontsevich [32] (see also [33]) claims that any algebraic relation between periods can be derived from the three fundamental operations associated with integration: additivity, change of variables, and Stokes' formula. It is considered completely out of reach by specialists, but recently Ayoub [10] proved a functional version of the conjecture (see also [9]). Despite the depth of this result, it does not help that much in deciding whether given G-functions are or are not algebraically independent.

A second motivation finds its source in enumerative combinatorics. Indeed, most generating series that have been studied so far by combinatorists turn out to be G-functions. To some extent, the nature of a generating series reflects the underlying structure of the objects it counts (see [13]). By nature, we mean for instance whether the generating series is rational, algebraic, or D-finite. In the same line, algebraic independence of generating series can be considered as a reasonable way to measure how distinct families of combinatorial objects may be (un)related. Though combinatorists have a long tradition of proving transcendence of generating functions, it seems that algebraic independence has never been studied so far in this setting.

Our approach rests on the following observation: a G-function often comes with not just a single linear differential equation, but also sometimes with an infinite family of linear difference equations obtained by reduction modulo prime ideals. Let us formalize this claim somewhat. Let K be a number field, $f(z) := \sum_{n=0}^{\infty} a(n) z^n$ be a G-function in $K[[z]]$, and let us denote by $\mathcal{O}_K$ the ring of integers of K. For prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ such that all coefficients

(1) A period is a complex number whose real and imaginary parts are values of absolutely convergent integrals of rational fractions over domains of $\mathbb{R}^n$ defined by polynomial inequalities with rational coefficients. Most complex numbers of interest to arithmeticians turn out to be periods.

of f belong to the localization of $\mathcal{O}_K$ at $\mathfrak{p}$, it makes sense to consider the reduction of f modulo $\mathfrak{p}$:

$$f|_{\mathfrak{p}}(z) := \sum_{n=0}^{\infty} \big(a(n) \bmod \mathfrak{p}\big) z^n \in (\mathcal{O}_K/\mathfrak{p})[[z]].$$

When $\mathfrak{p}$ is above the prime p, the residue field $\mathcal{O}_K/\mathfrak{p}$ is a finite field of characteristic p, and the linear difference equations mentioned above are of the form:

$$a_0(z) f|_{\mathfrak{p}}(z) + a_1(z) f|_{\mathfrak{p}}(z^p) + \cdots + a_d(z) f|_{\mathfrak{p}}(z^{p^d}) = 0\,, \tag{1.1}$$

where $a_i(z)$ belong to $(\mathcal{O}_K/\mathfrak{p})(z)$. That is, a linear difference equation associated with the Frobenius endomorphism $\sigma_p : z \mapsto z^p$. Note that $f|_{\mathfrak{p}}$ satisfies an equation of the form (1.1) if, and only if, it is algebraic over $(\mathcal{O}_K/\mathfrak{p})(z)$. A theorem of Furstenberg [29] and Deligne [23] shows that this holds true for all diagonals of multivariate algebraic power series and almost every prime ideal [(2)]. Furthermore, classical conjectures of Bombieri and Dwork would imply that this should also be the case for all globally bounded G-functions (see [16]). Note that even when a G-function is not globally bounded, but can still be reduced modulo $\mathfrak{p}$ for infinitely many prime ideals $\mathfrak{p}$, a similar situation may be expected. For instance, let us consider the hypergeometric function

$${}_2F_1\left[\begin{matrix}1/2, 1/2\\ 2/3\end{matrix}; z\right] = \sum_{n=0}^{\infty} \frac{(1/2)_n^2}{(2/3)_n n!} z^n,$$

where $(x)_n := x(x+1)\cdots(x+n-1)$ if $n \geq 1$ and $(x)_0 := 1$ denote the Pochhammer symbol. It is not globally bounded but satisfies a relation of the form (1.1) for all prime numbers congruent to 1 modulo 6 (see Section 8.2).

In this paper, we focus on a case of specific interest, that is when $f|_{\mathfrak{p}}$ satisfies a linear difference equation of order one with respect to a power of the Frobenius. Then one obtains a simpler equation of the form:

$$f|_{\mathfrak{p}}(z) = a(z) f|_{\mathfrak{p}}(z^{p^k})\,, \tag{1.2}$$

for some positive integer k and some rational fraction $a(z)$ in $(\mathcal{O}_K/\mathfrak{p})(z)$. As explained in Section 4, these equations lead to congruences for the coefficients of f that are reminiscent to a classical theorem of Lucas [36] on binomial coefficients and the so-called p-Lucas congruences. Let us introduce the following set of power series that will play a key role in the sequel of this paper.

Definition 1.1. – Let R be a Dedekind domain and K be its field of fractions. Let $\mathcal{S}$ be a set of non-zero prime ideals of R and let us denote by $R_{\mathfrak{p}}$ the localization of R at a non-zero prime ideal $\mathfrak{p}$. Let d be a positive integer and $\mathbf{x} = (x_1, \ldots, x_d)$ be a vector of indeterminates. We let $\mathcal{T}_d(R, \mathcal{S})$ denote the set of all power series $f(\mathbf{x})$ in $K[[\mathbf{x}]]$ with constant term equal to 1 and such that for every $\mathfrak{p}$ in $\mathcal{S}$:

(i) $f(\mathbf{x}) \in R_{\mathfrak{p}}[[\mathbf{x}]]$;

(ii) the residue field $R/\mathfrak{p}$ is finite (and its characteristic is denoted by p);

(2) Diagonals of algebraic power series form a distinguished class of G-functions (see for instance [2, 14, 15]).