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

by

B. Adamczewski, Jason P. Bell & E. 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".

Contents

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 [**48**] in his landmark 1929 paper under

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.

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 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 [**9, 26, 27, 36, 52**]).

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 (*). 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 [**35**] (see also [**36**]) 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 [**7**]). 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 [**12**]). 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 of f belong to the localization of $\mathcal{O}_K$ at $\mathfrak{p}$, it makes sense to consider the reduction of f modulo $\mathfrak{p}$:

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

*. 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.

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 [**31**] and Deligne [**23**] shows that this holds true for all diagonals of multivariate algebraic power series and almost every prime ideal (*). 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

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

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 [**39**] 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 $\mathcal{L}_d(R, \mathcal{S})$ 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);

(iii) There exist a positive integer k and a rational fraction $A_{\mathfrak{p}}$ in $K(\mathbf{x}) \cap R_{\mathfrak{p}}[[\mathbf{x}]]$ satisfying

$$f(\mathbf{x}) \equiv A_{\mathfrak{p}}(\mathbf{x}) f\left(\mathbf{x}^{p^k}\right) \mod \mathfrak{p}R_{\mathfrak{p}}[[\mathbf{x}]];$$

(iv) The height (*) of the rational fraction $A_{\mathfrak{p}}$ satisfies $H(A_{\mathfrak{p}}) \leq Cp^k$ for some constant C that does not depend on $\mathfrak{p}$.

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

*. Written $A_{\mathfrak{p}}(\mathbf{x}) = P(\mathbf{x})/Q(\mathbf{x})$ with P and Q two coprime polynomials, then $H(A_{\mathfrak{p}})$ is just the maximum of the total degree of P and Q.

Remark 1.2. — In the rest of the paper, we will omit the dependence on $\mathfrak{p}$ when considering the rational fraction $A_{\mathfrak{p}}$ of Definition 1.1, which we will thus denote by A.

We will prove the following criterion for algebraic independence. It shows that any set of algebraically dependent power series that belong to $\mathcal{L}_d(R, \mathcal{S})$, for some infinite set of non-zero prime ideals $\mathcal{S}$, should in fact satisfy a very special type of relation: a Laurent monomial is equal to a rational fraction. This kind of result is usually attached to the name of Kolchin.

Theorem 1.3. — *Let R be a Dedekind domain and $f_1(\mathbf{x}), \ldots, f_n(\mathbf{x})$ be power series in $\mathcal{L}_d(R, \mathcal{S})$ where $\mathcal{S}$ is an infinite set of non-zero prime ideals of R. Let K be the fraction field of R. Then the power series $f_1(\mathbf{x}), \ldots, f_n(\mathbf{x})$ are algebraically dependent over $K(\mathbf{x})$ if and only if there exist $a_1, \ldots, a_n \in \mathbb{Z}$ not all zero, such that*

$$f_1(\mathbf{x})^{a_1} \cdots f_n(\mathbf{x})^{a_n} \in K(\mathbf{x}). \tag{1.3}$$

Given a number field K, $\mathcal{O}_K$ its ring of integers, and $f_1(z), \ldots, f_n(z)$ some G-functions which belong to $\mathcal{L}_1(\mathcal{O}_K, \mathcal{S})$ for some infinite set of non-zero prime ideals, we stress that it is often possible to apply asymptotic techniques and analysis of singularities, as described in Section 7, to easily deduce a contradiction from (1.3) and finally prove that $f_1(z), \ldots, f_n(z)$ are algebraically independent over $\mathbb{C}(z)$.

Remark 1.4. — Since G-functions do satisfy linear differential equations, differential Galois theory provides a natural framework to look at these questions. For instance, it leads to strong results concerning hypergeometric functions [**11**]. However, the major drawback of this approach is that things become increasingly tricky when working with differential equations of higher orders. Given some G-functions $f_1(z), \ldots, f_n(z)$, it may be non-trivial to determine the differential Galois group associated with a differential operator annihilating these functions. The method developed in this paper follows a totally different road. An important feature is that, contrary to what would happen using differential Galois theory, we do not have to care about the derivatives of the functions $f_1(z), \ldots, f_n(z)$. It is also worth mentioning that in order to apply Theorem 1.3, we do not even need that the functions $f_1(z), \ldots, f_n(z)$ satisfy linear differential equations. We only need properties about their reduction modulo prime ideals. However, we only focus in this paper on applications of our method to G-functions.

At first glance, it may seem somewhat miraculous that a G-function could satisfy congruences of type (1.2) for infinitely many prime ideals. Surprisingly enough, we will show that this situation occurs remarkably often. For instance, motivated by the search of differential operators associated with particular families of Calabi-Yau varieties, Almkvist *et al.* [**6**] gave a list of more than 400 differential operators selected as potential candidates. They all have a unique solution analytic at the origin and it turns out that more than fifty percent of these analytic solutions do satisfy Lucas-type congruences (see the discussion in Section 8.5). More concretely, let us recall that a sequence $(a(n))_{n\geq 0}$ of integers satisfies the so-called p-Lucas property for some prime number p if

$$a(n) \equiv a(n_0)a(n_1)\cdots a(n_r) \bmod p\,,$$

where $n = n_0 + n_1 p + \cdots + n_r p^r$ denotes the base-p expansion of n. Another interesting example is due to Samol and van Straten [**46**]. Consider a Laurent polynomial

$$\Lambda(\mathbf{x}) = \sum_{i=1}^{k} \alpha_i \mathbf{x}^{\mathbf{a}_i} \in \mathbb{Z}[x_1^{\pm}, \ldots, x_d^{\pm}],$$

where $\mathbf{a}_i \in \mathbb{Z}^d$ and $\alpha_i \neq 0$ for i in $\{1, \ldots, k\}$. Then the Newton polyhedron of Λ is the convex hull of $\{\mathbf{a}_1, \ldots, \mathbf{a}_k\}$ in $\mathbb{R}^d$. In [**46**], it is proved that if $\Lambda(\mathbf{x})$ is a Laurent polynomial in $\mathbb{Z}[x_1^{\pm}, \ldots, x_d^{\pm}]$ such that the origin is the only interior integral point of the Newton polyhedron of Λ, then the sequence of the constant terms of its powers $([\Lambda(\mathbf{x})^n]_{\mathbf{0}})_{n\geq 0}$ has the p-Lucas property for all primes p. More generally, there is a long tradition (and a corresponding extensive literature) in proving that some sequences of natural numbers satisfy the p-Lucas property or some related congruences. Most classical sequences which are known to enjoy the p-Lucas property turn out to be multisums of products of binomial coefficients such as, for example, the Apéry numbers

$$\sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k} \quad \text{and} \quad \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2.$$

Other classical examples are ratios of factorials such as

$$\frac{(3n)!}{n!^3} \quad \text{and} \quad \frac{(10n)!}{(5n)!(3n)!n!^2}\,.$$

However, the known proofs are quite different and strongly depend on the particular forms of the binomial coefficients and of the number of sums involved in those sequences. We note that some attempts to obtain more systematic results can be found in [**41**] and more recently in [**40**]. We also refer the reader to [**43**] for a recent survey, including many references, about p-Lucas congruences. In Section 8, we provide a way to unify many proofs, as well as to obtain a lot of new examples. We describe p-adic properties of multivariate factorial ratio. Using specializations of their generating series, we are able to prove that a large variety of classical families of G-functions actually satisfy such congruences. This includes families of generating series associated with multisums of products of binomial coefficients, as well as more exotic examples such as

$$\sum_{n=0}^{\infty} \sum_{\substack{k=0 \\ k\equiv n \bmod 2}}^{\lfloor n/3 \rfloor} 2^k 3^{\frac{n-3k}{2}} \binom{n}{k} \binom{n-k}{\frac{n-k}{2}} \binom{\frac{n-k}{2}}{k} z^n\,.$$

We also give in Section 8 a simple criterion for generalized hypergeometric series to satisfy p-Lucas congruences.

To give a flavor of the kind of results we can obtain, we just add the following two examples. They correspond respectively to Theorems 9.8 and 9.9 proved in the sequel. The first one concerns several families of generating series associated with Apéry numbers, Franel numbers, and some of their generalizations. The second one involves a mix of hypergeometric series and generating series associated with factorial ratios and Apéry numbers.

Theorem 1.5. — *Let $\mathcal{F}$ be the set formed by the union of the three following sets:*

$$\left\{\sum_{n=0}^{\infty}\sum_{k=0}^{n} \binom{n}{k}^r z^n \,:\, r\geq 3\right\}, \quad \left\{\sum_{n=0}^{\infty}\sum_{k=0}^{n} \binom{n}{k}^r \binom{n+k}{k}^r z^n \,:\, r\geq 2\right\}$$

and

$$\left\{\sum_{n=0}^{\infty}\sum_{k=0}^{n} \binom{n}{k}^{2r} \binom{n+k}{k}^r z^n \,:\, r\geq 1\right\}.$$

Then all elements of $\mathcal{F}$ are algebraically independent over $\mathbb{C}(z)$.

Observe that the restriction made on the parameter r in each case is optimal since the functions

$$\sum_{n=0}^{\infty}\sum_{k=0}^{n}\binom{n}{k}z^n = \frac{1}{1-2z}, \quad \sum_{n=0}^{\infty}\sum_{k=0}^{n}\binom{n}{k}^2 z^n = \frac{1}{\sqrt{1-4z}}$$

and

$$\sum_{n=0}^{\infty}\sum_{k=0}^{n}\binom{n}{k}\binom{n+k}{k}z^n = \frac{1}{\sqrt{1-6z+z^2}}$$

are all algebraic over $\mathbb{Q}(z)$.

Theorem 1.6. — *The functions*

$$f(z) := \sum_{n=0}^{\infty}\frac{(4n)!}{(2n)!n!^2}z^n, \; g(z) := \sum_{n=0}^{\infty}\sum_{k=0}^{n}\binom{n}{k}^2\binom{n+k}{k}^2 z^n, \; h(z) := \sum_{n=0}^{\infty}\frac{(1/6)_n(1/2)_n}{(2/3)_n n!}z^n$$

and

$$i(z) := \sum_{n=0}^{\infty}\frac{(1/5)_n^3}{(2/7)_n n!^2}z^n$$

are algebraically independent over $\mathbb{C}(z)$.

2. A first example

The present work was initiated with the following concrete example. Given a positive integer r, the function

$$\mathfrak{f}_r(z) := \sum_{n=0}^{\infty}\binom{2n}{n}^r z^n$$

is a G-function annihilated by the differential operator

$$\mathcal{L}_r := \theta^r - 4^r z(\theta+1/2)^r\,,$$

where $\theta = z\frac{d}{dz}$. In 1980, Stanley [**50**] conjectured that the $\mathfrak{f}_r$'s are transcendental over $\mathbb{C}(z)$ unless for $r=1$, in which case we have $\mathfrak{f}_1(z) = (\sqrt{1-4z})^{-1}$. He also proved the transcendence in the case where r is even. The conjecture was solved independently by Flajolet [**29**] and by Sharif and Woodcock [**49**] with totally different methods. Incidentally, this result is also a consequence of work of Beukers and Heckman [**11**] concerning generalized hypergeometric series. Let us briefly describe these different proofs. We assume in the sequel that $r>1$.

(i) The proof of Flajolet is based on asymptotics. Indeed, it is known that for an algebraic function $f(z) = \sum_{n=0}^{\infty} a(n)z^n \in \mathbb{Q}[[z]]$, one has:

$$a(n) = \frac{\alpha^n n^s}{\Gamma(s+1)}\sum_{i=0}^{m} C_i\omega_i^n + \underset{n\to\infty}{O}(\alpha^n n^t),$$

where $s \in \mathbb{Q}\setminus\mathbb{Z}_{<0}$, $t<s$, α is an algebraic number and the C_i's and ω_i's are algebraic with $|\omega_i| = 1$. On the other hand, Stirling formula leads to the following asymptotics

$$\binom{2n}{n}^r \underset{n\to\infty}{\sim} \frac{2^{(2n+1/2)r}}{(2\pi n)^{r/2}}\,.$$

A simple comparison between these two asymptotics shows that $\mathfrak{f}_r$ cannot be algebraic when r is even, as already observed by Stanley in [**50**]. Flajolet [**29**] shows that it also leads to the same conclusion for odd r, but then it requires the transcendence of π.

(ii) The proof of Sharif and Woodcock is based on the Lucas theorem previously mentioned. Indeed, Lucas' theorem on binomial coefficients implies that

$$\binom{2(np+m)}{np+m}^r \equiv \binom{2n}{n}^r \binom{2m}{m}^r \bmod p$$

for all prime numbers p, all non-negative integers n and all m, $0 \leq m \leq p-1$. This leads to the algebraic equation:

$$\mathfrak{f}_{r|p}(z) = A_p(z)\mathfrak{f}_{r|p}(z)^p$$

where $A_p(z) := \sum_{n=0}^{p-1} \left(\binom{2n}{n} \bmod p\right) z^n$. In [**49**], Sharif and Woodcock prove that the degree of algebraicity of $\mathfrak{f}_{r|p}$ cannot remain bounded when p runs along the primes, which ensures the transcendence of $\mathfrak{f}_r$.

(iii) The proof based on the work of Beukers and Heckman used the fact that

$$\mathfrak{f}_r(z) = {}_{r+1}F_r \left[\begin{array}{c} 1/2, \ldots, 1/2 \\ 1, \ldots, 1 \end{array} ; 2^{2r} z \right]$$

is a hypergeometric function. Then it is easy to see that $\mathfrak{f}_r$ fails the beautiful interlacing criterion proved in [**11**]. In consequence, the differential Galois groups associated with the $\mathfrak{f}_r$'s are all infinite and these functions are thus transcendental.

Though there are three different ways to obtain the transcendence of $\mathfrak{f}_r$, not much was apparently known about their algebraic independence. In this line, we will complete in Section 7 the result of [**2**], proving that the functions $\mathfrak{f}_r$ are all algebraically independent.

Theorem 2.1. — *All elements of the set $\mathcal{F} := \{f_r(z) \,:\, r \geq 2\}$ are algebraically independent over $\mathbb{C}(z)$.*

Roughly, our approach can be summed up by saying that (ii) + (i) leads to algebraic independence in a rather straightforward manner, while differential Galois theory (that is, (iii)) would be the more usual method. Let us illustrate this claim by proving Theorem 2.1.

Proof. — Let us assume by contradiction that for some integer $n \geq 2$ the functions $\mathfrak{f}_2, \mathfrak{f}_3, \ldots, \mathfrak{f}_n$ are algebraically dependent over $\mathbb{C}(z)$ or equivalently over $\mathbb{Q}(z)$ (*). By (ii), we first get that each function $\mathfrak{f}_i$ belongs to the set $\mathcal{L}_1(\mathbb{Z}, \mathcal{P})$, where $\mathcal{P}$ denotes the set of prime numbers (identified here with the set of prime ideals of $\mathbb{Z}$). By Theorem 1.3, there thus exist $a_2, \ldots, a_n \in \mathbb{Z}$ not all zero, such that

$$\mathfrak{f}_2(z)^{a_2} \cdots \mathfrak{f}_n(z)^{a_n} = r(z)\,,$$

for some rational function in $\mathbb{Q}(z)$. Let s be the largest index such that $a_s \neq 0$. We obtain that

$$\mathfrak{f}_s(z)^{a_s} = r(z)\mathfrak{f}_2(z)^{-a_2} \cdots \mathfrak{f}_{s-1}(z)^{-a_{s-1}}\,. \tag{2.1}$$

We can assume that a_s is positive since otherwise we could write

$$\mathfrak{f}_s(z)^{-a_s} = r(z)^{-1}\mathfrak{f}_2(z)^{a_2} \cdots \mathfrak{f}_{s-1}(z)^{a_{s-1}}\,.$$

*. See Lemma 7.2

We infer now from the asymptotics given in (i) that the radius of convergence of $\mathfrak{f}_i$ is equal to 2^{-2i}, so that the the right-hand side is clearly meromorphic in a neighborhood of $z_0 := 2^{-2s}$. On the other hand, Pringsheim's theorem implies that $\mathfrak{f}_s^{a_s}$ has a singularity at z_0, but the same asymptotics show that it cannot be a pole. Hence we have a contradiction. □

3. Notation

Let us introduce some notation that will be used throughout this paper. We denote by $\mathbb{N}$ the set of non-negative integers $\{0, 1, 2, \ldots\}$. Let d be a positive integer. Given d-tuples of real numbers $\mathbf{m} = (m_1, \ldots, m_d)$ and $\mathbf{n} = (n_1, \ldots, n_d)$, we set $\mathbf{m}+\mathbf{n} := (m_1+n_1, \ldots, m_d+n_d)$ and $\mathbf{m}\cdot\mathbf{n} := m_1n_1+\cdots+m_dn_d$. If moreover λ is a real number, then we set $\lambda\mathbf{m} := (\lambda m_1, \ldots, \lambda m_d)$. We write $\mathbf{m} \geq \mathbf{n}$ if we have $m_k \geq n_k$ for all k in $\{1, \ldots, d\}$. We also set $\mathbf{0} := (0, \ldots, 0)$ and $\mathbf{1} := (1, \ldots, 1)$. We let $\mathcal{P}$ denote the set of all prime numbers.

3.0.1. *Polynomials.* — Given a d-tuple of natural numbers $\mathbf{n} = (n_1, \ldots, n_d)$ and a vector of indeterminates $\mathbf{x} = (x_1, \ldots, x_d)$, we will denote by $\mathbf{x}^{\mathbf{n}}$ the monomial $x_1^{n_1} \cdots x_d^{n_d}$. The (total) degree of such a monomial is the non-negative integer $n_1 + \cdots + n_d$. Given a ring R and a polynomial P in $R[\mathbf{x}]$, we denote by $\deg P$ the (total) degree of P, that is the maximum of the total degrees of the monomials appearing in P with non-zero coefficient. The partial degree of P with respect to the indeterminate x_i is denoted by $\deg_{x_i}(P)$. Given a polynomial $P(Y)$ in $R[\mathbf{x}][Y]$, we define the height of P as the maximum of the total degrees (in $\mathbf{x}$) of its coefficients.

3.0.2. *Algebraic functions.* — Let K be a field. We denote by $K[[\mathbf{x}]]$ the ring of formal power series with coefficients in K and associated with the vector of indeterminates $\mathbf{x}$. We denote by $K[[\mathbf{x}]]^\times$ the group of units of $K[[\mathbf{x}]]$, that is the subset of $K[[\mathbf{x}]]$ formed by all power series with non-zero constant coefficients. We say that a power series

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

is algebraic if it is algebraic over the field of rational functions $K(\mathbf{x})$, that is, if there exist polynomials $A_0, \ldots, A_m$ in $K[\mathbf{x}]$, not all zero, such that

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

Otherwise, f is said to be transcendental. The degree of an algebraic power series f, denoted by $\deg f$, is defined as the degree of the minimal polynomial of f, or equivalently, as the minimum of the natural numbers m for which such a relation holds. The (naive) height of f, denoted by $H(f)$, is then defined as the height of the minimal polynomial of f, or equivalently, as the minimum of the heights of the non-zero polynomials $P(Y)$ in $K[\mathbf{x}][Y]$ that vanish at f. For a rational function f, written as $A(\mathbf{x})/B(\mathbf{x})$ with A and B two coprime polynomials, then one has $H(f) = \max(\deg A, \deg B)$. Note that we just introduced two different notions: the degree of a polynomial and the degree of an algebraic function. Since polynomials are also algebraic functions we have to be careful. For instance, the polynomial x^2y^3 in $K[x, y]$ has degree 5 but viewed as an element of $K[[x, y]]$ it is an algebraic power series of degree 1. In the sequel, this should not be a source of confusion.

3.0.3. *Algebraic independence.* — Let $f_1, \dots, f_n$ be in $K[[\mathbf{x}]]$. We say that $f_1, \dots, f_n$ are algebraically dependent if they are algebraically dependent over the field $K(\mathbf{x})$, that is, if there exists a non-zero polynomial $P(Y_1, \dots, Y_n)$ in $K[\mathbf{x}][Y_1, \dots, Y_n]$ such that $P(f_1, \dots, f_n) = 0$. This is also equivalent to declaring that the field extension $K(\mathbf{x})(f_1, \dots, f_n)$ of $K(\mathbf{x})$ has transcendence degree less than n. When the degree of such a polynomial P (here, the total degree with respect to $Y_1, \dots, Y_n$) is at most d, then we say that $f_1, \dots, f_n$ satisfy a polynomial (or an algebraic) relation of degree at most d. When there is no algebraic relation between them, the power series $f_1, \dots, f_n$ are said to be algebraically independent (over $K(\mathbf{x})$). A set of power series is said to be algebraically independent if all finite subsets of S consist of algebraically independent elements.

3.0.4. *Dedekind domains.* — We recall here some basic facts about Dedekind domains (see for instance [**47**]). Let R be a Dedekind domain; that is, R is Noetherian, integrally closed, and every non-zero prime ideal of R is a maximal ideal. Let K denote the field of fractions of R. The localization of R at a non-zero prime ideal $\mathfrak{p}$ is denoted by $R_\mathfrak{p}$. Recall here that $R_\mathfrak{p}$ can be seen as the following subset of K:

$$R_\mathfrak{p} = \{a/b \,:\, a \in R, b \in R \setminus \mathfrak{p}\}\,.$$

Then $R_\mathfrak{p}$ is a discrete valuation ring and the residue field $R_\mathfrak{p}/\mathfrak{p}$ is equal to $R/\mathfrak{p}$. Furthermore, any non-zero element of R belongs to at most a finite number of non-zero prime ideals of R. In other words, given an infinite set $\mathcal{S}$ of non-zero prime ideals of R, then one always has $\bigcap_{\mathfrak{p}\in\mathcal{S}} \mathfrak{p} = \{0\}$. This property implies that any non-zero element of K belongs to $R_\mathfrak{p}$ for all but finitely many non-zero prime ideal $\mathfrak{p}$ of R. Furthermore, we also have $\bigcap_{\mathfrak{p}\in\mathcal{S}} \mathfrak{p}R_\mathfrak{p} = \{0\}$. For every power series $f(\mathbf{x}) = \sum_{\mathbf{n}\in\mathbb{N}^d} a(\mathbf{n})\mathbf{x}^\mathbf{n}$ with coefficients in $R_\mathfrak{p}$, we set

$$f_{|\mathfrak{p}}(\mathbf{x}) := \sum_{\mathbf{n}\in\mathbb{N}^d} \big(a(\mathbf{n}) \bmod \mathfrak{p}\big)\mathbf{x}^\mathbf{n} \in (R/\mathfrak{p})[[\mathbf{x}]]\,.$$

The power series $f_{|\mathfrak{p}}$ is called the reduction of f modulo $\mathfrak{p}$.

4. Lucas-type congruences and two special sets of power series

In this section, we introduce a special subset $\mathfrak{L}_d(R,\mathcal{S})$ of $\mathcal{L}_d(R,\mathcal{S})$ where condition (iii) is strengthened. We show that a power series belongs to this new set if, and only if, its coefficients satisfy the so-called p^k-Lucas congruences for some k. We also gather some basic properties about both sets $\mathfrak{L}_d(R,\mathcal{S})$ and $\mathcal{L}_d(R,\mathcal{S})$.

4.1. The set $\mathcal{L}_d(R,\mathcal{S})$.

— Let us first give below some remarks about the set $\mathcal{L}_d(R,\mathcal{S})$ that will be useful in the sequel of the paper.

Remark 4.1. — If $f(\mathbf{x})$ is a formal power series that belongs to $\mathcal{L}_d(R,\mathcal{S})$, then the constant coefficient $A(\mathbf{0})$ of the rational fraction A involved in (iii) must be equal to $1 \mod \mathfrak{p}$. In particular, $A(\mathbf{x})$ belongs to the group of units $R_\mathfrak{p}[[\mathbf{x}]]^\times$.

Remark 4.2. — Let $f(\mathbf{x})$ be a power series in $\mathcal{L}_d(R,\mathcal{S})$. Let $\mathfrak{p}$ be a prime in $\mathcal{S}$ such that $f(\mathbf{x}) \equiv A(\mathbf{x})f\big(\mathbf{x}^{p^k}\big) \mod \mathfrak{p}R_\mathfrak{p}[[\mathbf{x}]]$ with $H(A(\mathbf{x})) \leq Cp^k$. Iterating Congruence (iii), we observe that for all natural numbers m, we also have

$$f(\mathbf{x}) \equiv A(\mathbf{x})A\big(\mathbf{x}^{p^k}\big)\cdots A\big(\mathbf{x}^{p^{mk}}\big)f\big(\mathbf{x}^{p^{(m+1)k}}\big) \mod \mathfrak{p}R_\mathfrak{p}[[\mathbf{x}]],$$

with

$$\begin{aligned} H\big(A(\mathbf{x})A\big(\mathbf{x}^{p^k}\big)\cdots A\big(\mathbf{x}^{p^{mk}}\big)\big) &\leq Cp^k(1+p^k+\cdots+p^{km}) \\ &\leq Cp^k\frac{p^{(m+1)k}-1}{p^k-1} \\ &\leq 2Cp^{(m+1)k}. \end{aligned}$$

Remark 4.3. — In our applications, we will focus on the fundamental case where K is a number field. In that case, K is the fraction field of its ring of integers $R = \mathcal{O}_K$ which is a Dedekind domain. Furthermore, for every prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$ above a rational prime p, the residue field $\mathcal{O}_K/\mathfrak{p}$ is finite of characteristic p. In particular, we will consider the case $K = \mathbb{Q}$. In that case, we have $R = \mathcal{O}_K = \mathbb{Z}$ and, for every prime number p, the localization $\mathbb{Z}_{(p)}$ is the set of rational numbers whose denominator is not divisible by p. If there is no risk of confusion, we will simply write $\mathcal{L}_d(\mathcal{S})$ instead of $\mathcal{L}_d(\mathbb{Z},\mathcal{S})$ and $\mathcal{L}(\mathcal{S})$ instead of $\mathcal{L}_1(\mathbb{Z},\mathcal{S})$.

As we will see in the sequel, a good way to prove that some power series f belongs to $\mathcal{L}_1(R,\mathcal{S})$ is to show that f arises as some specialization of a multivariate power series known to belong to $\mathcal{L}_d(R,\mathcal{S})$. In this direction, we give the following useful result.

Proposition 4.4. — *Let R be a Dedekind domain with field of fractions K. Let d and e be two positive integers. Let f be in $\mathcal{L}_d(R,\mathcal{S})$ and g in $\mathcal{L}_e(R,\mathcal{S}')$, where S and S' are two sets of non-zero prime ideals of R. Then the following hold.*

(i) *Let $a_1,\dots,a_d$ be non-zero elements of K and $n_1,\dots,n_d$ be positive integers. Then $f(a_1x_1^{n_1},\dots,a_dx_d^{n_d})$ belongs to $\mathcal{L}_d(R,\mathcal{T})$, where $\mathcal{T}$ is the set of primes $\mathfrak{p}$ in $\mathcal{S}$ such that $a_1,\dots,a_d$ belong to $R_\mathfrak{p}$.*

(ii) *If $d\geq 2$ and x is an indeterminate, then $f(x,x,x_3,\dots,x_d)$ belongs to $\mathcal{L}_{d-1}(R,\mathcal{S})$.*

(iii) *If $\mathbf{x}$ and $\mathbf{y}$ are two vectors of indeterminates, then $f(\mathbf{x})\cdot h(\mathbf{y})$ is in $\mathcal{L}_{d+e}(R,\mathcal{S}\cap\mathcal{S}')$.*

The proof of Proposition 4.4 is a straightforward consequence of Definition 1.1 and of Remark 4.2.

4.2. The set $\mathfrak{L}_d(R,\mathcal{S})$ and p^k-Lucas congruences. — As we will see in the sequel, it often happens that elements of $\mathcal{L}_d(R,\mathcal{S})$ satisfy a stronger form of Condition (iii). Typically, the rational fraction $A(\mathbf{x})$ can just be a polynomial with even further restriction on its degree. This gives rise to stronger congruences that are of interest in combinatorics, and leads us to define the following distinguished subset of $\mathcal{L}_d(R,\mathcal{S})$.

Definition 4.5. — Let us define $\mathfrak{L}_d(R,\mathcal{S})$ as the subset of $\mathcal{L}_d(R,\mathcal{S})$ formed by the series $f(\mathbf{x})$ for which Condition (iii) is satisfied for a fixed k (*i.e.* independent of $\mathfrak{p}$) and a polynomial $A(\mathbf{x})\in R_\mathfrak{p}[\mathbf{x}]$ with $\deg_{x_i}(A(\mathbf{x}))\leq p^k-1$ for all i in $\{1,\dots,d\}$.

Again, if there is no risk of confusion, we will simply write $\mathfrak{L}_d(\mathcal{S})$ instead of $\mathfrak{L}_d(\mathbb{Z},\mathcal{S})$ and $\mathfrak{L}(\mathcal{S})$ instead of $\mathfrak{L}_1(\mathbb{Z},\mathcal{S})$.

Remark 4.6. — Let $f(\mathbf{x})\in\mathfrak{L}_d(R,\mathcal{S})$. Let $\mathfrak{p}$ be a prime ideal in $\mathcal{S}$ such that $f(\mathbf{x})\equiv A(\mathbf{x})f\big(\mathbf{x}^{p^k}\big) \mod \mathfrak{p}R_\mathfrak{p}[[\mathbf{x}]]$ where $A(\mathbf{x})$ belongs to $R_\mathfrak{p}[\mathbf{x}]$ with $\deg_{x_i}(A(\mathbf{x}))\leq p^k-1$ for all i in $\{1,\dots,d\}$. Iterating Condition (iii), we observe that for all natural numbers m, we also have

$$f(\mathbf{x})\equiv A(\mathbf{x})A\big(\mathbf{x}^{p^k}\big)\cdots A\big(\mathbf{x}^{p^{mk}}\big)f\big(\mathbf{x}^{p^{(m+1)k}}\big) \mod \mathfrak{p}R_\mathfrak{p}[[\mathbf{x}]],$$

with

$$\deg_{x_i}\left(A(\mathbf{x})A\left(\mathbf{x}^{p^k}\right)\cdots A\left(\mathbf{x}^{p^{mk}}\right)\right) \leq (p^k-1)(1+p^k+\cdots+p^{km}) \\ = p^{(m+1)k}-1.$$

We have the following practical characterization of power series in $\mathfrak{L}_d(R,\mathcal{S})$ in terms of congruences satisfied by their coefficients.

Definition 4.7. — We say that the family $(a(\mathbf{n}))_{\mathbf{n}\in\mathbb{N}^{\mathbf{d}}}$ with values in K^d satisfies the p^k-*Lucas property* with respect to $\mathcal{S}$ if for all non-zero prime ideals $\mathfrak{p}$ in $\mathcal{S}$, $(a(\mathbf{n}))_{\mathbf{n}\in\mathbb{N}^{\mathbf{d}}}$ takes values in $R_{\mathfrak{p}}$ and

$$a(\mathbf{v}+\mathbf{m}p^k) \equiv a(\mathbf{v})a(\mathbf{m}) \mod \mathfrak{p}R_{\mathfrak{p}},$$

for all $\mathbf{v}$ in $\{0,\ldots,p^k-1\}^d$ and $\mathbf{m}$ in $\mathbb{N}^d$. When $\mathcal{S}$ is the set of all non-zero prime ideals of R, then we say that $(a(\mathbf{n}))_{\mathbf{n}\in\mathbb{N}^{\mathbf{d}}}$, which takes thus values in R, satisfies the p^k-Lucas property. When $k=1$, we simply say that $(a(\mathbf{n}))_{\mathbf{n}\in\mathbb{N}^{\mathbf{d}}}$ satisfies the *p-Lucas property* (or the p-Lucas property with respect to $\mathcal{S}$).

Proposition 4.8. — *A power series $f(\mathbf{x}) := \sum_{\mathbf{n}\in\mathbb{N}^{\mathbf{d}}} a(\mathbf{n})\mathbf{x}^{\mathbf{n}}$ belongs to $\mathfrak{L}_d(R,\mathcal{S})$ if and only if there exists a positive integer k such that the family $(a(\mathbf{n}))_{\mathbf{n}\in\mathbb{N}^{\mathbf{d}}}$ satisfies $a(\mathbf{0})=\mathbf{1}$ and has the p^k-Lucas property with respect to $\mathcal{S}$.*

We will also say that a power series $f(\mathbf{x}) := \sum_{\mathbf{n}\in\mathbb{N}^{\mathbf{d}}} a(\mathbf{n})\mathbf{x}^{\mathbf{n}}$ satisfies the p^k-Lucas property with respect to $\mathcal{S}$ when the family $(a(\mathbf{n}))_{\mathbf{n}\in\mathbb{N}^{\mathbf{d}}}$ satisfies the p^k-Lucas property with respect to $\mathcal{S}$.

Proof of Proposition 4.8. — Let $f(\mathbf{x}) := \sum_{\mathbf{n}\in\mathbb{N}^{\mathbf{d}}} a(\mathbf{n})\mathbf{x}^{\mathbf{n}}$ belong to $\mathfrak{L}_d(R,\mathcal{S})$. By definition, there exists a positive integer k such that, for every $\mathfrak{p}$ in $\mathcal{S}$, one has

$$f(\mathbf{x}) \equiv A(\mathbf{x})f\left(\mathbf{x}^{p^k}\right) \mod \mathfrak{p}R_{\mathfrak{p}}[[\mathbf{x}]], \tag{4.1}$$

where $A(\mathbf{x})$ belongs to $R_{\mathfrak{p}}[\mathbf{x}]$ and $\deg_{x_i}(A(\mathbf{x})) \leq p^k-1$ for all $1\leq i\leq d$. Then we can write

$$A(\mathbf{x}) = \sum_{\mathbf{0}\leq\mathbf{v}\leq(p^k-1)\mathbf{1}} b(\mathbf{v})\mathbf{x}^{\mathbf{v}}$$

and thus

$$A(\mathbf{x})f\left(\mathbf{x}^{p^k}\right) = \sum_{\mathbf{m}\in\mathbb{N}^{\mathbf{d}}}\sum_{\mathbf{0}\leq\mathbf{v}\leq(p^k-1)\mathbf{1}} b(\mathbf{v})a(\mathbf{m})\mathbf{x}^{\mathbf{v}+\mathbf{m}\mathbf{p}^{\mathbf{k}}}.$$

The congruence satisfied by f now implies that

$$a(\mathbf{v}+\mathbf{m}p^k) \equiv b(\mathbf{v})a(\mathbf{m}) \mod \mathfrak{p}R_{\mathfrak{p}}, \tag{4.2}$$

for all $\mathbf{m}$ in $\mathbb{N}^d$ and all $\mathbf{0}\leq\mathbf{v}\leq(p^k-1)\mathbf{1}$. Choosing $\mathbf{m}=\mathbf{0}$, we obtain that $a(\mathbf{v})\equiv b(\mathbf{v})$ mod $\mathfrak{p}R_{\mathfrak{p}}$ for all $\mathbf{0}\leq\mathbf{v}\leq(p^k-1)\mathbf{1}$ because $a(\mathbf{0})=\mathbf{1}$. This shows that the family $(a(\mathbf{n}))_{\mathbf{n}\in\mathbb{N}^{\mathbf{d}}}$ satisfies the p^k-Lucas property with respect to $\mathcal{S}$.

Reciprocally, assume that $(a(\mathbf{n}))_{\mathbf{n}\in\mathbb{N}^{\mathbf{d}}}$ is a family with $a(\mathbf{0})=\mathbf{1}$ that satisfies the p^k-Lucas property with respect to $\mathcal{S}$. Then setting

$$A(\mathbf{x}) := \sum_{\mathbf{0}\leq\mathbf{v}\leq(p^k-1)\mathbf{1}} a(\mathbf{v})\mathbf{x}^{\mathbf{v}} \in R_{\mathfrak{p}}[\mathbf{x}]$$

and $f(\mathbf{x}) := \sum_{\mathbf{n}\in\mathbb{N}^{\mathbf{d}}} a(\mathbf{n})\mathbf{x}^{\mathbf{n}}$, we immediately obtain that

$$f(\mathbf{x}) \equiv A(\mathbf{x}) f\big(\mathbf{x}^{p^k}\big) \mod \mathfrak{p}R_{\mathfrak{p}}[[\mathbf{x}]],$$

which shows that f belongs to $\mathfrak{L}_d(R,\mathcal{S})$. □

Contrary to elements of $\mathcal{L}_d(R,\mathcal{S})$, those of $\mathfrak{L}_d(R,\mathcal{S})$ satisfy the following two additional useful properties. Recall that given two power series $f(\mathbf{x}) := \sum_{\mathbf{n}\in\mathbb{N}^d} a(\mathbf{n})\mathbf{x}^{\mathbf{n}}$ and $g(\mathbf{x}) = \sum_{\mathbf{n}\in\mathbb{N}^d} b(\mathbf{n})\mathbf{x}^{\mathbf{n}}$ with coefficients in an arbitrary ring, one can define the Hadamard product of f and g by

$$f \odot g := \sum_{\mathbf{n}\in\mathbb{N}^d} a(\mathbf{n})b(\mathbf{n})\mathbf{x}^{\mathbf{n}}$$

and the diagonal of f by

$$\Delta(f) := \sum_{n=0}^{\infty} a(n,\ldots,n)x^n\,.$$

Proposition 4.9. — *Let $f(\mathbf{x})$ and $g(\mathbf{x})$ belong to $\mathfrak{L}_d(R,\mathcal{S})$. Then the following hold.*
- (i) *$f \odot g \in \mathfrak{L}_d(R,\mathcal{S})$.*
- (ii) *$\Delta(f) \in \mathfrak{L}_1(R,\mathcal{S})$.*

The proof of Proposition 4.9 is straightforward using that the coefficients of f and g satisfy the p^k-Lucas property with respect to $\mathcal{S}$.

5. A criterion for algebraic independence

In this section, we prove Theorem 1.3 which is restated below as Theorem 5.1 for the convenience of the reader.

Theorem 5.1. — *Let R be a Dedekind domain and $f_1(\mathbf{x}),\ldots,f_n(\mathbf{x})$ be power series in $\mathcal{L}_d(R,\mathcal{S})$ where $\mathcal{S}$ is an infinite set of non-zero prime ideals of R. Let K be the fraction field of R. Then the power series $f_1(\mathbf{x}),\ldots,f_n(\mathbf{x})$ are algebraically dependent over $K(\mathbf{x})$ if and only if there exist $a_1,\ldots,a_n\in\mathbb{Z}$ not all zero, such that*

$$f_1(\mathbf{x})^{a_1}\cdots f_n(\mathbf{x})^{a_n} \in K(\mathbf{x}).$$

Remark 5.2. — We actually prove a slightly more precise version of Theorem 5.1: if $f_1(\mathbf{x}),\ldots,f_n(\mathbf{x})$ satisfy a polynomial relation of degree at most d over $K(\mathbf{x})$, then

$$f_1(\mathbf{x})^{a_1}\cdots f_n(\mathbf{x})^{a_n} = A(\mathbf{x})\,,$$

where $|a_1+\cdots+a_n| \leq d$, $|a_i| \leq d$ for $1 \leq i \leq n$, and $A(\mathbf{x})$ is a rational fraction of height at most $2Cdn$. Here C denotes the constant involved in Condition (iv) of Definition 1.1.

5.1. A Kolchin-like proposition. — Statements of the type of Proposition 5.3 below often appear in the study of systems of homogeneous linear differential/difference equations of order one. They are usually associated with the name of Kolchin who first proved one version in the differential case. We give here a rather general quantitative version in the case of difference equations associated with a field endomorphism. We provide the simple proof below for the sake of completeness.

Proposition 5.3. — *Let L be a field, let σ be an endomorphism of L, and let M be a subfield of L such that $\sigma(M) \subset M$. Let $f_1, \ldots, f_n$ be non-zero elements of L satisfying a non-trivial polynomial relation of degree d with coefficients in M. If there exist $a_1, \ldots, a_n$ in M such that $f_i = a_i\sigma(f_i)$ for all i in $\{1, \ldots, n\}$, then there exist $m_1, \ldots, m_n \in \mathbb{Z}$, not all zero, and $r \in M^*$ such that*

$$a_1^{m_1} \cdots a_n^{m_n} = \frac{\sigma(r)}{r}.$$

Furthermore, $|m_1 + \cdots + m_n| \leq d$, $|m_1| + \cdots + |m_n| \leq 2d$, and $|m_i| \leq d$ for $1 \leq i \leq n$.

Proof. — Let P be a polynomial with a minimal number of monomials among the non-zero polynomials in $M[X_1, \ldots, X_n]$ of degree at most d satisfying $P(f_1, \ldots, f_n) = 0$. We write

$$P(X_1, \ldots, X_n) = \sum_{(i_1,\ldots,i_n)\in I} r_{i_1,\ldots,i_n} X_1^{i_1} \cdots X_n^{i_n},$$

with $r_{i_1,\ldots,i_n}$ in $M \setminus \{0\}$. By assumption, we have

$$\begin{aligned} 0 = \sigma\big(P(f_1, \ldots, f_n)\big) &= \sum_{(i_1,\ldots,i_n)\in I} \sigma(r_{i_1,\ldots,i_n})\sigma(f_1)^{i_1} \cdots \sigma(f_n)^{i_n} \\ &= \sum_{(i_1,\ldots,i_n)\in I} \sigma(r_{i_1,\ldots,i_n}) \frac{f_1^{i_1} \cdots f_n^{i_n}}{a_1^{i_1} \cdots a_n^{i_n}}. \end{aligned} \tag{5.1}$$

Let us fix $\mathbf{i_0} = (s_1, \ldots, s_n)$ in I. We also have

$$\sigma(r_{\mathbf{i_0}})P(f_1, \ldots, f_n) = 0. \tag{5.2}$$

By multiplying (5.1) by $r_{\mathbf{i_0}} a_1^{s_1} \cdots a_n^{s_n}$ and subtracting (5.2), we obtain a new polynomial in $M[X_1, \ldots, X_n]$ of degree less than or equal to d, vanishing at $(f_1, \ldots, f_n)$, but with a smaller number of monomials, so this polynomial has to be zero. Since all the f_i's are non-zero, the cardinality of I is at least equal to 2. It follows that there exists $\mathbf{i_1} = (t_1, \ldots, t_n)$ in I, $\mathbf{i_1} \neq \mathbf{i_0}$, such that

$$r_{\mathbf{i_0}}\sigma(r_{\mathbf{i_1}})a_1^{s_1-t_1} \cdots a_n^{s_n-t_n} = \sigma(r_{\mathbf{i_0}})r_{\mathbf{i_1}},$$

which leads to

$$a_1^{s_1-t_1} \cdots a_n^{s_n-t_n} = \frac{\sigma(r_{\mathbf{i_0}})r_{\mathbf{i_1}}}{r_{\mathbf{i_0}}\sigma(r_{\mathbf{i_1}})}.$$

Hence it suffices to take $m_i = s_i - t_i$ and $r = r_{\mathbf{i_0}}/r_{\mathbf{i_1}}$. Furthermore, since P has total degree at most d, we have $|m_1 + \cdots + m_n| \leq d$, $|m_1| + \cdots + |m_n| \leq 2d$, and $|m_i| \leq d$, for $1 \leq i \leq n$. ☐

5.2. Reduction modulo prime ideals. — We can now proceed with the proof of Theorem 5.1. We first recall the following simple lemma.

Lemma 5.4. — *Let R be a Dedekind domain, K its field of fractions and $f_1, \ldots, f_n$ power series in $K[[\mathbf{x}]]$. Let $\mathcal{S}$ denote an infinite set of prime ideals of R such that $f_1, \ldots, f_n$ belong to $R_\mathfrak{p}[[\mathbf{x}]]$ for every $\mathfrak{p}$ in $\mathcal{S}$. If $f_{1|\mathfrak{p}}, \ldots, f_{n|\mathfrak{p}}$ are linearly dependent over $R/\mathfrak{p}$ for all ideals $\mathfrak{p}$ in $\mathcal{S}$, then $f_1, \ldots, f_n$ are linearly dependent over K.*

Proof. — Let $a_i(n)$ denote the n-th coefficient of the power series f_i. Let us consider

$$\begin{pmatrix} a_1(0) & a_1(1) & a_1(2) & \cdots \\ a_2(0) & a_2(1) & a_2(2) & \cdots \\ \vdots & \vdots & \vdots & \cdots \\ a_n(0) & a_n(1) & a_n(2) & \cdots \end{pmatrix},$$

the $n \times \infty$ matrix whose coefficient in position (i,j) is $a_i(j-1)$. By assumption, $f_{1|\mathfrak{p}}, \ldots, f_{n|\mathfrak{p}}$ are linearly dependent over $R/\mathfrak{p}$ for all $\mathfrak{p}$ in $\mathcal{S}$. This implies that, for such a prime ideal, every $n \times n$ minor has determinant that vanishes modulo $\mathfrak{p}$. In other words, every $n \times n$ minor has determinant that belongs to $\mathfrak{p}R_\mathfrak{p}$. Since R is a Dedekind domain, a non-zero element in K belongs to only finitely many ideals $\mathfrak{p}R_\mathfrak{p}$. Since $\mathcal{S}$ is infinite, we obtain that all $n \times n$ minors are actually equal to zero in K. This means that the set of all column vectors of our matrix generate a vector space E of dimension less than n. Hence there is a non-zero linear form on K^n which vanishes on E and we obtain a non-zero vector $(b_1, \ldots, b_n)$ in K^n such that $\sum_{i=1}^n b_i f_i = 0$. Thus $f_1, \ldots, f_n$ are linearly dependent over K. □

We can now complete the proof of Theorem 5.1.

Proof of Theorem 5.1. — Let $f_1(\mathbf{x}), \ldots, f_n(\mathbf{x})$ in $\mathcal{L}_d(R, \mathcal{S})$ be algebraically dependent over $K(\mathbf{x})$. Let $Q(\mathbf{x}, y_1, \ldots, y_n)$ be a non-zero polynomial in $R[\mathbf{x}][y_1, \ldots, y_n]$ of total degree at most d in $y_1, \ldots, y_n$ such that

$$Q\big(\mathbf{x}, f_1(\mathbf{x}), \ldots, f_n(\mathbf{x})\big) = 0.$$

With all $\mathfrak{p}$ in $\mathcal{S}$, we associate a prime number p such that the residue field $R/\mathfrak{p}$ is a finite field of characteristic p. Let $d_\mathfrak{p}$ be the degree of the field extension $R/\mathfrak{p}$ over $\mathbb{F}_p$. By Definition 1.1, for all i in $\{1, \ldots, n\}$, there exists a positive real number C_i such that, for all $\mathfrak{p}$ in $\mathcal{S}$, there are positive integers k_i and $A_i(\mathbf{x})$ in $K(\mathbf{x}) \cap R_\mathfrak{p}[[\mathbf{x}]]$ satisfying

$$f_i(\mathbf{x}) \equiv A_i(\mathbf{x}) f_i\big(\mathbf{x}^{p^{k_i}}\big) \mod \mathfrak{p}R_\mathfrak{p}[[\mathbf{x}]],$$

with $H(A_i) \leq C_i p^{k_i}$. We set $C := 2\max(C_1, \ldots, C_n)$ and $k := \mathrm{lcm}(d_\mathfrak{p}, k_1, \ldots, k_n)$. Hence by Remark 4.2, for all i in $\{1, \ldots, n\}$ and all $\mathfrak{p}$ in $\mathcal{S}$, there exists $B_i(\mathbf{x})$ in $K(\mathbf{x}) \cap R_\mathfrak{p}[[\mathbf{x}]]$ satisfying

$$f_i(\mathbf{x}) \equiv B_i(\mathbf{x}) f_i\big(\mathbf{x}^{p^k}\big) \mod \mathfrak{p}R_\mathfrak{p}[[\mathbf{x}]],$$

with $H(B_i) \leq Cp^k$.

Since Q is non-zero and R is a Dedekind domain, the coefficients of Q belong to at most finitely many prime ideals $\mathfrak{p}$ of $\mathcal{S}$. There thus exists an infinite subset $\mathcal{S}'$ of $\mathcal{S}$ such that, for every $\mathfrak{p}$ in $\mathcal{S}'$, $Q_{|\mathfrak{p}}$ is a non-zero polynomial in $(R/\mathfrak{p})[\mathbf{x}][y_1, \ldots, y_n]$ of total degree at most d in $y_1, \ldots, y_n$ that vanishes at $(f_{1|\mathfrak{p}}(\mathbf{x}), \ldots, f_{n|\mathfrak{p}}(\mathbf{x}))$. We can thus apply Proposition 5.3 to $f_{1|\mathfrak{p}}, \ldots, f_{n|\mathfrak{p}}$ with L the fraction field of $(R/\mathfrak{p})[[\mathbf{x}]]$, $M = (R/\mathfrak{p})(\mathbf{x})$, and σ the canonical extension to L of the injective endomorphism of $(R/\mathfrak{p})[[\mathbf{x}]]$ defined by

$$\sigma\big(g(\mathbf{x})\big) = g\big(\mathbf{x}^{p^k}\big) = g(\mathbf{x})^{p^k}, \ (g(\mathbf{x}) \in (R/\mathfrak{p})[[\mathbf{x}]]),$$

where the last equality holds because $d_\mathfrak{p}$ divides k. Then Proposition 5.3 implies that there exist integers $m_1, \ldots, m_s$, not all zero, and a non-zero rational fraction $r(\mathbf{x})$ in $(R/\mathfrak{p})(\mathbf{x})$ such that

$$B_{1|\mathfrak{p}}(\mathbf{x})^{m_1} \cdots B_{n|\mathfrak{p}}(\mathbf{x})^{m_n} = \frac{r\big(\mathbf{x}^{p^k}\big)}{r(\mathbf{x})} = r(\mathbf{x})^{p^k - 1}. \tag{5.3}$$

By Remark 4.1, the constant coefficient in the left-hand side of (5.3) is equal to 1. It thus follows that the constant coefficient of the power series r is non-zero. We can thus assume without any loss of generality that the constant coefficient of r is equal to 1. Furthermore, we have $|m_1 + \cdots + m_n| \leq d$ and $|m_i| \leq d$ for $1 \leq i \leq n$. Note that the rational fractions B_i, r and the integers m_i all depend on $\mathfrak{p}$. However, since all the m_i's belong to a finite set, the pigeonhole principle implies the existence of an infinite subset $\mathcal{S}''$ of $\mathcal{S}'$ and of integers $t_1, \ldots, t_n$ independent of $\mathfrak{p}$ such that, for all $\mathfrak{p}$ in $\mathcal{S}''$, we have $m_i = t_i$ for $1 \leq i \leq n$. Assume now that $\mathfrak{p}$ is a prime ideal in $\mathcal{S}''$ and write $r(\mathbf{x}) = s(\mathbf{x})/t(\mathbf{x})$ with $s(\mathbf{x})$ and $t(\mathbf{x})$ in $(R/\mathfrak{p})[\mathbf{x}]$ and coprime. Since $H(B_i) \leq Cp^k$, the degrees of $s(\mathbf{x})$ and $t(\mathbf{x})$ are bounded by

$$\frac{p^k}{p^k - 1} C\big(|t_1| + \cdots + |t_n|\big) \leq 2Cdn.$$

Set

$$h(\mathbf{x}) := f_1(\mathbf{x})^{-t_1} \cdots f_n(\mathbf{x})^{-t_n} \in K[[\mathbf{x}]].$$

Then, for every $\mathfrak{p}$ in $\mathcal{S}''$, we obtain that

$$\begin{aligned} h_{|\mathfrak{p}}\big(\mathbf{x}^{p^k}\big) &\equiv f_{1|\mathfrak{p}}\big(\mathbf{x}^{p^k}\big)^{-t_1} \cdots f_{n|\mathfrak{p}}\big(\mathbf{x}^{p^k}\big)^{-t_n} \mod \mathfrak{p}R_{\mathfrak{p}}[[\mathbf{x}]] \\ &\equiv f_{1|\mathfrak{p}}(\mathbf{x})^{-t_1} \cdots f_{n|\mathfrak{p}}(\mathbf{x})^{-t_n} B_1(\mathbf{x})^{t_1} \cdots B_n(\mathbf{x})^{t_n} \mod \mathfrak{p}R_{\mathfrak{p}}[[\mathbf{x}]] \\ &\equiv h_{|\mathfrak{p}}(\mathbf{x}) r(\mathbf{x})^{p^k - 1} \mod \mathfrak{p}R_{\mathfrak{p}}[[\mathbf{x}]]. \end{aligned}$$

Since $h_{|\mathfrak{p}}$ is not zero, we obtain that $h_{|\mathfrak{p}}(\mathbf{x})^{p^k-1} \equiv r(\mathbf{x})^{p^k-1}$ and there is a in a suitable algebraic extension of $R/\mathfrak{p}$ such that $h_{|\mathfrak{p}}(\mathbf{x}) = ar(\mathbf{x})$. But, the constant coefficients of both $h_{|\mathfrak{p}}$ and r are equal to 1, and hence $h_{|\mathfrak{p}}(\mathbf{x}) = r(\mathbf{x})$. Thus, for infinitely many prime ideals $\mathfrak{p}$, the reductions modulo $\mathfrak{p}$ of the power series in the set

$$\left\{\mathbf{x}^{\mathbf{m}} h(\mathbf{x}) : \sum_{i=1}^{d} m_i \leq 2Cdn\right\} \bigcup \left\{\mathbf{x}^{\mathbf{m}} : \sum_{i=1}^{d} m_i \leq 2Cdn\right\}$$

are linearly dependent over $R/\mathfrak{p}$. Since R is a Dedekind domain, Lemma 5.4 implies that these power series are linearly dependent over K, which means that $h(\mathbf{x})$ belong to $K(\mathbf{x})$. This ends the proof. $\square$

6. Algebraic functions in $\mathcal{L}_d(R, \mathcal{S})$ and $\mathfrak{L}_d(R, \mathcal{S})$

The aim of this section is to describe which power series among $\mathcal{L}_d(R, \mathcal{S})$ and $\mathfrak{L}_d(R, \mathcal{S})$ are algebraic over $K(\mathbf{x})$. Here, we keep the notation of Section 4, we fix a Dedekind domain R and K still denotes the fraction field of R. For every prime ideal $\mathfrak{p}$ of R with finite index [(*)], we write $d_{\mathfrak{p}}$ for the degree of the field extension $R/\mathfrak{p}$ over $\mathbb{F}_p$. As a consequence of Theorem 5.1, we deduce the following generalization of the main result of [**5**]. In their Theorem 1, Allouche, Gouyou-Beauchamps and Skordev [**5**] characterize the algebraic power series of one variable with rational coefficients that have the p-Lucas property with respect to primes in an arithmetic progression of the form $1 + s\mathbb{N}$.

Proposition 6.1. — *Let $f(\mathbf{x})$ be in $\mathcal{L}_d(R, \mathcal{S})$ for an infinite set $\mathcal{S}$. Assume that $f(\mathbf{x})$ is algebraic over $K(\mathbf{x})$ of degree less than or equal to κ. Then there exists a rational fraction $r(\mathbf{x})$ in $K(\mathbf{x})$, with $r(\mathbf{0}) = 1$, and a positive integer $a \leq \kappa$ such that $f(\mathbf{x}) = r(\mathbf{x})^{1/a}$.*

*. We recall that the term finite index simply means that $R/\mathfrak{p}$ is finite.

Reciprocally, if $f(\mathbf{x}) = r(\mathbf{x})^{1/a}$ *where* $r(\mathbf{x})$ *is in* $K(\mathbf{x})$*, with* $r(\mathbf{0}) = 1$*, and* a *is a positive integer, then* $f(\mathbf{x})$ *belongs to* $\mathcal{L}_d(R, \mathcal{S})$ *where* $\mathcal{S}$ *is the set of all prime ideals* $\mathfrak{p}$ *of* R *such that* $r(\mathbf{x}) \in R_{\mathfrak{p}}(\mathbf{x})$ *and* $R/\mathfrak{p}$ *is a finite field of characteristic in* $1 + a\mathbb{N}$*.*

Proof of Proposition 6.1. — Let us first assume that there is an infinite set $\mathcal{S}$ such that f belongs to $\mathcal{L}_d(R, \mathcal{S})$ and is algebraic. We can apply Theorem 5.1 in the case of a single function. We obtain that there exists a positive integer $a \leq \kappa$ and a rational fraction $r(\mathbf{x})$ in $K(\mathbf{x})$ such that $f(\mathbf{x})^a = r(\mathbf{x})$, and $r(\mathbf{0}) = 1$ as expected.

Conversely, assume that there is a positive integer $a \leq \kappa$ such that $f(\mathbf{x}) = r(\mathbf{x})^{1/a}$ with $r(\mathbf{x})$ in $K(\mathbf{x})$ and $r(\mathbf{0}) = 1$. Of course, f is algebraic over $K(\mathbf{x})$ with degree at most κ. Let $\mathfrak{p}$ be a prime ideal of R such that $r(\mathbf{x}) \in R_{\mathfrak{p}}(\mathbf{x})$ and $R/\mathfrak{p}$ is a finite field of characteristic p in $1 + a\mathbb{N}$. Note that there exists a natural number b such that $p = 1 + ab$, and thus we have $f(\mathbf{x})^{p-1} = f(\mathbf{x})^{ab} = r(\mathbf{x})^b$. This gives $f(\mathbf{x}) = r(\mathbf{x})^{-b} f(\mathbf{x})^p$ and thus

$$f(\mathbf{x}) = r(\mathbf{x})^{-b(1+p+\cdots+p^{d_{\mathfrak{p}}-1})} f(\mathbf{x})^{p^{d_{\mathfrak{p}}}}.$$

It follows that

$$f(\mathbf{x}) \equiv A(\mathbf{x}) f\big(\mathbf{x}^{p^{d_{\mathfrak{p}}}}\big) \mod \mathfrak{p}R_{\mathfrak{p}}[[\mathbf{x}]],$$

with $A(\mathbf{x})$ in $K(\mathbf{x}) \cap R_{\mathfrak{p}}[[\mathbf{x}]]$ and $H(A) \leq 2bp^{d_{\mathfrak{p}}-1} H(r) \leq 2H(r)p^{d_{\mathfrak{p}}}$. This shows that f and $\mathfrak{p}$ satisfy Conditions (i)–(iv) in Definition 1.1, as expected. □

We also have the following similar characterization of algebraic formal power series in $\mathfrak{L}_d(R, \mathcal{S})$.

Proposition 6.2. — *Let* $f(\mathbf{x})$ *be in* $\mathfrak{L}_d(R, \mathcal{S})$ *for an infinite set* $\mathcal{S}$*. Assume that* $f(\mathbf{x})$ *is algebraic over* $K(\mathbf{x})$ *of degree less than or equal to* κ*. Then there exists a polynomial* $P(\mathbf{x})$ *in* $K[\mathbf{x}]$*, with* $P(\mathbf{0}) = 1$*, and a positive integer* $a \leq \kappa$ *such that* $f(\mathbf{x}) = P(\mathbf{x})^{-1/a}$ *with* $\deg_{x_i}(P(\mathbf{x})) \leq a$ *for all* i *in* $\{1, \ldots, d\}$*.*

Reciprocally, if $f(\mathbf{x}) = P(\mathbf{x})^{-1/a}$ *where* $P(\mathbf{x})$ *is in* $K[\mathbf{x}]$*, with* $P(\mathbf{0}) = 1$*, and* a *is a positive integer such that* $\deg_{x_i}(P(\mathbf{x})) \leq a$ *for all* i *in* $\{1, \ldots, d\}$*, then for every prime ideal* $\mathfrak{p}$ *in* R *such that* $P(\mathbf{x})$ *is in* $R_{\mathfrak{p}}[\mathbf{x}]$ *and* $R/\mathfrak{p}$ *is a finite field of characteristic* p *in* $1 + a\mathbb{N}$*,* $f(\mathbf{x})$ *satisfies the* $p^{d_{\mathfrak{p}}}$*-Lucas property.*

Proof. — Let us first assume that there is an infinite set $\mathcal{S}$ such that f belongs to $\mathfrak{L}_d(R, \mathcal{S})$ and is algebraic. By Proposition 6.1, there are a positive integer $a \leq \kappa$ and a rational fraction $r(\mathbf{x})$ in $K(\mathbf{x})$, with $r(\mathbf{0}) = 1$, such that $f(\mathbf{x}) = r(\mathbf{x})^{1/a}$. We write $r(\mathbf{x}) = s(\mathbf{x})/t(\mathbf{x})$ with $s(\mathbf{x})$ coprime to $t(\mathbf{x})$ and $s(\mathbf{0}) = t(\mathbf{0}) = 1$. Since the resultant of $s(\mathbf{x})$ and $t(\mathbf{x})$ is a non-zero element of K, there exists an infinite subset $\mathcal{S}'$ of $\mathcal{S}$ such that $s_{|\mathfrak{p}}(\mathbf{x})$ and $t_{|\mathfrak{p}}(\mathbf{x})$ are coprime and non-zero for all prime ideals $\mathfrak{p}$ in $\mathcal{S}'$. We fix $\mathfrak{p}$ in $\mathcal{S}'$ and we let p be the characteristic of $R/\mathfrak{p}$. By assumption, there exist a positive integer k and $A(\mathbf{x})$ in $R_{\mathfrak{p}}[\mathbf{x}]$, with $\deg_{x_i}(A) \leq p^k - 1$ for all i in $\{1, \ldots, d\}$, such that

$$f(\mathbf{x}) \equiv A(\mathbf{x}) f(\mathbf{x}^{p^k}) \mod \mathfrak{p}R_{\mathfrak{p}}[[\mathbf{x}]].$$

By Remark 4.6, we can assume that $d_{\mathfrak{p}}$ divides k. This yields

$$f(\mathbf{x})^{p^k-1} \equiv A(\mathbf{x})^{-1} \mod \mathfrak{p}R_{\mathfrak{p}}[[\mathbf{x}]]$$

and

$$t(\mathbf{x})^{p^k-1} \equiv s(\mathbf{x})^{p^k-1} A(\mathbf{x})^a \mod \mathfrak{p}R_{\mathfrak{p}}[[\mathbf{x}]]\,. \tag{6.1}$$

Since $t_{|\mathfrak{p}}(\mathbf{x})$ is coprime to $s_{|\mathfrak{p}}(\mathbf{x})$ and $s(\mathbf{0}) = 1$, we deduce that $s_{|\mathfrak{p}}(\mathbf{x}) = 1$. Since $\mathcal{S}'$ is infinite, we obtain $s(\mathbf{x}) = 1$, as expected. Finally, we have $\deg_{x_i}(t) \leq a$ for all i in $\{1, \dots, d\}$. Indeed, Congruence (6.1) implies that $\deg_{x_i}(t_{|\mathfrak{p}}) \leq a$ for all i in $\{1, \dots, d\}$ and all $\mathfrak{p}$ in $\mathcal{S}'$.

Conversely, assume that $f(\mathbf{x}) = P(\mathbf{x})^{-1/a}$ where $P(\mathbf{x})$ is in $K[\mathbf{x}]$, with $P(\mathbf{0}) = 1$, and a is a positive integer such that $\deg_{x_i}(P(\mathbf{x})) \leq a$ for all i in $\{1, \dots, d\}$. Let $\mathfrak{p}$ be a prime ideal in R such that $P(\mathbf{x})$ is in $R_{\mathfrak{p}}[\mathbf{x}]$ and $R/\mathfrak{p}$ is a finite field of characteristic p in $1 + a\mathbb{N}$. Following the proof of Proposition 6.1, we obtain that

$$f(\mathbf{x}) = P(\mathbf{x})^{b(1+p+\cdots+p^{d_{\mathfrak{p}}-1})} f(\mathbf{x})^{p^{d_{\mathfrak{p}}}},$$

where b satisfies $p = 1 + ab$. It follows that

$$f(\mathbf{x}) \equiv A(\mathbf{x}) f\left(\mathbf{x}^{p^{d_{\mathfrak{p}}}}\right) \mod \mathfrak{p}R_{\mathfrak{p}}[[\mathbf{x}]],$$

with $A(\mathbf{x})$ in $R_{\mathfrak{p}}[\mathbf{x}]$ and $\deg_{x_i} A(\mathbf{x}) \leq p^{d_{\mathfrak{p}}} - 1$ as expected. $\square$

Remark 6.3. — With these first principles in hand, one can already deduce non-trivial results. As a direct consequence of Proposition 6.2 with $R = \mathbb{Z}$, we get that the bivariate power series $\frac{1}{1-x(1+y)}$ satisfies the p-Lucas property for all prime numbers p, which is equivalent to Lucas' theorem since we have

$$\frac{1}{1 - x(1+y)} = \sum_{n,k \geq 0} \binom{n}{k} x^n y^k .$$

Using Proposition 4.9 and Proposition 6.2, we also recover the following result of Rowland and Yassawi [**45**]. Given any polynomial $P(\mathbf{x})$ in $\mathbb{Q}[\mathbf{x}]$ with $P(\mathbf{0}) = 1$, then we have

$$\Delta\left(\frac{1}{P(\mathbf{x})^{1/a}}\right) \in \mathfrak{L}(\mathcal{S}),$$

for every positive integer $a \geq \max\{\deg_{x_i}(P(\mathbf{x})) \,:\, 1 \leq i \leq d\}$ and

$$\mathcal{S} = \left\{p \in \mathfrak{P} \,:\, p \equiv 1 \mod a \text{ and } P(\mathbf{x}) \in \mathbb{Z}_{(p)}[\mathbf{x}]\right\}.$$

This has interesting consequences. Choosing for instance $P(x_1, \dots, x_d) = 1 - (x_1 + \cdots + x_d)$ and $a = 1$, we deduce from Proposition 4.9 that for every positive integer t the power series $\sum_{n=0}^{\infty} \binom{dn}{n,n,\dots,n}^t x^n$ satisfies the p-Lucas property for all prime numbers p. Choosing $P(x_1, x_2, x_3, x_4) = (1 - x_1 - x_2)(1 - x_3 - x_4) - x_1x_2x_3x_4$ and $a = 1$, we recover a classical result of Gessel [**32**]: the sequence of Aprépry numbers

$$\left(\sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2\right)_{n \geq 0}$$

satisfies the p-Lucas property for all prime numbers p (*).

*. The fact that the diagonal of $1/P$ is the generating series of the Apéry numbers can be found in [**51**].

7. From asymptotics and singularity analysis to algebraic independence

In this section, we emphasize the relevance of Theorem 5.1 for proving algebraic independence by using complex analysis. We fix a Dedekind domain $R \subset \mathbb{C}$ and an infinite set $\mathcal{S}$ of non-zero prime ideals of R with finite index. We still write K for the fraction field of R. Let $f_1(\mathbf{x}), \ldots, f_n(\mathbf{x})$ be power series in $\mathcal{L}_d(R, \mathcal{S})$ algebraically dependent over $\mathbb{C}(\mathbf{x})$. By Lemma 7.2 below, those power series are algebraically dependent over $K(\mathbf{x})$. Then Theorem 5.1 yields integers $a_1, \ldots, a_n$, not all zero, and a rational fraction $r(\mathbf{x})$ in $K(\mathbf{x})$ such that

$$f_1(\mathbf{x})^{a_1} \cdots f_n(\mathbf{x})^{a_n} = r(\mathbf{x})\,. \tag{7.1}$$

We will describe in this section some basic principles that allow to reach a contradiction with (7.1) and that thus lead to the algebraic independence of the f_i's. The key feature when dealing with one-variable complex functions is that one can derive a lot of information from the study of their singularities and asymptotics for their coefficients. It is well-known that asymptotics of coefficients of analytic functions and analysis of their singularities are intimately related and there are strong transference theorems that allow to go from one to the other viewpoint. This connection is for instance described in great detail in the book of Flajolet and Sedgewick [**30**].

Remark 7.1. — If the multivariate functions $f_1(\mathbf{x}), \ldots, f_n(\mathbf{x})$ in $\mathcal{L}_d(R, \mathcal{S})$ are algebraically dependent over $K(\mathbf{x})$, then the univariate power series $f_i(\lambda_1 x^{n_1}, \ldots, \lambda_d x^{n_d})$, $1 \leq i \leq n$, where $\lambda_i \in \mathbb{C}^*$ and $n_i \geq 1$, are algebraically dependent over $K(x)$. We thus stress that the principles described in this section could also be used to prove the algebraic independence of multivariate functions.

As announced above, we recall the following classical and elementary result.

Lemma 7.2. — *Let K be a subfield of $\mathbb{C}$ and $f_1(\mathbf{x}), \ldots, f_n(\mathbf{x})$ be power series in $K[[\mathbf{x}]]$ algebraically dependent over $\mathbb{C}(\mathbf{x})$. Then those power series are algebraically dependent over $K(\mathbf{x})$.*

7.1. General principle.

— We write $\mathcal{L}(R, \mathcal{S})$ for $\mathcal{L}_1(R, \mathcal{S})$ and we let $\mathbb{C}\{z\}$ denote the set of complex functions that are analytic at the origin. For such a function $f(z)$, we denote by ρ_f its radius of convergence. We recall that when ρ_f is finite, f must have a singularity on the circle $|z| = \rho_f$.

Definition 7.3. — Let $\mathfrak{W}$ denote the set of all analytic functions $f(z)$ in $\mathbb{C}\{z\}$ whose radius of convergence is finite and for which there exists $z \in \mathbb{C}$, $|z| = \rho_f$, such that no positive integer power of f admits a meromorphic continuation to a neighborhood of z.

Proposition 7.4. — *Let $f_1(z), \ldots, f_n(z)$ be functions that belong to $\mathcal{L}(R, \mathcal{S}) \cap \mathfrak{W}$ for an infinite set $\mathcal{S}$, and such that $\rho_{f_1}, \ldots, \rho_{f_n}$ are pairwise distinct. Then $f_1(z), \ldots, f_n(z)$ are algebraically independent over $\mathbb{C}(z)$.*

Proof. — Let us assume by contradiction that $f_1, \ldots, f_n$ are algebraically dependent over $\mathbb{C}(z)$. By Lemma 7.2, they are algebraically dependent over $K(z)$. Since the f_i's belong to $\mathcal{L}(R, \mathcal{S})$, we can first apply Theorem 5.1. We obtain that there exist integers $a_1, \ldots, a_n$, not all zero, and a rational fraction $r(z)$ in $K(x)$ such that

$$f_1(z)^{a_1} \cdots f_n(z)^{a_n} = r(z)\,. \tag{7.2}$$

Thereby, it suffices to prove that (7.2) leads to a contradiction. We can assume without loss of generality that $\rho_{f_1} < \cdots < \rho_{f_n}$. Let j be the smallest index for which $a_j \neq 0$. We obtain that

$$f_j(z)^{a_j} = r(z) f_{j+1}(z)^{-a_{j+1}} \cdots f_n(z)^{-a_n} . \tag{7.3}$$

We can assume that a_j is positive since otherwise we could write

$$f_j(z)^{-a_j} = r(z)^{-1} f_{j+1}(z)^{a_{j+1}} \cdots f_n(z)^{a_n} .$$

By assumption, the function $f_j(z)$ belongs to $\mathfrak{W}$ and has thus a singularity at a point $z_0 \in \mathbb{C}$ with $|z_0| = \rho_{f_j}$ and such that $f_j^{a_j}$ has no meromorphic continuation to a neighborhood of z_0. But the right-hand side is clearly meromorphic in a neighborhood of z_0. Hence we have a contradiction. This ends the proof. $\square$

Remark 7.5. — The set $\mathfrak{W}$ contains all functions $f(z)$ in $\mathbb{C}\{z\}$ with a finite radius of convergence and whose coefficients $a(n)$ satisfy:

$$a(n) \in \mathbb{R}_{\geq 0} \quad \text{and} \quad a(n) = O\left(\frac{\rho_f^{-n}}{n}\right) .$$

Indeed, for such a function there exist positive constants C_1 and C_2 such that, for all z in $\mathbb{C}$ satisfying $\frac{\rho_f}{2} < |z| < \rho_f$, we have

$$\begin{aligned} |f(z)| &\leq |a(0)| + C_1 \sum_{n=1}^{\infty} \frac{(|z|/\rho_f)^n}{n} \\ &\leq -C_2 \log\left(1 - \frac{|z|}{\rho_f}\right) . \end{aligned}$$

By Pringsheim's theorem, f has a singularity at ρ_f. If f is not in $\mathfrak{W}$, then there exists a positive integer r such that f^r is meromorphic at ρ_f. On the other hand, the inequality above shows that f^r cannot have a pole at ρ_f. Thus f^r is analytic at ρ_f and $f^r(z)$ has a limit as z tends to ρ_f. But if this limit is non-zero, then f would be also analytic at ρ_f, a contradiction. It follows that

$$\lim_{z \to \rho_f} f(z) = 0 ,$$

but this is impossible because the coefficients of f are non-negative (and not all zero since ρ_f is finite). Hence $f(z)$ belongs to $\mathfrak{W}$.

In Proposition 7.4 and the application above, we use the fact that the radius of convergence of the involved functions are all distinct. We observe below that this condition is not necessary to apply our method.

Proposition 7.6. — *Let $f_1(z)$ and $f_2(z)$ be two transcendental functions in $\mathcal{L}(R, \mathcal{S})$ with same finite positive radius of convergence ρ. Assume that f_1 and f_2 have a singularity at a point $z_0 \in \mathbb{C}$, with $|z_0| = \rho$, such that the following hold.*

(i) *There is no (C, α) in $\mathbb{C}^* \times \mathbb{Q}$ such that $f_1(tz_0) \underset{\substack{t \to 1 \\ t \in (0,1)}}{\sim} C(t-1)^{\alpha}$.*

(ii) $\lim\limits_{\substack{t \to 1 \\ t \in (0,1)}} f_2(tz_0) = l \in \mathbb{C}^*$.

Then $f_1(z)$ and $f_2(z)$ are algebraically independent over $\mathbb{C}(z)$.

Proof. — Let us assume that f_1 and f_2 are algebraically dependent over $\mathbb{C}(z)$ and hence over $K(z)$ by Lemma 7.2. Since $f_1(z)$ and $f_2(z)$ belong to $\mathcal{L}_1(R,\mathcal{S})$, we can apply Theorem 5.1. We obtain that there exist $a_1, a_2 \in \mathbb{Z}$, not both equal to 0, and a rational function $r(z)$ such that

$$f_1(z)^{a_1} f_2(z)^{a_2} = r(z)\,. \tag{7.4}$$

Thereby, it suffices to prove that (7.4) leads to a contradiction. Note that since f_1 and f_2 are transcendental, we have $a_1 a_2 \neq 0$. Without loss of generality we can assume that $a_1 \geq 1$. Hence, we have

$$f_1(tz_0) \underset{\substack{t\to 1\\ t\in(0,1)}}{\sim} r(tz_0)^{1/a_1} \ell^{-a_2/a_1}\,,$$

which contradicts Assertion (i). This ends the proof. □

Let us give a first example of application of Proposition 7.6.

Theorem 7.7. — *The functions*

$$\sum_{n=0}^{\infty} \frac{(4n)!}{(2n)!n!^2} z^n \quad \text{and} \quad \sum_{n=0}^{\infty}\sum_{k=0}^{n} \binom{n}{k}^6 z^n$$

are algebraically independent over $\mathbb{Q}(z)$.

Proof. — Using Stirling formula, we obtain that

$$\frac{(4n)!}{(2n)!n!^2} \underset{n\to\infty}{\sim} \frac{2^{6n}}{\pi n}\,, \tag{7.5}$$

while a result of McIntosh [**42**] (stated in the proof of Theorem 9.8) gives that

$$\sum_{k=0}^{n} \binom{n}{k}^6 \underset{n\to\infty}{\sim} \frac{2^{6n}}{\sqrt{6(\pi n/2)^5}}\,. \tag{7.6}$$

By Flajolet's asymptotic for algebraic functions (see [**28**]), we know that if a power series $\sum_{n=0}^{\infty} a(n)z^n$ in $\mathbb{Q}[[z]]$ is algebraic over $\mathbb{Q}(z)$, then we have

$$a(n) \underset{n\to\infty}{\sim} \frac{\alpha^n n^s}{\Gamma(s+1)} \sum_{i=0}^{m} C_i \omega_i^n,$$

where $s \in \mathbb{Q}\setminus\mathbb{Z}_{<0}$ and α, the C_i's and the ω_i's are algebraic numbers. Since $\Gamma(-3/2)$ is a rational multiple of $\sqrt{\pi}$ and π is a transcendental number, we obtain that

$$f_1(z) := \sum_{n=0}^{\infty} \frac{(4n)!}{(2n)!n!^2} z^n \quad \text{and} \quad f_2(z) := \sum_{n=0}^{\infty}\sum_{k=0}^{n} \binom{n}{k}^6 z^n$$

are both transcendental over $\mathbb{Q}(z)$. It follows that f_1 and f_2 have the same radius of convergence $\rho = (1/2)^6$. Furthermore, (7.5) shows that f_1 does satisfy Assumption (i) of Proposition 7.6. Indeed, (7.5) shows that f_1 has a logarithmic singularity at ρ which is not compatible with an asymptotic of the form $C(z-\rho)^\alpha$. On the other hand, (7.6) shows that f_2 satisfies Assumption (ii) of Proposition 7.6. As we will prove in Section 8, f_1 and f_2 both belong to $\mathfrak{L}(\mathcal{P})$, and we can thus apply Proposition 7.6 to conclude the proof. □

7.2. Singularities of G-functions and asymptotics of their coefficients. — We are mainly interested in G-functions so we will focus on elements in sets of the form $\mathcal{L}_1(\mathcal{O}_K, \mathcal{S})$ (also denoted by $\mathcal{L}(\mathcal{O}_K, \mathcal{S})$), where $\mathcal{O}_K$ is the ring of integers of a number field K assumed to be embedded in $\mathbb{C}$. In this case, it is well-known that K is the fraction field of $\mathcal{O}_K$ which is a Dedekind domain. In this section, we briefly recall some background about the kind of singularities a G-function may have. As we will see, those are subject to severe restrictions. In particular, this explains why the same kind of asymptotics always comes up when studying the coefficients of G-functions.

Let f be a G-function and $\mathcal{L}$ be a non-zero differential operator in $\overline{\mathbb{Q}}[z, d/dz]$ of minimal order such that $\mathcal{L} \cdot f(z) = 0$. Then it is known that $\mathcal{L}$ is a Fuchsian operator, that is all its singularities are regular. Furthermore, its exponents at each singularity are rational numbers. This follows from results of Chudnovsky [**17**], Katz [**34**], and André [**8**] (see [**9**] for a discussion). In particular, these results have the following consequence. Let z_0 be a singularity of $\mathcal{L}$ at finite distance and consider a closed half-line Δ starting at z_0 and ending at infinity. Then there is a simply connected open set $U \supset \{0, z_0\}$ such that f admits an analytic continuation to $V := U \setminus \Delta$ (again denoted f) which is annihilated by $\mathcal{L}$. In an intersection W of V and a neighborhood of z_0, there exist rational numbers $\lambda_1, \ldots, \lambda_s$, natural numbers $k_1, \ldots, k_s$ and functions $f_{i,k}(z)$ in $\mathbb{C}\{z - z_0\}$ such that

$$f(z) = \sum_{i=1}^{s} \sum_{k=0}^{k_i} (z - z_0)^{\lambda_i} \log(z - z_0)^k f_{i,k}(z), \tag{7.7}$$

and where $\lambda_i - \lambda_j \in \mathbb{Z}$ implies that $\lambda_i = \lambda_j$. By grouping terms with $\lambda_i = \lambda_j$, we may assume that if $\lambda_i - \lambda_j$ is an integer, then $i = j$.

As a direct consequence of the linear independence over $\mathbb{C}\{z - z_0\}$ of the functions $(z - z_0)^{\lambda_i} \log(z - z_0)^k$ we get the following result. It shows that a G-function that does not belong to the set $\mathfrak{W}$ should have a decomposition of a very restricted form on its circle of convergence. Roughly speaking, this means that transcendental G-functions usually tend to belong to $\mathfrak{W}$.

Proposition 7.8. — *Let f be a G-function and let z_0 be a singularity of f. Then there is a positive integer m such that f^m has an analytic continuation to a neighborhood of z_0 which is meromorphic at z_0 if, and only if, in any decomposition of the form* (7.7)*, we have $s = 1$ and $k_1 = 0$, that is $f(z) = (z - z_0)^{\lambda} g(z)$ for $z \in W$, where $\lambda \in \mathbb{Q}$ and $g(z) \in \mathbb{C}\{z - z_0\}$.*

7.3. G-functions with integer coefficients. — In this section we focus on G-functions with integer coefficients. We first introduce the following set of analytic functions.

Definition 7.9. — Let $\mathfrak{G}$ denote the set of all analytic functions $f(z)$ in $\mathbb{C}\{z\}$ satisfying the following conditions.

(i) $f(z)$ satisfies a non-trivial linear differential equation with coefficients in $\mathbb{Q}[z]$.

(ii) $f(z)$ belongs to $\mathbb{Z}[[z]]$.

We observe that elements of $\mathfrak{G}$ are G-functions. The transcendental elements of $\mathfrak{G}$ have specific singularities.

Proposition 7.10. — *Every transcendental f in $\mathfrak{G}$ has a singularity $\beta \in \mathbb{C}$ with $|\beta| < 1$ such that no non-zero power of f admits a meromorphic continuation at β.*

Proof. — Let us argue by contradiction. Let f be an element of $\mathfrak{G}$ such that, for every complex numbers β with $|\beta| < 1$, there is a positive integer $n = n(\beta)$ such that f^n admits a meromorphic continuation at β. Since f is a G-function, it has only finitely many singularities and they all are at algebraic points. It implies that there exists a polynomial $P(z)$ in $\mathbb{Z}[z]$ and a positive integer N such that $g(z) := P(z)f(z)^N$ is holomorphic in the open unit disk. Hence g is a power series with integer coefficients such that $\rho_g \geq 1$. By the Pòlya-Carlson theorem, g is either a rational fraction or admits the unit circle as a natural boundary. Since g has only finitely many singularities, we obtain that g is a rational fraction and f is algebraic, which is a contradiction. ☐

We have the following generalization of Theorem 2.1 concerning algebraic independence of Hadamard powers of elements of $\mathfrak{G}$.

Theorem 7.11. — *Let $f(z) := \sum_{n=0}^{\infty} a(n)z^n$ be a transcendental function in $\mathcal{L}(\mathcal{S}) \cap \mathfrak{G}$ and such that*

$$a(n) \geq 0 \quad \textit{and} \quad a(n) = O\left(\frac{\rho_f^{-n}}{n}\right) \cdot$$

Then the functions $f_1 := f, f_2 := f \odot f, f_3 := f \odot f \odot f, \ldots$ are algebraically independent over $\mathbb{C}(z)$.

Proof. — By Proposition 7.10, the radius of convergence of $f(z)$ satisfies $0 < \rho_f < 1$. It follows that all the f_r's have distinct radii of convergence since $\rho_{f_r} = \rho_f^r$. On the other hand, Remark 7.5 implies that each f_r belongs to $\mathfrak{W}$. We can thus apply Proposition 7.4 to conclude the proof. ☐

In all previous applications of Theorem 5.1, we used some knowledge about asymptotics of coefficients and/or about the singularities of the functions involved. We give here a general result that does not require any *a priori* knowledge of this kind. It applies to any transcendental element of $\mathfrak{G}$ which satisfies some Lucas-type congruences.

Theorem 7.12. — *Let $f(z)$ be a transcendental function in $\mathcal{L}(\mathcal{S}) \cap \mathfrak{G}$. Then the following hold.*

(i) *Let $\lambda_1, \ldots, \lambda_n$ be non-zero algebraic numbers with distinct absolute values. Then the series $f(\lambda_1 z), \ldots, f(\lambda_n z)$ are algebraically independent over $\mathbb{Q}(z)$.*
(ii) *The family $\{f(z), f(z^2), f(z^3), \ldots\}$ is algebraically independent over $\mathbb{Q}(z)$.*

Proof. — Let us first prove Assertion (i). Let us denote by K the number field generated by $\lambda_1, \ldots, \lambda_n$ and set $R := \mathcal{O}_K$. Let $\mathcal{S}'$ be the set of non-zero prime ideals $\mathfrak{p}$ of R such that $\mathfrak{p} \cap \mathbb{Z} \in \mathcal{S}$, so that $f(z)$ belongs to $\mathcal{L}(R, \mathcal{S}')$.

We first note that, for all but finitely many non-zero prime ideals $\mathfrak{p}$ in $\mathcal{S}'$, the algebraic numbers $\lambda_1, \ldots, \lambda_n$ belong to $R_{\mathfrak{p}}$. We can thus replace $\mathcal{S}'$ by an infinite subset $\mathcal{S}''$ such that this holds for all non-zero prime ideals in $\mathcal{S}''$. Set $g_i(z) := f(\lambda_i z)$ for every i in $\{1, \ldots, n\}$. Taking $\mathfrak{p}$ in $\mathcal{S}''$ such that $\mathfrak{p} \cap \mathbb{Z} = (p)$, we write $d_{\mathfrak{p}}$ for the degree of the field extension $R/\mathfrak{p}$ over $\mathbb{F}_p$. Using that $f(z)$ belongs to $\mathcal{L}(\mathcal{S})$, we obtain that there exist a rational fraction $A(z)$

and a positive multiple k of $d_{\mathfrak{p}}$ such that $f(z) \equiv A(z)f(z^{p^k}) \bmod \mathfrak{p}R_{\mathfrak{p}}[[z]]$. This gives:

$$\begin{aligned} g_i(z) \equiv f(\lambda_i z) &\equiv A(\lambda_i z) f\big((\lambda_i z)^{p^k}\big) \bmod \mathfrak{p}R_{\mathfrak{p}}[[z]] \\ &\equiv A(\lambda_i z) f\big(\lambda_i z^{p^k}\big) \bmod \mathfrak{p}R_{\mathfrak{p}}[[z]] \\ &\equiv A(\lambda_i z) g_i\big(z^{p^k}\big) \bmod \mathfrak{p}R_{\mathfrak{p}}[[z]]. \end{aligned}$$

We thus have that $g_1(z), \ldots, g_n(z)$ all belong to $\mathcal{L}(R, \mathcal{S}'')$. Let us assume by contradiction that they are algebraically dependent over $K(z)$. Then Theorem 5.1 ensures the existence of integers $a_1, \ldots, a_n$, not all zero, and of a rational fraction $r(z)$ in $K(z)$ such that

$$g_1(z)^{a_1} \cdots g_n(z)^{a_n} = r(z). \tag{7.8}$$

Without any loss of generality, we can assume that $|\lambda_1| < \cdots < |\lambda_n|$. Let j be the largest index for which $a_j \neq 0$.

Let α denote the infimum of all $|\beta|$, where β ranges over all complex numbers such that, for all $n \geq 1$, $f(z)^n$ has no meromorphic continuation at β. By Proposition 7.10, we have that $0 < \alpha < 1$. We pick now a complex number β such that, for every positive integer n, $f(z)^n$ is not meromorphic at β and such that $|(\lambda_i/\lambda_j)\beta| < \alpha$ for all $i < j$. Then Equation (7.8) can be rewritten as

$$g_j(z)^{a_j} = r(z) \prod_{i=1}^{j-1} g_i(z)^{-a_i}.$$

We assume that $a_j > 0$, otherwise we would write $g_j(z)^{-a_j} = r(z)^{-1} \prod_{i=1}^{j-1} g_i(z)^{a_i}$. Our choice of β ensures, for every $i = 1, \ldots, j-1$, the existence of a positive integer n_i such that $g_i(z)^{n_i}$ is meromorphic at $z = \beta/\lambda_j$. Taking $n := \gcd(n_1, \ldots, n_{j-1})$, we obtain that $g_j(z)^{na_j}$ is meromorphic at β/λ_j. This provides a contradiction since no power of $f(z)$ is meromorphic at β. This proves Assertion (i).

A similar argument handles Assertion (ii). In that case, we have to choose j to be the smallest index for which $a_j \neq 0$ and β to be such that for every positive integer n, $f(z)^n$ is not meromorphic at β and such that $|\beta^{i/j}| < \alpha$ for all $i > j$. The rest of the proof remains unchanged. □

8. Lucas-type congruences among classical families of G-functions

In this section, we show that many classical families of G-functions do satisfy Lucas-type congruences. We first consider in Sections 8.1 and 8.2 two classical families: the generating series of factorial ratio and the generalized hypergeometric series. Then we discuss a family of generating series associated with multivariate factorial ratio denoted by $F_{e,f}(\mathbf{x})$ and already mentioned in Section 1. We give a simple criterion, proved in [**21**], which provides an efficient condition on the parameters e and f that forces $F_{e,f}(\mathbf{x})$ to belong to $\mathfrak{L}_d(\mathcal{P})$. A key idea is then that various specializations of the parameters or of the variables of functions of type $F_{e,f}$ lead us to prove that interesting families of G-functions belong to $\mathfrak{L}_1(\mathcal{P})$. This includes generating series associated with various sums and products of binomials, such as those associated with Apéry, Franel, Domb, and Delannoy numbers (see Section 8.4). In this direction, we stress that Propositions 8.8, 8.10, and 8.5 allow one to recover most examples in the literature of sequences known to satisfy p-Lucas congruences. They also provide a lot of new examples.

We mention that it is possible to prove a similar result for a general family of multivariate hypergeometric series in the spirit of the so-called A-hypergeometric series. This was done in a first version of that paper [**4**] and allows one to generalize in a same way both the multivariate factorial ratio and the generalized hypergeometric series. However, the proof involves rather technical p-adic considerations and we chose to drop it following the referee suggestion.

8.1. Generating series of factorial ratios. — Given two tuples of vectors of natural numbers, $e = (e_1, \dots, e_u)$ and $f = (f_1, \dots, f_v)$, the associated sequence of factorial ratio is defined by

$$\mathcal{Q}_{e,f}(n) := \frac{\prod_{i=1}^{u}(e_i n)!}{\prod_{i=1}^{v}(f_i n)!}\,.$$

The generating series of such a sequence is then denoted by

$$F_{e,f}(x) := \sum_{n\in\mathbb{N}} \mathcal{Q}_{e,f}(n) x^n\,.$$

In order to study when $\mathcal{Q}_{e,f}(n)$ is integer valued, Landau introduced the following simple step function $\Delta_{e,f}$ defined from $\mathbb{R}$ to $\mathbb{Z}$ by:

$$\Delta_{e,f}(x) := \sum_{i=1}^{u} \lfloor e_i x \rfloor - \sum_{j=1}^{v} \lfloor f_j x \rfloor\,.$$

According to Landau's criterion [**38**], and Bober's refinement [**13**], we have the following dichotomy.

- If, for all x in $[0, 1]$, one has $\Delta_{e,f}(x) \geq 0$, then $\mathcal{Q}_{e,f}(n) \in \mathbb{N}$, for all $n \geq 0$.
- If there exists x in $[0, 1]$ such that $\Delta_{e,f}(x) < 0$, then there are only finitely many prime numbers p such that $\mathcal{Q}_{e,f}(n)$ belongs to $\mathbb{Z}_{(p)}$ for all $n \geq 0$.

In the sequel, we always assume that the sets $\{e_1, \dots, e_u\}$ and $\{f_1, \dots, f_v\}$ are disjoint. We set $|e| := \sum_{i=1}^{u} e_i$, $|f| := \sum_{i=1}^{v} f_i$, and

$$m_{e,f} := (\max\{e_1, \dots, e_u, f_1, \dots, f_v\})^{-1}\,.$$

The following result is proved in [**21**].

Proposition 8.1. — *Let us assume that $|e| = |f|$ and that $\Delta_{e,f}(x) \geq 1$, for all real numbers x such that $m_{e,f} \leq x < 1$. Then $F_{e,f}(x) \in \mathfrak{L}_1(\mathcal{P})$. In other words, $F_{e,f}(x)$ satisfies the p-Lucas property for all prime numbers p.*

Remark 8.2. — When all the f_i's are equal to 1, it becomes obvious that $\Delta_{e,f}(x) \geq 1$, for all real numbers x such that $m_{e,f} \leq x < 1$. This shows that all generating series of the form

$$\sum_{n=0}^{\infty} \frac{\prod_{i=1}^{r}(e_i n)!}{(n!)^r} x^n\,,$$

where $e_1, \dots, e_r$ are positive integers, satisfy the p-Lucas property for all prime numbers p.

We also prove the following refinement of Proposition 8.1.

Proposition 8.3. — *The following assertions are equivalent.*

(i) *There exists an infinite set of primes $\mathcal{S}$ such that $F_{e,f}(x) \in \mathfrak{L}_1(\mathcal{S})$.*

(ii) *The sequence $\mathcal{Q}_{e,f}$ is integer-valued and has the p-Lucas property for all primes p.*

(iii) *We have $|e| = |f|$ and $\Delta_{e,f}(x) \geq 1$ for all real numbers x such that $m_{e,f} \leq x < 1$.*

Remark 8.4. — The equivalence of Assertions (ii) and (iii) is contained in [**21**, Theorem 3]. A consequence of Proposition 8.3 is that $F_{e,f}(x)$ belongs to $\mathfrak{L}_1(\mathcal{S})$ for an infinite set of primes $\mathcal{S}$ if and only if all Taylor coefficients at the origin of the associated mirror map $z_{e,f}$ are integers (see Theorems 1 and 3 in [**19**]). It would be interesting to investigate in more details this intriguing connection.

Proof of Proposition 8.3. — Obviously, Assertion (ii) implies Assertion (i), and Assertions (ii) and (iii) are shown to be equivalent in [**21**, Theorem 3]. Hence it suffices to prove that (i) implies (iii). From now on, we assume that Assertion (i) holds.

First, we prove that $|e| = |f|$. Since $\mathcal{S}$ is infinite and $F_{e,f}(x)$ belongs to $\mathbb{Z}_p[[x]]$ for every prime p in $\mathcal{S}$, Landau's criterion implies that $\Delta_{e,f}(x) \geq 0$ for all x in $[0,1]$. In particular, we obtain that $|e| - |f| = \Delta_{e,f}(1) \geq 0$. If $|e| > |f|$ then $\Delta_{e,f}(1) \geq 1$. Set $M_{e,f} := \max\{e_1, \ldots, e_u, f_1, \ldots, f_v\}$. Then, for all prime numbers $p > M_{e,f}$ and all positive integers k, we have

$$\begin{aligned} v_p\big(\mathcal{Q}_{e,f}(1+p^k)\big) &= \sum_{\ell=1}^{\infty} \Delta_{e,f}\left(\frac{1+p^k}{p^\ell}\right) \\ &\geq \Delta_{e,f}\left(1 + \frac{1}{p^k}\right) \\ &\geq 1\,. \end{aligned}$$

Our choice of p ensures that $v_p(\mathcal{Q}_{e,f}(1)) = 0$. We thus deduce that, for almost all primes p and all positive integers k, we have

$$\mathcal{Q}_{e,f}(1+p^k) \not\equiv \mathcal{Q}_{e,f}(1)\mathcal{Q}_{e,f}(1) \mod p\mathbb{Z}_{(p)}\,,$$

which provides a contradiction with Assertion (i). Hence we get that $|e| = |f|$.

Now, we prove the following identity. For all prime numbers p, all positive integers k, all a in $\{0, \ldots, p^k - 1\}$, and all natural integers n, we have

$$\frac{\mathcal{Q}_{e,f}(a+np^k)}{\mathcal{Q}_{e,f}(a)\mathcal{Q}_{e,f}(n)} \in \frac{\displaystyle\prod_{i=1}^{u} \prod_{j=1}^{\lfloor e_i a/p^k \rfloor} \left(1 + \frac{e_i}{j} n\right)}{\displaystyle\prod_{i=1}^{v} \prod_{j=1}^{\lfloor f_i a/p^k \rfloor} \left(1 + \frac{f_i}{j} n\right)} \big(1 + p\mathbb{Z}_{(p)}\big)\,. \tag{8.1}$$

Indeed, we have

$$\frac{\mathcal{Q}_{e,f}(a+np^k)}{\mathcal{Q}_{e,f}(a)\mathcal{Q}_{e,f}(n)} = \frac{\mathcal{Q}_{e,f}(a+np^k)}{\mathcal{Q}_{e,f}(a)\mathcal{Q}_{e,f}(np^k)} \prod_{j=0}^{k-1} \frac{\mathcal{Q}_{e,f}(np^{j+1})}{\mathcal{Q}_{e,f}(np^j)}\,.$$

Since $|e| = |f|$, we can apply [**20**, Lemma 7] $^{(*)}$ with $d = 1$, $\mathbf{c} = 0$, $\mathbf{m} = np^j$ and $s = 0$ which leads to

$$\frac{\mathcal{Q}_{e,f}(np^{j+1})}{\mathcal{Q}_{e,f}(np^j)} \in 1 + p\mathbb{Z}_{(p)} \,.$$

Furthermore, we have

$$\begin{aligned}
\frac{\mathcal{Q}_{e,f}(a+np^k)}{\mathcal{Q}_{e,f}(a)\mathcal{Q}_{e,f}(np^k)} &= \frac{1}{\mathcal{Q}_{e,f}(a)} \frac{\prod_{i=1}^{u}\prod_{j=1}^{e_i a}(j+e_i np^k)}{\prod_{i=1}^{v}\prod_{j=1}^{f_i a}(j+f_i np^k)} \\
&= \frac{\prod_{i=1}^{u}\prod_{j=1}^{e_i a}\left(1+\frac{e_i np^k}{j}\right)}{\prod_{i=1}^{v}\prod_{j=1}^{f_i a}\left(1+\frac{f_i np^k}{j}\right)} \\
&\in \frac{\prod_{i=1}^{u}\prod_{j=1}^{\lfloor e_i a/p^k\rfloor}\left(1+\frac{e_i n}{j}\right)}{\prod_{i=1}^{v}\prod_{j=1}^{\lfloor f_i a/p^k\rfloor}\left(1+\frac{f_i n}{j}\right)}\left(1+p\mathbb{Z}_{(p)}\right),
\end{aligned}$$

since, if p^k does not divide j, then $1 + (e_i np^k)/j$ belongs to $1 + p\mathbb{Z}_{(p)}$. This ends the proof of Equation (8.1).

Now we assume that there exists x in $[m_{e,f}, 1)$ such that $\Delta_{e,f}(x) = 0$ and we argue by contradiction.

By assumption, for all p in $\mathcal{S}$, there exists a positive integer k_p, such that, for all v in $\{0, \dots, p^{k_p} - 1\}$ and all natural integers m, we have

$$\mathcal{Q}_{e,f}(v + mp^{k_p}) \equiv \mathcal{Q}_{e,f}(v)\mathcal{Q}_{e,f}(m) \mod p\mathbb{Z}_{(p)} \,.$$

Let $\gamma_1 < \cdots < \gamma_t$ denote the abscissa of the points of discontinuity of $\Delta_{e,f}$ on $[0, 1)$. In particular, we have $\gamma_1 = m_{e,f}$. There exists i in $\{1, \dots, t-1\}$ such that $\Delta_{e,f}(x) = 0$ for all x in $[\gamma_i, \gamma_{i+1})$. For all large enough prime numbers $p \in \mathcal{S}$, we choose r_p in $\{0, \dots, p-1\}$ such that r_p/p belongs to $[\gamma_i, \gamma_{i+1})$ and we set $a_p = r_p p^{k_p - 1}$. Hence a_p/p^{k_p} belongs to $[\gamma_i, \gamma_{i+1})$. Then, by applying (8.1) in combination with [**20**, Lemma 16] (with $\mathbf{E} = e$ and $\mathbf{F} = f$), there are integers $m_1, \dots, m_i$ such that we have

$$\frac{\mathcal{Q}_{e,f}(a_p + p^{k_p})}{\mathcal{Q}_{e,f}(a_p)\mathcal{Q}_{e,f}(1)} \in \prod_{k=1}^{i}\left(1+\frac{1}{\gamma_k}\right)^{m_k}\left(1+p\mathbb{Z}_{(p)}\right)$$

and

$$\prod_{k=1}^{i}\left(1+\frac{1}{\gamma_k}\right)^{m_k} > 1 \,,$$

because $\Delta_{e,f}$ is non-negative on $[0, 1]$. For all large enough primes p in $\mathcal{S}$, we thus deduce that

$$\prod_{k=1}^{i}\left(1+\frac{1}{\gamma_k}\right)^{m_k} \notin 1 + p\mathbb{Z}_{(p)} \,.$$

---

*. The proof of this lemma uses a lemma of Lang which contains an error. Fortunately, Lemma 7 remains true. Details of this correction are presented in [**22**, Section 2.4].

Furthermore, for all large enough p in $\mathcal{S}$, we have $1/p < m_{e,f}$, and $(a_p + p^{k_p})/p^\ell < m_{e,f}$, for $\ell \geq k_p + 1$. It follows that $v_p(\mathcal{Q}_{e,f}(1)) = 0$, while

$$v_p\big(\mathcal{Q}_{e,f}(a_p)\big) = \sum_{\ell=1}^{k_p} \Delta_{e,f}\left(\left\{\frac{a_p}{p^\ell}\right\}\right) = \Delta_{e,f}\left(\frac{r_p}{p}\right) = 0\,,$$

and

$$v_p\big(\mathcal{Q}_{e,f}(a_p + p^{k_p})\big) = \sum_{\ell=1}^{k_p} \Delta_{e,f}\left(\left\{\frac{a_p + p^{k_p}}{p^\ell}\right\}\right) = \Delta_{e,f}\left(\frac{r_p}{p} + 1\right) = 0\,.$$

Hence $\mathcal{Q}_{e,f}(a_p + p^{k_p}) \not\equiv \mathcal{Q}_{e,f}(a_p)\mathcal{Q}_{e,f}(1) \mod p\mathbb{Z}_{(p)}$ which leads to a contradiction, and ends the proof of Proposition 8.3. $\square$

Let us remind to the reader that one easily obtains the graph of $\Delta_{e,f}$ on $[0,1]$ by translating a factorial ratio into hypergeometric form. We illustrate this process with the following example. We consider

$$F(x) := \sum_{n=0}^{\infty} \frac{(10n)!}{(5n)!(3n)!n!^2} x^n\,.$$

We have

$$\begin{aligned}
\frac{(10n)!}{(5n)!(3n)!n!^2} &= \frac{\prod_{k=0}^{n-1}\prod_{j=1}^{10}(10k+j)}{\prod_{k=0}^{n-1}\big(\prod_{j=1}^{5}(5k+j)\big)(3k+1)(3k+2)(3k+3)(k+1)^2} \\
&= \left(\frac{10^{10}}{5^5 3^3}\right)^n \frac{\prod_{k=0}^{n-1}\prod_{j=1}^{10}\big(k+\frac{j}{10}\big)}{\prod_{k=0}^{n-1}\big(\prod_{j=1}^{5}\big(k+\frac{j}{5}\big)\big)\big(k+\frac{1}{3}\big)\big(k+\frac{2}{3}\big)(k+1)^3} \\
&= \left(\frac{10^{10}}{5^5 3^3}\right)^n \frac{\prod_{j=1}^{10}(j/10)_n}{(1/3)_n(2/3)_n(1)_n^3\prod_{j=1}^{5}(j/5)_n} \\
&= \left(\frac{10^{10}}{5^5 3^3}\right)^n \frac{(1/10)_n(3/10)_n(1/2)_n(7/10)_n(9/10)_n}{(1/3)_n(2/3)_n(1)_n^3}\,.
\end{aligned}$$

Then we deduce that $\Delta_{e,f}$ has jumps of amplitude 1 at $1/10, 3/10, 1/2, 7/10$ and $9/10$, while the abscissa of its jumps of amplitude -1 are $1/3, 2/3$. Furthermore, $\Delta_{e,f}$ has a jump of amplitude -3 at 1. Since

$$\frac{1}{10} < \frac{3}{10} < \frac{1}{3} < \frac{1}{2} < \frac{2}{3} < \frac{7}{10} < \frac{9}{10} < 1\,,$$

we get that $\Delta_{e,f} \geq 1$ on $[1/10, 1)$ and it follows form Proposition 8.1 that the function $F(x)$ satisfies the p-Lucas property for all prime numbers. Along the same lines, one can prove for instance that the G-functions

$$\sum_{n=0}^{\infty} \frac{(5n)!(3n)!}{(2n)!^2 n!^4} x^n \quad \text{and} \quad \sum_{n=0}^{\infty} \frac{(4n)!}{(2n)!n!^2} x^n$$

also satisfy the p-Lucas property for all prime numbers.

8.2. Generalized hypergeometric series. — With two tuples $\boldsymbol{\alpha} := (\alpha_1, \dots, \alpha_r)$ and $\boldsymbol{\beta} := (\beta_1, \dots, \beta_s)$ of elements in $\mathbb{Q} \setminus \mathbb{Z}_{\leq 0}$, we can associate the generalized hypergeometric series

$$ {}_rF_s \left[\begin{array}{c} \alpha_1, \dots, \alpha_r \\ \beta_1, \dots, \beta_s \end{array} ; x \right] := \sum_{n=0}^{\infty} \frac{(\alpha_1)_n \cdots (\alpha_r)_n}{(\beta_1)_n \cdots (\beta_s)_n} \frac{x^n}{n!} \,. $$

Here, we set

$$ \mathcal{Q}_{\boldsymbol{\alpha},\boldsymbol{\beta}}(n) := \frac{(\alpha_1)_n \cdots (\alpha_r)_n}{(\beta_1)_n \cdots (\beta_s)_n} \quad \text{and} \quad F_{\boldsymbol{\alpha},\boldsymbol{\beta}}(x) := \sum_{n=0}^{\infty} \mathcal{Q}_{\boldsymbol{\alpha},\boldsymbol{\beta}}(n) x^n \,, $$

so that

$$ F_{\boldsymbol{\alpha},\boldsymbol{\beta}}(x) = {}_{r+1}F_s \left[\begin{array}{c} \alpha_1, \dots, \alpha_r, 1 \\ \beta_1, \dots, \beta_s \end{array} ; x \right] . $$

We let $d_{\boldsymbol{\alpha},\boldsymbol{\beta}}$ denote the least common multiple of the denominators of the rational numbers $\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_s$, written in lowest form. We also set $m_{\boldsymbol{\alpha},\boldsymbol{\beta}} = \min\{\alpha_i, \beta_j : 1 \leq i \leq r, 1 \leq j \leq s\}$. We define the step function $\Delta_{\boldsymbol{\alpha},\boldsymbol{\beta}}$ (or for short Δ) by:

$$ \Delta_{\boldsymbol{\alpha},\boldsymbol{\beta}}(x) = \sum_{i=1}^{r} \lfloor x - \alpha_i \rfloor - \sum_{j=1}^{s} \lfloor x - \beta_j \rfloor + r - s \,. $$

The following result corresponds to a special case of Proposition 7.1 in [**4**].

Proposition 8.5. — *Let us assume that $r = s$, that the α_i's and β_i's are in $\mathbb{Q} \cap (0, 1]$ and that $\Delta(x) \geq 1$ for all x in $[m_{\boldsymbol{\alpha},\boldsymbol{\beta}}, 1)$. Then $F_{\boldsymbol{\alpha},\boldsymbol{\beta}}(x)$ satisfies the p-Lucas property for all primes p in*

$$ \mathcal{S} := \{p \in \mathcal{P} \,:\, p \equiv 1 \mod d_{\boldsymbol{\alpha},\boldsymbol{\beta}}\} $$

In particular, $F_{\boldsymbol{\alpha},\boldsymbol{\beta}}(x)$ belongs to $\mathfrak{L}(\mathcal{S})$.

Example 8.6. — Let us illustrate Proposition 8.5 with two examples.

- We first choose $\boldsymbol{\alpha} = (1/5, 1/5)$ and $\boldsymbol{\beta} = (2/7, 1)$

$$ F_{\boldsymbol{\alpha},\boldsymbol{\beta}}(x) := \sum_{n=0}^{\infty} \frac{(1/5)_n^2}{(2/7)_n (1)_n} x^n \,. $$

For all x in $[0, 1)$, we have

$$ \Delta(x) = 2\lfloor x - 1/5 \rfloor - \lfloor x - 2/7 \rfloor + 1 $$

and $m_{\boldsymbol{\alpha},\boldsymbol{\beta}} = 1/5$. We clearly have that $\Delta(x) \geq 1$ on $[1/5, 1)$ (it takes the values 2 and 1 on this interval). Since $d_{\boldsymbol{\alpha},\boldsymbol{\beta}} = 35$, we get that for all primes $p \equiv 1 \mod 35$, $F_{\boldsymbol{\alpha},\boldsymbol{\beta}}(x)$ satisfies the p-Lucas property. This could actually be refined as in [**4**] in order to prove in addition that for all primes $p \equiv 6 \mod 35$, $F_{\boldsymbol{\alpha},\boldsymbol{\beta}}(x)$ satisfies the p^2-Lucas property. Furthermore, we stress that, according to Theorem A in [**22**] (which is a reformulation of Christol's result [**14**, Proposition 1]), the function $F_{\boldsymbol{\alpha},\boldsymbol{\beta}}$ is not globally bounded, that is there is no C in $\mathbb{Q}$ such that $F_{\boldsymbol{\alpha},\boldsymbol{\beta}}(Cx)$ belongs to $\mathbb{Z}[[x]]$. In particular, it cannot be expressed as the diagonal of a multivariate algebraic function.

- Let study another example by taking $\boldsymbol{\alpha} = (1/9, 4/9, 5/9)$ and $\boldsymbol{\beta} = (1/3, 1, 1)$. This choice of parameters was considered by Christol in [**14**]. We have $d_{\boldsymbol{\alpha},\boldsymbol{\beta}} = 9$ and

$$ \frac{1}{9} < \frac{1}{3} < \frac{4}{9} < \frac{5}{9} \,. $$

Hence $m_{\boldsymbol{\alpha},\boldsymbol{\beta}} = 1/9$ but $\Delta(1/3) = 0 < 1$, so we cannot just apply Proposition 8.5.

We end this section by observing that the condition of Proposition 8.5 is always fulfilled in the classical case where the hypergeometric differential equation associated with $F_{\boldsymbol{\alpha},\boldsymbol{\beta}}(x)$ has maximal unipotent monodromy at the origin.

Corollary 8.7. — *Let $\boldsymbol{\alpha} \in (\mathbb{Q} \cap (0,1))^r$ and $\boldsymbol{\beta} = (1, \ldots, 1) \in \mathbb{Q}^r$. Then the generalized hypergeometric series $F_{\boldsymbol{\alpha},\boldsymbol{\beta}}(x)$ belongs to $\mathfrak{L}_1(\mathcal{S})$, where $\mathcal{S}$ is the set of all primes larger than $d_{\boldsymbol{\alpha},\boldsymbol{\beta}}$.*

As suggested by the referee, this statement could also be proved in the following way.

Proof. — The generalized hypergeometric series $F_{\boldsymbol{\alpha},\boldsymbol{\beta}}(x)$ is the Hadamard product of power series of the form

$$f(x) = \sum_{n=0}^{\infty} \frac{(\alpha)_n}{n!} x^n = (1-x)^{-\alpha},$$

where α belongs to $\mathbb{Q} \cap (0,1)$. Let p be a prime number coprime to the exact denominator s of α. Then, there exists a positive integer k such that p^k is congruent to 1 modulo s, and we have

$$\begin{aligned} f(x) &= (1-x)^{(p^k-1)\alpha} f(x)^{p^k} \\ &\equiv (1-x)^{(p^k-1)\alpha} f(x^{p^k}) \mod p\mathbb{Z}_{(p)}[[x]], \end{aligned}$$

where $(1-x)^{(p^k-1)\alpha}$ is a polynomial of degree less than or equal to $p^k - 1$ because $\alpha < 1$. Hence $f(x)$ belongs to $\mathfrak{L}(\mathbb{Z}, \mathcal{S})$ where $\mathcal{S}$ is the set of all ideals (p) with p coprime to the exact denominator of α. It follows that the generalized hypergeometric series $F_{\boldsymbol{\alpha},\boldsymbol{\beta}}(x)$ belongs to $\mathfrak{L}_1(\mathcal{S})$, where $\mathcal{S}$ is the set of all primes larger than $d_{\boldsymbol{\alpha},\boldsymbol{\beta}}$. $\square$

8.3. Multivariate factorial ratios and specializations. — We consider now a class of multivariate power series which provides a higher-dimensional generalization of generating series associated with factorial ratios that we discussed in Section 8.1. Given two tuples of vectors in $\mathbb{N}^d$, $e = (\mathbf{e}_1, \ldots, \mathbf{e}_u)$ and $f = (\mathbf{f}_1, \ldots, \mathbf{f}_v)$, we write $|e| = \sum_{i=1}^{u} \mathbf{e}_i$ and, for all $\mathbf{n}$ in $\mathbb{N}^d$, we set

$$\mathcal{Q}_{e,f}(\mathbf{n}) := \frac{\prod_{i=1}^{u} (\mathbf{e}_i \cdot \mathbf{n})!}{\prod_{i=1}^{v} (\mathbf{f}_i \cdot \mathbf{n})!} \quad \text{and} \quad F_{e,f}(\mathbf{x}) := \sum_{\mathbf{n} \in \mathbb{N}^d} \mathcal{Q}_{e,f}(\mathbf{n}) \mathbf{x}^{\mathbf{n}}.$$

We consider the Landau function $\Delta_{e,f}$ defined from $\mathbb{R}^d$ to $\mathbb{Z}$ by:

$$\Delta_{e,f}(\mathbf{x}) := \sum_{i=1}^{u} \lfloor \mathbf{e}_i \cdot \mathbf{x} \rfloor - \sum_{j=1}^{v} \lfloor \mathbf{f}_j \cdot \mathbf{x} \rfloor .$$

We also recall that, as in the one-variable case, Landau's criterion [**38**], and Delaygue's refinement [**20**], give the following dichotomy.

- If, for all $\mathbf{x}$ in $[0,1]^d$, one has $\Delta_{e,f}(\mathbf{x}) \geq 0$, then $\mathcal{Q}_{e,f}(\mathbf{n})$ is an integer for all $\mathbf{n}$ in $\mathbb{N}^d$.
- If there exists $\mathbf{x}$ in $[0,1]^d$ such that $\Delta_{e,f}(\mathbf{x}) < 0$, then there are only finitely many prime numbers p such that $\mathcal{Q}_{e,f}(\mathbf{n})$ belongs to $\mathbb{Z}_{(p)}$ for all $\mathbf{n}$ in $\mathbb{N}^d$.

Set

$$\mathcal{D}_{e,f} := \left\{\mathbf{x} \in [0,1)^d \ : \ \text{there is } \mathbf{d} \text{ in } \{\mathbf{e_1}, \ldots, \mathbf{e}_u, \mathbf{f}_1, \ldots, \mathbf{f}_v\} \text{ such that } \mathbf{d} \cdot \mathbf{x} \geq 1\right\}.$$

The following result is proved in [**21**, Theorem 3].

Proposition 8.8. — *Let us assume that $|e| = |f|$ and that $\Delta_{e,f}(\mathbf{x}) \geq 1$ for all $\mathbf{x}$ in $\mathcal{D}_{e,f}$. Then $F_{e,f}(\mathbf{x})$ belongs to $\mathfrak{L}_d(\mathcal{P})$. More precisely, $F_{e,f}(\mathbf{x})$ satisfies the p-Lucas property for all primes p.*

Let us illustrate Proposition 8.8 with the following example. Set $e := ((2,1),(1,1))$ and $f := ((1,0),(1,0),(1,0),(0,1),(0,1))$. Then

$$F_{e,f}(x,y) = \sum_{(n,m)\in\mathbb{N}^2} \frac{(2n+m)!(n+m)!}{n!^3 m!^2} x^n y^m.$$

For all x_1 and x_2 in $[0,1)$, we have

$$\begin{aligned}\Delta_{e,f}(x_1,x_2) &= \lfloor 2x_1 + x_2 \rfloor + \lfloor x_1 + x_2 \rfloor - 3\lfloor x_1 \rfloor - 2\lfloor x_2 \rfloor \\ &= \lfloor 2x_1 + x_2 \rfloor + \lfloor x_1 + x_2 \rfloor.\end{aligned}$$

Clearly, we have that $\sum_{i=1}^r \mathbf{e}_i = \sum_{j=1}^s \mathbf{f}_j$. Furthermore, we have

$$\mathcal{D}_{e,f} = \left\{(x_1,x_2) \in [0,1)^2 \ : \ 2x_1 + x_2 \geq 1 \text{ or } x_1 + x_2 \geq 1\right\},$$

so that $\Delta_{e,f}(x_1,x_2) \geq 1$, for all (x_1,x_2) in $\mathcal{D}_{e,f}$. Hence we infer from Proposition 8.8 that $F_{e,f}$ satisfies the p-Lucas property for all prime numbers p.

We give below a simple case of Proposition 8.8 that turns out to be especially useful for applications.

Corollary 8.9. — *For every k in $\{1,\ldots,d\}$, let us denote by $\mathbf{1}_k$ the vector of $\mathbb{N}^d$ whose k-th coordinate is one and all others are zero. Let e and $f = (\mathbf{1}_{k_1},\ldots,\mathbf{1}_{k_v})$ be two disjoint tuples of non-zero vectors in $\mathbb{N}^d$ such that $|e| = |f|$ and $k_i \in \{1,\ldots,d\}$, $1 \leq i \leq v$. Then $F_{e,f}(\mathbf{x})$ satisfies the p-Lucas property for all primes p.*

Proof. — Let $\mathbf{x}$ be in $\mathcal{D}_{e,f}$. By assumption, there is a coordinate $\mathbf{d}$ of either e or f such that $\mathbf{d} \cdot \mathbf{x} \geq 1$. But, since $\mathbf{x}$ belongs to $[0,1)^d$ and $f = (\mathbf{1}_{k_1},\ldots,\mathbf{1}_{k_v})$, $\mathbf{d}$ has to be a coordinate of the vector e so that

$$\begin{aligned}\Delta_{e,f}(\mathbf{x}) &= \sum_{i=1}^u \lfloor \mathbf{e}_i \cdot \mathbf{x} \rfloor - \sum_{j=1}^v \lfloor \mathbf{1}_{k_j} \cdot \mathbf{x} \rfloor \\ &= \sum_{i=1}^u \lfloor \mathbf{e}_i \cdot \mathbf{x} \rfloor \\ &\geq 1.\end{aligned}$$

Proposition 8.8 then applies to conclude the proof. ∎

In order to transfer the p-Lucas property from multivariate series of type $F_{e,f}$ to one-variable formal power series, we will prove the following useful complement to Proposition 8.8.

Proposition 8.10. — *We keep all assumptions and notation of Proposition 8.8. Set*

$$\mathcal{N} := \left\{\mathbf{n} \in \mathbb{N}^d \,:\, \forall \mathbf{x} \in [0,1)^d \textit{ with } \mathbf{n}\cdot\mathbf{x} \geq 1,\ \textit{one has } \Delta_{e,f}(\mathbf{x}) \geq 1\right\}.$$

Let $\mathbf{n} = (n_1, \dots, n_d)$ be in $\mathcal{N}$ and $(b_1, \dots, b_d)$ be a vector of non-zero rational numbers. Then $F_{e,f}(b_1x^{n_1}, \dots, b_dx^{n_d})$ belongs to $\mathfrak{L}_1(\mathcal{S}')$, where

$$\mathcal{S}' := \left\{p \in \mathcal{S} \,:\, (b_1, \dots, b_d) \in \mathbb{Z}_{(p)}^d\right\}.$$

Let us illustrate this result with the example given just after Proposition 8.8, that is with the function

$$F_{e,f}(x,y) = \sum_{(n,m)\in\mathbb{N}^2} \frac{(2n+m)!(n+m)!}{n!^3m!^2} x^n y^m .$$

We consider the specialization given by $\mathbf{n} = (1,1)$ and $b_1 = b_2 = 1$. Then Proposition 8.10 applies because we already observed that $\Delta_{e,f}(x_1, x_2) \geq 1$ for all (x_1, x_2) in $[0,1)^2$ satisfying $x_1 + x_2 \geq 1$. A small computation shows that we obtain yet another proof of Gessel's result stating that the Apéry sequence

$$\left(\sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}\right)_{n\geq 0}$$

satisfies the p-Lucas property for all primes p.

Applying Proposition 8.10 to the same function but with the specialization given by $\mathbf{n} = (2,1)$, $b_1 = -1$ and $b_2 = 2$, we get that

$$F_{e,f}(-x^2, 2x) = \sum_{n=0}^{\infty} \sum_{k=0}^{\lfloor n/2\rfloor} (-1)^k 2^{n-2k} \binom{n}{k} \binom{n-k}{n-2k}^2 x^n$$

also satisfies the p-Lucas property for all primes p.

Now, we prove Proposition 8.10.

Proof of Proposition 8.10. — Set

$$\mathcal{N} := \left\{\mathbf{n} \in \mathbb{N}^d \,:\, \forall \mathbf{x} \in [0,1)^d \text{ with } \mathbf{n}\cdot\mathbf{x} \geq 1,\ \text{one has } \Delta_{e,f}(\mathbf{x}) \geq 1\right\}.$$

Let $\mathbf{n} = (n_1, \dots, n_d)$ be in $\mathcal{N}$, $(b_1, \dots, b_d)$ be a vector of non-zero rational numbers. Set

$$S' := \left\{p \in S \,:\, (b_1, \dots, b_d) \in \mathbb{Z}_{(p)}^d\right\}$$

and let p be a prime number in S'. We will simply write F for $F_{e,f}$, $\mathcal{Q}$ for $\mathcal{Q}_{e,f}$, and Δ for $\Delta_{e,f}$. By Proposition 8.8, the sequence $\mathcal{Q}(\mathbf{n})$ has the p-Lucas property, so that

$$F(\mathbf{x}) \equiv \left(\sum_{\mathbf{0}\leq\mathbf{a}\leq(p-1)\mathbf{1}} \mathcal{Q}(\mathbf{a})\mathbf{x}^{\mathbf{a}}\right) F(\mathbf{x}^p) \mod p\mathbb{Z}_{(p)}[[\mathbf{x}]] .$$

This gives:

$$F(b_1x^{n_1},\dots,b_dx^{n_d}) \equiv \left(\sum_{\mathbf{0}\le\mathbf{a}\le(p-1)\mathbf{1}} \mathbf{b}^{\mathbf{a}}\mathcal{Q}(\mathbf{a})x^{\mathbf{n}\cdot\mathbf{a}}\right) F\Big(b_1^px^{n_1p},\dots,b_d^px^{n_dp}\Big) \mod p\mathbb{Z}_{(p)}[[x]]$$
$$\equiv \left(\sum_{\mathbf{0}\le\mathbf{a}\le(p-1)\mathbf{1}} \mathbf{b}^{\mathbf{a}}\mathcal{Q}(\mathbf{a})x^{\mathbf{n}\cdot\mathbf{a}}\right) F\Big(b_1x^{n_1p},\dots,b_dx^{n_dp}\Big) \mod p\mathbb{Z}_{(p)}[[x]]\,,$$

since $b_i^p \equiv b_i \mod p\mathbb{Z}_{(p)}$ for all i in $\{1,\dots,d\}$. For all $\mathbf{a}$ in $\{0,\dots,p-1\}^d$ satisfying $\mathbf{n}\cdot\mathbf{a}\ge p$, we have $\mathbf{n}\cdot\mathbf{a}/p\ge 1$ and thus $\Delta(\mathbf{a}/p)\ge 1$. It follows that

$$v_p\big(\mathcal{Q}(\mathbf{a})\big) = \sum_{\ell=1}^{\infty}\Delta\left(\frac{\mathbf{a}}{p^\ell}\right) \ge \Delta\left(\frac{\mathbf{a}}{p}\right) \ge 1\,,$$

because Δ is non-negative on $\mathbb{R}^d$. Thus there is a polynomial $A(x)$ with coefficients in $\mathbb{Z}_{(p)}$ and of degree at most $p-1$ such that

$$F(b_1x^{n_1},\dots,b_dx^{n_d}) \equiv A(x)F\Big(b_1x^{n_1p},\dots,b_dx^{n_dp}\Big) \mod p\mathbb{Z}_{(p)}[[x]]\,.$$

This shows that $F(b_1x^{n_1},\dots,b_dx^{n_d})$ satisfies the p-Lucas property, as expected. ☐

8.4. Specializations of factorial ratios. — Our main interest when working with multivariate power series in this setting is to benefit from the following general philosophy: interesting classical power series in one variable can be produced as simple specializations of simple multivariate power series. In particular, we claim that specializations of functions of type $F_{e,f}$ lead to many classical examples of generating functions arising in combinatorics and number theory. As already mentioned in Section 8.3, the generating function of Apéry's numbers

$$f(x) = \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n}\binom{n}{k}^2\binom{n+k}{k}\right)x^n$$

can be for instance obtained as the specialization $f(x)=F_{e,f}(x,x)$ of the two-variate generating series of factorial ratios

$$F_{e,f}(x_1,x_2) = \sum_{(n_1,n_2)\in\mathbb{N}^2}\frac{(2n_1+n_2)!(n_1+n_2)!}{n_1!^3n_2!^2}x_1^{n_1}x_2^{n_2}, \tag{8.2}$$

corresponding to the choice

$$e=\big((2,1),(1,1)\big) \quad\text{and}\quad f=\big((1,0),(1,0),(1,0),(0,1),(0,1)\big)\,.$$

In order to support our claim, we gather in the following table some classical sequences for which we prove that they satisfy the p-Lucas property for all primes p. Indeed, they all arise from the specialization in (x,x) of bivariate power series $F_{e,f}(x_1,x_2)$ that belong to $\mathfrak{L}_2(\mathcal{P})$. The fact these bivariate power series belong to $\mathfrak{L}_2(\mathcal{P})$ is a direct consequence of Corollary 8.9. Proposition 8.10 then implies that the specialization $F_{e,f}(x,x)$ belong to $\mathfrak{L}_1(\mathcal{P})$.

As pointed out to us by the referee, there is also another way to prove that all (univariate) sequences listed in the following table have the p-Lucas property for all prime numbers p.

Indeed, the generating series corresponding to all two-variate sequences listed in this table are Hadamard products of multivariate power series whose coefficients have the form

$$\sum_{n_1,\ldots,n_k\geq 0} \frac{(a_1n_1+\cdots+a_kn_k)!}{(n_1!)^{a_1}\cdots(n_k!)^{a_k}}\,.$$

Furthermore, the latter power series turn out to be partial diagonalizations of the power series

$$\frac{1}{1-x_1-\cdots-x_m}$$

for which we already proved that they belong to $\mathfrak{L}_m(\mathbb{Z})$.

Sequence	$\mathcal{Q}_{e,f}(n_1,n_2)$	Reference from OEIS
$\binom{2n}{n}=\sum_{k=0}^{n}\binom{n}{k}^2$	$\frac{(n_1+n_2)!^2}{n_1!^2n_2!^2}$	Central binomial coefficients (A000984)
$\sum_{k=0}^{n}\binom{n}{k}^2\binom{n+k}{k}^2$	$\frac{(2n_1+n_2)!^2}{n_1!^4n_2!^2}$	Apéry numbers (A005259)
$\sum_{k=0}^{n}\binom{n}{k}^2\binom{n+k}{k}$	$\frac{(2n_1+n_2)!(n_1+n_2)!}{n_1!^3n_2!^2}$	Apéry numbers (A005258)
$\sum_{k=0}^{n}\binom{n}{k}^3$	$\frac{(n_1+n_2)!^3}{n_1!^3n_2!^3}$	Franel numbers (A000172)
$\sum_{k=0}^{n}\binom{n}{k}^4$	$\frac{(n_1+n_2)!^4}{n_1!^4n_2!^4}$	(A005260)
$\sum_{k=0}^{n}\binom{n}{k}\binom{2k}{k}\binom{2(n-k)}{n-k}$	$\frac{(n_1+n_2)!(2n_1)!(2n_2)!}{n_1!^3n_2!^3}$	(A081085)
$\sum_{k=0}^{n}\binom{n}{k}^2\binom{2k}{k}$	$\frac{(n_1+n_2)!^2(2n_1)!}{n_1!^4n_2!^2}$	Number of abelian squares of length $2n$ over an alphabet with 3 letters (A002893)
$\sum_{k=0}^{n}\binom{n}{k}^2\binom{2k}{k}\binom{2(n-k)}{n-k}$	$\frac{(n_1+n_2)!^2(2n_1)!(2n_2)!}{n_1!^4n_2!^4}$	Domb numbers (A002895)
$\sum_{k=0}^{n}\binom{n}{k}\binom{n+k}{k}$	$\frac{(2n_1+n_2)!}{n_1!^2n_2!}$	Central Delannoy numbers (A001850)
$\sum_{k=0}^{n}\binom{2k}{k}^2\binom{2(n-k)}{n-k}^2$	$\frac{(2n_1)!^2(2n_2)!^2}{n_1!^4n_2!^4}$	(A036917)

Let us end this section with an example of a different type, that is for which f is not of the form $(\mathbf{1}_{k_1},\ldots,\mathbf{1}_{k_v})$. Set

$$F_{e,f}(x_1,x_2):=\sum_{(n_1,n_2)\in\mathbb{N}^2}\frac{(3n_1+2n_2)!}{(n_1+n_2)!n_1!^2n_2!}x_1^{n_1}x_2^{n_2}\,.$$

In that case, we obtain $\mathcal{D}_{e,f} = \{(x,y) \in [0,1)^2 \,:\, 3x+2y \geq 1\}$. When (x_1,x_2) belongs to $\mathcal{D}_{e,f}$, we get that

$$\Delta_{e,f}(x_1,x_2) = \lfloor 3x_1 + 2x_2 \rfloor - \lfloor x_1 + x_2 \rfloor \geq 1\,.$$

By Proposition 8.8, it follows that $F_{e,f}(x_1,x_2)$ has the p-Lucas property for all primes. Using specializations in $(-x,x)$ and $(2x^3,3x^2)$, we then infer from Proposition 8.10 that both sequences

$$\sum_{k=0}^{n}(-1)^k\binom{2n+k}{n}\binom{n+k}{k}\binom{n}{k} \quad \text{and} \quad \sum_{\substack{k=0\\ k\equiv n \bmod 2}}^{\lfloor n/3\rfloor} 2^k 3^{\frac{n-3k}{2}}\binom{n}{k}\binom{n-k}{\frac{n-k}{2}}\binom{\frac{n-k}{2}}{k}$$

also satisfy the p-Lucas property for all prime numbers p.

8.5. Examples from differential equations of Calabi-Yau type. — Motivated by the search for differential operators associated with particular families of Calabi-Yau varieties, Almkvist *et al.* [**6**] gave a list of more than 400 differential operators satisfying some algebraic conditions [**6**, Section 1]. In particular, a condition is that the associated differential equation admits a unique power series solution near $z=0$ with constant term 1 and that this power series has integral Taylor coefficients. In most of the cases, this solution is also given in [**6**]. It turns out that our method enables us to prove that most of these solutions have the p-Lucas property for infinitely many primes p.

By studying the integrality of the Taylor coefficients of mirror maps, Kratthentaler and Rivoal in [**37**] and Delaygue in [**18**, Section 10.2] showed that the power series solutions near $z=0$ of 143 equations in Table [**6**] are specializations of series of type $F_{e,f}$. Furthermore, they showed that in 140 cases the associated functions Δ are greater than or equal to 1 on $\mathcal{D}_{e,f}$. Hence, to prove that these specializations have the p-Lucas property for all primes p, it suffices to show that the specialization is given by a vector $\mathbf{n}$ such that if $\mathbf{x} \in [0,1)^d$ and $\mathbf{n}\cdot\mathbf{x} \geq 1$, then $\Delta_{e,f}(\mathbf{x}) \geq 1$ and to apply Proposition 8.10. A similar approach also works in the more general framework of multivariate generalized hypergeometric series previously mentioned at the beginning of Section 8 (see [**4**] for more details).

Following this method, we checked that 212 cases have the p-Lucas property for infinitely many primes p, namely Cases 1–25, 29, 3^*, 4^*, 4^{**}, 6^*–10^*, 7^{**}–10^{**}, 13^*, 13^{**}, $\hat{1}$–$\hat{14}$, 30, 31, 34–41, 43–83, 85–108, 110–116, 119–122, 124–132, 145–153, 155–172, 180, 185, 188, 190–192, 197, 208, 209, 212, 232, 233, 237–241, 243, 278, 284, 288, 292, 307, 323, 330, 337, 338, 340, 367, 369–372, 377, 380, 398.

Among the cases not covered in [**37**] nor [**18**], we give two examples: Cases 4^* and 31. In Case 4^*, the power series solution near $z=0$ is

$$f(z) = \sum_{n=0}^{\infty}\sum_{k=0}^{n} 27^n\binom{2n}{n}\binom{-1/3}{k}^2\binom{-2/3}{n-k}^2 z^n\,.$$

Hence $f(z) = F(27z,27z)$ where

$$F(x,y) = \sum_{n_1,n_2\geq 0}\frac{(2n_1+2n_2)!(1/3)_{n_1}^2(2/3)_{n_2}^2}{(n_1+n_2)!^2 n_1!^2 n_2!^2}x^{n_1}y^{n_2}\,,$$

which is not a series of type $F_{e,f}$ but a two-variate generalized hypergeometric series. Using the general approach of [**4**], it can be shown that $f(z)$ has the p-Lucas property for all primes $p > 3$.

In Case 31, the power series solution near $z = 0$ can be rewritten as

$$f(z) = \sum_{n=0}^{\infty} \sum_{k=0}^{n} \sum_{i=0}^{k} 4^{3n} 4^{2(n-k)} 4^{k-i} (-1)^i \binom{2k}{k} \binom{2i}{i} \frac{(1/4)_n (1/4)_{n-k} (3/4)_k}{n!(n-k)!(k-i)!i!} z^n .$$

Hence $f(z) = F(4^5 z, 4^4 z, -4^3 z)$ where $F(x,y,z)$ is

$$\sum_{n_1,n_2,n_3 \geq 0} \binom{2(n_2+n_3)}{n_2+n_3} \binom{2n_3}{n_3} \frac{(1/4)_{n_1+n_2+n_3} (1/4)_{n_1} (3/4)_{n_2+n_3}}{(n_1+n_2+n_3)! n_1! n_2! n_3!} x^{n_1} y^{n_2} z^{n_3},$$

which is now a three-variate generalized hypergeometric series. Using the general approach of [**4**], it can be shown that $f(z)$ has the p-Lucas property for all primes $p \equiv 1 \mod 4$.

9. Algebraic independence of G-functions: a few examples

In this last section, we gather various examples of statements concerning algebraic independence of G-functions that follow from simple applications of our method.

9.1. Factorial ratios. — Given two tuples of vectors of natural numbers, $e = (e_1, \ldots, e_u)$ and $f = (f_1, \ldots, f_v)$, we recall that the associated sequence of factorial ratios is defined by

$$\mathcal{Q}_{e,f}(n) := \frac{\prod_{i=1}^{u} (e_i n)!}{\prod_{i=1}^{v} (f_i n)!}$$

and that the generating series of such a sequence is denoted by

$$F_{e,f}(x) := \sum_{n=0}^{\infty} \mathcal{Q}_{e,f}(n) x^n .$$

In the sequel, we always assume that the sets $\{e_1, \ldots, e_u\}$ and $\{f_1, \ldots, f_v\}$ are disjoint. We also recall that $|e| := \sum_{i=1}^{u} e_i$, $|f| := \sum_{i=1}^{v} f_i$, and

$$m_{e,f} := \left(\max\{e_1, \ldots, e_u, f_1, \ldots, f_v\}\right)^{-1} .$$

We set

$$C_{e,f} := \frac{\prod_{i=1}^{u} e_i^{e_i}}{\prod_{i=1}^{v} f_i^{f_i}} .$$

From Stirling's formula, we deduce the following general asymptotics:

$$\mathcal{Q}_{e,f}(n) \underset{n\to\infty}{\sim} C_{e,f}^n \left(\sqrt{2\pi n}\right)^{u-v} \sqrt{\frac{\prod_{i=1}^{u} e_i}{\prod_{i=1}^{v} f_i}} . \tag{9.1}$$

As an application of these asymptotics and Proposition 7.4, we obtain for instance the following result.

Theorem 9.1. — *The functions*

$$\sum_{n=0}^{\infty}\frac{(3n)!}{n!^3}z^n,\ \sum_{n=0}^{\infty}\frac{(5n)!(3n)!}{(2n)!^2n!^4}z^n \quad \text{and} \quad \sum_{n=0}^{\infty}\frac{(10n)!}{(5n)!(3n)!n!^2}z^n$$

are algebraically independent over $\mathbb{C}(z)$.

Proof. — We infer from (9.1) that these power series belong to $\mathfrak{M}$ and all have distinct radii of convergence, while Proposition 8.1 can be used to prove that they do satisfy the p-Lucas property for all prime numbers p. The results then follows from Proposition 7.4. □

Using Proposition 7.6, we can also obtain the following result.

Proposition 9.2. — *Let* e_1 *and* f_1*, respectively* e_2 *and* f_2*, be disjoint tuples of positive integers such that the following hold.*

(i) $v_1 - u_1 = 2$.

(ii) $v_2 - u_2 \geq 3$.

(iii) $\mathcal{Q}_{e_1,f_1}$ *and* $\mathcal{Q}_{e_2,f_2}$ *satisfy the* p*–Lucas property for all primes* p.

Then $F_{e_1,f_1}(z)$ *and* $F_{e_2,f_2}(z)$ *are algebraically independent over* $\mathbb{C}(z)$.

Proof. — We first observe that if $C_{e_1,f_1} \neq C_{e_2,f_2}$, we can use Proposition 7.4 as previously to obtain the desired result. We can thus assume that $C_{e_1,f_1} = C_{e_2,f_2} =: C$ and we will use Proposition 7.6.

We first remark that $F_{e_1,f_1}(z)$ and $F_{e_2,f_2}(z)$ are both transcendental. This follows for instance from applying Proposition 9.6 twice with a single function. Now, by Pringsheim's theorem, $F_{e_1,f_1}(z)$ and $F_{e_2,f_2}(z)$ have a singularity at $1/C$. Using (9.1), we infer from the assumption $v_1 - u_1 = 2$ that F_{e_1,f_1} satisfies Condition (i) of Proposition 7.6, while we infer from the assumption $v_2 - u_2 \geq 3$ that F_{e_2,f_2} satisfies Condition (ii) of Proposition 7.6. Since, by assumption, F_{e_1,f_1} and F_{e_2,f_2} both belong to $\mathfrak{L}(\mathcal{P})$, we can apply Proposition 7.6 to conclude the proof. □

Remark 9.3. — Using the discussion in [**44**], one can actually show that the only case where $F_{e,f}(z)$ both belongs to $\mathfrak{L}(\mathcal{P})$ and is an algebraic function corresponds to $e = (2)$ and $f = (1,1)$, that is to

$$F_{e,f}(z) = \frac{1}{\sqrt{1-z}}\,\cdot$$

We give the following illustration of Proposition 9.2.

Theorem 9.4. — *The functions*

$$\sum_{n=0}^{\infty}\frac{(4n)!}{(2n)!n!^2}z^n \quad \text{and} \quad \sum_{n=0}^{\infty}\frac{(2n)!^3}{n!^6}z^n$$

are algebraically independent over $\mathbb{C}(z)$.

Proof. — Here we have $e_1 = (4)$ and $f_1 = (2,1,1)$, so that $v_1 - u_1 = 2$. Furthermore, for all x in $[1/4, 1)$, we have

$$\Delta_{e_1,f_1}(x) = \lfloor 4x \rfloor - \lfloor 2x \rfloor \geq 1\,,$$

which shows that $\mathcal{Q}_{e_1,f_1}$ satisfies the p-Lucas property for all primes p. On the other hand, we also have $e_2=(2,2,2)$ and $f_2=(1,1,1,1,1,1)$, so that $v_2-u_2=3$. Furthermore, for all x in $[1/2,1)$, we have

$$\Delta_{e_2,f_2}(x)=3\lfloor 2x\rfloor\geq 1\,,$$

which shows that $\mathcal{Q}_{e_2,f_2}$ also satisfies the p-Lucas property for all primes p. Then the result follows from Proposition 9.2. □

9.2. Generalized hypergeometric functions. — Using Stirling formula, it is easy to give general asymptotics for the coefficients of generalized hypergeometric functions. Indeed, it implies that

$$\Gamma(x)\underset{x\to\infty}{\sim}x^{x-\frac{1}{2}}e^{-x}\sqrt{2\pi}\,,$$

and hence

$$(\alpha)_n=\frac{\Gamma(\alpha+n)}{\Gamma(\alpha)}\underset{n\to\infty}{\sim}(\alpha+n)^{\alpha-\frac{1}{2}+n}e^{-\alpha-n}\frac{\sqrt{2\pi}}{\Gamma(\alpha)}\,.$$

Let us recall that

$$\mathcal{Q}_{\boldsymbol{\alpha},\boldsymbol{\beta}}(n):=\frac{(\alpha_1)_n\cdots(\alpha_r)_n}{(\beta_1)_n\cdots(\beta_s)_n}\quad\text{and}\quad F_{\boldsymbol{\alpha},\boldsymbol{\beta}}(x):=\sum_{n=0}^{\infty}\mathcal{Q}_{\boldsymbol{\alpha},\boldsymbol{\beta}}(n)x^n\,.$$

When $r=s$, that is when $F_{\boldsymbol{\alpha},\boldsymbol{\beta}}(x)$ is a G-function, we thus obtain that

$$\mathcal{Q}_{\boldsymbol{\alpha},\boldsymbol{\beta}}(n)\underset{n\to\infty}{\sim}n^{\sum_{i=1}^r(\alpha_i-\beta_i)}\left(\frac{\prod_{i=1}^r(\alpha_i+n)}{\prod_{j=1}^r(\beta_j+n)}\right)^n e^{\sum_{i=1}^r(\beta_i-\alpha_i)}\frac{\prod_{i=1}^r\Gamma(\alpha_i)}{\prod_{j=1}^r\Gamma(\beta_j)}$$

which leads to the following simple asymptotics:

$$\mathcal{Q}_{\boldsymbol{\alpha},\boldsymbol{\beta}}(n)\underset{n\to\infty}{\sim}\left(\frac{\prod_{i=1}^r\Gamma(\alpha_i)}{\prod_{j=1}^r\Gamma(\beta_j)}\right)n^{\sum_{i=1}^r(\alpha_i-\beta_i)}\,.\tag{9.2}$$

Note that it is usually easy to detect from such asymptotics when the hypergeometric function $F_{\boldsymbol{\alpha},\boldsymbol{\beta}}(z)$ is transcendental by comparison with asymptotics of coefficients of algebraic functions. Otherwise, one can always use the interlacing criterion of Beukers and Heckman [**11**]. For instance, one can use our asymptotics to show that the hypergeometric function

$$\mathfrak{f}(z):=\sum_{n=0}^{\infty}\frac{(1/5)_n(4/5)_n}{n!^2}z^n$$

is transcendental and belongs to $\mathfrak{W}$ (see the proof of Theorem 9.7). Furthermore, Corollary 8.7 shows it has the p-Lucas property for all primes larger than 5. We can thus apply Proposition 7.4 to deduce the following result.

Theorem 9.5. — *All elements of the set $\{\mathfrak{f}(nz):n\geq 1\}$ are algebraically independent over $\mathbb{C}(z)$.*

As pointed out to us by the referee, this can actually be generalized as follows.

Proposition 9.6. — *Let $f_1,\ldots,f_s$ be transcendental generalized hypergeometric series with rational parameters, radii of convergence 1 and which all belong to $\mathcal{L}(\mathcal{S})$ for some infinite set $\mathcal{S}$ of non-zero prime ideals of $\mathbb{Z}$. Let $\lambda_1,\ldots,\lambda_s$ be pairwise distinct non-zero algebraic numbers, then $f_1(\lambda_1z),\ldots,f_s(\lambda_sz)$ are algebraically independent over $\mathbb{C}(z)$.*

Proof. — Let i be in $\{1, \dots, s\}$. Then f_i is a G-function annihilated by a differential operator with three singularities at $0, 1$ and ∞. Since f_i is transcendental, there is no power of f_i which is meromorphic at 1. Indeed, otherwise there would exist a positive integer n and a non-zero polynomial $Q(x)$ with integer coefficients such that $Q(x)f_i(x)^n$ would be an entire G-function and thus a polynomial. Since f_i is transcendental, this would provide a contradiction. Hence f_i belongs to $\mathfrak{M}$. Since the λ_j's are algebraic, there exist a number field K and a suitable infinite set $\mathcal{S}'$ of non-zero prime ideals of $\mathcal{O}_K$ such that the $f_j(\lambda_j z)$'s belong to $\mathcal{L}(\mathcal{O}_K, \mathcal{S}')$. The power series $f_1(\lambda_1 z), \dots, f_s(\lambda_s z)$ have pairwise distinct radii of convergence so the result follows from Proposition 7.4. $\square$

Let us give another kind of example derived from Proposition 7.6.

Theorem 9.7. — *The hypergeometric functions*

$$\mathfrak{f}_1(z) = \sum_{n=0}^{\infty} \frac{(1/5)_n(4/5)_n}{n!^2} z^n \quad \text{and} \quad \mathfrak{f}_2(z) = \sum_{n=0}^{\infty} \frac{(1/3)_n(1/2)_n^2}{(2/3)_n n!^2} z^n$$

are algebraically independent over $\mathbb{C}(z)$.

Proof. — For $\boldsymbol{\alpha} = (1/5, 4/5)$ and $\boldsymbol{\beta} = (1, 1)$, we infer from Equation (9.2) that

$$\mathcal{Q}_{\boldsymbol{\alpha},\boldsymbol{\beta}}(n) \underset{n\to\infty}{\sim} \frac{\Gamma(1/5)\Gamma(4/5)}{n} \tag{9.3}$$

which are the asymptotics of a transcendental series. For $\boldsymbol{\alpha} = (1/3, 1/2, 1/2)$ and $\boldsymbol{\beta} = (2/3, 1, 1)$, we have

$$\mathcal{Q}_{\boldsymbol{\alpha},\boldsymbol{\beta}}(n) \underset{n\to\infty}{\sim} \frac{\Gamma(1/3)\Gamma(1/2)^2}{\Gamma(2/3)} \frac{1}{n^{4/3}}, \tag{9.4}$$

so that $\mathfrak{f}_2$ belongs to $\mathfrak{W}$. By Corollary 8.7, we first get that $\mathfrak{f}_1$ belongs to $\mathfrak{L}(\mathcal{S}_0)$, where $\mathcal{S}_0$ is the set of primes larger than 5, while Proposition 8.5 implies that $\mathfrak{f}_2$ belongs to $\mathfrak{L}(\mathcal{S}_1)$, where $\mathcal{S}_1 = \{p \in \mathcal{P} : p \equiv 1 \mod 6\}$. In particular, both belong to $\mathfrak{L}(\mathcal{S}_1)$. The series $\mathfrak{f}_2$ belongs to $\mathfrak{W} \cap \mathfrak{L}(\mathcal{S}_1)$ so is transcendental over $\mathbb{C}(z)$ by Proposition 7.4. Note that these functions are hypergeometric and thus have the same radius of convergence 1. Then (9.3) and (9.4) show, as earlier, that one can apply Proposition 7.6, which ends the proof. $\square$

9.3. Sums and products of binomials. — As an application of Proposition 7.4, we give below a proof of the following result already mentioned in the introduction.

Theorem 9.8. — *Let $\mathcal{F}$ be the set formed by the union of the three following sets:*

$$\left\{\sum_{n=0}^{\infty}\sum_{k=0}^{n}\binom{n}{k}^r z^n \,:\, r \geq 3\right\}, \left\{\sum_{n=0}^{\infty}\sum_{k=0}^{n}\binom{n}{k}^r\binom{n+k}{k}^r z^n \,:\, r \geq 2\right\}$$

and

$$\left\{\sum_{n=0}^{\infty}\sum_{k=0}^{n}\binom{n}{k}^{2r}\binom{n+k}{k}^r z^n \,:\, r \geq 1\right\}.$$

Then all elements of $\mathcal{F}$ are algebraically independent over $\mathbb{C}(z)$.

Proof. — McIntosh [**42**] proves general asymptotics for sequences of the form

$$S(n) := \sum_{k=0}^{n} \prod_{j=0}^{m} \binom{n+jk}{k}^{r_j},$$

where $m, r_0, \ldots, r_m$ are natural integers. Indeed, he shows that

$$S(n) \underset{n\to\infty}{\sim} \frac{\mu^{n+1/2}}{\sqrt{\nu(2\pi\lambda n)^{r-1}}},$$

with $r = r_0 + \cdots + r_m$, and where λ, $0 < \lambda < 1$, is defined by

$$\prod_{j=0}^{m} \left(\frac{(1+j\lambda)^j}{\lambda(1+j\lambda-\lambda)^{j-1}} \right)^{r_j} = 1,$$

and where μ and ν are respectively defined by

$$\mu = \prod_{j=0}^{m} \left(\frac{1+j\lambda}{1+j\lambda-\lambda} \right)^{r_j}$$

and

$$\nu = \sum_{j=0}^{m} \frac{r_j}{(1+j\lambda-\lambda)(1+j\lambda)}.$$

The particular case we are interested in is considered in [**42**]. For a positive integer r, we then obtain the following asymptotics:

$$\sum_{k=0}^{n} \binom{n}{k}^r \underset{n\to\infty}{\sim} \frac{2^{rn}}{\sqrt{r(\pi n/2)^{r-1}}},$$

$$\sum_{k=0}^{n} \binom{n}{k}^r \binom{n+k}{k}^r \underset{n\to\infty}{\sim} \frac{(1+\sqrt{2})^{2nr+r}}{\sqrt{4r(\pi n\sqrt{2})^{2r-1}}},$$

and

$$\sum_{k=0}^{n} \binom{n}{k}^{2r} \binom{n+k}{k}^r \underset{n\to\infty}{\sim} \frac{\left((1+\sqrt{5})/2\right)^{5nr+4r}}{\sqrt{(5+2\sqrt{5})r(2\pi n)^{3r-1}}}.$$

These asymptotics show that all functions in $\mathcal{F}$ have distinct radii of convergence. Furthermore, we infer from Remark 7.5 and these asymptotics that they all belong to $\mathfrak{W}$ since $r \geq 3$ for the first family, $r \geq 2$ for the second, and $r \geq 1$ for the third. On the other hand, we already proved in Section 8.3 that all functions in $\mathcal{F}$ belong to $\mathfrak{L}(\mathcal{P})$. The result now follows directly from Proposition 7.4. □

9.4. A mixed example. — One special feature of our approach is that one can easily mix functions of rather different type without having to consider all their derivatives and finding a common differential equation for them. We illustrate this claim with the following simple example already mentioned in the introduction.

Theorem 9.9. — *The functions*

$$f(z) := \sum_{n=0}^{\infty} \frac{(4n)!}{(2n)!n!^2} z^n, \; g(z) := \sum_{n=0}^{\infty} \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2 z^n, \; h(z) := \sum_{n=0}^{\infty} \frac{(1/6)_n (1/2)_n}{(2/3)_n n!} z^n,$$

and

$$i(z) := \sum_{n=0}^{\infty} \frac{(1/5)_n^3}{(2/7)_n n!^2} z^n$$

are algebraically independent over $\mathbb{C}(z)$.

Note that the two last functions are not globally bounded so they cannot be obtained as the diagonal of some rational functions.

Proof. — On the one hand, we already shown in Section 8.1 that $f(z)$ belongs to $\mathfrak{L}(\mathcal{P})$, in Section 6 that $g(z)$ belongs to $\mathfrak{L}(\mathcal{P})$, in Section 8.2 that $h(z)$ belongs to $\mathfrak{L}(\mathcal{S})$, where $\mathcal{S} = \{p \in \mathcal{P} : p \equiv 1 \mod 6\}$, and it follows from Proposition 8.5 that $i(z)$ belongs to $\mathfrak{L}(\mathcal{S}')$, where $\mathcal{S}' = \{p \in \mathcal{P} : p \equiv 1 \mod 35\}$. Hence all belong to $\mathfrak{L}(\mathcal{S}_1)$, where $\mathcal{S}_1 = \{p \in \mathcal{P} : p \equiv 1 \mod 210\}$.

On the other hand, we infer from Remark 7.5 and asymptotics for the coefficients of these functions (see Sections 9.1, 9.2, and 9.3) that they all belong to $\mathfrak{W}$ and that $\rho_f = 4^{-3}$, $\rho_g := (1+\sqrt{2})^{-4}$, $\rho_h = 1$, and $\rho_i = 1$.

Now, let us assume that f, g, h, i are algebraically dependent over $\mathbb{C}(z)$. Then by Theorem 5.1, there should exist integers a, b, c, d, not all zero, such that

$$f(z)^a g(z)^b h(z)^c i(z)^d = r(z)\,,$$

where $r(z)$ is a rational fraction. If $a \neq 0$, we infer from the equality

$$f(z)^a = r(z) g(z)^{-b} h(z)^{-c} i(z)^{-d}$$

that $f(z)^a$ is meromorphic at ρ_f, which provides a contradiction with the fact that $f(z)$ belongs to $\mathfrak{W}$. Thus a equals 0. Now, if $b \neq 0$, we obtain in the same way that $g(z)^b$ is meromorphic at ρ_g, which provides a contradiction with the fact that $g(z)$ belongs to $\mathfrak{W}$. Thus $b = 0$ and we have

$$h(z)^c i(z)^d = r(z)\,,$$

with c and d not all zero. This means that h and i are algebraically dependent. However, using the asymptotics of Section 9.2, we see that h and i satisfy the assumption of Proposition 7.6 and are thus algebraically independent. We thus get a contradiction, concluding the proof. □

Acknowledgements. — The authors would like to thank the anonymous referee for his careful reading of a first version of this paper, as well as for his valuable comments.

References

[1] B. Adamczewski, J. P. Bell, *On vanishing coefficients of algebraic power series over fields of positive characteristic*, Invent. Math. **187** (2012), 343–393.

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

[3] B. Adamczewski, J. P. Bell, *A problem about Mahler functions*, to appear in Ann. Sc. Norm. Super. Pisa.

[4] B. Adamczewski, J. P. Bell, and E. Delaygue, *Algebraic independence of G-functions and congruences "à la Lucas"*, arXiv:1603.04187v1 [math.NT].

[5] J.-P. Allouche, D. Gouyou-Beauchamps, and G. Skordev, *Transcendence of binomial and Lucas' formal poxer series*, J. Algebra **210** (1998), no. 2, 577–592.

[6] G. Almkvist, C. van Eckenvort, D. van Straten, and W. Zudilin, *Tables of Calbi-Yau equations*, arXiv:0507430v2 [math.AG], 130 pages.

[7] Y. André, *Groupes de Galois motiviques et périodes*, Séminaire Bourbaki, exposé 1104, novembre 2015.

[8] Y. André, *Séries Gevrey de type arithmétique, I. Théorèmes de pureté et de dualité*, Ann. Math. **151** (2000), 705–740.

[9] Y. André, *G-functions and Geometry*, Aspects of Math. **E13**, Vieweg, Braunschweig/Wiesbaden (1989).

[10] J. Ayoub, *Une version relative de la conjecture des périodes de Kontsevich-Zagier*, Ann. Math. **181** (2015), 905–992.

[11] F. Beukers, G. Heckman, *Monodromy for the hypergeometric functions* ${}_nF_{n-1}$, Invent. Math. **95** (1989), 325–354.

[12] M. Bousquet-Mélou, *Rational and algebraic series in combinatorial enumeration*, International Congress of Mathematicians. Vol. III, 789–826, Eur. Math. Soc., Zürich, 2006.

[13] J. W. Bober, *Factorial ratios, hypergeometric series, and a family of step functions*, Journal of the London Mathematical Society (2) **79** (2009), 422–444.

[14] G. Christol, *Fonctions hypergéométriques bornées*, Groupe de travail d'analyse ultramétrique, tome **14** (1986-1987), exp. 8, 1-16.

[15] G. Christol, *Diagonales de fractions rationnelles*, Progress in Math. **75** (1988), 65–90.

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

[17] D. Chudnovsky, G. Chudnovsky, *Applications of Padé approximations to diophantine inequalities in values of G-functions*, in Number Theory (New York 1983–84), 9–51, Lecture Notes in Math. **1135**, Springer-Verlag, New York (1985).

[18] É. Delaygue, *Propriétés arithmétiques des applications mirroir*, PhD thesis (2011), available online at http://math.univ-lyon1.fr/ delaygue/articles/PhD_Thesis_delaygue.pdf.

[19] E. Delaygue, *Critère pour l'intégralité des coefficients de Taylor des applications miroir*, J. Reine Angew. Math. **662** (2012), 205–252.

[20] E. Delaygue, *A criterion for the integraity of the Taylor coefficients of mirror maps in several variables*, Adv. Math., **234** (2013) 414–452.

[21] E. Delaygue, *Arithmetic properties of Apéry-like numbers*, preprint (2013), arXiv:1310.4131v1 [math.NT], 22 pages, to appear in Compos. Math.

[22] E. Delaygue, T. Rivoal, and J. Roques, *On Dwork's p-adic formal congruences theorem and hypergeometric mirror maps*, preprint (2013), arXiv:1309.5902v1 [math.NT], 80 pages, to appear in Memoirs Amer. Math. Soc.

[23] P. Deligne, *Intégration sur un cycle évanescent*, Invent. Math. **76** (1983), 129–143.

[24] B. Dwork, *p-adic cycles*, Inst. Hautes Études Sci. Publ. Math., **37** (1969), 27–115.

[25] B. Dwork, *On p-adic differential equations. IV. Generalized hypergeometric functions as p-adic analytic functions in one variable*. Ann. Sci. École Norm. Sup. (4), **6** (1973), 295-315.

[26] B. Dwork, G. Gerotto, and F. Sullivan, An introduction to G-functions, Annals of Mathematics Studies **133**, Princeton University Press, 1994.

[27] S. Fischler and T. Rivoal, *On the values of G-functions* Comment. Math. Helv. **29** (2014), 313–341.

[28] P. Flajolet, *Ambiguity and transcendence*, Automata, languages and programming (Nafplion, 1985), 179–188, Lecture Notes in Comput. Sci., **194**, Springer, Berlin, 1985.

[29] P. Flajolet, *Analytic Models and Ambiguity of Context-Free Languages*, Theor. Comput. Sci. **49** (1987), 283–309.

[30] P. Flajolet and R. Sedgewick, Analytic combinatorics, Cambridge University Press, 2009.

[31] H. Furstenberg, *Algebraic functions over finite fields*, J. Algebra **7** (1967) 271–277.

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

[33] N. Katz, *Algebraic solutions of differential equations*. Invent. Math. **18** (1972), 1-118.

[34] N. M. Katz, *Nilpotent connections and the monodromy theorem: applications of a result of Turrittin*, Inst. Hautes Études Sci. Publ. Math. **35** (1970), 175–232.

[35] M. Kontsevich, *Periods*, Journée annuelle de la SMF, 1999.

[36] M. Kontsevich and D. Zagier, Periods, in *Mathematics unlimited—2001 and beyond*, pp. 771–808, Springer-Verlag, 2001.

[37] C. Krattenthaler and T. Rivoal, *Multivariate p-adic formal congruences and integrality of Taylor coefficients of mirror maps*, Séminaire et Congrès **23** (2011), 301–329. Actes de la conférence Théories galoisiennes et arithmétiques des équations différentielles (CIRM, septembre 2009).

[38] E. Landau, *Sur les conditions de divisibilité d'un produit de factorielles par un autre*, collected works, **I**, page 116. Thales-Verlag (1985).

[39] E. Lucas, *Sur les congruences des nombres eulériens et les coefficients différentiels des fonctions trigonométriques, suivant un module premier*, Bull. Soc. Math. France **6** (1877–1878), 49–54.

[40] A. Malik and A. Straub, *Divisibility properties of sporadic Apéry-like numbers*, Research in Number Theory **2** (2016), 1–26.

[41] R. J. McIntosh, *A generalization of a congruential property of Lucas*, Amer. Math. Monthly **99** (1992), 231–238.

[42] R. J. McIntosh, *An asymptotic formula for binomial sums*, J. Number Theory **58** (1996), 158–172.

[43] R. Meštrović, *Lucas' theorem: its generalizations, extensions ans applications (1878–2014)*, preprint (2014), arXiv:1409.3820v1.

[44] F. Rodriguez-Villegas, *Integral ratios of factorials and algebraic hypergeometric functions*, preprint (2007), arXiv:0701.1362v1 [math.NT], 3 pages.

[45] E. Rowland, R. Yassawi, *Automatic congruences for diagonals of rational functions*, Journal de Théorie des Nombres de Bordeaux **27** (2015), 245–288.

[46] K. Samol, D. van Straten, *Dwork congruences and reflexive polytopes*, preprint (2009), arXiv:0911.0797v1 [math.AG], 14pp.

[47] J.-P. Serre, Local Fields, Springer-Verlag, 1980.

[48] C. Siegel, *Über einige Anwendungen diohantischer Approximationen*, Abhandlungen Akad. Berlin 1929.

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

[50] R. Stanley, *Differentiably finite power series*, European J. Combin. **1** (1980), 175–188.

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

[52] M. Waldschmidt, *Transcendence of periods: the state of the art*, Pure Appl. Math. Q. **2** (2006), 435–463.

B. Adamczewski, CNRS, Université de Lyon, Université Lyon 1, Institut Camille Jordan, 43 boulevard du 11 novembre 1918, 69622 Villeurbanne Cedex, France • *E-mail :* `Boris.Adamczewski@math.cnrs.fr`

Jason P. Bell, Department of Pure Mathematics, University of Waterloo, Waterloo, ON, Canada, N2L 3G1 *E-mail :* `jpbell@uwaterloo.ca`

E. Delaygue, Université de Lyon, Université Lyon 1, Institut Camille Jordan, 43 boulevard du 11 novembre 1918, 69622 Villeurbanne Cedex, France • *E-mail :* `delaygue@math.univ-lyon1.fr`