ON THE VANISHING COEFFICIENTS OF ALGEBRAIC POWER SERIES

SHAOSHI CHEN, PIETRO CORVAJA, AND UMBERTO ZANNIER

Abstract. Given an *algebraic* power series $f(x) = \sum_{n=0}^{\infty} a_n x^n$, we study the distribution of the set $Z_f := \{n : a_n = 0\}$, in analogy with the Skolem-Mahler-Lech theorem for *rational* power series. Over a field of positive characteristic, the general pattern of vanishing coefficients of power series has been determined by Derksen [7] for rational functions and later generalized to the case of algebraic functions by Adamczewski and Bell [1]. In this paper we will investigate the case of characteristic zero, as in the original context.

We have two kinds of results. First, we bound by N^c, $c = c_f < 1$, the number of $n \leq N$ in Z_f outside suitable arithmetical progressions. This supersedes past results by various authors. Our approach is different from previous ones and goes through a new estimate for the number of 'small' values of exponential polynomials in intervals; this has independent motivation, as it answers open questions previously raised, e.g. in the book [9]. The method will also deliver similar bounds for the distribution of Z_f along *finite polynomial sequences* rather than *intervals*.

This technique relies on estimates for certain exponential sums, in turn depending on deep results from transcendental number theory.

Second, we investigate when the p-adic method of Skolem may possibly apply to irrational algebraic series. We prove that, contrary to the rational case, for any such series the approach *a priori* may work at most for finitely many primes, and we give examples when it definitely fails. But we also obtain some positive results, and criteria which often allow to decide effectively whether this principle does or does not apply, for a given function.

1. Introduction

Let $f(x) = \sum_{n=0}^{\infty} a_n x^n$ be a power series with coefficients in a field K. Especially when the coefficients a_n have arithmetical significance, it happens to be of interest to have information about the set of integers n for which a_n vanishes, a set which we denote by Z_f:

$$Z_f := \{n \in \mathbb{N} : a_n = 0\}. \tag{1.0.1}$$

A natural case, very relevant in the theory of Diophantine equations, occurs for series representing a rational function, in $K(x)$. In that situation the coefficients satisfy a nontrivial linear recurrence relation $\sum_{i=0}^{l} c_i a_{n-i} = 0$, valid for all large n, where the c_i lie in K and $c_0 \neq 0$. In turn, the solutions of such recurrences may be represented as values at integers of exponential polynomials, i.e. functions of the form

$$z \mapsto E(z) := \sum_{i=1}^{r} P_i(z) \beta_i^z \tag{1.0.2}$$

2010 *Mathematics Subject Classification.* Primary: 11G50. Secondary: 11G99.

Key words and phrases. Algebraic power series, exponential polynomials, Skolem–Mahler–Lech.

Shaoshi Chen was partially supported by the Strategic Priority Research Program of the Chinese Academy of Sciences (No. XDB0510201), the National Key R&D Programs of China (No. 2023YFA1009401), and the NSFC grants (No. 12271511 and No. 11688101).

for polynomials P_i over a finite extension K_1 of K and elements $\beta_i \in K_1^*$, called *roots* of the recurrence. (The values are well-defined *a priori* only for $z \in \mathbb{Z}$ but it is often useful to consider further possible values.)

When K has characteristic 0 (which is the only case we shall consider in this paper), the celebrated *Skolem–Mahler–Lech theorem* (see for instance the books [3], [6], [9], [24], and [25]) describes the structure of the set of natural numbers n with $E(n) = 0$, where E is a given exponential polynomial:

`Skolem-Mahler-Lech (SML) Theorem`: *The set* $\{n \in \mathbb{N} : E(n) = 0\}$ *differs by a finite set from a union of finitely many arithmetical progressions.* [1]

When no ratio β_i/β_j of two distinct *roots* is a root of unity, this easily implies that the whole set of integer zeros is necessarily finite, and so is Z_f for the corresponding rational function.

This conclusion sometimes admits easy proofs (for instance when there is a unique *dominant root* β_i with respect to some absolute value of K_1), but in the most general case it represents a delicate issue, which may be framed into the so-called *dynamical Mordell-Lang context* (see the monograph [3] and the recent survey [22], especially Conjecture 2.5). Skolem gave a proof by basic theory of p-adic analytic functions, which is still the simplest method working generally.[2] Then he applied this to certain Diophantine equations, obtaining elegant results. The subtlety of the context is also witnessed by the fact that no general algorithm is known to compute the said finite set (when the data are algebraic numbers). This is a longstanding open problem, now called *the Skolem Problem* (see a recent progress in [14]).

Now, a natural extension of this issue occurs when the series $f(x)$ represents an *algebraic* function of x, that is, it satisfies some polynomial equation $Q(x, f(x)) = 0$, where $Q \in K[x, y]$ is nonzero. The former case of rational functions is recovered by imposing $\deg_y Q = 1$.

This more general situation raises substantial new obstacles compared to the case of rational functions. The coefficients a_n continue to satisfy linear recurrences, however now with (usually) non-constant (polynomial) coefficients. This causes the loss of formulae like (1.0.2) above, and in turn, the method of Skolem does not work generally anymore in an evident way. Despite this, one could expect (or conjecture) that the same conclusion of the Skolem-Mahler-Lech theorem still holds; this is also asked by Rubel (see Problem 16 in [18]) for so-called *D-finite power series* (that satisfy linear differential equations with polynomial coefficients). However there are a wealth of easily written examples for which, to our knowledge, no available method is able to prove this (see also the final remark in the Appendix). To give a flavour of what may happen, here is one such simple instance:

Example 1.1. Consider the sequence

$$a_n = \binom{2n}{n} + (3 + \sqrt{-7})^n + (3 - \sqrt{-7})^n + Q(n), \tag{1.1.1}$$

where Q is a polynomial. This corresponds to a function $f(x)$ of the shape $f(x) = \sum_{n=0}^{\infty} a_n x^n = \frac{1}{\sqrt{1-4x}} + \frac{2-6x}{1-6x+16x^2} + R(x)$, where R is a rational function with denominator being a power of $1 - x$. Note that, setting $3 + \sqrt{-7} = 4\exp(i\theta)$ for a $\theta \in \mathbb{R}$, the sum of the second and third terms equals $4^n(2\cos n\theta)$, whereas the first

[1] See Derksen's paper [7] for the subtle and quite different case of positive characteristic, treated further in [1].

[2] Other proofs follow from hard Diophantine Approximation, see the remarks after Theorem 3.1.

term asymptotically behaves like $\frac{2\cdot 4^n}{\sqrt{\pi n}}$. Now, a number $\cos(n\theta), n \in \mathbb{N}$, may well approach suitably $-1/\sqrt{\pi n}$ for certain values of n, as is expected by heuristic of Diophantine Approximation. So it appears that we can not exclude the vanishing by mere asymptotic estimates.

As a consequence of the main theorem below, we obtain that for large enough N and for every interval of length N, the number of indices n in such an interval with vanishing a_n is bounded by N^c for some $c < 1$.

Actually, *for this specific example* we shall prove in an Appendix in the last section of this paper, by a different method, that the number of $n \leq N$ with vanishing a_n is asymptotically bounded as $\ll \log^{1+\epsilon} N$ for every $\epsilon > 0$. Still, even this different special method does not yield finiteness, and for a slightly more complicated example as

$$a_{2n} + a_n + R(n),$$

where a_n is as in (1.1.1) and $R(n)$ is a(n exponential) polynomial, the method used in the Appendix does not generally apply at all, although of course Theorem 1.2 below does apply.

1.1. **Main results.**

The general question has been the object of previous works; we slightly postpone a description of this, and say immediately that in this paper we adopt two viewpoints.

1. Firstly, we shall combine an analysis of small values of exponential polynomials (carried out in Section 3) with an asymptotic expansion (done in Section 4) for coefficients, to derive a result in the same spirit of the Skolem-Mahler-Lech theorem, in which, however, the *finite set* is replaced by a *sparse set*, in the sense that it contains at most N^c elements in each interval of length N, for a $c < 1$ and every large N.

Theorem 1.2. *Let* $\mathrm{char}(K) = 0$ *and let* $f(x) = \sum_{n=0}^{\infty} a_n x^n \in K[[x]]$ *be algebraic over* $K(x)$*. Then* Z_f *is the union of finitely many arithmetical progressions and a set* $\mathcal{A}$ *such that, for a* $c = c_f < 1$ *and for every large enough* N*, there are at most* N^c *elements of* $\mathcal{A}$ *in any interval of length* N*.*

As a simple corollary, we easily deduce for instance that:

A power series $\sum_{n=0}^{\infty} a_n x^n$ *such that* $a_p = 0$ *for all prime numbers* p *is either transcendental or has all coefficients vanishing along an arithmetical progression.*

And for such conclusion it even suffices to assume $a_p = 0$ for all primes in $[b, 2b]$ for infinitely many positive integers b. (See below for an analogue for a_{p^2}.)

Remark 1.3. (i) **About the relevant arithmetical progressions**. Here by arithmetical progression we mean a set of the form $l + q\,\mathbb{N}$, for some integer $l \geq 0$ and some positive integer q.

The proof will show that one can choose a common modulus q for all the arithmetical progressions in which a_n is identically zero. Such a modulus is any multiple of the orders of the roots of unity appearing as a ratio of two distinct singularities of the algebraic function represented by $f(x)$. In particular, *there are only finitely many maximal relevant progressions and these are effectively computable* if the data of the problem are effectively given (i.e. if the irreducible equation satisfied by f is given with coefficients over a computable field).

Concerning the above example when $a_p = 0$ for every prime p, if q is a suitable modulus, the set Z_f contains all the progressions $q\,\mathbb{N} + r$ with $\gcd(q, r) = 1$.

(ii) **Asymptotic**. Working over $K = \mathbb{C}$, the proof will also show that in fact for n not in Z_f, restricting n to suitable finitely many progressions, the a_n will satisfy an approximated equality of the shape $|a_n| = n^{\kappa+o(1)}b^n$, for a $\kappa \in \mathbb{R}$ and a $b > 0$, again with the exception of a set with the properties of $\mathcal{A}$.

(iii) **Vanishing along subsequences**. The method extends so as to give similar estimates for the number of vanishing a_n with n varying in a polynomial sequence $n = g(m)$ for $1 \leq m \leq N$ where $g \in \mathbb{Z}[x]$ is a polynomial, even with uniformity, i.e. it suffices that g has bounded degree and leading coefficient bounded by a small enough power of N.

More precisely, concentrating for simplicity on the case when Z_f does not contain whole progressions (by item (i) this causes no substantial loss of generality) for instance we have:

Theorem 1.4. *Let K be a field of characteristic 0 and let $f(x) = \sum_{n=0}^{\infty} a_n x^n \in K[[x]]$ be algebraic over $K(x)$ and such that Z_f does not contain any arithmetical progression. For any integer $e > 0$ there exist $l > 0$ and $c < 1$, depending only on e, f, with the following property: for all sufficiently large integers N, for any polynomial $g \in \mathbb{Z}[x]$ of degree e with positive leading coefficient bounded by N^l, there are at most N^c integers $n \in [1, N]$ with $a_{g(n)} = 0$.*

As a very special consequence, we obtain 'uniform sparseness' of Z_f along arithmetical progressions $\{qn + r\}$, for $n \leq N$, provided $0 < q \leq N^l$.

Also, as a simple application similar to the one stated after Theorem 1.4, this would prove for instance that:

If all coefficients a_{p^2} vanish for all prime numbers p, then either the series is transcendental or $a_n = 0$ for n in a whole arithmetical progression.

As we shall stress in the sequel, conclusions of this sort completely escape from previous methods, even thinking of weaker estimates, of mere zero-density.

(iv) **Effectivity**. As to the number c (and also l in the last statement), it is also effectively computable. See the remarks in Section 3 for more on this issue.

As said, the proof of these theorems will involve two main ingredients.

`Asymptotics`. On the one hand, there is the above alluded asymptotic expansion for coefficients, which should be somewhat classical, at any rate concerning the principles for obtaining it, which consist of using Cauchy's theorem applied to suitable contours; several examples occur in old literature. We have no knowledge of a systematic treatment, e.g. in standard books, and we refer to the fairly recent paper [17] for similar expansions. However for the sake of completeness we have reproduced here the proof of what we need, which is rather simple and direct, and also may give further information in special cases.

For instance, for the sequence in (1.1.1), by the formula of Stirling one obtains that $a_n = 2 \cdot 4^n(\cos n\theta + \frac{1}{\sqrt{\pi n}}(1 + \frac{c_1}{n} + \frac{c_2}{n^2} + \ldots))$ for suitable constants $c_1, c_2, \ldots$, in the sense of asymptotic expansions. [3]

Concerning these expansions, it is also to be remarked that they often immediately imply the finiteness of Z_f, i.e. when there is *a unique singularity of $f(z)$ of minimum (complex) absolute value*. In such cases the asymptotic carries a unique dominant term, which excludes vanishing for large n. This feature corresponds to the existence of a so-called *dominant root* (for the complex absolute value) in the cases of linear recurrences and exponential polynomials (see [9] for more). Naturally these cases (both for rational functions and algebraic functions) have little or no weight from

[3] By this we mean $a_n = 2 \cdot 4^n(\cos n\theta + \sum_{j \leq h} \frac{1}{\sqrt{\pi n}} \frac{c_j}{n}) + O(4^n n^{-h-3/2})$ for each $h > 0$.

the present viewpoint, hence, though they are in a sense *generic*, here we consider them to be special and uninteresting.

`Small values`. On the other hand, in general we have to deal with expansions in which several exponential terms have the same maximum absolute value (thus leading to possible cancellations). To treat these situations we shall obtain, and use, a result on the distribution of small values of exponential polynomials which looks novel, and actually seems to be not free of independent motivation, since e.g. in particular it delivers answers to questions raised in the book [9] (see especially p. 34 and the end of p. 35 therein).

To give a simple example, consider again the sequence in (1.1.1). From the above asymptotic one obtains that $a_n = 2 \cdot 4^n \cos n\theta + O(4^n n^{-1/2})$. Such an expression may vanish only if $\cos n\theta$ is suitably small, and this corresponds to a small value of the exponential polynomial $\exp(in\theta) + \exp(-in\theta)$.

Our estimates (for the number of such small values in large intervals) are sometimes best-possible in the sense of growth-type, and rely on deep (and effective) results from transcendental number theory, which seem absent from previous approaches to similar problems (as e.g. those explained in [9], which rely on Diophantine Approximation, however of a different nature). See especially the remarks below after Theorem 3.1.

In the paper, this part, because of its independent motivation, shall be developed in the first section of proofs. It is this kind of results that leads to the mentioned similar distributional results for the zeros of more general sequences.

2. Secondly, we shall investigate for which irrational algebraic functions the p-adic argument of SKOLEM is still possible. This method is not based on p-adic asymptotic, but rather on interpolation of the sequence of coefficients by means of p-adic analytic functions. [4]

Generalizations of such an approach to various contexts of Diophantine Geometry have been carried out in several works, some of which shall be mentioned in the next subsection 1.2. However, regarding the present purpose, the method and such extensions of it seem not to adapt in an obvious way, and to our knowledge the full possibilities have not been studied.

In this paper we shall see that indeed intrinsically *the method cannot be applied generally.* For instance, working over $\overline{\mathbb{Q}}$, for any given *rational* function, the method applies for all but finitely many primes p, whereas for any given *irrational algebraic* function the approach may possibly work at most for finitely many primes (as we shall prove in Section 6).

Nevertheless we have found also some positive examples (see for instance Proposition 1.8), and we have developed sufficient conditions under which the same approach is efficient; in such cases, it delivers a conclusion of the same strength as for rational functions (i.e. proving *finiteness* of Z_f apart from suitable progressions).

We shall also develop some effective criteria for deciding whether, given an explicit algebraic function defined over a computable field, such p-adic method does or does not apply. In particular, as an example we shall prove that the approach cannot work for the functions whose coefficients are as in (1.1.1) above.

[4] We also note in passing that seeking a dominant root for a p-adic valuation has not the same meaning and strength as over $\mathbb{C}$, because a significant asymptotic p-adic expansion for the coefficients seems not available in general. This increases the relevance of the SKOLEM method in the p-adic context.

Our notion of the Skolem method **in the present context**. Before giving any statement in this p-adic context, let us spend a few words so as to make it precise what we mean by the *Skolem method* for the present issues.

We argue exactly as in the rational case. We let p be a prime number, and we denote by $\mathbb{C}_p$ a completion of an algebraic closure of $\mathbb{Q}_p$, with $\mathcal{O} = \mathcal{O}_p$ the valuation ring of $\mathbb{C}_p$, and by $\overline{\mathbb{F}}_p$ an algebraic closure of $\mathbb{F}_p$.

Definition 1.5. *We say that a power series $f(x) = \sum_{n=0}^{\infty} a_n x^n \in \mathbb{C}_p[[x]]$ admits* `analytic interpolation` *if there is a p-adic analytic function $g(x) \in \mathbb{C}_p[[x]]$, converging in $\mathcal{O}_p$, such that $a_n = g(n)$ for every large enough $n \in \mathbb{N}$.*

We denote by Sk_p the set of such $f(x)$.

We say that `the Skolem method may be applied to` *$f(x)$ if there is a $q \geq 1$ such that for each $b = 0, 1, \ldots, q-1$, the function $f_{b,q}(x) := \sum_{n=0}^{\infty} a_{b+nq} x^n$ is in Sk_p.*

We further say that `the restricted Skolem method may be applied to` *$f(x)$ if there are at least a $q \geq 1$ and a $b \in \{0, 1, \ldots, q-1\}$ such that the function $f_{b,q}(x) := \sum_{n=0}^{\infty} a_{b+nq} x^n$ is in Sk_p.*

Remark 1.6. It is readily verified that Sk_p is a vector space over $\mathbb{C}_p$, and actually a module over $\mathbb{C}_p[x]$ that is also stable by differentiation. Then one may ask whether Sk_p actually forms a subring of $\mathbb{C}_p[[x]]$. Using Proposition 6.3 below one may verify that this is not true; anyway the same proposition shows that Sk_p is in a sense "almost" a ring. Since the ring property does not hold, we do not pause further here on this issue.

Replacing $\mathbb{C}_p$ by $\mathbb{C}$. It may be proved that every formal power series in $\mathbb{C}[[x]]$ admits analytic interpolation, which can be derived from the Weierstrass theorem (see [12, page 16, Corollary 1.5.4]). However this complex interpolation cannot be applied as in the Skolem method, since $\mathbb{Z}$ is not contained in any compact subset of $\mathbb{C}$, and hence it is of no use toward our issues (similarly to the case of rational functions).

We shall think of power series with algebraic coefficients. Then we can view them as having coefficients in $\mathbb{C}_p$, varying the prime p. This freedom is very useful in Skolem's original method.

Our criteria involve in particular a notion of *good reduction* for the algebraic curve $Q(x,y) = 0$ corresponding to $f(x)$. This notion, given in Section 6, requires a few explanations. Though they are elementary, for the reader's convenience we give at once a very easy 'naive' notion of good reduction, which is stronger than the mentioned one, so sufficient for illustrating immediately some results.

`Naive notion of good reduction`: Let $Q \in \mathcal{O}[x,y]$ and suppose that Q is irreducible over $\mathbb{C}_p$, of degree > 1 in y, and with nonzero reduction $\bar{Q} \in \overline{\mathbb{F}}_p[x,y]$. *We say that Q, or $f(x)$, has good reduction if $\bar{Q}$ has no factors in $\overline{\mathbb{F}}_p[x,y]$ which are linear in y.*

Of course the case $\deg_y Q = 1$ corresponds to $f(x)$ being a rational function, and hence falls anyway into the SML theorem and is not interesting for us.

We note that a well-known result by Ostrowski (see for instance [25] or [24] for simple proofs) implies that for a given irreducible $Q \in \overline{\mathbb{Q}}[x,y]$ there are only finitely many primes p such that Q does not have good reduction if we embed $\overline{\mathbb{Q}}$ in $\mathbb{C}_p$.

With this notion (and actually with the weaker notion recalled in Section 6) we shall prove in particular the following

Theorem 1.7. *(a) Suppose that the Skolem method may be applied to $f(x)$, relative to p. Then either $f(x)$ is rational or it does not have good reduction.*

(b) For $f \in \overline{\mathbb{Q}}[[x]]$, suppose that the restricted Skolem method may be applied to $f(x)$, relative to p. Then p belongs to a finite set depending only on the singularities of $f(x)$. Moreover there exists a finite set of integers $h > 0$ such that some function of the shape $\sum_{\theta^h=1} \theta^b f(\theta x)$ is either rational or does not have good reduction.

In fact, the proof of the theorem will yield more information on the relevant finite set of primes, and on the dependence on the singularities, and also will provide more consequences with respect to the loss of good reduction.

As mentioned above, we have found some simple instances in which the Skolem method may be applied for irrational algebraic functions: see for instance Example 6.5, giving the following

Proposition 1.8. *[see Example 6.5] Let p be a prime and A be a finite set of algebraic integers $\equiv 1 \pmod p$. For any $a \in A$ let c_a be nonzero algebraic numbers. Then $f(x) = (1-x)^{-3/2} \sum_{a\in A} c_a\sqrt{1+ax}$ is in Sk_p and the set Z_f is finite.*

This seems not obvious to prove directly with other methods. Also it will be clear from the arguments that this can be easily and widely generalized in various ways.

Finally, we give the following explicit negative example, showing an explicit limitation to the Skolem method.

Proposition 1.9. *There exists $f(x) \in \mathbb{Z}[[x]]$, algebraic of degree 2 over $\mathbb{Q}(x)$, such that the restricted Skolem method cannot be applied to f, no matter how we take the prime p. More precisely, this is true for the series corresponding to $f(x) = \frac{1}{\sqrt{1-4x}} + \frac{2-6x}{1-6x+16x^2} + R(x)$, where R is any rational function with denominator a power of $1-x$.*

Note that any such function corresponds to a sequence of coefficients as in (1.1.1), where we observed that there is no known asymptotic analysis which can generally prove $a_n \neq 0$ for all large n. This result shows that we cannot reach such deduction not even by the Skolem p-adic considerations, and not even restricting the sequence to a whole arithmetical progression. (However this does not mean that congruence considerations cannot be helpful; for instance, we remarked in a footnote that looking at the 2-adic digits of n can exclude some infinite sequence of a_n from vanishing. In fact, from that remark we can immediately conclude that *if $a_n = 0$ then the 2-adic order of $Q(n)$ equals the sum of the 2-adic digits of n*.)

1.2. Some precedent results on our general issue.

As we have mentioned above, the general issue has been already considered in a number of past papers. We recall some of these precedents, comparing them with our conclusions.

To start with, we mention a paper of Bézivin [4], where he proved a result somewhat in the spirit of Theorem 1.2 above, however with the weaker conclusion that $\mathcal{A}$ has *asymptotic density* 0, namely it contains $o(N)$ elements up to N.

In fact, he argued with power series more general than algebraic functions, requiring only that they satisfy a linear differential equations with polynomial coefficients (called *D-finite* by Stanley [20]); these series include algebraic functions as a very special subset. Any such differential equation yields a nontrivial linear recurrence $\sum_{i=0}^r c_i(n)a_{n-i} = 0$ for the a_n, with polynomial coefficients $c_i(n)$, like for algebraic functions (whereas the c_i can be taken constant in the case of rational functions).

The nice argument of Bézivin relies on the famous, and difficult, combinatorial theorem of Szemeredi that *a sequence of integers with positive upper density contains arbitrarily long (finite) arithmetical progressions.* With this in hand, assuming that the present $\mathcal{A}$ has nonzero density, Bézivin obtains in particular (finite) arithmetical progressions in it, longer than the length r of the recurrence relation; in fact it is well known that the result by Szemeredi is equivalent to a version of it for finite intervals, and in turn this entails the existence in $\mathcal{A}$ of infinitely many such (finite) progressions, all of the same length and with the same modulus and remainder. At this stage Bézivin uses the recurrence, but now for the sequence restricted to the complete arithmetical progression with that modulus and remainder, which is shown not to increase the recurrence length r. For n large enough so that the leading coefficient of that recurrence cannot vanish at n, the vanishing of the first r terms (obtained by construction) then implies by recursion the vanishing along the whole infinite progression.

Finally, to control such (complete) progressions he uses arguments involving singularities, not far from those that we shall also consider in our proof of Theorem 1.2 (however asymptotic expansions did not appear in his arguments).

Now, despite the several deep quantitative versions of the theorem of Szemeredi obtained after the original proof, until recently, the type of argument adopted by Bézivin will never yield itself an estimate N^c, $c < 1$, for the number of elements of $\mathcal{A}$ up to N, as in the present Theorem 1.2: in fact, a method of Moser [16] constructs an infinite sequence of integers with more than $\gg N^{1-\frac{\kappa}{\sqrt{\log N}}}$ terms up to N, and no three terms in arithmetical progression.

We also note that, disregarding the quality of the asymptotic estimates, no similar argument relying on the theorem of Szemeredi will give any conclusion such as in Theorem 1.4 above (not even of zero density).

Concerning the higher generality of the functions in Bézivin's theorem, we believe that the present arguments for Theorem 1.2 can be carried out too with appropriate modifications for D-finite series, at any rate assuming that there are only regular singularities. However in this paper for several reasons we stick to algebraic power series, both in the analytical and p-adic parts, and we leave a more general analysis to possible interested readers and future papers.

Another subsequent proof of a result in the same spirit as Bézivin's was found independently by Methfessel [15]. This time she argues with sequences satisfying recurrences of much more general type, and derives a suitable conclusion, again with a zero set included in a finite union of arithmetical progressions plus a set of density zero. She uses again the theorem of Szemeredi, in a way similar to Bézivin's.

Further, Bell, Chen, and Hossain [2] have studied methods related to the one of Skolem in a dynamical context. Once more with an application of the theorem of Szemeredi (similar to the former ones) they are able to obtain a density zero conclusion even concerning D-finite series and the set of n such that a_n lies in a prescribed finitely generated subgroup of K^* (here they also use deep results from Diophantine Approximation applied to S-unit theory).

`Concerning the SML theorem`: We conclude this brief description by recalling that the Skolem-Mahler-Lech theorem has been itself the object of several evolutions in Diophantine Geometry, due to various authors, like Chabauty, Demjanenko-Manin, Coleman, and others, until recently, with a sophisticated version by Minjong Kim, which has many startling applications by still other authors toward finding effectively the rational points on certain curves. (We do not give references here since the topic falls far from the present themes, but see Serre's book [19] for a clear illustration of past applications to modular curves.)

A version of the SML Theorem in the context of algebraic groups appears (as a tool) in the paper [23], studying the set of integers n such that g^n lies in a given subvariety X of an algebraic group G, where $g \in G$ is given. The original SML theorem is in fact recovered as the case when G is a product $\mathbb{G}_{\mathrm{a}} \times \mathbb{G}_{\mathrm{m}}^s$ and X is a hypersurface.

The method has also been studied in the context of dynamics (like in the above quoted paper [2]), with further applications to various types of recurrences; see the book [3] for several subtle results in such direction.

However these investigations regard more the context of Diophantine Geometry, whereas it seems that the method has not been analyzed as we do here, for studying Z_f in the general case of algebraic functions.

In the situation of positive characteristic, the SML structure of vanishing coefficients of rational functions is no longer true and need be replaced by so-called *automatic sets*. This was first investigated by Derksen for rational functions [7] and later generalized to the case of algebraic power series [1].

Finally, we remark that it would be not free of interest to investigate the method also in the more general context of D-finite series. It seems that only a part of the present arguments would adapt in a straightforward way.

2. Some notation

In this section we introduce a little notation.

As before, let $Q(x, f(x)) = 0$ be the minimal equation satisfied by $f(x)$ over $K[x]$. We let $K_0 \subset K$ be the field generated by the coefficients of Q. We may assume that K_0 and K are subfields of $\mathbb{C}$, or also, in the p-adic case, of $\mathbb{C}_p$ (i.e. a completion of an algebraic closure of $\mathbb{Q}_p$).

The leading coefficient of $Q(x, y)$, considered as a polynomial in y, contains so to say the 'polar' singularities of the algebraic function of x defined by that equation. Here we note that upon multiplying $f(x)$ by this coefficient, the new function will satisfy a *monic* equation over $K[x]$, so will be integral over that ring. This normalization is often useful.

The other possible singularities occur at branch points of the coordinate function x on the algebraic curve defined by $Q = 0$. The (finite) branch points are roots of the discriminant of Q (again, as a polynomial in y). In this way we obtain a finite set, denoted Ξ, of possible singularities.

By replacing x by a positive power of it at the outset, we can assume that 0 is not a branch point, so $\Xi \subset \mathbb{C}^*$.

The series $f(x)$, considered in $\mathbb{C}[[x]]$ has a finite positive radius of convergence, denoted $R > 0$, so is analytic in the open disk

$$D(R) = D(0, R^-) := \{z \in \mathbb{C} : |z| < R\}.$$

Similarly it holds in the p-adic case, as we shall recall.

But it can be analytically continued along any simply connected region containing $D(R)$ but not containing any of the (possibly) singular points mentioned above. Of course, the situation here is different in the p-adic case. We also define $\Xi(f) = \Xi \cap \{|z| \geq R\}$ as the set of singularities outside the open disk of convergence of f.

3. Small values of exponential polynomials

Just as the Skolem-Mahler-Lech theorem describes the zeros at integers of an exponential polynomial, here we study the distribution of the 'small' values of such polynomials, in an appropriate sense.

We shall use the familiar notation $e(\theta) := \exp(2\pi i\theta)$, where $i^2 = -1$ and we shall freely think of θ either as a point on the unit circle, or as a real number (considered modulo $\mathbb{Z}$).

For the present issues, we shall restrict to objects defined over the field $\overline{\mathbb{Q}}$ of algebraic numbers, for reasons made more explicit in the remarks below. And we assume that the field $\overline{\mathbb{Q}}$ of algebraic numbers is embedded in $\mathbb{C}$.

We shall prove the following theorem, where we say as usual that nonzero complex numbers $\alpha_1, \ldots, \alpha_r$ are *multiplicatively independent* if there is no relation $\prod_{i=1}^r \alpha_i^{m_i} = 1$ with integers m_i not all zero.

Theorem 3.1. *Let $P \in \overline{\mathbb{Q}}[x_1^{\pm 1}, \ldots, x_r^{\pm 1}]$ be nonzero, and let $\alpha_1, \ldots, \alpha_r$ be multiplicatively independent nonzero algebraic numbers. Also put $A = \max|\prod \alpha_j^{m_j}|$ over the monomials occurring in $P(\alpha_1, \ldots, \alpha_r)$, and let $\delta > 0$. Then there exists a positive $c = c(\delta, P, \alpha_1, ..., \alpha_r) < 1$ such that, for all sufficiently large integers N, and for all integers $v \geq 0$, the number of integers $n \in [1, N]$ with $|P(\alpha_1^{n+v}, \ldots, \alpha_r^{n+v})| \leq n^{-\delta} A^{n+v}$ is at most N^c.*

The following is a direct easy consequence, for linear recurrences:

Corollary 3.2. *Let $L(n) = \sum_{l=1}^s \gamma_l \beta_l^n$, where $\gamma_l, \beta_l \in \overline{\mathbb{Q}}^*$ are such that no ratio β_l/β_h, $l \neq h$, is a root of unity. Also put $B = \max|\beta_l|$, and let $\delta > 0$.*

Then there exists a positive $c = c(\delta, L) < 1$ such that, for all sufficiently large integers N, and for all integers $v \geq 0$, the number of integers $n \in [1, N]$ with $|L(n + v)| \leq n^{-\delta} B^{n+v}$ is at most N^c.

Before proving Theorem 3.1, we immediately list a number of remarks.

Remark 3.3. (i) **Necessity of assumptions**. The assumption of multiplicative independence in the theorem cannot be removed, as may be shown by easy examples. Also, it is easy to reduce the most general case to this assumption, on expressing the group $\{\alpha_1^{n_1} \cdots \alpha_r^{n_r} \mid n_1, \ldots, n_r \in \mathbb{Z}\}$ as a product of a free abelian group and a finite torsion group of roots of unity. (This will be done for the proof of the corollary.) The result will be that, after writing $\mathbb{Z}$ as a finite union of suitable arithmetic progressions, similar estimates hold on each of them. This is very well known in problems involving linear recurrences.

The assumption that the α_l are algebraic is also necessary for a bound of this strength: see part (iv) below (and see (v) for the transcendental case).

(ii) **Other inequalities**. Note that for all $n > 0$ we have the (trivial) estimate $|P(\underline{\alpha}^n)| := |P(\alpha_1^n, \ldots, \alpha_r^n)| \ll A^n$, where the implicit constant depends only on P. Regarding the converse inequality $|P(\underline{\alpha}^n)| \gg A^n$, it is easy to prove that it holds for infinitely many n (and much more). If we look at *all* integers n (with a possible finite number of exceptions), it still holds in the *trivial* case when there is a unique (dominant) monomial in $P(\underline{\alpha})$ with maximum absolute value A. But otherwise the various monomials in $P(\underline{\alpha}^n)$ with absolute value A^n could lead to cancellation for special values of n. The present result gives a quantitative shape to the assertion that a cancellation of order at least $n^{-\delta}$ can occur only 'very rarely'. (See (iv) in this series of remarks for examples showing that the exceptions cannot be generally avoided.)

On the other hand, using the Schmidt Subspace theorem (in the versions of Schlickewei) it can be proved (as done e.g. by Evertse, van der Poorten, Schlickewei) that $|P(\alpha_1^n,\dots,\alpha_r^n)| \gg_\epsilon A^{n(1-\epsilon)}$ for any $\epsilon > 0$ and for *all* integers n for which the value is nonzero (which may happen only finitely many times).[5] However this inequality, though deep and very useful and meaningful in Diophantine Geometry, is somewhat different from the present one and less suitable for certain special applications, like the one we have in mind here.

Answers to open issues. Still other significant inequalities are true, and we refer to the book [9] for details and references to these results. In particular, at the bottom of page 35 of [9], the authors write *"It would be interesting to obtain the same result for a bounded function ψ"*. Translating from their notation to the present one, this means to bound the number of integers $n \le N$ such that $|P(\alpha_1^n,\dots,\alpha_r^n)| \le A^n n^{-k}$ by a quantity which is $o(N)$. The present result reaches this goal, moreover with additional generality and precision of the bound. The authors of [9] further say (see the last two lines of page 35) that *possibly* a combination of their Theorem 2.5 with Szemerédi's theorem could provide that $|P(\alpha_1^n,\dots,\alpha_r^n)| \ge A^n n^{-k}$ for almost all $n \le N$. This is equivalent to the former statement, and is a very special immediate consequence of our results. Here we avoid the use of the deep theorem of Szemerédi, and therefore we avoid the weakness of the quantitative estimates coming from it. Simultaneously, we are able to treat polynomial subsequences, which escape completely from methods relying on Szemerédi's theorem.

(iii) **Effectivity**. A suitable number $c < 1$ may be effectively computed in terms of the other data, as can be seen from the proof; similarly for the minimal magnitude of the N for which the conclusion holds. A certain uniformity in these estimates, in terms of P, is also possible. Also, surely our arguments can be quantitatively refined in these directions, however we have not pursued in this kind of analysis, except for introducing the parameter v.

(iv) **Quality of the bounds**. Leaving aside the issue of how small one can take c, the result is qualitatively best-possible, in the sense that *we cannot generally estimate the number of exceptions by a function growing less than $N^{1/2}$*.

In fact, let for instance $r = 1$, $P(x_1) = x_1 - 1$, and let $\alpha = \alpha_1 = (3+4i)/5$ so $A = |\alpha| = 1$, and we may write $\alpha = e(\theta)$, where $\theta \in \mathbb{R}$ is easily proved to be irrational. We have $|P(\alpha^n)| = |e(n\theta) - 1| \ll ||n\theta||$, where here $||t||$ denotes the distance of t from the nearest integer. Now pick any large N and partition the interval $[0,1)$ into $N_1 := [N^{1/2}]$ subintervals of equal length. Then there are at least $M := [N/N_1]$ values of $n \in [1,N]$ such that $n\theta$ modulo 1 falls in the same subinterval. Enumerate these integers as $0 < n_1 < n_2 < \dots < n_M \le N$. Then the integers $m_l := n_l - n_1$, $l = 2,\dots,M$, are pairwise distinct, lie in $[1,N]$ and satisfy $||m_l\theta|| \le N_1^{-1}$. Hence $|P(\alpha^{m_l})| \ll N^{-1/2}$, whereas $M \ge N^{1/2} - 1$. Therefore, with any definite choice of $\delta < 1/2$, this proves that we cannot avoid a number of exceptions at least $N^{1/2} - 2$. (Refinements on this kind of idea allow for much more general Laurent polynomials P.)

This kind of argument also shows that the assumption that the α_l are algebraic cannot be removed. Indeed, with the same choice of P, let for instance $\lambda = \sum_{n=0}^{\infty} 10^{-n!}$ be the celebrated *Liouville constant*; if $q_m = 10^{m!}$, we have $||q_m\lambda|| = q_m^{-(m+1)} + q_m^{-(m+1)(m+2)} + \dots \le q_m^{-m}$. Letting now $\alpha = \alpha_1 = e(\lambda)$, we have for every integer $l > 0$, $|\alpha^{lq_m} - 1| \ll ||lq_m\lambda|| \ll lq_m^{-m}$, which is $< (lq_m)^{-1}$

[5] This method, though ineffective, actually allows much more general results, e.g. allowing the exponent of α_i to depend on i.

provided $l < q_m^{(m-1)/2}$. There are at least $q_m^{(m-1)/2} - 1$ such integers l, and the corresponding lq_m are $\leq q_m^{(m+1)/2}$. Since for any $c < 1$ we have $q_m^{(m-1)/2} - 1 > q_m^{c(m+1)/2}$ for all large m, this shows that the conclusion of the theorem becomes false (for every $\delta < 1$) for this (and similar) number(s) α admitting sufficiently excellent rational approximations. [6]

On the other hand, to have a fairly realistic quantification for a suitable c (in term of δ and the other data) seems a very difficult problem, related (as in the present example) to lower bounds for linear forms in logarithms of algebraic numbers; the known results (which we shall use in our arguments), deep as they are, do not seem to allow an estimate near to the expectations.

(v) **Density results**. As it will clearly appear from the proofs (see especially the NOTE therein), it would be easier to show e.g. that *the set of integers n such that $|P(\alpha_1^n, \ldots, \alpha_r^n)| \leq n^{-\delta} A^n$ has density* 0. In particular, to achieve such weaker conclusion would not require any deep result on lower bounds for linear forms in logarithms of algebraic numbers. This is especially relevant if we deal with transcendental quantities α_l. The method still allows some quantification. (The mere conclusion about density follows also from Theorem 2.6, p. 34 of [9], however with a different argument, and follows also from the suggestions given therein regarding the use of the difficult theorem of Szemeredi on arithmetical progressions. In any case, for general polynomial subsequences, to be mentioned in a moment, those methods break down even concerning mere density.)

Arithmetical Progressions and Polynomial subsequences. We further remark that a completely similar argument would estimate by $\ll N^c$ the number of integers $n \in [1, N]$ such that $|P(\alpha_1^{un+v}, \ldots, \alpha_r^{un+v})| \leq n^{-\delta} A^{un+v}$, *uniformly* in the positive integers $u < N^\kappa$, for a small enough $\kappa > 0$, depending on δ. That is, we may estimate the small values along arithmetical progressions, with a certain uniformity in the modulus. Even more generally, using the method of Weyl to estimate exponential sums, we can replace the linear $un + v$ by $g(n)$, where g is any non-constant polynomial of bounded degree and leading coefficient bounded by N^κ. More precisely, we have the following result, which we shall use for Theorem 1.4 (in the same way as Theorem 3.1 is used for Theorem 1.2):

Theorem 3.4. *Let $P, \alpha_1, \ldots, \alpha_r, A$ be as in Theorem 3.1, and let $e > 0$ be an integer. There exist positive numbers $l, \kappa, h > 0$ depending only on $e, P, \alpha_1, ..., \alpha_r$, with the following property: for all sufficiently large integers N, for any polynomial $g \in \mathbb{Z}[x]$ of degree e with positive leading coefficient bounded by N^l, and for any $\epsilon > N^{-\kappa}$, the number of integers $n \in [1, N]$ with $|P(\alpha_1^{g(n)}, \ldots, \alpha_r^{g(n)})| \leq \epsilon A^{g(n)}$ is at most $\epsilon^h N$.*

For clarity, we shall first prove Theorem 3.1 and then indicate in detail the modifications needed for this much more general conclusion.

Proof of Theorem 3.1. We start with a few easy but useful normalizations. Let P_1 be the part of P made up with monomials which, evaluated at $\underline{\alpha}$, have modulus A. Then $|P(\underline{\alpha}^{n+v})| = |P_1(\underline{\alpha}^{n+v})| + O(A_1^{n+v})$, where $0 \leq A_1 < A$. Therefore to prove

[6] This also shows that our theorem implies that $e(\lambda)$ is transcendental, which does not seem immediate to obtain directly. *A posteriori* this is not surprising because the proof of Theorem 3.1 uses deep results on lower bounds for linear forms in logarithms of algebraic numbers, which directly would also easily imply the stated transcendency. We add that any deep result can be avoided in this argument if we replace the Liouville constant with numbers admitting even better rational approximations, e.g. of the strength $0 < |\lambda - (p/q)| < \kappa^q$ with arbitrarily small positive κ.

the theorem we can replace P with P_1, and hence we may assume that all the monomials of P, evaluated at $\underline{\alpha}$, have modulus A. We may divide by a monomial and assume that $A = 1$, so $P_1(x_1, \dots, x_r)$ now is a linear combination of Laurent monomials, which evaluated at $\underline{\alpha}$ have absolute value 1. These monomials evaluated at $\underline{\alpha}$ generate a multiplicative subgroup of $\overline{\mathbb{Q}}^*$, which is torsion-free, since the α_l are multiplicatively independent: in fact, any element of such subgroup is itself a monomial evaluated at $\underline{\alpha}$, and if a power of this value is 1, the monomial must be identically trivial by the assumption. Thus the said multiplicative group is free abelian and finitely generated, and all its elements have modulus 1. Let then $e(\theta_1), \dots, e(\theta_p)$ be a basis for it, where the θ_l are real numbers (or rather elements of $T := \mathbb{R}/\mathbb{Z}$) which are $\mathbb{Z}$-linearly independent modulo $\mathbb{Z}$. Then each monomial appearing in $P(\underline{\alpha})$ may be expressed as a Laurent monomial in the $e(\theta_l)$; note that no two (distinct) monomials can be equal, because otherwise the α_l would be multiplicatively dependent.

Hence, after this normalization, we may directly suppose that $|\alpha_l| = 1$ for $l = 1, \dots, r$, that $p = r$, and that putting now $\alpha_l = e(\theta_l)$, the θ_l are real numbers which are $\mathbb{Z}$-linearly independent modulo $\mathbb{Z}$. Of course the $2\pi i\theta_l$ are determinations for the logarithms $\log \alpha_l$ of the algebraic numbers α_l. Also, multiplying P by a monomial $(x_1 \cdots x_r)^e$ with large enough e does not affect the statement, so we may assume that P is a polynomial.

We perform a final normalization: by replacing $\theta_1, \dots, \theta_r$ resp. by $a_1\theta_1, \theta_2 + a_2\theta_1, \dots, \theta_r + a_r\theta_1$, where $a_1, \dots, a_r$ are suitable coprime positive integers, we may assume that $P(x_1, \dots, x_r)$ *has a unique term of maximal degree in* x_1. Indeed, the exponents of x_1 in the terms appearing in $P(x_1^{a_1}, x_2x_1^{a_2}, \dots, x_rx_1^{a_r})$ are given by distinct linear forms in r variables, evaluated at $(a_1, \dots, a_r)$, and it suffices to find the coprime integers a_i so that the values of these linear forms at $(a_1, \dots, a_r)$ remain distinct.

For the torus $T := \mathbb{R}/\mathbb{Z}$ and for $\underline{\xi} := (\xi_1, \dots, \xi_r) \in T^r$, we set $F(\underline{\xi}) := P(e(\xi_1), \dots, e(\xi_r))$. Then, for a 'small' positive number $\epsilon > 0$, we consider the real positive function defined on T^r by

$$\varphi(\underline{\xi}) = \varphi(\xi_1, \dots, \xi_r) = \varphi_\epsilon(\xi_1, \dots, \xi_r) = \frac{1}{\epsilon + |F(\underline{\xi})|^2}.$$

Since $|F(\underline{\xi})|^2 = P(e(\xi_1), \dots, e(\xi_r)) \cdot \bar{P}(e(-\xi_1), \dots, e(-\xi_r))$ (where $\bar{P}$ is obtained conjugating the coefficients of P), this is a C^∞ (in fact a real-analytic) strictly positive real-valued function on T^r and hence admits an absolutely convergent Fourier series

$$\varphi(\underline{\xi}) = \sum_{\mathbf{m}} c_{\mathbf{m}} e(\mathbf{m} \cdot \underline{\xi}), \tag{3.4.1}$$

where $\mathbf{m} = (m_1, \dots, m_r)$ runs through $\mathbb{Z}^r$, where $\mathbf{m} \cdot \underline{\xi}$ denotes the scalar product $\mathbf{m} \cdot \underline{\xi} := m_1\xi_1 + \ldots + m_r\xi_r$, and where

$$c_{\mathbf{m}} = \int_{T^r} \varphi(\underline{\xi}) e(-\mathbf{m} \cdot \underline{\xi}) \mathrm{d}\underline{\xi}. \tag{3.4.2}$$

For fixed P, these quantities depend on ϵ, and we shall need estimates for the $|c_{\mathbf{m}}|$, with some uniformity with respect to ϵ. In the sequel of this proof the symbols $\ll$ shall be understood to imply constants independent of ϵ.[7]

[7] We leave it to the interested reader the task of making more explicit such dependence.

For $\mathbf{m} \neq 0$, let $|\mathbf{m}| := \sup |m_i|$ and say $|\mathbf{m}| = |m_h| > 0$. Integrating by parts s times in (3.4.2) with respect to ξ_h we get

$$c_{\mathbf{m}} = (-2\pi i m_h)^{-s} \int_{T^r} \varphi^{(s)}(\underline{\xi}) e(-\mathbf{m} \cdot \underline{\xi}) \mathrm{d}\underline{\xi},$$

where $\varphi^{(s)}$ denotes the s-th derivative with respect to ξ_h.

Now observe that for any positive C^∞ function g of ξ_h, we have $(1/g)^{(s)} = g_s/g^{s+1}$, where $g_0 = 1$ and $g_{s+1} = g_s' g - (s+1) g_s g'$, so g_s is given by a certain universal polynomial of degree $\leq s$ in the first s derivatives of g. We apply this observation on taking $g = \epsilon + |F|^2$. On the whole of T^r we have $|g(\underline{\xi})| \geq \epsilon$ and $|g_s(\underline{\xi})| \ll_s 1$, since all derivatives of F are bounded independently of $\epsilon < 1$ on T^r. Using these remarks in the last displayed formula, we obtain

$$|c_{\mathbf{m}}| \ll_s |\mathbf{m}|^{-s} \epsilon^{-s-1}, \quad \text{for } 0 < \epsilon < 1,\ \mathbf{m} \neq 0, \text{ and for all } s \geq 0. \tag{3.4.3}$$

Also, equation (3.4.2), and the fact that φ is positive on T^r, yields

$$|c_{\mathbf{m}}| \leq |c_0| = c_0, \tag{3.4.4}$$

and this leads us to the issue of estimating efficiently c_0 in terms of ϵ.

Recall that in view of our normalization we can write $F(\underline{\xi}) = Q_{\underline{\xi}'}(e(\xi_1))$, where $\underline{\xi}' := (\xi_2, \ldots, \xi_r) \in T^{r-1}$ and $Q_{\underline{\xi}'}(x) := P(x, e(\xi_2), \ldots, e(\xi_r))$ is a polynomial whose coefficients are polynomials in $e(\underline{\xi}')$, the leading coefficient being a monomial, hence with constant nonzero absolute value on T^{r-1}.

We can factor $F(\underline{\xi}) = Q_{\underline{\xi}'}(e(\xi_1)) = \gamma \prod_{l=1}^{d} (e(\xi_1) - \rho_l)$, where $d = \deg_{x_1} P$; as said, $|\gamma| = |\gamma_{\underline{\xi}'}|$ is constant as a function of $\underline{\xi}' \in T^{r-1}$. Then, for $0 < t < 1$, the inequality $|F(\underline{\xi})| \leq t$ implies $\min_l |e(\xi_1) - \rho_l|^d \ll |\gamma|^{-1} t \ll t$, and then it is easy to see that the real $\xi_1 \in T$ is restricted to a union of at most d intervals [8] which depend on $\underline{\xi}'$ but have total length $\ll t^{1/d}$. (In fact, the relevant ξ_1 lie in the intersection of the unit circle with a disk of radius $\ll t^{1/d}$ centered at some of the ρ_l.)

It is important here that the implicit constant depends only on F (and not on $\underline{\xi}'$), which in turn is a consequence of the constancy of $|\gamma|$ on T^{r-1}.

Then (taking into account that $\epsilon + t^2$ is increasing in t) we can write

$$\left| \int_T (\epsilon + |F|^2)^{-1} \mathrm{d}\xi_1 \right| \ll \int_0^1 (\epsilon + t^2)^{-1} \mathrm{d}t^{1/d} + 1 + \int_1^\infty t^{-2} \mathrm{d}t.$$

[9] The first integral is bounded by $d^{-1} \epsilon^{\frac{1}{2d}-1} \int_0^\infty u^{\frac{1}{d}-1} (1+u^2)^{-1} \mathrm{d}u$. Here and before the infinite integral is convergent, hence we obtain

$$|c_0| = \left| \int_{T^r} (\epsilon + |F|^2)^{-1} \mathrm{d}\underline{\xi} \right| \leq \sup_{\underline{\xi}' \in T^{r-1}} \left| \int_T (\epsilon + |F|^2)^{-1} \mathrm{d}\xi_1 \right| \ll \epsilon^{\frac{1}{2d}-1}. \tag{3.4.5}$$

Let us now come back to the original issue.

We remark at once that we can replace δ by any smaller number, at the cost of changing suitably c (since the relevant set of integers is decreasing as a function

[8] Here we use a slight abuse of language on identifying the points of T with real numbers; in fact we can view those points and intervals as lying on the unit circle.

[9] This inequality can be easily justified in full precision. However we can replace it by a simpler one. Namely, for every $t_0 < 1$, we can split the integral on the left into two parts according as $|F| \leq t_0$ or not; so the left-hand side is $\ll \epsilon^{-1} t_0^{1/d} + (\epsilon + t_0^2)^{-1}$. Now we optimize by choosing e.g. $t_0 = \epsilon^{\frac{d}{2d+1}}$, leading to $|c_0| \ll \epsilon^{\frac{1}{2d+1}-1}$, which is slightly weaker than (3.4.5) below, but still sufficient for our purposes.

of δ). Therefore later, if needed, we shall assume that δ is small enough to justify certain inequalities.

Let us fix $v \geq 0$, taking into account the opening normalizations and notation. There are at most $N^{1/2}$ integers in the interval $(v, v+N^{1/2}-1]$, hence it suffices to estimate by N^c (some $c<1$) the cardinality of the set

$$\mathcal{A} := \{n \in [v+1, v+N], |F(n\underline{\theta})| \leq N^{-\delta/2}\}, \tag{3.4.6}$$

which is included in the union of the set in the statement with the interval $(v, v+N^{1/2}-1]$.

Let us choose ϵ as any number $\geq N^{-\delta}$. Then, with the above notation, for $n \in \mathcal{A}$ we have $|F(n\underline{\theta})|^2 \leq \epsilon$, hence $\varphi(n\underline{\theta}) \geq (2\epsilon)^{-1}$ for all $n \in \mathcal{A}$.

Summing over $n \in [v+1, v+N]$ in equation (3.4.1) evaluated at $\underline{\xi} := n \cdot \underline{\theta}$, we then get

$$(2\epsilon)^{-1}|\mathcal{A}| \leq c_0 N + \sum_{\mathbf{m}\neq 0} |c_{\mathbf{m}}| \cdot |\sum_{v<n\leq v+N} e(n\mathbf{m}\cdot\underline{\theta})|. \tag{3.4.7}$$

We proceed to estimate the exponential sums on the right. Denoting $\theta_{\mathbf{m}} := \mathbf{m}\cdot\underline{\theta}$, we have the natural (folklore) estimate

$$|\sum_{v<n\leq v+N} e(n\theta_{\mathbf{m}})| \leq \min(N, ||\theta_{\mathbf{m}}||^{-1}), \tag{3.4.8}$$

where as before $||\cdot||$ denotes the natural distance in T. To obtain this, put $n = v+n'$ and sum the geometric partial-sum in n', obtaining $|(e(N\theta_{\mathbf{m}})-1)/(e(\theta_{\mathbf{m}})-1)|$. Now it suffices to take into account that $2||\xi|| \leq |e(\xi)-1| \leq 2$ for $\xi \in T$.

Now the $\mathbb{Z}$-linear independence of the θ_l modulo $\mathbb{Z}$, which we are assuming, comes into the picture. In fact, this says that no $\theta_{\mathbf{m}}$ can be 0 for $\mathbf{m} \neq 0$(as an element of T). This fact itself would not be enough for the estimate we are seeking. For it we have to use that the $2\pi i\theta_l$ are logarithms of algebraic numbers. Then we have strong and deep lower bounds (obtained originally by Alan BAKER and later refined by several authors) for the distances $||\theta_{\mathbf{m}}||$, for nonzero $\mathbf{m} \in \mathbb{Z}^r$.

There are a wealth of possible references for what we need. For instance, as a special case of the inequality in [21, page 6], we derive the existence of a number $q > 0$ depending (effectively) only on the degree and heights of $\alpha_1, \ldots, \alpha_r$, and on the degree of the polynomial P, [10] such that we have

$$||\theta_{\mathbf{m}}|| \gg |\mathbf{m}|^{-q}, \qquad \mathbf{m} \in \mathbb{Z}^r - \{0\}, \tag{3.4.9}$$

where the implied constant also depends effectively on the same quantities. Now, in the inequality (3.4.7) we split the sum over $\mathbf{m} \neq 0$ into two sums S_1, S_2, according as $|\mathbf{m}| < M$ or $|\mathbf{m}| \geq M$, where $M > 1$ is a parameter to be specified later.

In order to estimate the first sum S_1, we use that $|c_{\mathbf{m}}| \leq |c_0|$ in addition to (3.4.8) (where we take the second term in the minimum) and the last displayed inequality (3.4.9). Since the number of relevant vectors $\mathbf{m}$ is at most M^r this yields (in view also of (3.4.5))

$$|S_1| \ll |c_0| M^{r+q} \ll \epsilon^{\frac{1}{2d}-1} M^{r+q}.$$

In order to estimate the second sum S_2, we use inequality (3.4.3), with a suitable parameter s to be chosen later, and the trivial bound N in (3.4.8) for the exponential sums. This yields

$$|S_2| \ll \epsilon^{-s-1} N \sum_{|\mathbf{m}|\geq M} |\mathbf{m}|^{-s} \ll \epsilon^{-s-1} N M^{r-s}.$$

[10] This dependence appears because we have normalized the α_i suitably in terms of P.

Putting together all of these estimates we obtain

$$\begin{aligned} |\mathcal{A}| &\ll c_0 N\epsilon + \epsilon^{\frac{1}{2d}} M^{r+q} + \epsilon^{-s} N M^{r-s} \\ &\ll N\epsilon^{\frac{1}{2d}} + \epsilon^{\frac{1}{2d}} M^{r+q} + \epsilon^{-s} N M^{r-s}. \end{aligned} \tag{3.4.10}$$

In the present setting, on choosing $M = N^{\frac{1}{r+q}}$ we obtain

$$|\mathcal{A}| \ll \epsilon^{\frac{1}{2d}} N + \epsilon^{-s} N^{1+\frac{r-s}{r+q}}. \tag{3.4.11}$$

Further, we can choose $\epsilon := N^{-\delta}$, and this becomes

$$|\mathcal{A}| \ll N^{1-\frac{\delta}{2d}} + N^{1+s\delta+\frac{r-s}{r+q}}.$$

Let us also suppose that $\delta < \frac{1}{(r+q)}$, which can be done without loss of generality, as remarked at the outset. Finally, choose s as any integer $> \frac{r}{1-(r+q)\delta}$.

Then note that with such choices the second term on the right in the last displayed inequality equals $N^{1+\frac{r-s(1-(r+q)\delta)}{r+q}}$.

Under the present choice of s the exponent of N here is < 1, hence the last displayed inequality plainly yields $|\mathcal{A}| \ll N^c$ where $c < 1$ is the maximum between $1 - \frac{\delta}{2d}$ and $1 + \frac{r-s(1-(r+q)\delta)}{r+q}$.

This completes the proof, moreover with additional information as to the possible values of c in terms of δ; more precisely, these remarks prove that, on choosing s large enough, we may take c to be any number larger than $1 - \frac{1}{2d(r+q)}$. □

NOTE. In the former proof we assumed $1 > \epsilon \geq N^{-\delta}$. In fact the above argument gives the same estimate without exactly such lower bound for ϵ, provided we define a set $\mathcal{A}_\epsilon$ (now depending on ϵ) in a slightly different way, though completely similar, compared to (3.4.6), namely:

$$\mathcal{A} = \mathcal{A}_\epsilon := \{n \leq N : |P(\underline{\alpha}^{g(n)})| \leq \epsilon A^{g(n)}\},$$

that is, replacing $n^{-\delta}$ by ϵ. Note that this is convenient and more general, since we can estimate trivially the number of relevant integers n such that $|P(\underline{\alpha}^{g(n)})| \leq n^{-\delta} A^{g(n)}$ for small n, for instance by $N^{1/2}$ for $n \leq N^{1/2}$.

Referring to the above estimates, for instance we may choose $M = \epsilon^{-2}$ in (3.4.10), obtaining $|\mathcal{A}| \ll N\epsilon^{\frac{1}{2d}} + \epsilon^{\frac{1}{2d}-2(r+q)} + \epsilon^{s-2r}N$. We may then take $s \geq 2r+1$ so as to obtain a convenient bound tending to zero with respect to N, and actually more precise than that: in fact we obtain $|\mathcal{A}| \ll N\epsilon^{\frac{1}{2d}} + \epsilon^{\frac{1}{2d}-2(r+q)}$.

For example, this further simplifies to

$$|\mathcal{A}_\epsilon| \ll N\epsilon^{\frac{1}{2d}}, \qquad \text{for } \epsilon > N^{-\frac{1}{2(r+q)}},$$

which would be sufficient also for the present purposes.

We can state (part of) this conclusion as essentially a rephrasement of Theorem 3.1:

Theorem 3.5. *For $P, \alpha_1, \ldots, \alpha_r, A$ as in Theorem 3.1, there exist positive numbers $h, \kappa > 0$ depending only on $P, \alpha_1, ..., \alpha_r$ such that, for all sufficiently large integers N and for any $\epsilon > N^{-\kappa}$, the number of integers $n \in [1, N]$ with $|P(\alpha_1^{n+v}, \ldots, \alpha_r^{n+v})| \leq \epsilon A^{n+v}$ is at most $\epsilon^h N$.*

Moreover it is surely possible to improve somewhat on the exponent $h = 1/2d$ of ϵ appearing above, at any rate under mild assumptions on P. Of course the estimate implicitly requires that $\epsilon^h N \gg 1$, so a lower bound for ϵ of the shape imposed by the hypotheses is unavoidable.

However here we skip going ahead with a kind of analysis so as to optimize the quantities h, κ.

Compare also with Remark (v) above. Even if we miss the deep estimate (3.4.9) coming from Transcendental Number Theory, we can still obtain some non-empty conclusion. Indeed, we can simply *fix* a large enough M and proceed in the same way; for M large and ϵ small all the three terms in (3.4.6) will be small with respect to N, providing 'density 0' conclusions.

With this in mind, let us now go to the proof of Theorem 3.4.

Proof of Theorem 3.4. The proof of this Theorem 3.4 follows exactly the same path as outlined in the previous proof and the present NOTE; the only new point occurs in replacing suitably the easy inequality (3.4.8) by an analogous one when n is replaced by $g(n)$. We offer details for this step.

We shall use the method of Weyl (see for instance [5], Ch. IV, or [13], Ch. 8) to estimate the relevant exponential sums $|\sum_{n\leq N} e(g(n)\theta_{\mathbf{m}})|$, which appear in the above arguments.

In the sequel we shall denote by $\varepsilon_j > 0$ $(j = 1, 2, \ldots)$ sufficiently small positive numbers, dependent on the basic data but independent of N. (The argument shall clarify how these quantities can be chosen.)

For the argument to go through, it will suffice to obtain an estimate for the exponential sum $|\sum_{n\leq N} e(g(n)\theta_{\mathbf{m}})|$, of type $\ll N^{1-\varepsilon_1}$, valid uniformly for the nonzero vectors $\mathbf{m} \in \mathbb{Z}^r$ with $|\mathbf{m}| \leq N^{\varepsilon_2}$.

As to the method of Weyl, see especially [13], Prop. 8.2, p. 201 for an inequality almost ready-made for the present purposes. It may be stated as follows, where α now denotes the leading coefficient of a polynomial $f(x) \in \mathbb{R}[x]$ of degree $e \geq 1$:

$$\left|\sum_{n=1}^{N} e(f(n))\right| \leq 2N \left(N^{-e} \sum_{-N<l_1,\ldots,l_{e-1}<N} \min(N, ||\alpha e! l_1 \cdots l_{e-1}||^{-1})\right)^{2^{1-e}}.$$

We want to apply this with $f(x) = g(x)\theta_{\mathbf{m}}$, so $\alpha := g_0\theta_{\mathbf{m}}$, where g_0 is the leading coefficient of g.

For convenience we suppose here that $e \geq 2$, since the case $e = 1$ reduces to (3.4.8) and has been already worked out above.

Also, with the purpose of bounding appropriately the right hand side (i.e. by a power of N with fixed exponent < 1, provided that $|\mathbf{m}|$ is also bounded by a small power N^{ε_2} of N), it will be enough to obtain an estimate $\ll N^{\lambda}$ for the inner summation, for some fixed $\lambda < e$.

Consider first the contribution to the summation coming from terms with $l_1 \cdots l_{e-1} = 0$. There are at most $\ll N^{e-2}$ such terms, for which we can use N as an upper bound for the minimum. This will yield a total contribution $\ll N^{e-1}$ to the summation, which is alright for our purposes.

In order to estimate the rest, we group the terms according to the (nonzero) value $l_1 \cdots l_{e-1}$. So we may rewrite such part of the summation as

$$\sum_{0<|L|\leq N^{e-1}} \tau_L \cdot \min(N, ||\alpha e! L||^{-1}),$$

where τ_L denotes the number of solutions of $L = l_1 \cdots l_{e-1}$ with the stated constraints $0 < |l_i| < N$. By standard elementary estimates one has $\tau_L \ll_{e,\varepsilon_3} N^{\varepsilon_3}$ for every prescribed $\varepsilon_3 > 0$.

To go ahead, we use the celebrated *Dirichlet Lemma*, by which we may find coprime integers β, γ with $0 < \gamma \leq 4N^{e-1}$ such that $|e!\alpha - \beta/\gamma| \leq (4N^{e-1}\gamma)^{-1}$.

Let us first look at the terms in the summation such that γ does not divide L, grouping together the L such that $L\beta$ lies in a given nonzero class $\mu \in [1, \gamma - 1]$ modulo γ. For each given such μ, their number will be $\ll N^{e-1}/\gamma$. Since $Le!\alpha = (L\beta/\gamma) + \eta(4\gamma)^{-1} = \mu/\gamma + \eta(4\gamma)^{-1} +$ integer, where $|\eta| \leq 1$, such a term will produce a minimum $\min(N, ||\alpha e! L||^{-1}) \leq ||\alpha e! L||^{-1} \leq 2\gamma/\mu_1$, where $\mu_1 = \mu$ or $\mu_1 = \gamma - \mu$ according as $\mu \leq \gamma/2$ or not. Then it follows that the total contribution will not exceed $\ll N^{e-1+\varepsilon_3} \sum_{0<\mu_1\leq\gamma/2} \mu_1^{-1} \ll N^{e-1+\varepsilon_3} \log N$, which is fine for us as soon as $\varepsilon_3 < 1$.

Let us now consider the remaining terms, namely those such that $0 \neq L \equiv 0 \pmod{\gamma}$; there are at most $\ll N^{e-1}/\gamma$ such terms, and we choose N as an estimate for the minimum in every such term. This yields a total contribution $\ll N^{e+\varepsilon_3}/\gamma$ for these terms inside the summation.

So we are left with the task of bounding γ from below. Inequality (3.4.9) yields $||\gamma e! g_0 \theta_{\mathbf{m}}|| \geq |\gamma e! g_0 \cdot |\mathbf{m}||^{-q}$ for any nonzero $\mathbf{m} \in \mathbb{Z}^r$. On the other hand, by definition of γ, the left hand side is bounded by N^{-e+1}, hence $\gamma \geq N^{\frac{e-1}{q}}(e!|g_0| \cdot |\mathbf{m}|)^{-1}$. Here we assuming that $0 < |g_0| < N^{\varepsilon_5}$ for a small enough ε_5, and that $|\mathbf{m}| \leq N^{\varepsilon_2}$, whereas $e \geq 2$ is fixed. Then we obtain an estimate for the summation which is $\ll N^{e+\varepsilon_3+\varepsilon_2+\varepsilon_5-(e-1)/q}$, which is enough for our purposes as soon as we require that e.g. $\varepsilon_3 + \varepsilon_2 + \varepsilon_5 \leq (e-1)/2q$.

We have considered all possible cases, and this concludes our proof of the sought inequality. The rest of the argument is exactly as in the former proof of Theorem 3.1 (see also the NOTE). □

Proof of Corollary 3.2. The subgroup of $\overline{\mathbb{Q}}^*$ generated by the β_l may be expressed as a direct sum of a finite torsion group of order denoted $q > 0$, plus a finitely generated free abelian group, and then let $\alpha_1, \ldots, \alpha_r$ be free generators for it. Then for each $l = 1, \ldots, s$ we may write $\beta_l = \theta_l \mu_l$ where the θ_l are q-th roots of unity, and the μ_l are monomials in the α_j. By assumption these monomials are pairwise distinct. We have that for each $a = 0, 1, \ldots, q-1$, the function $n \mapsto L(nq + a)$ is the value at $(\alpha_1^{qn}, \ldots, \alpha_r^{qn})$ of a certain fixed *nonzero* Laurent polynomial (depending on a, not on n). Now, since the α_l^q are multiplicatively independent the μ_l^q remain distinct, and it suffices to apply Theorem 3.1 for each $a = 0, 1, \ldots, q-1$, to obtain the conclusion. □

There is a similar Corollary to Theorem 3.4, with the same argument.

3.1. A p-adic analogue.

One can formulate, and prove, similar results (for instance as in Theorem 3.5 above) replacing the usual absolute value by a p-adic valuation.[11]

[11] This has no relation to the p-adic method of Skolem, trated elsewhere in this paper.

The above approach relying on Fourier expansions may be replaced by the well-known method used in the context of the Skolem-Mahler-Lech theorem about zeros of exponential polynomials at integers. We give a brief hint of how one can proceed.

In this setting we assume that the Laurent polynomial P and the α_l are defined over a field K of characteristic 0, complete under an ultrametric valuation denoted $|\cdot|_p$ with finite residue field of characteristic $p > 0$. Roughly speaking, we seek an estimate for the number of integers $n \leq N$ such that $|P(\alpha_1^n, \dots, \alpha_r^n)|_p < \epsilon < 1$ for an $\epsilon > 0$, assumed to be not too small with respect to N, say larger than N^{-1}. (See also the already quoted book [9] for other results in the p-adic context.)

To outline the argument, first (similarly to the opening steps of the previous proof) it is easy to reduce to the case when $|\alpha_l|_p = 1$ for $l = 1, \dots, r$. By splitting $\mathbb{Z}$ into finitely many arithmetical progressions of modulus $p^a(p-1)$ (for a large enough integer a depending on the field of definition), one can further assume that $\alpha_l \equiv 1 \pmod{p^2}$ for each l. Then the functions $n \mapsto \alpha_l^n$ become the restrictions to $\mathbb{Z}$ of p-adic analytic functions on the disk $|x|_p \leq 1$, and then the same holds for $Q(n) := P(\alpha_1^n, \dots, \alpha_r^n)$. By well-known results (see for instance [8]), the analytic function $Q(x)$ may be written as a product $Q_1(x)Q_2(x)$, where Q_1 is a polynomial and $|Q_2(x)| = 1$ on the whole disk. Hence we are reduced to estimate the number of integers $n \leq N$ such that $|Q_1(n)|_p < \epsilon$ (where $\epsilon > N^{-1}$). As in the approach above (see the argument leading to (3.4.5)), this inequality implies that $|n - \rho|_p < \epsilon^b$ for a certain fixed $b > 0$ and some root ρ of Q_1. For every two such integers $n_1 < n_2$ we have $|n_2 - n_1|_p < \epsilon^b$, which means that n_1, n_2 are congruent modulo a certain 'large' power of p. Hence, clearly, for each of the finitely many roots ρ the number of such $n \leq N$ is at most $\epsilon^h N$, where $h > 0$ depends on b and the normalization for the absolute value. This completes our sketch.

It is to be remarked that this argument does not require the deep transcendental estimates needed in the former proof. However some similar result in the p-adic realm may be helpful in related problems.

4. Asymptotic expansions around singularities

In this section we shall obtain certain asymptotic expansions for the coefficients a_n of an algebraic function $f(x)$, in terms of the singularities nearest to the origin. As mentioned in the introduction, though the underlying methods are standard (Cauchy's theorem applied to suitable contours), we give the arguments (which are simple and short) in this section for completeness. For a more comprehensive and systematical investigations of asymptotic expansions, one can see the book by Flajolet and Sedgewick [11], especially Section 7 of Chapter VII, and also the recent paper [17] for similar results. One should also notice that Flajolet in [10] already applied asymptotic expansions of algebraic functions to prove a conjecture by Stanley [20] on the transcendence of the series $\sum_{n=0}^{\infty} \binom{2n}{n}^k x^n$ for all $k \geq 2$.

We let $\Xi_R := \Xi(f) \cap \{|z| = R\}$ denote the set of singularities of $f(x)$ nearest to the origin [12] and we choose a real number $R' > R$ strictly smaller than the least absolute value of a point in $\Xi(f) - \Xi_R$.

We have Cauchy's formula

[12] We note that there may be branch points of the function x on the curve $Q = 0$ which are nearer to the origin than R.

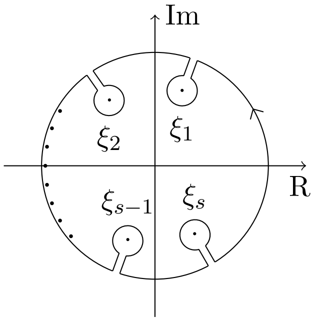

FIGURE 1. Contour for asymptotics

$$a_n = \frac{1}{2\pi i}\int_\Gamma z^{-n-1} f(z)\mathrm{d}z, \tag{4.0.1}$$

where Γ is any closed contour in $D(r)$ with $r < R$, turning positively once around 0 (e.g. a suitable circle centered at 0).

We want to deform Γ to a suitable contour convenient for our purposes.

We choose a small enough positive $\epsilon < (R'/R) - 1$ (which will later tend to 0) and define a contour C as follows: starting from $R'/R > 1$ we travel left on the real line up to $1 + \epsilon$; then we turn once counterclockwise around 1 (through a circle of radius ϵ), and finally go right backwards to R'/R.

For a $\xi \in \Xi$ of modulus $|\xi| = R$ we consider the contour ξC. We do this for each $\xi = \xi_j$, $j = 1 \ldots, s$, where ξ_j runs over the singularities with modulus R.

Now we consider a contour Γ' obtained by starting from any point p_0 at radius R', p_0 not in the union of the $\xi_j C$,then travelling counterclockwise (remaining at radius R'), and, whenever we meet a point p on $\xi_j C$, $|p| = R'$, travelling once along the whole $\xi_j C$ until we are again at p, and continuing in this way until we come back to the starting point p_0 (see Figure 1).

The function $f(z)$ may be analytically continued in the interior of Γ', which is simply connected.

Hence we may deform Γ to Γ' in formula (4.0.1). Since the function $f(z)$ is bounded on the circle $|z| = R'$, this yields the approximation

$$a_n = \frac{1}{2\pi i}\sum_{j=1}^{s}\int_{\xi_j C} z^{-n-1} f(z)\mathrm{d}z + O(R'^{-n}), \tag{4.0.2}$$

where one should note that the implied constants of asymptotics will only depend on R', f, not on n (see Formula 4.0.3).

We want now to analyze each summand. For this, we expand $f(z)$ as a Puiseux series around the center of the small disk associated with C_j. It will be convenient to perform the substitution $z \mapsto \xi_j z$, which yields

$$\int_{C_j} z^{-n-1} f(z)\mathrm{d}z = \xi_j^{-n}\int_C z^{-n-1} f(\xi_j z)\mathrm{d}z,$$

where C is as above. The function $z \mapsto f(\xi_j z)$ is algebraic and has a (potential) singularity at $z = 1$. Therefore let us see in general the possible asymptotic shape for the integral as above, replacing $f(\xi_j z)$ with an algebraic function $g(z)$.

First of all, let us write a Puiseux expansion for $g(z)$ at $z = 1$, i.e. as an infinite sum of terms of the form $c(z-1)^e$ where $c \neq 0$ and e is a rational number (bounded from below and with bounded denominator).

In this way, denoting by $C - 1$ the left translation of C by 1, we are reduced to estimate integrals of the shape

$$\int_C (z-1)^e z^{-n-1} \mathrm{d}z = \int_{C-1} z^e (z+1)^{-n-1} \mathrm{d}z,$$

as n tends to infinity. Though the theory of such integrals goes back to centuries, we give some detail.

First, if e is any integer ≥ 0 the integral over $C - 1$ vanishes. Hence at the outset we can consider, in the expansion of $g(z)$, only the terms with exponent e not in $\mathbb{N}$, and hence for our purposes we can assume that e is a rational number, not an integer ≥ 0.

Suppose first that e is an integer, hence ≤ -1.

Then the integral over $C - 1$ equals the integral over the small circle inside C, since the function is well defined in a connected neighbourhood of $C - 1$. Hence

$$\int_C (z-1)^e z^{-n-1} \mathrm{d}z = \int_{C-1} z^e (z+1)^{-n-1} \mathrm{d}z = \binom{-n-1}{-e-1}.$$

Suppose now that e is a rational non-integral number.

Integration by parts on $C - 1$ yields

$$\int_{C-1} z^e (z+1)^{-n-1} \mathrm{d}z = \frac{z^{e+1}(z+1)^{-n-1}}{e+1}\Big|_{v_0,v_1} + \frac{n+1}{e+1} \int_{C-1} z^{e+1} (z+1)^{-n-2} \mathrm{d}z,$$

where by the first term we intend to take the difference of the values of the function at the far right endpoint of $C - 1$, before and after turning around 0, the values being generally different because e is not integral. In absolute value these values will be $O((R'/R)^{-n})$, so will be negligible for our purposes, being of the same order of the error term coming from (4.0.2) above.

This process allows us to replace the pair (e, n) with $(e + 1, n + 1)$, at the cost of introducing the coefficient $(n + 1)/(e + 1)$. In particular we can reach a step when $e \geq 0$. But then we can let $\epsilon \to 0$ so that $C - 1$ becomes a segment, counted twice in opposite directions, namely the segment $[0, (R'/R) - 1]$. Of course since e is not an integer, the values of the function on the two copies of this segment will be different, in fact related by a factor which is a root of unity of order the denominator of e.

We are left with the task of estimating the integral over the segment; however, for large n the integral will be convergent on the half-line $[(R'/R) - 1, \infty)$, and with an error bounded by $O((R'/R)^{-n})$ with respect to the integral over the segment. In conclusion, we require some kind of asymptotic formula for the integrals $\int_0^\infty z^e(z + 1)^{-n-1}\mathrm{d}z$, for fixed $e \geq 0$ and $n \to \infty$. This is the value at $(e + 1, n - e)$ of the celebrated *Euler's Beta function*, and is given in terms of the Gamma function by $\Gamma(e+1)\Gamma(n-e)\Gamma(n+1)^{-1}$. Asymptotically, for fixed e, this is $= \Gamma(e+1)n^{-e-1}(1 + O(1/n))$. (Also observe that this asymptotic is in fact invariant by the process of integration by parts.)

From this discussion and from (4.0.2), we conclude that there exist nonzero constants κ_j and rational numbers e_j (which are ≤ 0 if they are integral), $j = 1, \ldots, s$, such that

$$a_n = \sum_{j=1}^{s} \kappa_j n^{-e_j} \xi_j^{-n} (1 + O(1/n)) + O(R'^{-n}). \tag{4.0.3}$$

5. Proof of main Theorems

Proof of Theorem 1.2. We start by considering the roots of unity which appear as ratios of two points in Ξ. These roots of unity generate a finite group, say of order $q \geq 1$.

Let us consider, for $b = 0, 1, \ldots, q-1$, the series

$$F_b(x) = x^{-b} \sum_{\theta^q=1} \theta^{-b} f(\theta x). \tag{5.0.1}$$

In view of the formula $\sum_{\theta^q=1} \theta^h = q$ or 0 according as h is or is not a multiple of q, we have $F_b(x) = \sum_{m=0}^{\infty} a_{b+mq} x^{mq}$. In particular, $F_b(x) = F_b(\zeta x)$ for each q-th root of unity ζ.

Also, F_b is an algebraic function, with singularities contained in the set $\bigcup_{\theta^q=1} \theta \cdot \Xi$.

We go ahead by reducing to the case when K is a field of algebraic numbers. First of all, the field K may be assumed to be finitely generated, since, as is well-known and easily proved, the field generated by the coefficients a_n may be in fact generated by finitely many of them. Indeed, let K_0 be as above the field generated by the coefficients of $Q(x, y)$. Then each of the a_j is algebraic over K_0, because $Q(x, f(x)) = 0$. Let then σ be an automorphism of $K_0(a_0, a_1, \ldots)$ fixing $a_0, \ldots, a_m$. Then $Q(x, f^\sigma(x)) = 0$ and $f(x) - f^\sigma(x)$ vanishes to order $\geq m+1$ at $x = 0$. But the order of zero of this function is bounded unless the function is 0. So if m is large enough σ fixes all coefficients, proving that $a_0, \ldots, a_m$ generate the said field. [13]

Therefore K may be viewed as the function field of some irreducible affine algebraic variety $\mathcal{V}$ defined over a number field.

Also, by the (function field version of) Eisenstein's theorem (see e.g. [25]), the denominators of the a_j contain only finitely many primes, which now means that the a_j may be seen as regular functions on the complement in $\mathcal{V}$ of a proper Zariski-closed subset $\mathcal{V}'$. Now, if $\dim \mathcal{V} = 0$, then $\mathcal{V}$ is a point and our field is already contained in $\overline{\mathbb{Q}}$. If the dimension is positive, we may specialize the a_j, viewed as functions on $\mathcal{V} - \mathcal{V}'$, at an algebraic point of such variety.

Take an integer $b \in [0, q-1]$ and consider the function F_b: it will be either a polynomial (and then the a_n vanish for $n = mq + l$ for a large enough $l \equiv b \pmod{q}$ and all $m \in \mathbb{N}$), or infinitely many such a_n are nonzero, and the function has some singularity. By suitable specialization (outside a proper subvariety of $\mathcal{V}$) this singularity will not disappear. In fact, it is well known that if an algebraic function defined over a function field is not a polynomial, it remains not a polynomial under suitable specializations. [14]

Also, by specialization the a_n which vanish will remain 0, and the set of roots of unity which appear as ratio of two singularities will be the same (since there are only finitely many singularities). Thus the number q will not change.

After these preliminaries, we are ready to complete the proof in the case of algebraic quantities. (Note that the radius of convergence will be possibly affected by the specialization, but this is harmless for us.)

We adopt the procedure carried out in Section 4, with $F_b(x)$ in place of $f(x)$, for each $b = 0, 1, \ldots, q-1$.

[13] Easy proofs are also possible by a recurrence formula for the a_j; see e.g. [25].

[14] This conclusion is a function-field version of a theorem of Ostrowski, see [25]. It may be proved for instance also by observing that if the function is a polynomial, its degree is bounded only in terms of the degrees of its minimal equation, which by specialization do not increase. So, if some coefficient of large enough degree is nonvanishing, the function cannot be a polynomial.

Select then any such b such that F_b is not a polynomial, and apply formula (4.0.3); taking into account that we have changed $f(x)$ with $F_b(x)$, and in view of (5.0.1), the formula will read

$$a_{nq+b} = \sum_{j=1}^{s} \kappa_j n^{-e_j} \xi_j^{-nq}(1 + O(1/n)) + O(R'^{-nq}), \tag{5.0.2}$$

where R, R' are as before, for F_b in place of f, the κ_j are nonzero, and the ξ_j belong to the set of singularities of F_b, i.e. they are in the set $\bigcup_{\theta^q=1} \theta \cdot \Xi$, and they have minimal distance R from the origin. This set is not empty (i.e. $s > 0$) since we are assuming that F_b is not a polynomial.

Also, the function F_b being invariant by $x \mapsto \zeta x$, for $\zeta^q = 1$, the numbers κ_j, e_j associated to singularities which differ by a factor which is a root of unity (necessarily of order dividing q) will be the same. Hence, after grouping the terms, we can assume that ξ_j/ξ_l is not a root of unity for $1 \le j < l \le s$.

Let J be the subset of $\{1, \ldots, s\}$ made up with the j such that $-e_j$ is maximum, denoting with $-e$ this maximum, and let $\delta = \min_{j \notin J}(e_j - e) > 0$.

Then, since $|\xi_j| = R$ for $j = 1, \ldots, s$, we have $|\sum_{j \notin J} \kappa_j n^{e-e_j} \xi_j^{-nq}| = O(n^{-\delta} R^{-nq})$.

Now, if $a_{nq+b} = 0$ we further obtain that

$$|\sum_{j \in J} \kappa_j \xi_j^{-nq}| = O(n^{-\delta} R^{-nq}) + O(n^{-1} R^{-nq}) + O(n^{e} R'^{-nq}).$$

Finally, since $R' > R$, and since we are assuming that no ratio between two distinct ones among the ξ_j is a root of unity, we can apply Corollary 3.2 and deduce that the set of these n has the required property. □

Remark 5.1. We note that the p-adic estimate obtained in Section 3.1, though giving a bound for the number of (p-adically) 'small values' of an exponential polynomial in large intervals, would not be useful for deriving the presently sought conclusion. In fact, in the bound for the exponential sum appearing in the last displayed formula, the last term on the right has a purely archimedean origin.

Proof of Theorem 1.4. The proof is completely similar to that of Theorem 1.2, using Theorem 3.4 in place of Theorem 3.1 (actually applied as in the corresponding corollaries). □

A simple application of Theorem 1.4. In particular, just to offer an instance of possible applications of Theorem 1.4 (e.g. in the simple case of a polynomial g independent of N).

Starting with an algebraic power series $\sum_{n=0}^{\infty} a_n x^n$, we can consider the vanishing of coefficients a_{n^2}, obtaining bounds for $\#\{n \le N : a_{n^2} = 0\}$ analogous to what we have obtained for the whole sequence of a_n, that is, $\ll N^c$, for a $c < 1$, for the number of such integers n outside a finite union of arithmetical progressions on which all a_n vanish.

Since the series of the shape $\sum_{n=0}^{\infty} a_{n^2} x^n$ or $\sum_{n=0}^{\infty} a_{n^2} x^{n^2}$ are generally not algebraic anymore (the first one is not even generally convergent anywhere for the complex absolute value, the second one is too lacunary to be possibly algebraic), such an extension of the method leads us to results of new type. Moreover such conclusions escape from the range of methods like Bézivin's, coming from the theorem of Szemeredi; indeed, the sequences like $(a_{n^2})_{n \in \mathbb{N}}$ do not generally satisfy linear recurrences.

6. Criteria with p-adic interpolation

In this section we develop some p-adic considerations, trying to understand when the method of Skolem may be possibly applied to an algebraic power series.

As above, for a prime number p, we denote by $\mathbb{C}_p$ a completion of an algebraic closure of $\mathbb{Q}_p$, with $\mathcal{O} = \mathcal{O}_p$ the valuation ring of $\mathbb{C}_p$, and by $\overline{\mathbb{F}}_p$ an algebraic closure of $\mathbb{F}_p$.

So $\mathcal{O}$ is the closed unit disk $D(0, 1^+) := \{x \in \mathbb{C}_p : |x|_p \leq 1\}$. Here $|\cdot|_p$ denotes the usual p-adic absolute value, normalized so that $|p|_p = p^{-1}$. We also denote $v(x) = v_p(x) = \mathrm{ord}_p(x) = -\log|x|_p/\log p$.

In Definition 1.5 we had denoted by Sk_p the space of the series $f(x) = \sum_{n=0}^{\infty} a_n x^n \in \mathbb{C}_p[[x]]$ such that for an analytic function $g(x) \in \mathbb{C}_p[[x]]$ converging in $\mathcal{O}_p$, we have $a_n = g(n)$ for all large n.

If this happens, then g is unique, because $\mathbb{N}$ is dense in $\mathcal{O}_p$ (see [8]). At the cost of modifying finitely many coefficients a_n, which amounts to adding a polynomial to $f(x)$, we may assume that $a_n = g(n)$ for all integers $n \in \mathbb{N}$.

We denote by Sk_p^* the subspace of these functions.

Before going ahead we give a definition of good reduction useful for us. We denote by $\widehat{\mathbb{C}_p(x)}$ the completion of $\mathbb{C}_p(x)$ with respect to the Gauss norm. [15]

Definition 6.1. *We say that $Q(x, y)$, or that $f(x)$, has* `good reduction` *(at p) if either* $\deg_y Q = 1$ *or if $Q(x, y)$ has no factor in $\widehat{\mathbb{C}_p(x)}[y]$ of degree 1 in y. We also say that the prime p* `is of good reduction` *if $f(x)$ has good reduction at p.*

Note that if $Q \in \mathcal{O}[x, y]$ and if its reduction $\bar{Q}(x, y) \in \overline{\mathbb{F}}_p[x, y]$ has degree > 1 in y, and has no linear factors in y, then Q has good reduction in the present sense. In fact, by Gauss's lemma, if it had a factor in $\widehat{\mathbb{C}_p(x)}[y]$ of degree 1 in y, this would yield a linear factor of $\bar{Q}$ by reduction.

Hence this notion is weaker than the 'naive' one given in the introduction.

Remark 6.2. **Effectivity**. We note that if $Q(x, y)$ has coefficients in a number field, for instance, there are known algorithms to check whether it has good reduction in the present sense. In practice this works after factoring modulo a suitably high, computable, power of p, and then using a kind of Hensel lifting. (See the exercises in Ch. 7 of [25] for an instance over $\mathbb{Z}_p$.)

It is also effective to compute a finite set S of primes such that there is good reduction for primes outside S. That such a finite set exists follows from a theorem of Ostrowski, see e.g. [25] for simple proofs.

6.1. Conditions for Sk_p and Sk_p^*.

Note that if $f(x) \in Sk_p$ then the same holds for $B(x)f(x)$, for every polynomial $B \in \mathbb{C}_p[x]$. In particular, suppose that we start with an $f(x)$ which is algebraic over $\mathbb{C}_p(x)$, satisfying an irreducible equation $Q(x, f(x)) = 0$ with $Q \in \mathcal{O}[x, y]$; then after multiplying $f(x)$ by the leading coefficient in y of $Q(x, y)$, we may assume that Q is monic in y, so that $f(x)$ is integral over $\mathcal{O}[x]$.

Note that such a power series has necessarily coefficients in $\mathcal{O}$, since the algebraic (monic) equation $Q(x, f(x)) = 0$ yields $\sup_{|x|_p \leq 1} |f(x)|_p \leq 1$, and we may apply the usual estimates (see [8]).

Now, adding to $f(x)$ a suitable polynomial, assume that $f(x) \in Sk_p^*$, so $a_n = g(n)$ for all n, where g is analytic in $\mathcal{O}$.

[15] This completion is sometimes called the *field of analytic elements*. See e.g. [8] for more on these concepts.

We can write $g(x) = \sum_{m=0}^{\infty} g_m x^m$, where $|g_m|_p \to 0$ as $m \to \infty$.

It will be convenient to expand in terms of binomial coefficients. [16] Namely, we can write $x^m = \sum_{r=0}^{m} c_{rm}\binom{x}{r}$, where c_{rm} is the r-th finite difference of x^m at 0. This fact, or induction, proves that c_{rm} is an integer divisible by $r!$.[17]

Substituting we find that $g(x) = \sum_{r=0}^{\infty}(\sum_{m=0}^{\infty} c_{rm}g_m)\binom{x}{r} =: \sum_{r=0}^{\infty} b_r\binom{x}{r}$, where we have written

$$b_r := \sum_{m=0}^{\infty} c_{rm}g_m.$$

Observe that $c_{rm} = 0$ for $m < r$, so the summation defining b_r runs in fact for $m \geq r$. Since $|g_m|_p \to 0$, we find that $b_r/r!$ tends p-adically to 0.

Recall that $v_p(r!) = [r/p] + [r/p^2] + \ldots = \frac{r-\sigma(r)}{p-1}$, where $\sigma(r) \leq (p-1)\frac{\log pr}{\log p}$ is the sum of the p-adic digits of r. So $v_p(b_r) - \frac{r-\sigma(r)}{p-1} \to \infty$.

Now writing $a_n = g(n) = \sum_{r=0}^{\infty} b_r\binom{n}{r}$, we have in the first place that the b_r lie in $\mathcal{O}$, since the a_n do: indeed, $b_0 = a_0$, $b_1 + b_0 = a_1, \ldots$.

Also, we find that $f(x) = \sum_r b_r \sum_n \binom{n}{r}x^n$.

Moreover, for $r \geq 0$ we have $\sum_n \binom{n}{r}x^n = \frac{x^r}{(1-x)^{r+1}}$, as is well known, and follows by differentiation of the usual identity $\sum_n x^n = (1-x)^{-1}$. In conclusion, putting

$$\varphi(x) := \sum_{r=0}^{\infty} b_r x^r,$$

we have the formula

$$(1-x)f(x) = \varphi\left(\frac{x}{1-x}\right), \tag{6.2.1}$$

in the sense of formal power series. Note that by the above remarks, the p-adic radius of convergence of φ is $\geq p^{\frac{1}{p-1}} := \rho_p > 1$.

We also have a reciprocal formula:

$$f\left(\frac{x}{1+x}\right) = (1+x)\varphi(x), \tag{6.2.2}$$

Note that all this entails that $\varphi(x)$ is also algebraic, satisfying the equation

$$Q\left(\frac{x}{1+x}, (1+x)\varphi(x)\right) = 0, \tag{6.2.3}$$

so in particular we have the minimal equation $Q_1(x, \varphi(x)) = 0$ over $\mathcal{O}[x, y]$, where $Q_1(x, y) = (1+x)^e Q(\frac{x}{1+x}, (1+x)y)$ for a suitable $e \geq 0$.

NOTE. If Q is monic in y (we remarked above that this may be assumed after multiplying $f(x)$ by a polynomial), then the leading coefficient in y of Q_1 will be a power of $1+x$. In any case the equation implies that $\sup_{|x|<\rho_p} |(1+x)^h\varphi(x)|$ is bounded for some $h \geq 0$, as $|x|$ approaches ρ_p, and the same holds for $\sup_{|x|<\rho_p} |\varphi(x)|$ (the bound depending in a certain way on the degrees in x of the coefficients of Q). But then we have this same bound for the $|b_r|_p\rho_p^r$ of $\varphi(x)$. This amounts to a

[16] This device also appears in a proof of the SML theorem hinted in the exercises in the book [6].

[17] Such facts are known since centuries.

slight sharpening of the former information. Namely, in addition to the fact that $(v_p(b_r) - \frac{r}{p-1}) + \frac{\sigma(r)}{p-1} \to \infty$ we get that $v_p(b_r) - \frac{r}{p-1}$ is bounded below.

We may partially reverse these calculation, so if (6.2.1) holds for a $\varphi \in \mathbb{C}_p[[x]]$ such that $v_p(b_r) - v_p(r!) \to \infty$, then $a_n = g(n)$ for $g(x) = \sum_r b_r \binom{x}{r}$, where g is analytic on $\mathcal{O}$, hence $f(x) \in Sk_p^*$. In fact, writing $\binom{x}{r} = \sum_{m \le r} \frac{k_{mr}}{r!} x^m$, with certain integers k_{mr}, we have $g_m = \sum_{r \ge m} \frac{b_r}{r!} k_{mr}$. Then the following proposition is proved.

Proposition 6.3. *Let $f(x) = \sum_{n=0}^{\infty} a_n x^n \in \mathcal{O}[[x]]$. Then $f(x) \in Sk_p^*$ if and only if $\varphi(x) := (1+x)^{-1} f(\frac{x}{1+x})$ admits a series expansion $\varphi(x) = \sum_{r=0}^{\infty} b_r x^r$ such that $(v_p(b_r) - \frac{r}{p-1}) + \frac{\sigma(r)}{p-1}$ tends to ∞ as $r \to \infty$.*

Remark 6.4. When $f(x)$ is a rational functions it is easy to see that to be in Sk_p or Sk_p^* substantially amounts that the (finite) poles of $f(x)$ are p-adically near 1, which is equivalent that this holds for the *roots* of the corresponding linear recurrence. In fact, this condition appears clearly if one looks at the arguments of Skolem.

This already yields some examples of series satisfying the condition, which represent algebraic not rational functions. Here is a simple one.

Example 6.5. Let $p > 2$. For $l \in \mathcal{O}$, $l \neq 0$, we put $\varphi_l(x) = \sum_{r=0}^{\infty} (lp)^r \binom{1/2}{r} x^r$, so $\varphi_l(x)$ converges for $|x|_p < p$ and represents the algebraic function $\sqrt{1 + lpx}$ (with $\varphi(0) = 1$) in the disk $D(0, p^-)$.

We have $v_p(b_r) \ge r$, so indeed our constraint is fulfilled, and we can use (6.2.1) to define $f_l(x)$, obtaining $f_l(x) = (1 + (lp-1)x)^{1/2}(1-x)^{-3/2}$. We can now take any finite linear combination of the f_l, so defining $f(x) = \sum_{l \in L} c_l f_l(x)$, where $L \subset \mathcal{O}$ is a finite set and where $c_l \in \mathbb{C}_p^*$.

Expanding with the binomial theorem we find

$$a_n = \sum_{r+s=n} \left(\sum_{l \in L} c_l (lp-1)^r \right) \binom{1/2}{r} \binom{-3/2}{s}.$$

The fact that $a_n = g(n)$ for a nonzero p-adic analytic function g (convergent in $\mathcal{O}$) yields that only finitely many a_n can vanish. Perhaps this may be proved otherwise, but does not look immediately obvious from the explicit formula just given. (Indeed, for instance the quantities $\sum_{l \in L} c_l (lp-1)^r$ cannot be estimated trivially in general as functions of r, since it is easy to choose L as a finite set of algebraic integers such that the $lp - 1$ have the same absolute value for $l \in L$, so the various terms can yield cancellations, and we may even choose them so that the complex absolute values $|lp - 1| = 1$ for all $l \in L$.)

Clearly the construction of this example proves Proposition 1.8.

We have another easy proposition:

Proposition 6.6. *If $f(x) \in Sk_p$ for an irrational algebraic $f(x)$ then there is no good reduction.*

Proof. The proof is clear: If $f(x) \in Sk_p$ then $f(x) - h(x) \in Sk_p^*$ for some polynomial h, so we may assume that $f(x) \in Sk_p^*$. If $f(x)$ is not rational then $\deg_y Q > 1$. On the other hand equation (6.2.1) obviously implies that $f(x) \in \widehat{\mathbb{C}_p(x)}$, since $v_p(b_r)$ tends to infinity. Then Q has a linear factor in y over $\widehat{\mathbb{C}_p(x)}$, concluding the argument. □

6.2. **Decomposing along arithmetical progressions.** Recall that the argument of Skolem works by interpolating the sequence of coefficients of a rational function by a p-adic analytic function, however *after* partitioning $\mathbb{N}$ into suitable arithmetical progressions, and restricting the sequence to each of them.

In this subsection we analyze this kind of decomposition in our case.

Let then $q \geq 1$ be a common modulus of the relevant progressions $b + q\,\mathbb{N}$, for $b = 0, \dots, q-1$. Then we have the following familiar formula

$$f_{b,q}(x^q) := \sum_{m=0}^{\infty} a_{b+mq} x^{mq} = x^{-b} \sum_{\theta^q=1} \theta^{-b} f(\theta x). \tag{6.6.1}$$

Here θ runs through all the q-th roots of unity. (The formula has been used also in Section 4.) Note that the function is invariant by $x \mapsto \zeta x$ for any q-th root of unity ζ.

This expression is relevant in our context because the method of Skolem will succeed (for the prime p) precisely when we can find a q such that all $f_{b,q}(x)$ belong to Sk_p.

For our purposes let us stick to algebraic power series with coefficients also in $\overline{\mathbb{Q}}$, so, after embedding $\overline{\mathbb{Q}}$ into $\mathbb{C}_p$, we can view them as being defined over $\mathbb{C}_p$, for every prime p.

We already know from Skolem's proof that if $f(x) \in \overline{\mathbb{Q}}(x)$, it is always possible to find a prime p for which the above requirement succeeds. So let us consider irrational algebraic series $f(x)$.

We have already used in the previous sections the set Ξ of (finite) branch points of the coordinate function x on the curve $Q(x, y) = 0$. As shown by the statement of Theorem 1.7, they will play an important role also now.

Proof of Theorem 1.7. Let us assume that the Skolem method may be applied to $f(x)$, so we have an integer $q > 0$ such that all the $f_{b,q}(x)$ are in Sk_p. In view of equation (6.2.1) applied to $f_{b,q}(x)$ in place of $f(x)$ we obtain that $f_{b,q}(x) \in \widehat{\mathbb{C}_p(x)}$, and this holds for each $b = 0, 1, \dots, q-1$. But then $f_{b,q}(x^q)$ also lies in $\widehat{\mathbb{C}_p(x)}$,[18] so this holds for $f(x) = \sum_{b=0}^{q-1} x^b f_{b,q}(x^q)$. Thus either $f(x)$ is a rational function or there is no good reduction, proving the first of the sought conclusions.

Things are similar if we only impose that the *restricted* Skolem method may be applied to $f(x)$, however a few further considerations are needed.

To outline our argument, let us first assume that no ratio ξ_i/ξ_j of distinct elements $\xi_i \neq \xi_j \in \Xi$ is a root of unity.

Then the algebraic functions defined by $f(\theta x)$, $\theta^q = 1$, generate fields $L_\theta = \mathbb{C}_p(x, f(\theta x))$ over $\mathbb{C}_p(x)$, which have linearly disjoint Galois closures $\hat{L}_\theta$, in the strong sense that each of the $\hat{L}_\theta$ is linearly disjoint from the product of the other ones over $\mathbb{C}_p(x)$. Indeed, in view of the present assumption, the Galois closures $\hat{L}_\theta$ have pairwise disjoint sets of branch points over $\mathbb{C}_p(x)$, whence each intersection is unbranched over $\mathbb{C}_p(x)$, and thus by general theory [19] must coincide with $\mathbb{C}_p(x)$.

Then the formula (6.6.1) expresses $f_{b,q}(x)$ as a sum of terms from these linearly disjoint fields.

[18] Note however that for a series $g \in \mathbb{C}_p[[x]]$ with radius of convergence r, the radius of convergence of $g(x^q)$ is $r^{1/q}$.

[19] One can use e.g. the Hurwitz genus formula.

By simple Galois theory, the field generated by $f_{b,q}(x)$ over $\mathbb{C}_p(x)$ contains each of the fields generated by the various terms (since an automorphism over $\mathbb{C}_p(x)$ fixing the sum must fix all the summands by linear disjointness).

Suppose then that one series $f_{b,q}(x)$ belongs to Sk_p. By the former considerations we deduce that $f_{b,q}(x)$ belongs to $\widehat{\mathbb{C}_p(x)}$. But then each summand, lying in $\mathbb{C}_p(x, f_{b,q}(x))$, belongs as well to $\widehat{\mathbb{C}_p(x)}$. We deduce that $f(\theta x)$ does not have good reduction, for any involved root of unity θ (conditions which are equivalent as θ varies).

Let us now deal with the general case, and then let $q_0 > 0$ be common multiple of the orders of the roots of unity which appear as ratios ξ_i/ξ_j for $\xi_i, \xi_j \in \Xi$. Let also $q_1 := \gcd(q_0, q)$.

Then in the formula (6.6.1) let us group together all the terms with θ in a same coset of the group U_q of q-th roots of unity modulo the subgroup U_{q_1} of q_1-th roots of unity. We contend that two different terms correspond to functions having disjoint set of branch points. Indeed, all terms in the coset θU_{q_1} have singularities in $\theta_1^{-1}\Xi$, for a $\theta_1 \in \theta U_{q_1}$. So, if terms in cosets θU_{q_1}, $\theta' U_{q_1}$ have a common singularity, then $\theta U_{q_1} \cap \theta' U_{q_1}$ intersect. But this means that the cosets are in fact equal.

Hence, after the grouping, distinct terms correspond to functions having disjoint set of branch points. Then, the former argument proves that the corresponding function either is rational or does not have good reduction.

So in particular, if $f(x) \in Sk_p$, there exists a divisor q_1 of q_0, and an integer b such that the function $\sum_{\theta}^{q_1} \theta^{-b} f(\theta x)$ either is rational or does not have good reduction.

Since this function belongs to a finite computable set, the proof of Theorem 1.7 is complete. □

Remark 6.7. As shown by the proof, the conditions on the singularities are explicit in terms of their ratios which are roots of unity.

Proof of Proposition 6.6. The singularities of the function are $(3 \pm \sqrt{-7})^{-1}, 1$, and $1/4$, and hence no two distinct of them have a ratio which is a root of unity. (Indeed, $3 \pm \sqrt{-7} = 4\exp(i\theta)$ for a real number θ such that θ/π is irrational, as is easy to see.)

So, by the proof of Theorem 1.7, the Skolem method cannot be applied except possibly for the primes p which are not of good reduction for $f(x)$.

Now, every odd prime p is of good reduction, since the minimal equation for the reduction of $f(x)$ over $\bar{\mathbb{F}}_p(x)$ has degree 2, so only the prime $p = 2$ remains.

Further, if 2 would not be of good reduction, then $f(x)$ would lie in $\widehat{\mathbb{C}_2(x)}$, and the same would happen for $\sqrt{1-4x}$. Hence we could write $4x = 1 - F^2(x)$ for some $F \in \widehat{\mathbb{C}_2(x)}$, so $F(x) = 1+2G(x)$ for some $G \in \widehat{\mathbb{C}_2(x)}$, satisfying $G^2(x) - G(x) - x = 0$. This G would satisfy $|G|_G \leq 1$ for the Gauss norm, and now it suffices to observe that there are no rational function solutions modulo 2. □

7. Appendix

As mentioned in the introduction, in this short appendix we want to sketch an *ad hoc* argument to improve on the general bound N^c of Theorem 1.2, for the number of zeros in $[0, N]$ of the special sequence of Example 1.1, namely the sequence

$$a_n := \binom{2n}{n} + (3+\sqrt{-7})^n + (3-\sqrt{-7})^n + Q(n),$$

where Q is a nonzero [20] polynomial with integer coefficients. As noted above, the generating function $\sum_{n=0}^{\infty} a_n x^n$ equals the algebraic function $\frac{1}{\sqrt{1-4x}} + \frac{2-6x}{1-6x+16x^2} + R(x)$, where R is a rational function with denominator a power of $1-x$.

We contend that the following holds:

Claim: *For any fixed $\epsilon > 0$, the number of positive integers $n < N$ such that $a_n = 0$ is $\ll \log^{1+\epsilon} N$.*

For a proof of the Claim, in the sequel we put $b_{\pm} := 3 \pm \sqrt{-7}$; we have $b_- = \bar{b}_+$ and $|b_{\pm}| = 4$.

We note that b_+, b_- are algebraic integers, actually divisible by 2 in the ring of integers $\mathcal{O}$ of $\mathbb{Q}(\sqrt{-7})$, whereas $\gcd(b_+/2, b_-/2) = 1$ in that ring: in fact $b_{\pm}/2$ are the two roots of the equation $x^2 - 3x + 4 = 0$. In particular, they are not units, but they divide 4 in $\mathcal{O}$; this also implies that $(b_-/2)^m - (b_+/2)^m$ is coprime with 2 for every integer $m > 0$.

Let $n_1 < n_2 < n_3$ be three large positive solutions of the equation $a_n = 0$. Let us also suppose that $n_3 < (1+\delta)n_1$, where $\delta > 0$ is a sufficiently small positive constant, to be chosen below.

We define $\Delta := \sqrt{-7}D$, where D is the determinant of the 3×3-matrix with rows $(b_+^{n_1}, b_+^{n_2}, b_+^{n_3})$, $(b_-^{n_1}, b_-^{n_2}, b_-^{n_3})$, $(Q(n_1), Q(n_2), Q(n_3))$.

Note that D is an algebraic integer and that complex conjugation switches the first two rows, so sends D into $-D$; hence Δ is invariant by conjugation and is an algebraic integer in $\mathcal{O}$, so Δ in fact is an integer in $\mathbb{Z}$.[21]

Also, we see that D is divisible in $\mathcal{O}$ by $(b_+b_-)^{n_1} = 16^{n_1}$. Hence Δ is an integer divisible by 16^{n_1}.

Using the very definition of a_n, and that $a_{n_i} = 0$ for $i = 1, 2, 3$, we see by evident row operations that the third row of D may be replaced by $-(\binom{2n_1}{n_1}, \binom{2n_2}{n_2}, \binom{2n_3}{n_3})$ without changing D.

Now, $\binom{2n}{n}$ is divisible by the product of prime numbers in the interval $(n, 2n)$, and therefore, since $n_1 < n_2 < n_3 < (1+\delta)n_1$, the $\gcd_{i=1,2,3} \binom{2n_i}{n_i}$ is divisible by the product P of primes in the interval $[(1+\delta)n_1, 2n_1]$. Hence the same holds for Δ.

Combining this with the former divisibility, we see that Δ is divisible by $16^{n_1}P$.

Therefore, either $\Delta = 0$, or $|\Delta| \geq 16^{n_1}P$.

On the other hand, looking at the original third row in the definition of D and Δ, we readily see that $|\Delta| \ll n_1^d 16^{n_3}$, where $d = \deg Q$.

Concerning the product P, by Chebyshev estimates we have $P \gg \alpha^{n_1}$, for a suitable absolute constant $\alpha > 1$, independent of $\delta > 0$ if this last number is small enough.[22]

Now, by the former remarks, either $\Delta = D = 0$ or we have $P \leq 16^{-n_1}|\Delta|$, hence $\alpha^{n_1} \ll P \ll n_1^d 16^{n_3 - n_1} \leq n_1^d 16^{\delta n_1}$.

In the second case, on choosing δ so small that $\alpha > 16^{\delta}$, we obtain that n_1 is bounded, hence the set of these triples of solutions is finite.

[20] If $Q = 0$, then $a_n = 0$ implies that $\binom{2n}{n}$ is divisible by 2^n, which cannot happen for $n > 1$, so a_n will never vanish.

[21] We could also limit to consider D in the arguments below.

[22] By the Prime Number Theorem, not needed here, we could choose α as any number less than $e^{1-\delta}$.

In the first case, the condition $D = 0$ yields a polynomial exponential Diophantine equation in the variables n_1, n_2, n_3. We could then apply well known results, e.g. of M. Laurent, or Evertse, but it is simpler to argue directly. Putting $m_i := n_i - n_1$, the determinantal equation yields

$$(b_-^{m_2} - b_+^{m_2})Q(n_3) = (b_-^{m_3} - b_+^{m_3})Q(n_2) - (b_-^{m_3} b_+^{m_2} - b_-^{m_2} b_+^{m_3})Q(n_1). \tag{7.0.1}$$

Then, upon dividing throughout by 2^{m_2}, and recalling that $(b_-/2)^m - (b_+/2)^m$ is coprime to 2 for every integer $m > 0$, equation (7.0.1) yields that $Q(n_3)$ is divisible by $2^{m_3 - m_2} = 2^{n_3 - n_2}$ in $\mathcal{O}$, hence in $\mathbb{Z}$. This implies in the first place that $n_3 \leq n_2 + O(\log n_3)$, which would lead to a bound $\ll \log^2 N$ for the number of zeros, already better than our general bound. But with a little care we can further improve on it.

For that, let us write a factorization $Q(x) = q \prod (x - \rho_j)^{e_j}$ with a nonzero integer q, integers $e_j > 0$, and distinct ρ_j in a finite extension of $\mathbb{Q}_2$, with valuation denoted v extending the standard one of $\mathbb{Q}_2$.

Since $v(Q(n_3)) \geq n_3 - n_2$ we deduce that there exists j so that $v(n_3 - \rho_j) \gg n_3 - n_2$, or, setting $s := n_3 - n_2 > 0$, $\rho := \rho_j - n_2$, $v(s - \rho) \gg s$. Then, if for fixed j, n_2 we order the integer solutions of this inequality in a sequence $0 < s_1 < s_2 < \ldots < s_k$, we have $v(s_{l+1} - s_l) \gg s_l$ for $l = 1, \ldots, k-1$, hence $s_{l+1} \geq s_l + 2^{\eta s_l}$ for some fixed $\eta > 0$. In particular, for fixed ρ_j, n_1, n_2, the number of solutions n_3 in the interval $(n_2, (1+\delta)n_1]$ is $\ll \log^{\epsilon} n_1$, for every $\epsilon > 0$.[23] And in the argument we may choose n_2 as the smallest solution in the interval which is $> n_1$ (if there are any).

In conclusion, we deduce that for large T, the interval $[T, (1+\delta)T]$ contains at most $\ll \log^{\epsilon} T$ solutions of $a_n = 0$, and this implies that the number of solutions up to N is $\ll \log^{1+\epsilon} N$, as claimed.

Remark 7.1. This method, though admitting some obvious variations, is very special of the sequence in question, and is very far from applying to general algebraic functions. For instance, it does not apply to a sequence of the shape $a_{2n} + a_n + R(n)$ with a polynomial $R(n)$, since the crucial divisibility property by 'many primes' in an interval is completely lost.

Still concerning this special sequence, another possible approach to detect its zeros, mentioned in a footnote above, would be to use that the exact power of 2 dividing $\binom{2n}{n}$ is the number σ_n of nonzero 2-adic digits of n. Then if $a_n = 0$ we easily obtain that $2^{\sigma_n} || Q(n)$. However at first sight this kind of condition looks puzzling to exploit without special assumptions on $Q(x)$. For instance, if $Q(x) = x$, say, the condition is met for every integer n of the shape $n = 2^k + 2^{e_2} + \ldots + 2^{e_k}$ with positive integers $0 < k < e_2 < \ldots < e_k$. We also note that the counting function of such integers up to N obviously grows faster than any power of $\log N$ and in fact faster than any power N^c with $c < 1$ (for this, choose k near to $\log_2 \sqrt{N}$).

Still a further different approach might come from Diophantine approximation, as mentioned above together with the example. However this method too seems not to lead to a substantial improvement on the general bound, even for the special sequence into account.

Remark 7.2. We end with a remark on the relation of the present issues to some simple looking functional equations like

$$f(x) + f(-x) = cf(x^2),$$

[23] Actually, the argument plainly delivers a bound growing more slowly than any iterated logarithm of n_1.

for some non-zero constant c.

Writing $f(x) = \sum_{n=0}^{\infty} a_n x^n$, this equation yields $2a_{2n} = ca_n$. Therefore, the vanishing of one single coefficient a_n, $n \neq 0$, implies the vanishing of coefficients on the whole infinite geometric progression $n, 2n, 4n, \ldots$. Note also that this functional equation is not incompatible with D-finiteness; actually we have for instance the solutions $f(x) = (1-x)^{-1}$ (with $c = 2$) and $f(x) = \log(1-x)$ (with $c = 1$); in both cases no coefficient vanishes.

In particular, a positive solution to Rubel's problem mentioned in the introduction would imply that in every D-finite power series satisfying the above functional equation *either no coefficient vanishes, or else there are vanishing coefficients along a whole arithmetical progression.* Maybe this could be checked directly, but of course one could widely modify the functional equation and obtain similar deductions, which look puzzling *a priori.*

In conclusion, a conjecture regarding finiteness of vanishing seems to be a delicate issue.

Acknowledgements. We thank Igor Shparlinsky for many discussions, especially about results in the book [9].

References

[1] Boris Adamczewski and Jason P. Bell. On vanishing coefficients of algebraic power series over fields of positive characteristic. *Invent. Math.*, 187(2):343–393, 2012.

[2] Jason P. Bell, Shaoshi Chen, and Ehsaan Hossain. Rational dynamical systems, S-units, and D-finite power series. *Algebra Number Theory*, 15(7):1699–1728, 2021.

[3] Jason P. Bell, Dragos Ghioca, and Thomas J. Tucker. *The dynamical Mordell-Lang conjecture*, volume 210 of *Mathematical Surveys and Monographs.* American Mathematical Society, Providence, RI, 2016.

[4] Jean-Paul Bézivin. Une généralisation du théorème de Skolem-Mahler-Lech. *Quart. J. Math. Oxford Ser. (2)*, 40(158):133–138, 1989.

[5] J. W. S. Cassels. *An introduction to Diophantine approximation*, volume No. 45 of *Cambridge Tracts in Mathematics and Mathematical Physics.* Cambridge University Press, New York, 1957.

[6] J. W. S. Cassels. *Local fields*, volume 3 of *London Mathematical Society Student Texts.* Cambridge University Press, Cambridge, 1986.

[7] Harm Derksen. A Skolem-Mahler-Lech theorem in positive characteristic and finite automata. *Invent. Math.*, 168(1):175–224, 2007.

[8] Bernard Dwork, Giovanni Gerotto, and Francis J. Sullivan. *An introduction to G-functions*, volume 133 of *Annals of Mathematics Studies.* Princeton University Press, Princeton, NJ, 1994.

[9] Graham Everest, Alf van der Poorten, Igor Shparlinski, and Thomas Ward. *Recurrence sequences*, volume 104 of *Mathematical Surveys and Monographs.* American Mathematical Society, Providence, RI, 2003.

[10] Philippe Flajolet. Analytic models and ambiguity of context-free languages. volume 49, pages 283–309. 1987. Twelfth international colloquium on automata, languages and programming (Nafplion, 1985).

[11] Philippe Flajolet and Robert Sedgewick. *Analytic combinatorics.* Cambridge University Press, Cambridge, 2009.

[12] Lars Hörmander. *An introduction to complex analysis in several variables*, volume 7 of *North-Holland Mathematical Library.* North-Holland Publishing Co., Amsterdam, third edition, 1990.

[13] Henryk Iwaniec and Emmanuel Kowalski. *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications.* American Mathematical Society, Providence, RI, 2004.

[14] Richard Lipton, Florian Luca, Joris Nieuwveld, Joël Ouaknine, David Purser, and James Worrell. On the Skolem problem and the Skolem conjecture. In *Proceedings of the 37th Annual*

ACM/IEEE Symposium on Logic in Computer Science, LICS '22, New York, NY, USA, 2022. Association for Computing Machinery.

[15] Cordelia Methfessel. On the zeros of recurrence sequences with non-constant coefficients. *Arch. Math. (Basel)*, 74(3):201–206, 2000.

[16] Leo Moser. On non-averaging sets of integers. *Canad. J. Math.*, 5:245–252, 1953.

[17] T. Rivoal and J. Roques. Hadamard products of algebraic functions. *J. Number Theory*, 145:579–603, 2014.

[18] Lee A. Rubel. Some research problems about algebraic differential equations. *Trans. Amer. Math. Soc.*, 280(1):43–52, 1983.

[19] Jean-Pierre Serre. *Lectures on the Mordell-Weil theorem*, volume E15 of *Aspects of Mathematics*. Friedr. Vieweg & Sohn, Braunschweig, 1989.

[20] Richard P. Stanley. Differentiably finite power series. *European J. Combin.*, 1(2):175–188, 1980.

[21] G. Wüstholz. One century of logarithmic forms. In *A panorama of number theory or the view from Baker's garden (Zürich, 1999)*, pages 1–10. Cambridge Univ. Press, Cambridge, 2002.

[22] Junyi Xie. Around the dynamical Mordell–Lang conjecture. *To appear in the Proceedings of the Simons Symposium "Algebraic, Complex, and Arithmetic Dynamics"*, arXiv:2307.05885, 2023.

[23] Umberto Zannier. Hyperelliptic continued fractions and generalized Jacobians. *Amer. J. Math.*, 141(1):1–40, 2019.

[24] Umberto Zannier. *Lecture notes on Diophantine analysis*. EMS Series of Lectures in Mathematics. European Mathematical Society (EMS), Zürich, second edition, [2024] ©2024. With an appendix by Francesco Amoroso.

[25] Umberto Zannier. *Introductory notes on valuation rings and function fields in one variable*. Higher Education Press, Beijing, China, 2026.

Shaoshi Chen, KLMM, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, China
Email address: schen@amss.ac.cn

Pietro Corvaja, Dipartimento di Scienze Matematiche, Informatiche e Fisiche, Università di Udine, Via delle Scienze, 206, 33100 Udine, Italy
Email address: pietro.corvaja@dimi.uniud.it

Umberto Zannier, Scuola Normale Superiore, Classe di Scienze Matematiche e Naturali, Pisa, Italy
Email address: umberto.zannier@sns.it