Invent. math. (2002)
Digital Object Identifier (DOI) 10.1007/s002220200221

Inventiones mathematicae

Finiteness of integral values for the ratio of two linear recurrences

Pietro Corvaja[1], **Umberto Zannier**[2]

[1] Dipartimento di Mat. e Inf., via delle Scienze, 206, 33100 Udine, Italy
(e-mail: corvaja@dimi.uniud.it)
[2] I.U.A.V. – DCA, S. Croce, 191, 30135 Venezia, Italy
(e-mail: zannier@iuav.it)

Oblatum 12-XI-2001 & 31-I-2002
Published online: 29 April 2002 –

Abstract. Let $\{F(n)\}_{n\in\mathbf{N}}$, $\{G(n)\}_{n\in\mathbf{N}}$, be linear recurrent sequences. In this paper we are concerned with the well-known diophantine problem of the finiteness of the set $\mathcal{N}$ of natural numbers n such that $F(n)/G(n)$ is an integer. In this direction we have for instance a deep theorem of van der Poorten; solving a conjecture of Pisot, he established that if $\mathcal{N}$ coincides with $\mathbf{N}$, then $\{F(n)/G(n)\}_{n\in\mathbf{N}}$ is itself a linear recurrence sequence. Here we shall prove that if $\mathcal{N}$ is an infinite set, then there exists a nonzero polynomial P such that $P(n)F(n)/G(n)$ coincides with a linear recurrence for all n in a suitable arithmetic progression. Examples like $F(n) = 2^n - 2$, $G(n) = n + 2^n + (-2)^n$, show that our conclusion is in a sense best-possible. In the proofs we introduce a new method to cope with a notorious crucial difficulty related to the existence of a so-called *dominant root*. In an appendix we shall also prove a zero-density result for $\mathcal{N}$ in the cases when the polynomial P cannot be taken a constant.

1. Introduction

A sequence of complex numbers $\{G(n)\}_{n\in\mathbf{N}}$ is called a *linear recurrence* if there exist complex numbers $c_0, \ldots, c_{k-1}$ $(k \geq 1)$ such that $G(n+k) = c_0G(n) + \ldots + c_{k-1}G(n+k-1)$ for all $n \in \mathbf{N}$. This implies the rationality of the generating function $\sum_{n=0}^{\infty} G(n)X^n$; also, this is equivalent to a (unique) expression

$$G(n) = \sum_{i=1}^{r} g_i(n)\alpha_i^n, \qquad \text{for all } n \in \mathbf{N}, \tag{1}$$

with nonzero polynomials $g_i \in \mathbf{C}[X]$ and distinct nonzero $\alpha_i \in \mathbf{C}^*$, which are classically called the "roots" of the recurrence. The recurrence is called

"simple" when all the $g_i(n)$ are constant. It is said "nondegenerate" when no ratio α_i/α_j, $i \neq j$, is a root of unity. For the general theory, see [vdP2], [S2] or [ShT].

The main result of the present paper is the following

Theorem 1. *Let $F(n)$, $G(n)$ be linear recurrences and let $\mathcal{R}$ be a finitely generated subring of $\mathbf{C}$. Assume that for infinitely many $n \in \mathbf{N}$, we have $G(n) \neq 0$ and $F(n)/G(n) \in \mathcal{R}$. Then there exist a nonzero polynomial $P(X) \in \mathbf{C}[X]$ and positive integers q, r such that both sequences $n \mapsto P(n)F(qn+r)/G(qn+r)$ and $n \mapsto G(qn+r)/P(n)$ are linear recurrences.*

We tacitly mean that $G(qn+r) \neq 0$ for all $n \in \mathbf{N}$. We may reformulate the conclusion by saying that $G(qn+r) = P(n)H(n)$, where H is a linear recurrence dividing (in the appropriate sense) the recurrence $n \mapsto F(qn+r)$. We shall point out later that one cannot always conclude that $G(qn+r)$ divides $F(qn+r)$.

In the same direction, van der Poorten, solving a conjecture of Pisot, proved the "Hadamard-quotient Theorem": *if $F(n)$, $G(n)$ are linear recurrences such that the ratio $F(n)/G(n)$ is an integer for all large $n \in \mathbf{N}$, then $F(n)/G(n)$ is itself a linear recurrence.* In fact, van der Poorten too worked more generally, by assuming that $F(n)/G(n)$ lies in a fixed finitely generated ring for all $n \in \mathbf{N}$. (See [vdP1], or [R] for a more detailed argument.)

Note that in this last statement we need that *all* the values $F(n)/G(n)$ are integral, while in Theorem 1 above it suffices that this holds just for an infinite set. Actually, the problem of handling this much weaker assumption was raised explicitly in [vdP2]. A similar situation occurs in connection with the paper [BPvdP], where the so-called *divisibility sequences* are characterized. The proofs therein use van der Poorten's theorem; the use of Theorem 1 leads to a substantial weakening of the assumptions.

Note that Theorem 1 corresponds to a finiteness result for semi-exponential diophantine equations $F(x) = yG(x)$. Diophantine equations involving recurrences have indeed an old tradition. (See e.g. [L], [vdP2], [S2], [ShT].) M. Laurent [L] investigated the general semi-exponential equation. He was able to prove finiteness in remarkable generality. However, our equations, though linear in y, escape from his analysis.

Among other papers involving divisibility between values of recurrences, we mention e.g. [E], where the condition $G(n)|G(m)$, for an $m < n$, is studied, for a recurrence $G(n)$. The methods of the present paper should allow to deal with the more general condition $G(n)|F(m)$ for $m \ll n$.

In his proof, van der Poorten first treated the fundamental number-field case by means of ingenious auxiliary constructions of p-adic nature.[1] Then he reduced to this case by specialization arguments. Such a method of proof does not yield any information towards the proof of Theorem 1, namely under the much weaker assumption that $F(n)/G(n)$ is an integer infinitely

[1] Similar but incomplete arguments also appeared in the paper [P].

often. The specialization arguments are still possible, but the proof breaks down in the number field case.

In the paper [CZ], among others, we attacked such questions by means of the Schmidt Subspace Theorem. We considered only the case of simple recurrences with positive integer roots (i.e. $\alpha_i \in \mathbf{N}$) and constant coefficients $g_i \in \mathbf{Q}$, obtaining in this case a complete answer. In particular, we proved [CZ, Theorem 1] that *if $F(n)/G(n)$ is an integer infinitely often, where F, G are simple recurrences with positive integer roots, then F/G is again a linear recurrence of that type*.

As observed in [CZ] (see the few lines following Theorem 1 as well as Remarks 4 and 5), our method in fact could be applied successfully with the only assumption that the recurrence $G(n)$ admits a *dominant root* with respect to some valuation of the relevant number field K. By this we mean that *there exists an absolute value v of K such that $G(n)$ admits a unique root which is maximal with respect to v*. This assumption, though rather weak, had represented a well-known crucial difficulty in the whole subject of diophantine properties of recurrence sequences.

Let us look a little more closely at this assumption. When $G(n)$ is nondegenerate and has at most two roots, one verifies that a dominant root exists. However, there are nondegenerate examples with three or more roots, when the assumption is not verified. A particularly simple and elegant instance has been proposed to us by Pethö. He starts with an analogue of the Fibonacci sequence, defining $G(n)$ by $G(0) = G(1) = 0$, $G(2) = 1$ and $G(n+3) = G(n+2) + G(n+1) + G(n)$. This recurrence admits three roots α_i which are the solutions of the equation $X^3 = X^2 + X + 1$. It is nondegenerate and the unique real root is "dominant" with respect to the standard complex absolute value. In particular, the methods of [CZ] apply to $F(n)/G(n)$ for any recurrence F. If we now change $G(n)$ with $G(-n)$ the roots become the α_i^{-1} and one may check that the dominant-root assumption is not verified, for any choice of the valuation. And then, even a simply stated question such as *"does $G(-n)$ divide $2^n + 1$ infinitely often?"* does not fall into the realm of [CZ] nor in any other known method, to the best of our knowledge.

Theorem 1 answers generally such questions, showing that the dominant-root assumption, as well as any other technical hypothesis, may be completely removed. We shall derive it in a moment from our next result, namely

Theorem 2. *Let $F(n), G(n)$ be linear recurrences such that their roots generate together a torsion-free multiplicative group. Let $\mathcal{R}$ be a finitely generated subring of $\mathbf{C}$ and assume that for infinitely many $n \in \mathbf{N}$, we have $G(n) \neq 0$ and $F(n)/G(n) \in \mathcal{R}$. Then there exists a nonzero polynomial $P(X) \in \mathbf{C}[X]$ such that both sequences $n \mapsto P(n)F(n)/G(n)$ and $n \mapsto G(n)/P(n)$ are linear recurrences.*

We pause, to note that the condition "$G(n) \neq 0$" is described by the Skolem-Mahler-Lech Theorem (see e.g. [vdP2] for an elegant proof). This asserts that the set of zeros of a linear recurrence is a union of a finite

set with a finite union of arithmetic progressions. When G is nonzero and nondegenerate, it is a finite set. In particular, under the assumptions for Theorem 2 we have $G(n) \neq 0$ for all large $n \in \mathbf{N}$; we shall often use this remark in the proofs.

The "torsion-free" assumption in Theorem 2 is harmless, and may in fact be considered as a normalization condition. For this reason we shall assume it in our next statements. The condition may be actually achieved just by partitioning $\mathbf{N}$ into a finite number of suitable arithmetic progressions and by considering separately the restrictions of the involved functions to each progression. We illustrate this by deducing Theorem 1 from Theorem 2. Observe that, if q is the order of the torsion in the multiplicative group Γ generated by the roots of F, G altogether, then for each $r = 0, 1, \dots, q-1$, the recurrences $F_r(n) = F(nq + r)$, $G_r(n) = G(nq + r)$ have roots generating a torsion-free group: in fact, their roots are among the q-th powers of the roots of F and G, so they lie in the torsion-free group Γ^q. To obtain Theorem 1 it now suffices to take into account Theorem 2 for each of these pairs of recurrences. We note that this argument in fact produces a possible modulus q for Theorem 1. In general one cannot take $q = 1$ there, even if F, G are both nondegenerate: a simple counterexample is provided by $F(n) = 2^n + 1$, $G(n) = 2^n + (-1)^n$.

In many cases (but not always!) the polynomial P may be directly taken to be a constant. For instance it suffices that G has no polynomial factors; in fact, we have

Corollary 1. *Let $F, G, \mathcal{R}$ be as in Theorem 2, and assume moreover that in the canonical expression (1), the g_i are coprime polynomials. Then, if $F(n)/G(n)$ lies in $\mathcal{R}$ for infinitely many $n \in \mathbf{N}$, the sequence $n \mapsto F(n)/G(n)$ is a linear recurrence.*

This of course applies when G is a simple recurrence. (Without the assumption that the relevant group is torsion-free, we have a conclusion analogous to Theorem 1.) This corollary is a direct consequence of Theorem 2: in fact, if $P(n)$ is as in that theorem, we have in particular that $G(n)/P(n)$ is a linear recurrence, which we write in the form $\sum_{i=1}^{s} \tilde{g}_i(n)\tilde{\alpha}_i^n$, with nonzero polynomials $\tilde{g}_i$ and distinct $\tilde{\alpha}_i \in \mathbf{C}^*$. From the uniqueness of the expression (1), it follows that $r = s$ and $g_i = P\tilde{g}_{\sigma(i)}$ for $i = 1, \dots, r$, where σ is a permutation of $\{1, \dots, r\}$. By the coprimality assumption in the corollary, $P(n)$ is then a nonzero constant c and by Theorem 2 again, $cF(n)/G(n)$ is a linear recurrence, so the same holds for $F(n)/G(n)$.

More generally, this argument shows that $P(n)$ may be taken as a GCD of the g_i's in (1).

Note however that in Theorems 1,2, we cannot generally take $P(n)$ to be a constant. This is shown by examples like $F(n) = 2^n$, $G(n) = n^d$, or $F(n) = 2^n - 2$, $G(n) = n$. In this last example, the set of integers n such that $F(n)/G(n)$ is an integer not only is infinite but contains the set of prime numbers, which is fairly "large" in $\mathbf{N}$. As a counterpart, we state our last result, where we restrict to number fields for simplicity.

Corollary 2. *Let F, G be recurrence sequences with coefficients and roots in a number field K, and assume that their roots generate a torsion-free group. Let $\mathcal{R} \subset K$ be finitely generated. Then, either $F(n)/G(n)$ is a linear recurrence, or the set of integers $n \in \mathbf{N}$ such that $F(n)/G(n) \in \mathcal{R}$ has zero density.*

The conclusion means that the proportion of relevant integers in an interval $1 \leq n \leq X$ tends to zero as $X \to \infty$. This result gives as a byproduct a sharpening of the mentioned theorem by van der Poorten (see Remark 3 below). Also, in the special case of the equations $F(x) = yG(x)$, this answers a question by Laurent [L] who asked whether "almost all" the integral solutions must come from an algebraic identity. The deduction of this corollary falls somewhat apart from the main theme of the paper, and so will be given in an appendix. There, we shall also briefly discuss some examples as to whether $F(n)/G(n)$ can be an integer infinitely often, when G is a polynomial.

Remarks. **(1)** We stress that for given recurrences F, G, it is easy to test effectively whether the conclusions of the theorems hold, actually in a purely algebraic way (i.e. there is no more arithmetic involved). We have already noted that the polynomial P may be determined by G and moreover it is well known (and we shall prove it again in Lemma 2.1 below) that F, G correspond to certain (Laurent) polynomials f, g in several variables, in such a way that the given condition amounts to check divisibility of Pf by g in the relevant polynomial ring. It is an easy well-known fact that such a test admits an effective procedure.

(2) Corollary 1 admits the obvious converse stating that if the conclusion is true, the values $F(n)/G(n)$ all lie in some fixed finitely generated ring.

On the other hand, there is no simple general converse for Theorems 1 or 2: take e.g. $F(n) = 2^n$ and $G(n) = n$ or $G(n) = n(n+1)$. In both cases the conclusions are satisfied. However, while in the first case the relevant set is infinite, this cannot happen in the second case, no matter $\mathcal{R}$, in virtue of the well-known fact that the greatest prime factor of $n(n+1)$ tends to infinity with n.

However, if we assume the conclusions of Theorems 1,2, we find that the values $F(n)/G(n)$ are "quasi integral", in the sense that the denominators grow polynomially rather than exponentially. With this in mind, we note that our arguments in fact lead to slightly more general results. In the number-field case we may prove that *if there exist nonzero integers d_n such that* $\log |d_n| = o(n)$ *and* $d_n F(n)/G(n) \in \mathcal{R}$ *for infinitely many* $n \in \mathbf{N}$*, then the conclusion of Theorem 1 holds*. It is this more technical formulation which admits a simple converse, similarly to Corollary 1.

For the sake of simplicity we omit the proofs, which do not involve new difficulties. In some cases (e.g. $F(n) = b^n - 1$, $G(n) = a^n - 1$) it is even possible to obtain nearly best-possible upper bounds for $\mathrm{GCD}(F(n), G(n))$: see [BCZ].

(3) The mentioned theorem by van der Poorten (i.e. a former conjecture by Pisot) follows easily from Theorem 1. We sketch the argument in the crucial number-field case. First, we recall the elementary result by Cantor [C] (proved long before van der Poorten's solution) that *if a sequence* $\{H(n)\}_{n\in\mathbf{N}}$ *of S-integers is such that* $H_1(n) := P(n)H(n)$ *is a recurrence for some nonzero polynomial* P*, then* $H(n)$ *is itself a recurrence.* (See e.g. [vdP2] or [R] for a sketch of the simple proof, as well as the present Appendix for a quantitative version of the argument.)

Assume now that $F(n)/G(n)$ is an S-integer for all large $n \in \mathbf{N}$, and let q be the order of the torsion in the group generated by the roots of F, G. As above we find that the recurrences $n \mapsto F(qn + r)$, $n \mapsto G(qn + r)$ have roots generating a torsion-free group, whence Theorem 2 implies that $P_r(n)F(qn + r)/G(qn + r)$ is a recurrence for $r = 0, \dots, q - 1$, where $P_0, \dots P_{q-1}$ are suitable nonzero polynomials. Applying Cantor's result for $r = 0, 1, \dots, q - 1$ then shows that each $a_r(n) := F(qn + r)/G(qn + r)$ is a linear recurrence.

In turn, we find that the power series $f_r(X) := \sum_{n=0}^{\infty} a_r(n)X^n$ is rational for each $r = 0, 1, \dots, q - 1$. Therefore $\sum_{n=0}^{\infty} \frac{F(n)}{G(n)} X^n = \sum_{r=0}^{q-1} X^r f_r(X^q)$ is rational as well, and the final conclusion follows at once.

By using Corollary 2 in place of Cantor's result, one may correspondingly strengthen van der Poorten's Theorem.

2. Proofs

In this section we shall prove Theorem 2 in the crucial case of number-fields. In the next section we shall apply specialization arguments to deduce it in full generality.

As in [CZ], our arguments will make heavy use of the Schmidt Subspace Theorem. For the reader's convenience, we state a relevant version of it, due to H.P. Schlickewei:

Subspace Theorem. *Let* K *be a number field,* S *be a finite set of absolute values of* K *containing the archimedean ones,* $N \geq 1$ *be an integer. Let, for each* $v \in S$, $L_{v,1}, \dots, L_{v,N}$ *be linearly independent linear forms in* N *variables, defined over* K*. Then, for every* $\epsilon > 0$*, the solutions of the inequality*

$$\log(\prod_{i=1}^{N} \prod_{v\in S} |L_{v,i}(\mathbf{x})|_v) < -\epsilon h(\mathbf{x})$$

in points $\mathbf{x} \in \mathcal{O}_S^N$ *are contained in a finite union of hyperplanes of* K^N *defined over* K.

Here as usual $h(\cdot)$ is the absolute logarithmic Weil height and the absolute values v are normalized so that for $x \in K^*$, $h(x) = \sum_v \log \max(1, |x|_v)$, the sum running over all places of K. Also, $\mathcal{O}_S$ denotes the ring of S-integers

in K made up of all $x \in K$ with $|x|_v \leq 1$ for all $v \notin S$. This statement follows immediately from the projective version [S1, Theorem 1D′], taking into account that here the coordinates of $\mathbf{x}$ lie in $\mathcal{O}_S$.

A brief outline of the proof. Our strategy for the proof will be roughly as follows, where to fix ideas we shall assume that all the involved recurrences are simple. A first easier case occurs when G has a dominant root with respect to some place v of K. Now, as in [CZ, Theorem 1], we may expand $F(n)/G(n)$ as a convergent "recurrence with infinitely many roots". Truncating the expansion allows us to approximate $F(n)/G(n)$ by a recurrence $H(n)$. At this point we may apply the Subspace Theorem: namely, we view the difference $(F(n)/G(n)) - H(n)$ as a "small" linear form, where the variables are represented by the integer $F(n)/G(n)$ and by the n-th powers of the roots of the approximating recurrence $H(n)$. This yields the conclusion.

When a dominant root does not exist, we may still approximate $F(n)/G(n)$ by using simultaneously all the roots with maximal absolute value (as in formula (2.3) below). However the previous method is no longer sufficient, since the term $F(n)/G(n)$ now appears in too many of the variables in the relevant linear form; the effect of these "bad" variables (they are S-integers, but not necessarily S-units) is that the inequality needed for the Subspace Theorem does not hold in general.

We can get rid of this difficulty by constructing many other small linear forms, linearly independent, out from the given one. This may be done, somewhat surprisingly, just by multiplying the given small linear form by suitable terms of the form β^n, for β a monomial in the dominant roots. In this way, the total number of bad variables also increases, but not enough to compensate what is gained. We believe that this principle may be helpful in a more general context as well.

We now go on with the details. As in Theorem 2, we shall restrict our attention to the class of linear recurrences having roots which belong to a given torsion-free multiplicative group. (We have already remarked that this normalization is not a real restriction.) The structure of the ring of such recurrences is clarified by the following known lemma (see e.g. [vdP2] and [R]), whose short proof we give for completeness.

Lemma 2.1. *Let $\Gamma \subset \mathbf{C}^*$ be a torsion-free multiplicative subgroup of rank $t \geq 1$. The ring of linear recurrences whose roots belong to Γ is isomorphic to the ring $\mathbf{C}[X, T_1, \ldots, T_t, T_1^{-1}, \ldots, T_t^{-1}]$. In particular it is a unique factorization domain.*

Proof. Let $(\beta_1, \ldots, \beta_t)$ be a basis of Γ. Note that $\beta_1, \ldots, \beta_t$ are multiplicatively independent. To each variable T_i $(i = 1, \ldots, t)$ we associate the exponential function $n \mapsto \beta_i^n$. To the variable X we associate the identity function $n \mapsto n$. We thus obtain a surjective ring homomorphism from $\mathbf{C}[X, T_1, \ldots, T_t, T_1^{-1}, \ldots, T_t^{-1}]$ to the ring of linear recurrences having their roots in Γ. Injectivity follows from the fact that $\beta_1, \ldots, \beta_t$ are multiplicatively independent, whence, as is well known, the functions $n \mapsto n$, $n \mapsto \beta_1^n, \ldots, n \mapsto \beta_t^n$ are algebraically independent.

In virtue of this result, when dealing with recurrences having roots in a given Γ, we will view them as elements of a ring $\mathbf{C}[X, T_1, \dots, T_t, T_1^{-1}, \dots, T_t^{-1}]$ as in Lemma 2.1; correspondingly, divisibility properties such as coprimality, will be understood in this sense. (It may be worthwile to note that enlarging Γ does not affect coprimality in the corresponding ring of Laurent polynomials. This is easily checked, and in any case will not be needed in what follows, so we omit the proof.)

We now state a proposition which represents the fundamental point in the paper.

Proposition 2.1. *Let K be a number field, S be a finite set of absolute values of K containing the archimedean ones, $F(n), G(n)$ be linear recurrences with roots and coefficients in K. Suppose that the roots of F and G generate a torsion-free multiplicative subgroup Γ of K^*. Suppose also that F and G are coprime (with respect to Γ) and that G has more than one root. Then the set of integers*

$$\mathcal{N} := \left\{ n \in \mathbf{N} \;\middle|\; \frac{F(n)}{G(n)} \in \mathcal{O}_S \right\}$$

is finite.

This immediately implies Theorem 2 in the crucial number-field case, i.e. when all the involved quantities are algebraic numbers. In fact, after simplification of the fraction F/G, we may assume that F, G are coprime (in the notion introduced above). Now, if $G(n) = P(n)\beta^n$ (P a polynomial) has only one root β, the conclusion of Theorem 2 holds. Otherwise, we may apply the proposition, by choosing K and S large enough so that $\mathcal{R} \subset \mathcal{O}_S$. We obtain that $\mathcal{N}$ is finite, in contradiction with the assumptions for Theorem 2.

Proof of Proposition 2.1. Without loss we may enlarge S and assume that it is a finite set of absolute values of K containing the archimedean ones, and such that all the roots and nonzero coefficients of F, G are S-units in K.

By assumption G has at least two roots, and no ratio of two of them can be a root of unity, because Γ is torsion-free. Therefore there exists a place ν of K such that not all of the roots of G have the same ν-adic absolute value. Automatically, $\nu \in S$. For simplicity of notation, we replace $F(n)$ (resp. $G(n)$) by $F(n)/\beta^n$ (resp. $G(n)/\beta^n$), where β is some root of $G(n)$ with maximal absolute value with respect to ν; this does not affect assumptions and conclusions, and leads to the case when the maximal ν-adic absolute value of the roots of $G(n)$ is 1.

Then we can write $G(n)$ as the difference of two linear recurrences

$$G(n) = G_1(n) - R(n),$$

where G_1 is a nonzero linear recurrence whose roots have ν-adic absolute value 1 while all the roots of the nonzero recurrence R have ν-adic absolute value strictly less then 1.

Recall that the roots of F, G generate a free abelian multiplicative group Γ. Let Γ^* be the subgroup of Γ formed with elements of ν-adic absolute value 1. Note that this is a *primitive* subgroup, namely, Γ/Γ^* is torsion-free. It is an elementary known fact that then there exists a basis $\beta_1, \dots, \beta_t$ for Γ such that $\beta_1, \dots, \beta_p$ is a basis for Γ^*. (Just pick a basis of Γ^* and complete it with representatives in Γ for a basis of Γ/Γ^*.)

Since all the roots of G_1 have ν-adic absolute value equal to 1, they lie in Γ^* and we may write

$$G_1(n) = g\big(n, \beta_1^n, \dots, \beta_p^n\big), \tag{2.1}$$

where $g \in K[X, T_1, T_1^{-1}, \dots, T_p, T_p^{-1}]$. By multiplying both F, G by a suitable power of $\beta_1^n \cdots \beta_p^n$ (which again does not affect assumptions and conclusions), we may assume that g is in fact a polynomial in its arguments, say of total degree $\leq D$.

By our assumption on the roots of R, there exists a positive real number $\rho < 1$ such that

$$|R(n)|_\nu \ll \rho^n. \tag{2.2}$$

For $G(n) \neq 0$, put $z_n := \dfrac{F(n)}{G(n)}$. We suppose that for all n in an infinite set $\mathcal{N}$ of positive integers, we have $G(n) \neq 0$ and $z_n \in \mathcal{O}_S$; we proceed to derive a contradiction.

We fix a positive integer s and write

$$G_1(n)^s = (G(n) + R(n))^s = G(n)\left(\sum_{i=0}^{s-1} \binom{s}{i} G(n)^{s-1-i} R(n)^i\right) + R(n)^s.$$

Therefore

$$\begin{aligned} G_1(n)^s z_n &= G_1(n)^s \frac{F(n)}{G(n)} \\ &= F(n)\left(\sum_{i=0}^{s-1} \binom{s}{i} G(n)^{s-1-i} R(n)^i\right) + \frac{F(n)}{G(n)} R(n)^s, \end{aligned}$$

whence, by (2.2)

$$\left| G_1(n)^s z_n - F(n) \sum_{i=0}^{s-1} \binom{s}{i} G(n)^{s-1-i} R(n)^i \right|_\nu \ll \rho^{ns} |z_n|_\nu. \tag{2.3}$$

We now fix two other positive integers h, k; later on we shall impose that s, h, k satisfy suitable inequalities.

For every $\mathbf{d} = (d_1, \dots, d_p) \in \mathbf{N}^p$, with $d_1 + \ldots + d_p \leq h$, and every $u \in \mathbf{N}$ with $u < k$, we consider the quantity

$$\phi_{\mathbf{d},u}(n) := n^u \underline{\beta}^{n\mathbf{d}} \left(G_1(n)^s z_n - F(n) \sum_{i=0}^{s-1} \binom{s}{i} G(n)^{s-1-i} R(n)^i \right), \quad (2.4)$$

where we have abbreviated $\underline{\beta}^{(a_1,\dots,a_p)} = \beta_1^{a_1} \cdots \beta_p^{a_p}$.

Inequality (2.3) and the fact that $|\beta_i|_v = 1$ for $i = 1, \dots, p$ give

$$|\phi_{\mathbf{d},u}(n)|_v \ll \rho^{ns} |z_n|_v n^u, \quad (2.5)$$

where we have used the bound $|n|_v \le n$.

Let us remark that the term $n^u \underline{\beta}^{n\mathbf{d}} G_1(n)^s z_n$ appearing in the right side of (2.4) can be written as

$$n^u \underline{\beta}^{n\mathbf{d}} G_1(n)^s z_n = \sum_{\mathbf{b},l} p_{\mathbf{b},l,\mathbf{d},u} n^l \underline{\beta}^{n\mathbf{b}} z_n \quad (2.6)$$

where the coefficients $p_{\mathbf{b},l,\mathbf{d},u}$ belong to K and the index $(\mathbf{b}, l)$ runs over the vectors $(b_1, \dots, b_p, l) \in \mathbf{N}^{p+1}$ with $b_1 + \ldots + b_p \le h + sD, 0 \le l < k + sD$. This follows from our previous expression (2.1) of G_1 as a polynomial of degree $\le D$ in $n, \beta_1^n, \dots, \beta_p^n$.

Put

$$N_1 := \binom{p + h + sD}{p} \cdot (k + sD).$$

Observe that N_1 represents the number of monomials of the form $X^l T_1^{b_1} \cdots T_p^{b_p}$, with natural numbers $l < k + sD$ and $b_1 + \ldots + b_p \le h + sD$. Then the number of nonzero terms on the right of (2.6) is $\le N_1$.

We denote by $H(n)$ the recurrence $-F(n) \sum_{i=0}^{s-1} \binom{s}{i} G(n)^{s-1-i} R(n)^i$, so the other term on the right side of (2.4) is $n^u \underline{\beta}^{n\mathbf{d}} H(n)$.

Note that the recurrence $H(n)$ may be expanded as a sum of terms each of the type $n^l \alpha^n$, for suitable l and $\alpha \in \Gamma$. Therefore the remaining part of (2.4) is a linear combination of terms of the type $n^{u+l} (\underline{\beta}^{\mathbf{d}} \alpha)^n$, for suitable $u, \mathbf{d}, l, \alpha$. We let N_2 be the cardinality of the set of all such terms.

Finally, we let $N = N_1 + N_2$, so in particular we can write $\phi_{\mathbf{d},u}$ as a linear combination of at most N nonzero terms of the mentioned types.

Let us choose an ordering for the N_1 terms of the form $n^l \underline{\beta}^{n\mathbf{b}} z_n$ with $0 \le l < k + sD$, $b_1 + \ldots + b_p \le h + sD$, and denote such terms with $x_1(n), \dots, x_{N_1}(n)$. Then we can write (2.6) as

$$n^u \underline{\beta}^{n\mathbf{d}} G_1(n)^s z_n = A_{\mathbf{d},u,1} x_1(n) + \ldots + A_{\mathbf{d},u,N_1} x_{N_1}(n).$$

Here the coefficients $A_{\mathbf{d},u,i}$ for $i = 1, \dots, N_1$ are the same as the $p_{\mathbf{b},l,\mathbf{d},u}$ (appearing in (2.6)) in a suitable ordering.

We do the same for the remaining part of (2.4); namely, we choose an ordering for the N_2 mentioned terms and write

$$n^u \underline{\beta}^{n\mathbf{d}} H(n) = A_{\mathbf{d},u,N_1+1} x_{N_1+1}(n) + \ldots + A_{\mathbf{d},u,N_1+N_2} x_{N_1+N_2}(n),$$

where each of the terms $x_i(n)$ for $N_1 < i \leq N = N_1 + N_2$ is of the mentioned type. In particular, of the type $n^v\gamma^n$ for suitable v's in $\mathbf{N}$ and suitable γ's in Γ.

Observe that by assumption the point $\mathbf{x}(n) := (x_1(n), \ldots, x_N(n))$ has S-integers coordinates for all $n \in \mathcal{N}$.

Let us now further define an ordering for the vectors $(\mathbf{d}, u) \in \mathbf{N}^p \times \mathbf{N}$ with $d_1 + \ldots + d_p \leq h$ and $0 \leq u < k$ and let M be their number. Then

$$M := \binom{p+h}{p} \cdot k,$$

so in particular $M < N_1$, since $s > 0$.

If $(\mathbf{d}, u)$ is the j-th vector with respect to the chosen ordering we put

$$L_j(X_1, \ldots, X_N) = \sum_{i=1}^{N} A_{\mathbf{d},u,i} X_i, \qquad j = 1, \ldots, M. \tag{2.7}$$

These L_j are linear forms in N variables with coefficients in K. They verify the important formula

$$\phi_{\mathbf{d},u}(n) = L_j(x_1(n), \ldots, x_N(n)). \tag{2.8}$$

We now pause to prove a lemma.

Lemma 2.2. *The linear forms* $L_1(X_1, \ldots, X_{N_1}, 0, \ldots, 0), \ldots, L_M(X_1, \ldots, X_{N_1}, 0, \ldots, 0)$ *are linearly independent.*

Proof. Observe that, beyond (2.8), we also have the formula

$$L_j(x_1(n), \ldots, x_{N_1}(n), 0, \ldots, 0) = n^u \underline{\beta}^{n\mathbf{d}} G_1(n)^s z_n,$$

where $(\mathbf{d}, u)$ is the j-th vector in the given ordering. This formula holds just by construction. Now, a dependence relation among the linear forms $L_1(X_1, \ldots, X_{N_1}, 0, \ldots, 0), \ldots, L_M(X_1, \ldots, X_{N_1}, 0, \ldots, 0)$, entails a relation $(\sum_{u,\mathbf{d}} c_{u,\mathbf{d}} n^u \underline{\beta}^{n\mathbf{d}}) G_1^s(n) z_n = 0$, valid for all integers $n \in \mathbf{N}$, where not all the $c_{u,\mathbf{d}}$ are zero. Now, $G_1^s(n) z_n$ can vanish only for finitely many integers n, by the Skolem-Mahler-Lech Theorem. Also, no ratio of two terms of the form $\underline{\beta}^{n\mathbf{d}}$ for two distinct values of $\mathbf{d}$, can be a root of unity, since the β_i are multiplicatively independent by assumption. Therefore, by the Skolem-Mahler-Lech Theorem again, the sum into brackets is nonzero for large n. This is a contradiction, which proves the lemma.

Applying the lemma and renumbering if necessary the first N_1 variables, we may thus assume that $L_1, \ldots, L_M, X_{M+1}, \ldots, X_N$ are linearly independent.

Let us now define linear forms $L_{v,j}(\mathbf{X}) \in K[X_1, \ldots, X_N]$ in N variables, for $(v, j) \in S \times \{1, \ldots, N\}$, as follows. For $j \leq M$ put

$$L_{v,j}(\mathbf{X}) = L_j(\mathbf{X})$$

where $L_j(\mathbf{X})$ is defined in (2.7). For all other pairs $(v, j) \in S \times \{1, \dots, N\}$, put

$$L_{v,j}(\mathbf{X}) = X_j.$$

We shall apply the Subspace Theorem with this choice for the linear forms. We observe that the independence assumption is verified for each $v \in S$: this is clear for $v \neq \nu$ and follows from Lemma 2.2 and the subsequent remark for $v = \nu$.

We consider a double product made out of the previously defined linear forms and vectors, namely:

$$\prod_{i=1}^{N} \prod_{v \in S} |L_{v,i}(x_1(n), \dots, x_N(n))|_v. \tag{2.9}$$

We have already observed that for $j \leq N_1$, $x_j(n) = n^l \underline{\beta}^{n\mathbf{b}} z_n$ for a suitable vector $(\mathbf{b}, l)$ depending on j; hence $x_j(n) = 0$ if and only if z_n vanishes. This may happen only for finitely many n, in view of the previously mentioned Skolem-Mahler-Lech Theorem. We shall disregard this finite set, and so assume that $x_j(n) \neq 0$ for $j = 1, \dots, N_1$. Since the linear forms $L_{v,j}(\mathbf{X})$ with either $j > M$ or $v \neq \nu$ are just the projections X_j, the double product (2.9) can be rewritten as

$$\left(\prod_{j=1}^{N} \prod_{v \in S} |x_j(n)|_v \right) \cdot \left(\prod_{j=1}^{M} \frac{|L_{v,j}(x_1(n), \dots, x_N(n))|_v}{|x_j(n)|_v} \right).$$

In order to apply the Subspace Theorem to the S-integer vectors $(x_1(n), \dots, x_N(n))$, for n in the set $\mathcal{N}$ in the statement of the Proposition (recall that we are assuming that $\mathcal{N}$ is infinite by contradiction), we shall estimate separately both factors.

Recall that the terms $x_j(n)$ are either of the form $n^l \underline{\beta}^{n\mathbf{b}} z_n$ (if $j \leq N_1$) or of the form $n^l \alpha^n$, $(N_1 < j \leq N)$ for suitable integers l and S-units α depending on j. We let L be an upper bound for all exponents l in n^l in these expressions.

Taking the product over all places of S, the S-unit part disappears by the product formula, whence we see that the first factor is bounded according to the inequality

$$\log \left(\prod_{j=1}^{N} \prod_{v \in S} |x_j(n)|_v \right) \leq NL \log n + N_1 h(z_n).$$

In order to estimate the second factor, we shall exploit the bound (2.5) for the ν-adic absolute values of the quantities $\phi_{\mathbf{d},u}$. Observe that since $M < N_1$, all the terms $x_j(n)$ with $j \leq M$ are of the form $n^l \underline{\beta}^{n\mathbf{b}} z_n$ for suitable $(l, \mathbf{b})$

depending on j. Also, $|\underline{\beta}^{n\mathbf{d}}|_v = 1$. Hence, for $1 \le j \le M$, we find

$$\log |x_j(n)|_v = \log |z_n|_v + l \log |n|_v,$$

for a suitable $l \in \{0, \dots, L\}$, depending on j. Then we obtain from (2.5) and (2.8) that for each $j = 1, \dots, M$,

$$\log \left(\frac{|L_{v,j}(x_1(n), \dots, x_N(n))|_v}{|x_j(n)|_v} \right) \le sn \log \rho + 2L \log n.$$

Taking the product over all indices $j = 1, \dots, M$ we then obtain

$$\log \left(\prod_{j=1}^{M} \frac{|L_{v,j}(x_1(n), \dots, x_N(n))|_v}{|x_j(n)|_v} \right) \le M \left(sn \log \rho + 2L \log n \right).$$

Finally, for large $n \in \mathcal{N}$, the double product (2.9) can be estimated by

$$\begin{aligned} &\log \Big(\prod_{i=1}^{N} \prod_{v \in S} |L_{v,i}(x_1(n), \dots, x_N(n))|_v \Big) \\ &\le M \left(sn \log \rho + 2L \log n \right) + N_1 h(z_n) + NL \log n \\ &\le N_1 h(z_n) + Msn \log \rho + 3NL \log n. \end{aligned} \tag{2.10}$$

The height of $z_n = F(n)/G(n)$ plainly verifies

$$h(z_n) \le h(F(n)) + h(G(n)) \le nC_1,$$

for large values of n, where C_1 is a positive number depending only on F, G. Using this in (2.10), we find

$$\log \Big(\prod_{i=1}^{N} \prod_{v \in S} |L_{v,i}(x_1(n), \dots, x_N(n))|_v \Big) \le (C_1 N_1 + Ms \log \rho) n + 3NL \log n. \tag{2.11}$$

Define $C_2 = C_1 / - \log \rho$; this is a positive real number depending only on F, G. Choose $s > 2C_2$ and $k > 3sD$. Then $sk > 2C_2 k > \frac{3}{2} C_2 (k + sD)$. Now, the function $\binom{p+x}{p}$ is a polynomial of degree p, whence, for large h,

$$sk \binom{p+h}{p} > C_2 (k + sD) \binom{p + sD + h}{p}.$$

In fact for fixed s, D, C_2, k, p with $s > 2C_2$ and $k > 3sD$, both sides are polynomials in h of the same degree p, and the leading coefficient on the left side is larger then the one on the right.

Therefore, we may choose h sufficiently large so that this inequality is verified.

(This inequality actually represents the fundamental point. It expresses the fact that in the vector $\mathbf{x}(n)$, the number of coordinates involving z_n is not too large.)

In turn, the inequality means that $C_1 N_1 < -Ms \log \rho$, so (2.11) implies

$$\log(\prod_{i=1}^{N} \prod_{v \in S} |L_{v,i}(x_1(n), \ldots, x_N(n))|_v) < -C_3 n, \tag{2.12}$$

for large $n \in \mathcal{N}$, where now C_3 is a suitable positive number independent of n.

In order to apply the Subspace Theorem, we just need an estimate for the height of the point $\mathbf{x}(n)$. This is easily obtained, since each coordinate has exponential growth at most, so we have $h(\mathbf{x}(n)) \leq C_4 n$, where $C_4 > 0$ does not depend on n. Then (2.12) implies that

$$\log(\prod_{i=1}^{N} \prod_{v \in S} |L_{v,i}(x_1(n), \ldots, x_N(n))|_v) < -\frac{C_3}{C_4} h(\mathbf{x}(n)). \tag{2.13}$$

We are therefore able to apply the above stated version of Subspace Theorem, with $\epsilon = C_3/C_4$, concluding that there exists a nontrivial linear relation of the kind

$$A_1 x_1(n) + \ldots + A_N x_N(n) = 0,$$

with $A_1, \ldots, A_N \in K$, not all zero, valid for infinitely many $n \in \mathcal{N}$. Let us rewrite this dependence relation as $A_1 x_1(n) + \ldots + A_{N_1} x_{N_1}(n) = -A_{N_1+1} x_{N_1+1}(n) - \ldots - A_N x_N(n)$.

Recall that the terms $x_j(n)$ are of the form $n^l \underline{\beta}^{n\mathbf{b}} z_n$ for $j \leq N_1$, and of the form $n^l \alpha^n$ for $N_1 < j \leq N$, where the α's lie in the torsion-free group Γ. Thus we obtain a relation of the kind

$$z_n A(n) = B(n),$$

valid for an infinite subsequence of integers $n \in \mathcal{N}$, where $A(n)$ and $B(n)$ are linear recurrences with roots in Γ, and where all the roots of $A(n)$ lie in the group Γ^* generated by $\beta_1, \ldots, \beta_p$.

Observe that the coefficients $A_1, \ldots, A_{N_1}$ cannot all be zero, for otherwise $B(n)$ would vanish for an infinite sequence of integers. By the Skolem-Mahler-Lech Theorem, this in turn would imply that $A_i = 0$ for all $i = 1, \ldots, N$, a contradiction.

Therefore $A(n)$ is a nonzero recurrence whose roots lie in the subgroup Γ^* of Γ.

Recall also that by definition $z_n = F(n)/G(n)$, whence we obtain the relation

$$F(n)A(n) = B(n)G(n),$$

for infinitely many $n \in \mathcal{N}$, where all the four recurrences have their roots in Γ. By the Skolem-Mahler-Lech Theorem again, this relation holds identically, and corresponds by Lemma 2.1 to a relation

$$fa = bg,$$

in the ring $\mathcal{A} = \mathbf{C}[X, T_1, \dots, T_t, T_1^{-1}, \dots, T_t^{-1}]$, obtained as in the proof of that lemma, where we may use the basis $\beta_1, \dots, \beta_p, \dots, \beta_t$ for Γ.

By the assumptions of the proposition, g is coprime with f, whence g must divide a.

Now, the Laurent polynomial a in fact lies in the ring $\mathbf{C}[X, T_1, \dots, T_p, T_1^{-1}, \dots, T_p^{-1}]$ (since $A(n)$ has its roots in Γ^*). It easily follows that g must be of the form $g = g_1\mu$, where μ is a product of powers of the T_i, $i = 1, \dots, t$, and $g_1 \in \mathbf{C}[X, T_1, \dots, T_p, T_1^{-1}, \dots, T_p^{-1}]$.

However, this implies that all the roots of $G(n)$ have the same ν-adic absolute value, a contradiction which completes our proof.

3. Specializations

In this section we are going to deduce the general case of Theorem 2 from the number-field case (i.e. essentially Proposition 2.1). As remarked in the introduction, this is possible by a specialization argument developed by van der Poorten and Rumely [R]. Actually, we shall proceed in a slightly different way with respect to [R], taking from that approach just the following lemma, which is a special case of Theorem 7 in [R].

Lemma 3.1. *Let $\mathcal{O}$ be a finitely generated subring of $\mathbf{C}$. Let $\rho \in \mathcal{O}$ be nonzero and let Γ be a finitely generated torsion-free subgroup of $\mathcal{O}^*$. Then there exists a ring homomorphism $\varphi : \mathcal{O} \to \overline{\mathbf{Q}}$ such that $\varphi(\rho) \neq 0$ and such that the restriction of φ to Γ is injective.*

We now prove Theorem 2, letting $\mathcal{N}$ be an infinite set of positive integers such that $F(n)/G(n) \in \mathcal{R}$, where F, G are recurrences as in the assumptions.

We let $\mathcal{O}$ be the ring generated over $\mathcal{R}$ by all coefficients of F, G and by their roots and their respective reciprocals. We are going to apply Lemma 3.1 to $\mathcal{O}$, defining Γ as before to be the group generated by the roots; it is torsion-free by assumption, and we denote by $\gamma_1, \dots, \gamma_t$ a set of independent generators for it.

Using the isomorphism of Lemma 2.1, we associate to F, G elements f, g respectively, of the ring $\mathbf{C}[X, T_1, T_1^{-1}, \dots, T_t, T_t^{-1}]$. Namely, we associate the variable X to the function $n \mapsto n$ and the variable T_i to the function $n \mapsto \gamma_i^n$. Observe that the units of this ring are precisely the terms $cT_1^{a_1} \cdots T_t^{a_t}$ with $c \in \mathbf{C}$ and $a_i \in \mathbf{Z}$.

We can assume that f, g are coprime in this ring and that g is not a unit times an element of $\mathbf{C}[X]$: in fact, if this were the case our conclusion would be proved.

Therefore, on multiplying both f, g by a suitable unit, we may assume that they lie in the polynomial ring $\mathbf{C}[X, T_1, \dots, T_t]$, that they are coprime there, and that g has more than one term as a polynomial in $T_1, \dots, T_t$. In particular, there exists a variable T_i, say T_1, appearing in the terms of g with at least two different degrees. Also, we may assume that $f, g \in \mathcal{O}[X, T_1, \dots, T_t]$.

We now consider the resultant $\omega(X, T_2, \dots, T_t)$ of f, g with respect to T_1. It is clearly nonzero and has coefficients in $\mathcal{O}$.

At this point we apply Lemma 3.1 by taking ρ to be the product of the nonzero coefficients of ω and of f, g. Let φ be a homomorphism as in that lemma. In particular the elements $\varphi(\gamma_i)$ are multiplicatively independent.

The specializations f^φ, g^φ are polynomials in $\overline{\mathbf{Q}}[X, T_1, \dots, T_t]$ and they are coprime with respect to T_1, in view of the nonvanishing of the respective resultant and leading coefficients. Also, g^φ contains at least two terms with respect to T_1, in view of our initial choice of this variable, and in view of the nonvanishing of φ on the coefficients. Write $f^\varphi = df_1$, $g^\varphi = dg_1$, where d, f_1, g_1 are polynomials in $\overline{\mathbf{Q}}[X, T_1, \dots, T_t]$ and f_1, g_1 are coprime. Then d does not depend on T_1, whence g_1 again contains at least two terms (with respect to T_1).

Then, f_1 and g_1 correspond in turn to coprime (w.r. to Γ) linear recurrences $\tilde{F}, \tilde{G}$ with algebraic coefficients and roots, simply by associating the function $n \mapsto n$ to the variable X and the function $n \mapsto \varphi(\gamma_i)^n$ to the variable T_i. Since φ is injective on Γ and since g_1 contains at least two terms, $\tilde{G}$ has at least two distinct roots. By the same reason, the roots of these recurrences generate a torsion-free group. In particular, such recurrences are both nondegenerate, so the Skolem-Mahler-Lech Theorem implies that $\tilde{G}(n) = 0$ only for finitely many $n \in \mathbf{N}$. In the sequel we shall tacitly disregard such integers.

Then, it is clear that, for $n \in \mathcal{N}$,

$$\frac{\tilde{F}(n)}{\tilde{G}(n)} = \varphi\left(\frac{F(n)}{G(n)}\right).$$

In particular, for $n \in \mathcal{N}$, $\tilde{F}(n)/\tilde{G}(n)$ lies in $\varphi(\mathcal{R})$, which is a finitely generated subring of a number field. Since we are assuming that $\mathcal{N}$ is infinite, and since by our previous remark $\tilde{G}$ has at least two roots, this contradicts Proposition 2.1, concluding the proof.

4. Appendix[2]

Throughout this appendix we shall restrict to the number-field case. Theorems 1,2 show in particular that in studying the finiteness of the set

$$\mathcal{N} = \{n \in \mathbf{N} : F(n)/G(n) \in \mathcal{R}\},$$

it is sufficient to consider the case when G is a polynomial. In fact, assuming for instance that the roots of F, G generate a torsion-free group, Theorem 2 predicts that either $\mathcal{N}$ is finite or $F(n)/G(n) = H(n)/P(n)$, where $H(n)$ is a recurrence and $P(n)$ is a nonzero polynomial.

We have noticed that it may well happen that $\mathcal{N}$ is infinite without $F(n)/G(n)$ being a recurrence, when $G(n)$ is a polynomial. On the other hand, it seems very difficult in this case to decide in general about the finiteness of $\mathcal{N}$. The question is sometimes related with classical conjectures on primes, and seems to fall far from Diophantine Approximation techniques. Let us look at some examples, where we take for simplicity $K = \mathbf{Q}$ and $\mathcal{R} = \mathbf{Z}$.

(i) $F(n) = 2^n - 2$, $G(n) = n^2 + n - 1$: even in this simply stated case we do not know the answer, despite the fact that probabilistic arguments seem to indicate that now the values in question should be infinitely many. In fact, if we let n be such that $n^2 + n - 1$ is a prime p, then $2^n - 2 = 2(2^{\frac{p-1}{n+2}} - 1)$ should have "probability" $\geq 1/(n+2)$ of being divisible by p. On the other hand, the probability that $n^2 + n - 1$ is a prime should be roughly $1/2\log n$, so the expected number of elements in $\mathcal{N}$ should be at least $\sum \frac{1}{2(n+2)\log n} = \infty$.

(ii) $F(n) = 2^n - 2$, $G(n) = n(2n - 1)$. Now $G(n)$ is reducible and the question looks a little simpler. For instance, one verifies that $(2^n - 2)/n(2n - 1)$ is an integer for all primes $n \equiv 1 \pmod 8$ such that $2n - 1$ is a prime; that there should exist infinitely many such integers is a very special case of the well-known Schinzel's conjecture on simultaneous prime values of polynomials.

(iii) On the opposite side, we find that $\mathcal{N}$ is finite (no matter $\mathcal{R}$) when F too is a polynomial and F/G has at least two distinct poles: in fact it is a well-known (nontrivial) diophantine result that the greatest prime factor of $P(n)$ tends to infinity with n if P is a polynomial with at least two distinct roots.

(iv) Here is another instance: $F(n) = 4^n + 1$, $G(n) = 4n + 3$: it goes back to Fermat that $\mathcal{N}$ is empty in this case! However one verifies that $\mathcal{N}$ is infinite if we allow $1/3 \in \mathcal{R}$ (consider the odd integers $n = 3m$, where $4m + 1$ is prime). Actually, we do not have any example of a recurrence F with at least two roots and a polynomial G when we can prove that

[2] **Note added in proof.** Lemma A.1 may be derived (actually in a sharpened form) from Lemma 7 of R. Canetti et al., On the statistical properties of Diffie-Hellmann distributions, Israel J. of Math., **120** (2000), 23–46. The arguments presented therein are different from ours and the full result is not needed for our application.

$\mathcal{N}$ is finite no matter $\mathcal{R}$. Could $F(n) = 4^n + 1$, $G(n) = 4n^3 + 3$ be such an instance?

We conclude this appendix by giving a proof of Corollary 2 (where we shall proceed somewhat briefly). Our method uses Theorem 2 and then combines Cantor's argument [C] (mentioned in Remark 3 above) with a sieve inequality. (In fact, the arguments below may be considered as a quantification of Cantor's proof, where sieves do not appear.) A straightforward sieve method seems not to work directly however, since the involved moduli are of type $p(p-1)$, and so are not pairwise coprime. To reduce to the usual situation, we shall start with three lemmas, not free of some independent motivation. The first two of them concern the number of zeros of a recurrence over $\mathbf{F}_p$.

Lemma A.1. *Let $c_1, \dots, c_r, a_1, \dots, a_r \in \mathbf{F}_p^*$. Let N be the minimum of the orders of the a_i/a_j $(i \neq j)$ in $\mathbf{F}_p^*$. Then the number of solutions of $\sum_{i=1}^r c_i a_i^m = 0$ in an interval $[l+1, l+L]$, where $1 \leq L \leq N$, is at most $4L^{1-\frac{1}{2^{r-2}}}$.*

Proof. We argue by induction on r, the assertion being clear for $r = 1$, and we assume $L \geq 2$, as we may. Let $r > 1$, write $\varphi(m) := \sum_{i=1}^r c_i a_i^m$ and let $m_1 < m_2 < \ldots < m_k$ be the distinct solutions of $\varphi(m) = 0$ in the given interval. Among the $k(k-1)/2$ positive differences $m_j - m_i < L$, $1 \leq i < j \leq k$, some difference $d < L$, will occur at least $k(k-1)/2(L-1)$ times. Let $I = \{m_i : m_i + d \in \{m_1, \dots, m_k\}\}$, so $\#I \geq k(k-1)/2(L-1)$. Consider the function

$$\psi(m) := \varphi(m+d) - a_1^d \varphi(m) = \sum_{i=2}^{r} c_i \big(a_i^d - a_1^d\big) a_i^m.$$

Then $\psi(m)$ vanishes for $m \in I$. Also, it is of the same type of φ, but with $r-1$ in place of r. In fact, for $i \geq 2$ the new coefficients $c_i(a_i^d - a_1^d)$ do not vanish, since $1 \leq d < L \leq N$ and since N does not exceed the order of a_i/a_1. By the induction hypothesis we have $k(k-1)/2(L-1) \leq \#I \leq 4L^{1-\frac{1}{2^{r-3}}}$, whence $(k-1)^2 \leq 8L^{2-\frac{1}{2^{r-3}}}$. Therefore $k \leq (1+\sqrt{8})L^{1-\frac{1}{2^{r-2}}} \leq 4L^{1-\frac{1}{2^{r-2}}}$, proving the lemma.

An estimate for the total number of solutions is now immediate, on dividing the interval $[1, p-1]$ into $(p-1)/N$ blocks of N consecutive integers, and then applying Lemma A.1 to each block. We find:

Proposition A.1. *Let $c_1, \dots, c_r, a_1, \dots, a_r \in \mathbf{F}_p^*$. Let N be the minimum of the orders of the a_i/a_j $(i \neq j)$ in $\mathbf{F}_p^*$. Then the number of solutions of $\sum_{i=1}^r c_i a_i^m = 0$ with $1 \leq m \leq p-1$ is $\leq 4(p-1)N^{-\frac{1}{2^{r-2}}}$.*

A Vandermonde argument shows that there cannot be r consecutive solutions if the a_i's are distinct. This leads however to weaker estimates in general, especially if the number N is large. In fact, we shall apply the proposition trying to get a large N. This is accomplished by the following

Lemma A.2. *Let $\beta_1, \dots, \beta_s$ lie in a number field K and suppose that none of them is zero or a root of unity. Then the number of prime numbers $p < X$ such that some β_i has order $< p^{1/4}$ modulo some prime ideal in K above p is $\ll \sqrt{X}$, where the implied constant depends only on s and the β_i.*

Proof. We shall give the proof (by a familiar trick) when the β_i are integers > 1, the general argument being completely similar. Put $Y = X^{1/4}$ and consider the product $\Pi := \prod_{1 \le n \le Y} \prod_{i=1}^{s} (\beta_i^n - 1)$. Then Π is divisible by the product of all the primes in the statement and, being nonzero, is therefore at least 2^H, where H is the number of such primes. On the other hand $|\Pi| < \prod_i \beta_i^{Y^2}$, whence $H \log 2 \le s \max \beta_i \sqrt{X}$, as wanted.

We now proceed to prove the Corollary 2, where we may assume that $\mathcal{N}$ is infinite. The opening argument of this section shows that we reduce via Theorem 2 to the case when $G(n)$ is a polynomial, as we shall suppose. Enlarging the number field K and S we may assume that $\mathcal{R} \subset \mathcal{O}_S$, that G has coefficients and zeroes in $\mathcal{O}_S$ and that

$$F(n) = \sum_{i=1}^{r} f_i(n) \alpha_i^n, \tag{A1}$$

with distinct roots α_i which are S-units in K and polynomials $f_i \in \mathcal{O}_S[X]$.

Suppose that $F(n)/G(n)$ is not a recurrence; then $G(n)$ does not divide all the polynomials $f_i(n)$ in (A1) and we have to prove that $\mathcal{N}$ has zero density. Factoring out the G.C.D. $(G, f_1, \dots, f_r)$ we may even assume that $(G, f_1, \dots, f_r) = 1$ and that G is not constant. In particular, $(G(n), f_1(n), \dots, f_r(n))$ is bounded and we may assume it is an S-unit for all $n \in \mathbf{N}$.

Let $\mathcal{P}$ be the set of prime numbers which split completely in K, which are large enough not to be S-units and such that the minimum order of the α_j/α_i $(i \ne j)$ modulo any prime above p is $\ge p^{1/4}$. Then it follows from analytic number theory and from Lemma A.2 (applied to the α_j/α_i) that this set contains $\gg X/\log X$ elements up to a large real number X. In particular the infinite product $\prod_{p \in \mathcal{P}} (1 - p^{-1})$ diverges to zero.

For $p \in \mathcal{P}$ we choose once and for all a prime ideal π in $\mathcal{O}_S$ lying above p. Then $\mathcal{O}_S/\pi \cong \mathbf{F}_p$.

Let $z \in K$ be a zero of G. Then z is a π-integer and $z \equiv z_p \pmod{\pi}$, for some $z_p \in \mathbf{Z}$. Now, define

$$\mathcal{N}_p = \{n \in \mathcal{N} : n \equiv z_p \pmod{p}\}.$$

Write $n = z_p + mp$ for $n \in \mathcal{N}_p$. Then $n - z$ is divisible by π, so the same must hold for $G(n)$. Since $n \in \mathcal{N}$, we have that $F(n)/G(n) \in \mathcal{O}_S$, whence $F(n)$ too is divisible by π. Hence

$$\sum_{i=1}^{r} f_i(z_p)\alpha_i^{z_p}\alpha_i^m \equiv \sum_{i=1}^{r} f_i(z_p)\alpha_i^n \equiv F(n) \equiv 0 \pmod{\pi},$$

the first congruence holding because p splits completely in K. Then we may apply Proposition A.1 to the resulting congruence in $\mathbf{F}_p$: the number r may decrease, but the $f_i(z_p)$ cannot all vanish modulo π, since $\pi | G(z_p)$ and since $(G(z_p), f_1(z_p), \ldots, f_r(z_p)) \in \mathcal{O}_S$. Also, N may be taken $> p^{1/4}$ in view of the definition of $\mathcal{P}$. We conclude that the possible values of m modulo $p-1$ are at most $4(p-1)p^{-\eta}$ in number, where $\eta > 0$ is independent of p (and may be taken 2^{-r}).

In particular, we find that $\mathcal{N}_p$ has (upper) density $\leq 4p^{-\gamma}$ where $\gamma = 1+\eta > 1$ is independent of p. Define, for given positive real numbers $y < Y$, $\mathcal{N}_{y,Y} = \bigcup_{p\in\mathcal{P}, y<p<Y} \mathcal{N}_p$. Then $\mathcal{N}_{y,Y}$ has upper density $\leq 4\sum_{p>y} p^{-\gamma}$.

On the other hand $\mathcal{N} \setminus \mathcal{N}_{y,Y}$ misses a whole class modulo p, for every prime $p \in \mathcal{P}$ with $y < p < Y$. Therefore, by Erathostenes's sieve, it has (upper) density $\leq \prod_{p\in\mathcal{P}, y<p<Y}(1 - p^{-1})$. Combining this with the previous estimate proves that $\mathcal{N}$ has upper density $\leq 4\sum_{p>y} p^{-\gamma} + \prod_{p\in\mathcal{P}, y<p<Y}(1 - p^{-1})$. Let now $\epsilon > 0$ and choose first y so large that $4\sum_{p>y} p^{-\gamma} < \epsilon$. Then, since $\prod_{p\in\mathcal{P}}(1 - p^{-1}) = 0$, we may choose $Y > y$ such that $\prod_{p\in\mathcal{P}, y<p<Y}(1 - p^{-1}) < \epsilon$. In particular, this proves that $\mathcal{N}$ has upper density $< 2\epsilon$. This holds for every positive ϵ, so in fact $\mathcal{N}$ has density zero, completing the proof.

Remark. A refinement of the argument gives an explicit function $\varepsilon(X)$ tending to zero as $X \to \infty$, such that $\mathcal{N}$ has at most $\varepsilon(X) \cdot X$ elements up to X. In fact, by choosing y a suitable power of $\log X$ and $Y = \sqrt[3]{X}$, one can show (using e.g. a large-sieve inequality) that $\varepsilon(X)$ may be taken $\ll (\log X)^{-\delta}$ for some positive δ depending only on the field K, not on F, G. By considering simultaneously all the primes π above p, it is even possible to take any $\delta < 1$. The example $F(n) = 2^n - 2$, $G(n) = n$ shows that the resulting estimate is nearly best-possible.

References

[BPvdP] J.P. Bézivin, A. Pethö, A.J. van der Poorten, A full characterization of divisibility sequences, Amer. J. of Math. **112** (1990), 985–1001

[BCZ] Y. Bugeaud, P. Corvaja, U. Zannier, An upper bound for the $G.C.D.$ $(a^n - 1, b^n - 1)$, to appear in Math. Z.

[C] D. Cantor, On arithmetic properties of the Taylor series of rational functions, Canadian J. Math. **21** (1969), 378–382

[CZ] P. Corvaja, U. Zannier, Diophantine equations with power sums and universal Hilbert sets, Indagationes Math. **9** (3), (1998), 317–332

[E] J.-H. Evertse, On sums of S-units and linear recurrences, Compositio Math. **53** (1984), 225–244

[L] M. Laurent, Equations exponentielles-polynômes et suites récurrentes linéaires, Journées arithmétiques de Besançon 1985, Astérisques **147–148** (1987), 121–139

[vdP1] A.J. van der Poorten, Solution de la conjecture de Pisot sur le quotient de Hadamard de deux fractions rationnelles, C. R. Acad. Sc. Paris **306**, Série I (1988)

[vdP2] A.J. van der Poorten, Some facts that should be better known, especially about rational functions, in: Number Theory and Applications (Banff, AB 1988), 497–528, Kluwer Acad. Publ., Dordrecht, 1989

[P] Y. Pourchet, Solution du problème arithmétique du quotient de Hadamard de deux fractions rationnelles, C. R. Acad. Sc. Paris **288**, Série I (1979), A 1055–1057

[R] R. Rumely, Note on van der Poorten's proof of the Hadamard quotient theorem I, II, Séminaire de Théorie des nombres de Paris, 1986–87, 349–382, 383–409, Progress in Math. **75**, Birkhäuser, Boston, 1988

[S1] W.M. Schmidt, Diophantine approximations and diophantine equations, Springer-Verlag Lecture Notes in Mathematics **1467**, 1991

[S2] W.M. Schmidt, Linear Recurrence Sequences and Polynomial-Exponential Equations, in: Proceedings of the CIME Conference in Diophantine Approximation, Cetraro (Italy) 2000, to appear as a Springer-Verlag Lecture Note

[ShT] T.N. Shorey, R. Tijdeman, Exponential Diophantine Equations, Cambridge Univ. Press, 1986