

# ON THE SKOLEM PROBLEM AND SOME RELATED QUESTIONS FOR PARAMETRIC FAMILIES OF LINEAR RECURRENCE SEQUENCES

ALINA OSTAFE AND IGOR E. SHPARLINSKI

**ABSTRACT.** We show that in a parametric family of linear recurrence sequences  $a_1(\alpha)f_1(\alpha)^n + \dots + a_k(\alpha)f_k(\alpha)^n$  with the coefficients  $a_i$  and characteristic roots  $f_i$ ,  $i = 1, \dots, k$ , given by rational functions over some number field, for all but a set of  $\alpha$  of bounded height in the algebraic closure of  $\mathbb{Q}$ , the Skolem problem is solvable, and the existence of a zero in such a sequence can be effectively decided. We also discuss several related questions.

## 1. INTRODUCTION

**1.1. Motivation and background.** We recall that a linear recurrence sequence  $(u_n)_{n=1}^\infty$  of order  $k$  over a field  $\mathbb{K}$  is a sequence which satisfies a relation of the form

$$(1.1) \quad u_{n+k} = A_{k-1}u_{n+k-1} + \dots + A_0u_n, \quad n \geq 0,$$

with some constants  $A_0, \dots, A_{k-1}, u_0, \dots, u_{k-1} \in \mathbb{K}$ ; we refer to [18] for a background on recurrence sequences.

The famous *Skolem problem* is a problem of decidability of the existence of a zero  $u_n = 0$  amongst the elements of a linear recurrence sequence  $(u_n)_{n=0}^\infty$ . This problem remains widely open for most of the interesting fields  $\mathbb{K}$  of characteristic zero, including  $\mathbb{K} = \mathbb{Q}$  for  $k \geq 5$ , a brief outline of the current state of affairs is given by Sha [33]. In particular, although there are very good, uniform in all parameters and depending only on  $k$ , bounds on the number of zeros, see [3] there are no effectively computable bounds on the index  $n$  of a possible zero  $u_n = 0$ .

Here we address a parametric version of this problem for a family of linear recurrence sequences and for all but finitely many values of the parameter for which the specialised sequence is not degenerate we give a bound on the largest possible zero. In particular, the Skolem

---

2010 *Mathematics Subject Classification.* 11B37, 11D61.

*Key words and phrases.* Skolem problem, perfect power, linear recurrence sequence.

problem is effectively decidable for all but a set of values of bounded height of the parameter  $\alpha \in \mathbb{C}$ . Note that in our settings the values of parameters which corresponds to zeros in the families we study are always algebraic numbers, so their height is correctly defined.

More precisely, we now recall that if the characteristic polynomial

$$\Psi(Z) = Z^k - A_{k-1}Z^{k-1} - \dots - A_0$$

has  $k$  distinct roots  $\lambda_1, \dots, \lambda_k$  then for any sequence  $(u_n)_{n=1}^\infty$  as in (1.1) there are some  $\mu_1, \dots, \mu_k$  in an algebraic extension of  $\mathbb{K}$  such that

$$u_n = \sum_{i=1}^k \mu_i \lambda_i^n, \quad n \geq 0.$$

Linear recurrence sequences of this type are called *simple*. Some of the results in the background of our arguments are also known for arbitrary sequences, for example, those of [33], but some are known only under this condition, for example, those of [2].

In the case of  $\mathbb{K} = \mathbb{C}$ , the characteristic roots  $\lambda_i$ ,  $i = 1, \dots, k$ , of the largest absolute value, that is, with

$$|\lambda_i| = \max\{|\lambda_1|, \dots, |\lambda_k|\}$$

are called *dominant* and play a major role in investigating various Diophantine properties of linear recurrence sequences.

We recall that a sequence  $(u_n)_{n=1}^\infty$  satisfying (1.1) is called *degenerate* if one of the ratios  $\lambda_i/\lambda_j$ ,  $1 \leq i < j \leq k$ , is a root of unity. We call a sequence *non-degenerate* otherwise.

It is very well-known that the Skolem problem for a degenerate sequence  $u_n$  can be reduced to a series of the Skolem problems for finitely many non-degenerate sequences of the form  $u_{nh+j}$ ,  $j = 0, \dots, h-1$ , where  $h$  is bounded only in terms of the degree  $[\mathbb{Q}(\lambda_1, \dots, \lambda_k) : \mathbb{Q}]$ , see [6]. Hence here we are mostly interested in non-degenerate sequences.

More precisely, here we study the case when both the coefficients  $\mu_i$  and the roots  $\lambda_i$  are rational functions of a parameter  $\alpha \in \mathbb{C}$ . This scenario is close to that of Amoroso, Masser and Zannier [2], see also [24, Proposition 2.2]. In particular, we also appeal to some of the results from [2], however our method is based on a different argument.

More precisely, given two vectors of rational functions

$$\mathbf{a} = (a_1, \dots, a_k), \mathbf{f} = (f_1, \dots, f_k) \in \overline{\mathbb{Q}}(X)^k,$$

over the algebraic closure  $\overline{\mathbb{Q}}$  of  $\mathbb{Q}$  we consider linear recurrence sequences of the form

$$(1.2) \quad F_n(X) = \sum_{i=1}^k a_i f_i^n, \quad n \geq 0.$$

We give a bound for the largest zero in (all but finitely many) specialisations of this sequence such that the new sequence is not degenerate, which is based on recent results of Pakovich and the second author [32] about finiteness of points on curves that lie on the unit circle, a bound for the largest zero in a linear recurrence with at most two dominant roots due to Sha [33] and a result of Amoroso, Masser and Zannier [2, Theorem 1.5] giving an upper bound for the height of zeros of polynomials of the form (1.2). We then couple our result with a general ABC theorem for polynomials [11, Theorem 12.4.4] to give a lower bound on the degree of the splitting field of  $F_n$  over  $\mathbb{Q}$  when  $a_i, f_i$  are all polynomials.

We also look at complex numbers which are zeros of two functions of the form (1.2), which makes the connection to studying the greatest common divisors of elements of two sequences defined by such functions. This point of view has been introduced by Ailon and Rudnick [1] for polynomials of the form  $f^n - 1$  and  $g^m - 1$ ,  $n, m \geq 1$ , and further developed in recent works [16, 26, 27, 31, 32] for different other sequences. In turn, this builds on number field analogues of this problem, initiated by Bugeaud, Corvaja and Zannier [14] for sequences of the form  $a^n - 1$  and  $b^m - 1$ ,  $n, m \geq 1$ , where  $a, b \in \mathbb{Z}$  are multiplicatively independent, and further extended in many works, including generalisations to  $S$ -units [15].

## 2. MAIN RESULTS

**2.1. Skolem problem for parametric families.** We use  $M_{\mathbb{K}}$  to denote a complete set of inequivalent absolute values on a number field  $\mathbb{K}$ , normalized so that the absolute Weil height  $h : \overline{\mathbb{Q}} \rightarrow [0, \infty)$  is defined via  $v$ -adic valuations  $\|\alpha\|_v$  as follows

$$h(\alpha) = \sum_{v \in M_{\mathbb{K}}} \frac{[\mathbb{K}_v : \mathbb{Q}_v]}{[\mathbb{K} : \mathbb{Q}]} \log \max \{ \|\alpha\|_v, 1 \},$$

where  $\mathbb{K}$  is any number field containing  $\alpha$  and  $\mathbb{K}_v$  is the completion of  $\mathbb{K}$  with respect to the absolute value  $v$ . See [11, 22, 37, 42] for further details on absolute values and height functions.

To formulate our results we need to recall that a *finite Blaschke product* is a rational function  $B(z) \in \mathbb{C}(z)$  of the form

$$B(z) = \zeta \prod_{i=1}^n \left( \frac{z - a_i}{1 - \bar{a}_i z} \right)^{m_i},$$

where  $a_i$  are complex numbers in the open unit disc  $\{z \in \mathbb{C} : |z| < 1\}$ , the exponents  $m_i$ ,  $i = 1, \dots, n$ , are positive integers, and  $|\zeta| = 1$ .

A rational function  $Q(z)$  of the form  $Q(z) = B_1(z)/B_2(z)$ , where  $B_1$  and  $B_2$  are finite Blaschke products, is called a *quotient of finite Blaschke products*.

We say that a pair of rational functions  $(g_1(X), g_2(X)) \in \mathbb{C}(X)^2$  is *exceptional* if they can be decomposed as

$$(2.1) \quad g_1 = Q_1 \circ g \quad \text{and} \quad g_2 = Q_2 \circ g$$

for some quotients of finite Blaschke products  $Q_1$  and  $Q_2$  and rational function  $g$ . Otherwise we say that  $(g_1(X), g_2(X))$  is a *non-exceptional* pair.

Since as we have mentioned, the Skolem problem for degenerate sequences is easily reducible to the case of non-degenerate sequences, it motivates us to define for the parametric family (1.2) the exceptional set of  $\alpha \in \overline{\mathbb{Q}}$  such that  $f_i(\alpha)/f_j(\alpha)$  is not a root of unity for some  $1 \leq i < j \leq k$ . It is also convenient to eliminate the roots of  $a_i(X)$  and  $f_i(X)$ ,  $1 \leq i \leq k$ . That is, we define the set

$$\mathfrak{E}_{\mathbf{a}, \mathbf{f}} = \{\alpha \in \overline{\mathbb{Q}} : f_i(\alpha)/f_j(\alpha) \text{ is a root of unity for some } 1 \leq i < j \leq k \\ \text{or } a_i(\alpha) = 0 \text{ or } f_i(\alpha) = 0 \text{ for some } 1 \leq i \leq k\}.$$

Using [37, Theorem 3.11] we immediately derive that elements of  $\mathfrak{E}_{\mathbf{a}, \mathbf{f}}$  are of bounded height.

Our first result is the following:

**Theorem 2.1.** *Let  $a_i, f_i \in \overline{\mathbb{Q}}(X)$ ,  $i = 1, \dots, k$ , be nonzero rational functions of degree at most  $d$  such that  $f_i/f_j$  is non-constant for any  $1 \leq i < j \leq k$ . We also assume that for any  $1 \leq r < s < t \leq k$ , the pairs of rational functions  $(f_s/f_r, f_t/f_r)$  are non-exceptional. Let the sequence  $(F_n)_{n=0}^\infty$  be defined by (1.2). Then for all but at most  $2d^2k^3/3$  elements  $\alpha \in \overline{\mathbb{Q}} \setminus \mathfrak{E}_{\mathbf{a}, \mathbf{f}}$  any zero  $n \in \mathbb{N}$  of the equation*

$$(2.2) \quad F_n(\alpha) = 0$$

*satisfies*

$$n \leq \exp(CD_\alpha^4),$$

*where  $D_\alpha$  is the degree of the smallest Galois field  $\mathbb{K}$  over  $\mathbb{Q}$  with  $\alpha \in \mathbb{K}$ , and  $C$  is an effective constant which depends only on  $a_1, f_1, \dots, a_k, f_k$ .*

**Remark 2.2.** We note that the condition that  $f_i(\alpha)/f_j(\alpha)$  are not roots of unity for any  $i \neq j$  is necessary for any bound on  $n$  as otherwise the sequence can have infinitely many zeros. However, if this is the case, then by the celebrated Skolem-Mahler-Lech Theorem, see for example [18, Theorem 2.1], the set of zeros is the union of a finite set with finitely many arithmetic progressions, and by [6] these arithmetic progressions can be effectively determined, while our methods allows to estimate the elements in the remaining finite set.

It is natural to ask whether a generalisation of Theorem 2.1 to parametric  $S$ -unit equations is possible, see Section 8 for more details and an exact question.

Theorem 2.1 immediately implies the following:

**Corollary 2.3.** Let  $a_i, f_i \in \overline{\mathbb{Q}}[X]$ ,  $i = 1, \dots, k$ , be as in Theorem 2.1. Let  $\mathcal{A}_D$  be the union of all Galois fields of degree at most  $D$  over  $\mathbb{Q}$ . Then there is an effectively computable constant  $C_0$  which depends only on  $a_1, f_1, \dots, a_k, f_k$  such that for all but at most  $12dD^2k^2 + d^2k^3$  elements  $\alpha \in \mathcal{A}_D$ , any zero  $n \in \mathbb{N}$  of the equation (2.2) satisfies

$$n \leq \exp(C_0 D^4).$$

**Corollary 2.4.** Let  $a_i, f_i \in \overline{\mathbb{Q}}[X]$ ,  $i = 1, \dots, k$ , be as in Theorem 2.1. Then there exists a finite set  $\mathcal{E} \subseteq \overline{\mathbb{Q}}$  such that for all roots  $\alpha$  of  $F_n$ ,  $n \geq 1$ , with  $\alpha \notin \mathcal{E} \cup \mathfrak{E}_{\mathbf{a}, \mathbf{f}}$  the degree  $D_\alpha$  of the smallest Galois extension over  $\mathbb{Q}$  containing  $\alpha$  satisfies

$$D_\alpha \geq c(\log n)^{1/4},$$

where  $c$  is an effective constant depending only on  $a_1, f_1, \dots, a_k, f_k$ .

**Corollary 2.5.** Let  $a_i, f_i \in \overline{\mathbb{Q}}[X]$ ,  $i = 1, \dots, k$ , be as in Theorem 2.1 and such that  $\gcd(a_1 f_1, \dots, a_k f_k) = 1$ . Then the splitting field  $\mathbb{L}_n$  of the polynomial  $F_n$  defined by (1.2) is of degree

$$[\mathbb{L}_n : \mathbb{Q}] \geq c_0(\log n)^{1/4},$$

where  $c_0$  is an effective constant depending only on  $a_1, f_1, \dots, a_k, f_k$ .

Note that Corollary 2.5 provides an explicit version of the claim that

$$[\mathbb{L}_n : \mathbb{Q}] \rightarrow \infty$$

as  $n \rightarrow \infty$  given in [2, Example 2].

The bound for  $n$  in Theorem 2.1 depends on the degree of the specialisation  $\alpha$ . We would like to obtain a bound which is independent of  $\alpha$ , when we restrict  $\alpha$  to special subsets of  $\overline{\mathbb{Q}}$ , such as the set of all roots of unity. This in particular would imply that the set

$$\{\alpha \in \overline{\mathbb{Q}} : \alpha^n = 1, F_m(\alpha) = 0 \text{ for some } n, m \geq 1\},$$

is finite, where  $F_m$  is defined by (1.2).

More generally, since  $G_n(X) = X^n - 1$ ,  $n \geq 1$ , also defines a linear recurrence sequence, we would like to generalise the above situation and formulate the following problem.

**Question 2.6.** *Given two simple linear recurrence sequences  $(F_n)_{n=1}^\infty$ ,  $(G_m)_{m=1}^\infty$  over  $\mathbb{C}(X)$ , prove that, under certain conditions, the set*

$$(2.3) \quad \mathcal{L}(F_n, G_m) = \{\alpha \in \mathbb{C} : F_n(\alpha) = G_m(\alpha) = 0 \text{ for some } n, m \geq 1\}$$

*is finite.*

This would extend the result of [2] which already gives the bound-ness of heights of  $\alpha \in \overline{\mathbb{Q}}$  that satisfy only one such relation.

We answer Question 2.6 for binary sequences in Section 2.3 below, which in fact is a direct consequence of [9, Theorem 2].

**2.2. Perfect powers in specialisations at roots of unity.** We now restrict  $\alpha$  to the set  $\mathbb{U}$  of all roots of unity. In this case, for all but finitely many  $\alpha \in \mathbb{U}$  we can effectively answer some other questions about  $F_n(\alpha)$  besides vanishing. We illustrate this approach on the case of perfect powers.

We say that  $\vartheta \in \mathbb{Z}_{\overline{\mathbb{Q}}}$  is a perfect  $m$ th power if for some  $\rho \in \mathbb{Q}(\vartheta)$  we have  $\vartheta = \rho^m$ .

For a polynomial  $f \in \mathbb{C}[X]$ , we use  $\overline{f}$  to denote the complex conjugate polynomial, that is, the polynomial obtained from  $f$  by conjugating all its coefficients.

**Theorem 2.7.** *Let  $a_i, f_i \in \mathbb{Z}_{\overline{\mathbb{Q}}}[X]$ ,  $i = 1, \dots, k$ , be nonzero polynomials of degree at most  $d$  such that for any  $1 \leq r < s < t \leq k$ , the pairs of rational functions  $(f_s/f_r, f_t/f_r)$  are non-exceptional. We also assume that for  $1 \leq i \neq j \leq k$  the polynomials  $f_i(X)\overline{f_i}(Y) - f_j(X)\overline{f_j}(Y)$  do not have any factor of the form  $X^r Y^s - u$  or  $X^r - uY^s$  where  $u$  is a root of unity. Let the sequence of polynomials  $(F_n)_{n=0}^\infty$  be defined by (1.2). Then for all but at most  $d^2(k^3 + 22k^2)$  elements  $\alpha \in \mathbb{U} \setminus \mathfrak{E}_{\mathbf{a}, \mathbf{f}}$  for any  $m \geq 1$  the set of  $n \in \mathbb{N}$  such that  $F_n(\alpha)$  is a perfect  $m$ th power either contains an infinite arithmetic progression  $m\ell + r$ ,  $\ell = 1, 2, \dots$ , with some  $r \in \{0, \dots, m-1\}$  or is finite and its size can be effectively bounded.*

**Remark 2.8.** *We note that by a result of Lang [25] the set  $\mathbb{U} \cap \mathfrak{E}_{\mathbf{a}, \mathbf{f}}$  is in fact finite, thus the number of exceptions in Theorem 2.7 is finite.*

**2.3. Greatest common divisors of binary linear recurrence sequences.** We note that the finiteness conclusion in Question 2.6 would

imply that there are finitely many  $\alpha \in \overline{\mathbb{Q}}$  such that

$$(X - \alpha) \mid \gcd(F_n(X), G_m(X))$$

for some  $n, m \geq 1$ , where by the *greatest common divisor of two rational functions*, we mean the greatest common divisor of their numerators.

Studying the greatest common divisor of sequences of polynomials has been initiated in [1] for sequences  $F_n = f^n - 1$  and  $G_m = g^m - 1$ ,  $n, m \geq 1$ , where  $f, g \in \mathbb{C}[X]$ , and recently extended in several directions in [16, 26, 27, 31, 32].

We note that in the case of simple binary linear recurrence sequences defined over  $\mathbb{C}$ , under some multiplicative independence conditions, a finiteness result follows directly from [31, Theorem 1.3]. In fact, such a result follows directly from [9, Theorem 2] and we present it here only in the following form.

**Remark 2.9.** *Let  $a, b, f, g \in \mathbb{C}(X)$  be multiplicatively independent rational functions. Let  $(F_n)_{n=1}^\infty, (G_m)_{m=1}^\infty$  be defined by*

$$\begin{aligned} F_n(X) &= a(X)f(X)^n + 1, \quad n \geq 1, \\ G_m(X) &= b(X)g(X)^m + 1, \quad m \geq 1. \end{aligned}$$

*Then the set  $\mathcal{L}(F_n, G_m)$  defined by (2.3) is finite and its cardinality is uniformly bounded only in terms of the functions  $a, b, f, g$ . Moreover, under the additional condition*

$$\mathcal{Z}(a) \cap \mathcal{R}(f) = \mathcal{R}(a) \cap \mathcal{Z}(f) = \mathcal{Z}(b) \cap \mathcal{R}(g) = \mathcal{R}(b) \cap \mathcal{Z}(g) = \emptyset,$$

*where  $\mathcal{Z}(f)$  and  $\mathcal{R}(f)$  are the sets of zeros and poles of  $f$  in  $\mathbb{C}$  (and the same for  $g$ ), respectively, there exists a polynomial  $h \in \mathbb{C}[X]$  such that for all  $n, m \geq 1$ ,*

$$(2.4) \quad \gcd(F_n, G_m) \mid h.$$

*Indeed, as in the proof of [31, Theorem 1.3], for any zero  $\alpha \in \mathbb{C}$  of  $\gcd(af^n + 1, bg^m + 1)$  we have*

$$a(\alpha)f(\alpha)^n = b(\alpha)g(\alpha)^m = -1.$$

*Since  $a, b, f, g$  are multiplicatively independent, the finiteness of the set of such  $\alpha \in \mathbb{C}$  follows directly from [10, 30] (which in turn generalise [9, Theorem 2]). See also [8] for some effective results for rational functions over  $\mathbb{Q}$  and  $G_m = X^m - 1$ . To obtain the divisibility (2.4) we only need to bound the multiplicity of such zeros  $\alpha \in \mathbb{C}$ , and this follows directly from [31, Lemma 2.9].*

**Remark 2.10.** Clearly, after appropriate scaling, Remark 2.9 can be reformulated for binary sequences in a more common form

$$\begin{aligned} F_n(X) &= a_1(X)f_1(X)^n + a_2(X)f_2(X)^n, \quad n \geq 1, \\ G_m(X) &= b_1(X)g_1(X)^m + b_2(X)g_2(X)^m, \quad m \geq 1, \end{aligned}$$

with  $a_1, a_2, b_1, b_2, f_1, f_2, g_1, g_2 \in \mathbb{C}(X)$ .

We formulate our next result when  $a, b$  in Remark 2.9 are constants, and moreover we vary them over a finitely generated subgroup of  $\overline{\mathbb{Q}}^*$ .

**Theorem 2.11.** Let  $f, g \in \overline{\mathbb{Q}}(X)$  be multiplicatively independent with constants, and let  $\Gamma \subseteq \overline{\mathbb{Q}}^*$  be a finitely generated subgroup. There exists a polynomial  $h \in \overline{\mathbb{Q}}[X]$  depending only on  $f, g$  and the generators of  $\Gamma$  such that for any  $n, m \geq 1$  and any  $u, v \in \Gamma$  one has

$$\gcd(f(X)^n - u, g(X)^m - v) \mid h.$$

**Remark 2.12.** We note that one can give an explicit uniform bound on the degree of  $h$  in Theorem 2.11, depending only on  $f, g$  and  $\Gamma$ . Indeed, this bound follows from [5, Theorem 2.2], which in turn gives bounds for the degree and height of roots of  $\gcd(f(X)^n - u, g(X)^m - v)$  only in terms of  $f, g$  and  $\Gamma$ , coupled with a result of Schmidt [34] which gives an estimate on the number of algebraic numbers of bounded degree and height.

**Remark 2.13.** We note here that when  $|u| = |v| = 1$  in Theorem 2.11, one also has a result for  $f, g \in \mathbb{C}(X)$ . Indeed, under some further conditions on  $f$  and  $g$ , such a result follows from [32, Theorem 2.2], see Lemma 3.1 below.

As a direct consequence of Theorem 2.11 we have the following corollary which we hope to be of independent interest.

**Corollary 2.14.** Let  $f, g \in \overline{\mathbb{Q}}[X]$  be multiplicatively independent with constants and let  $\Gamma \subseteq \overline{\mathbb{Q}}^*$  be a finitely generated subgroup. Then there exists a polynomial  $H \in \overline{\mathbb{Q}}[X]$  such that for any  $n, m \geq 1$  and any polynomials  $F, G \in \overline{\mathbb{Q}}[X]$  of degree at most  $d \geq 1$  with roots from  $\Gamma$ , one has

$$\gcd(F(f^n), G(g^m)) \mid H.$$

**2.4. Specialisations of sequences of rational functions.** Finally, we show that a sequence of rational functions  $F_n(X) \in \mathbb{C}(X)$ ,  $n \geq 0$ , satisfies a linear recurrence relation if and only if this is also true for specialisations  $F_n(\alpha)$ ,  $n \geq 0$ , for a sufficiently “massive” set of  $\alpha \in \mathbb{C}$ .



**Theorem 2.15.** *Let  $(F_n)_{n=0}^\infty$  be an infinite sequence of rational functions  $F_n \in \mathbb{C}(X)$ ,  $n \geq 0$ , and let  $K \geq 1$ . Assume there exist infinitely many  $\alpha \in \mathbb{C}$  such that each  $F_n(\alpha)$  is well defined and  $(F_n(\alpha))_{n=0}^\infty$  is a linear recurrence of order at most  $K$ . Then  $(F_n)_{n=0}^\infty$  is a linear recurrence sequence over  $\mathbb{C}(X)$  of order at most  $K$ .*

We now immediately derive the following result where we do not restrict the order of the sequences.

**Corollary 2.16.** *Let  $(F_n)_{n=0}^\infty$  be an infinite sequence of polynomials  $F_n \in \mathbb{C}[X]$ ,  $n \geq 0$ . Assume that  $(F_n(\alpha))_{n=0}^\infty$  is a linear recurrence sequence for uncountably many  $\alpha \in \mathbb{C}$ . Then  $(F_n)_{n=0}^\infty$  is a linear recurrence sequence in  $\mathbb{C}[X]$ .*

**Remark 2.17.** *It is natural to ask whether it is possible to merge Theorem 2.15 and Corollary 2.16 where simply the infinitude of  $\alpha \in \mathbb{C}$  such that  $(F_n(\alpha))_{n=0}^\infty$  is a linear recurrence sequence (without any restriction on the order) implies that  $(F_n)_{n=0}^\infty$  is a linear recurrence sequence in  $\mathbb{C}[X]$  as well. It is easy to show that such a result is impossible, for example, the sequence*

$$F_n(X) = X^{2^{n^2}} + X^{6^n} + X^{2^{\lfloor \sqrt{n} \rfloor}} + 1, \quad n = 0, 1, \dots,$$

*does not satisfy any linear recurrent relation (as the degree grows too fast). However it is a linear recurrence sequence for every root of unity of order  $2^m$ ,  $m = 0, 1, \dots$ .*

### 3. PRELIMINARIES

**3.1. Intersections of level curves of rational functions.** Our approach depends on a generalisation of a result of Ailon and Rudnick [1, Theorem 1] which is given in [32, Theorem 2.2].

Recall the definition of non-exceptional pairs of rational functions, which avoid relations of the form (2.1).

**Lemma 3.1.** *Let  $(g_1(X), g_2(X)) \in \mathbb{C}(X)$  be complex rational functions of degrees  $n_1$  and  $n_2$ , respectively. Then*

$$\#\{z \in \mathbb{C} : |g_1(z)| = |g_2(z)| = 1\} \leq (n_1 + n_2)^2,$$

*unless  $(g_1(X), g_2(X))$  is exceptional.*

It is easy to see that if  $g_1$  and  $g_2$  are polynomials the conclusion of Lemma 3.1 reduces to

$$g_1 = g^{m_1} \quad \text{and} \quad g_2 = g^{m_2}$$

for some  $g \in \mathbb{C}[X]$  and integers  $m_1, m_2 \geq 0$ .

**3.2. Zeros of linear recurrence sequences with at most two dominant roots.** We say that a root  $\lambda$  of a polynomial  $\psi(Z) \in \mathbb{C}[Z]$  is dominant if  $|\lambda| \geq |\rho|$  for any other root  $\rho$  of  $\psi$ . Clearly  $\psi$  may have up to  $\deg \psi$  dominant roots. We are mostly interested in the case of one or two dominant roots.

We note the following result which represents a simplified combination of two results (for  $\nu = 1$  and  $\nu = 2$ ) of Sha [33, Theorem 1.1 and 1.2].

**Lemma 3.2.** *Let  $\psi(X) \in \overline{\mathbb{Q}}[X]$  be a monic square-free polynomial of degree  $k$  and with  $\nu \leq 2$  dominant roots. If  $\nu = 2$ , we also impose that the ratio of the two dominant roots is not a root of unity. Then for any linear recurrence sequence  $\mathbf{u} = (u_n)$  given by*

$$u_n = \sum_{i=1}^k \alpha_i \lambda_i^n, \quad n \geq 0,$$

*with characteristic polynomial  $\psi$  having roots  $\lambda_i$ ,  $i = 1, \dots, k$ , if*

$$u_n = 0$$

*then*

$$n \leq \exp \left( C_1 D^4 \left( \max_{i=1, \dots, k} h(\alpha_i) + 1 \right) \right),$$

*where  $C_1$  is an effective constant which depends only on  $k$ ,  $D$  is the degree  $D = [\mathbb{K} : \mathbb{Q}]$  of the smallest Galois field  $\mathbb{K}$  containing the coefficients of  $\psi$  and the initial values  $u_0, \dots, u_{k-1}$ .*

**3.3. Zeros of linear recurrence sequences in families.** We now recall a special case of a result of Amoroso, Masser and Zannier [2, Theorem 1.5].

**Lemma 3.3.** *Let  $f_i \in \overline{\mathbb{Q}}(X)$ ,  $i = 1, \dots, k$ , be nonzero rational functions such that  $f_s/f_r$  is non-constant for any  $1 \leq r < s \leq k$ . There exists an effectively computable constant  $C_2$ , which depends on  $f_1, \dots, f_k$  such that if for any  $b_1, \dots, b_k \in \overline{\mathbb{Q}}$ , any  $n \geq C_2$  and any  $\alpha \in \overline{\mathbb{Q}} \setminus \mathfrak{C}_{\mathbf{a}, \mathbf{f}}$ , one has*

$$\sum_{i=1}^k b_i f_i(\alpha)^n = 0,$$

*then*

$$h(\alpha) \leq \frac{k \max\{h(b_1), \dots, h(b_k)\}}{n} + C_2.$$

We remark that in [2, Theorem 1.5] the bound is given in terms of height of the projective vector  $(b_1 : \dots : b_k) \in \mathbb{P}^{k-1}(\overline{\mathbb{Q}})$  which is bounded by the maximum used in Lemma 3.3. Furthermore, in [2,

Theorem 1.5] only one ratio is assumed to be non-constant, however there is an additional request of non-vanishing of subsums in the sum of Lemma 3.3 (under our condition on  $f_s/f_r$  one can simply consider the shortest vanishing subsum).

We also note that the effectiveness is not explicitly stated in [2, Theorem 1.5] however it is discussed after the formulation of [2, Theorem 1.5].

**Corollary 3.4.** *Let  $a_i, f_i \in \overline{\mathbb{Q}}(X)$ ,  $i = 1, \dots, k$ , be nonzero rational functions such that  $f_s/f_r$  is non-constant for any  $1 \leq r < s \leq k$ . There exists an effectively computable constant  $C_3$ , which depends on  $a_1, \dots, a_k, f_1, \dots, f_k$  such that if for any*

$$n \geq 2k \max\{\deg a_1, \dots, \deg a_k, C_3\}$$

and any  $\alpha \in \overline{\mathbb{Q}}$  one has

$$\sum_{i=1}^k a_i(\alpha) f_i(\alpha)^n = 0,$$

then

$$h(\alpha) \leq C_3.$$

*Proof.* If  $\alpha \in \mathfrak{E}_{\mathbf{a}, \mathbf{f}}$ , as we have mentioned, this follows from [37, Theorem 3.11].

We can now assume that  $\alpha \in \overline{\mathbb{Q}} \setminus \mathfrak{E}_{\mathbf{a}, \mathbf{f}}$ . We can also assume that  $n > C_2$  where  $C_2$  is as in Lemma 3.3 since otherwise  $\alpha$  is a root of an equation of bounded degree and height.

We now recall that for any  $\alpha \in \overline{\mathbb{Q}}$  and  $a \in \overline{\mathbb{Q}}(X)$  we have

$$h(a(\alpha)) \leq h(\alpha) \deg a + C_4,$$

where  $C_4$  is an effectively computable constant that depends only on  $a$ , see [37, Theorem 3.11]. Hence for

$$n \geq 2k \max\{\deg a_1, \dots, \deg a_k\}$$

the bound of Lemma 3.3 becomes

$$\begin{aligned} h(\alpha) &\leq \frac{k \max\{h(a_1(\alpha)), \dots, h(a_k(\alpha))\}}{n} + C_2 \\ &\leq \frac{k \max\{\deg a_1, \dots, \deg a_k\} h(\alpha) + kC_4}{n} + C_2 \\ &\leq \frac{1}{2} h(\alpha) + C_4/2 + C_2. \end{aligned}$$

Hence  $h(\alpha)$  is bounded only in terms of  $a_1, f_1, \dots, a_k, f_k$ , and the result follows.  $\square$

**3.4. Polynomial ABC theorem.** We need the following generalisation [11, Theorem 12.4.4] of the ABC Theorem for polynomials proved first by Stothers [40], and then independently by Mason [29] and Silverman [36]. This is a special case of a more general result for  $S$ -units in function fields due to Voloch [41] and then also Brownawell and Masser [13].

**Lemma 3.5.** *Let  $g_1, \dots, g_m \in \overline{\mathbb{Q}}[X]$ ,  $m \geq 3$ , be such that  $g_1, \dots, g_m$  have no common zero in  $\overline{\mathbb{Q}}$ . Assume that*

$$g_1(X) + \dots + g_m(X) = 0$$

*and also that no proper subsum*

$$\sum_{i \in \mathcal{I}} g_i(X), \quad \mathcal{I} \subseteq \{1, \dots, m\}, \quad 1 \leq \#\mathcal{I} < m,$$

*vanishes identically. Then*

$$\max_{i=1, \dots, m} \deg g_i \leq \frac{(m-1)(m-2)}{2} \max \left\{ \deg \operatorname{rad} \left( \prod_{i=1}^m g_i \right) - 1, 0 \right\}.$$

**3.5. Zeros of linear recurrence sequences in function fields.**

It is well known that the Skolem Problem is settled in the case of linear recurrence sequences over function fields. An effective (but not explicit) bound on the largest zero in such a sequence is given in [21, Corollary 3.1]. We present it in a simplified form as needed for our setting.

**Lemma 3.6.** *Let  $a_i, f_i \in \overline{\mathbb{Q}}[X]$ ,  $i = 1, \dots, k$ , be such that  $f_i/f_j \notin \overline{\mathbb{Q}}^*$  for all  $1 \leq i < j \leq k$ . Let polynomials  $F_n$ ,  $n \geq 1$ , be defined by (1.2). Then there exists an effectively computable constant  $C_5$  depending on  $a_i, f_i$ ,  $i = 1, \dots, k$ , such that if  $F_n = 0$  then  $n < C_5$ .*

We also have the following lower bound on the number of distinct zeros of  $F_n(X)$  in (1.2).

**Lemma 3.7.** *Let  $a_i, f_i \in \overline{\mathbb{Q}}[X]$ ,  $i = 1, \dots, k$ , be as in Theorem 2.1 and such that  $\gcd(a_1 f_1, \dots, a_k f_k) = 1$ . Then there exists an effective positive constant  $C_6$  depending only on  $a_i, f_i$ ,  $i = 1, \dots, k$ , such that for any  $n \geq C_6$ , the polynomial  $F_n$  defined by (1.2) has at least*

$$\frac{2}{k(k-1)} \max_{i=1, \dots, n} \{\deg a_i + n \deg f_i\} - 2dk$$

*distinct roots.*

*Proof.* Let  $C_5$  be as in Lemma 3.6. Then, for any  $n \geq C_5$  we know that  $F_n \neq 0$ . We consider now the equation

$$(3.1) \quad F_n(X) - \sum_{i=1}^k a_i(X) f_i(X)^n = 0.$$

We also note that for  $n \geq C_5$  no subsum of the terms from the set

$$\{F_n(X), a_1(X) f_1(X)^n, \dots, a_k(X) f_k(X)^n\}$$

vanishes identically. Indeed, if this happens, then there is a proper subset  $\mathcal{I} \subseteq \{1, \dots, k\}$  such that

$$\sum_{i \in \mathcal{I}} a_i(X) f_i(X)^n = 0.$$

Since  $n \geq C_5$ , this contradicts Lemma 3.6.

Let  $\mathcal{S}_n$  be the set of all distinct zeros of  $F_n$ . We can now apply Lemma 3.5 to (3.1) to conclude that

$$\max_{i=1, \dots, k} \{\deg a_i + n \deg f_i\} \leq \frac{k(k-1)}{2} \left( \#\mathcal{S}_n + \sum_{i=1}^k (\deg a_i + \deg f_i) \right).$$

From here we obtain

$$\#\mathcal{S}_n \geq \frac{2 \max_{i=1, \dots, k} \{\deg a_i + n \deg f_i\}}{k(k-1)} - 2dk,$$

which concludes the proof (with  $C_6 = C_5$ ).  $\square$

**Remark 3.8.** We note that under a more restrictive condition that the  $n$  products  $a_1 f_1, \dots, a_k f_k$  are pairwise relatively prime, one can take  $C_6 = 1$  in Lemma 3.7. Furthermore, under the more restrictive condition that  $2k$  polynomials  $a_1, f_1, \dots, a_k, f_k$  are pairwise relatively prime, one can also use the result of Brindza [12, Theorem 1] to show that the polynomial  $F_n$  has at least  $n/(k-1) - (d+1)k$  distinct roots.

We also remark that a tight lower bound for the degree of  $F_n$  has recently been given in [20, Corollary 2] (in fact for arbitrary non-degenerate linear recurrences including non-simple ones).

**3.6. Characterisation of linear recurrence sequences.** To test whether an arbitrary sequence  $(v_n)_{n=1}^\infty$  of elements of a field  $\mathbb{F}$  is a linear recurrence sequence, we recall the following well-known result which is based on the vanishing of the *Kronecker–Hankel determinants*

$$(3.2) \quad \Delta_h = \det (v_{i+j})_{0 \leq i, j \leq h-1}.$$

More precisely, by [28, Theorem 8.75] (see also [18, Theorem 1.6] and [23, Lemma 5, Chapter V] for variations) we have:

**Lemma 3.9.** *A sequence  $(v_n)_{n=1}^\infty$  of elements of a field  $\mathbb{F}$  is a linear recurrence sequence of order  $k$  if and only if for the determinants (3.2) we have  $\Delta_h = 0$  for all  $h \geq k + 1$ .*

#### 4. PROOFS OF RESULTS TOWARDS THE SKOLEM PROBLEM

**4.1. Proof of Theorem 2.1.** Multiplying by common denominators of  $a_i(X)$  and of  $f_i(X)$ ,  $i = 1, \dots, k$ , we can assume that  $a_i(X), f_i(X) \in \overline{\mathbb{Q}}[X]$ ,  $i = 1, \dots, k$ .

Let  $\alpha \in \overline{\mathbb{Q}} \setminus \mathfrak{E}_{\mathbf{a}, \mathbf{f}}$  be such that (2.2) holds.

We now consider the case when we have at least three dominant roots, that is, there exist distinct integers  $1 \leq r < s < t \leq k$  such that

$$|f_r(\alpha)| = |f_s(\alpha)| = |f_t(\alpha)|,$$

or equivalently,

$$\frac{|f_s(\alpha)|}{|f_r(\alpha)|} = \frac{|f_t(\alpha)|}{|f_r(\alpha)|} = 1.$$

Since by hypothesis,  $(f_s/f_r, f_t/f_r)$  is a non-exceptional rational function, from Lemma 3.1 we see that for each of the  $k(k-1)(k-2)/6$  possible choices of the triple  $(r, s, t)$  there are at most  $4d^2$  such  $\alpha \in \overline{\mathbb{Q}}$ .

Hence in total we have excluded at most

$$(4.1) \quad 4d^2 k(k-1)(k-2)/6 = 2d^2 k(k-1)(k-2)/3 \leq 2d^2 k^3/3.$$

We thus assume that we have at most two dominant roots. In this case we apply Lemma 3.2 to all elements  $\alpha \in \overline{\mathbb{Q}} \setminus \mathfrak{E}_{\mathbf{a}, \mathbf{f}}$  and derive that

$$n \leq \exp(C_7 D_\alpha^4 (h(\alpha) + 1)),$$

for an effectively computable constant  $C_7$ , which depends only on  $a_1, \dots, a_k, f_1, \dots, f_k$ . Now, recalling Corollary 3.4 we obtain the desired result.

**4.2. Proof of Corollary 2.3.** By Theorem 2.1 we only need to estimate the number  $R(D)$  of roots of unity of degree at most  $D$  over  $\mathbb{Q}$ . Clearly

$$R(D) = \sum_{m: \varphi(m) \leq D} \varphi(m) \leq D \sum_{m: \varphi(m) \leq D} 1,$$

where  $\varphi(m)$  is the Euler function. Using the bound

$$\sum_{m: \varphi(m) \leq D} 1 \leq 23D$$

of Dubickas and Sha [17, Lemma 4.1], we see that

$$(4.2) \quad R(D) \leq 23D^2$$

(using partial summation one can certainly obtain a tighter bound). Now, since each of  $k(k-1)/2$  ratios  $f_i(\alpha)/f_j(\alpha)$  can be a root of unity of degree at most  $D$ , there are at most

$$dR(D) \frac{k(k-1)}{2} < 12dD^2k^2$$

such  $\alpha \in \mathcal{A}_D$ , which we need to exclude.

Taking into account that we also need to exclude at most other  $2d^2k(k-1)(k-2)/3$  elements  $\alpha \in \mathcal{A}_D$  as in Theorem 2.1, see (4.1), and at most  $2dk$  zeros of  $a_i f_i$ ,  $i = 1, \dots, k$ , and thus at most

$$2d^2k(k-1)(k-2)/3 + 2dk \leq d^2k^3$$

elements (indeed, for  $k = 2$  this bound is obvious, for  $k \geq 3$  we use  $2dk \leq dk^3/3$ ), we conclude the proof.

**4.3. Proof of Corollary 2.4.** Let  $\mathbb{K}$  be a number field with  $[\mathbb{K} : \mathbb{Q}] = D$  such that  $a_i, f_i \in \mathbb{K}[X]$ ,  $i = 1, \dots, k$ .

Let  $\alpha \notin \mathfrak{E}_{\mathbf{a}, \mathbf{f}}$  be a root of  $F_n$  for some  $n \geq 1$ . Let  $G$  be its minimal polynomial over  $\mathbb{K}$ , which implies that  $G \mid F_n$ . Let  $D_G = \deg G = [\mathbb{K}(\alpha) : \mathbb{K}]$  and let  $\mathbb{M}_\alpha$  be the smallest Galois extension of  $\mathbb{Q}$  which includes  $\mathbb{K}(\alpha)$ .

For any  $\sigma \in \text{Gal}(\mathbb{K}(\alpha)/\mathbb{K})$ , conjugating the relation  $F_n(\alpha) = 0$  gives us

$$(4.3) \quad \sum_{i=1}^k a_i(\sigma(\alpha)) f_i(\sigma(\alpha))^n = 0.$$

We may assume that  $D_G > d^2k^3$ . Indeed, if  $D_G \leq d^2k^3$ , then

$$[\mathbb{K}(\alpha) : \mathbb{Q}] \leq DD_G \leq Dd^2k^3,$$

and since by Corollary 3.4,  $h(\alpha)$  is bounded from the above by a constant depending only on  $a_1, f_1, \dots, a_k, f_k$ , by Northcott's Theorem there are finitely many such  $\alpha$ . Thus we can exclude the irreducible factors of  $F_n$ ,  $n \geq 1$ , corresponding to these finitely many elements.

Now, since there are  $D_G > d^2k^3$  distinct elements  $\sigma(\alpha)$  satisfying (4.3), and taking into account the hypothesis on the polynomials  $f_i$ , we can apply Theorem 2.1 to conclude that there exists  $\sigma \in \text{Gal}(\mathbb{K}(\alpha)/\mathbb{K})$  such that (4.3) holds and for which

$$n \leq \exp(C_8[\mathbb{M}_\alpha : \mathbb{Q}]^4)$$

for some constant  $C_8$  which depends only on  $a_1, f_1, \dots, a_k, f_k$ . This concludes the proof.

**4.4. Proof of Corollary 2.5.** Let the set  $\mathcal{E}$  be as in Corollary 2.4. Clearly, if  $F_n$  has a root outside of the set  $\mathcal{E} \cup \mathfrak{E}_{\mathbf{a}, \mathbf{f}}$  the result is instant from Corollary 2.4.

Otherwise, since  $\mathcal{E}$  is a finite set and so are the sets of  $\alpha \in \overline{\mathbb{Q}}$  with  $f_i(\alpha) = 0$  or  $a_i(\alpha) = 0$ , for some  $1 \leq i \leq k$ , adjusting the constant  $c_0$  we can make the desired result valid for these values of  $\alpha$  as well.

Hence it remains to consider the case when the ratio  $f_i(\alpha)/f_j(\alpha)$  is a root of unity for some  $1 \leq i < j \leq k$ . We recall that by Lemma 3.7  $F_n$  has at least  $2n/k(k-1) + O(1)$  roots  $\alpha$ . By our assumption, for each of them at least one ratio  $f_i(\alpha)/f_j(\alpha)$  is a root of unity for some  $1 \leq i < j \leq k$ . For each  $\gamma \in \overline{\mathbb{Q}}$  the equation  $f_i(\alpha)/f_j(\alpha) = \gamma$  has at most  $d$  solutions  $\alpha \in \overline{\mathbb{Q}}$ . Hence the ratios  $f_i(\alpha)/f_j(\alpha)$  generate a set  $\mathcal{U}_{\mathbf{f}}$  of at least

$$\#\mathcal{U}_{\mathbf{f}} \geq 2n/dk(k-1) + O(1)$$

distinct roots of unity  $\rho$  for some  $1 \leq i < j \leq k$ .

Recall the bound (4.2) on the number of roots of unity of degree at most  $D$ . Hence at least one of the above roots of unity is of degree at least

$$\sqrt{\frac{1}{23}\#\mathcal{U}_{\mathbf{f}}} \geq \sqrt{\frac{2n}{23dk(k-1)}} + O(1).$$

and thus so is  $\alpha$ .

## 5. PROOF OF THEOREM 2.7 ON PERFECT POWERS IN SPECIALISATIONS AT ROOTS OF UNITY

Let  $\mathbb{K}$  be the field of definition of the polynomials  $a_i, f_i$ . Thus,  $a_i, f_i \in \mathbb{Z}_{\mathbb{K}}[X]$ , where  $\mathbb{Z}_{\mathbb{K}}$  is the ring of integers of  $\mathbb{K}$ .

By the proof of Theorem 2.1, we know that for all but at most  $d^2k^3$  elements  $\alpha \in \mathbb{U} \setminus \mathfrak{E}_{\mathbf{a}, \mathbf{f}}$ , the sequence  $(F_n(\alpha))_{n=1}^{\infty}$  has at most two dominant roots. Let us assume first that for such an  $\alpha \in \mathbb{U} \setminus \mathfrak{E}_{\mathbf{a}, \mathbf{f}}$ , the sequence  $(F_n(\alpha))_{n=1}^{\infty}$  has two dominant roots, that is, for some  $1 \leq i \neq j \leq k$ ,  $|f_i(\alpha)| = |f_j(\alpha)|$ . This implies that

$$(5.1) \quad f_i(\alpha)\overline{f_i(\overline{\alpha})} = f_i(\alpha)\overline{f_i(\alpha)} = f_j(\alpha)\overline{f_j(\alpha)} = f_j(\alpha)\overline{f_j(\overline{\alpha})},$$

where  $\overline{\alpha}$  is the complex conjugate of  $\alpha$ , which is again a root of unity.

Since by our assumption,

$$f_i(X)\overline{f_i(Y)} - f_j(X)\overline{f_j(Y)} \in \mathbb{K}[X, Y], \quad 1 \leq i \neq j \leq k,$$

do not have any factor of the form  $X^r Y^s - u$  or  $X^r - u Y^s$  with  $u \in \mathbb{U}$ , by a result of Lang [25] we know that there are finitely many solutions  $(\alpha, \beta)$



in roots of unity (and thus also of the form  $(\alpha, \bar{\alpha})$ ) to the equation (5.1). Moreover, by [7, Section 4.1], the equation

$$f_i(X)\bar{f}_i(Y) - f_j(X)\bar{f}_j(Y) = 0$$

has at most  $44d^2$  solutions  $(\alpha, \beta)$  in roots of unity. Thus, there are at most  $22d^2k(k-1) < 22d^2k^2$  such elements  $\alpha \in \mathbb{U} \setminus \mathfrak{E}_{\mathbf{a}, \mathbf{f}}$  such that the sequence  $(F_n(\alpha))_{n=1}^\infty$  has two dominant roots.

Thus, for all but  $d^2(k^3 + 22k^2)$  elements  $\alpha \in \mathbb{U} \setminus \mathfrak{E}_{\mathbf{a}, \mathbf{f}}$ , the sequence  $(F_n(\alpha))_{n=1}^\infty$  has only one dominant root. Let such an element  $\alpha \in \mathbb{U} \setminus \mathfrak{E}_{\mathbf{a}, \mathbf{f}}$ . We now apply the result of Fuchs [19, Corollary 2.10] to conclude the proof.

## 6. PROOFS OF RESULTS ON COMMON ZEROS

**6.1. Proof of Theorem 2.11.** The proof follows from several results in [1, 5]. We first note that if  $u, v$  are roots of unity, then the result follows from [1, Theorem 1] which is in fact a consequence of the finiteness of torsion points on plane curves conjectured by Lang [25] and proved by Ihara, Serre and Tate. We also note that for this particular case we need that  $f$  and  $g$  are multiplicatively independent only.

We assume now the general case, and we look at  $\alpha \in \overline{\mathbb{Q}}$  such that

$$(6.1) \quad f(\alpha)^n, g(\alpha)^m \in \Gamma,$$

for some  $n, m \geq 1$ .

Let us define the plane curve

$$\mathcal{C} = \{(f(t), g(t)) \in \overline{\mathbb{Q}}\}.$$

We define the division group of  $\Gamma$  by

$$\bar{\Gamma} = \{t \in \overline{\mathbb{Q}} : t^n \in \Gamma \text{ for some } n \geq 1\}.$$

Then, (6.1) implies that

$$(f(\alpha), g(\alpha)) \in \mathcal{C} \cap (\bar{\Gamma} \times \bar{\Gamma}).$$

The finiteness conclusion now follows from [5, Theorem 2.2], which gives bounds for the degree and height of  $\alpha$  only in terms of  $f, g$  and  $\Gamma$  (the height and degrees of the generators of  $\Gamma$ ), coupled with Northcott's Theorem. We denote by  $\mathcal{S}_{f,g,\Gamma}$  the finite set of zeros of  $f(X)^n - u$  and  $g(X)^m - v$  for all  $n, m \geq 1$  and all  $u, v \in \Gamma$ .

To finish the proof, we only need to conclude that the multiplicity of these roots is also bounded independently of  $n, m$  and  $u, v$ . This follows directly from [31, Lemma 2.9], which in turn is based on the polynomial *ABC* theorem [29, 36, 40]. More precisely, by [31, Lemma 2.9] we conclude that the multiplicity of any root of  $f(X)^n - u$  and  $g(X)^m - v$ ,

$n, m \geq 1$  and  $u, v \in \Gamma$ , is bounded by  $\deg f$  and  $\deg g$ , respectively. Thus, we can define the polynomial  $h \in \overline{\mathbb{Q}}[X]$  by

$$h(X) = \prod_{\gamma \in \mathcal{S}_{f,g,\Gamma}} (X - \gamma)^{\min\{\deg f, \deg g\}},$$

which concludes the proof.

**6.2. Proof of Corollary 2.14.** Let  $F, G \in \overline{\mathbb{Q}}[X]$  be of degree at most  $d \geq 1$  with all roots in  $\Gamma$ . We reduce the problem to looking at each greatest common divisor

$$\gcd(f^n - \gamma_1, g^m - \gamma_2), \quad n, m \geq 1, \quad F(\gamma_1) = 0, \quad G(\gamma_2) = 0.$$

By Theorem 2.11 there exists a polynomial  $h \in \overline{\mathbb{Q}}[X]$  that depends only on  $f, g$  and the generators of  $\Gamma$  such that for all  $n, m \geq 1$  and  $\gamma_1, \gamma_2 \in \Gamma$  one has

$$\gcd(f^n - \gamma_1, g^m - \gamma_2) \mid h.$$

Since both  $F$  and  $G$  have at most  $d$  roots in  $\Gamma$ , we conclude the proof with  $H = h^d$ .

## 7. PROOFS OF RESULTS ON FUNCTIONS WHOSE SPECIALISATIONS ARE LINEAR RECURRENCE SEQUENCES

**7.1. Proof of Theorem 2.15.** For each  $\alpha \in \mathbb{C}$  we consider the sequence  $(\Delta_h(\alpha))_{h=0}^\infty$  of Kronecker-Hankel determinants

$$\Delta_h(\alpha) = \det (F_{i+j}(\alpha))_{0 \leq i, j \leq h-1}, \quad h = 0, 1, \dots$$

Assume there exist infinitely many  $\alpha \in \mathbb{C}$  such that  $(F_n(\alpha))_{n=0}^\infty$  is a linear recurrence of order at most  $K$ . Hence, by Lemma 3.9 for all  $h \geq K + 1$  we have

$$\Delta_h(\alpha) = 0$$

for infinitely many  $\alpha \in \mathbb{C}$ . Therefore, for all  $h \geq K + 1$ , the rational function

$$\Delta_h(X) = \det (F_{i+j}(X))_{0 \leq i, j \leq h-1}$$

has infinitely many zeros, and thus is identical to zero.

Applying Lemma 3.9 again, we conclude the proof.

**7.2. Proof of Corollary 2.16.** Assume  $(F_n(\alpha))_{n=0}^\infty$  is a linear recurrence sequence of order  $k(\alpha)$  for uncountably many  $\alpha \in \mathbb{C}$ . Since the set

$$\mathcal{K} = \{k(\alpha) : \alpha \in \mathbb{C}\} \subseteq \mathbb{N}$$

is countable, at least one element in  $\mathcal{K}$  comes from infinitely many  $\alpha \in \mathbb{C}$  (in fact uncountably many times). Thus, there are infinitely many  $\alpha \in \mathbb{C}$  such  $(F_n(\alpha))_{n=0}^\infty$  is a linear recurrence of some order  $k$  and by Theorem 2.15 the result follows.

## 8. COMMENTS AND FURTHER QUESTIONS

As we have mentioned Theorem 2.1 can be extended to non-simple sequences without new ideas and just at the cost of introducing more complicated notations.

We also remark that Theorem 2.1 is an analogue of a result of Kulka-rni, Mavraki, and Nguyen [24, Proposition 2.2], see also [4, Proposition 2.2], in which the coefficients  $a_1, \dots, a_k$  of  $F_n(X)$  in (1.2) are constants rather than polynomials as in our case. Moreover, [24, Proposition 2.2] is not effective while Theorem 2.1 is.

Furrrhermore, if as in [24] the coefficients  $a_1, \dots, a_k$  of  $F_n(X)$  in (1.2) are constants then analysing the bounds of [33] underlying Lemma 3.2 we see that  $D^4$  can be replaced with  $D_0^3 D$ , where  $D_0$  is the degree of the Galois closure of  $\mathbb{Q}(a_1, \dots, a_k)$  over  $\mathbb{Q}$ . In turn, in this case, this leads to a single exponential bound of the form

$$n \leq \exp(CD_\alpha),$$

in Theorem 2.1.

We describe a possible generalisation of Theorem 2.1 to  $S$ -unit equations in  $\overline{\mathbb{Q}}(X)$ . Let  $\Gamma$  be a finitely generated subgroup of  $\overline{\mathbb{Q}}(X)$  and fix rational functions  $a_1, \dots, a_k \in \overline{\mathbb{Q}}(X)$ . By [2, Proposition 6.1], for any rational functions  $u_1, \dots, u_k \in \Gamma$  such that

$$u_i/u_j \notin \overline{\mathbb{Q}}, \quad 1 \leq i < j \leq k, \quad \text{and} \quad \sum_{i=1}^k a_i u_i \neq 0,$$

the set of  $\alpha \in \overline{\mathbb{Q}}$  such that

$$(8.1) \quad \sum_{i=1}^k a_i(\alpha) u_i(\alpha) = 0$$

is a set of bounded height, depending only on  $a_1, \dots, a_k$  and the generators of  $\Gamma$ .

We now ask for an analogue of Theorem 2.1 for such equations. It is convenient to define the notion of a *primitive solution* to (8.1) as a solution with  $u_i(\alpha) = 1$  for some  $i = 1, \dots, k$ . We now ask the following.

**Question 8.1.** *Is it true, under some natural conditions on the generators of  $\Gamma$ , that outside of a set of bounded height of values  $\alpha \in \overline{\mathbb{Q}}$ , then for every primitive solution to (8.1),  $\max_{i=1, \dots, k} \deg u_i$  is bounded only in terms of the degree  $D_\alpha$  of the smallest Galois field  $\mathbb{K}$  over  $\mathbb{Q}$  with  $\alpha \in \mathbb{K}$ , the functions  $a_1, \dots, a_k$  and the generators of  $\Gamma$ ?*

We note that the idea of the proof of [2, Proposition 6.1] which reduces  $S$ -unit equations to equations of the type (2.2), can perhaps help to tackle Question 8.1. Unfortunately, during this reduction we do not control well the corresponding polynomials  $a_1, f_1, \dots, a_k, f_k \in \overline{\mathbb{Q}}(X)$  and in particular it is not immediately clear how to verify the necessary condition of Theorem 2.1.

We remark that the proof of Theorem 2.1 relies on the fact that outside of a small set of parameters the corresponding specialisations are sequences with at most two dominant roots. On the other hand, in the proof of Theorem 2.7 we show that for all but finitely many specialisations at roots of unity these sequences have only one dominant root. These ideas can be used to study many other properties of the corresponding linear recurrence sequences. For example, by combining this approach with results and ideas of [35, 38, 39] one can study prime ideal divisors of elements of these sequences.

#### ACKNOWLEDGEMENT

This work was supported, in part, by the Australian Research Council Grant DP180100201. The authors are grateful to Umberto Zannier for useful discussions on previous versions of the file. The first author gratefully acknowledges the hospitality and generosity of the Max Planck Institute of Mathematics, where parts of this paper were developed.

#### REFERENCES

- [1] N. Ailon and Z. Rudnick, ‘Torsion points on curves and common divisors of  $a^k - 1$  and  $b^k - 1$ ’, *Acta Arith.*, **113** (2004), 31–38. [3](#), [7](#), [9](#), [17](#)
- [2] F. Amoroso, D. Masser and U. Zannier, ‘Bounded height in pencils of finitely generated subgroups’, *Duke Math. J.*, **166** (2017) 2599–2642. [2](#), [3](#), [5](#), [6](#), [10](#), [11](#), [19](#), [20](#)
- [3] F. Amoroso and E. Viada, ‘On the zeros of linear recurrence sequences’, *Acta Arith.*, **147** (2011), 387–396. [1](#)

- [4] J. P. Bell, K. D. Nguyen and U. Zannier, ‘ $D$ -finiteness, rationality, and height’, *Trans. Amer. Math. Soc.*, **373** (2020), 4889–4906. [19](#)
- [5] A. Bérczes, J.-H. Evertse, K. Györy and C. Pontreau, ‘Effective results for points on certain subvarieties of tori’, *Math. Proc. Cambridge Phil. Soc.* **147** (2009), 69–94. [8](#), [17](#)
- [6] J. Berstel and M. Mignotte, ‘Deux propriétés décidables des suites récurrentes linéaires’, *Bull. Soc. Math. France*, **104** (1976), 175–184. [2](#), [5](#)
- [7] F. Beukers and C. J. Smyth, ‘Cyclotomic points on curves’, *Number Theory for the Millenium* (Urbana, Illinois, 2000), I, A K Peters, 2002, 67–85. [17](#)
- [8] Y. Bilu and F. Luca, ‘Binary polynomial power sums vanishing at roots of unity’, *Preprint*, 2020, available at <https://arxiv.org/abs/2005.05500>. [7](#)
- [9] E. Bombieri, D. Masser and U. Zannier, ‘Intersecting a curve with algebraic subgroups of multiplicative groups’, *Int. Math. Res. Not.*, **20** (1999), 1119–1140. [6](#), [7](#)
- [10] E. Bombieri, D. Masser and U. Zannier, ‘On unlikely intersections of complex varieties with tori’, *Acta Arith.*, **133** (2008), 309–323. [7](#)
- [11] E. Bombieri and W. Gubler, *Heights in Diophantine geometry*, Cambridge Univ. Press, Cambridge, 2006. [3](#), [12](#)
- [12] B. Brindza, ‘Zeros of polynomials and exponential diophantine equations’, *Compos. Math.*, **61** (1987), 137–157.
- [13] W. D. Brownawell, D. Masser, ‘Vanishing sums in function fields’, *Math. Proc. Cambridge Philos. Soc.*, **100** (1986), 427–434. [13](#)
- [14] Y. Bugeaud, P. Corvaja and U. Zannier, ‘An upper bound for the G.C.D. of  $a^n - 1$  and  $b^n - 1$ ’, *Math. Z.*, **243** (2003), 79–84. [12](#)
- [15] P. Corvaja and U. Zannier, ‘A lower bound for the height of a rational function at  $S$ -unit points’, *Monatsh. Math.*, **144** (2005), 203–224. [3](#)
- [16] P. Corvaja and U. Zannier, ‘Some cases of Vojta’s conjecture on integral points over function fields’, *J. Alg. Geometry*, **17** (2008), 295–333. [3](#), [7](#)
- [17] A. Dubickas and M. Sha, ‘The distance to square-free polynomials’, *Acta Arith.*, **186** (2018), 243–256. [14](#)
- [18] G. Everest, A. J. van der Poorten, I. E. Shparlinski and T. B. Ward, *Recurrence sequences*, Amer. Math. Soc., 2003. [1](#), [5](#), [13](#)
- [19] C. Fuchs, ‘Polynomial-exponential equations and linear recurrences’, *Glasnik Matem.*, **38** (2003), 233–252. [17](#)
- [20] C. Fuchs and S. Heintze, ‘On the growth of linear recurrences in function fields’, *Preprint*, 2020, available at <https://arxiv.org/abs/2006.11074>. [13](#)
- [21] C. Fuchs, and A. Pethö, ‘Effective bounds for the zeros of linear recurrences in function fields’, *Journal de Théorie des Nombres de Bordeaux*, **17** (2005), 749–766. [12](#)
- [22] M. Hindry and J. H. Silverman, *Diophantine geometry*, Graduate Texts in Mathematics **201**, Springer, New York, 2000. [3](#)
- [23] N. Koblitz,  *$p$ -adic numbers,  $p$ -adic analysis, and zeta-functions*, Springer-Verlag, New York, 1977. [13](#)
- [24] A. Kulkarni, N. M. Mavraki, and K. D. Nguyen, ‘Algebraic approximations to linear combinations of powers: an extension of results by Mahler and Corvaja-Zannier’, *Trans. Amer. Math. Soc.*, (to appear). [2](#), [19](#)

- [25] S. Lang, ‘Division points on curves’, *Ann. Mat. Pura Appl.*, **70** (1965), 229–234. [6](#), [16](#), [17](#)
- [26] A. Levin, ‘Greatest common divisors and Vojta’s conjecture for blowups of algebraic tori’, *Invent. Math.*, **215** (2019), no. 2, 493–533. [3](#), [7](#)
- [27] A. Levin and J. T.-Y. Wang, ‘Greatest common divisors of analytic functions and Nevanlinna theory of algebraic tori’, *J. Reine Angew. Math.*, (to appear). [3](#), [7](#)
- [28] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge Univ. Press, Cambridge, 1997. [13](#)
- [29] R. C. Mason, *Diophantine equations over function fields*, London Mathematical Society Lecture Note Series **96** (1984), Cambridge University Press. [12](#), [17](#)
- [30] G. Maurin, ‘Courbes algébriques et équations multiplicatives’, *Math. Ann.*, **341** (2008), 789–824. [7](#)
- [31] A. Ostafe, ‘On some extensions of the Ailon-Rudnick theorem’, *Monat. für Math.*, **181** (2016), 451–471. [3](#), [7](#), [17](#)
- [32] F. Pakovich and I. E. Shparlinski, ‘Level curves of rational functions and unimodular points on rational curves’, *Proc. Amer. Math. Soc.*, **148** (2020), 1829–1833. [3](#), [7](#), [8](#), [9](#)
- [33] M. Sha, ‘Effective results on the Skolem problem for linear recurrence sequences’, *J. Number Theory*, **197** (2019) 228–249. [1](#), [2](#), [3](#), [10](#), [19](#)
- [34] W. M. Schmidt, ‘Northcott’s theorem on height I. A general estimate’, *Monat. Math.*, **115** (1993), 169–181. [8](#)
- [35] I. E. Shparlinski, ‘Prime divisors of recurrent sequences’, *Isv. Vyssh. Uchebn. Zaved. Math*, no.4, (1980), 101–103 [20](#)
- [36] J. H. Silverman, ‘The S-unit equation over function fields’, *Proc. Camb. Philos. Soc.*, **95** (1984), 3–4. [12](#), [17](#)
- [37] J. H. Silverman, *The arithmetic of dynamical systems*, Springer-Verlag, New York, 2007. [3](#), [4](#), [11](#)
- [38] C. L. Stewart, ‘On divisors of terms of linear recurrence sequences’, *J. Reine Angew. Math.*, **333** (1982), 12–31. [20](#)
- [39] C. L. Stewart, ‘On the greatest square-free factor of terms of a linear recurrence sequence’, *Diophantine Equations* Tata Inst. Fund. Res. Stud. Math., 20, Tata Inst. Fund. Res., Mumbai, 2008, 257–264, [20](#)
- [40] W. W. Stothers, ‘Polynomial identities and Hauptmoduln’, *Quarterly J. Math. Oxford*, **32** (1981), 349–370. [12](#), [17](#)
- [41] J. F. Voloch, ‘Diagonal equations over function fields’, *Bol. Soc. Brasil. Mat.*, **16** (1985), 29–39. [12](#)
- [42] U. Zannier, *Lecture notes on Diophantine analysis*, Publ. Scuola Normale Superiore, Pisa, 2009. [3](#)

SCHOOL OF MATHEMATICS AND STATISTICS, UNIVERSITY OF NEW SOUTH WALES, SYDNEY NSW 2052, AUSTRALIA

*E-mail address:* [alina.ostafe@unsw.edu.au](mailto:alina.ostafe@unsw.edu.au)

SCHOOL OF MATHEMATICS AND STATISTICS, UNIVERSITY OF NEW SOUTH WALES, SYDNEY NSW 2052, AUSTRALIA

*E-mail address:* [igor.shparlinski@unsw.edu.au](mailto:igor.shparlinski@unsw.edu.au)