ON THE DIOPHANTINE EQUATION $G_n(x) = G_m(y)$ WITH $Q(x, y) = 0$

CLEMENS FUCHS*, ATTILA PETHŐ‡, AND ROBERT F. TICHY*

Dedicated to Wolfgang Schmidt on his 70th birthday.

Abstract. Let $\mathbf{K}$ be a field of characteristic 0 and let $(G_n(X))_{n=0}^{\infty}$ be a linear recurring sequence of degree d in $\mathbf{K}[X]$ defined by the initial terms $G_0, \ldots, G_{d-1} \in \mathbf{K}[X]$ and by the difference equation

$$G_{n+d}(X) = A_{d-1}(X)G_{n+d-1}(X) + \ldots + A_0(X)G_n(X), \quad \text{for } n \geq 0,$$

with $A_0, \ldots, A_{d-1} \in \mathbf{K}[X]$. Finally, let $Q(X, Y) \in \mathbf{K}[X, Y]$. In this paper we are giving conditions depending only on $G_0, \ldots, G_{d-1}$, on Q, and on $A_0, \ldots, A_{d-1}$ under which the Diophantine equation

$$G_n(x) = G_m(y) \quad \text{with} \quad Q(x, y) = 0$$

has only finitely many solutions $(n, m) \in \mathbb{Z}^2$. This paper is a continuation of the work of the authors on this equation in the special case of $Q(X, Y) = Y - P(X)$ (cf. [7, 6, 8]) and of a recent result due to U. Zannier [14].

2000 *Mathematical Subject Classification*: Primary 11D45; Secondary 11D04, 11D61, 11B37.

Key words and phrases. Diophantine equations, linear recurring sequences, S-unit equations

1. Introduction

Let $\mathbf{K}$ denote an algebraically closed field of characteristic 0, and let $A_0, \ldots, A_{d-1}, G_0, \ldots, G_{d-1} \in \mathbf{K}[X]$ and $(G_n(X))_{n=0}^{\infty}$ be a sequence of polynomials defined by the d-th order linear recurring relation

$$(1) \quad G_{n+d}(X) = A_{d-1}(X)G_{n+d-1}(X) + \ldots + A_0(X)G_n(X), \quad \text{for } n \geq 0.$$

Furthermore, let $P(X) \in \mathbf{K}[X], \deg P \geq 1$. Recently, the authors investigated the question, what can be said about the number of solutions of the

* *Address:* Institut für Mathematik A, TU Graz, Steyrergasse 30/II, 8010 Graz, Austria. *E-mail addresses:* clemens.fuchs@tugraz.at and tichy@tugraz.at.

‡ *Address:* Institute of Informatics, University of Debrecen, PO Box 12, 4010 Debrecen, Hungary. *E-mail address:* pethoe@inf.unideb.hu.

This work was supported by the Austrian Science Foundation FWF, grant S8307-MAT.

The second author was supported by the Hungarian National Foundation for Scientific Research Grant No. 38225 and 42985.

Diophantine equation

$$G_n(X) = G_m(P(X)). \tag{2}$$

The problem was motivated by properties of families of orthogonal polynomials. For example, the Chebyshev polynomials of the first kind , which are defined by

$$T_n(X) = \cos(n \arccos X),$$

have the well known property that

$$T_{2n}(X) = T_n(2X^2 - 1)$$

for all integers n. Let us mention that all orthogonal polynomials satisfy a second order linear recurring sequence, e.g. for the Chebyshev polynomials we have $T_0(X) = 1, T_1(X) = X$ and $T_{n+2}(X) = 2XT_{n+1}(X) - T_n(X), n = 0, 1, 2, \ldots$.

Recently, the authors [7] were able to formulate conditions for sequences of polynomials satisfying a second order linear recurrence under which they could conclude that (2) has only finitely many solutions $m, n \in \mathbb{Z}, m, n \geq 0, m \neq n$. For the proof they used the Main Theorem on S-unit equations over finitely generated fields of characteristic zero [3, 5]. Furthermore, they were able to quantify their results by transforming their problem in the function field generated by the characteristic root of the recurrence over the rational function field $\mathbf{K}(x)$.

The first author gave suitable extensions of the above results for third order linear recurring sequences (cf. [6]). Later on, the authors generalized their results to linear recurring sequences $G_n(X)$ of arbitrary large order [8]. The conditions are somehow complicated to state, essentially, they ensure that there exist valuations in the underlying function field, which have special properties. Let

$$\mathcal{G}(X, T) = T^d - A_{d-1}(X)T^{d-1} - \ldots - A_0(X) \in \mathbf{K}[X][T]$$

denote the characteristic polynomial of the sequence $(G_n(X))_{n=0}^{\infty}$ and $D(X)$ be the discriminant of $\mathcal{G}(X, T)$. We let $\alpha_1, \ldots, \alpha_r$ denote the distinct roots of the characteristic polynomial $\mathcal{G}(X, T)$ in the splitting field L of $\mathcal{G}(X, T)$. It is well known that $(G_n(X))_{n=0}^{\infty}$ has a nice "analytic" representation. More precisely, there exist polynomials $C_1(T), \ldots, C_r(T) \in L[T]$ such that

$$G_n(X) = C_1(n)\alpha_1^n + \ldots + C_r(n)\alpha_r^n, \tag{3}$$

holds for all $n \geq 0$. Assuming that $\mathcal{G}(X, T)$ has no multiple roots, i.e. $D(X) \neq 0$, we have that the $C_i(T) = c_i$ are all constant for all $i = 1, \ldots, r = d$. Assume now that the d-th order ($d \geq 2$) linear recurring sequence $(G_n(X))_{n=0}^{\infty}$ and the polynomial $P \in \mathbf{K}[X]$ satisfy the following conditions:

1. None of the roots and the quotients of distinct roots of the characteristic polynomial of $(G_n(X))_{n=0}^{\infty}$ is an element of $\mathbf{K}^*$,
2. $\deg P \geq 2$ and $\deg D \geq 1$,

(3) $\gcd(D, A_0) = 1$ and
(4) $\gcd(D, R(A_0, \dots, A_d, G_0, \dots, G_d)) = 1$,

for some polynomial $R(A_0, \dots, A_d, G_0, \dots, G_d) \in \mathbb{Q}[A_0, \dots, A_d, G_0, \dots, G_d]$ (for details we refer to [8]). Then equation

$$G_n(X) = c\, G_m(P(X)), \tag{4}$$

where $c \in \mathbf{K}^* = \mathbf{K}\backslash\{0\}$ is variable, has at most

$$C(d, A_0, D, P) := \\ = e^{(6d)^{4d}} \left(\log\left(d^{2d^2} \deg D(\deg P + 1)\right)\right)^{2d^2} (2ed)^{30d^3 d!^2 \deg A_0 \deg P}$$

solutions $(n, m) \in \mathbb{Z}^2$ with $n, m \geq 0, n \neq m$. We also obtained the result under the following conditions:

(1) None of the roots and the quotients of distinct roots of the characteristic polynomial of $(G_n(X))_{n=0}^{\infty}$ is an element of $\mathbf{K}^*$,
(2) $\deg P \geq 1$, and $\deg D \geq 1$,
(3) $\deg A_0 \geq 1$, $R(A_0, \dots, A_d, G_0, \dots, G_d) \neq 0$, and
(4) the set of zeroes of A_0 is not equal to that of $A_0(P)$.

Then equation (4) has at most $C(d, A_0, D, P)$ solutions $(n, m) \in \mathbb{Z}^2$ with $n, m \geq 0, n \neq m$.

For the special case of the equation

$$G_n(X) = G_m(P(X)) \tag{5}$$

we could even show more. Namely, assuming the conditions from above with

(1') None of the roots and the quotients of distinct roots of the characteristic polynomial of $(G_n(X))_{n=0}^{\infty}$ is a root of unity,

instead of (1), respectively, we proved that equation (5) has at most

$$e^{(12d)^{6d}},$$

solutions $(n, m) \in \mathbb{Z}^2$ with $n, m \geq 0, n \neq m$.

Very recently, U. Zannier used elementary method from the theory of function fields to improve on these results. In fact, he was able to completely describe the matter: suppose that $\deg P \geq 2$ and that the recurring sequence $G_n(X)$ is simple with characteristic roots $\alpha_1, \dots, \alpha_d$ satisfying that no ratio α_i/α_j, $i \neq j$, lies in $\mathbf{K}$. Then if there are only finitely many solutions m, n of

$$G_n(X) = c\, G_m(P(X)), \quad m, n \in \mathbb{N},$$

where $c = c(m, n) \in \mathbf{K}^*$ may depend on m, n, their number is at most $8d^6$. If there are infinitely many solutions then for suitable $r, s \in \mathbb{N}$ we have an identity

$$G_{sn+v_0}(P(X)) = \eta\xi^n G_{rn+u_0}(X), \quad n \in \mathbb{N}, \quad |r| = |s|\deg P > 0,$$

for suitable $\xi, \eta \in \mathbf{K}^*$, and two cases may occur, which he calls the "cyclic" (which denotes essentially the case $G_n(X) = X^n, P(X) = X^p$) and the

"Chebyshev" case (which is essentially the example from the motivation, i.e. $G_n(X) = T_n(X), P(X) = T_p(X)$). More precisely we have:

Cyclic case: P is of the form $\lambda' \circ X^p \circ \lambda$ for suitable $\lambda, \lambda' \in \mathrm{PGL}_2(\mathbf{K})$. Also, the α_i are in $\mathbf{K}(X)$, of the form $c_i X^{\delta_i} \circ \lambda$, for integers δ_i and $c_i \in \mathbf{K}$,

Chebyshev case: $P(X) = \lambda' \circ T_p \circ \lambda$, λ, λ' as above. The α_i are quadratic over $\mathbf{K}(X)$ and of the form $c_i(X \pm \sqrt{X^2-1})^{\delta_i} \circ \lambda$.

Our aim is to generalize this result to the equation

$$G_n(x) = c\, G_m(y), \tag{6}$$

where $c = c(m,n) \in \mathbf{K}^*$ may vary with m, n and where x, y are algebraically dependent, i.e. a relation $Q(x,y) = 0$ holds for some polynomial $Q(X,Y) \in \mathbf{K}[X,Y]$. Moreover, we want to consider arbitrary linear recurring sequences $(G_n(X))_{n=0}^\infty$ (and not only simple linear recurrences as before). This equation can be understood as an identity in $\mathbf{K}[X,Y]/(Q(X,Y))$, which denotes the residue class ring of the curve $Q(x,y) = 0$. Using the ideas introduced in [14], we want to give necessary conditions under which the more general problem has at most finitely many solutions.

Observe that we may assume without loss of generality that $Q(X,Y)$ is absolutely irreducible and we will assume this for the rest of the paper.

2. Results

Before we state our results, let us start with a small discussion about the polynomial $Q(X,Y)$, which is assumed to be absolutely irreducible. We can also assume that the leading coefficient of Y in $Q(X,Y)$ belongs to $\mathbf{K}$, or equivalently that y is integral over $\mathbf{K}(x)$. Otherwise, there exists a valuation ν in the function field $\mathbf{K}(x,y)$, which is a pole of y. But this implies by our equation $G_n(x) = c\, G_m(y)$ that

$$0 \le \nu(G_n(x)) = \nu(G_m(y)) \le \nu(y) < 0,$$

which is a contradiction. Observe that clearly the $G_n(x)$ are integral (they are polynomials). Because of symmetry, we can also assume that x is integral over $\mathbf{K}(y)$ and therefore that the leading coefficient of X in $Q(X,Y)$ does not depend on Y. Therefore, we have

$$Q(X,Y) = Y^{\deg Q_Y} + q_1(X) Y^{\deg Q_Y - 1} + \ldots + q_p' X^{\deg Q_X} + q_p(X),$$

with $q_p' \in \mathbf{K}, q_i(X) \in \mathbf{K}[X], i = 1, \ldots, p$ and $\deg q_p(X) < \deg Q_X =: p$.

We do not immediately start with our special case: first we study the general situation of intersections of two linear recurrences defined over a function field. The following proposition is a generalization of [14, Corollary 2] to the case of arbitrary (also non-simple) linear recurring sequences G_n and H_n given by

$$\begin{aligned} G_n &= C_1(n)\alpha_1^n + C_2(n)\alpha_2^n + \ldots + C_p(n)\alpha_p^n, \\ H_n &= D_1(n)\beta_1^n + D_2(n)\beta_2^n + \ldots + D_q(n)\beta_q^n, \end{aligned}$$

where $\alpha_i, \beta_j \in L^*$ and $0 \neq C_i, D_i \in L[X]$ and L is a function field in one variable over $\mathbf{K}$, and which is therefore of interest on its own.

Theorem 1. *Assume that no α_i or β_j and no ratio α_i/α_j or $\beta_i/\beta_j, i \neq j$ lies in $\mathbf{K}^*$. Then the equation $G_n = c\,H_m, c = c(n,m) \in \mathbf{K}^*$ has at most*

$$C(\operatorname{ord} G_n, \operatorname{ord} H_n) := 9d^4(3d^2 + e^{e^{e^{20d}}} + rd^2)$$

solutions $(m,n) \in \mathbb{Z}^2$, where $d = \max\{\operatorname{ord} G_n, \operatorname{ord} H_n\}$ and r is the rank of the multiplicative group generated by the α_i and β_j, unless there are integers n_0, m_0, r, s, with $rs \neq 0$, elements $\xi, \eta \in \mathbf{K}^*$ and polynomials $0 \neq P, Q \in \mathbf{K}[X]$ such that the identity

$$G_{n_0+rm} = \frac{P(m)}{Q(m)}\eta\xi^m H_{m_0+sm}$$

holds for $m \in \mathbb{Z}$.

Moreover, in this case we have that there exist $S_1, \ldots, S_p \in L[X]$ such that

$$C_i(n_0 + rX) = \eta\alpha_i^{-n_0}P(X)S_i(X) \text{ and } D_{\pi(i)}(m_0 + sX) = \beta_{\pi(i)}^{-m_0}Q(X)S_i(X),$$

and for the corresponding roots $\alpha_i^r/\beta_{\pi(i)}^s \in \mathbf{K}$ for $i = 1, \ldots, p = q$ and where π is a permutation of the set $\{1, \ldots, p\}$.

The proof of this result follows the line of proof from [14, Corollary 2] and uses a result due to Shorey and Tijdeman, which is shown by Baker's method of linear forms in logarithms of algebraic numbers (see [12, pp. 84-85] and [4, Lemma 3]). Some more remarks are in order.

Remark 1. First of all, it is quite clear that there can exist infinitely many solutions and that the statement about the polynomials P, Q is necessary. Because, if we assume that

$$G_n = P(n)S_n, \quad H_n = Q(n)S_n,$$

where $P, Q \in \mathbf{K}[X]$ and $(S_n)_{n=0}^{\infty}$ is a linear recurring sequences defined over L, then we have $G_n = c\,H_n$ with $c = \frac{P(n)}{Q(n)}$ for all $n \in \mathbb{Z}$.

Remark 2. We want to mention that such a conclusion also appears in a similar context about arbitrary (non-simple) linear recurring sequences. Namely in [2], Corvaja and Zannier proved that if G_n/H_n is an integer for infinitely many n, then there exists a polynomial P such that $P(n)G_n/H_n$ is a linear recurring sequence for all n in an arithmetic progression.

Remark 3. If we are interested in solutions of the equation $G_n = H_m$, then infinitely many solutions can come only from an identity of the form $G_{n_0+rm} = H_{m_0+sm}$ for all $m \in \mathbb{Z}$, which means that

$$C_i(n_0 + rX)\alpha_i^{n_0} = \eta D_{\pi(i)}(m_0 + sX)\beta_{\pi(i)}^{m_0}, \eta \in \mathbf{K} \quad \text{and} \quad \alpha_i^r/\beta_{\pi(i)}^s \in \mathbf{K}$$

for $i = 1, \ldots, p = q$ and where π is permutation of $\{1, \ldots, p\}$.

Now, we are ready to come to our special case, where $G_n = G_n(x)$ and $H_n = G_n(y)$. From the above Theorem it follows at once that either equation (6) has at most $C(\operatorname{ord} G_n, \operatorname{ord} G_n)$ many solutions or an identity of the above type must hold. We investigate the latter case in this more special situation and we prove the following theorem.

Theorem 2. *Assume that the d-th order ($d \geq 1$) linear recurring sequence $(G_n(X))_{n=0}^{\infty}$ and the irreducible polynomial $Q(X, Y) \in \mathbf{K}[X, Y]$ satisfy the following conditions:*

(i) None of the α_i and the ratios α_i/α_j, $i \neq j$ is an element of $\mathbf{K}^*$, and
(ii) the set of zeros of the polynomial $A_0(X)$ is not equal to that of $\operatorname{Res}_Y(A_0(Y), Q(X, Y))$.

Then there are at most $\tilde{C}(ord G_n)$ pairs $(m, n) \in \mathbb{Z}^2$ for which equation (6) holds, where

$$\tilde{C}(d) := 9d^4(3d^2 + e^{e^{e^{20d}}} + rd^2)$$

and where r is the rank of the multiplicative group generated by the α_i.

As usual $\operatorname{Res}_Y(f, g)$ denotes the resultant of the two polynomials f, g with respect to Y.

The question now is the following: do there occur infinite families of solutions other then those in the cyclic and Chebyschev case from above, when we consider curves $Q(x, y) = 0$, which are not of the form $y = P(x)$?

Remark 4. First of all, it is clear that additional infinite families of solutions may appear. For example we have for

$$Q(x, y) = acx^m - ay^m - b(1 - c) = 0$$

with $a, b, c \in \mathbf{K}, m \geq 3$ and $P(X) = aX^m + b$ that $P(y) = c\,P(x)$. Therefore, we get for $G_n(x) = P(x)^n, n \in \mathbb{Z}$ that

$$G_n(y) = P(y)^n = (cP(x))^n = c^n P(x)^n = c^n G_n(x)$$

for all $n \in \mathbb{Z}$. By [13, VI.3.3. Example, page 197] the genus of $Q(x, y) = 0$ is $g = \frac{(m-1)(m-2)}{2} > 0$. This example shows that at least in the case of positive genus also other infinite families may occur.

Remark 5. We may mention that condition (ii) also naturally appears in the context of the conditions given in our previous papers (see [7, 6, 8]). Namely, it is easy to see that we have

$$\operatorname{Res}_Y(A_0(Y), Q(X, Y)) = (\mathrm{lc} A_0)^{\deg Q_Y} X^{\deg Q_X + \deg A_0} + \ldots,$$

where $\mathrm{lc}A_0$ denotes the leading coefficient of A_0. If we additionally assume that $\deg_X Q \geq 2$, we therefore have a valuation ν with $\nu(D(y)) > \nu(D(x))$, which was the main point in our previous considerations.

We mention that from the proof we see that we must exclude that $A_0^r(y) = cA_0(x)^s$ for some $r, s \in \mathbb{N}, c \in \mathbf{K}^*$. Whenever, we can find

$$Q(X,Y) \,\big|\, A_0(Y)^r - cA_0(X)^s,$$

we have other infinite families as described above (observe that the example before was constructed with the trivial case $Q(X,Y) = A_0(Y) - cA_0(X)^q$). It follows by Schinzel (see [9, page 58]) that if $A_0(X)$ is indecomposable over $\mathbf{K}$, which means that if $A_0(X) = F_1(F_2(X)), F_1, F_2 \in \mathbf{K}[X]$ then $\deg F_1 = 1$ or $\deg F_2 = 1$, and $\deg A_0 > 31$, then $A_0(Y) - cA_0(X)^q$ is irreducible over $\mathbf{K}$. We conjecture that $F(X,Y) = A_0(Y) - cA_0(X)^q$ with A_0 indecomposable (and it is clear that this is needed) and $A_0(y) \neq B(y)^p$ or $-4B(y)^4$ is always irreducible. Schinzel mentioned to us that this conjecture - if true - lies deeper than Capelli's theorem (e.g. see [9, Theorem 19, page 92]), since it depends on the characteristic of $\mathbf{K}$ while Capelli's theorem does not.

Remark 6. The motivation to look at this generalisation is the following: if it would be possible to prove that $G_n(x) = c\,G_m(y)$ with $Q(x,y) = 0$ has no solution unless we have a trivial infinite family, then it would be possible to handle the Diophantine equation $G_n(X) = G_m(Y)$ in integers X, Y by the method of Bilu and Tichy [1].

3. Proof of Theorem 1

We start by rewriting our equation $G_n = c\,H_m$ as

$$G_n - c\,H_m = \sum_{i=1}^{p} C_i(n)\alpha_i^n 1^m - \sum_{i=1}^{q} cD_i(n)1^n\beta_i^m = 0.$$

We define vectors $A_i = (\alpha_i, 1) \in (L^*)^2$ for $i = 1, \ldots, p, A_{p+i} = (1, \beta_i) \in (L^*)^2$ for $i = 1, \ldots, q$ and polynomials $P_i = C_i, i = 1, \ldots, p, P_{p+i} = D_i, i = 1, \ldots, q$, respectively.

Now we apply the following theorem due to Zannier (see [14, Theorem 1] and also [14, Definition 1]):

Lemma 3. *Let $A_1, \ldots, A_h \in (L^*)^r$ and let $P_1, \ldots, P_h \in L[X_1, \ldots, X_r] = L[\mathbf{X}]$ satisfy deg $P_i \leq d_i$. Then the set*

$$S = \{\mathbf{m} \in \mathbb{Z}^r \,:\, P_i(\mathbf{m})A_i^{\mathbf{m}}, i = 1, \ldots, h \textit{ are linearly independent over} \mathbf{K}\},$$

(here for $A = (\alpha_1, \ldots, \alpha_r)$ we define $A^{\mathbf{m}} = \alpha_1^{m_1} \cdots \alpha_r^{m_r}$) may be expressed as a union of no more than

$$\left(d_1 + \ldots + d_h + \binom{h}{2}\right)^r$$

classes, where we say that $S \subset \mathbb{Z}^r$ is a class relative to a nonempty subset B of $\{1, \ldots, h\}$, if

- *(i) for every $\mathbf{m} \in S$ the elements $P_i(\mathbf{m})A_i^{\mathbf{m}}, i \in B$ are linearly independent over $\mathbf{K}$ and* *(ii) for some* $\mathbf{m}_0 \in S$ *the set* S *is made up by all* $\mathbf{m}$ *satisfying (i) and such that for* $i,j \in B$ *we have* $(A_iA_j^{-1})^{\mathbf{m}-\mathbf{m}_0} \in \mathbf{K}^*$.

Now, we get by applying Lemma 3 that all solutions $(m,n) \in \mathbb{Z}^2$ of our equation are contained in at most

$$\left(\operatorname{ord} G_n + \operatorname{ord} H_n + \binom{p+q}{2}\right)^2 \leq \left(3\max\{\operatorname{ord} G_n, \operatorname{ord} H_n\}^2\right)^2$$

classes (for a definition of classes see Lemma 3 or [14, Definition 2]).

We are going to estimate the number of solutions in each class Ω, corresponding to the subset $B = B_\Omega \subset \{1,\dots,p+q\}$. As in the proof of [14, Corollary 2] it is easy to see by [14, Corollary 1(b)] that there are at most $\max\{\operatorname{ord} G_n, \operatorname{ord} H_n\} + \binom{p+q}{2}$ solutions in every class containing distinct integers i,j in $[1,p]$ or $[p+1,p+q]$, respectively, having $C_1(n)\cdots C_p(n) \neq 0$ or $D_1(n)\cdots D_q(n) \neq 0$, respectively. Since these cases appear for at most $\max\{\operatorname{ord} G_n, \operatorname{ord} H_n\}$ many n, we get that the number of solutions is bounded by

$$2\max\{\operatorname{ord} G_n, \operatorname{ord} H_n\} + \binom{p+q}{2} \leq 3\max\{\operatorname{ord} G_n, \operatorname{ord} H_n\}^2.$$

In the case that B contains integers i_0, j_0+p with $1 \leq i_0 \leq p, 1, \leq j_0 \leq q$ it is also plain (by the proof of [14, Corollary 2]) that the solutions in the class Ω correspond to integers m such that

$$G_{n_0+rm} = c\,H_{m_0+sm} \tag{7}$$

with integers $n_0, m_0, r, s, rs \neq 0$.

In this case we first group together in a single γ^m two exponentials α_i^{rm} and β_j^{sm}, which are linearly dependent over $\mathbf{K}$. Namely, if $\alpha_i^r = \gamma_{(i,j)}, \beta_j^s = \delta_{(i,j)}\gamma_{(i,j)}$ with $\delta_{(i,j)} \in \mathbf{K}^*$ we have

$$C_i(n_0+rm)\alpha_i^{n_0}\gamma_{(i,j)}^m - cD_j(m_0+sm)\beta_j^{m_0}\delta_{(i,j)}^m\gamma_{(i,j)}^m. \tag{8}$$

Now, we write

$$C_i(n_0+rX)\alpha_i^{n_0} = \sum_{l=1}^u \rho_l Q_{il}(X),$$

$$D_j(m_0+sX)\beta_j^{m_0} = \sum_{l=1}^u \rho_l \tilde{Q}_{jl}(X),$$

where the $\rho_l \in L^*, l = 1,\dots,u$ are linearly independent over $\mathbf{K}$ and the $Q_{il}, \tilde{Q}_{jl}$ lie in $\mathbf{K}[X]$ for each i,j,l. Clearly this is possible for some u with,

$$u \leq (p+q)\max\{\deg C_1,\dots,\deg C_p, \deg D_1,\dots,\deg D_q\}.$$

Thus, (8) becomes

$$\sum_{l=1}^u \left(Q_{il}(m) - c\delta_{(i,j)}^m \tilde{Q}_{jl}(m)\right)\rho_l\gamma_{(i,j)}^m.$$

Up to now we have rewritten (7) as a $\mathbf{K}$-linear combination of expressions of the from $\rho_l \gamma_i^m$, where all these expressions are linearly independent and where $\gamma_i = \gamma_{(i,j)}$ or α_i, β_j, respectively, depending on whether they could be paired with some other term in (7) or not. We have two possible cases: those m for which all coefficients vanish and those for which not all coefficients vanish. In the latter case the elements $\rho_l \gamma_i^m$ are linearly dependent over $\mathbf{K}$, which can happen (by [14, Lemma 2]) for at most $\binom{2(\operatorname{ord} G_n + \operatorname{ord} H_n) - 1}{2}$ many m.

In the first case all terms in G_{n_0+rm} must be paired with the terms in H_{m_0+sm}, so we have $p = q$ and $u \leq 2\operatorname{ord} G_n$. Moreover, there exists a permutation π of the set $\{1, \ldots, p\}$ which pairs each α_i with some $\beta_j = \beta_{\pi(i)}$ such that (7) can be rewritten as

$$\sum_{i=1}^{p} \sum_{l=1}^{u} \left(Q_{il}(m) - c\delta_i^m \tilde{Q}_{\pi(i)l}(m) \right) \rho_l \gamma_i^m = 0.$$

For simplicity we have written here γ_i, δ_i instead of $\gamma_{(i,\pi(i))}, \delta_{(i,\pi(i))}$, respectively. Observe that there are at most $\max\{\operatorname{ord} G_n, \operatorname{ord} H_n\}$ many m for which $C_i(n_0 + rm)$ or $D_j(m_0 + sm) = 0$. For all other m we have

$$\frac{Q_{il}(m)}{\tilde{Q}_{\pi(i)l}(m)} \delta_i^{-m} = c$$

(recall that c here may depend on m) for all i, l or

$$\frac{Q_{il}(m)}{\tilde{Q}_{\pi(i)l}(m)} \frac{\tilde{Q}_{\pi(j)r}(m)}{Q_{jr}(m)} \left(\frac{\delta_j}{\delta_i} \right)^m = 1 \tag{9}$$

for all i, l, j, r.

Now, we pause for a moment to cite the following result from [4, page 148].

Lemma 4. *Let $P \in \overline{\mathbb{Q}}(X)$ be a rational function with no poles outside the disc $\{z \in \mathbb{C} : |z| \leq A\}$ and let $\alpha \in \overline{\mathbb{Q}}$. If there are infinitely many pairs of integers m, n with*

$$m > n \geq A, \quad P(m)\alpha^m = P(n)\alpha^n,$$

then P is constant and α is a root of unity.

We use a specialization argument to reduce our case to the above lemma. For this let $U \subset \mathbf{K}$ be a finite set consisting of all transcendental elements from the $Q_{il}, \tilde{Q}_{\pi(i)l}$ and δ_i for all i, l, together with all possible differences and all multiplicative inverses of these elements. Then by [5, Lemma 3.1] there exists a ring homomorphism $\varphi : \overline{\mathbb{Q}}[U] \longrightarrow \overline{\mathbb{Q}}$ whose restriction to $\overline{\mathbb{Q}}$ is the identity. Applying this map to (9) leads to

$$\frac{\varphi(Q_{ij}(m))}{\varphi(\tilde{Q}_{\pi(i)j}(m))} \frac{\varphi(\tilde{Q}_{\pi(j)r}(m))}{\varphi(Q_{jr}(m))} \left(\frac{\varphi(\delta_j)}{\varphi(\delta_i)} \right)^m = 1. \tag{10}$$

Now, if there are infinitely many such m, then there are infinitely many m, n such that

$$\frac{\varphi(Q_{ij}(m))}{\varphi(\tilde{Q}_{\pi(i)j}(m))}\frac{\varphi(\tilde{Q}_{\pi(j)r}(m))}{\varphi(Q_{jr}(m))}\left(\frac{\varphi(\delta_j)}{\varphi(\delta_i)}\right)^m = \frac{\varphi(Q_{ij}(n))}{\varphi(\tilde{Q}_{\pi(i)j}(n))}\frac{\varphi(\tilde{Q}_{\pi(j)r}(n))}{\varphi(Q_{jr}(n))}\left(\frac{\varphi(\delta_j)}{\varphi(\delta_i)}\right)^n.$$

Therefore, $\max\{m,n\} \longrightarrow \infty$ and the above lemma implies that $\varphi(\delta_j/\delta_i)$ and therefore also δ_j/δ_i is a root of unity. Moreover,

$$\frac{Q_{il}(X)}{\tilde{Q}_{\pi(i)l}(X)} = \frac{Q_{ir}(X)}{\tilde{Q}_{\pi(i)r}(X)} \quad \text{and} \quad \frac{Q_{jl}(X)}{\tilde{Q}_{\pi(j)l}(X)} = \frac{Q_{jr}(X)}{\tilde{Q}_{\pi(j)r}(X)}$$

differ just by a constant (in fact again a root of unity) for all $i \neq j, l \neq r$ (observe that the equalities follow from (10) at once). It follows that there exist polynomials $P, Q \in \mathbf{K}[X]$ such that

$$P(X)S'_{il}(X) = \eta_i Q_{il}(X), \quad Q(X)S'_{il}(X) = \tilde{\eta}_{\pi(i)}\tilde{Q}_{\pi(i)l}(X)$$

for all i, l with $\eta_i, \tilde{\eta}_{\pi(i)} \in \mathbf{K}$ (independent of l) and for some polynomials $S'_{il}(X)$. From this discussion it follows that this case can only hold for all m in the intersection of certain arithmetic progressions, which is either empty or again an arithmetic progression. Moreover, we see that in this case we have $\tilde{\eta}_{\pi(i)}/\eta_i = \eta$ with η a suitable root of unity. Therefore, also the second part of the conclusion of Theorem 1 follows from this.

Further, equation (10) can have finitely many solutions in the following two cases: either $\varphi(\delta_j)/\varphi(\delta_i)$ is a root of unity or not. In the second case the number of m satisfying (10) can be bounded by the zero multiplicity of the underlying linear recurring sequence, hence by

$$\exp(\exp(\exp(20(\operatorname{ord} G_n + \operatorname{ord} H_n)))$$

by [10, 11], since the degrees of the polynomials are bounded by the order of the recurrences. On the other hand, if $\varphi(\delta_j)/\varphi(\delta_i)$ is a root of unity of order ℓ say, then in the ℓ arithmetic progressions $m = k\ell + r, 0 \leq r \leq \ell - 1$, we can bound the number of m's by the degrees of $Q_{il}(X)\tilde{Q}_{jr}(X)$ and $\tilde{Q}_{il}(X)Q_{jr}(X)$, respectively. Therefore, we can bound the number of solutions coming from this case by the rank of the multiplicative group generated by $\alpha_1, \ldots, \alpha_p, \beta_1, \ldots, \beta_p$, which is an upper bound for ℓ, times $\operatorname{ord} G_n + \operatorname{ord} H_n$.

Altogether, we see that there are at most $C(\operatorname{ord} G_n, \operatorname{ord} H_n)$ solutions, which do not come from a trivial relation, which finishes the proof. □

4. Proof of Theorem 2

We already know that we have to study the equation

$$G_{n_0+mr}(x) = \frac{P(m)}{Q(m)} \eta \xi^m G_{m_0+ms}(y) \tag{11}$$

with $\xi, \eta \in \mathbf{K}^*, P(X), Q(X) \in \mathbf{K}[X]$ and with integers $n_0, m_0, r, s, rs \neq 0$, which is an identity in the function field $\mathbf{K}(x, y)$. Moreover, we have

$$G_n(x) = C_1(n)\alpha_1^n + \ldots + C_p(n)\alpha_p^n,$$
$$G_n(y) = D_1(n)\beta_1^n + \ldots + D_p(n)\beta_p^n,$$

where α_i are the zeros of $\mathcal{G}(x, T)$ and β_j are the zeros of $\mathcal{G}(y, T)$, respectively. Obviously, the field $L_0 := \mathbf{K}(x, \alpha_1, \ldots, \alpha_p)$ and $L_1 := \mathbf{K}(y, \beta_1, \ldots, \beta_p)$ are isomorphic over $\mathbf{K}$ and we denote the isomorphism (which sends $x \mapsto y$ and $\alpha_i \mapsto \beta_i$) by $\psi : L_0 \to L_1$. We have the following situation:[1]

$= 4\mathbf{K}(x, y, \alpha_1, \ldots, \alpha_p, \beta_1, \ldots, \beta_p)\psi : \mathbf{K}(x, \alpha_1, \ldots, \alpha_p)^{\cong}\mathbf{K}(y, \beta_1, \ldots, \beta_p)\mathbf{K}(x, y)\mathbf{K}(x)\mathbf{K}(y)(0, 0)(1, 1)($

From Theorem 1 we know that there are polynomials $S_1(X), \ldots, S_p(X)$ and a permutation π of $\{1, \ldots, p\}$ such that $C_i(n_0 + rX) = \eta\alpha_i^{-n_0}P(X)S_i(X)$, $D_{\pi(i)}(m_0 + sX) = \beta_{\pi(i)}^{-m_0}Q(X)S_i(X)$ and $\alpha_i^r/\beta_{\pi(i)}^s \in \mathbf{K}$ for $i = 1, \ldots, p$. Since by the above isomorphism ψ, we have that α_i and β_i have the same multiplicity and therefore we have $\deg C_i = \deg D_i$ for all $i = 1, \ldots, p$, it follows that

$$\deg S_{\pi(i)} = \deg S_i + \deg Q - \deg P$$

for all $i = 1, \ldots, p$. This implies

$$\deg S_{\pi^k(i)} = \deg S_i + k(\deg Q - \deg P)$$

for every $k \in \mathbb{N}$, where π^k denotes as usual the k-th iterate of the map π. Let ℓ be the order of π. Then, we get $\deg S_i = \deg S_i + \ell(\deg Q - \deg P)$ and therefore $\deg Q = \deg P$. This means that α_i and $\beta_{\pi(i)}$ have the same multiplicity as roots of the characteristic polynomial $\mathcal{G}(x, T)$ and $\mathcal{G}(y, T)$, respectively.

The proof of Theorem 2 now follows easily from what we have proved up to now. Namely, by assuming that our equation has infinitely many solutions we have that the characteristic roots of $G_n(x)$ and $G_n(y)$ satisfy

$$\alpha_i^r = c\beta_{\pi(i)}^s,$$

where π is a permutation of the set $\{1, \ldots, p\}$ and $c \in \mathbf{K}^*$ (here c may depend on i). Moreover, the multiplicities of α_i and $\beta_{\pi(i)}$ are the same. By

[1] The diagram was typsetted with kuvio.tex, which we kindly acknowledge.

multiplying all these relations according the multiplicities, we therefore get

$$\begin{aligned} A_0(x)^r &= \prod_{i=1}^{p}\prod_{j=1}^{\deg C_i+1}\alpha_i^r = \prod_{i=1}^{p}\prod_{j=1}^{\deg C_i+1} c\beta_{\pi(i)}^s \\ &= \tilde{c}\left(\prod_{i=1}^{p}\prod_{j=1}^{\deg D_{\pi(i)}}\beta_{\pi(i)}\right)^s = \tilde{c}A_0(y)^s, \end{aligned}$$

where A_0 is the constant polynomial in the linear recurring equation. But now, condition (ii) of our assumptions excludes that this equation can hold. Therefore, we obtain a contradiction, which shows the finiteness of the number of solutions in this case. □

References

1. Yu. Bilu and R. F. Tichy, *The Diophantine equation $f(x) = g(y)$*, Acta Arith. **95** (2000), 261–288.
2. P. Corvaja and U. Zannier, *Finiteness of integral values for the ratio of two linear recurrences*, Invent. Math. **149** (2002), 431–451.
3. J.H. Evertse and K. Győry, *On the number of solutions of weighted unit equations*, Compositio Math. **66** (1988), 329–354.
4. J.H. Evertse, K. Győry, C. L. Stewart and R. Tijdeman, *S-unit equations and their applications.* In: New advances in transcendence theory (ed. by A. Baker), 110–174, Cambridge Univ. Press, Cambridge, 1988.
5. J.H. Evertse, H.P. Schlickewei and W. M. Schmidt, *Linear equations in variables which lie in a multiplicative group*, Ann. Math. **155** (2002), 1–30.
6. C. Fuchs, *On the equation $G_n(x) = G_m(P(x))$ for third order linear recurring sequences*, Port. Math. (N.S.) **61** (2004), 1–24.
7. C. Fuchs, A. Pethő and R. F. Tichy, *On the Diophantine equation $G_n(x) = G_m(P(x))$*, Monatsh. Math. **137** (2002), 173–196.
8. C. Fuchs, A. Pethő and R. F. Tichy, *On the Diophantine equation $G_n(x) = G_m(P(x))$: Higher-order recurrences*, Trans. Amer. Math. Soc. **355** (2003), 4657-4681.
9. A. Schinzel, *Polynomials with special regard to reducibility*, Cambridge University Press, Cambridge - New York, 2000.
10. W. M. Schmidt, *The zero multiplicity of linear recurrence sequences*, Acta Math. **182** (1999), 243–282.
11. W. M. Schmidt, *Zeros of linear recurrence sequences*, Publ. Math. Debrecen **56** (2000), 609–630.
12. T. N. Shorey and R. Tijdeman, *Exponential Diophantine Equations*, Cambridge, Univ. Press, 1986.
13. H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer Verlag, Berlin, 1993.
14. U. Zannier, *On the integer solutions of exponential equations in function fields*, Preprint.