Clemens Fuchs
Karl-Morre Str. 46/15
8020 Graz

Quantitative Finiteness Results for Diophantine Equations

Dissertation[‡]

Ausgeführt zum Zwecke der Erlangung
des akademischen Grades eines
Doktors der Technischen Wissenschaften

Betreuer:
O.Univ.-Prof. Dr. Robert F. Tichy

Eingereicht an der
Technischen Universität Graz
Technisch-Naturwissenschaftliche Fakultät

Graz, am 15.01.2002

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

Preface

The study of Diophantine equations, in general terms, is the study of solvability of equations in integers. Although researches in this field have their roots in antiquity and a history of the subject amounts more or less, to a history of mathematics itself, it is only in relatively recent times that there have emerged any general theories, and we shall begin in 1900 by referring to Hilbert's famous list of problems.

The tenth of these asked for a universal algorithm for deciding whether or not a given Diophantine equation, that is, an equation $f(x_1, \ldots, x_n) = 0$, where f denotes a polynomial with integer coefficients is solvable in integers $x_1, \ldots, x_n$. Though Hilbert posed his question in terms of solvability, there are, of course, many other sorts of information that one might like to have; for instance, one might enquire as to whether a particular equation has infinitely many solutions, or one might seek some bounds on the number of solutions. In 1970, Matijasevic, proved that a general algorithm of the type sought by Hilbert does not in fact exist.

The first major advance towards a coherent theory was made by Thue in 1909 when he proved that the equation $F(x, y) = m$, where F denotes an irreducible binary form with integer coefficients and degree at least 3, possesses only a finite number of solutions in integers x, y.

In the midth of the 20th century two main branches have their origins. The first one started 1955 with Roth's Theorem, for which Roth received the Fields medal. This theorem was generalized and quantified between 1965 and 1972 by W. M. Schmidt and then by many other authors; a development that had its climax in the various quantified versions of Schmidt's Subspace Theorem. We are going to use these theorems frequently, especially they will enable us to calculate explicit upper bounds for the number of solutions of certain classes of Diophantine equations. Thereby, a remarkable feature is that these bounds will depend on very few parameters.

The second development has its roots in about the same time. In 1968, A. Baker derived lower bounds for the absolute value of linear forms of logarithms in algebraic numbers. This was a breakthrough in the field of effective methods which made it possible to compute upper bounds for the solutions themselves. For example Baker himself gave upper bounds for the solutions of the Thue equation.

In the first chapter, we will survey these main developments (this is mainly due to R. Tijdeman and can be found in [36, Chapter II]). Furthermore, we will collect some very important general methods to quantify the number of solutions of Diophantine equations. The first subsection will be about W. M. Schmidt's celebrated Subspace Theorem. In the second subsection, we will give applications of the Subspace Theorem to S-unit equations and then in turn to the zero-multiplicity of nondegenerate linear recurring sequences. In the third subsection, we will introduce Baker's method on linear forms of logarithms in algebraic numbers and in the fourth subsection, we state the analog of Baker's method in algebraic function fields of one variable which is referred to as Mason's inequality. Here we also collect applications to S-unit equations and to hyperelliptic equations in function fields.

The second chapter is devoted to the number of perfect powers in a linear recurring sequences. We will consider the Diophantine equation

$$G_n = Ex^q,$$

where $(G_n)_{n=0}^{\infty}$ is a linear recurring sequence, E is a nonzero and q a positive integer. In the introductory section, we survey some known results concerning this type of equation, in the second subsection we present our results, in the third subsection, we collect some useful lemmas and in the last subsection we present the proofs of the theorems. This chapter is identical with a joint paper with R. F. Tichy [51].

The third chapter is a generalization and continuation of the quantitative work done in the previous chapter. Now, we will consider the equation

$$f(G_n, x) = 0,$$

where f is polynomial in two variables that is monic in x and $(G_n)_{n=0}^{\infty}$ is again a linear recurring sequence. We will present quantitative finiteness results for this Diophantine equation in subsection two and prove them in the following subsections.

In the fourth chapter, we turn to finiteness results concerning the equation

$$G_n(x) = G_m(P(x))$$

where $(G_n(x))_{n=0}^{\infty}$ is a sequence of polynomials satisfying a second order linear recurring sequence and $P(x)$ is a fixed polynomials with $\deg P \geq 1$, i.e. we consider identities of polynomials. Under certain conditions, we will quantify the number of solutions

$(n, m) \in \mathbb{Z}^2$ of this equation. After a introductory section, we will present the new theorems and then, we will prove them in the following subsections. This chapter is identically equal to a joint paper with R. F. Tichy and A. Pethő [49].

The fourth chapter is a continuation of the previous chapter on the equation

$$G_n(x) = G_m(P(x))$$

where now $(G_n(x))_{n=0}^{\infty}$ denotes a sequence of polynomials satisfying a third order linear recurring sequence. Because of Cardano's formulae, it is possible to use the ideas from the second order case and to derive quantitative finiteness results in this case too. This chapter is equal to a manuscript which is joint work with R. F. Tichy and A. Pethő [50].

The last two chapters are about Diophantine m-tuples. Thereby, we will call a set $\{a_1, \ldots, a_m\}$ of positive integers a Diophantine m-tuple with property $D(n)$ for $n \in \mathbb{Z}$ if the product of any two of them increased by n is a perfect square, i.e. a square of a positive integer. Here, we will not study the classical case but analogues problems for polynomials (which was already studied e.g. by Jones in [55], [56]). In chapter five, we prove that there does not exist a set of four polynomials with integer coefficients such that the product of two of them minus one is a square of a polynomials with integer coefficients. This chapter is equal to a joint paper with A. Dujella [33].

In the last chapter, we will consider the case where n is a linear polynomial. We will show that there are at most 26 polynomials with integer coefficients such that the product of two of them plus a linear polynomial is a square of a polynomial with integer coefficients. This chapter is equal to a manuscript which is joint work with A. Dujella and R. F. Tichy [34].

Last but not least, I want to express my gratitude to Prof. Robert F. Tichy, who is the advisor of this thesis and who is coauthor of many of the papers forming the main part of this work. Moreover, I want to thank the other coauthors of the papers involved, namely Prof. Andrej Dujella from Zagreb, Croatia and Prof. Attila Pethő from Debrecen, Hungary. I am most thankful to them for valuable suggestions and fruitful discussions. For financial support, I am indebted to the Austrian Science Foundation (FWF - "Fond zur Förderung der wissenschaftlichen Forschung"), grant S8307-MAT. Finally, I am grateful to my family, especially to my father, for permanent encouragement and support.

Graz, January 2002 CLEMENS FUCHS

Contents

Chapter 1

General methods for quantitative finiteness results

1.1 The Subspace Theorem

In 1844, Liouville proved that transcendental numbers do exist. He derived this result from the following approximation theorem.

Theorem 1.1. (Liouville) *Suppose α is a real algebraic number of degree d. Then there is a constant $c(\alpha) > 0$ such that*

$$\left|\alpha - \frac{p}{q}\right| > c(\alpha)q^{-d}$$

for every rational number p/q, $q > 0$ distinct from α.

Using this result, Liouville deduced that numbers like $\sum_{\nu=1}^{\infty} 2^{-\nu!}$ are transcendental. Furthermore, Liouville's Theorem implies that the inequality

$$\left|\alpha - \frac{p}{q}\right| < q^{-\mu} \tag{1.1}$$

has only finitely many rational solutions p/q if $\mu > d$. Thue showed in 1909 that (1.1) has only finitely many solutions if $\mu > d/2+1$. Then, Siegel (1921) showed in his thesis that this is already true if $\mu > 2\sqrt{d}$. A slight improvement to $\mu > \sqrt{2d}$ was made by Dyson in 1947. Finally, Roth proved in 1955 that (1.1) has only finitely many solutions if $\mu > 2$. He received the Fields medal for this achievement. So, for $d \geq 2$ this theorem, together with Lagrange's Theorem from 1770 which says that every irrational real α admits infinitely many rational p/q such that

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2},$$

shows that the number 2 as exponent is best possible. For $d = 2$ Liouville's Theorem is stronger than Roth's one.

In a series of papers published between 1965 and 1972, W.M. Schmidt made an important step forward. One of his results is the following extension of Roth's Theorem.

Theorem 1.2. (W. M. Schmidt) *Suppose α is a real algebraic number. Let $k \geq 1$ and $\delta > 0$. Then there are only finitely many algebraic number β of degree $\leq k$ with*

$$|\alpha - \beta| < H(\beta)^{-(k+1+\delta)}$$

where $H(\beta)$ denotes the classical absolute height.

This result follows by applying the so-called Subspace Theorem which, in its simplest form, reads as follows. For $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{Z}^n$ put

$$|\mathbf{x}| = \sqrt{x_1^2 + \cdots + x_n^2}.$$

Then we have

Theorem 1.3. (Subspace Theorem, W. M. Schmidt) *Suppose $L_1(\mathbf{x}), \ldots, L_n(\mathbf{x})$ are linearly independent linear forms in $\mathbf{x} = (x_1, \ldots, x_n)$ with algebraic coefficients. Given $\delta > 0$, there are finitely many proper linear subspaces $T_1, \ldots, T_w$ of $\mathbb{R}^n$ such that every integer point $\mathbf{x} \neq \mathbf{0}$ with*

$$|L_1(\mathbf{x}) \cdots L_n(\mathbf{x})| < |\mathbf{x}|^{-\delta}$$

lies in one of these subspaces.

In fact, Roth's Theorem is equivalent to $n = 2$ of the above stated theorem.

Up to now, apart from Liouville's Theorem, all results stated in this section are ineffective, that is, the method of proof does not enable us to determine the finitely many exceptions. However, the method makes it possible to derive upper bounds for the number of exceptions. This was proved by Schmidt in 1989 (see [79]).

Theorem 1.4. (Quantitative Subspace Theorem, W. M. Schmidt) *Let $L_1, \ldots, L_n$ be linearly independent linear forms with coefficients in some algebraic number field of degree d. Consider the inequality*

$$|L_1(\mathbf{x}) \cdots L_n(\mathbf{x})| < |\det(L_1, \ldots, L_n)||\mathbf{x}|^{-\delta} \text{ where } 0 < \delta < 1. \tag{1.2}$$

The set of solutions of (1.2) with

$$\mathbf{x} \in \mathbb{Z}^n, \quad |\mathbf{x}| \gg \max\{(n!)^{8/\delta}, H(L_1), \ldots, H(L_n)\}$$

is contained in the union of at most $[(2d)^{2^{26n}\delta^{-2}}]$ proper linear subspaces of $\mathbb{R}^n$.

A second result in this direction is due to Vojta [93]. Essentially this result says that, apart from finitely many exceptions which may depend on δ, the solutions of (1.2) are in the union of finitely many, at least in principle effectively computable, proper linear subspaces of $\mathbb{R}^n$ which are independent of δ.

In 1977, Schlickewei extended Schmidt's Subspace Theorem of 1972 to the p-adic case and to number fields. In 1990 (see [75]), he generalized Schmidt's quantitative Subspace Theorem to the p-adic case over $\mathbb{Q}$ and later 1992 to number fields (cf. [76]). We shall see that these results posses many important applications. Vojta proved the p-adic assertion of the above mentioned result himself.

Evertse [40] derived in 1996 an improved version of Schlickewei's and Schmidt's quantitative Subspace Theorem. Below we state this result of Evertse and to this end we introduce suitably normalized absolute values and heights.

Let K be an algebraic number field. Denote its ring of integers by O_K and its collection of places by M_K. For $v \in M_K$, $x \in K$, we define the absolute value $|x|_v$ by
(i) $|x|_v = |\sigma(x)|^{1/[K:\mathbb{Q}]}$ if v corresponds to the embedding $\sigma : K \hookrightarrow \mathbb{R}$;
(ii) $|x|_v = |\sigma(x)|^{2/[K:\mathbb{Q}]} = |\overline{\sigma}(x)|^{2/[K:\mathbb{Q}]}$ if v corresponds to the pair of conjugate complex embedding $\sigma, \overline{\sigma} : K \hookrightarrow \mathbb{C}$;
(iii) $|x|_v = (N\wp)^{-\mathrm{ord}_\wp(x)/[K:\mathbb{Q}]}$ if v corresponds to the prime ideal $\wp$ of O_K.
Here $N\wp = \#(O_K/\wp)$ is the norm of $\wp$ and $\mathrm{ord}_\wp(x)$ the exponent of $\wp$ in the prime ideal composition of (x) with $\mathrm{ord}_\wp(0) := \infty$. In case (i) or (ii) we call v real infinite or complex infinite, respectively; in case (iii), we call v finite. These absolute values satisfy the *Product formula*

$$\prod_{v \in M_K} |x|_v = 1 \quad \text{for } x \in K^*. \tag{1.3}$$

The *height* of $\mathbf{x} = (x_1, \dots, x_n) \in K^n$ with $\mathbf{x} \neq \mathbf{0}$ is defined as follows: for $v \in M_K$ put

$$\begin{aligned} |\mathbf{x}|_v &= \left(\textstyle\sum_{i=1}^n |x_i|_v^{2[K:\mathbb{Q}]}\right)^{1/(2[K:\mathbb{Q}])} && \text{if}\, v \,\text{is real infinite,} \\ |\mathbf{x}|_v &= \left(\textstyle\sum_{i=1}^n |x_i|_v^{[K:\mathbb{Q}]}\right)^{1/[K:\mathbb{Q}]} && \text{if}\, v \,\text{is complex infinite,} \\ |\mathbf{x}|_v &= \max(|x_1|_v, \dots, |x_n|_v) && \text{if}\, v \,\text{is finite} \end{aligned}$$

(note that for infinite places v, $|\cdot|_v$ is a power of the Euclidean norm). Now define

$$\mathcal{H}(\mathbf{x}) = \mathcal{H}(x_1, \dots, x_n) = \prod_v |\mathbf{x}|_v.$$

For a linear form $l(\mathbf{X}) = a_1X_1 + \cdots + a_nX_n$ with algebraic coefficients we define $\mathcal{H}(l) := \mathcal{H}(\mathbf{a})$, where $\mathbf{a} = (a_1, \dots, a_n)$ and if $\mathbf{a} \in K^n$ then, we put $|l|_v = |\mathbf{a}|_v$ for

$v \in M_K$. Furthermore, we define the number field $K(l) := K(a_1/a_j, \dots, a_n/a_j)$ for any j with $a_j \neq 0$; this is independent of the choice of j.

We are now ready to state Evertse's result [40]. The following notation is used:

- S is a finite set of places on K of cardinality s containing all infinite places;
- $\{l_{1v}, \dots, l_{nv}\}$, $v \in S$ are linearly independent sets of linear forms in n variables with algebraic coefficients such that

$$\mathcal{H}(l_{iv}) \le H, \quad [K(l_{iv}) : K] \le D \quad \text{for } v \in S,\ i = 1, \dots, n.$$

We choose for every place $v \in M_K$ a continuation of $|\cdot|_v$ to the algebraic closure of K and denote it by $|\cdot|_v$, too.

Theorem 1.5. (Quantitative Subspace Theorem, Evertse) *Let* $0 < \delta < 1$ *and consider the inequality for* $\mathbf{x} \in K^n$

$$\prod_{v \in S} \prod_{i=1}^{n} \frac{|l_{iv}(\mathbf{x})|_v}{|\mathbf{x}|_v} < \left(\prod_{v \in S} |\det(l_{1v}, \dots, l_{nv})|_v \right) \cdot \mathcal{H}(\mathbf{x})^{-n-\delta}. \tag{1.4}$$

Then the following assertions hold:
(i) There are proper linear subspaces $T_1, \dots, T_{t_1}$ *of* K^n*, with*

$$t_1 \le (2^{60n^2} \cdot \delta^{-7n})^s \log 4D \cdot \log\log 4D$$

such that every solution $\mathbf{x} \in K^n$ *of (1.4) satisfying* $\mathcal{H}(\mathbf{x}) \ge H$ *belongs to* $T_1 \cup \dots \cup T_{t_1}$.
(ii) There are proper linear subspaces $S_1, \dots, S_{t_2}$ *of* K^n*, with*

$$t_2 \le (150 n^4 \cdot \delta^{-1})^{ns+1} (2 + \log\log 2H)$$

such that every solution $\mathbf{x} \in K^n$ *of (1.4) satisfying* $\mathcal{H}(\mathbf{x}) < H$ *belongs to* $S_1 \cup \dots \cup S_{t_2}$.

Very recently (unpublished yet) Evertse and Schlickewei were able to extend the arguments in order to handle arbitrary vectors in $\overline{\mathbb{Q}}^n$ instead of just vectors in K^n for some fixed number field K. So, they derived a result which is much more general than the classical Subspace Theorem, in fact, it is an "absolute" generalization of the Subspace Theorem, dealing with vectors $\mathbf{x}$ in $\overline{\mathbb{Q}}^n$ rather than in K^n. The theorem is as follows and can be found in [44].

Let E be a number field. Let S be a finite subset of M_E of cardinality s and suppose that for each $v \in S$ we have linearly independent linear forms $l_{1v}, \dots, l_{nv}$ with coefficients in $\overline{\mathbb{Q}}$. We suppose that for $i = 1, \dots, n$ and for $v \in S$

$$[E(l_{iv}) : E] \le D,$$

and moreover that

$$H(l_{iv}) \leq H, \quad v \in S,\ i = 1, \ldots, n.$$

Each normalized absolute value $|\cdot|_v$ on E has a unique extension $|\cdot|'_v$, say, to $\overline{E}_v$, the algebraic closure of the completion E_v. Fix an embedding τ_v of $\overline{\mathbb{Q}}$ over E into $\overline{E}_v$. Then, we extend $|\cdot|_v$ from E to $\overline{\mathbb{Q}}$ by putting

$$|x|_v = |\tau_v(x)|'_v \quad \text{for} \quad x \in \overline{\mathbb{Q}}.$$

Using this notation, we obtain

Theorem 1.6. (Absolute Subspace Theorem, Evertse and Schlickewei) *Let E, S and the linear forms $l_{1v}, \ldots, l_{nv}$ in $\mathbf{X} = (X_1, \ldots, X_n)$ be as above. Let $0 < \delta < 1$. Then there exist proper linear subspaces $T_1, \ldots, T_{t_2}$ of $\overline{\mathbb{Q}}^n$, all defined over E, where*

$$t_2 = t_2(n, s, D, \delta) \leq (3n)^{2ns} 2^{3(n+9)^2} \delta^{-ns-n-4} \log(4D) \log\log(4D)$$

with the following property. The set of solutions $\mathbf{x} \in \overline{\mathbb{Q}}^n$ of the inequalities

$$\prod_{v \in S} \prod_{i=1}^{n} \max_{\sigma \in Gal(\overline{\mathbb{Q}}/E)} \frac{|l_{iv}(\sigma(\mathbf{x}))|_v}{|\sigma(\mathbf{x})|_v} \leq \left(\prod_{v \in S} |\det(l_{1v}, \ldots, l_{nv})|_v \right) \cdot \mathcal{H}(\mathbf{x})^{-n-\delta}$$

and

$$\mathcal{H}(\mathbf{x}) > \max\{n^{4n/\delta}, H\} \tag{1.5}$$

is contained in the union

$$T_1 \cup \ldots \cup T_{t_2}.$$

Observe that Evertse's result stated before is a special case with the restriction that the solutions $\mathbf{x}$ lie in E^n. Furthermore, the bound obtained in the absolute Subspace Theorem is better than the bound in Evertse's quantitative Subspace Theorem. However, Evertse has only to assume $\mathcal{H}(\mathbf{x}) \geq H$ instead of (1.5).

1.2 S-unit equations

In this section, we will deal with the most important application of the Subspace Theorem. Therefore, let $\mathbf{K}$ be an algebraically closed field of characteristic 0, $n \geq 1$ an integer, $\alpha_1, \ldots, \alpha_n$ elements of $\mathbf{K}^*$, and Γ a finitely generated multiplicative subgroup of $\mathbf{K}^*$. A solution $(x_1, \ldots, x_n)$ of the so called *weighted unit equation*

$$\alpha_1 x_1 + \cdots + \alpha_n x_n = 1 \text{ in } x_1, \ldots, x_n \in \Gamma \tag{1.6}$$

is called *nondegenerate* if

$$\sum_{j \in J} \alpha_j x_j \neq 0 \text{ for each non-empty subset } J \text{ of } \{1, \ldots, n\} \tag{1.7}$$

and *degenerate* otherwise. It is clear that if Γ is infinite and if (1.6) has a degenerate solution then (1.6) has infinitely many degenerate solutions. For nondegenerate solutions, we have the following result which is due to Evertse, Schlickewei and Schmidt [45].

Theorem 1.7. (Evertse, Schlickewei and Schmidt) *Let* $\mathbf{K}$ *be a field of characteristic* 0*, let* $\alpha_1, \ldots, \alpha_n$ *be nonzero elements of* $\mathbf{K}$ *and let* Γ *be a multiplicative subgroup of* $(\mathbf{K}^*)^n$ *of rank* r*. Then the equation*

$$\alpha_1 x_1 + \ldots + \alpha_n x_n = 1$$

has at most

$$\exp((6n)^{3n}(r+1))$$

nondegenerate solutions $(x_1, \ldots, x_n) \in \Gamma$.

This theorem is the Main Theorem on S-unit equations over fields with characteristic 0. It is a generalization of earlier results due to Evertse and Győry [41], Evertse [38], and van der Poorten and Schlickewei [72] on the finiteness of the number of nondegenerate solutions of (1.6). For a general survey on these equations and their applications, we refer to Evertse, Győry, Stewart and Tijdeman [42].

The above theorems can be applied to the following important Diophantine equation which will be needed later. Let $U = (u_m)_{m \in \mathbb{Z}}$ be a sequence of complex numbers satisfying a recurrence relation of order q,

$$u_m = c_1 u_{m-1} + \ldots + c_q u_{m-q}$$

with $c_1, \ldots, c_q \in \mathbb{C},\ c_q \neq 0$. As it is well-known, we have

$$u_m = \sum_{i=1}^{n} g_i(m) \alpha_i^m \quad \text{for } m \in \mathbb{Z},$$

where $\alpha_1, \ldots, \alpha_n$ are distinct, nonzero complex numbers and $g_1, \ldots, g_n \in \mathbb{C}[T]$ polynomials with

$$\prod_{i=1}^{n} (T - \alpha_i)^{\deg g_i + 1} = T^q - c_1 T^{q-1} - \ldots - c_q.$$

Denote by $N_U(a)$ the number of integers m with

$$u_m = a.$$

The sequence U is called *nondegenerate* if no quotient α_i/α_j $(1 \leq i < j \leq n)$ is equal to a root of unity. From the Theorem of Skolem-Mahler-Lech (cf. [60]) it follows that then $N_U(a)$ is finite for every $a \in \mathbb{C}$. Using this, Schlickwei [77] showed that if U is nondegenerate, $\alpha_1, \ldots, \alpha_n$ are not roots of unity too, and $\alpha_1, \ldots, \alpha_n$ and the coefficients of $g_1, \ldots, g_n$ generate an algebraic number field K of degree d then for every $a \in K$, we have

$$N_U(a) \leq d^{6q^2} 2^{2^{28q!}}.$$

If we assume that $g_1, \ldots, g_n$ are all constant, we obtain the following improvement by applying Theorem 1.7 to the group generated by $\alpha_1, \ldots, \alpha_n$ which has at most rank n.

Theorem 1.8. *Let U be a recurrence sequence satisfying*

$$u_m = g_1\alpha_1^m + \ldots + g_n\alpha_n^m \quad \textit{for} \quad m \in \mathbb{Z},$$

where $\alpha_1, \ldots, \alpha_n$ are nonzero complex numbers such that neither $\alpha_1, \ldots, \alpha_n$ nor any of the quotients α_i/α_j $(1 \leq i < j \leq n)$ are roots of unities and where $g_1, \ldots, g_n$ are nonzero complex numbers. Then for every $a \in \mathbb{C}$, we have

$$N_U(a) \leq \exp((n+2) \cdot (6n)^{3n}).$$

Very recently, Schmidt [82] obtained the following remarkable result concerning the zero multiplicity of an arbitrary nondegenerate complex recurring sequences (i.e., with arbitrary polynomials $g_1, \ldots, g_n$).

Theorem 1.9. (W. M. Schmidt) *Suppose that $(G_n)_{n\in\mathbb{Z}}$ is a nondegenerate linear recurring sequence of complex numbers, whose characteristic polynomial has k distinct roots of multiplicity $\leq a$. Then the number of solutions $n \in \mathbb{Z}$ of the equation*

$$G_n = 0,$$

can be bounded from above by

$$c(k,a) = e^{(7k^a)^{8k^a}}.$$

(This number of solutions is called the zero multiplicity of the recurrence.)

In recent work [22], [23], David and Philippon have proved a slight sharpening of the above results. The bound in Theorem 1.7 can be improved to

$$\exp(\exp(c_1 n)(r+1)).$$

Therefore, also the bound in Theorem 1.8 can be improved to

$$\exp(\exp(c_1 n)).$$

Here c_1 is an absolute constant.

1.3 Baker's Method

Liouville's Theorem was also the starting point of a development of effective methods, too. Hermite, in 1873 and Lindemann in 1882 established the transcendence of the numbers e and π, respectively. The Theorem of Lindemann-Weierstrass (1885) says that $\beta_1 e^{\alpha_1} + \cdots + \beta_n e^{\alpha_n} \neq 0$ for any distinct algebraic numbers $\alpha_1, \ldots, \alpha_n$ and any nonzero algebraic numbers $\beta_1, \ldots, \beta_n$.

A new development started in 1929 when Gelfond showed the transcendence of $2^{\sqrt{2}}$. In 1934, Gelfond and Schneider, independently of each other, proved the transcendence of α^β for α, β algebraic, $\alpha \neq 0, 1$ and β irrational. Alternatively, this result says that for any nonzero algebraic numbers $\alpha_1, \alpha_2, \beta_1, \beta_2$ with $\log \alpha_1, \log \alpha_2$ linearly independent over the rationals, we have

$$\beta_1 \log \alpha_1 + \beta_2 \log \alpha_2 \neq 0.$$

In 1966, Baker proved the transcendence of $e^{\beta_0} \alpha_1^{\beta_1} \cdots \alpha_n^{\beta_n}$ for algebraic numbers $\alpha_1, \ldots,$ α_n, different from 0 or 1, and $\beta_1, \ldots, \beta_n$ with either $\beta_0 \neq 0$ or $1, \beta_1, \ldots, \beta_n$ linearly independent over the rationals. This follows from the following result.

Theorem 1.10. (A. Baker) *Let $\alpha_1, \ldots, \alpha_n$ be nonzero algebraic numbers such that their logarithms $\log \alpha_1, \ldots, \log \alpha_n$ are linearly independent over the field of all rational numbers. Then $1, \log \alpha_1, \ldots, \log \alpha_n$ are linearly independent over the field of all algebraic numbers.*

The above results have p-adic analogues and also analogues in the theory of elliptic functions.

The effective character of the above result can be expressed in form of the transcendence measures. Between 1972 and 1977, Baker [4] derived the following important estimate.

Theorem 1.11. (A. Baker) *Let $\alpha_1, \ldots, \alpha_n$ be nonzero algebraic numbers with degrees at most d and (classical absolute) heights at most $A_1, \ldots, A_n$ (all ≥ 2), respectively. Let $b_1, \ldots, b_n$ be rational integers of absolute values at most B (≥ 2). Put $\Lambda = b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n$. Then either $\Lambda = 0$ or*

$$\log |\Lambda| > -(16nd)^{200n} \left(\prod_{j=1}^{n} \log A_j \right) \log \left(\prod_{j=1}^{n-1} \log A_j \right) \log B.$$

Later on, the constants have been improved and the $\log(\prod \log)$ factor has been removed. The best bound known at present is due to Baker and Wüstholz [7] in the classical case and due to Waldschmidt and his colleagues, in the p-adic case.

Later, we will need the following special form of the above theorem of A. Baker [2]. Therefore, let us start by recalling the definition of the absolute logarithmic Weil height: for an algebraic number β let $P_\beta(x) = x^k + a_{k-1}x^{k-1} + \cdots + a_0 \in \mathbb{Z}[x]$ denote the minimal polynomial of β. Furthermore, let $\beta_1 = \beta, \beta_2, \ldots, \beta_k$ denote the conjugates of β. Then we call

$$h(\beta) = \frac{1}{k} \log \left(\prod_{i=1}^{k} \max\{1, |\beta_i|\} \right)$$

the *absolute logarithmic Weil height* of β.

Theorem 1.12. (A. Baker) *Let $\alpha_1, \ldots, \alpha_k$ be algebraic numbers, different from* 0 *or* 1, *$K = \mathbb{Q}(\alpha_1, \ldots, \alpha_k)$ and let d be the degree of $[K : \mathbb{Q}]$. For $i = 1, \ldots, k$ set*

$$h_i = \max\left\{ h(\alpha_i), \frac{e\,|\log \alpha_i|}{d}, \frac{1}{d} \right\}.$$

Let $b_1, \ldots, b_k \in \mathbb{Z}$, $b_k > 0$, $\Lambda = b_1 \log \alpha_1 + \cdots + b_k \log \alpha_k \neq 0$ and $B = \max\{2, |b_1|, \ldots, |b_{k-1}|\}$. Then we have

$$\log|\Lambda| > -C(k) d^{k+2} h_1 \cdots h_k \log\left(C(k) d^{k+2} h_1 \cdots h_{k-1}\right) \log b_k - \frac{B}{b_k}, \tag{1.8}$$

where

$$C(k) = 2^{26k} k^{3k}.$$

A proof of this theorem with the given explicit constants can be found in the monograph of Waldschmidt [95], page 309, Corollary 9.24.

Baker's estimates from 1967 on linear forms of logarithms in algebraic numbers caused a breakthrough in computing upper bounds for the solutions of Diophantine equations themselves. Baker himself gave upper bounds for the solutions of the Thue equation [3] and the super-elliptic equation [1]

$$y^m = P(x)$$

where $m \geq 2$ is a fixed given positive integer and $P(x) \in \mathbb{Z}[x]$ is a polynomial with at least three simple roots if $m = 2$ and at least two simple roots if $m \geq 3$. Later, this conditions were weakened.

Later, Baker's sharpening made it possible to deal with Diophantine equations which cannot be treated by the mentioned ineffective methods. E.g. Schinzel and Tijdeman showed that the hyperelliptic equation with m, x, y variable and $P(x) \in \mathbb{Z}[x]$ a given polynomial with at least two distinct roots implies that m is bounded. Tijdeman also showed that the Catalan equation $x^m - y^n = 1$ in integers m, n, x, y all > 1 implies that x^m is bounded by some effectively computable number [92]. The bounds obtained in equations involving a power with both base and exponent variable are, however, so large that it is not yet possible to solve such equations in practice.

The best bounds for linear forms known at present make it, however, possible to solve for example the Thue equation completely. Additional algorithms are needed to achieve this (cf. e.g. [11]).

1.4 Mason's inequality and applications

In this section, we want to study analogues of the previous results for function fields in one variable. Therefore, let $\mathbf{K}$ be an algebraically closed field with characteristic 0. Corresponding to the integers there is the polynomial ring $\mathbf{K}[x]$ and the object of concern is the set of solutions in $\mathbf{K}[x]$. The results in fact refer to a more general situation; actually, we shall deal with the solutions integral over $\mathbf{K}[x]$ in an arbitrary finite extension L rather than to consider just those in $\mathbf{K}[x]$ itself.

Let us begin by recalling the definitions of discrete valuations on the field $\mathbf{K}(x)$ where x is transcendental over $\mathbf{K}$. For $\xi \in \mathbf{K}$ define the valuation ν_ξ such that for $Q \in \mathbf{K}(x)$ we have $Q(x) = (x-\xi)^{\nu_\xi(Q)}A(x)/B(x)$ where A, B are polynomials with $A(\xi)B(\xi) \neq 0$. Furthermore, for $Q = A/B$ with $A, B \in \mathbf{K}[x]$ we put $\deg Q := \deg A - \deg B$; thus $\nu_\infty := -\deg$ is a discrete valuation on $\mathbf{K}(x)$. These are all discrete valuations on $\mathbf{K}(x)$. Now let L be a finite extension of $\mathbf{K}(x)$. Such an L is called a function field in one variable with constant field $\mathbf{K}$. Each of the valuations ν_ξ, ν_∞ can be extended in at most $[L : \mathbf{K}(x)] =: d$ ways to a discrete valuation on L and in this way one obtains all discrete valuations on L. A valuation on L is called finite if it extends ν_ξ for some $\xi \in \mathbf{K}$ and infinite if it extends ν_∞.

We need the following generalization of the degree from $\mathbf{K}[x]$ to L. Define the *height* of $f \in L$ by

$$\mathcal{H}(f) = -\sum_{\nu} \min\{0, \nu(f)\}$$

where the sum is taken over all discrete valuations on L; thus for $f \in \mathbf{K}(x)$ the height $\mathcal{H}(f)$ is just the number of poles of f, counted according to multiplicity. We note that if f lies in $\mathbf{K}[x]$ then $\mathcal{H}(f) = d \deg f$. We also want to define the height of a polynomial with coefficients in L. In order to do this, let us denote for any finite set S of elements of L

$$\nu(S) = \min_{s \in S}\{\mathcal{H}(s)\} \quad \text{and} \quad \mathcal{H}(S) = -\sum_{\nu} \min\{0, \nu(S)\}$$

where the sum again runs over all valuations in L. If $P \in L[T]$ and S is the set of its coefficients, then the quantities $\nu(P)$ and $\mathcal{H}(P)$ are defined to be $\nu(S)$ and $\mathcal{H}(S)$

respectively.

Let $\mathcal{O}$ denote the ring of elements of L integral over $\mathbf{K}[x]$. These elements have the property that $\nu(f) \geq 0$ for all finite valuations on L.

Now, we are ready to formulate Mason's inequality which may be regarded as a form of lower bound for linear forms in logarithms of algebraic functions but we avoid the actual use of such logarithms and the consequent discussion of units in function fields.

Theorem 1.13. (Mason's inequality, R. C. Mason) *Suppose that γ_1, γ_2 and γ_3 are nonzero elements of L with $\gamma_1 + \gamma_2 + \gamma_3 = 0$, and such that $\nu(\gamma_1) = \nu(\gamma_2) = \nu(\gamma_3)$ for each valuation ν not in the finite set $\mathcal{V}$. Then either γ_1/γ_2 lies in $\mathbf{K}$, in which case $\mathcal{H}(\gamma_1/\gamma_2) = 0$, or*

$$\mathcal{H}(\gamma_1/\gamma_2) \leq |\mathcal{V}| + 2g - 2,$$

where $|\mathcal{V}|$ denotes the number of elements of $\mathcal{V}$.

This theorem was generalized later on by Mason to the case of n summands [63], i.e. to the equation

$$\gamma_1 + \gamma_2 + \ldots + \gamma_n = 0. \tag{1.9}$$

In 1986, his bound was improved by Brownawell and Masser [15] who proved

$$\mathcal{H}(\gamma_1, \ldots, \gamma_n) \leq (n-1)(n-2)\{|\mathcal{V}| + 2g - 2\},$$

for every solution of (1.9) which is nondegenerate (i.e. every non-empty proper subset of $\{\gamma_1, \ldots, \gamma_n\}$ is $\mathbf{K}$-linearly independent), where we have used the notation as above. This bound was independently discovered by Voloch [94] who gave a different proof.

Using Mason's inequality, we are able to solve completely the general hyperelliptic equation over an algebraic function field L of characteristic 0. A proof of this theorem can be found in the monograph of Mason (cf. [64, Theorem 6]).

Theorem 1.14. (R. C. Mason) *Let $\alpha_1, \ldots, \alpha_n \in \mathcal{O}$. All the solutions $X, Y \in \mathcal{O}$ of the hyperelliptic equation*

$$Y^2 = (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n) \tag{1.10}$$

satisfy

$$\mathcal{H}(X) \leq 26H + 8g + 4(r-1);$$

here H denotes the height of the polynomial on the right hand side of (1.10), g denotes the genus of $L/\mathbf{K}$ and r denotes the number of infinite valuations on L.

Let us note that this bound varies only as a linear function of the height of the hyperelliptic equation, in contrast with the multiple exponential bounds for the classical case obtained by Baker [1]. This shows that the fundamental inequality due to Mason on which the proof of this theorem is based and which is the function field analog of Baker's method of linear forms in logarithms is very sharp. Let us also mention that in the same way it is possible to construct an algorithm for the effective determination of all the solutions of a general Thue equation in the case of function fields.

Next, we will consider equation (1.6) over function fields, too. Let L be an algebraic function field in one variable with algebraically closed constant field $\mathbf{K}$ of characteristic 0. Thus, L is a finite extension of $\mathbf{K}(t)$ where t is a transcendental element of L over $\mathbf{K}$. As we have seen, the field L can be endowed with a set M_L of additive valuations with value group $\mathbb{Z}$ for which

$$\mathbf{K} = \{0\} \cup \{z \in L \mid \nu(z) = 0 \text{ for each } \nu \text{ in } M_L\}$$

holds. Let S be a finite subset of M_L. An element z of L is called an *S-unit* if $\nu(z) = 0$ for all $\nu \in M_L \backslash S$. The S-units form a multiplicative group which is denoted by U_S. The group U_S contains $\mathbf{K}^*$ as a subgroup and $U_S/\mathbf{K}^*$ is finitely generated. Now, the analogue of Theorem 1.7 for the function field case holds.

Theorem 1.15. (Evertse and Győry) *Let $L, \mathbf{K}, S$ be as above. Let g be the genus of $L/\mathbf{K}$, s the cardinality of S, and $n \geq 2$ an integer. Then for every $\alpha_1, \ldots, \alpha_n \in L^*$ the set of solutions of*

$$\alpha_1 x_1 + \ldots + \alpha_n x_n = 1 \text{ in } x_1, \ldots, x_n \in U_S \tag{1.11}$$

$$\text{with } \alpha_1 x_1, \ldots, \alpha_n x_n \text{ not all in } \mathbf{K} \tag{1.12}$$

is contained in the union of at most

$$\log(g+2) \cdot (e(n+1))^{(n+1)s+2}$$

$(n-1)$-dimensional linear subspaces of L^n.

For deriving this upper bound the effective upper bound of Brownawell and Masser [15] for the heights of solutions of (1.11) is used. For $n = 2$ the theorem gives the upper bound

$$\log(g+2)(3e)^{3s+2}$$

for the number of solution of (1.11). We note that in case $n = 2$ Evertse [39] established an upper bound which is better and independent of g.

Theorem 1.16. (Evertse) *Let $L, \mathbf{K}, S$ be as above. For each pair λ, μ in L^* the equation*

$$\lambda x + \mu y = 1 \text{ in } x, y \in U_S$$

has at most $2 \cdot 7^{2s}$ solutions with $\lambda x/\mu y \notin \mathbf{K}$. As above, s denotes the cardinality of S.

Let us mention that there exists an analog of the quantitative version of the Main Theorem on S-unit equations over fields with characteristic 0 due to Evertse, Schlickewei and Schmidt in case of the rational function field $\mathbf{K}(x)$, too. It is due to J. Müller and can be found in [66].

Chapter 2

Perfect powers in linear recurring sequences

P. Corvaja and U. Zannier [20] showed for linear recurring sequences defined by $G_n = a_1\alpha_1^n + \ldots + a_t\alpha_t^n$ $(t \geq 2)$ with nonzero rational numbers a_i and integral characteristic roots $\alpha_1 > \ldots > \alpha_t > 0$ $(\alpha_1, \alpha_2$ coprime) that the equation $G_n = x^q$ (for $q \geq 2$) has only finitely many solutions $(n, x) \in \mathbb{N}^2$. In this chapter we want to use a quantitative version of W. M. Schmidt's Subspace Theorem (due to J.-H. Evertse [40]) to calculate an upper bound for the number of solutions (n, x). Combining this with an earlier result of I. Nemes and A. Pethő [67] we establish also an upper bound for the number of solutions (n, x, q).

This chapter is identically equal to a joint paper with R. F. Tichy which is to appear in Acta Arith. (cf. [51]).

2.1 Introduction

Let $A_1, A_2, \ldots, A_k$ and $G_0, G_1, \ldots, G_{k-1}$ be algebraic numbers over the rationals and let (G_n) be a k-th order linear recurring sequence given by

$$G_n = A_1G_{n-1} + \cdots + A_kG_{n-k} \quad \text{for} \quad n = k, k+1, \ldots. \tag{2.1}$$

Let $\alpha_1, \alpha_2, \ldots, \alpha_t$ be the distinct roots of the corresponding characteristic polynomial

$$X^k - A_1X^{k-1} - \cdots - A_k. \tag{2.2}$$

Then for $n \geq 0$

$$G_n = P_1(n)\alpha_1^n + P_2(n)\alpha_2^n + \cdots + P_t(n)\alpha_t^n,$$

where $P_i(n)$ is a polynomial with degree less than the multiplicity of α_i; the coefficients of $P_i(n)$ are elements of the field: $\mathbb{Q}(G_0, \ldots, G_{k-1}, A_1, \ldots, A_k, \alpha_1, \ldots, \alpha_t)$.

The recurring sequence is called simple, if all characteristic roots are simple. (G_n) is called nondegenerate, if no quotient α_i/α_j for all $1 \leq i < j \leq t$ is equal to a root of unity and degenerate otherwise. Observe that, even if (G_n) is degenerate, there exists a positive integer d such that, (G_{r+md}) is nondegenerate on each of the d arithmetic progressions with $0 \leq r < d$. Therefore, restricting to nondegenerate recurring sequences causes no substantial loss of generality.

In the present chapter we deal with the Diophantine equation

$$G_n = Ex^q, \quad E \in \mathbb{Z}\backslash\{0\} \tag{2.3}$$

which was earlier investigated by several authors (e.g. cf. [85]).

For the Fibonacci sequence (F_n), Cohn [18] and Wyler [97], independently, proved that F_n is a square only if $n = 0, 1, 2$ and 13. Cohn [19] and Steiner [88] solved the equations $F_n = 2x^2$ and $F_n = 3x^2$. They also proved the corresponding results for the Lucas sequence (L_n). London and Finkelstein [61] determined all cubes in the Fibonacci sequence; Lagarias and Weisser [59] gave another proof. Steiner [87] derived some partial results for higher powers. The proofs of these results do not depend on estimates for linear forms in logarithms. Pethő [70], [71] used the theory of linear forms in logarithms and computer calculations to determine all the cubes and fifth powers in the Fibonacci sequence.

For a nondegenerate recurring sequence (G_n) of order 2 induced by a (rational) integral recurrence, it has been proved, independently, by Pethő [69] and Shorey and Stewart [83] that for the solutions $x \in \mathbb{Z}, |x| > 1$ and $q \geq 2$ of (2.3) $\max(|x|, q, n)$ is bounded by an effectively computable constant depending only on E and the sequence (G_n). In fact, Pethő proved that $\max(|x|, q, n)$ is bounded by an effectively computable number depending only on the greatest prime divisor of E and on the coefficients and initial values of (G_n) (provided that the coefficients are coprime integers). Pethő extended this result to the equation $G_n = bx^q$ with $b \in S$, where S is a set of integers composed solely of a finite number of primes.

Shorey and Stewart [83] proved the above finiteness result for certain recurring sequences of order > 2. Let (G_n) be a nondegenerate linear recurring sequence given by

$$G_n = \lambda_1\alpha_1^n + P_2(n)\alpha_2^n + \cdots + P_t(n)\alpha_t^n, \tag{2.4}$$

where λ_1 is a nonzero constant, $|\alpha_1| > |\alpha_j|$ for $j = 2, \ldots, t$, and $G_n - \lambda_1\alpha_1^n \neq 0$. Then assuming $x, q > 1$ the solutions q of (2.3) can be bounded by an effectively computable constant which depends on the coefficients and initial values of the recurrence. Kiss [58] proved that, in fact, q is less than a number which is effectively computable in terms of the greatest prime divisor of E and the coefficients and the initial values of the sequence (G_n).

Shorey and Stewart [84] considered recurring sequences (G_n) satisfying (2.4). Assuming that $P_2(n)$ is a nonzero constant, $t = 3$ and $|\alpha_1| = |\alpha_2| = |\alpha_3|$ they showed, that (2.3) has only finitely many integral solutions E, x, q and n with the greatest prime divisor of E bounded by a given positive integer P, and $|x| > 1, q > 2$ and $n \geq 0$.

Finkelstein [46], Williams [96] and Steiner [88] proved that $1, 2$ and 5 are the only Fibonacci numbers of the form $x^2 + 1$. Finkelstein [47] established a similar result for Lucas numbers. Stewart [89] and Shorey and Stewart [84] investigated the equation

$$G_n = x^q + c, \tag{2.5}$$

where $c \in \mathbb{Z}$ and (G_n) is a simple, nondegenerate second order recurring sequence of rational integers. Assuming $|A_2| = 1$, they showed for the integral solutions of (2.5) that the maximum of $n \geq 0, |x| > 1$ and $q \geq 3$ is less than an effectively computable constant depending on c, the coefficients and the initial values of the recurrence. In the case $q = 2$ they obtained a similar result under additional technical conditions. Furthermore, Shorey and Stewart [84] proved, that if α and β are multiplicatively independent with one root inside the unit circle, then (2.5) has only finitely many solutions in integers n, x and q with $n \geq 0, |x| > 1$ and $q > 2$.

Nemes and Pethő [67], [68] studied the more general equation

$$G_n = Ex^q + T(x), \tag{2.6}$$

where $T(x)$ is a polynomial of degree r and of height H with integral coefficients. For fixed $E \in \mathbb{Z}$ and T they established bounds for the integral solutions n, q, x with $|x|, q > 1$. Let (G_n) be defined as in (2.4) and assume

$$|\alpha_1| > |\alpha_2| > |\alpha_j|, \quad \text{for} \quad j = 3, \ldots, t, \tag{2.7}$$

with $\alpha_2 \neq \pm 1$. Nemes and Pethő showed that $q < C_1$ provided that $n > C_2$ and $r < C_3 q$, where C_1, C_2 and C_3 are suitable positive numbers which are effectively computable in terms of E, H and the coefficients and initial values of the recurrence. Nemes and Pethő were also able to show that if q is a fixed integer larger than one and (2.6) has infinitely many integral solutions n and x, then $T(x)$ can be characterized in terms of the Chebyshev polynomials. Kiss [58] and Shorey and Stewart [84] dealt with equation (2.6) for nondegenerate linear recurring sequences (G_n) of arbitrary order, under condition (2.7) and the additional assumptions that $E = 1$ and d is the degree of α_1 over $\mathbb{Q}$, α_1 and α_2 are multiplicatively independent and $\alpha_2 \neq \pm 1$. Then they showed that there are only finitely many integers n, x and q with $n \geq 0, |x| > 1$ and

$$q > \max\left(\frac{d \log|\alpha_1|}{\log(|\alpha_1| / \max(1, |\alpha_2|))}, d + r\right)$$

for which (2.6) holds.

Recently Corvaja and Zannier [20] considered linear recurrences defined by

$$G_n = a_1\alpha_1^n + a_2\alpha_2^n + \cdots + a_t\alpha_t^n,$$

where $t \geq 2, a_1, a_2, \ldots, a_t$ are nonzero rational numbers, $\alpha_1 > \alpha_2 > \cdots > \alpha_t > 0$ are integers. They used Schmidt's Subspace Theorem [80], [81] to show that for every integer $q \geq 2$ the equation

$$G_n = x^q \tag{2.8}$$

has only finitely many solutions $(n, x) \in \mathbb{N}^2$ assuming that G_n is not identically a perfect qth power for any n in a suitable arithmetic progression.

2.2 Results

Our first main result gives a quantitative version of the above result of Corvaja and Zannier [20].

Theorem 2.1. *Let (G_n) be a linear recurring sequence defined by*

$$G_n = a_1\alpha_1^n + a_2\alpha_2^n + \cdots + a_t\alpha_t^n, \tag{2.9}$$

where $t \geq 2, a_1, a_2, \ldots, a_t$ are nonzero rational numbers, $\alpha_1 > \alpha_2 > \cdots > \alpha_t > 0$ are integers and such that for given $q \geq 2$ there is no $r \in \{0, \ldots, q-1\}$ with G_{mq+r} a perfect qth power for all $m \in \mathbb{N}$. Then the number of solutions $(n, x) \in \mathbb{N}^2$ of the equation

$$G_n = x^q$$

is finite and can be bounded above by an explicitly computable number depending on $q, a_1, a_2, \ldots, a_t, \alpha_1, \ldots, \alpha_t$.

Remark 2.1. Corvaja and Zannier [20] showed that (2.9) is the qth power of an integer for infinitely many $n \in \mathbb{N}$, if and only if there exist integers $r \in \{0, \ldots, q-1\}$, $b \geq 1$ and

$$H_n = c_1\beta_1^n + \ldots + c_s\beta_s^n,$$

where $c_1, \ldots, c_s$ are nonzero rational numbers and $\beta_1 > \ldots > \beta_s > 0$ are integers as above, such that

$$G_n = b^{n-r}H_n^q.$$

In particular, at least one of the functions $m \mapsto G_{mq+r}$, $(r = 0, \ldots, q-1)$ is a qth power in the ring of complex functions (with pointwise multiplication) of the form (2.9), or

G_n is a perfect qth power for any n in a suitable arithmetic progression.

Remark 2.2. Observe that one can effectively determine whether G_{mq+r} is a perfect qth power or not (see again [20]). A sufficient condition is that α_1, α_2 are coprime.

Remark 2.3. The example

$$G_n = 18^n + 2 \cdot 6^n + 2^n$$

shows that the condition in Theorem 2.1 that G_{mq+r} not be a perfect qth power for every m can not be removed. Indeed, in this example the coefficients and roots of G_n satisfy the conditions of Theorem 2.1, but

$$G_{2m} = (18^m + 2^m)^2,$$

so G_{2m} is a perfect square for all $m \in \mathbb{N}$.

Remark 2.4. The assumption $\alpha_1 > \alpha_2 > \cdots > \alpha_t > 0$ guarantees that the recurring sequence (G_n) is nondegenerate.

Remark 2.5. We want to mention that the proof of Theorem 2.1 should also work in the case when (G_n) is a linear recurring sequence with algebraic characteristic roots $\alpha_1, \ldots, \alpha_t$, which are multiplicatively independent and satisfy

$$|\alpha_1| > |\alpha_i|, \quad \forall i = 2, \ldots, t,$$

and with $a_i \in \mathbb{Q}(\alpha_1, \ldots, \alpha_t)$ for all $i = 1, \ldots, t$.

Our second main result extends Theorem 2.1 to the situation when also q is considered to be variable.

Theorem 2.2. *Let (G_n) be a linear recurring sequence defined by*

$$G_n = a_1\alpha_1^n + a_2\alpha_2^n + \cdots + a_t\alpha_t^n,$$

where $a_1, \ldots, a_t$ $(t \geq 3)$ are nonzero rational numbers, $\alpha_1 > \ldots > \alpha_t > 0$ are integers and such that (for fixed $q \geq 2$) there is no $r \in \{0, \ldots, q-1\}$ with G_{mq+r} a perfect qth power for all $m \in \mathbb{N}$. Then the equation

$$G_n = x^q$$

has only finitely many integral solutions $n, x > 1, q$. The number of solutions can be bounded by an explicitly computable constant C depending only on the recurrence.

Remark 2.6. The assumption $t \geq 3$ means no loss of generality, because for $t = 2$ this theorem is already well known (see [69], [83]).

Remark 2.7. Our proof of Theorem 2.2 depends on an application of the result of Nemes and Pethő [67] which was mentioned in the introduction in detail.

Remark 2.8. By Remark 2.2 and the theorem in [67] it should also be possible to obtain the following finiteness result: Let G_n be the nth term of a linear recurrence sequence defined by (2.9), where $t \geq 3, \alpha_1 \ldots, \alpha_t$ are multiplicatively independent algebraic numbers with

$$|\alpha_1| > |\alpha_2| > |\alpha_i|, \quad \forall i = 3, \ldots, t,$$

and $a_i \in \mathbb{Q}(\alpha_1, \ldots, \alpha_t)$ for all $i = 1 \ldots, t$. Assuming that for fixed $q \geq 2$ there is no $r \in \{0, \ldots, q-1\}$ with G_{mq+r} a perfect qth power for all $m \in \mathbb{N}$, the equation

$$G_n = x^q$$

has only finitely many integral solutions $n, x > 1, q$.

2.3 Auxiliary results

We have collected some simple lemmas which are needed in our proofs.

Lemma 2.1. *Let $N_{j,k}$ denote the number of formal summands of $(a_1 + \cdots + a_k)^j$, where $a_1, \ldots, a_k$ denote formal commuting variables. Then*

$$N_{j,k} = \binom{k+j-1}{j}.$$

This is well known from combinatorics.

Lemma 2.2. *Let d be a positive integer. Then for the complex function $f(z) = (1 + z)^{1/d}$ we have*

$$\left| f(z) - \sum_{k=0}^{n} \binom{1/d}{k} z^k \right| \leq \frac{1}{d(n+1)(1-|z|)} \cdot |z|^{n+1}$$

for $z \in \mathbb{C},\ |z| < 1$, where we have chosen the branch of $(1+z)^{1/d}$ which is holomorphic on $\mathbb{C} \backslash (-\infty, -1]$ and which is equal to the positive d-th root of $(1+z)$ for $z \in \mathbb{R},\ z > -1$.

Proof. It is well-known that for $z \in \mathbb{C},\ |z| < 1$ we have

$$f(z) = \sum_{k=0}^{\infty} \binom{1/d}{k} z^k.$$

Because of

$$(n+1)\left|\binom{1/d}{n+1}\right| = \frac{\frac{1}{d}\cdot(1-\frac{1}{d})\cdot\ldots\cdot(n-\frac{1}{d})}{1\cdot\ldots\cdot n} < \frac{1}{d} < 1$$

we obtain

$$\begin{aligned}\left|f(z)-\sum_{k=0}^{n}\binom{1/d}{k}z^k\right| &\le \sum_{k=n+1}^{\infty}\left|\binom{1/d}{k}\right|\cdot|z|^k \le \\ &\le \frac{1}{d(n+1)}\sum_{k=n+1}^{\infty}|z|^k = \\ &= \frac{1}{d(n+1)(1-|z|)}\cdot|z|^{n+1},\end{aligned}$$

and therefore the proof is complete. □

Lemma 2.3. *Let $a, b \ge 0$ and let $x \in \mathbb{R}$ be the largest solution of $x = a + b\log x$. If $b > e^2$ then*

$$x < 2\,(a + b\log b)\,.$$

This lemma is due to A. Pethő and B.M.M. de Weger [86].

2.4 Proof of Theorem 2.1

According to Theorem 1.9 the number of solutions of (2.8) of the form $(n, 0)$, $n \in \mathbb{N}$ can be estimated by

$$c_1(t) \le e^{(7t)^{8t}}.$$

Therefore we can restrict ourselves to solutions of the form $(n, x) \in \mathbb{N}^2$ with $x \neq 0$. These solutions are denoted by $(n, x_n) \in \mathbb{N}^2$ with $n \in \Sigma$, where Σ is a set of positive integers.

Let us now consider the expansion of the function $f(z) = (1+z)^{1/q}$ around the origin

$$(1+z)^{1/q} = \sum_{j=0}^{\infty}\binom{1/q}{j}z^j, \quad \text{with } |z| \le 1, z \neq -1.$$

We approximate $G_n^{1/q}$ by defining

$$H_m := (a_1\alpha_1^r)^{1/q}\cdot\alpha_1^m\left[1+\sum_{j=1}^{R}\binom{1/q}{j}\cdot\left(\sum_{i=2}^{t}\frac{a_i\alpha_i^{mq+r}}{a_1\alpha_1^{mq+r}}\right)^j\right],$$

where $R \geq 1$ is an integer to be chosen later and where we have set $n = mq + r$ with $n \in \mathbb{N}$, $r \in \{0, \dots, q-1\}$. We write

$$H_m = \sum_{i=1}^{h} d_i \left(\frac{e_i}{b}\right)^m ,$$

where $d_i \in \mathbb{Q}\left((a_1\alpha_1^r)^{1/q}\right)^*$, e_i, b are integers, $b > 0$, and the e_i/b are nonzero distinct rational numbers. Clearly, H_m is nondegenerate (the roots are all positive) and we have

$$\left[\mathbb{Q}\left((a_1\alpha_1^r)^{1/q}\right) : \mathbb{Q}\right] \leq q.$$

By Lemma 2.1 we obtain

$$h \leq \binom{R+t-1}{R}.$$

On the other hand, we have

$$\left|\sum_{i=2}^{t} \frac{a_i\alpha_i^{mq+r}}{a_1\alpha_1^{mq+r}}\right| \leq (t-1)c\left(\frac{\alpha_2}{\alpha_1}\right)^{mq+r} \leq \frac{1}{2} < 1$$

where

$$c := \max\left\{\left|\frac{a_i}{a_1}\right| \mid i = 2, \dots, t\right\},$$

if

$$m \geq \frac{\log 2(t-1)c}{q\log\frac{\alpha_1}{\alpha_2}}. \tag{2.10}$$

Therefore, by Lemma 2.2 for m we get for m large enough

$$\begin{aligned}
|H_m - x_{mq+r}| &= |G_{mq+r}^{1/q} - H_m| \leq \\
&\leq \left|a_1^{1/q}\right| \cdot \alpha_1^{r/q} \cdot \alpha_1^m \cdot \frac{1}{q(R+1)\left(1 - \left|\sum_{i=2}^{t} \frac{a_i\alpha_i^{mq+r}}{a_1\alpha_1^{mq+r}}\right|\right)} \left|\sum_{i=2}^{t} \frac{a_i\alpha_i^{mq+r}}{a_1\alpha_1^{mq+r}}\right|^{R+1} \leq \\
&\leq \left|a_1^{1/q}\right| \cdot \alpha_1 \cdot \alpha_1^m \cdot \frac{2}{q(R+1)}\left[(t-1)c\left(\frac{\alpha_2}{\alpha_1}\right)^r\left(\frac{\alpha_2}{\alpha_1}\right)^{mq}\right]^{R+1} \leq \\
&\leq \left|a_1^{1/q}\right| \cdot \alpha_1^{r/q} \cdot [(t-1)c]^{R+1} \cdot \alpha_1^m \cdot \left(\frac{\alpha_2}{\alpha_1}\right)^{mq(R+1)} .
\end{aligned}$$

Thus we derive

$$|H_m - x_{mq+r}| \leq c_2(R) \cdot l_1^m \tag{2.11}$$

where we have set

$$l_1 := \alpha_1 \cdot \left(\frac{\alpha_2}{\alpha_1}\right)^{q(R+1)}$$

and

$$c_2(R) := \left|a_1^{1/q}\right| \cdot \alpha_1 \cdot [(t-1)c]^{R+1}\,.$$

Now choose

$$R > \max\left\{1, \frac{1}{q}\frac{\log \alpha_1}{\log \frac{\alpha_1}{\alpha_2}} - 1\right\}. \tag{2.12}$$

Then $0 < l_1 < 1$. Put

$$l := \frac{l_1 + 1}{2}.$$

Then for m large enough, to be more precise, for

$$m > \frac{\log c_2(R)}{\log \frac{l}{l_1}} \tag{2.13}$$

we have

$$c_2(R) \cdot l_1^m = c_2(R)\left(\frac{l_1}{l}\right)^m \cdot l^m < l^m.$$

Consequently we obtain

$$|H_m - x_{mq+r}| < l^m \quad \text{with}\, 0 < l < 1, \tag{2.14}$$

provided that R satisfies (2.12) and m satisfies (2.10) and (2.13).

Now let S be the set of places of $\mathbb{Q}$ consisting of ∞ and all primes dividing some of the e_i or b. Extend each place in S to $K := \mathbb{Q}\left((a_1\alpha_1^r)^{1/q}\right)$ in some way, the infinite place being extended such that it coincides with the complex absolute value in the given embedding of K in $\mathbb{C}$. Define the linear forms $L_{i,v}$ for $v \in S$ and $i = 1, \ldots, h$ as follows: $L_{0,\infty} := L := X_0 - \sum_{i=1}^{h} d_i X_i$, $L_{i,\infty} := X_i$ for $i = 1, \ldots, h$, while for $v \in S$, $v \neq \infty$, put $L_{i,v} := X_i$ for $i = 1, \ldots, h$. Then $\{L_{0,v}, \ldots, L_{h,v}\}$, $v \in S$ are linearly independent sets of linear forms in $h+1$ variables with coefficients in K. Furthermore we have

$$\mathcal{H}(L_{i,v}) = \begin{cases} \mathcal{H}(1, -d_1, \ldots, -d_h) =: \tilde{H} & \text{for } i = 0, v = \infty \\ \mathcal{H}(0, \ldots, 0, 1, 0, \ldots, 0) = 1 & \text{else.} \end{cases}$$

We set $H := \max\{1, \tilde{H}\}$ then it follows $\mathcal{H}(L_{i,v}) \leq H$, for $v \in S$, $i = 0, \ldots, h$. Then $\mathbb{Q}(L_{i,v}) = \mathbb{Q}$, for $v \neq \infty$, $[\mathbb{Q}(L_{0,\infty}) : \mathbb{Q}] \leq q$ and therefore

$$[\mathbb{Q}(L_{i,v}) : \mathbb{Q}] \leq q \quad \forall v \in S,\ i = 0, \ldots, h.$$

For $n \in \Sigma$ define the vector $\mathbf{x}_m = (b^m x_{mq+r}, e_1^m, \ldots, e_h^m) \in \mathbb{Z}^{h+1}$.

From (2.14) we obtain $|L_{0,\infty}(\mathbf{x}_m)| \leq (bl)^m$. Recall that S includes all primes dividing b and that the x_{mq+r} are integers. Thus by the product formula (1.3),

$$\prod_{v \in S \backslash \{\infty\}} |L_{0,v}(\mathbf{x}_m)|_v = \prod_{v \in S \backslash \{\infty\}} |b^m x_{mq+r}|_v \leq \prod_{v \in S \backslash \{\infty\}} |b^m|_v = b^{-m}.$$

Moreover, since S includes also the primes dividing the numbers e_i the product formula (1.3) gives

$$\prod_{v \in S} \prod_{i=1}^{h} |L_{i,v}(\mathbf{x}_m)|_v = \prod_{v \in S} \prod_{i=1}^{h} |e_i^m|_v = 1.$$

Thus we obtain

$$\prod_{v \in S} \prod_{i=0}^{h} \frac{|L_{i,v}(\mathbf{x}_m)|_v}{|\mathbf{x}_m|_v} \leq \left(\prod_{v \in S} |\mathbf{x}_m|_v \right)^{-h-1} \cdot l^m.$$

Since the coordinates of the vectors $\mathbf{x}_m$ are integers we have $|\mathbf{x}_m|_v \leq 1$ for $v \in M_{\mathbb{Q}} \backslash \{\infty\}$. Further, we have

$$|\mathbf{x}_m|_\infty \leq A^m$$

for some real A independent of m. Indeed, we have

$$|x_{mq+r}| \leq |x_{mq+r} - H_m| + |H_m| \leq l^m + h \cdot \tilde{c} \cdot a^m \leq 1 + h \cdot \tilde{c} \cdot a^m \leq \tilde{a}^m,$$

with

$$\begin{aligned} \tilde{c} &:= \max\{|d_i| \mid i = 1, \ldots, h\}, \\ a &:= \max\left\{ \left| \frac{e_i}{b} \right| \mid i = 1, \ldots, h \right\}, \end{aligned}$$

and $\tilde{a} := (1 + h \cdot \tilde{c})(1 + a)$. Hence

$$\begin{aligned} |\mathbf{x}_m|_\infty &= \left(|b^m x_{mq+r}|^2 + \sum_{i=1}^{h} |e_i|^2 \right)^{1/2} \leq \\ &\leq \left((b\tilde{a})^{2m} + h(ba)^{2m} \right)^{1/2} \leq A^m \end{aligned}$$

with $A := (h+1)\tilde{a}b$. It follows that

$$\mathcal{H}(\mathbf{x}_m) = \prod_{v \in M_{\mathbb{Q}}} |\mathbf{x}_m|_v \leq \prod_{v \in S} |\mathbf{x}_m|_v \leq |\mathbf{x}_m|_\infty \leq A^m.$$

Lastly we have

$$\det(L_{0,v},\dots,L_{h,v}) = \begin{vmatrix} 1 & 0 & 0 & \cdots & 0 \\ * & 1 & 0 & \cdots & 0 \\ * & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ * & 0 & 0 & \cdots & 1 \end{vmatrix} = 1,$$

which yields

$$|\det(L_{0,v},\dots,L_{h,v})|_v = 1 \quad \forall v \in S.$$

Combining our estimates we get

$$\prod_{v\in S}\prod_{i=0}^{h} \frac{|L_{i,v}(\mathbf{x}_m)|_v}{|\mathbf{x}_m|_v} < \left(\prod_{v\in S} |\det(L_{0,v},\dots,L_{h,v})|_v\right) \cdot \mathcal{H}(\mathbf{x}_m)^{-h-1-\delta}$$

for all m with (2.13), provided that $\delta < \log(1/l)/\log A$. By Theorem 1.5 there exist finitely many nonzero rational linear forms $\Lambda_1(X_0,\dots,X_h)$, $\dots,\Lambda_g(X_0,\dots,X_h)$ with

$$\begin{aligned} g \le {} & (2^{60(h+1)^2}\cdot\delta^{-7(h+1)})^s \log 4q \cdot \log\log 4q + \\ & +(150(h+1)^4\cdot\delta^{-1})^{(h+1)s+1}(2+\log\log 2H), \end{aligned}$$

such that each vector $\mathbf{x}_m$ is a zero of some Λ_j.

Suppose first Λ_j does not depend on X_0. Then, if $\Lambda_j(\mathbf{x}_m)=0$, we have a nontrivial relation

$$\sum_{i=1}^{h} u_i\left(\frac{e_i}{b}\right)^m = 0, \quad u_i \in \mathbb{Q},\ i=1,\dots,h.$$

By Theorem 1.9 this can hold for at most a finite number of m. More precisely, the number of solutions m can be estimated by

$$c_1(h) = e^{(7h)^{8h}},$$

since (H_m) is nondegenerate.

Suppose that Λ_j depends on X_0 and that $\Lambda_j(\mathbf{x}_m)=0$. Then we have

$$\sum_{i=1}^{h} v_i\left(\frac{e_i}{b}\right)^m = x_{mq+r}, \quad v_i \in \mathbb{Q},\ i=1,\dots,h. \tag{2.15}$$

Set

$$U_m := \sum_{i=1}^{h} v_i\left(\frac{e_i}{b}\right)^m,$$

then U_m is a nondegenerate, simple recurring sequence and we obtain

$$U_m^q = x_{mq+r}^q = G_{mq+r}.$$

Hence

$$V_m := \left(\sum_{i=1}^{h} v_i \left(\frac{e_i}{b}\right)^m\right)^q - \sum_{i=1}^{t} a_i \alpha_i^r (\alpha_i^q)^m,$$

has the form

$$V_m = \sum_{i=1}^{p} b_i \beta_i^m$$

with $b_i \in \mathbb{Q}$, $\beta_i \in \mathbb{Q}^+$, $i = 1, \dots, p$. Therefore V_m is a nondegenerate, simple recurring sequence, and we conclude by Lemma 2.1

$$p \leq t + \binom{h+q-1}{q} \leq t + \binom{\binom{R+t-1}{t} + q - 1}{q}.$$

Observe that by our assumptions $V_m = 0$ does not hold for every m hence an i with $b_i \neq 0$ exists. Again by Theorem 1.9 we can bound the number of solutions of (2.15) by

$$c_1(p) = e^{(7p)^{8p}}.$$

Therefore the number of solutions of (2.8) can be estimated by

$$\begin{aligned}
\tilde{C}(q) :=& \\
&= e^{(7t)^{8t}} + \frac{\log 2(t-1)c}{\log \frac{\alpha_1}{\alpha_2}} + q \cdot \Big[\Big\{ (2^{60(\tilde{h}+1)^2} \cdot \delta^{-7(\tilde{h}+1)})^s \cdot \\
&\cdot \log 4q \cdot \log\log 4q + (150(\tilde{h}+1)^4 \cdot \delta^{-1})^{(\tilde{h}+1)s+1} \cdot (2 + \log\log 2H) \Big\} \cdot \\
&\cdot \Big\{ e^{(7\tilde{h})^{8\tilde{h}}} + e^{(7\tilde{p})^{8\tilde{p}}} \Big\} + \frac{\log c_2(R)}{\log \frac{l}{l_1}} \Big],
\end{aligned}$$

where

$$\begin{aligned}
&\tilde{h} = \binom{R+t-1}{R}, \quad \tilde{p} = \binom{\tilde{h}+q-1}{q} + t \\
&H = \max\{1, \mathcal{H}(1, -d_1, \dots, -d_h)\} \\
&s = |S|, \\
&c_2(R) = \left|a_1^{1/q}\right| \cdot \alpha_1 \cdot [(t-1)c]^{R+1}, \\
&\delta < \log(1/l)/\log A,
\end{aligned}$$

and l is as in (2.14). □

2.5 Proof of Theorem 2.2

Assume that $n, x > 1, q \geq 2$ is a solution of (2.8) and write

$$x^q = G_n = a_1\alpha_1^n + B(n).$$

We distinguish two cases:

Case 1: $B(n) = 0$.
Here we get

$$|B(n)| = \left| a_2\alpha_2^n \left(1 + \sum_{i=3}^{t} \frac{a_i}{a_2}\left(\frac{\alpha_i}{\alpha_2}\right)^n\right)\right| \geq |a_2|\alpha_2^n \left|1 - \left|\sum_{i=3}^{t} \frac{a_i}{a_2}\left(\frac{\alpha_i}{\alpha_2}\right)^n\right|\right| > 0,$$

since

$$\begin{aligned} &\left|\sum_{i=3}^{t} \frac{a_i}{a_2}\left(\frac{\alpha_i}{\alpha_2}\right)^n\right| \leq \\ \leq\ & \max\left\{\left|\frac{a_i}{a_2}\right| \mid i = 3, \ldots, t\right\} \cdot (t-2) \cdot \left(\frac{\alpha_3}{\alpha_2}\right)^n \leq \\ \leq\ & tc|a_2|^{-1}\left(\frac{\alpha_3}{\alpha_2}\right)^n < 1, \end{aligned}$$

where $c = \max\{|a_i| \mid i = 1, \ldots, t\}$, whenever

$$n > \frac{\log(tc|a_2|^{-1})}{\log\frac{\alpha_2}{\alpha_3}} =: n_1.$$

Therefore $n \leq n_1$ must hold and we obtain from $a_1\alpha_1^n = x^q$ and $x \geq 2$

$$q = \frac{\log(|a_1|\alpha_1^n)}{\log x} \leq \frac{\log(c\alpha_1^{n_1})}{\log 2}.$$

Case 2: $B(n) \neq 0$.
In this case we first set

$$\delta := \frac{1}{2}\left(1 - \frac{\log\alpha_2}{\log\alpha_1}\right).$$

Then we get

$$|B(n)| \leq tc\alpha_2^n < \frac{1}{2}\alpha_1^{n(1-\delta)},$$

if

$$n > \frac{2\log(2ct)}{\log\frac{\alpha_1}{\alpha_2}} =: n_2.$$

Further

$$\frac{x^q}{a_1\alpha_1^n} = 1 + \frac{B(n)}{a_1\alpha_1^n}, \tag{2.16}$$

so

$$1 - (|a_1|\alpha_1^{\delta n})^{-1} \leq |a_1|^{-1}\alpha_1^{-n}x^q \leq 1 + (|a_1|\alpha_1^{\delta n})^{-1}, \tag{2.17}$$

where we have used that $(|a_1|\alpha_1^{\delta n})^{-1} < \frac{1}{2}$, if

$$n > \frac{\log(2|a_1|^{-1})}{\delta \log \alpha_1} =: n_3.$$

Taking logarithms and using the inequalities $|\log(1+x)| \leq x$ and $|\log(1-x)| \leq 2x$ for $0 \leq x < \frac{1}{2}$, we derive by (2.17)

$$-2|a_1|^{-1}\alpha_1^{-\delta n} \leq -\log|a_1| - n\log\alpha_1 + q\log x \leq 2|a_1|^{-1}\alpha_1^{-\delta n}.$$

Thus

$$|-\log|a_1| - n\log\alpha_1 + q\log x| \leq 2|a_1|^{-1}\alpha_1^{-\delta n}. \tag{2.18}$$

Put $\Lambda = -\log|a_1| - n\log\alpha_1 + q\log x$. From (2.16) and the fact that $B(n) \neq 0$, we get $\Lambda \neq 0$. Thus we can employ Theorem 1.12 and obtain for $n \geq 2$

$$|\Lambda| > \exp\left\{-C(3)h_1h_2\log\left(C(3)h_1h_2\right)e\log x\log q - \frac{n}{q}\right\}, \tag{2.19}$$

where $C(3) = 2^{78}3^9$ and

$$\begin{aligned} h_1 &= \max\{h(|a_1|^{-1}), e\,|\log|a_1||, 1\}, \\ h_2 &= \max\{h(\alpha_1), e\,\log\alpha_1, 1\} = e\log\alpha_1. \end{aligned}$$

Set

$$c_3 := C(3)h_1h_2\log\left(C(3)h_1h_2\right)e.$$

A comparison of (2.18) and (2.19) reveals that

$$-c_3\log q\log x - \frac{n}{q} < \log(2|a_1|^{-1}) - n\delta\log\alpha_1. \tag{2.20}$$

However, for $n > \max\{n_1, n_2\}$,

$$\frac{1}{2}|a_1|\alpha_1^n \leq |a_1|\alpha_1^n - |B(n)| \leq x^q \leq |a_1|\alpha_1^n + |B(n)| \leq ct\alpha_1^n.$$

Thus, for

$$n > \max\left\{\frac{\log ct}{\log\alpha_1}, \frac{2\log(2|a_1|^{-1})}{\log\alpha_1}\right\} =: n_4$$

we obtain
$$\frac{\log \alpha_1}{2} n < q \log x < 2 \log \alpha_1 n.$$
Writing this as
$$\frac{n}{q} < \frac{2\log x}{\log \alpha_1}, \quad \frac{\log x}{2\log \alpha_1} q < n,$$
(2.20) can be reformulated as
$$q < \frac{2\log(\frac{1}{2}|a_1|^{-1})}{\delta \log 2} + \frac{4}{\delta \log \alpha_1} + \frac{2c_3}{\delta} \log q.$$

Thus by Lemma 2.3
$$q < 2\left(\frac{2\log(\frac{1}{2}|a_1|^{-1})}{\delta \log 2} + \frac{4}{\delta \log \alpha_1} + \frac{2c_3}{\delta} \log\left(\frac{2c_3}{\delta}\right)\right) =: C_1,$$
if $n > \max\{2, n_2, n_3, n_4\} =: n_5$. Otherwise, we have
$$q \leq \frac{\log\left(ct\alpha_1^{n_5}\right)}{\log 2}.$$

Altogether we derive
$$q \leq \max\left\{\frac{\log\left(ct\alpha_1^{\bar{c}}\right)}{\log 2}, C_1(q)\right\} =: C,$$
where $\bar{c} := \max\{2, n_1, n_2, n_3, n_4\}$. For the number of solutions $n, x > 1, q \geq 2$ of (2.8) we finally obtain the upper bound
$$\sum_{q=2}^{C} \tilde{C}(q),$$
and therefore the proof is finished. □

Chapter 3

Exponential–polynomial equations and linear recurrences

Let K be an algebraic number field and let (G_n) be a linear recurring sequence defined by $G_n = \lambda_1\alpha_1^n + P_2(n)\alpha_2^n + \cdots + P_t(n)\alpha_t^n$, where $\lambda_1, \alpha_1, \ldots, \alpha_t$ are nonzero elements of K and where $P_i(x) \in K[x]$ for $i = 2, \ldots, t$. Furthermore let $f(z,x) \in K[z,x]$ monic in x. In this chapter we want to study the exponential–polynomial Diophantine equation $f(G_n, x) = 0$. We want to use a quantitative version of W. M. Schmidt's Subspace Theorem (due to J.-H. Evertse [40]) to calculate an upper bound for the number of solutions (n, x) under some additional assumptions.

This chapter is similar to a preprint of my paper [48].

3.1 Introduction

Let $A_1, A_2, \ldots, A_k$ and $G_0, G_1, \ldots, G_{k-1}$ be algebraic numbers over the rationals and let (G_n) be a k-th order linear recurring sequence given by

$$G_n = A_1 G_{n-1} + \cdots + A_k G_{n-k} \quad \text{for} \quad n = k, k+1, \ldots. \tag{3.1}$$

Let $\alpha_1, \alpha_2, \ldots, \alpha_t$ be the distinct roots of the corresponding characteristic polynomial

$$X^k - A_1 X^{k-1} - \cdots - A_k. \tag{3.2}$$

Then for $n \geq 0$

$$G_n = P_1(n)\alpha_1^n + P_2(n)\alpha_2^n + \cdots + P_t(n)\alpha_t^n, \tag{3.3}$$

where $P_i(n)$ is a polynomial with degree less than the multiplicity of α_i; the coefficients of $P_i(n)$ are elements of the field: $\mathbb{Q}(G_0, \ldots, G_{k-1}, A_1, \ldots, A_k, \alpha_1, \ldots, \alpha_t)$. We shall be interested in linear recurring sequences (G_n), where G_n defined as in (3.3) for which $P_1(n)$ is a nonzero constant, λ_1 say. Thus

$$G_n = \lambda_1\alpha_1^n + P_2(n)\alpha_2^n + \cdots + P_t(n)\alpha_t^n. \tag{3.4}$$

The recurring sequence is called simple, if all characteristic roots are simple. (G_n) is called nondegenerate, if no quotient α_i/α_j for all $1 \leq i < j \leq t$ is equal to a root of unity and degenerate otherwise. Observe that, even if (G_n) is degenerate, there exists a positive integer d such that, (G_{r+md}) is nondegenerate on each of the d arithmetic progressions with $0 \leq r < d$. Therefore, restricting to nondegenerate recurring sequences causes no substantial loss of generality.

Let $f \in \mathbb{Q}[z, x]$ be a polynomial, which is monic in x. In the present chapter we deal with the Diophantine equation

$$f(G_n, x) = 0, \tag{3.5}$$

which was earlier investigated by several authors in the special case $f(z, x) = Ex^q - z, E \in \mathbb{Z}\backslash\{0\}$, which yields the Diophantine equation

$$G_n = Ex^q, \quad E \in \mathbb{Z}\backslash\{0\}. \tag{3.6}$$

A survey about this equation can be found in [51] (see also Chapter 2). We cite here only those papers, which are of interest for us. We will repeat some results also we have stated them already in the introduction of the previous chapter.

Let us repeat the following finiteness result due to Shorey and Stewart [83]. Let (G_n) be an integral nondegenerate linear recurring sequence given by

$$G_n = \lambda_1\alpha_1^n + P_2(n)\alpha_2^n + \cdots + P_t(n)\alpha_t^n, \tag{3.7}$$

where λ_1 is a nonzero constant, $|\alpha_1| > |\alpha_j|$ for $j = 2, \ldots, t$, and $G_n - \lambda_1\alpha_1^n \neq 0$. Then assuming $x, q > 1$ the solutions q of (3.6) can be bounded by an effectively computable constant which depends on E and the coefficients and initial values of the recurrence. Kiss [58] proved that, in fact, q is less than a number which is effectively computable in terms of the greatest prime divisor of E and the coefficients and the initial values of the sequence (G_n).

Nemes and Pethő [67], [68] studied the more general equation

$$G_n = Ex^q + T(x), \tag{3.8}$$

where $T(x)$ is a polynomial of degree r and of height H with integral coefficients. For fixed $E \in \mathbb{Z}$ and T they established bounds for the integral solutions n, q, x with $|x|, q > 1$. Let (G_n) be defined as in (3.7) and assume

$$|\alpha_1| > |\alpha_2| > |\alpha_j|, \quad \text{for} \quad j = 3, \ldots, t, \tag{3.9}$$

with $\alpha_2 \neq \pm 1$. Nemes and Pethő showed that $q < C_1$ provided that $n > C_2$ and $r < C_3 q$, where C_1, C_2 and C_3 are suitable positive numbers which are effectively computable in terms of E, H and the coefficients and initial values of the recurrence. Kiss [58] and Shorey and Stewart [84] dealt with equation (3.8) for nondegenerate linear recurring sequences (G_n) of arbitrary order, under condition (3.9) and the additional assumptions that d is the degree of α_1 over $\mathbb{Q}$, α_1 and α_2 are multiplicatively independent and $\alpha_2 \neq \pm 1$. Then they showed that there are only finitely many integers n, x and q with $n \geq 0, |x| > 1$ and

$$q > \max\left(\frac{d \log|\alpha_1|}{\log(|\alpha_1|/\max(1, |\alpha_2|))}, d + r\right)$$

for which

$$G_n = x^q + T(x)$$

holds.

Recently Corvaja and Zannier [20] considered linear recurrences defined by

$$G_n = a_1\alpha_1^n + a_2\alpha_2^n + \cdots + a_t\alpha_t^n,$$

where $t \geq 2, a_1, a_2, \ldots, a_t$ are nonzero rational numbers, $\alpha_1 > \alpha_2 > \cdots > \alpha_t > 0$ are integers. They used Schmidt's Subspace Theorem [80], [81] to show that for every integer $q \geq 2$ the equation

$$G_n = x^q \tag{3.10}$$

has only finitely many solutions $(n, x) \in \mathbb{N}^2$ assuming that G_n is not identically a perfect qth power for any n in a suitable arithmetic progression. Tichy and the author [51] gave a quantitative version of the above result of Corvaja and Zannier (cf. Theorem 2.1).

Tichy and the author [51] also showed by combining their result with the previously mentioned result of Nemes and Pethő [67] that the following is true (cf. Theorem 2.2): Let (G_n) be a linear recurring sequence defined as above, such that (for fixed $q \geq 2$) there is no $r \in \{0, \ldots, q-1\}$ with G_{mq+r} a perfect qth power for all $m \in \mathbb{N}$. Then the equation

$$G_n = x^q$$

has only finitely many integral solutions $n, x > 1, q$. The number of solutions can be bounded by an explicitly computable constant C depending only on the recurrence.

Very recently, Pethő [71] used the above result of Corvaja and Zannier to show that there are only finitely many perfect powers in a third order linear recurring sequence G_n, if we assume that the characteristic polynomial of G_n is irreducible and has a dominating root.

3.2 Results

Our main result is the generalization of the above quantitative result to the Diophantine equation $f(G_n, x) = 0$, where (G_n) is defined by (3.4). This will generalize and quantify a very resent result due to Corvaja and Zannier [21].

Theorem 3.1. *Let K be an algebraic number field and let (G_n) be a linear recurring sequence defined by*

$$G_n = \lambda_1\alpha_1^n + P_2(n)\alpha_2^n + \cdots + P_t(n)\alpha_t^n,$$

where $t \geq 2, \lambda_1$ is a nonzero elements of K, $P_i(x) \in K[x]$ for all $i = 2, \ldots, t$ and where $\alpha_1, \ldots, \alpha_t$ are multiplicatively independent numbers with $1 \neq |\alpha_1| > |\alpha_j|$ for all $j = 2, \ldots, t$. Let $f(z, x) \in K[z, x]$ be monic in x and suppose that there do not exist nonzero algebraic (over K) numbers β_j and polynomials $d_j(n) \in \overline{K}[n]$ for $j = 1, \ldots, k$ such that

$$f\left(G_n, \sum_{j=1}^{k} d_j(n)\beta_j^n\right) = 0 \tag{3.11}$$

for all n in an arithmetic progression. Then the number of solutions $(n, x) \in \mathbb{N} \times K$ of the equation

$$f(G_n, x) = 0$$

is finite and can be bounded by an explicitly computable number C depending on f and on the coefficients and the initial values of the recurrence.

Remark 3.1. Corvaja and Zannier showed in [21], under the restriction that the recurrence is simple, that the assumption of $f(G_n, x) = 0$ having infinitely many solutions implies that there exist $d_j, \beta_j \in \overline{K}^{\times}, j = 1, \ldots, k$, and an arithmetic progression $\mathcal{P}$ such that

$$f\left(G_n, \sum_{j=1}^{k} d_j\beta_j^n\right) = 0, \quad \text{for } n \in \mathcal{P}.$$

Remark 3.2. The assumption that the roots of the recurrence $\alpha_1, \ldots, \alpha_t$ are multiplicatively independent is also necessary for our proof. It would be possible to relax this condition. In fact, we only need that certain linear recurrences, where the roots lie in the multiplicative group generated by powers of the α_i, are nondegenerate.

In fact, the proof of Theorem 3.1 does also work in the case when the roots are different positive (rational) integers.

Theorem 3.2. *Let (G_n) be a linear recurring sequence defined by*

$$G_n = \lambda_1 \alpha_1^n + P_2(n)\alpha_2^n + \cdots + P_t(n)\alpha_t^n,$$

where $t \geq 2, \lambda_1$ is a nonzero rational numbers, $P_i(x) \in \mathbb{Q}[x]$ for all $i = 2, \ldots, t$ and where $\alpha_1 > \alpha_2 > \ldots > \alpha_t > 0$ are integers. Let $f(z,x) \in \mathbb{Q}[z,x]$ be monic in x and suppose that there do not exist nonzero algebraic (over $\mathbb{Q}$) numbers β_j and polynomials $d_j(n) \in \overline{\mathbb{Q}}[n]$ for $j = 1, \ldots, k$ such that

$$f\left(G_n, \sum_{j=1}^{k} d_j(n)\beta_j^n\right) = 0$$

for all n in an arithmetic progression. Then the number of solutions $(n,x) \in \mathbb{N} \times \mathbb{Q}$ of the equation

$$f(G_n, x) = 0$$

is finite and can be bounded by an explicitly computable number C depending on f and on the coefficients and the initial values of the recurrence.

Remark 3.3. Observe that one can effectively determine whether there do exist nonzero numbers $\beta_j \in \overline{K}$ and polynomials $d_j(n) \in \overline{K}[n]$ for $j = 1, \ldots, k$ such that (3.11) holds for all n in an arithmetic progression or not (see [21]). This will also follow from the proof of Theorem 3.1. The following example shows that this condition is necessary: let

$$G_n = 18^n + 2 \cdot 6^n + 2^n,$$

and $f(z,x) = x^2 - z$. The coefficients and roots have the desired properties, but

$$G_{2k} = (18^k + 2^k)^2,$$

so $f(G_{2k}, 18^k + 2^k) = 0$ for all $k \in \mathbb{N}$. Another much simpler example is obtained by taking $f(z,x) = x - z$.

Remark 3.4. We want to note that the above assumption (3.11) also means (for $k = 0$) that $f(z,0) = 0$ does not hold identically or equivalently x is not a divisor of $f(z,x)$. For example $f(z,x) = x - z \cdot x$, which yields solutions $(n,0) \in \mathbb{N}^2$ for all $n \in \mathbb{N}$, is excluded.

Remark 3.5. Let us mention that the condition on the dominant root α_1 is crucial. The proof of the theorem heavily depends on that assumption.

Remark 3.6. For simplicity we have introduced the condition that $f(z,x)$ is monic in x. There is no problem at all, if we assume that the leading coefficient of f with respect to x does not depend on z. Moreover, it is a well-known trick how to get rid of the this assumption (with a corresponding modification of the theorem); namely we may replace $f(z,x)$ with the polynomial $a(z)^{d-1}f(z,x/a(z))$, where $a(z),d$ is the leading coefficient, the degree respectively of f with respect to x.

Next we want to state some conclusion concerning special cases of the above result.

Corollary 3.1. *Let (G_n) be a linear recurring sequence defined by*

$$G_n = \lambda_1\alpha_1^n + P_2(n)\alpha_2^n + \cdots + P_t(n)\alpha_t^n,$$

where $t \geq 2, \lambda_1$ is a nonzero rational number, $P_i(x) \in \mathbb{Q}[x]$ for all $i = 2,\dots,t$ and where $\alpha_1,\dots,\alpha_t$ are multiplicatively independent rational numbers with $1 \neq |\alpha_1| > |\alpha_j|$ for all $j = 2,\dots,t$. Let $P(x) \in \mathbb{Q}[x]$ be monic and suppose that there do not exist nonzero algebraic (over $\mathbb{Q}$) numbers β_j and polynomials $d_j(n) \in \overline{\mathbb{Q}}[n]$ for $j = 1,\dots,k$ such that

$$G_n = P\left(\sum_{j=1}^{k} d_j(n)\beta_j^n\right) \tag{3.12}$$

for all n in an arithmetic progression. Then the number of solutions $(n,x) \in \mathbb{N}\times\mathbb{Q}$ of the equation

$$G_n = P(x)$$

is finite and can be bounded by an explicitly computable number C depending on P and on the coefficients and the initial values of the recurrence.

Remark 3.7. The above corollary is also true, if we assume $P(x) \in \mathbb{Q}(x)$, say $P(x) = f(x)/g(x)$, where $f(x)$ is a monic polynomial.

Remark 3.8. Also the classical case $P(x) = x^q$, concerning the number of perfect powers in the linear recurring sequence (G_n) is included. So we get a generalisation of the results stated in [51]. Observe that from [20] it follows that condition (3.12) is equivalent to the assumption that G_n is not equal to a perfect qth power for all n in an arithmetic progression (cf. also [98]).

Last we want to discuss some families of Diophantine equations related to the above types of equations.

Corollary 3.2. *Let (G_n) be an integral linear recurring sequence with (3.4), where $t \geq 2, \lambda_1$ is a nonzero element of $K = \mathbb{Q}(\alpha_1,\dots,\alpha_t)$, $P_i(x) \in K[x]$ for all $i = 2,\dots,t$ and where $\alpha_1,\dots,\alpha_t$ are multiplicatively independent algebraic integers with $1 \neq |\alpha_1| >$*

$|\alpha_j|$ for all $j = 2, \ldots, t$. Furthermore, suppose that there do not exist nonzero numbers $\beta_j \in \overline{K}$ and polynomials $d_j(n) \in \overline{K}[n]$ for $j = 1, \ldots, k$ such that

$$G_n = \left(\sum_{j=1}^{k} d_j(n)\beta_j^n \right)^q \tag{3.13}$$

for all n in an arithmetic progression and for given $q \geq 2$. Then the number of solutions $(n, x, q) \in \mathbb{N}^3$ with $n, x, q > 1$ of the equation

$$G_n = x^q$$

is finite and can be bounded by an explicitly computable number C depending only on the coefficients and the initial values of the recurrence.

Remark 3.9. Observe that condition (3.13) can be verified effectively, because under the other assumptions one can calculate an upper bound for q first. Then condition (3.13) must only be verified for q smaller than this bound.

Corollary 3.3. *Let (G_n) be an integral linear recurring sequence with (3.4), where $t \geq 2, \lambda_1$ is a nonzero rational element of $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_t)$, $P_i(x) \in K[x]$ for all $i = 2, \ldots, t$ and where $\alpha_1, \ldots, \alpha_t$ are multiplicatively independent algebraic integers with $1 \neq |\alpha_1| > |\alpha_2| > |\alpha_j|$ for all $j = 3, \ldots, t$. Let $\alpha_2 \neq \pm 1$ and let $T(x)$ be a polynomial with integer coefficients and degree r; we take $r = 0$ if $T(x)$ is the zero polynomial. Furthermore, suppose that there do not exist nonzero numbers $\beta_j \in \overline{K}$ and polynomials $d_j(n) \in \overline{K}[n]$ for $j = 1, \ldots, k$ such that*

$$G_n = \left(\sum_{j=1}^{k} d_j(n)\beta_j^n \right)^q + T\left(\sum_{j=1}^{k} d_j(n)\beta_j^n \right) \tag{3.14}$$

for all n in an arithmetic progression and for given $q \geq 2$. Then there are only finitely many integers n, x and q with $n \geq 0, q \geq 1$ and $|x| > 1$ for which

$$G_n = x^q + T(x)$$

holds.

3.3 Auxiliary results

We need some results from the theory of algebraic functions fields, which can be found in the monographs of Eichler [37] and Iwasawa [54], namely the theory of Puiseux expansions.

Let K be an algebraic number field, which is generated over the field of rational numbers $\mathbb{Q}$. We assume that $f(x,y)$ is an absolutely irreducible polynomial in x and y, with coefficients in the algebraic number field K, that is f is irreducible over the algebraic closure $\overline{K}$ of K. We denote by F the field obtained by adjoining a root of $f(x,y)$ to $\overline{K}(x)$, the field of rational functions in x with coefficients in the algebraic closure of K. Then F is an algebraic function field over the algebraically closed field $\overline{K}$ of characteristic 0.

Theorem 3.3. (Puiseux's Theorem) *Let F be an algebraic functions field over an algebraically closed field $\overline{K}$ of characteristic 0, given by $f(x,y)=0$. For simplicity we suppose $f(x,y)$ to be monic in y. Let us denote by $n=[F:\overline{K}(x)]$ the degree of F over $\overline{K}(x)$. Then with every element $\xi\in K$ there are associated $r=r(\xi)\leq n$ natural number $e_i=e_i(\xi)$ whose sum is*

$$e_1+\cdots+e_r=n;$$

similar numbers $e_i(\infty)$ are associated with the symbol $\xi=\infty$. These numbers have the following meaning: Setting

$$z_\xi=x-\xi,\quad z_\infty=1/x, \tag{3.15}$$

the irreducible equation $f(x,y)=0$ satisfied by an arbitrary function y of F over $\overline{K}$ has for solutions the $r=r(\xi)$ power series

$$y_i=\sum_{k=v_i}^{\infty}a_{ik}(\sqrt[e_i(\xi)]{z_\xi})^k,\quad a_{iv_i}\neq 0,\quad i=1,2,\ldots,r(\xi). \tag{3.16}$$

With a primitive e_ith root of unity ζ form

$$y_{ij}=\sum_k a_{ik}\zeta^{jk}(\sqrt[e_i(\xi)]{z_\xi})^k,\quad j=0,\ldots,e_i(\xi)-1; \tag{3.17}$$

then the left side of $f(x,y)=0$ is identical with

$$f(x,y)=\prod_{j,i}(y-y_{ij}). \tag{3.18}$$

The coefficients a_{ik} are elements of a finite field extension K' of K, and their images under isomorphisms of K' give permutations of the y_{ij} in (3.18). The power series have respective radii of convergence $\neq 0$.

Let us mention that the theory of Puiseux expansions is equivalent to the valuation theory. The numbers $e_i(\xi)$, $i=1,\ldots,r(\xi)$ are called ramifications indices related to the place generated by $z_\xi=x-\xi$, respectively $z_\infty=1/x$ in the rational function field

$\overline{K}(x)$. They have the following meaning in valuation theory: The place generated by z_ξ in the rational function field can be extended to $r(\xi)$ places $P_1, \ldots, P_r$ in the extension field F. For the valuation of the extended place we have

$$v_{P_i} = e_i v_{z_\xi},$$

for all $i = 1, \ldots, r$.

We also want to state an explicit form of the last theorem, which enables us to derive estimates for the coefficients of the Puiseux expansions of an algebraic function and which is due to Coates (cf. [17]).

We introduce the following notation first. If α is an algebraic number, then $\deg \alpha$, $\delta(\alpha)$, $h(\alpha)$ denote respectively the degree of α, the least positive rational integer such that $\delta(\alpha)\alpha$ is an algebraic integer, and the maximum of the absolute values of the conjugates of α, and we put $\sigma(\alpha) = \max\{\deg \alpha, \delta(\alpha), h(\alpha)\}$. Let $f(x, y)$ be as above and let the maximum of the absolute values of the conjugates of the coefficients of $f(x, y)$ be at most f, where $f \geq 2$, and let $f(x, y)$ have degree m and n in x and y, respectively. Put $N = \max\{n, m, 3\}$.

Theorem 3.4. (Explicit Puiseux's Theorem, Coates) *Let F be an algebraic functions field over an algebraically closed field $\overline{K}$ of characteristic 0, given by $f(x, y) = 0$. Let $\xi \in \overline{K}$ and A_i $(1 \leq i \leq r = r(\xi))$ be the valuations of F extending the valuation of $\overline{K}(x)$ defined by $x - \xi$, and let e_i be the ramification index of A_i. We write*

$$y = \sum_{k=0}^{\infty} w_{ik}(x - \xi)^{k/e_i}$$

for the Puiseux expansion of y at A_i. Then the coefficients w_{ik} $(1 \leq i \leq r, k = 0, 1, \ldots)$ are algebraic numbers, and the number field K' obtained by adjoining ξ and these coefficients to K has degree at most $(N \deg \xi)^N$ over K. Further, K' is generated over K by ξ and w_{ik} $(1 \leq i \leq r, 0 \leq k \leq 2N^4)$. Finally, there exists a positive rational integer Δ such that $\Delta^{k+1} w_{ik}$ $(1 \leq i \leq r, k = 0, 1, \ldots)$ is an algebraic integer with

$$h(w_{ik}) \leq \left(\frac{\Lambda}{\Delta}\right)^{k+1}, \tag{3.19}$$

where $\Lambda = (f\sigma(\xi))^\mu$, $\mu = (N^4 n \deg \xi)^{3N^4}$.

Let Q_i $(1 \leq i \leq r(\infty))$ be the valuations of F extending the valuation of $\overline{K}(x)$ defined by $1/x$. Let e_i be the ramification index of Q_i, and let

$$y = \left(\frac{1}{x}\right)^{-e_i} \sum_{k=0}^{\infty} w_{ik} \left(\frac{1}{x}\right)^{k/e_i}$$

be the expansion of y at Q_i. Then the coefficients are algebraic numbers, and the number field K' obtained by adjoining them to K has degree at most N^N over K. Further K' is generated over K by the w_{ik} $(1 \le i \le r, 0 \le k \le 2N^4)$. Finally, there exists a positive rational integer Δ such that $\Delta^{k+1} w_{ik}$ $(1 \le i \le r, k = 0, 1, \ldots)$ is an algebraic integer with

$$h(w_{ik}) \le \left(\frac{\Lambda}{\Delta}\right)^{k+1}, \tag{3.20}$$

where $\Lambda = f^{\mu}$, $\mu = (N^4 n)^{3N^4}$.

We want to remark that the proof of the last theorem yields an algorithm for the actual determination of the coefficients of the Puiseux expansion of an algebraic function. In fact, for the proof one constructs polynomials $p_i(w)$ with coefficients in the field obtained by adjoining the first i coefficients of the Puiseux expansion in question, such that the $(i+1)$st coefficient is a root of $p_i(w)$. From this sequence of polynomials everything follows (see [17]). We want to show this construction by looking at the following example.

Example. We want to derive the Puiseux expansions of

$$g(x, y) = y^2 - xy + 1 \in \mathbb{Q}(x)[y],$$

at all infinite places of the functional field $F = \overline{\mathbb{Q}}(x, y)$ generated by $g(x, y) = 0$. First of all, we have

$$y_{1,2} = \frac{x}{2} \pm \frac{\sqrt{x^2 - 4}}{2}$$

for the roots of the equation $g(x, y) = 0$. Thus, we have $F = \overline{\mathbb{Q}}(x)(\sqrt{x^2 - 4})$. From this we see (see e.g. [90]) that F is a so called Kummer extension (which is a special Galois extension). Therefore we know that there are $r = 2$ places P_1, P_2 lying over the place generated by $1/x$ in the rational function field and the corresponding ramification indices e_1, e_2 are both equal, say e, and the common value is $e = 1$.

First we set

$$G(x, y) = x^{\delta e} g(x^{-e}, x^{-e} y) = x^2 - x + y^2,$$

where δ is the total degree of $g(x, y)$, so $G(x, y)$ is a polynomial in x, y. Next we write $G(x, y) = x^{r_0} G_0(x, y) = x^2 - x + y^2$, where G_0 is not divisible by x, then we choose $p_0(w) = g_0(0, w)$. So we have $p_0(w) = w(w - 1)$, which has the zeros $0, 1$. So the first coefficient of each expansion is know. Next we set $y = xw$, $y = 1 + xw$ respectively and substitute it into $G(x, y)$ and repeat the procedure. We do it only for the second case. There we have

$$G(x, 1 + xw) = (1 + xw)^2 - 1 - xw + x^2 = x(xw^2 - 3w + x),$$

which gives $p_1(w) = -3w$, which yields that the next coefficient is 0. Next we consider

$$G(x, 1 + x^2 w) = x^2(w + x^2 w^2 + 1),$$

which implies $p_2(w) = w + 1$ and therefore the coefficient 1. The next step is

$$G(x, 1 - x^2 + x^3 w) = x^3(w + x - 2x^2 w + x^3 w^2),$$

which gives $p_3(w) = w$ and thus again the coefficient 0. Continuing in this way we get

$$y_1 = x - \frac{1}{x} - \frac{1}{x^3} - 2\frac{1}{x^5} + \mathcal{O}\Big(\frac{1}{x^7}\Big),$$
$$y_2 = \frac{1}{x} + \frac{1}{x^3} + 2\frac{1}{x^5} + \mathcal{O}\left(\frac{1}{x^7}\right).$$

So we have constructed the first terms of the requested Puiseux expansions.

3.4 Proof of the Main Theorem

First of all we can assume that $f(z, x) = 0$ depends on z and x, otherwise the assertion of our Theorem 3.1 would be trivially false. We can also suppose without loss of generality that $f(z, x)$ is absolutely irreducible. Otherwise we can find a finite extension field L of K such that $f(z, x)$ splits into a product of absolutely irreducible factors in $L[z, x]$. Then we can proceed with each of those factors as below and sum up the number of solutions to get the final result. So let us denote by F the functions field obtained by adjoining a root of $f(z, x) = 0$ to $\overline{K}(z)$, where $\overline{K}$ denotes the algebraic closure of K.

We work only in the case $|\alpha_1| > 1$ and consider the Puiseux expansion at $z = \infty$ of the solution $x = x(z)$ of $f(z, x) = 0$. The arguments in the case $|\alpha_1| < 1$ are completely analogous and use the expansion at $z = 0$.

In the sequel $C_1, C_2, \ldots$ will denote positive numbers depending only on $f(z, x)$ and on λ_1 and on the P_i, α_i.

According to Theorem 1.9 and Remark 3.2 the number of solutions of (3.5) of the form $(n, 0)$, $n \in \mathbb{N}$ can be estimated by

$$C_2 = e^{7C_1^{8C_1}}.$$

Observe that this follows from the fact that the $\alpha_1, \ldots, \alpha_t$ are multiplicatively independent. Therefore also $G_n^2, G_n^3, \ldots$ are nondegenerate recurring sequences. Consequently, we can restrict ourselves to solutions of the form $(n, x) \in \mathbb{N} \times K$ with $x \neq 0$. These solutions are denoted by $(n, x_n) \in \mathbb{N} \times K$ with $n \in \Sigma$, where Σ is a set of positive integers.

Now by Puiseux's Theorem 3.3 we can conclude that

$$f(z, x) = \prod_{j,i} (x - x_{ij}),$$

where

$$x_{ij} = \sum_{k=v_i}^{\infty} a_{ik} \zeta^{jk} \left(\frac{1}{z}\right)^{\frac{k}{e_i}},$$

for $j = 0, \ldots, e_i - 1$, $i = 1, 2, \ldots, r$ and where $e_1, \ldots, e_r$ are the ramification indices of the valuations extending $1/z$ to the function field F. Furthermore by the Explicit Puiseux's Theorem 3.4 we get that all coefficients lie in a fixed finite extension field K' of K and we have

$$h(a_{ik}\zeta^{jk}) \leq C_3^{k+1},$$

for $j = 0, \ldots, e_i - 1$, $i = 1, 2, \ldots, r$. Therefore for each solution (n, x_n) of (3.5) we get

$$x_n = \sum_{k=v}^{\infty} \beta_k G_n^{-\frac{k}{e}}, \tag{3.21}$$

for some v, e and β_k with

$$|\beta_k| \leq C_3^{k+1}$$

for all $k = 1, 2, \ldots$, which lie in a fixed finite extension of K. In what follows we will only consider those n, lying in a subsequence $\mathcal{R} \subseteq \Sigma$, for which the same expansion occurs. The final number is just the sum of all numbers obtained by all those expansions.

Let us remark that for $n > C_4$ the above series converges absolutely; this is because

$$\begin{aligned} |G_n| &= |\lambda_1 \alpha_1^n + \ldots + P_t(n)\alpha_t^n| = |\lambda_1||\alpha_1|^n \left| 1 + \sum_{j=2}^{t} \frac{P_j(n)}{\lambda_1} \left(\frac{\alpha_j}{\alpha_1}\right)^n \right| \geq \\ &\geq |\lambda_1||\alpha_1|^n \left| 1 - \underbrace{\sum_{j=2}^{t} \left|\frac{P_j(n)}{\lambda_1}\right| \left|\frac{\alpha_j}{\alpha_1}\right|^n}_{\leq 1/2 \text{ for } n > C_5} \right| \geq C_6 C_7^n \longrightarrow \infty, \end{aligned}$$

because $C_7 = |\alpha_1| > 1$. Thus

$$\sum_{k=v}^{\infty} |\beta_k||G_n|^{-k/e} \leq \sum_{k=v}^{\infty} C_3^{k+1} \left[C_6 C_7^n\right]^{-k/e} = C_3 \sum_{k=v}^{\infty} \left[C_3 \left[C_6 C_7^n\right]^{-1/e}\right]^k < \infty,$$

if $n > C_4$.

Since $|\alpha_1| > |\alpha_i|$ for $i = 2, \ldots, t$, we have binomial expansions

$$\begin{aligned} G_n^{-\frac{k}{e}} &= \lambda_1^{-\frac{k}{e}} \alpha_1^{-\frac{kn}{e}} \left(1 + \sum_{i=2}^{t} \frac{P_i(n)}{\lambda_1} \left(\frac{\alpha_i}{\alpha_1}\right)^n\right)^{-\frac{k}{e}} = \\ &= \lambda_1^{-\frac{k}{e}} \alpha_1^{-\frac{kn}{e}} \sum_{r=0}^{\infty} \binom{-\frac{k}{e}}{r} \left(\sum_{i=2}^{t} \frac{P_i(n)}{\lambda_1} \left(\frac{\alpha_i}{\alpha_1}\right)^n\right)^r, \end{aligned}$$

for some choice of the eth roots of λ_1 and α_1, which we may assume to be fixed for all $n \in \mathcal{R}$. Because of the fact that

$$\left|\sum_{i=2}^{t} \frac{P_i(n)}{\lambda_1} \left(\frac{\alpha_i}{\alpha_1}\right)^n\right| \leq C_8 n^{C_9} C_{10}^n < 1,$$

because $C_{10} = |\alpha_2/\alpha_1| < 1$, if $n > C_{11}$, the expansion converges again absolutely for large n.

Next we are going to approximate x_n by a finite sum extracted from the Puiseux expansion (3.21). We define

$$H_n := \sum_{k=v}^{H} \beta_k \lambda_1^{-\frac{k}{e}} \alpha_1^{-\frac{kn}{e}} \sum_{r=0}^{H} \binom{-\frac{k}{e}}{r} \left(\sum_{i=2}^{t} \frac{P_i(n)}{\lambda_1} \left(\frac{\alpha_i}{\alpha_1}\right)^n\right)^r,$$

where $H \geq 1$ is an integer to be chosen later. We may write

$$H_n = \sum_{j=1}^{h} \tau_j(n) \gamma_j^n, \quad n \in \mathcal{R},$$

where the $\tau_j(n) \in \overline{K}[n]$ and the γ_j are distinct and lie in the multiplicative group generated by $\alpha_1^{1/e}$ and $\alpha_2, \ldots, \alpha_t$. Clearly H_n is nondegenerate, in fact the roots γ_j are again multiplicatively independent. Moreover, we have

$$h \leq C_{12}(H), \tag{3.22}$$

where $C_{12}(H)$ means that the constant depends also on H.

We enlarge K at once and assume that it contains all the $\alpha_i^{1/e}$ and all the coefficients β_j in the Puiseux series. In particular, we may assume that K contains all the coefficients of τ_j and the γ_j.

Next we estimate the approximation error we make, when we approximate x_n through H_n. We have

$$|x_n - H_n| = \left| x_n - \sum_{k=v}^{H} \beta_k \lambda_1^{-\frac{k}{e}} \alpha_1^{-\frac{kn}{e}} \sum_{r=0}^{H} \binom{-\frac{k}{e}}{r} \left(\sum_{i=2}^{t} \frac{P_i(n)}{\lambda_1} \left(\frac{\alpha_i}{\alpha_1}\right)^n \right)^r \right| \leq$$

$$\leq \left| \sum_{k=v}^{H} \beta_k \lambda_1^{-\frac{k}{e}} \alpha_1^{-\frac{kn}{e}} \sum_{r=H+1}^{\infty} \binom{-\frac{k}{e}}{r} \left(\sum_{i=2}^{t} \frac{P_i(n)}{\lambda_1} \left(\frac{\alpha_i}{\alpha_1}\right)^n \right)^r \right| + \tag{3.23}$$

$$+ \left| \sum_{k=H+1}^{\infty} \beta_k \lambda_1^{-\frac{k}{e}} \alpha_1^{-\frac{kn}{e}} \underbrace{\sum_{r=0}^{\infty} \binom{-\frac{k}{e}}{r} \left(\sum_{i=2}^{t} \frac{P_i(n)}{\lambda_1} \left(\frac{\alpha_i}{\alpha_1}\right)^n \right)^r}_{=G_n^{-k/e}} \right| \leq$$

$$\leq \sum_{k=v}^{H} C_{13}^{k+1} C_{14}^{kn} C_{15}(k,H) \left| \sum_{i=2}^{t} \frac{P_i(n)}{\lambda_1} \left(\frac{\alpha_i}{\alpha_1}\right)^n \right|^{H+1} + \tag{3.24}$$

$$+ \sum_{k=H+1}^{\infty} C_{13}^{k+1} C_{14}^{kn} \left[C_6 C_7^n\right]^{-k/e} \leq$$

$$\leq \sum_{k=v}^{H} C_{13}^{k+1} C_{14}^{kn} C_{15}(k,H) \left[C_8 n^{C_9} C_{10}^n\right]^{H+1} + \tag{3.25}$$

$$+C_{13} \frac{\left[C_{13} C_{14}^n \left(C_6 C_7^n\right)^{-1/e}\right]^{H+1}}{1 - \underbrace{C_{13} C_{14}^n \left(C_6 C_7^n\right)^{-1/e}}_{\leq 1/2 \text{ for } n > C_{16}}} \leq$$

$$\leq C_{17}(H) \left[C_8 n^{C_9} C_{10}^n\right]^{H+1} \underbrace{C_{19}^n}_{\leq 1} + C_{20} \left[C_{21} n^{C_{22}} C_{23}^n\right]^{H+1} \leq \tag{3.26}$$

$$\leq \left[C_{24} n^{C_{25}} C_{26}^n\right]^{H+1} \left(C_{17}(H) + C_{20}\right) = \tag{3.27}$$

$$= C_{27}(H) n^{C_{25}(H+1)} C_{26}^{n(H+1)}, \tag{3.28}$$

where $C_{10}, C_{14} < 1$, $C_7 > 1$ thus $C_{23} < 1$ and therefore also $C_{26} < 1$. Observe that we have used

$$\left| \sum_{r=H+1}^{\infty} \binom{d}{r} w^r \right| \leq C(d,H) |w|^{H+1}$$

and

$$\left| \sum_{k=H+1}^{\infty} q^k \right| \leq \frac{q^{H+1}}{1-q}$$

to estimate the tails of the above series.

For later purposes we need an estimate of $|x_n|$. For n larger than a constant C_{27} we obtain

$$|x_n| = \left|\sum_{k=v}^{\infty} \beta_k G_n^{-\frac{k}{e}}\right| \leq C_3 \frac{\left[C_3\left[C_6 C_7^n\right]^{-1/e}\right]^v}{1 - \underbrace{C_3[C_6C_7^n]^{-1/e}}_{\leq 1/2 \text{ for } n>C_{27}}} \leq C_{28} C_{29}^n \tag{3.29}$$

Observe that $v \in \mathbb{Z}$, so that we cannot conclude that $C_{29} < 1$ holds.

We choose H so that

$$C_{26}^{H+1} C_{29} < 1. \tag{3.30}$$

To get this, we must have

$$H > \max\left\{1, \frac{\log C_{29}}{\log C_{26}^{-1}} - 1\right\}.$$

Observe that from now on H is fixed and therefore also $h, \tau_i(n), \gamma_i, i = 1, \ldots, h$ are fixed. Also, we choose a finite set S so that it contains all infinite absolute values of K. Moreover we require that all the α_j, λ_1 and all coefficients of the $P_j(n)$, all the nonzero coefficients of $f(z,x)$ and of $\tau_1(n), \ldots, \tau_h(n)$ are S-units, which means that the $|\cdot|_v$ of those values $= 1$ for each $v \notin S$. In particular, with this choice all γ_j are S-units. Also, the G_n are S-integer, that is $|G_n|_v \leq 1$ for each $v \notin S$, and $f(z,x)$ is monic in x; therefore, the x_n too are S-integers, in view of the equations $f(G_n, x_n) = 0$.

We shall apply Theorem 1.5, so let us define, for every $s \in S$, $h+1$ independent linear forms in $\mathbf{X} := (X_0, \ldots, X_h)$ as follows: put

$$L_{0,\infty}(\mathbf{X}) = X_0 + X_1 + \cdots + X_h$$

and for $v \in S, 0 \leq i \leq h, (i,v) \neq (0,\infty)$ put

$$L_{i,v}(\mathbf{X}) = X_i.$$

Here ∞ denotes the infinite absolute value, which coincides with the complex absolute value in the embedding of K in $\mathbb{C}$. We have

$$\mathcal{H}(L_{i,v}) \leq C_{30}$$

for $v \in S, i = 0, \ldots, h$. Furthermore $K(L_{i,v}) = K$ and therefore

$$[K(L_{i,v}) : K] = 1 \quad \forall v \in S, i = 0, \ldots, h.$$

Moreover, we have

$$\det(L_{0,v},\ldots,L_{h,v}) = \begin{vmatrix} 1 & 0 & 0 & \ldots & 0 \\ 1 & 1 & 0 & \ldots & 0 \\ 1 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & 0 & 0 & \ldots & 1 \end{vmatrix} = 1,$$

which yields

$$|\det(L_{0,v},\ldots,L_{h,v})|_v = 1 \quad \forall\, v \in S.$$

For $n \in \mathcal{P}$ define the vectors $\mathbf{x}_n = (-x_n, \tau_1(n)\gamma_1^n, \ldots, \tau_h(n)\gamma_h^n) \in K^{h+1}$ and consider the double product

$$\prod_{v\in S}\prod_{i=0}^{h} \frac{|L_{i,v}(\mathbf{x}_n)|_v}{|\mathbf{x}_n|_v}.$$

By putting

$$\sigma = -x_n + \tau_1(n)\gamma_1^n + \ldots + \tau_h(n)\gamma_h^n = L_{0,\infty}(\mathbf{x}_n),$$

we can rewrite the double product as

$$|\sigma|_\infty \cdot \left(\prod_{v\in S\setminus\{\infty\}} |x_n|_v\right)\left(\prod_{v\in S}\prod_{i=1}^{h} |\tau_i(n)\gamma_i^n|_v\right)\left(\prod_{v\in S}|\mathbf{x}_n|_v\right)^{-(h+1)}.$$

Observe that x_n is an S-integer and that, due to our choice of S, the $\tau_i(n)\gamma_i^n$ are S-units for $i \geq 1$. In particular, this implies

$$\left(\prod_{v\in S}\prod_{i=1}^{h} |\tau_i(n)\gamma_i^n|_v\right) = 1 \tag{3.31}$$

and

$$\left(\prod_{v\in S\setminus\{\infty\}} |x_n|_v\right) = \prod_{v\notin S} |x_n|_v \cdot |x_n|_\infty \leq |x_n|_\infty \leq C_{28}C_{29}^n, \tag{3.32}$$

where we have used the product formula (1.3) and (3.29). Therefore we get using (3.28), (3.31) and (3.32)

$$\prod_{v\in S}\prod_{i=0}^{h} \frac{|L_{i,v}(\mathbf{x}_n)|_v}{|\mathbf{x}_n|_v} \leq C_{27}(H)n^{C_{25}(H+1)}C_{26}^{n(H+1)}C_{28}C_{29}^n\left(\prod_{v\in S}|\mathbf{x}_n|_v\right)^{-(h+1)}.$$

Last we need an upper bound for $\mathcal{H}(\mathbf{x}_n)$. We have

$$\mathcal{H}(\mathbf{x}_n) \leq \prod_{v\in S} |\mathbf{x}_n|_v \leq C_{31} \prod_{v\in S} \max\{|x_n|_v, |\tau_1(n)\gamma_1^n|_v, \ldots, |\tau_h(n)\gamma_h^n|_v\},$$

where we have used again our choice of S and the fact the two norms on K^{h+1} are equivalent. Observe that C_{31} does only depend on h and on $[K : \mathbb{Q}]$. We need an estimate for $|x_n|_v$ and we derive it from the equation $f(G_n, x_n) = 0$. Observe that we trivially have an estimate

$$|G_n|_v \leq C_{32} n^{C_{33}} C_{34}^n.$$

On the other hand, we can estimate the absolute value of the roots of an equation in terms of the absolute value of the coefficients. We finally obtain

$$|x_n|_v \leq C_{35} n^{C_{36}} C_{37}^n.$$

Moreover we have

$$|\tau_i(n)\gamma_i^n|_v \leq C_{38} n^{C_{39}} C_{40}^n,$$

for all $i = 1, \ldots, h$. Consequently we get

$$\mathcal{H}(\mathbf{x}_n) \leq C_{41} n^{C_{42}} C_{43}^n. \tag{3.33}$$

Let us point out that these constants depend not on n.

We now choose $0 < \delta < 1$ so that

$$C_{26}^{H+1} C_{29} C_{43}^{\delta} < 1. \tag{3.34}$$

This will be possible for small δ in view of (3.30).

In view of the bound for the double product we derived and (3.33), the verification of (1.4) of the Quantitative Subspace Theorem 1.5 will follow from

$$C_{27}(H) C_{28} n^{C_{25}(H+1)} \left(C_{26} C_{29}\right)^n < \left(C_{41} n^{C_{42}} C_{43}^n\right)^{-\delta},$$

which is the same as

$$n^{C_{25}(H+1)+\delta C_{42}} \left(C_{26}^{H+1} C_{29} C_{43}^{\delta}\right)^n < \left(C_{27}(H) C_{28} C_{41}^{\delta}\right)^{-1}.$$

However, this latter inequality follows from (3.34) for $n > C_{44}$.

Therefore, by the Quantitative Subspace Theorem 1.5, there exist finitely many nonzero linear forms $\Lambda_1(\mathbf{X}), \ldots, \Lambda_g(\mathbf{X})$ with coefficients in $\overline{K}$ and with

$$g \leq C_{45},$$

such that each vector $\mathbf{x}_n$ is a zero of some Λ_j.

Suppose first Λ_j does not depend on X_0. Then, if $\Lambda_j(\mathbf{x}_n) = 0$, we have a nontrivial relation

$$\sum_{i=1}^{h} u_i \tau_i(n) \gamma_i^n = 0, \quad u_i \in \overline{K}, i = 1, \ldots, h.$$

By Theorem 1.9 this can hold for at most a finite number of n. More precisely, we can conclude that the number of those solutions can be bounded by a constant C_{46}, since the γ_i are nondegenerate.

Suppose that Λ_j depends on X_0 and that $\Lambda_j(\mathbf{x}_n) = 0$. Then we have

$$x_n = \sum_{i=1}^{h} v_i \tau_i(n) \gamma_i^n, \quad v_i \in \overline{K}, i = 1, \ldots, h. \tag{3.35}$$

Substituting this into $f(z, x) = 0$ we get

$$f\left(G_n, \sum_{i=1}^{h} v_i \tau_i(n) \gamma_i^n\right) = 0. \tag{3.36}$$

If the above equation does not hold identically and we have assumed that this is not the case, we can conclude that

$$|\{n | n \text{ satisfies } (3.36)\}| < C_{47}$$

also in this case, because the left hand side of (3.36) defines a nondegenerate linear recurring sequence and the conclusion follows again by Theorem 1.9. Observe that from the assumption that the $\alpha_1, \ldots, \alpha_t$ are multiplicatively independent, we conclude the nondegeneracy.

Then the number of solutions of (3.5) can be bounded by

$$C_2 + \sum_{i=1}^{r} \sum_{j=0}^{e_i - 1} \left[C_{45}(C_{46} + C_{47}) + \max\{C_4, C_{11}, C_{16}, C_{27}, C_{44}\}\right],$$

where the constants in the sum clearly can depend on i, j. This completes the proof. □

3.5 Proof of Theorem 3.2 and the corollaries

Proof of Theorem 3.2.

The proof is the same as the proof of Theorem 3.1, except that we can conclude the degeneracy of H_n and the recurring sequence defined by the left hand side of (3.36) by the fact that the roots $\alpha_1, \ldots, \alpha_t$ of G_n are different positive integers. Therefore possibly the order of the recurrence becomes smaller, but it cannot happen that we get roots which differ by a root of unity different from 1. □

Proof of Corollary 3.2.

This follows readily from Theorem 3.1 in form of Corollary 3.1 and a result, mentioned in the introduction, which is due to Shorey and Stewart [84, Theorem 3]. Let us remark that by Eisenstein's criterion for absolutely irreducibility the polynomials $f(z,x) = x^q - z$ are absolutely irreducible for all q. Moreover, observe that $G_n - \lambda_1\alpha_1^n \neq 0$, because of our assumption $t \geq 2$. □

Proof of Corollary 3.3.

Let d be the degree of α_1 over $\mathbb{Q}$. Using a result of Shorey and Stewart [84, Corollary 1], also mentioned in the introduction, we can conclude that the number of solutions n, x and q with $n \geq 0, |x| > 1$, and

$$q > \max\left(\frac{d\log|\alpha_1|}{\log(|\alpha_1|/\max(1,|\alpha_2|))}, d+r\right)$$

of the equation

$$G_n = x^q + T(x)$$

is finite. It remains to show that the number of solutions n, x and q with $n \geq 0, |x| > 1$ and

$$1 \leq q \leq \max\left(\frac{d\log|\alpha_1|}{\log(|\alpha_1|/\max(1,|\alpha_2|))}, d+r\right)$$

is also finite. But this follows now from our Theorem 3.1. Observe that only for the solutions with small q, an upper bound for the number of solutions can be given. □

3.6 Example

In this section we consider the very special equation

$$2^n x = x^2 + 1, \quad n \neq 0, x \in \mathbb{Z}, \tag{3.37}$$

and we calculate an upper bound for the number of solutions. We have

$$f(z,x) = x^2 - zx + 1 \quad \text{and} \quad G_n = 2^n.$$

This example does not fit perfectly, because $t = 1$, but after all it will show the important steps used in our method. We will use the notations of the proof of Theorem 3.1.

We have already calculated the Puiseux expansions we need. Let us repeat them:

$$x_1 = z - \frac{1}{z} - \frac{1}{z^3} - 2\frac{1}{z^5} + \mathcal{O}\Big(\frac{1}{z^7}\Big), \tag{3.38}$$

$$x_2 = \frac{1}{z} + \frac{1}{z^3} + 2\frac{1}{z^5} + \mathcal{O}\left(\frac{1}{z^7}\right). \tag{3.39}$$

By the Explicit Puiseux's Theorem 3.4 we get the following bound for the coefficients of the above series

$$\Lambda = C_3 = 2^{(3^4)^{3\cdot 2^4}}.$$

Moreover we get $C_2 = 0, C_5 = 1, C_6 = 1, C_7 = 2$.

Let us now consider the solutions (n, x_n), which come from (3.38). We approximate x_n by $H_n = 2^n - 2^{-n}$ with error $C_{27}(H) = 2\Lambda^{H+2}, C_{25} = 0, C_{26} = 1/2$ and $H = 1$, if

$$n > C_{16} = \frac{\log\Lambda}{\log 2} + 1.$$

Next we have to choose $S = \{\infty, 2\}$ and we get $C_{30} = \sqrt{3}, C_{41} = 2\sqrt{3}, C_{43} = 0, C_{39} = 4$. Choosing $\delta = 1/4$ we get, if

$$n > C_{44} = \frac{\log\left((2\sqrt{3})^{1/4}\cdot 4\Lambda^3\right)}{\log\left(2\cdot 4^{-1/4}\right)},$$

for the number of relevant subspaces

$$g \leq \left(2^{540}\cdot 4^{21}\right)^2 \log 4 \log\log 4 + (150\cdot 81\cdot 4)^7(2 + \log\log 2\sqrt{3}) = C_{45}.$$

Last we get

$$C_{46} = e^{14^{16}} \quad \text{and} \quad C_{47} = e^{28^{32}}.$$

In the same way we handle the solutions (n, x_n), which come from (3.39). Here we approximate x_n by $H_n = 2^{-n}$ and therefore choose $H = 1$ as before. Again we have to choose $S = \{\infty, 2\}$ and we get $C_{30} = \sqrt{2}, C_{41} = 2\sqrt{2}, C_{42} = 0, C_{43} = 2$, provided that

$$n > \frac{2\log\Lambda}{\log 2}.$$

We choose $\delta = 1/2$ and get for

$$n > \frac{\log\left(4\Lambda^5\sqrt{2\sqrt{2}}\right)}{\log(8\sqrt{2})}$$

an upper bound for the number of relevant subspaces. Because of the fact that $H_n = 2^{-n}$, we can choose $C_{46} = C_{47} = 0$.

At last we get the following upper bound for the number of solutions (n, x) of (3.37)

$$\left(2^{540} \cdot 4^{21}\right)^2 \log 4 \log\log 4 + (150 \cdot 81 \cdot 4)^7 (2 + \log\log 2\sqrt{3})(e^{14^{16}} + e^{28^{32}}) +$$

$$+ \max\left\{ \frac{\log \Lambda}{\log 2} + 1, \frac{\log\left((2\sqrt{3})^{1/4} \cdot 4\Lambda^3\right)}{\log\left(2 \cdot 4^{-1/4}\right)}, \frac{2 \log \Lambda}{\log 2}, \frac{\log\left(4\Lambda^5 \sqrt{2\sqrt{2}}\right)}{\log(8\sqrt{2})} \right\} < e^{10^{47}},$$

where $\Lambda = 2^{(3^4)^{3 \cdot 2^4}}$.

We can see from this example that we cannot expect the bound to be small. This is also clear from the point of view, that we use quite general estimates for the zero multiplicity of nondegenerate recurring sequences and for the coefficients of Puiseux expansions. Let us remark, that it is easy to show that our equation (3.37) has only the trivial solution $(n, x) = (1, 1)$.

Chapter 4

On the Diophantine equation $G_n(x) = G_m(P(x))$

Let $\mathbf{K}$ be a field of characteristic 0 and let $p, q, G_0, G_1, P \in \mathbf{K}[x], \deg P \geq 1$. Further let the sequence of polynomials $(G_n(x))_{n=0}^{\infty}$ be defined by the second order linear recurring sequence

$$G_{n+2}(x) = p(x)G_{n+1}(x) + q(x)G_n(x), \quad \text{for } n \geq 0.$$

In this chapter we give conditions under which the Diophantine equation $G_n(x) = G_m(P(x))$ has at most $\exp(10^{18})$ many solutions $(n, m) \in \mathbb{Z}^2, n, m \geq 0$. The proof uses a very recent result on S-unit equations over fields of characteristic 0 due to J.-H. Evertse, H. P. Schlickewei and W. M. Schmidt (cf. Theorem 1.7 and [45]). Under the same conditions we present also bounds for the cardinality of the set

$$\{(m, n) \in \mathbb{N} \,|\, m \neq n, \exists\, c \in \mathbf{K}\backslash\{0\} \text{ such that } G_n(x) = c\, G_m(P(x))\}.$$

In the last part we specialize our results to certain families of orthogonal polynomials.

This chapter is identically equal to a joint paper with A. Pethő and R. F. Tichy which is submitted for publication in Monatsh. Math. (cf. [49]).

4.1 Introduction

Let $\mathbf{K}$ denote a field of characteristic 0. There is no loss of generality in assuming that this field is algebraically closed and we will assume this for the rest of the chapter. Let $p, q, G_0, G_1 \in \mathbf{K}[x]$ and let the sequence of polynomials $(G_n(x))_{n=0}^{\infty}$ be defined by the second order linear recurring sequence

$$G_{n+2}(x) = p(x)G_{n+1}(x) + q(x)G_n(x), \quad \text{for } n \geq 0. \tag{4.1}$$

By $\alpha(x), \overline{\alpha}(x)$ we denote the roots of the corresponding characteristic polynomial

$$T^2 - p(x)T - q(x). \tag{4.2}$$

Let $\Delta(x) = p(x)^2 + 4q(x)$ be the discriminant of the characteristic polynomial of the recurring sequence $(G_n)_{n=0}^{\infty}$. Then we have

$$\alpha(x) = \frac{p(x) + \sqrt{\Delta(x)}}{2}, \quad \overline{\alpha}(x) = \frac{p(x) - \sqrt{\Delta(x)}}{2}.$$

We will always assume that the recurring sequence is simple, which means that $\Delta(x) \neq 0$. Then for $n \geq 0$

$$G_n(x) = g_1(x)\alpha(x)^n + g_2(x)\overline{\alpha}(x)^n, \tag{4.3}$$

where

$$g_1(x) = \frac{G_1(x) - G_0(x)\overline{\alpha}(x)}{\alpha(x) - \overline{\alpha}(x)} \quad \text{and} \quad g_2(x) = \frac{G_1(x) - G_0(x)\alpha(x)}{\alpha(x) - \overline{\alpha}(x)}. \tag{4.4}$$

Notice that

$$g_1, g_2 \in \mathbf{K}(x, \sqrt{p(x)^2 + 4q(x)}) = \mathbf{K}(x, \sqrt{\Delta}).$$

In fact we have

$$G_n(x) = \frac{G_1(x) - G_0(x)\overline{\alpha}(x)}{\alpha(x) - \overline{\alpha}(x)}\alpha(x)^n + \frac{G_1(x) - G_0(x)\alpha(x)}{\alpha(x) - \overline{\alpha}(x)}\overline{\alpha}(x)^n.$$

$(G_n(x))_{n=0}^{\infty}$ is called nondegenerate, if the quotient $\overline{\alpha}(x)/\alpha(x)$ is not a root of unity.

Many Diophantine equations involving the recurrence $(G_n(x))_{n=0}^{\infty}$ were studied previously. For example let us consider the equation

$$G_n(x) = s(x), \tag{4.5}$$

where $s(x) \in \mathbf{K}[x]$ is given. We denote by $N(s(x))$ the number of integers n for which (4.5) holds. Schlickewei [78] established an absolute bound for $N(s(x))$, provided that the sequence is nondegenerate and that also $\alpha, \overline{\alpha}$ are not equal to a root of unity. His bound was substantially improved by Beukers and Schlickewei [9] who showed that

$$N(s(x)) \leq 61.$$

In the particular case that not all algebraic functions $g_1(x)/s(x), g_2(x)/s(x), \alpha(x), \overline{\alpha}(x)$ are constants (which is always the case here), Beukers and Tijdemann (cf. Theorem 2 on p. 206 in [10]) showed that

$$N(s(x)) \leq 3.$$

Very recently, Schmidt [82] obtained the remarkable result that for arbitrary nondegenerate complex recurring sequences of order q one has $N(a) \leq C(q)$, where $a \in \mathbb{C}$ and $C(q)$ depends only (and in fact triply exponentially) on q (cf. Theorem 1.9).

Another kind of result is due to Glass, Loxton and van der Poorten [53]. They showed that, if $(G_n(x))_{n=0}^{\infty}$ is nonperiodic and nondegenerate, then there are only finitely many pairs of integers m, n with $m > n \geq 0$ and

$$G_n(x) = G_m(x). \tag{4.6}$$

In a recent paper Dujella and Tichy [35] showed for linear recurring sequences $G_{n+1}(x) = xG_n(x) + BG_{n-1}(x),\ \ G_0(x) = 0,\ \ G_1(x) = 1$ of polynomials with $B \in \mathbb{Z} \backslash \{0\}$ that there does not exist a polynomial $P(x) \in \mathbb{C}[x]$ satisfying

$$G_n(x) = G_m(P(x)) \tag{4.7}$$

(for all $m, n \geq 3, \quad m \neq n$). Applying a general theorem of Bilu and Tichy [12], this result was used to show that the Diophantine equation $G_n(x) = G_m(y)$ has only finitely many solutions in integers n, m, x, y, with $n \neq m$.

It is the aim of this chapter to present suitable extensions of the results (4.5) and (4.7).

4.2 General results

Our first main result is a generalization of (4.6) to the Diophantine equation

$$G_n(x) = G_m(P(x)), \tag{4.8}$$

where $P \in \mathbf{K}[x], \deg P \geq 1$ is arbitrary.

Theorem 4.1. *Let $p, q, G_0, G_1, P \in \mathbf{K}[x]$, $\deg P \geq 1$ and $(G_n(x))_{n=0}^{\infty}$ be defined as above. Assume that the following conditions are satisfied: $2 \deg p > \deg q \geq 0$ and*

$$\begin{aligned} \deg G_1 &> \deg G_0 + \deg p \geq 0, \quad \textit{or} \\ \deg G_1 &< \deg G_0 + \deg q - \deg p. \end{aligned}$$

Then there are at most $\min\{\exp(18^{10}), C(p, q, P)\}$ pairs of integers (n, m) with $n, m \geq 0$ with $n \neq m$ such that

$$G_n(x) = G_m(P(x))$$

holds. We have

$$C(p, q, P) = 10^{28} \cdot \log(2C_1 \deg p) \cdot (4e)^{8C_1 \deg q} \cdot 7^{4C_1 \deg q},$$

where $C_1 = 2(\deg P + 1)$.

Remark 4.1. It is clear that for $m = n$ Theorem 4.1 cannot hold.

Remark 4.2. Let us consider the following example, which shows that all sequences must be excluded, where $\deg G_n(x) = 0$ for all n:

$$\begin{aligned} &G_0(x) = 1, \quad G_1(x) = 1, \\ &G_{n+2}(x) = \frac{1}{2} G_{n+1}(x) + \frac{1}{2} G_n(x). \end{aligned}$$

This means

$$2 \deg p = \deg q = 0 \text{ and } \deg G_0 = \deg G_1 = 0.$$

We have

$$G_n(x) = 1 \quad \forall n.$$

Clearly (4.8) is satisfied for all m, n and all polynomials $P \in \mathbf{K}[x]$.

Remark 4.3. This example shows that also in the polynomial case the condition $2 \deg p > \deg q$ is needed. Assume that

$$\begin{aligned} &G_0(x) = 1, \quad G_1(x) = x, \\ &G_{n+2}(x) = \frac{x}{2} G_{n+1}(x) + \frac{x^2}{2} G_n(x). \end{aligned}$$

Here we have

$$2 \deg p = \deg q = 2 \text{ and } \deg G_0 = 0, \deg G_1 = 1.$$

It follows that

$$G_n(x) = x^n \quad \forall n.$$

In this case the following equation holds

$$G_{2n}(x) = G_n(x^2)$$

for all integers n.

Remark 4.4. Let us consider the Chebyshev polynomials of the first kind, which are defined by

$$T_n(x) = \cos(n \arccos x).$$

It is well known that they satisfy the following second order recurring relation:

$$\begin{aligned} &T_0(x) = 1, \quad T_1(x) = x, \\ &T_{n+2}(x) = 2x T_{n+1}(x) - T_n(x). \end{aligned}$$

In this case we have

$$2\deg p > \deg q \ \text{ and } \ \deg T_1 = \deg T_0 + \deg p = 1.$$

It is also well known and in fact easy to prove that

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

holds for all integers n. This example shows that also the second assumption in Theorem 4.1 is needed.

Actually, it is also possible to give an upper bound for the number of pairs (m,n) with $G_n(x) = c\,G_m(P(x))$, $c \in \mathbf{K}^* = \mathbf{K}\backslash\{0\}$ variable. This means that we can give an upper bound for the cardinality of the set

$$\{(m,n) \in \mathbb{N} \,|\, m \neq n, \exists\, c \in \mathbf{K}^* \text{ such that } G_n(x) = c\,G_m(P(x))\}.$$

(Here c may vary with m, n). In fact, the second part of the upper bound in the last theorem, which depends on the degrees of the polynomials involved, follows from this more general theorem. The bound has the advantage that it is only exponential whereas the absolute bound of Theorem 4.1 is double exponential.

Theorem 4.2. *Let* $p, q, G_0, G_1, P \in \mathbf{K}[x]$*,* $\deg P \geq 1$ *and* $(G_n(x))_{n=0}^{\infty}$ *be defined as above. Assume that the following conditions are satisfied:* $2\deg p > \deg q \geq 0$ *and*

$$\begin{array}{rcl} \deg G_1 & > & \deg G_0 + \deg p \geq 0, \quad \textit{or} \\ \deg G_1 & < & \deg G_0 + \deg q - \deg p. \end{array}$$

Then the number of pairs of integers (n,m) *with* $n, m \geq 0, n \neq m$ *for which there exists* $c \in \mathbf{K}^*$ *with*

$$G_n(x) = c\,G_m(P(x))$$

is at most $C(p,q,P)$*. We have*

$$C(p,q,P) = 10^{28} \cdot \log(2C_1 \deg p) \cdot (4e)^{8C_1 \deg q} \cdot 7^{4C_1 \deg q},$$

where $C_1 = 2(\deg P + 1)$*.*

It is also possible to replace the conditions concerning the degree by algebraic conditions.

Theorem 4.3. *Let* $p, q, G_0, G_1, P \in \mathbf{K}[x]$ *and* $(G_n(x))_{n=0}^{\infty}$ *be defined as above. Assume that*

(1) $\deg \Delta \neq 0$,

(2) $\deg P \geq 2$,

(3) $\gcd(p, q) = 1$ *and*

(4) $\gcd(2G_1 - G_0 p, \Delta) = 1$.

Then there are at most $\min\{\exp(10^{18}), \tilde{C}(p, q, P)\}$ *pairs of integers* (n, m) *with* $n, m \geq 0$ *such that*

$$G_n(x) = G_m(P(x))$$

holds. We have

$$\tilde{C}(p, q, P) = 10^{28} \cdot \log(C_1 \max\{2 \deg p, \deg q\}) \cdot (4e)^{8C_1 \deg q} \cdot 7^{4C_1 \deg q},$$

where $C_1 = 2(\deg P + 1)$.

Remark 4.5. The reason for this different kind of assumptions lie in the fact that the infinite valuation in the rational function field $\mathbf{K}(x)$ leads to degree assumptions, whereas by looking at finite valuations one gets divisibility conditions as in the above theorem.

Remark 4.6. It is obvious that for $\deg P = 1$ Theorem 4.3 cannot hold in full generality. For example: if $G_n(x)$ is a polynomial in x^2 for all n we get

$$G_n(x) = G_n(-x)$$

for all n.

Remark 4.7. By looking at the proof, it is clear that Theorem 4.3 also holds, if we assume instead of (2)

(2′) There is no $c \in \mathbf{K}$ such that $\Delta(P(x)) = c\Delta(x)$ holds.

To our knowledge this is the weakest condition under which our proof works.
It is clear that (2′) holds if $\deg P \geq 2$ or if P is a constant. If $P(x) = x$ then $\Delta(P(x)) = c\Delta(x)$ holds with $c = 1$. Suppose that $P(x) = ax + b$ with $a, b \in \mathbf{K}$ and $a \neq 0$, $(a, b) \neq (1, 0)$. Denote by $P^{(k)}$ the k-th iterate of P. Let Δ_0 be the leading coefficient of $\Delta(x)$. It is left to the reader to show that (2′) does not hold if and only if $a^{\deg \Delta} = c$, a is a root of unity of order $k > 1$ and

$$\Delta(x) = \Delta_0 \Big(x + \frac{b}{a-1}\Big)^s \prod_{i=1}^{r} \prod_{j=0}^{k-1} (x - P^{(j)}(x_i)),$$

where r, s are non-negative integers with $rk + s = \deg \Delta$ and $-\frac{b}{a-1}, x_1, \ldots, x_r$ are distinct elements of $\mathbf{K}$.

Again we can handle the case $G_n(x) = c\,G_m(P(x))$ with $c \in \mathbf{K}^*$ variable under this conditions and actually the second part of the bound of the last theorem follows from this theorem.

Theorem 4.4. *Let* $p, q, G_0, G_1, P \in \mathbf{K}[x]$ *and* $(G_n(x))_{n=0}^{\infty}$ *be defined as above. Assume that the conditions (1)-(4) of Theorem 4.3 are satisfied. Then the number of pairs of integers* (n, m) *with* $n, m \geq 0$ *for which there exists* $c \in \mathbf{K}^*$ *with*

$$G_n(x) = c\,G_m(P(x))$$

is at most $\tilde{C}(p, q, P)$. *We have*

$$\tilde{C}(p, q, P) = 10^{28} \cdot \log(C_1 \max\{2 \deg p, \deg q\}) \cdot (4e)^{8C_1 \deg q} \cdot 7^{4C_1 \deg q},$$

where $C_1 = 2(\deg P + 1)$.

4.3 Results for families of orthogonal polynomials

We will turn now our discussion to sequences of certain orthogonal polynomials satisfying (4.1). The following results can be found in the monograph of Borwein and Erdélyi [13, Chapter 2.3], Chihara [16, Chapter I and II] or Szegő [91, Chapter III]. Let $(\mu_n)_{n=0}^{\infty}$ be a sequence of complex numbers and let $\mathcal{L} : \mathbb{C}[x] \longrightarrow \mathbb{C}$ be linear functional defined by

$$\mathcal{L}[x^n] = \mu_n, \quad n = 0, 1, 2, \ldots.$$

Then $\mathcal{L}$ is called the *moment functional* determined by the formal *moment sequence* (μ_n). The number μ_n is called the *moment of order n*. A sequence $(P_n(x))_{n=0}^{\infty}$ is called an *orthogonal polynomial sequence* (OPS) with respect to a moment functional $\mathcal{L}$ provided that for all nonnegative integers m and n the following conditions are satisfied:

(i) $\deg P_n(x) = n$,

(ii) $\mathcal{L}[P_m(x)P_n(x)] = 0$ for $m \neq n$,

(iii) $\mathcal{L}[P_n^2(x)] \neq 0$.

If there exists an OPS for $\mathcal{L}$, then each $P_n(x)$ is uniquely determined up to an arbitrary nonzero factor. An OPS in which each $P_n(x)$ is monic will be referred to as a *monic* OPS; it is indeed unique.

It is well known that a necessary and sufficient condition for the existence of an OPS for a moment functional $\mathcal{L}$ with moment sequence (μ_n) is that for the determinants defined by

$$\Delta_n = \det(\mu_{i+j})_{i,j=0}^n = \begin{vmatrix} \mu_0 & \mu_1 & \cdots & \mu_n \\ \mu_1 & \mu_2 & \cdots & \mu_{n+1} \\ \vdots & \vdots & \ddots & \vdots \\ \mu_n & \mu_{n+1} & \cdots & \mu_{2n} \end{vmatrix}$$

the following conditions hold

$$\Delta_n \neq 0, \quad n = 0, 1, 2, \ldots .$$

In this case $\mathcal{L}$ is called *quasi-definite.*

A moment functional $\mathcal{L}$ is called *positive-definite* if $\mathcal{L}[\pi(x)] > 0$ for every $\pi(x) \in \mathbb{C}[x]$ that is not identically zero and which satisfies $\pi(x) \geq 0$ for all real x. The following holds: $\mathcal{L}$ is positive-definite if and only if its moments are all real and $\Delta_n > 0$ for all $n \geq 0$. Furthermore, using the Gram-Schmidt process, a corresponding OPS consisting of real polynomials exists. Moreover, $\mathcal{L}$ is positive-definite if and only if a bounded, non-decreasing function ψ exists, whose moments

$$\mu_n = \int_{-\infty}^{\infty} x^n d\psi(x), \quad n = 0, 1, 2, \ldots,$$

are all finite and the set

$$\mathfrak{S}(\psi) = \{x \mid \psi(x+\delta) - \psi(x-\delta) > 0 \text{ for all } \delta > 0\}$$

is infinite. Further for the function ψ

$$\int_{-\infty}^{\infty} x^n d\psi(x) = \mu_n = \mathcal{L}[x^n], \quad n = 0, 1, 2, \ldots$$

is valid. This is known as the representation theorem for positive-definite moment functionals or as the solution to the *Hamburger* moment problem.

Thus, an OPS with respect to a positive-definite moment functional $\mathcal{L}$ induces an inner product defined by

$$\langle p, q \rangle = \mathcal{L}[p(x)\overline{q(x)}], \quad p, q \in \mathbb{C}[x],$$

where $\overline{q(x)}$ is obtained by taking the complex conjugates of the coefficients of $q(x)$, on the linear space of polynomials with complex coefficients. In particular, we have $\langle P_m, P_n \rangle = \mathcal{L}[P_m(x)\overline{P_n(x)}] = 0, \quad m \neq n$. Thus our definition of orthogonality for the OPS is consistent with the usual definition of orthogonality in an inner product space.

One of the most important characteristics of an OPS is the fact that any three consecutive polynomials are connected by a very simply relation: Let $\mathcal{L}$ be a quasi-definite moment functional and let $(P_n(x))_{n=0}^{\infty}$ be the corresponding monic OPS. Then there exist constants c_n and $\lambda_n \neq 0$ such that

$$P_n(x) = (x - c_n)P_{n-1}(x) - \lambda_n P_{n-2}(x), \quad n = 1, 2, 3, \ldots, \tag{4.9}$$

where we define $P_{-1}(x) = 0$. Moreover, if $\mathcal{L}$ is positive-definite, then c_n is real and $\lambda_{n+1} > 0$ for $n \geq 1$ (λ_1 is arbitrary).

The converse is also true and it is referred to as Favard's theorem: Let $(c_n)_{n=0}^{\infty}$ and $(\lambda_n)_{n=0}^{\infty}$ be arbitrary sequences of complex numbers and let $(P_n(x))_{n=0}^{\infty}$ be defined by the recurring formula

$$P_n(x) = (x - c_n)P_{n-1}(x) - \lambda_n P_{n-2}(x), \quad n = 1, 2, 3, \ldots, \tag{4.10}$$
$$P_{-1}(x) = 0, \; P_0(x) = 1. \tag{4.11}$$

Then there is a unique moment functional $\mathcal{L}$ such that

$$\mathcal{L}[1] = \lambda_1, \; \mathcal{L}[P_m(x)P_n(x)] = 0 \text{ for } m \neq n, \; m, n = 0, 1, 2, \ldots.$$

$\mathcal{L}$ is quasi-definite and $(P_n(x))_{n=0}^{\infty}$ is the corresponding monic OPS if and only if $\lambda_n \neq 0$ for all $n \geq 1$, while $\mathcal{L}$ is positive-definite if and only if c_n is real and $\lambda_n > 0$ for all $n \geq 1$.

More generally, let $(P_n(x))_{n=0}^{\infty}$ be a sequence of polynomials in $\mathbb{C}[x]$ satisfying

$$P_n(x) = (A_n x + B_n)P_{n-1}(x) + D_n P_{n-2}(x) \quad (n \geq 1)$$
$$P_{-1}(x) = 0, \; P_0(x) = g \neq 0,$$

where A_n, B_n, D_n are complex numbers with $A_n \neq 0, D_n \neq 0$ for every $n \geq 1$. It follows easily by induction on n that P_n has degree n and that P_n has leading coefficient $k_n = gA_1 \cdots A_n$ for $n \geq 0$. Let $k_{-1} := 1$. For $n \geq -1$ write $P_n(x) = k_n \hat{P}_n(x)$. Thus $\hat{P}_n(x)$ is monic for $n \geq 0$. Further, $\hat{P}_{-1}(x) = 0$, $\hat{P}_1(x) = 1$ and the sequence $(\hat{P}_n(x))_{n=0}^{\infty}$ satisfies (8) with $c_n = -B_n k_{n-1}/k_n = -B_n/A_n$, λ_1 arbitrary and $\lambda_n = -D_n k_{n-2}/k_n = -D_n/A_{n-1}A_n$ for $n \geq 2$. So by Favard's Theorem, $(\hat{P}_n(x))_{n=0}^{\infty}$ is a monic OPS and therefore, $(P_n(x))_{n=0}^{\infty}$ is an OPS for some quasi-definite moment functional $\mathcal{L}$. Moreover, $\mathcal{L}$ is positive definite if $B_n/A_n \in \mathbb{R}$ and $D_n/A_{n-1}A_n < 0$ for $n \geq 2$.

We now consider the special case that $A_1 = e/g$, $B_1 = f/g$, $D_1 = 0$ where $g \neq 0$ and $A_n = a$, $B_n = b$, $D_n = d$ do not depend on n for $n \geq 2$, that is, we consider the sequence of polynomials $(P_n(x))_{n=0}^{\infty}$ with $P_n(x) \in \mathbb{C}[x]$ given by

$$P_{n+1}(x) = (ax + b)P_n(x) + dP_{n-1}(x), \quad n \geq 1, \tag{4.12}$$
$$P_0(x) = g, \; P_1(x) = ex + f, \tag{4.13}$$

where a, b, d, e, f, g are complex numbers with $adeg \neq 0$. By the comments just made this sequence is an OPS for some quasi-definite moment functional $\mathcal{L}$.

In the view of Remark 4.2 it is clear that Theorem 4.1 and Theorem 4.2 cannot hold for all OPS $(P_n(x))_{n=0}^{\infty}$, because the Chebyshev polynomials of the first kind are orthogonal with respect to the positive-definite moment functional

$$\mathcal{L}[\pi(x)] = \int_{-1}^{1} \pi(x)(1-x^2)^{-1/2}dx.$$

Using the same methods as above we will prove the following analogues of Theorems 4.1 and 4.2.

Theorem 4.5. *Let $a, b, d, e, f, g \in \mathbb{C}$, $adeg \neq 0$ and $(P_n(x))_{n=0}^{\infty}$ a sequence of polynomials in $\mathbb{C}[x]$ defined by (4.12) and (4.13). Let $S(x) \in \mathbb{C}[x], \deg S \geq 1$. If we assume that $e = ag$, then there are at most $\min\{\exp(18^{10}), C(S)\}$ pairs of integers (n, m) with $n, m \geq 0$ with $n \neq m$ such that*

$$P_n(x) = P_m(S(x))$$

holds. We have

$$C(S) = 10^{28} \cdot \log(4(\deg S + 1)).$$

Again we can prove the following result concerning the more general equation $P_n(x) = c\,P_m(S(x))$ with some $c \in \mathbb{C}^*$ variable and again the second part of the last theorem follows from this theorem.

Theorem 4.6. *Let $a, b, d, e, f, g \in \mathbb{C}$, $adeg \neq 0$ and $(P_n(x))_{n=0}^{\infty}$ defined by (4.12) and (4.13). Let $S(x) \in \mathbb{C}[x], \deg S \geq 1$ and $e = ag$. Then the number of pairs of integers (n, m) with $n \neq m$ for which there exists $c \in \mathbb{C}^*$ with*

$$P_n(x) = c\,P_m(S(x))$$

is at most $C(S)$. We have

$$C(S) = 10^{28} \cdot \log(4(\deg S + 1)).$$

Remark 4.8. We want to mention that Theorem 4.3 and therefore also Theorem 4.4 can be applied to this situation. The conditions (1) and (3) are trivially satisfied in this case. Condition (4) holds, if $\Delta(x) = p(x)^2 + 4q(x) = (ax+b)^2 + 4d$ and $2P_1(x) - P_0(x)p(x) = 2(ex+f) - g(ax+b) = (2e-ag)x + 2f - bg$ have no common roots. This means that, if $2e = ag, 2f = bg$ does not hold or

$$x = \frac{bg - 2f}{2e - ag}$$

is not a root of $\Delta(x)$, then we get our assertion for all $S(x) \in \mathbb{C}[x], \deg S \geq 2$.

This is satisfied for example if we consider sequences $P_n(x) \in \mathbb{C}[x]$ defined by

$$\begin{aligned} &P_{n+1}(x) = (ax+b)P_n(x) + dP_{n-1}(x), \quad n \geq 1, \\ &P_{-1}(x) = 0, \ P_0(x) = g \neq 0, \end{aligned}$$

where a, b, d, g are complex numbers with $adg \neq 0$.

4.4 Auxiliary results

In this section we collect some important theorems which we will need in our proofs. We need some results from the theory of algebraic function fields, which can be found for example in the monograph of Stichtenoth [90]. We will need the following estimates for the genus of a function field F/K (cf. [90], page 130 and 131).

Theorem 4.7. (Castelnuovo's Inequality) *Let F/K be a function field with constant field K. Suppose there are given two subfields F_1/K and F_2/K of F/K satisfying*

(1) $F = F_1F_2$ is the compositum of F_1 and F_2.

(2) $[F : F_i] = n_i$, and F_i/K has genus g_i $(i = 1, 2)$.

Then the genus g of F/K is bounded by

$$g \leq n_1g_1 + n_2g_2 + (n_1 - 1)(n_2 - 1).$$

In the special case $F_1 = K(x)$ and $F_2 = K(y)$, Castelnuovo's Inequality yields:

Theorem 4.8. (Riemann's Inequality) *Let φ be a non-constant irreducible polynomial in two variables with coefficients in K and suppose that $F = K(x, y)$ with $\varphi(x, y) = 0$. Then we have the following estimate for the genus g of F/K:*

$$g \leq ([F : K(x)] - 1) \cdot ([F : K(y)] - 1).$$

Observe that Riemann's Inequality (and therefore also Castelnuovo's Inequality) is often sharp, and it cannot be improved in general.

Let $\mathbf{K}$ be an algebraically closed field of characteristic 0. Let K be a finite extension of $\mathbf{K}(x)$ where x is transcendental over $\mathbf{K}$. For $\xi \in \mathbf{K}$ define the valuation ν_ξ such that for $Q \in \mathbf{K}(x)$ we have $Q(x) = (x-\xi)^{\nu_\xi(Q)}A(x)/B(x)$ where A, B are polynomials with $A(\xi)B(\xi) \neq 0$. Further, for $Q = A/B$ with $A, B \in \mathbf{K}[x]$ we put $\deg Q := \deg A - \deg B$; thus $\nu_\infty := -\deg$ is a discrete valuation on $\mathbf{K}(x)$. Each of the valuations ν_ξ, ν_∞ can be extended in at most $[K : \mathbf{K}(x)]$ ways to a discrete valuation on K and in this way one obtains all discrete valuations on K. A valuation on K is called finite if it extends ν_ξ for some $\xi \in \mathbf{K}$ and infinite if it extends ν_∞. We choose one of the extensions of ν_∞ to L and denote this by $-\mathrm{ord}$. Thus ord is a function from K to $\mathbb{Q}$ having the properties

$$\begin{array}{ll} \text{(a)} & \mathrm{ord}(Q) = \deg Q \text{ for } Q \in \mathbf{K}[x], \\ \text{(b)} & \mathrm{ord}(AB) = \mathrm{ord}(A) + \mathrm{ord}(B) \text{ for } A, B \in K, \\ \text{(c)} & \mathrm{ord}(A+B) \leq \max\{\mathrm{ord}(A), \mathrm{ord}(B)\} \text{ for } A, B \in K, \\ \text{(d)} & \mathrm{ord}(A+B) = \max\{\mathrm{ord}(A), \mathrm{ord}(B)\} \text{ for } A, B \in K \\ & \qquad\qquad \text{with } \mathrm{ord}(A) \neq \mathrm{ord}(B). \end{array}$$

4.5 Proof of Theorem 4.1

First we reduce the solvability of (4.8) to the solvability of three systems of exponential equations in n, m. We start with a sequence of polynomials $(P_n(x))_{n=0}^\infty$ defined by (4.1). Then, in the sequel $\alpha(x), \overline{\alpha}(x), g_1(x), g_2(x)$ are always be given by (4.3).

Lemma 4.1. *Let $(G_n(x))_{n=0}^\infty$ be a sequence of polynomials defined by (4.1) and let $P \in \mathbf{K}[x], \deg P \geq 1$. Then (4.8) has at most* $\exp(18^9 \cdot 3)$ *solutions $m, n \in \mathbb{Z}, m \neq n$, if $g_1(x), g_2(x) \neq 0$ and which do not satisfy any of the systems:*

$$\begin{cases} g_1(x)\alpha(x)^n + g_2(x)\overline{\alpha}(x)^n = 0 \\ g_1(P(x))\alpha(P(x))^m + g_2(P(x))\overline{\alpha}(P(x))^m = 0 \end{cases} \tag{4.14}$$

$$\begin{cases} g_1(x)\alpha(x)^n = g_1(P(x))\alpha(P(x))^m \\ g_2(x)\overline{\alpha}(x)^n = g_2(P(x))\overline{\alpha}(P(x))^m \end{cases} \tag{4.15}$$

$$\begin{cases} g_2(x)\overline{\alpha}(x)^n = g_1(P(x))\alpha(P(x))^m \\ g_1(x)\alpha(x)^n = g_2(P(x))\overline{\alpha}(P(x))^m \end{cases} \tag{4.16}$$

Proof. First we define

$$K = \mathbf{K}(x, \sqrt{p(x)^2 + 4q(x)}, \sqrt{p(P(x))^2 + 4q(P(x))}).$$

Clearly, K is finitely generated extension field of $\mathbb{Q}$. Furthermore, let Γ be the multiplicative subgroup of $(K^*)^3$ generated by

$$(\alpha(x), \overline{\alpha}(x), 1) \quad \text{and} \quad (\overline{\alpha}(P(x))^{-1}, \overline{\alpha}(P(x))^{-1}, \alpha(P(x))/\overline{\alpha}(P(x))).$$

We consider now for $n \neq m$ the equation $G_n(x) = G_m(P(x))$ and obtain

$$g_1(x)\alpha(x)^n + g_2(x)\overline{\alpha}(x)^n - g_1(P(x))\alpha(P(x))^m - g_2(P(x))\overline{\alpha}(P(x))^m = 0.$$

This yields

$$\frac{g_1(x)}{g_2(P(x))}\frac{\alpha(x)^n}{\overline{\alpha}(P(x))^m} + \frac{g_2(x)}{g_2(P(x))}\frac{\overline{\alpha}(x)^n}{\overline{\alpha}(P(x))^m} - \frac{g_1(P(x))}{g_2(P(x))}\frac{\alpha(P(x))^m}{\overline{\alpha}(P(x))^m} = 1. \tag{4.17}$$

Now we consider the weighted unit equation

$$\frac{g_1(x)}{g_2(P(x))}x_1 + \frac{g_2(x)}{g_2(P(x))}x_2 - \frac{g_1(P(x))}{g_2(P(x))}x_3 = 1 \text{ in } (x_1, x_2, x_3) \in \Gamma. \tag{4.18}$$

According to Theorem 1.7, equation (4.18) has at most $\exp(18^9 \cdot 3)$ solutions if no non-trivial subsum vanishes. By observing that $g_1(x), g_2(x) \neq 0$ this means that (4.17) has at most $\exp(18^9 \cdot 3)$ solutions m, n not satisfying (4.14), (4.15) and (4.16). □

In the next lemma we calculate the order of $\alpha(x)$ and $\overline{\alpha}(x)$ respectively in the function field $K/\mathbf{K}$, where K is defined as in the previous proof. We will assume that

$$\operatorname{ord}(\alpha) \geq \operatorname{ord}(\overline{\alpha}).$$

If this is not satisfied we can achieve this by interchanging $\alpha(x)$ and $\overline{\alpha}(x)$. Then we have:

Lemma 4.2. *Let $(G_n(x))_{n=0}^{\infty}$ be a sequence of polynomials defined by (4.1) and assume that $2\deg p > \deg q \geq 0$. Then*

$$\operatorname{ord}(\alpha) = \deg p, \tag{4.19}$$

$$\operatorname{ord}(\overline{\alpha}) = \deg q - \deg p < \deg p. \tag{4.20}$$

Proof. First assume $\operatorname{ord}(\alpha) = \operatorname{ord}(\overline{\alpha})$. Then by (a), (c), (b) we have

$$\deg p = \operatorname{ord}(\alpha + \overline{\alpha}) \leq \operatorname{ord}(\alpha) = \frac{1}{2}\deg q$$

which is against our assumption. Therefore, $\operatorname{ord}(\alpha) > \operatorname{ord}(\overline{\alpha})$. Now it follows from (a), (d) that $\deg p = \operatorname{ord}(\alpha + \overline{\alpha}) = \operatorname{ord}(\alpha)$. Using (a), (b) and $\alpha(x)\overline{\alpha}(x) = -q(x)$ we then obtain

$$\operatorname{ord}(\overline{\alpha}) = \deg q - \deg p < \deg p.$$

Therefore the proof is finished. □

Next we prove the following lemma.

Lemma 4.3. *Let $(G_n(x))_{n=0}^{\infty}$ be a sequence of polynomials defined by (4.1) and let $P \in \mathbf{K}[x], \deg P \geq 1$. Assume that neither $\alpha(x)/\overline{\alpha}(x)$, nor $\alpha(P(x))/\overline{\alpha}(P(x))$ is a root of unity. We consider the systems of equations*

$$\begin{cases} g_1(x)\alpha(x)^n + g_2(x)\overline{\alpha}(x)^n = 0 \\ g_1(P(x))\alpha(P(x))^m + g_2(P(x))\overline{\alpha}(P(x))^m = 0 \end{cases}$$

The first equation has at most one solution in n, and the second one at most one solution in m.

Proof. This follows from the fact that neither $\alpha(x)/\overline{\alpha}(x)$, nor $\alpha(P(x))/\overline{\alpha}(P(x))$ are roots of unity. In particular, assume that we have two solutions n_1, n_2. Then we obtain

$$-\frac{g_1(x)}{g_2(x)} = \left(\frac{\overline{\alpha}(x)}{\alpha(x)}\right)^{n_1} = \left(\frac{\overline{\alpha}(x)}{\alpha(x)}\right)^{n_2},$$

which implies that $n_1 = n_2$. □

Proof of Theorem 4.1.

First, it is clear that we have

$$\operatorname{ord}(\alpha - \overline{\alpha}) = \deg p.$$

Moreover, the following relations hold

$$\begin{aligned} \operatorname{ord}(\alpha(P)) &= \deg p \ \deg P, \\ \operatorname{ord}(\overline{\alpha}(P)) &= (\deg q - \deg p) \deg P, \\ \operatorname{ord}(\alpha(P) - \overline{\alpha}(P)) &= \deg p \ \deg P. \end{aligned}$$

The important relations

$$g_1(x)(\alpha(x) - \overline{\alpha}(x)) = G_1(x) - G_0(x)\overline{\alpha}(x), \tag{4.21}$$

$$g_2(x)(\overline{\alpha}(x) - \alpha(x)) = G_1(x) - G_0(x)\alpha(x) \tag{4.22}$$

are consequences of (4.4). Observe that under the condition $2\deg p > \deg q \geq 0$ our sequence $(G_n(x))_{n=0}^{\infty}$ is nondegenerate. This follows from the fact that $\alpha(x)^n = \overline{\alpha}(x)^n$ implies ord(α)=ord($\overline{\alpha}$), which by Lemma 4.2 yields a contradiction. The same is true for the quotient $\alpha(P(x))/\overline{\alpha}(P(x))$.

In order to finish our proof, we want to show that $g_1(x), g_2(x) \neq 0$ and that (4.15) and (4.16) have no solutions.

Case 1. $\deg G_1 > \deg G_0 + \deg p$.
In this case we have

$$\begin{aligned} \operatorname{ord}(G_1 - G_0\overline{\alpha}) &= \deg G_1, \\ \operatorname{ord}(G_1 - G_0\alpha) &= \deg G_1. \end{aligned}$$

This implies

$$\begin{aligned} \operatorname{ord}(G_1(P) - G_0(P)\overline{\alpha}(P)) &= \deg G_1 \ \deg P, \\ \operatorname{ord}(G_1(P) - G_0(P)\alpha(P)) &= \deg G_1 \ \deg P. \end{aligned}$$

Therefore we get

$$\begin{aligned}\operatorname{ord}(g_1) &= \deg G_1 - \deg p,\\ \operatorname{ord}(g_2) &= \deg G_1 - \deg p.\end{aligned}$$

Observe that from this we can conclude that $g_1(x), g_2(x) \neq 0$. Now assume that m, n is a solution of (4.15). Then we obtain by calculating the order of both sides of the equations and by using Lemma 4.2

$$(\deg G_1 - \deg p) + n \deg p = (\deg G_1 - \deg p) \deg P + m \deg p \deg P, \quad (4.23)$$

$$\begin{aligned}(\deg G_1 - \deg p) + n(\deg q - \deg p) = (\deg G_1 - \deg p) \deg P + \quad (4.24)\\ +m(\deg q - \deg p) \deg P.\end{aligned}$$

Subtraction yields

$$n(2 \deg p - \deg q) = m(2 \deg p - \deg q) \deg P.$$

By our assumption $2 \deg p > \deg q$ we derive

$$n = m \deg P \ , \quad (4.25)$$

and substituting this in (4.23) implies

$$(\deg G_1 - \deg p) = (\deg G_1 - \deg p) \deg P.$$

But this yields $\deg P = 1$, which by (4.25) gives $m = n$, or $\deg G_1 = \deg p$, leading to a contradiction.

In the same way we conclude that a solution m, n of (4.16) implies

$$\begin{aligned}(\deg G_1 - \deg p) + n \deg p = (\deg G_1 - \deg p) \deg P +\\ +m(\deg q - \deg p) \deg P,\\ (\deg G_1 - \deg p) + n(\deg q - \deg p) = (\deg G_1 - \deg p) \deg P +\\ +m \deg p \deg P.\end{aligned}$$

Again subtraction yields

$$n(2 \deg p - \deg q) = m(\deg q - 2 \deg p) \deg P \ ,$$

and therefore we get $n = -m \deg P$, which contradicts $\deg P \neq 0$.

Case 2. $\deg G_1 < \deg G_0 + \deg q - \deg p$.
Here we have

$$\begin{aligned}\operatorname{ord}(G_1 - G_0\overline{\alpha}) &= \deg G_0 + \deg q - \deg p,\\ \operatorname{ord}(G_1 - G_0\alpha) &= \deg G_0 + \deg p.\end{aligned}$$

Thus

$$\begin{aligned} \operatorname{ord}(g_1) &= \deg G_0 + \deg q - 2\deg p, \\ \operatorname{ord}(g_2) &= \deg G_0. \end{aligned}$$

From this we derive $g_1(x), g_2(x) \neq 0$. We again can conclude by Lemma 4.2 that a solution of (4.15) would imply

$$\begin{aligned} (\deg G_0 + \deg q - 2\deg p) + n\deg p = (\deg G_0 + \deg q - \quad & \quad (4.26) \\ -2\deg p)\deg P + +m\deg p \deg P, & \\ \deg G_0 + n(\deg q - \deg p) = \deg G_0 \deg P + m(\deg q - \deg p)\deg P. & \quad (4.27) \end{aligned}$$

Subtraction yields

$$(n-1)(2\deg p - \deg q) = (m-1)\deg P(2\deg p - \deg q)$$

and therefore

$$(n-1) = (m-1)\deg P.$$

By (4.26) we obtain

$$(\deg G_0 + \deg q - \deg p)(1 - \deg P) = 0.$$

This yields $\deg P = 1$, which again implies $n = m$, or $\deg G_0 + \deg q - \deg p = 0$, which gives $\deg G_1 < 0$, in both cases a contradiction.

Again we get from (4.16)

$$\begin{aligned} (\deg G_0 + \deg q - 2\deg p) + n\deg p &= \deg G_0 \deg P + \\ &\quad +m(\deg q - \deg p)\deg P, \\ \deg G_0 + n(\deg q - \deg p) &= (\deg G_0 + \deg q - 2\deg p)\deg P + \\ &\quad +m\deg p \deg P. \end{aligned}$$

Subtraction gives

$$(n-1) = -(m-1)\deg P,$$

which implies $\deg P = 0$, a contradiction.

Now by Lemma 4.1 we get that (4.8) has at most

$$1 + \exp(18^9 \cdot 3) \leq \exp(18^{10})$$

solutions $n, m \in \mathbb{Z}, n, m \geq 0$ with $m \neq n$. The second part of our upper bound will follow from the proof of Theorem 4.2 where a different proof method is used and thus the proof is finished. □

4.6 Proof of Theorem 4.5

Here $(P_n(x))_{n=0}^{\infty}$ is an OPS and we have in the sense of (4.12) and (4.13)

$$p(x) = ax + b, \;\; q(x) = d.$$

Again we want to apply Lemma 4.1 to show that the equation

$$P_n(x) = P_m(S(x)), \tag{4.28}$$

where $S(x) \in \mathbb{C}[x], \deg S \geq 1$, has only finitely many solutions $m, n \in \mathbb{Z}, m \neq n$. Let $\alpha(x), \overline{\alpha}(x), g_1(x), g_2(x)$ be given by (4.3).

As above we can assume without loss of generality that $\operatorname{ord}(\alpha) \geq \operatorname{ord}(\overline{\alpha})$. By observing $2 \deg p = 2 > 0 = \deg q$, we get by Lemma 4.2 that

$$\operatorname{ord}(\alpha) = 1 \quad \text{and} \quad \operatorname{ord}(\overline{\alpha}) = -1.$$

This yields

$$\begin{aligned} &\operatorname{ord}(\alpha - \overline{\alpha}) = 1, \\ &\operatorname{ord}(P_1 - P_0\overline{\alpha}) = 1. \end{aligned}$$

We have to calculate $\operatorname{ord}(P_1 - P_0\alpha)$. Using that $P_0(x) = g$, $P_1(x) = ex + f$ and the assumption that $e = ag$ we get

$$\begin{aligned} (P_1(x) - P_0(x)\alpha(x))(P_1(x) - P_0(x)\overline{\alpha}(x)) = \\ &= P_1(x)^2 - P_0(x)P_1(x)p(x) - P_0(x)^2q(x) = \\ &= (ex + f)^2 - g(ex + f)(ax + b) - g^2d = sx + t \end{aligned}$$

for certain $s, t \in \mathbb{C}$. By invoking (a), (b) we then obtain

$$\operatorname{ord}(P_1 - P_0\alpha) =: w \leq 1 - \operatorname{ord}(P_1 - P_0\overline{\alpha}) = 0.$$

Observe that Lemma 4.3 can be sharpened in this case. Because of the fact that $\deg P_n = n$ the number of solutions of (4.14) is zero. Furthermore it is clear that $g_1(x), g_2(x)$ cannot be zero in this case, because the following relations hold

$$\begin{aligned} &\operatorname{ord}(g_1) = 0, \\ &\operatorname{ord}(g_2) = w - 1 < 0. \end{aligned}$$

Now assume that $m, n \in \mathbb{Z}, m \neq n$ is a solution of (4.15). Then we get

$$\begin{aligned} &n = m \deg S, \\ &(w - 1) - n = [(w - 1) - m] \deg S. \end{aligned}$$

Consequently $\deg S = 1$, and therefore $m = n$, a contradiction.

In the same way we get for a solution of (4.16), that

$$\begin{aligned}(w-1) - n &= m \deg S,\\ n &= [(w-1) - m] \deg S.\end{aligned}$$

Adding the two equations gives $\deg S = 1$, and thus $n = (w-1) - m$, a contradiction because the left side of the equation is positive and the right side negative.

By Lemma 4.1 the theorem follows and the proof is finished as the second part of the bound will follow from Theorem 4.6. □

4.7 Proof of Theorem 4.3

We start our proof with some useful lemmas.

Lemma 4.4. *Let* $A, B, P \in \mathbf{K}[x]$. *If* $\gcd(A, B) = 1$ *then* $\gcd(A(P), B(P)) = 1$.

This lemma is a special case of a lemma in the monograph of Schinzel [74], page 16. It was originally proved in [73].

We will use the same notations as introduced in the proof of Theorem 4.1. There we calculated the order which was defined as the negative value of some valuation extending $1/x$ from $\mathbf{K}(x)$ to the function field

$$K = \mathbf{K}(x)(\sqrt{\Delta(x)}, \sqrt{\Delta(P(x))})$$

of the elements $g_1(x), g_2(x)$ by using the equations (4.21) and (4.22). Here we want to calculate the valuations $\nu(g_1)$ and $\nu(g_2)$ where ν extends ν_ξ to K for some $\xi \in \mathbf{K}$.

Lemma 4.5. *Let* $(G_n(x))_{n=0}^{\infty}$ *be a sequence of polynomials defined by (4.1) and assume that* $\gcd(2G_1 - G_0p, \Delta) = 1$. *If* ν *is a finite valuations on* K *with* $\nu(\Delta) > 0$ *then* $\nu(g_1\sqrt{\Delta}) = \nu(g_2\sqrt{\Delta}) = 0$.

Proof. We have equation (4.21)

$$g_1(x)(\alpha(x) - \overline{\alpha}(x)) = G_1(x) - G_0(x)\overline{\alpha}(x),$$

which we may rewrite in the form

$$2g_1(x)\sqrt{\Delta(x)} = 2G_1(x) - G_0(x)p(x) + G_0(x)\sqrt{\Delta(x)}.$$

By our assumption that $\gcd(2G_1 - G_0p, \Delta) = 1$ we have that

$$\nu(2G_1 - G_0p) = 0.$$

Because of the fact that

$$\nu(G_0\sqrt{\Delta}) = \nu(G_0) + \frac{1}{2}\nu(\Delta) > 0$$

we get that

$$\nu(g_1\sqrt{\Delta}) = \nu(2g_1\sqrt{\Delta}) = \min\{\nu(2G_1 - G_0 p\}, \nu(G_0\sqrt{\Delta})) = 0$$

which was our assumption.

The same holds for $g_2(x)$ and therefore the proof is finished. □

Assumption (4) of Theorem 4.3 together with Lemma 4.4 imply

$$\gcd(2G_1(P) - G_0(P)p(P), \Delta(P)) = 1.$$

As

$$\begin{aligned} &2g_1(P(x))\sqrt{\Delta(P(x))} = \\ &\quad = 2G_1(P(x)) - G_0(P(x))p(P(x)) + G_0(P(x))\sqrt{\Delta(P(x))} \end{aligned}$$

we have again, as in the proof of the previous lemma, that for a finite valuation ν on K with $\nu(\Delta(P)) > 0$ we have $\nu(g_1\sqrt{\Delta(P)}) = \nu(g_2\sqrt{\Delta(P)}) = 0$.

Proof of Theorem 4.3.

We are intended to prove that the systems of equations (4.15) and (4.16) are not solvable.

Consider for example the equation

$$g_1(x)\alpha(x)^n = g_1(P(x))\alpha(P(x))^m. \tag{4.29}$$

The other equations can be handled analogously.

We have $\deg \Delta(P) = \deg \Delta \deg P > \deg \Delta > 0$, as $\deg P > 1$ by assumption (2). Hence $\Delta(P)$ has a zero ξ such that

$$\nu_\xi(\Delta(P)) > \nu_\xi(\Delta) \geq 0.$$

This implies that there is a finite valuation ν on K such that

$$\nu(g_1(P)) = -\nu(\Delta(P)).$$

Next we want to show that $\nu(\alpha(P)) = 0$. Indeed, as $\nu(\Delta(P)) > 0$ and

$$\alpha(P(x)) = \frac{p(P(x)) + \sqrt{\Delta(P(x))}}{2}$$

we have

$$\nu\left(\alpha(P) - \frac{1}{2}p(P)\right) > 0. \tag{4.30}$$

By assumption (3) of Theorem 4.3 and Lemma 4.4 we have $\gcd(p(P), q(P)) = 1$ which implies $\min\{\nu(p(P)), \nu(q(P))\} = 0$. If $\nu(p(P)) > 0$ then from

$$\nu(\Delta(P)) = \nu(p(P)^2 + 4q(P)) > 0$$

it follows that then also $\nu(q(P)) > 0$ which is impossible. Therefore, $\nu(p(P)) = 0$. Consequently we have $\nu(\alpha(P)) = 0$. In a similar fashion it follows that $\nu(\overline{\alpha}(P)) = 0$.

Thus equation (4.29) implies

$$\nu(g_1) + n\nu(\alpha) = \nu(g_1(P)),$$

which yields

$$n\nu(\alpha) = \nu(g_1(P)) - \nu(g_1) < 0,$$

hence (4.29) has no solution in n, if $\nu(\alpha) \geq 0$ and at most one, if $\nu(\alpha) < 0$.

Studying the second equation of (4.15) we may conclude in the same way that this equation has no solution in n, if $\nu(\overline{\alpha}) \geq 0$ and at most one if $\nu(\overline{\alpha}) < 0$. Thus the system of equations (4.15) may have a solution only if $\nu(\alpha), \nu(\overline{\alpha}) < 0$. Observe that this is impossible since $\alpha(x), \overline{\alpha}(x)$ are integral over $\mathbf{K}[x]$, as they are zeros of the monic equation $T^2 - p(x)T - q(x) = 0$ with coefficients in $\mathbf{K}[x]$. The integral closure of $\mathbf{K}[x]$ in K consists of those elements f such that $\nu(f) \geq 0$ for every finite valuation ν of K. So in particular, $\nu(\alpha) \geq 0, \nu(\overline{\alpha}) \geq 0$. Hence (4.15) has no solution.

The proof of the unsolvability of (4.16) is analogous. It is clear that $g_1(x), g_2(x) \neq 0$ holds, because from assumption (1) we can conclude that there is a zero ζ of $\Delta(x)$, for which we can derive using Lemma 4.5 that $\nu(g_1) < 0$ and $\nu(g_2) < 0$, where ν is a finite valuation extending ν_ζ to K. Consequently they must be different from zero. Since Lemma 4.3 is true also in this case, (because $\alpha(x)/\overline{\alpha}(x)$ and $\alpha(P(x))/\overline{\alpha}(P(x))$ are not roots of unity), we get the assertion of Theorem 4.3 by Lemma 4.1. The second part of the bound will follow from Theorem 4.4. □

4.8 Proof of the Theorems 4.2, 4.4 and 4.6

Again we will use all notations from above. Especially, let $K/\mathbf{K}$ be the algebraic function field in one variable defined by

$$K = \mathbf{K}(x, \sqrt{p(x)^2 + 4q(x)}, \sqrt{p(P(x))^2 + 4q(P(x))}).$$

Moreover, we consider

$$\Gamma = \langle \alpha(x), \overline{\alpha}(x), \alpha(P(x)), \overline{\alpha}(P(x)) \rangle_{(K^*,\cdot)}$$

which means that Γ is the subgroup of $(K^*, \cdot)$ the multiplicative group of K generated by $\alpha(x), \overline{\alpha}(x), \alpha(P(x)), \overline{\alpha}(P(x))$. Now we have the following lemma.

Lemma 4.6. *There exists a finite subset $S \subset M_K$ of valuations of the function field K such that Γ is contained in the group of S-units U_S and such that*

$$|S| \leq 4 \deg q(\deg P + 1) + 4.$$

Proof. Let S_∞ be the set of infinite valuations of K and S_0 the set of finite valuations of K. Note that for every $\nu \in S_0$ we have $\nu(\alpha) \geq 0$, $\nu(\overline{\alpha}) \geq 0$, $\nu(\alpha(P)) \geq 0$, $\nu(\overline{\alpha}(P)) \geq 0$ since these functions are integral over $\mathbf{K}[x]$. Take $S = S_\infty \cup S_1 \cup S_2 \cup S_3 \cup S_4$, where

$$\begin{aligned} S_1 &= \{\nu \in S_0 | \, \nu(\alpha) > 0\}, \\ S_2 &= \{\nu \in S_0 | \, \nu(\overline{\alpha}) > 0\}, \\ S_3 &= \{\nu \in S_0 | \, \nu(\alpha(P)) > 0\}, \\ S_4 &= \{\nu \in S_0 | \, \nu(\overline{\alpha}(P)) > 0\}. \end{aligned}$$

Then clearly Γ is a subgroup of U_S. Since $[K : \mathbf{K}(x)] \leq 4$, we have $|S_\infty| \leq 4$. Further, $\alpha(x) \cdot \overline{\alpha}(x) \cdot \alpha(P(x)) \cdot \overline{\alpha}(P(x)) = q(x) \cdot q(P(x)) =: Q(x)$. Therefore, $S_1 \cup S_2 \cup S_3 \cup S_4 =: S_5 := \{\nu \in S_0 : \nu(Q) > 0\}$. Each of the valuations in S_5 is an extension to K of some valuation ν_ξ on $\mathbf{K}(x)$ corresponding to a zero ξ of $Q(x)$. The polynomial $Q(x)$ has at most $\deg Q = \deg q(\deg P + 1)$ zeros, and for each of these zeros ξ, the valuation ν_ξ can be extended in at most four ways to a valuation on K. Therefore, $|S_5| \leq 4 \deg q(\deg P + 1)$. This implies Lemma 8. □

Next we want to estimate the genus of the function field $K/\mathbf{K}$. This can be done using Castelnuovo's Inequality (Theorem 4.7).

Lemma 4.7. *We denote by g the genus of the function field $K/\mathbf{K}$. Then we have*

$$g \leq 2 \max\{2 \deg p, \deg q\}(\deg P + 1) - 3.$$

Proof. First observe that we have

$$F = \mathbf{K}(x, \sqrt{\Delta(x)}, \sqrt{\Delta(P(x))}) = \mathbf{K}(x, \sqrt{\Delta(x)}) \cdot \mathbf{K}(x, \sqrt{\Delta(P(x))}).$$

Let us denote $F_1 = \mathbf{K}(x, \sqrt{\Delta(x)}), F_2 = \mathbf{K}(x, \sqrt{\Delta(P(x))})$. Thus we have

$$F_1 = \mathbf{K}(x, y), \quad \varphi_1(x, y) = y^2 - \Delta(x) = 0$$

and

$$F_2 = \mathbf{K}(x, y), \quad \varphi_2(x, y) = y^2 - \Delta(P(x)) = 0.$$

Furthermore we denote by g_i the genus of $F_i/\mathbf{K}$ $(i = 1, 2)$. We have

$$n_1 = [F : F_1] \leq 2 \quad \text{and} \quad n_2 = [F : F_2] \leq 2.$$

By Riemann's Inequality (Theorem 4.8) we get the following estimates:

$$\begin{aligned} g_1 &\leq ([F_1 : \mathbf{K}(x)] - 1) \cdot ([F_1 : \mathbf{K}(y)] - 1) \leq \deg \Delta - 1, \\ g_2 &\leq ([F_2 : \mathbf{K}(x)] - 1) \cdot ([F_2 : \mathbf{K}(y)] - 1) \leq \deg \Delta \, \deg P - 1. \end{aligned}$$

Since $\Delta(x) = p(x)^2 + 4q(x)$ we have $\deg \Delta \leq \max\{2 \deg p, \deg q\}$. Now using Castelnuovo's Inequality (Theorem 4.7) we get

$$g \leq 2(\deg \Delta - 1) + 2(\deg \Delta \deg P - 1) + 1 = 2 \deg \Delta(\deg P + 1) - 3,$$

and therefore our proof is finished. □

Finally, we need the following lemma.

Lemma 4.8. *Assume* $2 \deg p > \deg q \geq 0$ *or* $\gcd(p, q) = 1$ *and* p, q *not both in* $\mathbf{K}$. *Let* γ_1, γ_2 *be nonzero elements of* K. *Then there is at most one pair of integers* n, m *such that*

$$\gamma_1 \frac{\alpha(x)^n}{\overline{\alpha}(P(x))^m} \in \mathbf{K}^* \quad \text{and} \quad \gamma_2 \frac{\overline{\alpha}(x)^n}{\overline{\alpha}(P(x))^m} \in \mathbf{K}^* \tag{4.31}$$

or

$$\gamma_1 \frac{\alpha(x)^n}{\overline{\alpha}(P(x))^m} \in \mathbf{K}^* \quad \text{and} \quad \gamma_2 \frac{\alpha(P(x))^m}{\overline{\alpha}(P(x))^m} \in \mathbf{K}^* \tag{4.32}$$

or

$$\gamma_1 \frac{\overline{\alpha}(x)^n}{\overline{\alpha}(P(x))^m} \in \mathbf{K}^* \quad \text{and} \quad \gamma_2 \frac{\alpha(P(x))^m}{\overline{\alpha}(P(x))^m} \in \mathbf{K}^*, \tag{4.33}$$

respectively.

Proof. First we prove equation (4.31). Suppose there are two such pairs (n_1, m_1), (n_2, m_2). Let $n = n_1 - n_2$, $m = m_1 - m_2$. Then $(\gamma_1/\gamma_2)(\alpha(x)/\overline{\alpha}(x))^{n_i} \in \mathbf{K}^*$ for $i = 1, 2$, hence $(\alpha(x)/\overline{\alpha}(x))^n \in \mathbf{K}^*$. Suppose $n \neq 0$. Then $\alpha(x)/\overline{\alpha}(x) \in \mathbf{K}^*$. Using $p(x) = \alpha(x) + \overline{\alpha}(x)$, $q(x) = \alpha(x) \cdot \overline{\alpha}(x)$ it follows that $p(x) = c_1\alpha(x)$, $q(x) = c_2\alpha(x)^2$ with $c_1, c_2 \in \mathbf{K}^*$ and so $p(x)^2 = c_3 q(x)$ with $c_3 \in \mathbf{K}^*$. But this contradicts both $2 \deg p > \deg q \geq 0$ and $\gcd(p, q) = 1$. It follows that $n = 0$, whence $n_1 = n_2$ and so $(n_1, m_1) = (n_2, m_2)$. This proves the first part of the lemma.

Now we consider equation (4.32). As above we assume that there are two such pairs. Hence we get $(\alpha(P(x))/\overline{\alpha}(P(x)))^m \in \mathbf{K}^*$. This implies that either $\alpha(P(x))/\overline{\alpha}(P(x)) \in \mathbf{K}^*$ which is impossible by the same arguments as above or $m = 0$. But now, using the other expression in (4.32) we get that also $n = 0$ must hold. Consequently we have $(n_1, m_1) = (n_2, m_2)$. So we proved the second part of our lemma.

The arguments for (4.33) are the same as for (4.32). This proves the lemma also in the third case. □

Assume that n, m are integers satisfying $G_n(x) = c\,G_m(P(x))$ for some $c \in \mathbf{K}^*$. It follows that

$$\beta_1 x_1 + \beta_2 x_2 + \beta_3 x_3 = 1$$

where

$$\beta_1 := \frac{g_1(x)}{g_2(P(x))},\ \beta_2 := \frac{g_2(x)}{g_2(P(x))},\ \beta_3 := -\frac{g_1(P(x))}{g_2(P(x))}, \tag{4.34}$$
$$x_1 = c^{-1}\frac{\alpha(x)^n}{\overline{\alpha}(P(x))^m},\ x_2 = c^{-1}\frac{\overline{\alpha}(x)^n}{\overline{\alpha}(P(x))^m},\ x_3 = \frac{\alpha(P(x))^m}{\overline{\alpha}(P(x))^m}.$$

Observe that x_1, x_2, x_3 are elements of the set U_S which exists by Lemma 4.6. This is because of fact that Γ is contained in U_S and $c \in \mathbf{K}^*$. Lemma 4.8 implies that any given pair of elements (x_i, x_j) gives rise to at most one pair (n, m), especially any triple (x_1, x_2, x_3) induces at most one solution (n, m) of the equation in consideration.

By Theorem 1.15, either $\beta_1 x_1, \beta_2 x_2, \beta_3 x_3$ all belong to $\mathbf{K}^*$, which by Lemma 4.8 is possible for at most one pair (n, m), or (x_1, x_2, x_3) lies in one of at most $\log(g + 2) \cdot (4e)^{4s+2}$ proper linear subspaces of K^3, where s denotes the cardinality of the set of valuations S introduced by Lemma 4.8. That is, (x_1, x_2, x_3) satisfies one of at most $\log(g + 2)(4e)^{4s+2}$ relations of the shape

$$\gamma_1 x_1 + \gamma_2 x_2 + \gamma_3 x_3 = 0 \tag{4.35}$$

with $(\gamma_1, \gamma_2, \gamma_3)$ a nonzero triple in K^3. Assume for the moment that $\gamma_i \neq 0$ for $i = 1, 2, 3$ and write $\Delta_{ij} = \gamma_j^{-1}(\beta_i\gamma_j - \beta_j\gamma_i)$. Assume for the moment also that all Δ_{ij} are nonzero. Then we have

$$\Delta_{13}x_1 + \Delta_{23}x_2 = 1, \quad \Delta_{12}x_1 + \Delta_{32}x_3 = 1, \quad \Delta_{21}x_2 + \Delta_{31}x_3 = 1.$$

In fact it suffices to consider one of these equation for example the first one

$$\Delta_{13}x_1 + \Delta_{23}x_2 = 1.$$

Lemma 4.8 implies that there is at most one pair (n, m) such that both quantities $\Delta_{13}x_1$ and $\Delta_{23}x_2$ belong to $\mathbf{K}$. Theorem 1.16 implies that there are at most $2 \cdot 7^{2s}$ pairs (x_1, x_2) such that at least one of these quantities does not belong to $\mathbf{K}$. It follows that there are at most $1 + 2 \cdot 7^{2s}$ pairs (n, m) for which $\gamma_1 x_1 + \gamma_2 x_2 + \gamma_3 x_3 = 0$.

Next, we handle the case that one of the Δ_{ij}, where $(i, j) = (1, 3)$ or $(2, 3)$, is zero. We assume that all $\gamma_i \neq 0$ for $i = 1, 2, 3$. It is clear that $\Delta_{ij} = 0$ implies also $\Delta_{ji} = 0$. Moreover, we remark that if $\Delta_{ij} = 0$ then neither $\Delta_{ik} = 0$ nor $\Delta_{jk} = 0$ where $\{i, j, k\} = \{1, 2, 3\}$ can hold. Because assume that $\Delta_{ij} = 0$ and $\Delta_{ik} = 0$. This implies that also $\Delta_{jk} = 0$ which means that all the quantities $\Delta_{13}, \dots, \Delta_{31}$ are zero. Hence we would get

$$\beta_1 x_1 + \beta_2 x_2 + \beta_3 x_3 = (\gamma_1 x_1 + \gamma_2 x_2 + \gamma_3 x_3)\left(\frac{\beta_3}{\gamma_3}\right) = 1,$$

a contradiction to equation (4.35). From this discussion it follows that $\Delta_{ij} = 0$ for $(i,j) = (1,3)$ or $(2,3)$ implies that we have

$$\Delta_{ik} x_i + \Delta_{jk} x_j = 1,$$

with nonzero Δ_{ik}, Δ_{jk} and $\{i,j,k\} = \{1,2,3\}$. As above, Theorem 1.16 implies that there are at most $2 \cdot 7^{2s}$ pairs (x_i, x_j) such that at least one of these quantities does not belong to $\mathbf{K}$ which can happen for at most one pair (n,m) by Lemma 4.8.

Finally, we handle the case that $\gamma_i = 0$ for some $i = 1,2,3$. Observe that at most one of the γ_i can be zero. Now we assume that $\gamma_1 = 0$. Then (4.35) becomes

$$\gamma_2 x_2 + \gamma_3 x_3 = 0.$$

Therefore we have

$$\beta_1 x_1 + \left(\beta_3 - \frac{\gamma_3}{\gamma_2}\beta_2\right) x_3 = 1.$$

From here we can deduce that there are at most $1 + 2 \cdot 7^{2s}$ pairs of solutions (n,m) under the condition that $\beta_3 - (\gamma_3/\gamma_2)\beta_2 \neq 0$. If this condition is not satisfied then we have

$$\beta_1 x_1 = 1 \quad \text{and} \quad \beta_2 x_2 + \beta_3 x_3 = 0$$

which means that (4.34) has a vanishing subsum. The cases $\gamma_2 = 0$ and $\gamma_3 = 0$ are totally analogous. We get in both cases that there are at most $1 + 2 \cdot 7^{2s}$ pairs of solutions (n,m), if we assume that (4.34) has no vanishing subsum.

The cases for vanishing subsums of equation (4.34) can be rewritten in the following form:

$$\begin{cases} g_1(x)\alpha(x)^n = c\, g_2(P(x))\overline{\alpha}(P(x))^m \\ g_2(x)\overline{\alpha}(x)^n = c\, g_1(P(x))\alpha(P(x))^m \end{cases}$$

$$\begin{cases} g_2(x)\overline{\alpha}(x)^n = c\, g_2(P(x))\overline{\alpha}(P(x))^m \\ g_1(x)\alpha(x)^n = c\, g_1(P(x))\alpha(P(x))^m \end{cases}$$

$$\begin{cases} g_1(x)\alpha(x)^n + g_2(x)\overline{\alpha}(x)^n = 0 \\ g_1(P(x))\alpha(P(x))^m + g_2(P(x))\overline{\alpha}(P(x))^m = 0 \end{cases}$$

But these three equations are up to the constant c totally the same as in the proof of Theorem 4.1, 4.3 and 4.5 . Because of the fact that we have shown the unsolvability of the first and second of the above systems by calculating the valuation at some finite or infinite valuation in our function field K and the fact that for every valuation on K we have

$$\nu(c) = 0,$$

we get that the third system has at most one solution in (n, m), where the second and the third systems do not have a solution at all.

Altogether we get for the number of pairs (n, m) of integers with $n \neq m$ such that there exists a $c \in \mathbf{K}^*$ with $G_n(x) = c\, G_m(P(x))$ the upper bound

$$1 + \log(g+2)(4e)^{4s+2} \cdot \left[7 + 12 \cdot 7^{2s}\right] \leq \log(g+2)(4e)^{4s+2} 7^{2s+2}.$$

Now using the estimation for the genus of our function field (Lemma 4.7) and the estimate for the cardinality of the set S (Lemma 4.8) we get that the number of solutions can be bounded by

$$\begin{aligned} C(p,q,P) = \tilde{C}(p,q,P) &= \log(2\max\{2\deg p, \deg q\}(\deg P + 1)) \cdot \\ &\cdot (4e)^{16 \deg q (\deg P+1)+18} 7^{8 \deg q (\deg P+1)+10}. \end{aligned}$$

Last observe that in Theorem 4.2 we have assumed that $2\deg p > \deg q$ and in Theorem 4.6 we have

$$p(x) = ax + b \quad \text{and} \quad q(x) = d,$$

consequently we know that $\deg q = 0$ and $\deg p = 1$. This proves the bounds as claimed.

□

Chapter 5

On the equation $G_n(x) = G_m(P(x))$ for third order linear recurring sequences

Let $\mathbf{K}$ be a field of characteristic 0 and let $a, b, c, G_0, G_1, G_2, P \in \mathbf{K}[x], \deg P \geq 1$. Further let the sequence of polynomials $(G_n(x))_{n=0}^{\infty}$ be defined by the third order linear recurring sequence

$$G_{n+3}(x) = a(x)G_{n+2}(x) + b(x)G_{n+2}(x) + c(x)G_n(x), \quad \text{for } n \geq 0.$$

In this chapter we give conditions under which the Diophantine equation

$$G_n(x) = G_m(P(x))$$

has at most $\exp(10^{24})$ many solutions $(n, m) \in \mathbb{Z}^2, n, m \geq 0$. The proof uses a very recent result on S-unit equations over fields of characteristic 0 due to J.-H. Evertse, H. P. Schlickewei and W. M. Schmidt (cf. Theorem 1.7 and [45]).

This chapter is identically equal to a manuscript which is a joint work with A. Pethő and R. F. Tichy [50]. This paper is a continuation of the work of the authors on this equation in the case of second order linear recurring sequences (cf. Chapter 4 and [49]).

5.1 Introduction

Let $\mathbf{K}$ denote a field of characteristic 0. There is no loss of generality in assuming that this field is algebraically closed and we will assume this for the rest of the chapter. Let $a, b, c, G_0, G_1, G_2 \in \mathbf{K}[x]$ and let the sequence of polynomials $(G_n(x))_{n=0}^{\infty}$ be defined by the third order linear recurring sequence

$$G_{n+3}(x) = a(x)G_{n+2}(x) + b(x)G_{n+1}(x) + c(x)G_n(x), \quad \text{for } n \geq 0. \tag{5.1}$$

By $\alpha_1(x), \alpha_2(x), \alpha_3(x)$ we denote the roots of the corresponding characteristic polynomial

$$T^3 - a(x)T^2 - b(x)T - c(x). \tag{5.2}$$

Setting $S = T - \frac{1}{3}a(x)$ the characteristic polynomial becomes

$$S^3 - p(x)S - q(x),$$

where

$$p(x) = \frac{1}{3}a(x)^2 + b(x), \quad q(x) = \frac{2}{27}a(x)^3 + \frac{1}{3}a(x)b(x) + c(x).$$

Let

$$\begin{aligned} D(x) = \left(\frac{q(x)}{2}\right)^2 - \left(\frac{p(x)}{3}\right)^3 = \\ = \frac{1}{27}a(x)^3c(x) - \frac{1}{108}a(x)^2b(x)^2 + \frac{1}{6}a(x)b(x)c(x) + \frac{1}{4}c(x)^2 - \frac{1}{27}b(x)^3. \end{aligned}$$

Moreover, let

$$u(x) = \sqrt[3]{\frac{q(x)}{2} + \sqrt{D(x)}}, \quad v(x) = \sqrt[3]{\frac{q(x)}{2} - \sqrt{D(x)}}.$$

Then we have by Cardano's formulae

$$\alpha_1(x) = u(x) + v(x) + \frac{1}{3}a(x), \tag{5.3}$$

$$\alpha_2(x) = -\frac{u(x)+v(x)}{2} + i\sqrt{3}\frac{u(x)-v(x)}{2} + \frac{1}{3}a(x) \quad \text{and} \tag{5.4}$$

$$\alpha_3(x) = -\frac{u(x)+v(x)}{2} - i\sqrt{3}\frac{u(x)-v(x)}{2} + \frac{1}{3}a(x). \tag{5.5}$$

We will always assume that the sequence $(G_n(x))_{n=0}^{\infty}$ is simple which means $D(x) \neq 0$. Then, for $n \geq 0$

$$G_n(x) = g_1(x)\alpha_1(x)^n + g_2(x)\alpha_2(x)^n + g_3(x)\alpha_3(x)^n, \tag{5.6}$$

where

$$g_1(x), g_2(x), g_3(x) \in \mathbf{K}(i\sqrt{3})(x, \sqrt{D(x)}, u(x), v(x)).$$

$(G_n(x))_{n=0}^{\infty}$ is called nondegenerate, if no quotient $\alpha_i(x)/\alpha_j(x), 1 \leq i < j \leq 3$ is equal to a root of unity and degenerate otherwise.

Many Diophantine equations involving the recurrence $(G_n(x))_{n=0}^{\infty}$ were studied previously. For example let us consider the equation

$$G_n(x) = s(x), \tag{5.7}$$

where $s(x) \in \mathbf{K}[x]$ is given. We denote by $N(s(x))$ the number of integers n for which (5.7) holds. Schlickewei [78] established an absolute bound for $N(s(x))$, provided that the sequence is nondegenerate and that also $\alpha_1\alpha_2, \alpha_3$ are not equal to a root of unity. His bound was substantially improved by Beukers and Schlickewei [9] who showed that

$$N(s(x)) \leq 61.$$

Very recently, Schmidt [80] obtained the remarkable result that for arbitrary nondegenerate complex recurrence sequences of order q one has $N(a) \leq C(q)$, where $a \in \mathbb{C}$ and $C(q)$ depends only (and in fact triply exponentially) on q (cf. Theorem 1.9).

Recently, the Pethő, Tichy and the author used new developments on S-unit equations over fields of characteristic 0 due to Evertse, Schlickewei and Schmidt (cf. Theorem 1.7 and [45]) to handle the equation $G_n(x) = G_m(P(x))$ for sequences $(G_n(x))_{n=0}^{\infty}$ of polynomials satisfying a second order linear recurring sequence (see Chapter 4). The result was: Let $p, q, G_0, G_1, P \in \mathbf{K}[x]$, $\deg P \geq 1$ and $(G_n(x))_{n=0}^{\infty}$ be defined by the second order linear recurrence

$$G_{n+2}(x) = p(x)G_{n+1}(x) + q(x)G_n(x), \quad n \geq 0.$$

Assume that the following conditions are satisfied: $2\deg p > \deg q \geq 0$ and

$$\begin{aligned} \deg G_1 &> \deg G_0 + \deg p \geq 0, \quad \text{or} \\ \deg G_1 &< \deg G_0 + \deg q - \deg p. \end{aligned}$$

Then there are at most $\exp(10^{18})$ pairs of integers (n, m) with $n, m \geq 0$ with $n \neq m$ such that

$$G_n(x) = G_m(P(x))$$

holds. They showed a second result in their paper: Let $\Delta(x) = p(x)^2 + 4q(x)$. Assume that

(1) $\deg \Delta \neq 0$,

(2) $\deg P \geq 2$,

(3) $\gcd(p, q) = 1$ and

(4) $\gcd(2G_1 - G_0 p, \Delta) = 1$.

Then there are at most $\exp(10^{18})$ pairs of integers (n, m) with $n, m \geq 0$ such that

$$G_n(x) = G_m(P(x))$$

holds.

The motivation for this equation was the following observation which shows that the problem is non-trivial: Consider the Chebyshev polynomials of the first kind, which are defined by

$$T_n(x) = \cos(n \arccos x).$$

It is well known that they satisfy the following second order recurring relation:

$$\begin{aligned} &T_0(x) = 1, \quad T_1(x) = x, \\ &T_{n+2}(x) = 2xT_{n+1}(x) - T_n(x). \end{aligned}$$

It is also well known and in fact easy to prove that

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

This example shows that at least some conditions are needed to exclude this case.

It is the aim of this chapter to present suitable extensions of the above results for third order linear recurrences.

5.2 General results

Our first main result is a suitable analog of Theorem 1 in [49] (cf. Theorem 4.1) for the number of solutions of

$$G_n(x) = G_m(P(x)) \tag{5.8}$$

for third order linear recurring sequence $(G_n(x))_{n=0}^{\infty}$.

Theorem 5.1. *Let $a, b, c, G_0, G_1, G_2, P \in \mathbf{K}[x]$, $\deg P \geq 1$ and $(G_n(x))_{n=0}^{\infty}$ be defined as above. Assume that the following conditions are satisfied: $3 \deg a > \deg c \geq 0, 2 \deg a > \deg b$ and $\deg a + \deg c > 2 \deg b$. Moreover, assume*

$$\begin{aligned} \deg G_2 &> \deg G_1 + \deg a \geq 0, \quad \textit{and} \\ \deg G_1 &> \deg G_0 + \frac{1}{2}(\deg c - \deg a). \end{aligned}$$

Then there are at most $\exp(10^{24})$ pairs of integers (n, m) with $n, m \geq 0$ with $n \neq m$ such that

$$G_n(x) = G_m(P(x))$$

holds.

Remark 5.1. We can also assume that

$$\begin{aligned}\deg G_2 &< \deg G_1 + \deg a, \quad \text{and}\\ \deg G_1 &< \deg G_0 + \frac{1}{2}(\deg c - \deg a).\end{aligned}$$

instead of the conditions concerning the initial polynomials of the recurrence in the above theorem.

The case $a(x) = 0$ is excluded by the conditions in Theorem 5.1. This special case is handled in the following theorem.

Theorem 5.2. *Let $b, c, G_0, G_1, G_2, P \in \mathbf{K}[x]$, $\deg P \geq 1$ and $(G_n(x))_{n=0}^{\infty}$ be defined by*

$$G_{n+3}(x) = b(x)G_{n+1}(x) + c(x)G_n(x), \quad \textit{for} \quad n \geq 0.$$

Assume that the following conditions are satisfied: $3\deg b > 2\deg c \geq 0$ and

$$\begin{aligned}\deg G_2 &> \deg G_1 + 2\deg b \geq 0, \quad \textit{and}\\ \deg G_1 &> \deg G_0 + 2\deg b - \deg c.\end{aligned}$$

Then there are at most $\exp(10^{24})$ pairs of integers (n, m) with $n, m \geq 0$ with $n \neq m$ such that

$$G_n(x) = G_m(P(x))$$

holds.

Remark 5.2. Observe that the conditions in this special case are quite similar to those for second order linear recurring sequences proved in [49] and mentioned in the introduction.

It is also possible to replace the conditions concerning the degree by algebraic conditions.

Theorem 5.3. *Let $a, b, c, G_0, G_1, G_2, P \in \mathbf{K}[x]$ and $(G_n(x))_{n=0}^{\infty}$ be defined as above. Assume that*

(1) $\deg D \neq 0, \deg q \neq 0$

(2) $\deg P \geq 2$,

(3) $\gcd(c, D) = 1, \gcd(p, q) = 1$,

(4) $\gcd(G_2 - \frac{2}{3}aG_1 - \frac{2}{9}a^2G_0 - bG_0, q) = 1, \gcd(G_2^2 - \frac{4}{3}bG_2G_0 - \frac{1}{3}bG_1^2 + \frac{4}{9}b^2G_0^2, D) = 1$ *and*

(5) $\gcd(a, 27c^2 - 4b^3) > 1$.

Then there are at most $\exp(10^{24})$ *pairs of integers* (n, m) *with* $n, m \geq 0$ *such that*

$$G_n(x) = G_m(P(x))$$

holds.

Remark 5.3. The reason for this different kind of assumptions lie in the fact that the infinite valuation in the rational function field $\mathbf{K}(x)$ leads to degree assumptions, whereas by looking at finite valuations one gets divisibility conditions as in the above theorem.

In this case $a(x) = 0$ is included in the above theorem. Let us mention it as a corollary.

Corollary 5.1. *Let* $b, c, G_0, G_1, G_2, P \in \mathbf{K}[x]$ *and* $(G_n(x))_{n=0}^{\infty}$ *be defined by*

$$G_{n+3}(x) = b(x)G_{n+1}(x) + c(x)G_n(x), \quad \textit{for} \quad n \geq 0.$$

Assume that

(1) $\deg D \neq 0, \deg c \neq 0$

(2) $\deg P > 1$,

(3) $\gcd(b, c) = 1$,

(4) $\gcd(G_2 - bG_0, c) = 1$, *and* $\gcd(G_2^2 - \frac{4}{3}bG_2G_0 - \frac{1}{3}bG_1^2 + \frac{4}{9}b^2G_0^2, D) = 1$,

where $D(x) = (c(x)/2)^2 - (b(x)/3)^3$. *Then there are at most* $\exp(10^{24})$ *pairs of integers* (n, m) *with* $n, m \geq 0$ *such that*

$$G_n(x) = G_m(P(x))$$

holds.

Again we want to remark that this condition are quite similar to those obtained in the case of second order linear recurring sequences [49] (see Theorem 4.3).

5.3 Auxiliary results

In this section we collect some important theorems which we will need in our proofs.

Let $\mathbf{K}$ be an algebraically closed field of characteristic 0, $n \geq 1$ an integer, $\alpha_1, \ldots, \alpha_n$ elements of $\mathbf{K}^* = \mathbf{K} \backslash \{0\}$ and Γ a finitely generated multiplicative subgroup of $\mathbf{K}^*$. A solution $(x_1, \ldots, x_n)$ of the so called *weighted unit equation*

$$\alpha_1 x_1 + \cdots + \alpha_n x_n = 1 \text{ in } x_1, \ldots, x_n \in \Gamma \tag{5.9}$$

is called *nondegenerate* if

$$\sum_{j \in J} \alpha_j x_j \neq 0 \text{ for each non-empty subset } J \text{ of } \{1, \ldots, n\} \tag{5.10}$$

and *degenerate* otherwise. It is clear that if Γ is infinite and if (5.9) has a degenerate solution then (5.9) has infinitely many degenerate solutions. For the nondegenerate solutions we have Theorem 1.7, which is due to Evertse, Schlickewei and Schmidt [45]. It is sufficient for us to state their result for finite type subgroups of $\mathbb{C}^*$ (cf. [45] and [43, Theorem 2] for the following version). First, we remark that Γ is called a *finite type* subgroup of $\mathbb{C}^* = \mathbb{C} \backslash \{0\}$ if it has a free subgroup Γ_0 of finite rank such that Γ / Γ_0 is a torsion group; the *rank* of Γ is then defined as the rank of Γ_0.

Theorem 5.4. (Evertse, Schlickewei and Schmidt) *Let Γ be a finite type subgroup of $\mathbb{C}^*$ of rank r and $\alpha_1, \ldots, \alpha_n \in \mathbb{C}^*$. Then the number of nondegenerate solutions of the equation*

$$\alpha_1 x_1 + \ldots + \alpha_n x_n = 1 \quad \textit{in} \quad x_1, \ldots, x_n \in \Gamma$$

is at most

$$\exp((6n)^{3n}(r+1)).$$

This theorem is a special case of the Main Theorem on S-unit equations over fields with characteristic 0. It is a generalization of earlier results due to Evertse and Győry [41], Evertse [38] and van der Poorten and Schlickewei [72] on the finiteness of the number of nondegenerate solutions of (5.9). For a general survey on these equations and their applications we refer to Chapter 1.2.

In the special case $n = 2$ a much better result is known due to Baker [5] and to Beukers and Schlickewei (cf. [9] and [43, Theorem F]).

Theorem 5.5. (Beukers and Schlickewei) *Let Γ be a finite type subgroup of $\mathbb{C}^*$ of rank r and $a, b \in \mathbb{C}^*$. Then the equation*

$$ax + by = 1 \quad \textit{in} \quad x, y \in \Gamma$$

has at most

$$2^{16(r+1)}$$

solutions.

This result is comparable to Evertse's upper bound 3×7^{4s} for the case $\Gamma = \mathcal{O}_S^*$ the ring of S-integers, where S has cardinality s (cf. [40]).

5.4 Reduction to a system of equations

We start with a sequence of polynomials $(P_n(x))_{n=0}^{\infty}$ defined by (5.1). Then, in the sequel $\alpha_1(x), \alpha_2(x), \alpha_3(x), g_1(x), g_2(x), g_3(x), u(x), v(x), D(x)$ are always be given by (3), (4) and (5) (see introduction).

First we remark that in fact $G_n(x) \in K[x]$ for all $n \in \mathbb{N}$ where K is finitely generated over $\mathbb{Q}$. We may take

$$K = \mathbb{Q}(\text{coefficients of } a, b, c, G_0, G_1, G_2).$$

Let us define

$$F = K(x\sqrt{D(x}, \sqrt{P(x)}), u(x), u(P(x)), v(x), v(P(x))).$$

Clearly, F is a finitely generated extension field of $\mathbb{Q}$. In fact F is an algebraic function field in one variable over the constant field K. Furthermore, we set

$$\Gamma = \langle \alpha_1(x), \alpha_2(x), \alpha_3(x), \alpha_1(P(x)), \alpha_2(P(x)), \alpha_3(P(x)) \rangle_{(F^*,\cdot)},$$

so Γ is the subgroup of the multiplicative group of F generated by the characteristic roots of $(G_n(x))_{n=0}^{\infty}$ and $(G_n(P(x)))_{n=0}^{\infty}$.

It is obvious that Γ can be seen as a finitely generated subgroup of $\mathbb{C}^*$, because we can embed K^* into $\mathbb{C}^*$ by sending the transcendental elements which appear in the coefficients of a, b, c, G_0, G_1, G_2 and the variable x to linearly independent transcendental elements of $\mathbb{C}$. Moreover, it is clear that the rank r of Γ is at most 6.

First we reduce the solvability of (5.8) to the solvability of seven types of systems of exponential equations in n, m.

We consider for $n \neq m$ the equation $G_n(x) = G_m(P(x))$ and obtain

$$\begin{aligned} &g_1(x)\alpha_1(x)^n + g_2(x)\alpha_2(x)^n + g_3(x)\alpha_3(x)^n - \\ &\quad -g_1(P(x))\alpha_1(P(x))^m - g_2(P(x))\alpha_2(P(x))^m - g_3(P(x))\alpha_3(P(x))^m = 0. \end{aligned}$$

This can be rewritten as

$$\frac{g_1(x)}{g_3(P(x))}x_1 + \frac{g_2(x)}{g_3(P(x))}x_2 + \frac{g_3(x)}{g_3(P(x))}x_3 - \frac{g_1(P(x))}{g_3(P(x))}x_4 - \frac{g_2(P(x))}{g_3(P(x))}x_5 = 1$$
$$\text{in} \quad x_1, \ldots, x_5 \in \Gamma.$$

According to the theorem of Evertse, Schlickewei and Schmidt (Theorem 5.4) we conclude that, if $g_1(x), g_2(x), g_3(x) \neq 0$ and the following systems have only finitely many solutions $(m,n) \in \mathbb{Z}^2$ with $n, m \geq 0$ which can be estimated by C say, then our original equation (5.8) has only finitely many solutions which can be bounded by

$$C + \exp(30^{15} \cdot 7).$$

The systems which correspond to the non-trivial vanishing subsums of the above weighted unit equation are:

$$\begin{cases} g_1(x)\alpha_1(x)^n + g_2(x)\alpha_2(x)^n + g_3(x)\alpha_3(x)^n = g_k(P(x))\alpha_k(P(x))^m \\ g_i(P(x))\alpha_i(P(x))^m + g_j(P(x))\alpha_j(P(x))^m = 0 \end{cases} \tag{5.11}$$

$$\begin{cases} g_i(x)\alpha_i(x)^n + g_j(x)\alpha_j(x)^n = 0 \\ g_1(P(x))\alpha_1(P(x))^m + g_2(P(x))\alpha_2(P(x))^m + \\ \qquad + g_3(P(x))\alpha_3(P(x))^m = g_k(x)\alpha_k(x)^n \end{cases} \tag{5.12}$$

$$\begin{cases} g_i(x)\alpha_i(x)^n = g_j(P(x))\alpha_j(P(x))^m \\ g_j(x)\alpha_j(x)^n + g_k(x)\alpha_k(x)^n = g_i(P(x))\alpha_i(P(x))^m + \\ \qquad + g_k(P(x))\alpha_k(P(x))^m \end{cases} \tag{5.13}$$

$$\begin{cases} g_i(x)\alpha_i(x)^n = g_i(P(x))\alpha_i(P(x))^m \\ g_j(x)\alpha_j(x)^n + g_k(x)\alpha_k(x)^n = g_j(P(x))\alpha_j(P(x))^m + \\ \qquad + g_k(P(x))\alpha_k(P(x))^m \end{cases} \tag{5.14}$$

$$\begin{cases} g_1(x)\alpha_1(x)^n + g_2(x)\alpha_2(x)^n + g_3(x)\alpha_3(x)^n = 0 \\ g_1(P(x))\alpha_1(P(x))^m + g_2(P(x))\alpha_2(P(x))^m + \\ \qquad + g_3(P(x))\alpha_3(P(x))^m = 0 \end{cases} \tag{5.15}$$

$$\begin{cases} g_i(x)\alpha_i(x)^n + g_j(x)\alpha_j(x)^n = g_i(P(x))\alpha_i(P(x))^m \\ g_j(P(x))\alpha_j(P(x))^m + g_k(P(x))\alpha_k(P(x))^m = g_k(x)\alpha_k(x)^n \end{cases} \tag{5.16}$$

$$\begin{cases} g_i(x)\alpha_i(x)^n + g_j(x)\alpha_j(x)^n = g_k(P(x))\alpha_k(P(x))^m \\ g_i(P(x))\alpha_i(P(x))^m + g_j(P(x))\alpha_j(P(x))^m = g_k(x)\alpha_k(x)^n \end{cases} \tag{5.17}$$

where i, j, k are always such that $\{i, j, k\} = \{1, 2, 3\}$. Now we have the following lemma.

Lemma 5.1. *Let $g_1(x), g_2(x), g_3(x), g_1(P(x)), g_2(P(x)), g_3(P(x)) \neq 0$ and assume that both $(G_n(x))_{n=0}^{\infty}$ and $(G_n(P(x)))_{n=0}^{\infty}$ are nondegenerate. Then for every choice of $\{i, j, k\} = \{1, 2, 3\}$ we have*

(5.11) and (5.12) have at most $3 + \exp(18^9 \cdot 4)$,

(5.15) has at most 3721,

(5.16) and (5.17) have at most 2^{64}

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

Proof. First observe that an equation of the type

$$h_1(x)\alpha(x)^n + h_2(x)\beta(x)^n = 0 \tag{5.18}$$

with $h_1, h_2, \alpha, \beta \in F^*$ and $\alpha(x)/\beta(x)$ not equal to a root of unity has at most one solution in $n \in \mathbb{Z}$. In particular, assume that we have two solutions n_1, n_2. Then we obtain

$$-\frac{h_1(x)}{h_2(x)} = \left(\frac{\beta(x)}{\alpha(x)}\right)^{n_1} = \left(\frac{\beta(x)}{\alpha(x)}\right)^{n_2},$$

which implies that $n_1 = n_2$.

Let us first look at (5.11) with some choice of $\{i, j, k\} = \{1, 2, 3\}$. The second equation is of the above type (5.18) and therefore it has at most one solution $m \in \mathbb{N}$. Now the first equation in this system becomes

$$b_1(x)\alpha_1(x)^n + b_2(x)\alpha_2(x)^n + b_3(x)\alpha_3(x)^n = 1,$$

with

$$b_i(x) = \frac{g_i(x)}{g_k(P(x))\alpha_k(P(x))^m}, \quad i = 1, 2, 3,$$

which can be seen as a 3-dimensional weighted unit equation over the field F of characteristic 0 where we search for solutions in the finitely generated subgroup which is generated by $\alpha_1(x), \alpha_2(x), \alpha_3(x)$. By our assumptions we have $b_i(x) \neq 0$ for $i = 1, 2, 3$. Moreover, each of the three non-trivial subsums vanishes for at most one $n \in \mathbb{N}$ as this subsums are again of the type (5.18). By using Theorem 5.4 again, we can conclude that there are at most

$$3 + \exp(18^9 \cdot 4)$$

pairs of solutions (n, m). The second system (5.12) is completely analogous.

Now for the equations in (5.15) we can calculate the number of solutions by using the bound for the zero multiplicity of nondegenerate third order linear recurring sequences (see introduction). Therefore the first equation has at most 61 solutions in n and the second at most 61 solutions in m. Consequently, there are at most $61 \cdot 61 = 3721$ pairs (n, m) for which (5.15) holds.

Each of the equations in the system (5.16) can be seen as a 2-dimensional weighted unit equations where we are interested in solutions which lie in the group generated by the three characteristic roots which are involved in the equation. Therefore by Theorem 5.5 we can conclude that the first and the second equation has at most $2^{16 \cdot 4}$ solutions. Altogether the systems has at most $2^{16 \cdot 4}$ solutions as claimed in the lemma. □

Lemma 5.2. *Let $g_1(x), g_2(x), g_3(x), g_1(P(x)), g_2(P(x)), g_3(P(x)) \neq 0$ and assume that both $(G_n(x))_{n=0}^{\infty}$ and $(G_n(P(x)))_{n=0}^{\infty}$ are nondegenerate. Then (5.12) and (5.13) have at most*

$$1 + \exp(18^9 \cdot 7)$$

solutions $(n, m) \in \mathbb{Z}^2$ with $n, m \geq 0, n \neq m$ respectively, provided that none of the following systems has a solution:

$$\begin{cases} g_i(x)\alpha_i(x)^n = g_i(P(x))\alpha_i(P(x))^m \\ g_j(x)\alpha_j(x)^n = g_j(P(x))\alpha_j(P(x))^m \\ g_k(x)\alpha_k(x)^n = g_k(P(x))\alpha_k(P(x))^m \end{cases} \tag{5.19}$$

$$\begin{cases} g_i(x)\alpha_i(x)^n = g_i(P(x))\alpha_i(P(x))^m \\ g_j(x)\alpha_j(x)^n = g_k(P(x))\alpha_k(P(x))^m \\ g_k(x)\alpha_k(x)^n = g_j(P(x))\alpha_j(P(x))^m \end{cases} \tag{5.20}$$

$$\begin{cases} g_i(x)\alpha_i(x)^n = g_j(P(x))\alpha_j(P(x))^m \\ g_j(x)\alpha_j(x)^n = g_k(P(x))\alpha_k(P(x))^m \\ g_k(x)\alpha_k(x)^n = g_i(P(x))\alpha_i(P(x))^m \end{cases} \tag{5.21}$$

where i, j, k are such that $\{i, j, k\} = \{1, 2, 3\}$.

Proof. We handle only the system (5.12) since (5.13) is completely analogous. Let $\{i, j, k\} = \{1, 2, 3\}$ be fixed. The second equation in both systems can be seen as a 3-dimensional weighted unit equation

$$\frac{g_j(x)}{g_k(P(x))}x_1 + \frac{g_k(x)}{g_k(P(x))}x_2 - \frac{g_i(P(x))}{g_k(P(x))}x_3 = 1 \quad \text{in} \quad x_1, x_2, x_3 \in \Gamma.$$

According to Theorem 5.4 this equation has at most

$$\exp(18^9 \cdot 7)$$

solutions in Γ for which no non-trivial subsum vanishes. But the vanishing subsums are

$$\begin{cases} g_j(x)\alpha_j(x)^n + g_k(x)\alpha_k(x)^n = 0 \\ g_i(P(x))\alpha_i(P(x))^m + g_k(P(x))\alpha_k(P(x))^m = 0 \end{cases}$$

which has at most one pair of solutions (n, m) by the proof of Lemma 5.1, and the first and the last system in our assumptions, which are assumed to have no solutions in (n, m) at all. Therefore we have proved the upper bound for the number of solutions $(n, m) \in \mathbb{Z}^2$ with $n, m \geq 0, n \neq m$ as claimed in the lemma. □

From this discussion we see that it suffices to prove that $g_1(x), g_2(x), g_3(x), g_1(P(x))$, $g_2(P(x)), g_3(P(x)) \neq 0$, that $\alpha_i(x)/\alpha_j(x)$ and $\alpha_i(P(x))/\alpha_j(P(x))$ is not equal to a root of unity for $1 \leq i < j \leq 3$ and that the systems (5.19), (5.20) and (5.21) do not have a solution $(n, m) \in \mathbb{Z}^2$ with $n, m \geq 0, n \neq m$. We will show this for each of our theorems separately in the following sections.

5.5 Proof of Theorem 5.1

In the next lemma we calculate the order of $\alpha_1(x), \alpha_2(x)$ and $\alpha_3(x)$ respectively in the function field F/K, where F and K are defined as in the previous section. Then we have:

Lemma 5.3. *Let $(G_n(x))_{n=0}^{\infty}$ be a sequence of polynomials defined by (5.1) and assume that* $3 \deg a > \deg c, 2 \deg a > \deg b$ *and* $\deg a + \deg c > 2 \deg b$. *Then*

$$\operatorname{ord}(\alpha_1) = \deg a, \tag{5.22}$$

$$\operatorname{ord}(\alpha_2) = \operatorname{ord}(\alpha_3) = \frac{1}{2}(\deg c - \deg a) < \deg a. \tag{5.23}$$

Proof. First of all, observe that we have

$$\deg q = 3 \deg a \quad \text{and} \quad \deg p = 2 \deg a.$$

Moreover, we have by our assumptions

$$\deg D = 3 \deg a + \deg c.$$

Therefore, we trivially have

$$\operatorname{ord}(u) = \operatorname{ord}(v) = \deg a$$

and the leading coefficients of the Puiseux expansions of $u(x)$ and $v(x)$ at the absolute value which corresponds to ord are equal to $1/3$ times the leading coefficient of $a(x)$. Consequently, we have $\operatorname{ord}(\alpha_1) = \deg a$. Now it follows from (b) and from the following equation

$$u(x)^3 - v(x)^3 = 2\sqrt{D(x)}$$

that

$$\operatorname{ord}(u^3 - v^3) = \frac{1}{2}(3 \deg a + \deg c).$$

But using

$$u(x)^3 - v(x)^3 = (u(x) - v(x)) \left(u(x)^2 + u(x)v(x) + v(x)^2\right)$$

and the observation that $\operatorname{ord}(u^2 + uv + v^2) = 2 \deg a$, which follows again from the fact that all the summands have the same leading coefficient in their Puiseux expansion, we get

$$\operatorname{ord}(u - v) = \frac{1}{2}(\deg c - \deg a).$$

We want to remark that we have

$$\alpha_1(x)\alpha_2(x)\alpha_3(x) = -c(x). \tag{5.24}$$

Now assume that $\mathrm{ord}(\alpha_2) \neq \mathrm{ord}(\alpha_3)$. Furthermore, we may assume without loss of generality that $\mathrm{ord}(\alpha_2) > \mathrm{ord}(\alpha_3)$. But then we have using (d)

$$\mathrm{ord}(\alpha_2) = \mathrm{ord}(\alpha_2 - \alpha_3) = \mathrm{ord}(u - v) = \frac{1}{2}(\deg c - \deg a)$$

which yields by (5.24)

$$\mathrm{ord}(\alpha_3) = \frac{1}{2}(\deg c - \deg a) = \mathrm{ord}(\alpha_2),$$

a contradiction. Therefore we conclude again using (5.24) that

$$\mathrm{ord}(\alpha_2) = \mathrm{ord}(\alpha_3) = \frac{1}{2}(\deg c - \deg a).$$

This means that the proof is finished. □

It is clear that

$$\begin{aligned} \mathrm{ord}(\alpha_1 - \alpha_3) &= \mathrm{ord}(\alpha_1 - \alpha_2) = \deg a, \\ \mathrm{ord}(\alpha_2 - \alpha_3) &= \mathrm{ord}\left(2i\sqrt{3}\frac{u-v}{2}\right) = \frac{1}{2}(\deg c - \deg a). \end{aligned}$$

To finish our proof, we want to calculate the order of $g_1(x), g_2(x)$ and $g_3(x)$. From the initial conditions

$$\begin{aligned} G_0(x) &= g_1(x) + g_2(x) + g_3(x), \\ G_1(x) &= g_1(x)\alpha_1(x) + g_2(x)\alpha_2(x) + g_3(x)\alpha_3(x), \\ G_2(x) &= g_1(x)\alpha_1(x)^2 + g_2(x)\alpha_2(x)^2 + g_3(x)\alpha_3(x)^2, \end{aligned}$$

we get

$$\begin{aligned} g_1(x)\Delta(x) &= G_2(x)\left(\alpha_3(x) - \alpha_2(x)\right) + G_1(x)\left(\alpha_2(x)^2 - \alpha_3(x)^2\right) + \qquad (5.25) \\ &\quad + G_0(x)\alpha_2(x)\alpha_3(x)\left(\alpha_3(x) - \alpha_2(x)\right), \\ g_2(x)\Delta(x) &= G_2(x)(\alpha_1(x) - \alpha_3(x)) + G_1(x)\left(\alpha_3(x)^2 - \alpha_1(x)^2\right) + \qquad (5.26) \\ &\quad + G_0(x)\alpha_1(x)\alpha_3(x)(\alpha_1(x) - \alpha_3(x)), \\ g_3(x)\Delta(x) &= G_2(x)(\alpha_2(x) - \alpha_1(x)) + G_1(x)\left(\alpha_1(x)^2 - \alpha_2(x)^2\right) + \qquad (5.27) \\ &\quad + G_0(x)\alpha_1(x)\alpha_2(x)(\alpha_2(x) - \alpha_1(x)), \end{aligned}$$

where

$$\begin{aligned} \Delta(x) &= \alpha_1(x)\alpha_2(x)(\alpha_2(x) - \alpha_1(x)) + \alpha_1(x)\alpha_3(x)(\alpha_1(x) - \alpha_3(x)) + \\ &\quad + \alpha_2(x)\alpha_3(x)(\alpha_3(x) - \alpha_2(x)) = \\ &= -6i\sqrt{3}\sqrt{D(x)}. \end{aligned}$$

In the proof of Lemma 5.3 we have already seen that $a(x)^3 c(x)$ is the dominant term in $D(x)$. Consequently, we have

$$\operatorname{ord}(\Delta) = \frac{1}{2}(3\deg a + \deg c).$$

Therefore, we can conclude

$$\begin{aligned} \operatorname{ord}(g_1) &= \operatorname{ord}(G_2) + \frac{1}{2}(\deg c - \deg a) - \frac{1}{2}(3\deg a + \deg c) = \\ &= \deg G_2 - 2\deg a, \\ \operatorname{ord}(g_2) &= \operatorname{ord}(g_3) = \deg G_2 + \deg a - \frac{1}{2}(3\deg a + \deg c) = \\ &= \deg G_2 - \frac{1}{2}\deg a - \frac{1}{2}\deg c. \end{aligned}$$

Thus, we deduce that $g_1(x), g_2(x), g_3(x)$ and therefore also $g_1(P(x)), g_2(P(x)), g_3(P(x))$ are different from zero.

Next we are intended to show that $\alpha_i(x)/\alpha_j(x)$ is not equal to a root of unity for $1 \leq i < j \leq 3$. First observe that

$$\alpha_1(x) = \zeta\alpha_2(x) \quad \text{or} \quad \alpha_1(x) = \zeta\alpha_2(x)$$

with ζ a root of unity is impossible because of the different order. Namely this would imply

$$\operatorname{ord}(\alpha_1) = \operatorname{ord}(\alpha_2) \quad \text{or} \quad \operatorname{ord}(\alpha_1) = \operatorname{ord}(\alpha_3)$$

respectively, a contradiction. Now assume that we have

$$\alpha_2(x) = \zeta\alpha_3(x)$$

with ζ a root of unity. Observe that the leading coefficients in the Puiseux expansion of $\alpha_2(x), \alpha_3(x)$ are conjugate complex numbers. This follows from the fact that

$$\operatorname{ord}(\alpha_2) = \operatorname{ord}(\alpha_3) = \operatorname{ord}(u - v)$$

and $u(x) - v(x)$ is one of the summands in the definition of those characteristic roots. Thus the only possibilities are $\zeta = 1$ or -1 which both lead to a contradiction since

$$\operatorname{ord}(\alpha_2 - \alpha_3) = \frac{1}{2}(\deg c - \deg a)$$

and $\alpha_2(x) + \alpha_3(x) = a(x) - \alpha_1(x) \neq 0$.

The proof that the sequence $(G_n(P(x)))_{n=0}^{\infty}$ is nondegenerate is completely analogous to the above case since we are only considering the order of the elements.

It remains to show the unsolvability of (5.19), (5.20) and (5.21). Because of

$$\operatorname{ord}(\alpha_2) = \operatorname{ord}(\alpha_3) \quad \text{and} \quad \operatorname{ord}(g_2) = \operatorname{ord}(g_3)$$

it suffices to consider the following two cases:

$$\begin{cases} g_1(x)\alpha_1(x)^n = g_1(P(x))\alpha_1(P(x))^m \\ g_2(x)\alpha_2(x)^n = g_2(P(x))\alpha_2(P(x))^m \end{cases} \tag{5.28}$$

$$\begin{cases} g_1(x)\alpha_1(x)^n = g_2(P(x))\alpha_2(P(x))^m \\ g_2(x)\alpha_2(x)^n = g_1(P(x))\alpha_1(P(x))^m \\ g_3(x)\alpha_3(x)^n = g_3(P(x))\alpha_3(P(x))^m \end{cases} \tag{5.29}$$

Calculating orders we get

$$\begin{aligned} &\deg G_2 - 2\deg a + n\deg a = (\deg G_2 - 2\deg a)(\deg P + m\deg a \deg P) \\ &\left(\deg G_2 - \frac{\deg a}{2} - \frac{\deg c}{2}\right)(1 - \deg P) = (m\deg P - n)\frac{\deg c - \deg a}{2} \end{aligned}$$

or

$$\begin{aligned} &(\deg G_2 - 2\deg a)(1 - \deg P) = (m\deg P - n)\deg a \\ &(2\deg G_2 - \deg a - \deg c)(1 - \deg P) = (m\deg P - n)(\deg c - \deg a) \end{aligned}$$

This yields

$$(m-1)\deg P = n - 1.$$

Substituting this into the first equation leads to

$$(\deg G_2 - \deg a)(1 - \deg P) = 0,$$

which implies $\deg P = 1$ and therefore $n = m$ or $\deg G_2 = \deg a$ and therefore $\deg G_1 < 0$, in both cases a contradiction.

The second system leads to

$$\begin{aligned} \deg G_2 - 2\deg a + n\deg a = (\deg G_2 - \frac{1}{2}\deg a - \frac{1}{2}\deg c)\deg P + \\ + m\deg P\frac{1}{2}(\deg c - \deg a) \end{aligned}$$

$$\begin{aligned} &\deg G_2 - \frac{1}{2}\deg c - \frac{1}{2}\deg a + n\frac{1}{2}(\deg c - \deg a) = \\ &\quad = (\deg G_2 - \frac{1}{2}\deg a - \frac{1}{2}\deg c)\deg P + m\deg P\frac{1}{2}(\deg c - \deg a) \\ &\deg G_2 - \frac{1}{2}\deg c - \frac{1}{2}\deg a + n\frac{1}{2}(\deg c - \deg a) = \\ &\quad = (\deg G_2 - 2\deg a)\deg P + m\deg a \deg P, \end{aligned}$$

which yields

$$0 \leq \frac{1}{2}(3\deg a - \deg c) = -m\frac{1}{2}(\deg a + \deg c) < -m\deg b < 0,$$

a contradiction.

So the proof of Theorem 5.1 is finished. By Lemma 5.1 and Lemma 5.2 we get by counting how often each system can appear, the following bound:

$$\exp\left(30^{15} \cdot 7\right) + 2 \cdot 3 \cdot \left[3 + \exp\left(18^9 \cdot 4\right)\right] + 3721 + 9 \cdot 2^{64} + 9 \cdot \left(1 + \exp\left(18^9 \cdot 7\right)\right)$$

which can be estimated by

$$\exp(10^{24}).$$

This was the claim of Theorem 5.1. □

5.6 Proof of Theorem 5.2

First we want to mention that $a(x) = 0$ means that we have

$$p(x) = b(x), \quad q(x) = c(x) \quad \text{and} \quad D(x) = \frac{1}{4}c(x)^2 - \frac{1}{27}b^3.$$

By our assumption that $3\deg b > 2\deg c$ we get

$$\mathrm{ord}(u) = \mathrm{ord}(v) = \frac{1}{2}\deg b$$

and the leading coefficients of the relevant Puiseux expansions are equal to $i\sqrt{3}$ and $-i\sqrt{3}$ times the square root of the leading coefficient of $b(x)$. Therefore we can conclude

$$\mathrm{ord}(u - v) = \frac{1}{2}\deg b \quad \text{and} \quad \mathrm{ord}(u + v) = \deg c - \deg b.$$

Thus we get

$$\begin{aligned}
&\mathrm{ord}(\alpha_1) = \deg c - \deg b, \\
&\mathrm{ord}(\alpha_2) = \mathrm{ord}(\alpha_3) = \frac{1}{2}\deg b, \\
&\mathrm{ord}(\alpha_1 - \alpha_2) = \mathrm{ord}(\alpha_1 - \alpha_3) = \frac{1}{2}\deg b, \\
&\mathrm{ord}(\alpha_2 - \alpha_3) = \frac{1}{2}\deg b \\
&\mathrm{ord}(\alpha_1 + \alpha_2) = \mathrm{ord}(\alpha_1 + \alpha_3) = \deg c - \deg b, \\
&\mathrm{ord}(\alpha_2 + \alpha_3) = \frac{1}{2}\deg b.
\end{aligned}$$

Using (5.25), (5.26) and (5.27) we get from our assumptions concerning the degrees of the initial polynomials

$$\begin{aligned} \operatorname{ord}(g_1) &= \deg G_2 - 2\deg b, \\ \operatorname{ord}(g_2) = \operatorname{ord}(g_3) &= \deg G_2 - 2\deg b. \end{aligned}$$

Therefore we can conclude that $g_1(x), g_2(x), g_3(x), g_1(P(x)), g_2(P(x)), g_3(P(x))$ are nonzero. The proof that $(G_n(x))_{n=0}^{\infty}$ and $(G_n(P(x)))_{n=0}^{\infty}$ are nondegenerate is analogous to the proof of this fact in Theorem 5.1.

As in the proof of Theorem 5.1 it suffices to prove the unsolvability of (5.28) and (5.29). By calculating orders we get

$$\begin{aligned} \deg G_2 - 2\deg b + n(\deg c - \deg b) &= (\deg G_2 - 2\deg b)\deg P + \\ &\quad + m\deg P(\deg c - \deg b) \\ \deg G_2 - 2\deg b + n\frac{\deg b}{2} &= (\deg G_2 - 2\deg b)\deg P + m\deg P\frac{\deg b}{2} \end{aligned}$$

This yields $n = m\deg P$ and by substituting this into one of the equations above we get $\deg P = 1$ which implies $n = m$ or $\deg G_2 = 2\deg b$ from which we get $\deg G_1 < 0$, in both cases a contradiction. The second system (5.28) can be handled analogously.

By Lemma 5.1 and 5.2 the theorem follows and the proof is finished. □

5.7 Proof of Theorem 5.3

We start our proof with some useful lemmas.

Lemma 5.4. *Let* $A, B, P \in \mathbf{K}[x]$. *Then* $\gcd(A, B) = 1$ *if and only if* $\gcd(A(P), B(P)) = 1$.

Proof. Let us assume that $\gcd(A(P), B(P)) = 1$ and that $\gcd(A, B) > 1$. Then there exists a common root of $A(x)$ and $B(x)$ which we denote by $\xi \in \mathbf{K}$ (observe that $\mathbf{K}$ is algebraically closed). Now let $\zeta \in \mathbf{K}$ be a root of the polynomial $P(x) - \xi$ with coefficients in $\mathbf{K}$. Thus we have $A(P(\zeta)) = B(P(\zeta)) = 0$, contradicting our assumption.
The proof of the converse can be found in [49, Lemma 4]. □

We will use the same notations as introduced in the proof of Theorem 5.1.

First of all we have because of $\deg D \neq 0$ and $\gcd(c, D) = 1$ that $c(x) \neq 0$. Therefore, from

$$\alpha_1(x)\alpha_2(x)\alpha_3(x) = -c(x),$$

it follows that $\alpha_1(x), \alpha_2(x), \alpha_3(x) \neq 0$. Next we show that $\alpha_1(x), \alpha_2(x), \alpha_3(x)$ are non-degenerate. We take $\xi \in \mathbf{K}$ such that $a(\xi) = 27c(\xi)^2 - 4b(\xi)^3 = 0$. This implies that $D(\xi) = 0$. From this we can conclude

$$u(\xi) = \sqrt[3]{\frac{q(\xi)}{2}} = \sqrt{\frac{p(\xi)}{2}} = \sqrt{\frac{b(\xi)}{3}} \quad \text{and} \quad v(\xi) = u(\xi).$$

Therefore we have

$$\alpha_1(\xi) = 2\sqrt{\frac{b(\xi)}{3}}.$$

On the other hand we get

$$\alpha_2(\xi) = \alpha_3(\xi) = -\sqrt{\frac{b(\xi)}{3}},$$

which implies that $\alpha_1(x)$ differs from $\alpha_2(x)$ and $\alpha_3(x)$ by more than a root of unity, because $b(\xi) \neq 0$ by condition (3) in the theorem.

Now assume that we have

$$\alpha_2(x) = \zeta\alpha_3(x), \quad \zeta \in K.$$

This yields

$$(1+\zeta)i\sqrt{3}\frac{u(x)-v(x)}{2} = \frac{1-\zeta}{2}(u(x)+v(x)) - \frac{1-\zeta}{2}a(x).$$

As above we derive a contradiction unless $\zeta = 1$. But assuming $\zeta = 1$ yields

$$2i\sqrt{3}\frac{u(x)-v(x)}{2} = 0,$$

contradicting the fact that $u(x) = v(x) \iff D(x) = 0$.

Because of Lemma 5.4 we can conclude in the same way as above that the same holds for $\alpha_1(P(x)), \alpha_2(P(x)), \alpha_3(P(x))$.

Next we want to proof the $g_1(x), g_2(x), g_3(x) \neq 0$ holds. Observe that they are given by (5.25), (5.26) and (5.27) respectively.

First observe that for $\xi \in \mathbf{K}$ we have: $\Delta(\xi) = 0 \iff \alpha_2(\xi) = \alpha_3(\xi)$ and $\Delta(\xi) = 0 \Rightarrow \alpha_1(\xi) \neq \alpha_2(\xi), \alpha_3(\xi)$. We will need

$$g_1(x) = \frac{\alpha_3(x)-\alpha_2(x)}{\Delta(x)}(G_2(x) - G_1(x)[a(x) - \alpha_1(x)] + G_0(x)\alpha_2(x)\alpha_3(x))$$

and

$$\begin{aligned}
&G_2(x) - G_1(x)[a(x) - \alpha_1(x)] + G_0(x)\alpha_2(x)\alpha_3(x) = \\
&\quad = G_2(x) - a(x)G_1(x) + \frac{a(x)}{3}G_1(x) + G_1(x)[u(x) + v(x)] + G_2(x)[u(x)^2 \\
&\quad\quad +v(x)^2] - G_2(x)\frac{a(x)}{3}[u(x) + v(x)] + G_2(x)\frac{a(x)^2}{9} - G_2(x)u(x)v(x).
\end{aligned}$$

Observe that $3u(x)v(x) = p(x)$. Let $\xi \in \mathbf{K}$ with $q(\xi) = 0$. This implies

$$u(\xi) = \frac{i}{\sqrt{3}}\sqrt{p(\xi)} \quad \text{and} \quad v(\xi) = -\frac{i}{\sqrt{3}}\sqrt{p(\xi)}$$

and therefore $u(\xi) + v(\xi) = 0$. Because of the above equation and condition (4) from the theorem we get

$$g_1(\xi) \neq 0.$$

To handle $g_2(x), g_3(x)$ we prove the following lemma which will also enable us to calculate $\nu(g_2)$ and $\nu(g_2)$ where ν extends ν_ξ to F for some $\xi \in \mathbf{K}$.

Lemma 5.5. *Let $(G_n(x))_{n=0}^{\infty}$ be a sequence of polynomials defined by (5.1) and assume that* $\gcd(G_2^2 - \frac{4}{3}bG_2G_0 - \frac{1}{3}bG_1^2 + \frac{4}{9}b^2G_0^2, D) = 1$. *Let $\xi \in \mathbf{K}$ be a common root of $a(x)$ and $D(x)$ and let ν be an extension of ν_ξ to F. Then $\nu(g_1\Delta) = \nu(g_2\Delta) = 0$.*

Proof. Since $D(\xi) = 0$ we have $\alpha_2(\xi) = \alpha_3(\xi)$ and by equation (5.26) we have to show that

$$\nu(G_2 - G_1(a - \alpha_2) + G_0\alpha_1\alpha_3) = 0.$$

Observe that it is clear that we have ≥ 0 since the $\alpha_i(x)$, $i = 1, 2, 3$ are integral over $\mathbf{K}[x]$ and the integral closure is a ring. Therefore it suffices to show that

$$(G_2 - G_1(a - \alpha_2) + G_0\alpha_1\alpha_3)(\xi) \neq 0,$$

but this follows from our condition: We have

$$(G_2 + G_1\alpha_2 + G_0\alpha_1\alpha_3)(\xi) = \left(G_2 - \frac{1}{3}G_1\sqrt{3b} - \frac{2}{3}bG_0\right)(\xi).$$

Assume this value to be zero. Then

$$\left[(G_2 - \frac{2}{3}bG_0)^2 - \frac{1}{3}bG_1^2\right](\xi) = 0,$$

contradicting the assumption in our Lemma.

The same holds for $g_2(x)$ and therefore the proof is finished. □

We are intended to prove that the systems of equations (5.19), (5.20) and (5.21) are not solvable. Observe that each of this systems contain at least one equation of the form

$$g_i(x)\alpha_i(x)^n = g_k(P(x))\alpha_k(P(x))^m \tag{5.30}$$

with $i, k \in \{2, 3\}$ not necessarily different. We will show that already this equation cannot have a solution.

We have $\deg D(P) = \deg D \deg P > \deg D > 0$, as $\deg P > 1$ by assumption (2). Hence $D(P(x))$ has a zero $\xi \in \mathbf{K}$ such that

$$\nu_\xi(D(P)) > \nu_\xi(D) \geq 0$$

which is also a zero of $a(P(x))$ which means $\nu_\xi(a(P)) > 0$. This implies that there is a finite valuation ν on F such that by Lemma 5.5

$$\nu(g_1(P)) = \nu(g_2(P)) = -\nu(\Delta(P)) = -\frac{1}{2}\nu(D(P)).$$

Moreover, we can conclude that $\nu(\alpha_2(P)) = \nu(\alpha_3(P)) = 0$, because otherwise we would get a contradiction to condition (2) of our theorem.

Thus equation (5.30) implies

$$\nu(g_i) + n\nu(\alpha_i) = \nu(g_k(P)),$$

which yields

$$n\nu(\alpha_i) = \nu(g_k(P)) - \nu(g_i) \leq -\nu(\Delta(P)) + \nu(\Delta) < 0,$$

hence (5.30) has no solution in n, if $\nu(\alpha_i) \geq 0$ and at most one, if $\nu(\alpha_i) < 0$, which is impossible since $\alpha_1(x), \alpha_2(x), \alpha_3(x)$ are integral over $\mathbf{K}[x]$, as they are zeros of the monic equation $T^3 - a(x)T^2 - b(x)T - c(x) = 0$ with coefficients in $\mathbf{K}[x]$. Therefore, we have $\nu(\alpha_i) \geq 0$. Consequently (5.30) has no solution.

So, we have shown that (5.19), (5.20) and (5.21) have no solutions $(n, m) \in \mathbb{Z}^2$ with $n, m \geq 0, n \neq m$. It is clear that we get the same bound as in Theorem 5.1. □

Chapter 6

A polynomial variant of a problem of Diophantus and Euler

In this chapter, we prove that there does not exist a set of four polynomials with integer coefficients, which are not all constant, such that the product of any two of them is one greater than a square of a polynomial with integer coefficients.

This chapter is identically equal to a joint paper with A. Dujella which is to appear in Rocky Mount. J. Math. (cf. [33]).

6.1 Introduction

Let n be an integer. A set of m positive integers is called a Diophantine m-tuple with the property $D(n)$ or simply $D(n)$-m-tuple, if the product of any two of them increased by n is a perfect square. The first $D(1)$-quadruple, the set $\{1, 3, 8, 120\}$, was found by Fermat. The folklore conjecture is that there does not exist a $D(1)$-quintuple. In 1969, Baker and Davenport [6] proved that the Fermat's set cannot be extended to a $D(1)$-quintuple. Recently, Dujella proved that there does not exist a $D(1)$-sextuple and there are only finitely many $D(1)$-quintuples (see [32]).

In the case $n = -1$, the conjecture is that there does not exist a $D(-1)$-quadruple (see [27]). It is known that some particular $D(-1)$-triples cannot be extended to $D(-1)$-quadruples (see [14], [28], [65], [57]). Let us mention that from [29, Theorem 4] it follows that there does not exist a $D(-1)$-33-tuple.

This $n = -1$ case is closely connected with an old problem of Diophantus and Euler. Namely, Diophantus studied the problem of finding numbers such that the product of any two increased by the sum of these two gives a square. He found two triples $\{4, 9, 28\}$ and $\{\frac{3}{10}, \frac{21}{5}, \frac{7}{10}\}$ satisfying this property. Euler found a quadruple $\{\frac{5}{2}, \frac{9}{56}, \frac{9}{224}, \frac{65}{224}\}$ (see

[25], [24]). In [31] an infinite family of rational quintuples with the same property was given. Since

$$xy + x + y = (x + 1)(y + 1) - 1,$$

we see that the problem of finding integer m-tuples with the same property is equivalent to finding $D(-1)$-m-tuples.

A polynomial variant of the above problems was first studied by Jones [55], [56], and it was for the case $n = 1$.

Definition 6.1. *Let n be an integer. A set $\{a_1, a_2, \ldots, a_m\}$ of m polynomials with integer coefficients, which are not all constant, is called a* polynomial $D(n)$-m-tuple *if for all $1 \leq 1 < j \leq m$ the following holds: $a_i \cdot a_j + n = b_{ij}^2$, where $b_{ij} \in \mathbb{Z}[x]$.*

A natural question is how large such sets can be. Let us define

$$P_n = \sup\{\,|S| : S \text{ is a polynomial } D(n)\text{-tuple}\,\}.$$

From [29, Theorem 1] it follows that $P_n \leq 22$ for all $n \in \mathbb{Z}$. The above mentioned result about the existence of only finitely many $D(1)$-quintuples implies that $P_1 = 4$.

In the present chapter, we will prove that $P_{-1} = 3$. First of all, $P_{-1} \geq 3$. More precisely, if $a \cdot b - 1 = r^2$, then

$$\{a, b, a + b + 2r\}$$

is a polynomial $D(-1)$-triple. E.g.

$$\{x^2 + 1, x^2 + 2x + 2, 4x^2 + 4x + 5\}$$

is a polynomial $D(-1)$-triple (see [14]). Therefore, we have to prove that $P_{-1} < 4$, and this is the statement of our main theorem.

Theorem 6.1. *There does not exist a polynomial $D(-1)$-quadruple.*

The proof of Theorem 6.1 is divided into several parts. In section 6.2, we transform our problem into a system of polynomial Pellian equations, which leads to finding intersections of some binary recursive sequences. We obtain some useful information about initial terms of these sequences.

In section 6.3, we show that there is no loss of generality in assuming that one element of our initial triple is equal to 1. This, together with results from section 6.2, allow us to completely determine initial terms of corresponding sequences.

In section 6.4, we prove Theorem 6.1 by showing that our sequences cannot have nontrivial common terms. This is done by comparing degrees and leading coefficients of corresponding polynomials.

6.2 Two sequences of polynomials

Let $\mathbb{Z}^+[x]$ denote the set of all polynomials with integer coefficients with positive leading coefficient. For $a, b \in \mathbb{Z}[x]$, $a < b$ means that $b - a \in \mathbb{Z}^+[x]$. The usual fundamental properties of inequality hold for this order. For $a \in \mathbb{Z}[x]$, we define $|a| = a$ if $a \geq 0$, and $|a| = -a$ if $a < 0$.

If $\{a, b, c, d\}$, $a < b < c < d$ is a polynomial $D(-1)$-quadruple, then d is nonconstant. Assume now that a and b are constant polynomials. Considering leading coefficients of $ad - 1$ and $bd - 1$ we conclude that ab is a perfect square, contradicting the assertion that $ab - 1$ is also a perfect square. Therefore, we proved that in a polynomial $D(-1)$-quadruple there is at most one constant polynomial. It is also clear that all leading coefficients of the polynomials in a polynomial $D(-1)$-m-tuple have the same sign. This implies that there is no loss of generality in assuming that they are all positive, i.e. that all polynomials are in $\mathbb{Z}^+[x]$.

Let $\{a, b, c\}$, where $0 < a < b < c$, be a polynomial $D(-1)$-triple and let $r, s, t \in \mathbb{Z}^+[x]$ be defined by

$$ab - 1 = r^2, \; ac - 1 = s^2, \; bc - 1 = t^2.$$

In this chapter, the symbols r, s, t will always have this meaning. Assume that $d \in \mathbb{Z}^+[x], d > c$, is a polynomial such that $\{a, b, c, d\}$ is a polynomial $D(-1)$-quadruple. We have

$$ad - 1 = u^2, \; bd - 1 = y^2, \; cd - 1 = z^2, \tag{6.1}$$

with $u, y, z \in \mathbb{Z}^+[x]$. Eliminating d from (6.1) we obtain the following system of polynomial Pellian equations

$$az^2 - cu^2 = c - a, \tag{6.2}$$

$$bz^2 - cy^2 = c - b. \tag{6.3}$$

We will describe the sets of solutions of equations (6.2) and (6.3). We will follow the arguments in the classical case of Pellian equations in integers (cf. [30]).

Lemma 6.1. *If (z, u) and (z, y), with $u, y, z \in \mathbb{Z}^+[x]$, are polynomial solutions of (6.2) and (6.3) respectively, then there exist $z_0, u_0 \in \mathbb{Z}[x]$ and $z_1, y_1 \in \mathbb{Z}[x]$ with*

(i) (z_0, u_0) and (z_1, y_1) are solutions of (6.2) and (6.3) respectively,

(ii) the following inequalities are satisfied:

$$0 \leq |u_0| < s, \tag{6.4}$$

$$0 < z_0 < c, \tag{6.5}$$

$$0 \le |y_1| < t, \tag{6.6}$$

$$0 < z_1 < c, \tag{6.7}$$

and there exist integers $m, n \ge 0$ *such that*

$$z\sqrt{a} + u\sqrt{c} = (z_0\sqrt{a} + u_0\sqrt{c})(s + \sqrt{ac})^{2m}, \tag{6.8}$$

$$z\sqrt{b} + y\sqrt{c} = (z_1\sqrt{b} + y_1\sqrt{c})(t + \sqrt{bc})^{2n}, \tag{6.9}$$

where this means that the coefficients of $\sqrt{a}$, $\sqrt{b}$ *and* $\sqrt{c}$ *respectively on both sides are equal.*

Proof. It is clear that it suffices to prove the statement of the lemma for equation (6.2). First observe that

$$(s + \sqrt{ac})^{2m} = (s^2 + ac + 2s\sqrt{ac})^m = (2ac - 1 + 2s\sqrt{ac})^m$$

and by multiplying with the conjugate $(s - \sqrt{ac})^{2m}$ we see that

$$(s + \sqrt{ac})^{2m}(s - \sqrt{ac})^{2m} = (s^2 - ac)^{2m} = (-1)^{2m} = 1. \tag{6.10}$$

Let now (z, u) be a solution of (6.2) in polynomials from $\mathbb{Z}^+[x]$. Consider all pairs (z^*, u^*) of polynomials of the form

$$z^*\sqrt{a} + u^*\sqrt{c} = (z\sqrt{a} + u\sqrt{c})(s + \sqrt{ac})^{2m}, \ m \in \mathbb{Z}.$$

By (6.10) it is clear that (z^*, u^*) satisfies (6.2).

We would like to show that $z^* > 0$. We write $(s + \sqrt{ac})^{2m} = A + B\sqrt{ac}$, where $A, B \in \mathbb{Z}[x]$ satisfying $A^2 - acB^2 = 1$. Therefore we have

$$z^*\sqrt{a} + u^*\sqrt{c} = (z\sqrt{a} + u\sqrt{c})(A + B\sqrt{ac}) = (Az + cuB)\sqrt{a} + (Au + azB)\sqrt{c},$$

and this yields

$$z^* = Az + cuB.$$

Now, if $m \ge 0$ then we have $A, B > 0$ and thus $z^* > 0$. On the other hand, if $m < 0$ we have $A > 0, B < 0$. If we assume that $z^* \le 0$, we have $Az \le -Bcu$ and both sides are > 0. Squaring yields $A^2z^2 \le B^2c^2z^2$. Using the fact that $A^2 - acB^2 = 1$ we obtain $z^2B^2ac + z^2 \le B^2c^2u^2$ and therefore

$$z^2 \le cB^2(cu^2 - az^2) = cB^2(a - c) < 0,$$

a contradiction.

Among all pairs (z^*, u^*), we can now choose a pair with the property that z^* is minimal, and we denote that pair by (z_0, u_0). Define polynomials z' and u' by

$$z'\sqrt{a} + u'\sqrt{c} = (z_0\sqrt{a} + u_0\sqrt{c})(2ac - 1 - 2s\varepsilon\sqrt{ac}),$$

where $\varepsilon = 1$ if $u_0 > 0$, and $\varepsilon = -1$ if $u_0 < 0$. From the minimality of z_0 we conclude that $z' = z_0(2ac - 1) - 2csu_0\varepsilon \geq z_0$ and this leads to $cs|u_0| \leq z_0(ac - 1)$ and further to $c|u_0| \leq sz_0$. Squaring this inequality we obtain

$$acz_0^2 - c(c - a) = c^2u_0^2 \leq acz_0^2 - z_0^2$$

and finally

$$z_0^2 \leq c(c - a) < c^2,$$

which implies (6.5). Now we have

$$cu_0^2 = az_0^2 - c + a \leq ac^2 - a^2c - c + a < ac^2 - c = cs^2 \tag{6.11}$$

and therefore we obtain also (6.4). Hence, we have proved that there exists a solution (z_0, u_0) of (6.2), which satisfies (6.4) and (6.5), and an integer $m \in \mathbb{Z}$ such that

$$z\sqrt{a} + u\sqrt{c} = (z_0\sqrt{a} + u_0\sqrt{c})(s + \sqrt{ac})^{2m}.$$

It remains to show that $m \geq 0$. Suppose that $m < 0$. Then, as above, we have $(s + \sqrt{ac})^{2m} = A - B\sqrt{ac}$, with $A, B \in \mathbb{Z}^+[x]$ satisfying $A^2 - acB^2 = 1$. We have $u = Au_0 - z_0Ba$ and from the condition $u > 0$ we obtain $Au_0 > z_0Ba$ and by squaring $u_0^2 > B^2a(c - a) \geq ac - a^2$, which by (6.11) implies

$$ac^2 - a^2c \leq cu_0^2 \leq ac^2 - a^2c - c + a.$$

This implies $-c + a \geq 0$, which is clearly a contradiction. □

The solutions z arising, for given (z_0, u_0), from formula (6.8) for varying $m \geq 0$ form a binary recurrent sequence $(v_m)_{m\geq 0}$ whose initial terms are found by solving equation (6.8) for z when $m = 0$ and 1, and whose characteristic equation has the roots $(s + \sqrt{ab})^2$ and $(s - \sqrt{ab})^2$. Therefore, we conclude that $z = v_m$ for some (z_0, u_0) with the above properties and integer $m \geq 0$, where

$$v_0 = z_0,\ v_1 = (2ac - 1)z_0 + 2scu_0,\ v_{m+2} = (4ac - 2)v_{m+1} - v_m. \tag{6.12}$$

In the same manner, from (6.9), we conclude that $z = w_n$ for some (z_1, y_1) with the above properties and integer $n \geq 0$, where

$$w_0 = z_1,\ w_1 = (2bc - 1)z_1 + 2tcy_1,\ w_{m+2} = (4bc - 2)w_{n+1} - w_n. \tag{6.13}$$

Now the following congruence relations follow easily from (6.12) and (6.13) by induction.

Lemma 6.2. *Let the sequences (v_m) and (w_n) be given by (6.12) and (6.13). Then we have*

$$v_m \equiv (-1)^m z_0 \pmod{2c}, \quad w_n \equiv (-1)^n z_1 \pmod{2c}.$$

Proof. It suffices to prove the statement of the lemma for v_m. By looking on (6.12) we have

$$v_0 = z_0, \; v_1 \equiv -z_0 \pmod{2c}.$$

Proceeding the induction step, we see using (6.12)

$$v_{m+2} \equiv -2(-1)^{m+1} z_0 - (-1)^m z_0 = (-1)^{m+2} z_0 \pmod{2c},$$

as stated. □

Now we can prove the following lemma, which says that a solution of $v_m = w_n$ implies also a solution at the beginning of the sequences.

Lemma 6.3. *If the equation $v_m = w_n$ has a solution, then $z_0 = z_1$.*

Proof. Assume that $v_m = w_n$ has a solution. By Lemma 6.2 we conclude

$$z_0 \equiv \pm z_1 \pmod{2c}.$$

If we assume that $z_0 \equiv z_1 \pmod{2c}$, then we can conclude by using (6.4) and (6.7) from Lemma 6.1, namely

$$0 < z_0 < c, \quad 0 < z_1 < c,$$

that $z_0 = z_1$ holds. If we assume that $z_0 \equiv -z_1 \pmod{2c}$, we have $2c | z_0 + z_1$, which contradicts the fact that $z_0 + z_1 < 2c$. This finishes the proof. □

6.3 Reduction to the case $a = 1$

In this section, we show that it suffices to prove that polynomial $D(-1)$-triples $\{a, b, c\}$, where $a = 1$, cannot be extended to a polynomial $D(-1)$-quadruple.

Lemma 6.4. *Let $\{a, b, c, d\}$ with $0 < a < b < c < d$ be a polynomial $D(-1)$-quadruple. Then there exists $d_0 \in \mathbb{Z}^+[x]$ with $d_0 < c$ such that $ad_0 - 1$, $bd_0 - 1$, $cd_0 - 1$ are perfect squares.*

Proof. We are interested in sequences (v_m) (and (w_n)) such that $z^2 = v_m^2 = w_n^2 = cd - 1$, where $d \in \mathbb{Z}^+[x]$. This implies that $v_m^2 \equiv -1 \pmod{c}$. By Lemma 6.2 this means

$$z_0^2 \equiv -1 \pmod{c}.$$

In this case we define

$$d_0 = \frac{z_0^2+1}{c} \in \mathbb{Z}^+[x].$$

For this d_0 we have

$$cd_0 - 1 = z_0^2.$$

By Lemma 6.3 we find

$$bd_0 - 1 = b\frac{z_1^2+1}{c} - 1 = \frac{cy_1^2 + c - b + b}{c} - 1 = y_1^2$$

and finally also

$$ad_0 - 1 = a\frac{z_0^2+1}{c} - 1 = \frac{1}{c}(az_0^2 + a - c) = \frac{1}{c}cu_0^2 = u_0^2$$

holds. Furthermore, we have

$$cd_0 = z_0^2 + 1 < c^2,$$

which implies

$$d_0 < c.$$

□

Assume now that $\{a, b, c, d\}$ is a polynomial $D(-1)$-quadruple with minimal d. We may use Lemma 4 to construct d_0. From the minimality of d, it follows that $\{a, b, c, d_0\}$ is not a polynomial $D(-1)$-quadruple and this means that $d_0 \in \{a, b\}$. But this implies that $d_0^2 - 1$ is a perfect square, which can only hold in the case when $d_0 = 1$. Since $b > a \geq 1$, we conclude that $a = 1$.

Remark 6.1. It follows that it suffices to consider polynomial $D(-1)$-quadruples, which contain the constant polynomial 1.

Now let $\{1, b, c\}$ with $1 < b < c$ be a polynomial $D(-1)$-triple. By the previous discussion, we have $d_0 = 1$. This implies that $z_0^2 + 1 = c$ and therefore we have $z_0 = \pm s$. Because of the fact that $z_0 > 0$ we have $z_0 = s$. In the same way, we can conclude that $z_1 = s$. Now we have

$$cu_0^2 = z_0^2 - c + 1 = c - 1 - c + 1 = 0$$

and this yields $u_0 = 0$. Finally we get

$$cy_1^2 = bz_1^2 - c + b = b(c-1) - c + b = bc - c = cr^2$$

and therefore $y_1 = \pm r$. To sum up, it suffices to consider the following three sequences

$$v_0 = s, \; v_1 = (2c-1)s, \; v_{m+2} = (4c-2)v_{m+1} - v_m, \tag{6.14}$$

and

$$w_0 = s,\ w_1 = (2bc-1)s + 2tcr,\ w_{n+2} = (4bc-2)w_{n+1} - w_n, \tag{6.15}$$

$$w'_0 = s,\ w'_1 = (2bc-1)s - 2tcr,\ w'_{n+2} = (4bc-2)w'_{n+1} - w'_n. \tag{6.16}$$

6.4 Proof of Theorem 6.1

Let $\{1, b, c\}$ be a polynomial $D(-1)$-triple. Let us repeat the defining equations:

$$b - 1 = r^2,\ c - 1 = s^2,\ bc - 1 = t^2.$$

In what follows, we need the leading coefficients of b and c. We know that b and c are non-constant, and thus their leading coefficients are perfect squares. Let us give them names:

$$\mathrm{lc}(b) = \beta^2,\ \mathrm{lc}(c) = \gamma^2,$$

where β and γ are positive integers. Let v_m and w_n, w'_n be the remaining sequences from the last section. To finish the proof, we have to show that no nontrivial solution is obtained from these sequences. The trivial solution is always $v_0 = w_0 = s$, which leads to $d = 1$, which does not yield the extension of our triple $\{1, b, c\}$. We divide the proof in three cases. The first one is handled in the following lemma.

Lemma 6.5. *The equation $v_m = w_n$ has no nontrivial solution.*

Proof. First let us mention that $\deg v_m < \deg v_{m+1}$, $m = 0, 1, 2, \ldots$. To be precise we have

$$\deg v_m = \frac{1}{2}\deg c + m \deg c, \quad m \geq 0. \tag{6.17}$$

This follows at once by induction using the recurring formula (6.14). The same is also true for the second sequence w_n with

$$\deg w_n = \frac{1}{2}\deg c + n\left(\deg b + \deg c\right), \quad n \geq 0. \tag{6.18}$$

Again, by induction, we can now read off the leading coefficient of v_m, which is

$$2^{2m-1}\gamma^{2m+1}, \quad m \geq 1.$$

We have $\mathrm{lc}(v_0) = \gamma$, $\mathrm{lc}(v_1) = 2\gamma^3$ and using the recursive formula (6.14) we get

$$\mathrm{lc}(v_{m+1}) = 4\gamma^2 \mathrm{lc}(v_m) = 4\gamma^2 2^{2m-1}\gamma^{2m+1} = 2^{2(m+1)-1}\gamma^{2(m+1)+1}.$$

In the same way, we find the leading coefficient of w_n, which is

$$2^{2n}\beta^{2n}\gamma^{2n+1}.$$

First we have $\mathrm{lc}(w_0) = \gamma$, $\mathrm{lc}(w_1) = 2\beta^2\gamma^2\gamma + 2\beta\gamma\gamma^2\beta = 4\beta^2\gamma^3$. By using the recursive formula for w_n, one finds

$$\mathrm{lc}(w_{n+1}) = 4\beta^2\gamma^2\mathrm{lc}(w_n) = 2^{2n+2}\beta^{2n+2}\gamma^{2n+3}.$$

If the equation $v_m = w_n$ has a solution, we must have equal leading coefficients, which means

$$2^{2m-1}\gamma^{2m+1} = 2^{2n}\beta^{2n}\gamma^{2n+1}.$$

This implies

$$\left(\frac{2^{m-n}\gamma^{m-n}}{\beta^n}\right)^2 = 2,$$

which yields

$$\sqrt{2} = \frac{2^{m-n}\gamma^{m-n}}{\beta^n} \in \mathbb{Q},$$

a contradiction. Thus $v_m = w_n$ cannot hold and the proof is finished. □

To handle the equation $v_m = w'_n$, we have to distinguish whether $\deg b < \deg c$ or $\deg b = \deg c$ holds.

Lemma 6.6. *Assume that* $\deg b < \deg c$. *Then the equation* $v_m = w'_n$ *has no nontrivial solution.*

Proof. First we calculate

$$\begin{aligned} w'_1 w_1 &= (2bc-1)^2 s^2 - 4t^2c^2r^2 = \\ &= -4b^2c^2 + 4bc + c - 1 + 4bc^3 - 4c^2. \end{aligned}$$

Because of our assumption $\deg b < \deg c$, we obtain that the dominating summand is $4bc^3$. Therefore we get

$$\mathrm{lc}(w'_1 w_1) = 4\beta^2\gamma^6$$

and

$$\deg w'_1 w_1 = 3\deg c + \deg b.$$

On the other hand, we already know that

$$\mathrm{lc}(w_1) = 4\beta^2\gamma^3$$

and

$$\deg w_1 = \deg b + \frac{3}{2}\deg c.$$

Hence, we can conclude that

$$\mathrm{lc}(w'_1) = \gamma^3 \quad \text{and} \quad \deg w'_1 = \frac{3}{2}\deg c.$$

Now by induction and by the recursion (6.16) we get that $\deg w'_n < \deg w'_{n+1}$ and that the leading coefficient of w'_n is given by

$$2^{2n-2}\beta^{2n-2}\gamma^{2n+1}, \quad n \geq 1.$$

Namely we have $\mathrm{lc}(w'_0) = \gamma, \mathrm{lc}(w'_1) = \gamma^3$ and using (6.16) we obtain

$$\mathrm{lc}(w'_{n+1}) = 4\beta^2\gamma^2\mathrm{lc}(w'_n) = 2^{2n}\beta^{2n}\gamma^{2n+3}.$$

Again, if $v_m = w'_n$ has a solution, we can conclude by comparing the leading coefficients that

$$2^{2m-1}\gamma^{2m+1} = 2^{2n-2}\beta^{2n-2}\gamma^{2n+1}.$$

As before we get

$$\sqrt{2} = 2^{n-m}\gamma^{n-m}\beta^{n-1} \in \mathbb{Q},$$

which is a contradiction. This yields that in this case no solution can exist. □

Before we can prove the remaining part, we need the following useful gap principle for the elements of a polynomial $D(-1)$-m-tuple. The principle is a direct modification from the integer case (see [29, Lemma 3]). The analogous statement for polynomial $D(1)$-triples was proved by Jones in [56].

Lemma 6.7. *Let $\{a,b,c\}$ be a polynomial $D(-1)$-triple. Then there exist polynomials $e,u,y,z \in \mathbb{Z}[x]$ such that*

$$ae+1 = u^2, \ be+1 = y^2, \ ce+1 = z^2$$

and

$$c = a+b-e+2(abe+ruy).$$

Proof. Define

$$e = -(a+b+c)+2abc-2rst.$$

Then

$$\begin{aligned}(ae+1)-(at-rs)^2 &= -a(a+b+c)+2a^2bc-2arst+1- \\ &\quad -a^2(bc-1)+2arst-(ab-1)(ac-1) = 0.\end{aligned}$$

Hence, we may take $u = at-rs$, and analogously $y = bs-rt, z = cr-st$. We have

$$\begin{aligned}abe+ruy &= -ab(a+b+c)+2a^2b^2c-2abrst+abrst- \\ &\quad -a(ab-1)(bc-1)-b(ab-1)(ac-1)+rst(ab-1) = \\ &= abc-(a+b)-rst,\end{aligned}$$

and finally

$$a+b-e+2(abe+ruy)=2a+2b+c-2abc+2rst+2abc-2a-2b-2rst=c.$$

□

Using this lemma we can finish our proof.

Lemma 6.8. *Assume that* $\deg b=\deg c$. *Then the equation* $v_m=w'_n$ *has no nontrivial solution.*

Proof. First we conclude by Lemma 6.7 that there exist polynomials e,f,g,h such that

$$e+1=f^2,\ \ be+1=g^2,\ \ ce+1=h^2 \tag{6.19}$$

and

$$c=1+b-e+2(be+rfg).$$

By looking at the proof of Lemma 6.7, we see that we have

$$e=-1-b-c+2bc-2rst.$$

We want to show that $e=0$. Let us assume $e\neq 0$ and define

$$\bar{e}=-1-b-c+2bc+2rst.$$

Then

$$\deg\bar{e}=\deg b+\deg c=2\deg c=\deg c^2. \tag{6.20}$$

Let us calculate

$$\begin{aligned} e\bar{e} &= (2bc-1-b-c)^2-4r^2s^2t^2= \\ &= (2bc-1-b-c)^2-4(b-1)(c-1)(bc-1)= \\ &= 1+b^2+c^2-2b-2bc-2c+4. \end{aligned}$$

This yields

$$\deg e+\deg\bar{e}=\deg e\bar{e}\leq\deg c^2.$$

Using (6.20), we can conclude

$$\deg e\leq 0.$$

But looking at (6.19) we see that

$$e+1=\varphi^2 \quad \text{and} \quad e=\psi^2$$

must hold with $\varphi,\psi\in\mathbb{Z}$. This is only possible if $e=0$.

This implies now that $f = 1, g = 1$ and $c = 1 + b + 2r$. Next let us express all polynomials in terms of the polynomial r. We have

$$b = r^2 + 1,$$

and therefore

$$c = r^2 + 2r + 2.$$

Next we calculate $s^2 = c - 1 = b + 2r = r^2 + 2r + 1 = (r+1)^2$, thus

$$s = r + 1.$$

In the same way, we get via $t^2 = bc - 1 = (r^2+1)(r^2+2r+2) - 1 = r^4+2r^3+3r^2+2r+1 = (r^2 + r + 1)^2$, that

$$t = r^2 + r + 1.$$

This gives us

$$\begin{aligned} w_1' &= (2bc-1)s - 2tcr = \\ &= (2r^4 + 4r^3 + 6r^2 + 4r + 3)(r+1) - 2(r^3 + r^2 + r)(r^2 + 2r + 2) = \\ &= 2r^2 + 3r + 3. \end{aligned}$$

From this we conclude that

$$\deg w_1' = \deg c$$

and by induction, using the recurring formula (6.16), we get

$$\deg w_n' = \deg c + 2(n-1)\deg c, \quad n \geq 1.$$

Let us assume that $v_m = w_n'$ has a solution. Then by comparing the degree of v_m, which is given by (6.17), and the degree of w_n', we get

$$\frac{1}{2}\deg c + m \deg c = \deg c + 2(n-1)\deg c$$

and

$$\frac{1}{2} + m = 2n - 1,$$

a contradiction. Therefore $v_m = w_n'$ cannot have a solution and the proof is finished. □

Now Theorem 6.1 follows directly from Lemma 6.5, Lemma 6.6 and Lemma 6.8.

Chapter 7

Diophantine m-tuples for linear polynomials

In this chapter, we prove that there does not exist a set with more than 26 polynomials with integer coefficients such that the product of any two of them plus a linear polynomial is a square of a polynomial with integer coefficients.

This chapter is equal to a manuscript which is joint work with A. Dujella and R. F. Tichy (cf. [34]).

7.1 Introduction

Let n be a nonzero integer. A set of m positive integers $\{a_1, a_2, \ldots, a_m\}$ is called a Diophantine m-tuple with the property $D(n)$ or simply $D(n)$-m-tuple, if the product of any two of them increased by n is a perfect square.

Diophantus [25] found the first quadruple $\{1, 33, 68, 105\}$ with the property $D(256)$. The first $D(1)$-quadruple, the set $\{1, 3, 8, 120\}$, was found by Fermat. The folklore conjecture is that there does not exist a $D(1)$-quintuple. In 1969, Baker and Davenport [6] proved that the Fermat's set cannot be extended to a $D(1)$-quintuple. Recently, Dujella proved that there does not exist a $D(1)$-sextuple and there are only finitely many $D(1)$-quintuples (see [32]).

The natural question is how large such sets can be. We define

$$M_n = \sup\{|S| : S \text{ has the property } D(n)\},$$

where $|S|$ denotes the number of elements in the set S. Dujella proved that M_n is finite for all $n \in \mathbb{Z}\backslash\{0\}$. In his proof he estimated the number of "large" (greater than $|n|^3$), "small" (between n^2 and $|n|^3$) and "very small" (less than n^2) elements of a set with the property $D(n)$ by using a theorem of Bennett [8] on simultaneous approximations of algebraic numbers and a gap principle in the first, a weaker variant of the gap principle in the second and a large sieve method due to Gallagher [52] in the third case respectively (cf. [29]). Let us introduce the following notation:

$$\begin{aligned} A_n &= \sup\{|S \cap [|n|^3, \infty\rangle| : S \text{ has the property} D(n)\}, \\ B_n &= \sup\{|S \cap [n^2, |n|^3\rangle| : S \text{ has the property} D(n)\}, \\ C_n &= \sup\{|S \cap [1, n^2\rangle| : S \text{ has the property} D(n)\}. \end{aligned}$$

His result was (cf. [29, Theorem 1, 2, 3 and 4])

$$\begin{aligned} &A_n \leq 21, \\ &B_n \leq 0.65 \log |n| + 2.24, \\ &C_n \leq \begin{cases} 265.55 \log |n| (\log\log |n|)^2 + 9.01 \log\log |n| & \text{for } |n| > 400, \\ 5 & \text{for } |n| \leq 400. \end{cases} \end{aligned}$$

Therefore

$$\begin{aligned} &M_n \leq 32 \quad \text{for } |n| \leq 400, \\ &M_n < 267.81 \log |n| (\log\log |n|)^2 \quad \text{for } |n| > 400. \end{aligned}$$

A polynomial variant of the above problems was first studied by Jones [55], [56], and it was for the case $n = 1$.

Definition 7.1. *Let $n \in \mathbb{Z}[x]$ and let $\{a_1, a_2, \ldots, a_m\}$ be a set of m nonzero polynomials with integer coefficients. We assume that there does not exist a polynomial $p \in \mathbb{Z}[x]$ such that $a_1/p, \ldots, a_m/p$ and n/p^2 are integers. The set $\{a_1, a_2, \ldots, a_m\}$ is called a* polynomial $D(n)$-m-tuple *if for all $1 \leq i < j \leq m$ the following holds: $a_i \cdot a_j + n = b_{ij}^2$, where $b_{ij} \in \mathbb{Z}[x]$.*

Let us mention that the assumption that there does not exist a polynomial p such that $a_1/p, \ldots, a_m/p$ and n/p^2 are integers means for constant n that not all elements $a_1, \ldots, a_m$ of a polynomial $D(n)$-m-tuple are allowed to be constant (compare with Definition 1 in [33] and with Definition 6.1). For linear n the condition under consideration is trivially always satisfied.

In analog to above we are interested in the size of

$$P_n = \sup\{|S| : S \text{ is a polynomial } D(n)\text{-tuple}\}.$$

From the result above (cf. [29, Theorem 1]) it follows that $P_n \leq 22$ for all $n \in \mathbb{Z}$. The above mentioned result about the existence of only finitely many $D(1)$-quintuples implies that $P_1 = 4$. Recently, Dujella and the author proved that $P_{-1} = 3$ (cf. [33], see also Chapter 6) by successfully transferring the needed methods to the polynomial case.

The results of [29], by specialization, give a bound for P_n in terms of the degree and the maximum of the coefficients of n. We conjecture that there should exist a bound for P_n, which depends only on the degree of n. As we have seen, this is true for constant polynomials, and in the present chapter we will prove this conjecture for linear polynomials.

We want to handle the case for linear polynomials, i.e. $n = ax + b$, with integers $a \neq 0$ and b. Let us define

$$L = \sup\{|S| : S \text{ is a polynomial } D(ax+b)\text{-tuple for some } a \neq 0 \text{ and } b\}.$$

We are intended to prove that $L < \infty$. More precisely, we want to find some good upper bound for L.

It is easy to prove that $L \geq 4$. E.g. the set

$$\{x, 16x+8, 25x+14, 36x+20\}$$

is a polynomial $D(16x+9)$-quadruple and the set

$$\{1, 9x^2+8x+1, 9x^2+14x+6, 36x^2+44x+13\}$$

is a polynomial $D(4x+3)$-quadruple (see [26]).

The idea is to estimate the number of polynomials in S with given degree and to consider separate cases whether the degree is “large” or “small”.

In analog to the classical case, we prove our result for “large” degree by using a theorem due to Mason [62] on the polynomial solutions of hyperelliptic equations over function fields in one variable and a gap principle. Let S be a polynomial $D(ax+b)$-m-tuple with integers $a \neq 0$ and b. We prove

Theorem 7.1. *There are at most* 15 *polynomials in* S *with degree* ≥ 4.

We want to remark that a weaker result can be shown by applying the results from the classical integer case. From that it is possible to show that there are at most 21 polynomials in S with degree ≥ 4.

We have to estimate the number of constant, linear, quadratic and cubic polynomials in S. We denote these numbers by L_0, L_1, L_2, L_3 respectively and we will consider them separately. First of all it is trivial to see that we have

$$L_0 \leq 1.$$

By using the mentioned gap principle once more, we get

Theorem 7.2. *There are at most three polynomials in S of degree 3. Therefore, we have*

$$L_3 \leq 3.$$

Let us remark that in fact the proof gives us the following result: There is no polynomial $D(ax+b)$-quadruple which consists of polynomials all having the same degree $\mu \geq 3$. For the case $n=1$ this was already proved by Jones in [56].

By more detailed analysis we get

Theorem 7.3. *There are at most five polynomials in S of degree 2. Therefore, we have*

$$L_2 \leq 5.$$

Theorem 7.4. *There are at most eight linear polynomials in S. Therefore, we have*

$$L_1 \leq 8.$$

Altogether, we can prove the following bound for the size of polynomial $D(n)$-m-tuples for linear polynomials $n = ax+b$.

Theorem 7.5.

$$L \leq 26.$$

In section 7.2, we will collect auxiliary results which are needed to prove our theorems. In section 7.3, we handle Theorem 7.1 and 7.2 which are the cases of large degrees. In section 7.4, we prove the results for the small degrees, i.e. Theorem 7.3 and 7.4 and therefore finally get Theorem 7.5.

7.2 Auxiliary results

Before we can go to the proofs of the theorems, we need the following useful construction with the elements of a polynomial $D(n)$-triple where n is a polynomial with integer coefficients. The construction is a direct modification from the integer case (see [29, Lemma 3]). The analogous statement for polynomial $D(1)$-triples was proved by Jones in [56] and we did already use it in the case $n=-1$ (cf. [33] and Lemma 6.7 in section 6.4).

Lemma 7.1. *Let $\{a,b,c\}$ be a polynomial $D(n)$-triple and let $ab+n=r^2, ac+n=s^2, bc+n=t^2$. Then there exist polynomials $e,u,v,w \in \mathbb{Z}[x]$ such that*

$$ae+n^2=u^2,\ be+n^2=v^2,\ ce+n^2=w^2.$$

More precisely,

$$e = n(a+b+c)+2abc-2rst.$$

Furthermore, it holds:

$$c = a + b + \frac{e}{n} + \frac{2}{n^2}(abe + ruv),$$

where $u = at - rs, v = bs - rt$.

Proof. We have

$$\begin{aligned}(ae + n^2) - (at - rs)^2 &= an(a + b + c) + 2a^2bc - 2arst + n^2 - \\ &\quad -a^2(bc + n) + 2arst - (ab + n)(ac + n) = 0.\end{aligned}$$

Hence, we may take $u = at - rs$, and analogously $y = bs - rt, z = cr - st$. We have

$$\begin{aligned}abe + ruv &= abn(a + b + c) + 2a^2b^2c - 2abrst + abrst - \\ &\quad -a(ab + n)(bc + n) - b(ab + n)(ac + n) + rst(ab + n) = \\ &= -abcn - n^2(a + b) + rstn,\end{aligned}$$

and finally

$$a + b + \frac{e}{n} + \frac{2}{n^2}(abe + ruv) = 2a + 2b + c + \frac{2abc}{n} - \frac{2rst}{n} - \frac{2abc}{n} - 2a - 2b + \frac{2rst}{n} = c.$$

□

If we also define

$$\overline{e} = n(a + b + c) + 2abc + 2rst, \tag{7.1}$$

then easy computation shows that

$$e \cdot \overline{e} = n^2(c - a - b - 2r)(c - a - b + 2r). \tag{7.2}$$

This equation will be very useful in the proof of Theorem 7.2, 7.3 and 7.4.

We conclude this section with the following definition: Let $\mathbb{Z}^+[x]$ denote the set of all polynomials with integer coefficients with positive leading coefficient. For $a, b \in \mathbb{Z}[x]$, $a < b$ means that $b - a \in \mathbb{Z}^+[x]$. The usual fundamental properties of inequality hold for this order. For $a \in \mathbb{Z}[x]$, we define $|a| = a$ if $a \geq 0$, and $|a| = -a$ if $a < 0$.

Observe that it is clear that all leading coefficients of the nonconstant polynomials in a polynomial $D(n)$-m-tuple have the same sign. This implies that there is no loss of generality in assuming that they are all positive, i.e. that all polynomials are in $\mathbb{Z}^+[x]$.

7.3 Elements with large degree

Assume that the set $\{a, b, c, d\}$ is a polynomial $D(n)$-quadruple with $n \in \mathbb{Z}[x]$. Let $ab+n = r^2, ac+n = s^2, bc+n = t^2$ where $r, s, t \in \mathbb{Z}^+[x]$. In this chapter, the symbols r, s, r will always have this meaning. Moreover, we have

$$ad + n = u^2, \quad bd + n = v^2, \quad cd + n = w^2,$$

with $u, v, w \in \mathbb{Z}^+[x]$. Multiplying this equations we get the following hyperelliptic equation

$$(uvw)^2 = (ad + n)(bd + n)(cd + n),$$

where we search for polynomial solutions $d \in \mathbb{Z}[x]$. We will apply Mason's Theorem 1.14 to this equation.

Lemma 7.2. *Let $\{a, b, c, d\}$, $0 < a < b < c < d$ be a polynomial $D(n)$-quadruple with $n \in \mathbb{Z}[x]$. Then*

$$\deg d \leq 51(\deg a + \deg b + \deg c) + 78 \deg n.$$

Proof. Let us denote $X = abcd$ and $Y = abcuvw$. Then by multiplying the above equation with $a^2b^2c^2$ we get

$$Y^2 = (X + nbc)(X + nac)(X + nab).$$

The polynomial on the left hand side becomes

$$\begin{aligned}(X + nbc)(X + nac)(X + nab) &= \\ &= X^3 + n(ab + bc + ac)X^2 + n^2abc(a + b + c)X + n^3a^2b^2c^2\end{aligned}$$

so this polynomial has coefficients and roots in $\mathbb{Z}[x]$. Let S be the set of coefficients of this polynomial, i.e.

$$S = \{1, n(ab + bc + ac), n^2abc(a + b + c), n^3a^2b^2c^2\}.$$

Since the elements of S are polynomials, we get for each $\xi \in \mathbb{C}$ that

$$\nu_\xi(S) = \min_{s\in S}\{0, \nu_\xi(s)\} = 0.$$

Moreover, we have

$$\nu_\infty(S) = \min_{s\in S}\{0, \nu_\infty(s)) = \min_{s\in S}\{-\deg s\} = -\max_{s\in S} \deg s,$$

and by comparing the degrees of the elements of S we get

$$\nu_\infty(S) = -2(\deg a + \deg b + \deg c) - 3 \deg n.$$

Therefore,

$$\begin{aligned}\mathcal{H}(S) = -\sum_{\nu}\min\{0,\nu(S)\} = -\sum_{\xi\in\mathbb{C}}\min\{0,\nu_{\xi}(S)\} - \min\{0,\nu_{\infty}(S)\} =\\ = -\min\{0,\nu_{\infty}(S)\} = 2(\deg a+\deg b+\deg c)+3\deg n.\end{aligned}$$

Thus, we have for the height H of the polynomial on the right hand side of our hyperelliptic equation

$$H = 2(\deg a+\deg b+\deg c)+3\deg n.$$

By Mason's Theorem 1.14 with $L=\mathbb{C}(x)$ and $\mathcal{O}=\mathbb{C}[x]$ we therefore get

$$\deg X \le 52(\deg a+\deg b+\deg c)+78\deg n,$$

where we have used that the genus of the rational function field $\mathbb{C}(x)$ is zero (which can be found e.g. in [90], page 22) and that $\mathbb{C}(x)$ has only one infinite valuation, namely ν_{∞}. But now by the definition of $X = abcd$ we get

$$\deg d \le 51(\deg a+\deg b+\deg c)+78\deg n$$

as claimed in our lemma. □

Observe that due to the sharpness of the fundamental inequality this bound is very good. Especially, it does not depend on a gap which has to appear between the elements of the quadruple as in the classical case (cf. [29, Lemma 2]).

We use Lemma 7.1 to prove the following gap principle. This is very similar to [29, Lemma 4] in the classical case for integers.

Lemma 7.3. *If $\{a,b,c,d\}$ is a polynomial $D(n)$-quadruple where $n\in\mathbb{Z}[x]$ and $2n^2 < a < b < c < d$, then*

$$n^2d > 2bc.$$

Proof. We apply Lemma 7.1 to the triple $\{a,c,d\}$. Let e be defined as in Lemma 7.1. Since $ce+n^2$ is a perfect square, we have that $ce+n^2\ge 0$. Assume that $e\le -1$, then

$$ce+n^2 < -2n^2+n^2 = -n^2 < 0,$$

a contradiction. Therefore, we have $e\ge 0$. Observe that, if $n>0$ we have

$$\begin{aligned}&a^2 < ac+r^2 = ac+ab+n \iff na^2 < na(b+c)+n^2 \iff\\ &a^2t^2 = a^2(n+bc) = na^2+a^2bc < a^2bc+na(b+c)+n^2 =\\ &\qquad\qquad\qquad\qquad = (ab+n)(ac+n) = r^2s^2 \iff\\ &at < rs \iff u < 0,\end{aligned}$$

and

$$\begin{aligned}&b^2 < bc + r^2 = bc + ab + n \iff nb^2 < nb(a+c) + n^2 \iff\\ &b^2s^2 = b^2(ac+n) = ab^2c + b^2n < ab^2c + nb(a+c) + n^2 =\\ &\qquad\qquad\qquad = (ab+n)(bc+n) = r^2t^2 \iff\\ &bs < rt \iff v < 0.\end{aligned}$$

In the same way one can show that $n < 0$ implies

$$u > 0 \quad \text{and} \quad v > 0.$$

If $e = 0$, then $d = a + c + 2s$. If $e \geq 1$, then

$$n^2d = n^2(a+b) + en + 2(abe + ruv) > 2ab.$$

Note that we need here that $uv > 0$ which follows from the comments just made.

Analogously, we apply Lemma 7.1 to the triple $\{b, c, d\}$ and obtain either $d = b+c+2t$ or $n^2d > 2bc$. However, $d = b+c+2t$ is impossible since $s^2 = ac+n < bc+n = t^2$ and therefore $s < t$ which implies $a + c + 2s < b + c + 2t$ and

$$n^2(b + c + 2t) < n^2 4c < 2ac,$$

which follows from

$$t^2 = bc + n \leq (c-1)c + n = c^2 + n - c < c^2 + n - n^2 < c^2$$

since $c > 2n^2$ and consequently $t < c$.

Hence, we proved

$$n^2d > 2bc,$$

as claimed in our lemma. □

Proof of Theorem 7.1.

Assume that $\{a, b, c, a_4, a_5, \ldots, a_{16}\}$ is a polynomial $D(n)$-16-tuple and $|n|^3 \leq a < b < c < a_4 < a_5 < \ldots < a_{16}$. We apply Lemma 7.2 to the quadruple $\{a, b, c, a_{16}\}$ and obtain

$$d_{16} < (abc)^{52}n^{78} < c^{156}n^{78} < c^{182}, \tag{7.3}$$

since $|n|^3 < c$.

Lemma 7.3 implies $n^2a_4 > bc > |n|^3c$ and $a_4 > c|n|$. Furthermore, $n^2a_5 > a_4c > c^2|n|$ and $|n|a_5 > c^2$. In the same manner, Lemma 7.3 gives

$$\begin{array}{lll} n^2a_6 > a_5a_4 > c^3, & |n|^5a_7 > |n|^3a_6a_5 > c^5, & |n|^9a_8 > c^8,\\ n^{16}a_9 > c^{13}, & |n|^{27}a_{10} > c^{21}, & |n|^{45}a_{11} > c^{34},\\ n^{74}a_{12} > c^{55}, & |n|^{121}a_{13} > c^{89}, & |n|^{197}a_{14} > c^{144},\\ |n|^{320}a_{15} > c^{233}, & |n|^{519}a_{16} > c^{377}, & \end{array}$$

which implies (since $|n|^3 < c$) that

$$c^{173}a_{16} > c^{377}$$

and therefore

$$a_{16} > c^{204},$$

a contradiction to (7.3). □

Proof of Theorem 7.2.

Let $S = \{a, b, c\}$ with $a < b < c$ be a polynomial $D(n)$-triple with linear $n \in \mathbb{Z}[x]$ and let $\deg a = \deg b = \deg c = 3$. Then by (7.1) we get $\deg \overline{e} = 9$. But from (7.2) it follows that $\deg e\overline{e} \leq 8$. Thus we have a contradiction unless $e = 0$, i.e. $c = a + b + 2r$. Consequently, if we fix a and b, then c is unique, which implies that S cannot be extended to a polynomial $D(n)$-quadruple. Therefore,

$$L_3 \leq 3,$$

as claimed in our theorem. □

Observe that Theorem 7.2 follows directly from Lemma 7.3, but the above proof gives more information on triples of cubic polynomials.

7.4 Elements with small degree

First we prove Theorem 7.3. Here the argument from the proof of Theorem 7.2 does not longer work. The polynomials e which are induced by a polynomial $D(ax+b)$-triple in Lemma 7.1 are constants. The proof uses the fact that $u^2 - n^2 = (u - n)(u + n)$ is a complete factorization of the polynomial a up to the constant factor e.

Proof of Theorem 7.3.

Let $\{a, b, c\}$ with $a < b < c$ be a polynomial $D(n)$-triple with linear $n \in \mathbb{Z}[x]$ and let $\deg a = \deg b = \deg c = 2$. Then by (7.1) we get $\deg \overline{e} = 6$. Now (7.2) implies that e is a constant. Assume that two distinct e's exist. We call them e and f. From $ae + n^2 = u^2$ we see that a is a product of two linear polynomials:

$$a = \alpha(x - a_0)(x - a_1).$$

Let us assume that we have

$$u - n = \varepsilon_1(x - a_0), \quad u + n = \varepsilon_2(x - a_1),$$

where $\varepsilon_1\varepsilon_2 = \alpha\varepsilon$. It implies

$$2n = x(\varepsilon_2 - \varepsilon_1) + \varepsilon_1 a_0 - \varepsilon_2 a_1.$$

In the same manner, we can conclude from $af + n^2 = u^2$ that

$$u - n = \varphi_1(x - a_0), \quad u + n = \varphi_2(x - a_1),$$

or

$$u - n = \varphi_1(x - a_1), \quad u + n = \varphi_2(x - a_0)$$

holds. Let us first consider that the first of this equations holds. Then we get

$$2n = x(\varphi_2 - \varphi_1) + \varphi_1 a_0 - \varphi_2 a_1,$$

where $\varphi_1\varphi_2 = \alpha f$. Hence, $\varepsilon_2 - \varepsilon_1 = \varphi_2 - \varphi_1, \varepsilon_1 a_0 - \varepsilon_2 a_1 = \varphi_1 a_0 - \varphi_2 a_1$. Consequently, we have $a_0(\varepsilon_1 - \varphi_1) = a_1(\varepsilon_2 - \varphi_2) = a_1(\varepsilon_1 - \varphi_1)$. We have two possibilities: $\varepsilon_1 = \varphi_1$ or $a_0 = a_1$.

We first assume $\varepsilon_1 = \varphi_1$. This implies also $\varepsilon_2 = \varphi_2$ and therefore $e = f$, a contradiction. Now we assume that $a_0 = a_1$ holds. Then $x - a_0|n$ and together with $ab + n = r^2$ this implies $x - a_0|r$. Therefore $(x - a_0)^2|n$, and we obtained a contradiction since n is a linear polynomial.

Now let us consider the second case. So assume that we have

$$u - n = \varphi_1(x - a_1), \quad u + n = \varphi_2(x - a_0),$$

where φ_1, φ_2 are as above. It implies

$$2n = x(\varphi_2 - \varphi_1) + \varphi_1 a_1 - \varphi_2 a_0.$$

Hence, $\varepsilon_2 - \varepsilon_1 = \varphi_2 - \varphi_1, \varepsilon_1 a_0 - \varepsilon_2 a_1 = \varphi_1 a_1 - \varphi_2 a_0$. This yields, $a_0(\varepsilon_1 + \varphi_2) = a_1(\varphi_1 + \varepsilon_2) = a_0(\varepsilon_1 + \varphi_2)$. We have again two possibilities: $\varepsilon_1 = -\varphi_2$ which implies $\varepsilon_2 = -\varphi_1$ and therefore $e = f$, a contradiction, or $a_0 = a_1$. But as above this yields a contradiction with the assumption that n is a linear polynomial.

Therefore, there is at most one such constant e. It follows that for fixed a and b, there are at most three c, namely $c = a + b + 2r$ and two possible $c(e)$ which come from

$$c = a + b + \frac{e}{n} + \frac{2}{n^2}(abe + 2ruv),$$

where u, v satisfy $ae + n^2 = u^2, be + n^2 = v^2$. This last equations fix u and v only up to the sign and therefore we get two possible c's in this case. Consequently we get

$$L_2 \leq 5,$$

which was claimed in Theorem 7.3. □

As in the proof before we will see that also the proof of Theorem 7.4 heavily depends on the fact that we are considering linear polynomials. Especially, we will use that (7.2) is the complete factorization of the product $e\overline{e}$.

Proof of Theorem 7.4.

Let $S = \{a, b, c\}$ with $a < b < c$ be polynomial $D(n)$-triple with linear $n \in \mathbb{Z}[x]$ and let $\deg a = \deg b = \deg c = 1$. Then by (7.1) we get $\deg \overline{e} = 3$. Now (7.2) implies that

$$\deg e \leq 1.$$

From $ab + n = r^2$ it follows that at most one of the elements in S is divisible by n. Indeed, assume that a and b are divisible by n. Then $n|r$ and $n^2|n$, which contradicts the assumption that n is linear polynomial. Thus we may assume that a, b, c are not divisible by n. We have

$$e + \overline{e} = 2n(a + b + c) + 4abc. \tag{7.4}$$

$$\overline{e} - e = 4rst. \tag{7.5}$$

If $n|e$, then (7.2) implies that $n|\overline{e}$ and therefore, by (7.4), we get $n|abc$, a contradiction.

Therefore, $e = \delta \cdot (c - a - b \pm 2r)$, $\delta \in \mathbb{Q}$. Assume that $\delta \neq 0$. We have

$$\overline{e} = n^2(c - a - b \mp 2r)\frac{1}{\delta}.$$

This implies

$$\frac{e}{\delta} - \frac{\overline{e}\delta}{n^2} = \pm 4r$$

or

$$\frac{n^2 e}{\delta} - \overline{e}\delta = \pm 4n^2 r$$

or

$$\frac{n^2 e}{\delta} - e\delta = 4r(\delta st \pm n^2).$$

This can be written as

$$\frac{e}{\delta}(n^2 - \delta^2) = 4r(\delta st \pm n^2).$$

Hence, there are two possibilities: $r|e$ or $r|n \pm \delta$.

If $r|e$, then by (7.5) we have $r|\overline{e}$ which yields

$$r^2|n^2(c - a - b - 2r)(c - a - b + 2r).$$

If $r|n$, then from $ab+n=r^2$ we conclude $r|a$ or $r|b$. Both cases lead to a contradiction since this would imply $n|a$ or $n|b$. Observe that r and n only differ by a constant factor since they are both linear. Thus, $r|c-a-b$, say $c=a+b+r\cdot\rho$, $\rho\in\mathbb{Q}$. But from this we get

$$ac+n=a^2+ab+ar\rho+n=a^2+r^2+\rho ar=s^2$$

or

$$(2r+\rho a)^2-(\rho^2-4)a^2=(2s)^2.$$

Now, if $\rho=\pm 2$ then $c=a+b\pm 2r$. Observe that by considering leading coefficients it is clear that $a+b-2r<b$ so this case is impossible and it remains the possible case $c=a+b+2r$. Otherwise if $\rho\neq\pm 2$, we have

$$(\rho^2-4)a^2=(2r+\rho a-2s)(2r+\rho a+2s)$$

which implies $a|r$ and $a|s$, and moreover, using $ab+n=r^2$, we get $a|n$ or equivalently $n|a$, a contradiction.

Therefore, it remains the case $r|n\pm\delta$. It means that δ is unique. It is defined by $n\equiv\mp\delta \pmod r$. Let $n\equiv\delta_0 \pmod r$. We have the following possibilities for c, namely $c=a+b+2r$ and $c(e)$, where $e=(c-a-b+2r)(-\delta_0)$ or $e=(c-a-b-2r)\cdot\delta_0$. Each of this two e's induce at most two c's as we have seen at the end of the proof of Theorem 7.3. Therefore, we have at most seven linear polynomials in S which are not divisible by n. We get

$$L_1\leq 8,$$

and so the proof is finished. □

Now we are ready to prove our bound for L.

Proof of Theorem 7.5.

Let S be a polynomial $D(ax+b)$-m-tuple with some integers $a\neq 0$ and b. From the fact that the product of each two elements from S plus $ax+b$ is a square of a polynomial with integer coefficients it follows that the set S contains a polynomial with degree ≥ 2, then it contains either polynomials with even or polynomials with odd degree only. Together with the upper bound for the number of polynomials in S with degree ≥ 4, this implies that we have

$$|S|\leq 11+16=27.$$

This proves our theorem. □

Curriculum vitae

Personal Data

Date of Birth: 10.11.1976

Place of Birth: Lienz (Austria)

Nationality: Austrian

Parents: Josef Fuchs (Unterassling 47, 9911 Thal-Assling)
Notburga Fuchs, maiden name: Salcher (deceased in June 1998)

Brothers and Sisters: Thomas, Michael, Daniela, Ursula, Anna

Address: Karl-Morre Str. 46/15, 8020 Graz (Austria)

Phone: +43-316-573513

Education

1983–1987 Primary School in Assling, Tyrol

1987–1991 Secondary School in Lienz, Tyrol

1991–1995 High School in Lienz (with special emphasis on natural science)
School Leaving Examination on June 14, 1995 with honours

1995–2000 Study of Technical Mathematics at the Technical University of Vienna,
Branch: Mathematical Computer Science
First Diploma Examination on March 23, 1997 with first honours
Second Diploma Examination on October 23, 2000 with first honours
Diploma Thesis: "Algebraisch-geometrische Codes"
Advisor: Ao.Univ-Prof. Dr. M. Drmota
Graduation to "Diplom-Ingenieur" (corresponding to Master of Science)

Since 2000 PhD-Studies in Mathematics at the Technical University of Graz
Working Title of the PhD-Thesis: "Quantitative Finiteness Results for

Diophantine Equations"
Advisor: O.Univ-Prof. Dr. R. F. Tichy

Career History

WS 1998/99 Teaching assistent at the Department of Applied and Numerical Mathematics at the Technical University of Vienna

WS 1999/00 Teaching assistent at the Department of Applied and Numerical Mathematics at the Technical University of Vienna

WS 2000/01 Teaching assistent at the Department of Mathematics at the Technical University of Graz

SS 2001 Teaching assistent at the Department of Mathematics and Applied Geometry at the Montanistic University of Leoben and
Teaching assistent at the Department of Mathematics at the Technical Univeristy of Graz

WS 2001/02 Teaching assistent at the Department of Mathematics and Applied Geometry at the Montanistic University of Leoben and
Teaching assistent at the Department of Mathematics at the Technical Univeristy of Graz

June 2000 Collaborator in the research project "Algorithmic Diophantine Problems" (S-8307 MAT) via working contract

July-September 2000 Collaborator in the research project "Algorithmic Diophantine Problems" (S-8307 MAT) via a "Forschungsbeihilfe"

Since November 2000 Employment in the research project "Algorithmic Diophantine Problems" (S-8307 MAT)

Research Interests

Algebraic Number Theory, Diophantine equations, Algebraic Geometry, Algebraic Coding Theory.

Publications

1. A. Dujella and C. Fuchs (2001)
   A polynomial variant of a problem of Diophantus and Euler, to appear in Rocky Mount. J. Math.

2. C. Fuchs and R. F. Tichy (2001)
   Perfect Powers in Linear Recurring Sequences, to appear in Acta Arith.

3. C. Fuchs, A. Pethő and R. F. Tichy (2001)
   On the Diophantine equation $G_n(x) = G_m(P(x))$, submitted for publication.

4. C. Fuchs (2001)
   Exponential-polynomial Equations and Linear Recurring Sequences, submitted for publication.

5. C. Fuchs (2001)
   An upper bound for the G.C.D. of two linear recurring sequences, manuscript.

6. C. Fuchs, A. Pethő and R. F. Tichy (2001)
   On the Diophantine equation $G_n(x) = G_m(P(x))$ for third order linear recurrrences, manuscript.

7. A. Dujella, C. Fuchs and R. F. Tichy (2001)
   Diophantine m-tuples for linear polynomials, manuscript.

Posters and Oral Contributions

1. C. Fuchs: Algebraisch-geometrische Codes, Zahlentheoretisches Kolloquium, Graz, Austria, 17.11.2000.

2. C. Fuchs: On the equation $G_n(x) = G_m(P(x))$, AMS-Sectional Meeting, Hoboken, New Jersey, USA, 28.04.2001.

3. A. Dujella and C. Fuchs: A Polynomial Variant of a Problem of Diophantus and Euler, 15. ÖMG-Kongress, Vienna, Austria, 20.09.2001.

4. C. Fuchs: Exponential-polynomial Equations and Linear Recurring Sequences, Workshop on “Effective methods for Diophantine Equations”, Debrecen, Hungary, 26.10.2001.

5. C. Fuchs: Exponential-polynomial Equations and Linear Recurring Sequences, Zahlentheoretisches Kolloquium, Graz, Austria, 30.11.2001.

Bibliography

[1] A. Baker, Bounds for the solutions of the hyperelliptic equation, *Proc. Cambr. Philos. Soc.* **65** (1969), 439-444.

[2] A. Baker, A sharpening of the bounds for linear forms in logarithms II, *Acta Arith.* **24** (1973), 33-36.

[3] A. Baker, *Transcendental number theory*, Cambridge Univ. Press, Cambridge, 1975.

[4] A. Baker, *The theory of linear forms in logarithms*, In: Transcendence Theory: Advances and Applications, Academic Press, 1977, 1-27.

[5] A. Baker, *New advances in transcendence theory*, Cambridge Univ. Press, Cambridge, 1988.

[6] A. Baker and H. Davenport, The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$, *Quart. J. Math. Oxford Ser.* (2) **20** (1969), 129-137.

[7] A. Baker and G. Wüstholz, Logarithmic forms and group varieties, *J. Reine Angew. Math.* **442** (1993), 19-62.

[8] M. A. Bennett, On the number of solutions of simultaneous Pell equations, *J. Reine Angew. Math.* **498** (1998), 129-137.

[9] F. Beukers and H. P. Schlickewei, The equations $x + y = 1$ in finitely generated groups, *Acta Arith.* **78** (1996), 189-199.

[10] F. Beukers and R. Tijdeman, On the multiplicities of binary complex recurrences, *Compos. Math.* **51** (1984), 193-213.

[11] Y. Bilu and G. Hanrot, Solving Thue equations of high degree, *J. Number Theory* **60** (1996), *no.* 2, 373-392.

[12] Y. Bilu and R. F. Tichy, The diophantine equation $f(x) = g(y)$, *Acta Arith.* **95** (2000), no. 3, 261-288.

[13] P. Borwein and T. Erdélyi, *Polynomials and Polynomial Inequalities*, Springer Verlag, Berlin, 1995.

[14] E. Brown, Sets in which $xy + k$ is always a square, *Math. Comp.* **45** (1985), 613-620.

[15] W. D. Brownawell and D. W. Masser, Vanishing sums in function fields, *Proc. Cambridge Philos. Soc.* **100** (1986), 427-434.

[16] T. S. Chihara, *An Introduction to Orthogonal Polynomials*, Gordon and Breach Science Publishers, New York - London - Paris, 1978.

[17] J. Coates, Construction of rational functions on a curve, *Proc. Camb. Phil. Soc.* **68** (1970), 105-123.

[18] J. H. E. Cohn, On square Fibonacci numbers, *J. Lond. Math. Soc.* **39** (1964), 537-540.

[19] J. H. E. Cohn, Lucas and Fibonacci numbers and some diophantine equations, *Proc. Glasgow Math. Assoc.* **7** (1965), 24-28.

[20] P. Corvaja and U. Zannier, Diophantine equations with power sums and universal Hilbert sets, *Indag. Math., New Ser.* **9 (3)** (1998), 317-332.

[21] P. Corvaja and U. Zannier, Some new applications of the Subspace Theorem, submitted to *Comp. Math.*, 2001.

[22] S. David and P. Philippon, Minorations des hauteurs normalisées des sous-variétés des tores, *Ann. Scuola Norm. Sup. Pisa* **28**, *Cl. Sci.* (4) (1999), 489-543.

[23] S. David and P. Philippon, Errata à: Minorations des hauteurs normalisées des sous-variétés des tores, *Ann. Scuola Norm. Sup. Pisa* **29**, *Cl. Sci.* (4) (2000), 729-731.

[24] L. E. Dickson, "History of the Theory of Numbers" Vol. 2, Chelsea, New York, 1966, 518-519.

[25] Diophantus of Alexandria, Arithmetics and the Book of Polygonal Numbers, (I. G. Bashmakova, Ed.) (Nauka, 1974) (in Russian), 85-86, 215-217.

[26] A. Dujella, Generalization of a problem of Diophantus, Acta Arith. **65** (1993), 15-27.

[27] A. Dujella, On the exceptional set in the problem of Diophantus and Davenport, *Application of Fibonacci Numbers* Vol. 7, (G. E. Bergum, A. N. Philippou, A. F. Horadam, eds.), Kluwer, Dordrecht, 1998, 69-76.

[28] A. Dujella, Complete solution of a family of simultaneous Pellian equations, *Acta Math. Inform. Univ. Ostraviensis* **6** (1998), 59-67.

[29] A. Dujella, On the size of Diophantine m-tuples, *Math. Proc. Cambridge Philos. Soc.* **132** (2002), 23-33.

[30] A. Dujella, An absolute bound for the size of Diophantine m-tuples, *J. Number Theory*, to appear.

[31] A. Dujella, An extension of an old problem of Diophantus and Euler II, *Fibonacci Quart.*, to appear.

[32] A. Dujella, There are only finitely many Diophantine quintuples, preprint.

[33] A. Dujella and C. Fuchs, A polynomial variant of a problem of Diophantus and Euler, *Rocky Mount. J. Math.*, to appear.

[34] A. Dujella, C. Fuchs and R. F. Tichy, Diophantine m-tuples for linear polynomials, manuscript.

[35] A. Dujella and R.F. Tichy, Diophantine equations for second order recursive sequences of polynomials, *Quarterly Journal of Mathematics (Oxford)*, to appear.

[36] B. Edixhoven and J.H. Evertse, *Diophantine Approximation and Abelian Varieties*, Springer Verlag, Berlin, LN **1566**, 1993.

[37] M. Eichler, *Introduction to the theory of algebraic numbers and functions*, Academic Press, New York and London, 1966.

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

[39] J.H. Evertse, On equations in two S-units over function fields of characteristic 0, *Acta Arith.* **47** (1986), 233-253.

[40] J.H. Evertse, An improvement of the quantitative subspace theorem, *Compos. Math.* **101 (3)** (1996), 225-311.

[41] J.H. Evertse and K. Győry, On the number of solutions of weighted unit equations, *Compositio Math.* **66** (1988), 329-354.

[42] 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.

[43] J.H. Evertse and H.P. Schlickewei, The Absolute Subspace Theorem and linear equations with unknowns from a multiplicative group, *Number Theory in Progress* Vol. 1 (Zakopane-Kościelisko, 1997), 121-142, de Gruyter, Berlin, 1999.

[44] J.H. Evertse and H.P. Schlickwei, A quantitative version of the absolute Subspace theorem, *J. reine angew. Math.*, to appear.

[45] J.H. Evertse, H.P. Schlickewei and W. M. Schmidt, Linear equations in variables which lie in a multiplicative group, *Ann. Math.*, to appear.

[46] R. Finkelstein, On Fibonacci numbers which are one more than a square, *J. reine angew. Math.* **262/263** (1973), 171-178.

[47] R. Finkelstein, On Lucas numbers which are one more than a square, *Fibonacci Quart.* **13** (1975), 340-342.

[48] C. Fuchs, Exponential-polynomial equations and linear recurrences, submitted.

[49] C. Fuchs, A. Pethő and R. F. Tichy, On the diophantine equation $G_n(x) = G_m(P(x))$, submitted.

[50] C. Fuchs, A. Pethő and R. F. Tichy, On the equation $G_n(x) = G_m(P(x))$ for third order linear recurrences, manuscript.

[51] C. Fuchs and R. F. Tichy, Perfect powers in linear recurring sequences, *Acta Arith.*, to appear.

[52] P. X. Gallagher, A large sieve, *Acta Arith.* **18** (1971), 77-81.

[53] J. P. Glass, J. H. Loxton and A. J. van der Poorten, Identifying a rational function, *C. R. Math. Rep. Acad. Sci. Canada* **3** (1981), 279-284. Corr. **4** (1982), 309-314.

[54] K. Iwasawa, *Algebraic Functions*, Translations of Mathematical Monographs Vol. 118, American Mathematical Society, Providence, Rhode Island, 1993.

[55] B. W. Jones, A variation of a problem of Davenport and Diophantus, *Quart. J. Math. Oxford* Ser.(2) **27** (1976), 349-353.

[56] B. W. Jones, A second variation of a problem of Davenport and Diophantus, *Fibonacci Quart.* **15** (1977), 323-330.

[57] K. S. Kedlaya, Solving constrained Pell equations, *Math. Comp.* **67** (1998), 833-842.

[58] P. Kiss, Differences of the terms of linear recurrences, *Studia Sci. Math. Hung.* **20** (1985), 285-293.

[59] J. C. Lagarias and D. P. Weisser, Fibonacci and Lucas cubes, *Fibonacci Quart.* **19** (1981), 39-43.

[60] C. Lech, A note on recurring series, Ark. Mat. **2** (1953), 417-421.

[61] H. London and R. Finkelstein, On Fibonacci and Lucas numbers which are perfect powers, *Fibonacci Quart.* **7** (1969), 476-481, 487. Corr. **8** (1970), 248.

[62] R. C. Mason, The hyperelliptic equation over function fields, *Proc. Camb. Philos. Soc.* **93** (1983), 219-230.

[63] R. C. Mason, Equations over function fields, *Proc. Journ. arith.*, Noordwijkerhout/Neth. 1983, LN **1068** (1984), 149-157.

[64] R. C. Mason, *Diophantine equations over function fields*, London Math. Soc. LNS, Cambrdige Univ. Press, Cambridge, 1984.

[65] S. P. Mohanty and A. M. S. Ramasamy, The simultaneous Diophantine equations $5y^2 - 20 = x^2$ and $2y^2 + 1 = z^2$, *J. Number Theory* **18** (1984), 356-359.

[66] J. Müller, S-unit equations in function fields via the *abc*-theorem, *Bull. London Math. Soc.* **32** (2000), *no.* 2, 163-170.

[67] I. Nemes and A. Pethő, Polynomial values in linear recurrences, *Publ. Math.* **31** (1984), 229-233.

[68] I. Nemes and A. Pethő, Polynomial values in linear recurrences II, *J. Number Theory* **24** (1986), 47-53.

[69] A. Pethő, Perfect powers in second order linear recurrences, *J. Number Theory* **15** (1982), 5-13.

[70] A. Pethő, Perfect powers in second order recurrences, Topics in classical number theory, Vol.I,II, Proceedings of the Conference in Budapest 1981, Colloq. Soc. János Bolyai 34, North-Holland, Amsterdam, 1217-1227.

[71] A. Pethő, Full cubes in the Fibonacci sequence, *Publ. Math. Debrecen* **30** (1983), 117-127.

[72] J. van der Poorten and H. P. Schlickewei, *The growth conditions for recurrence sequences*, Macquarie Univ. Math. Rep. 82-0041, North Ryde, Australia, 1982.

[73] A. Schinzel, Reducibility of polynomials in several variables, *Bull. Acad. Polon. Sci., Ser. Sci. Math.* **11** (1963), 633-638.

[74] A. Schinzel, *Polynomials with special regard to reducibility*, Cambridge University Press, Cambridge - New York, 2000.

[75] H. P. Schlickewei, The number of subspaces occurring in the p-adic Subspace Theorem in Diophantine approximation, *J. reine angew. Math.* **406** (1990), 44-108.

[76] H. P. Schlickwei, The quantitative Subspace Theorem for number fields, *Compos. Math.* **82** (1992), 245-273.

[77] H. P. Schlickewei, Multiplicities of recurrence sequences, *Acta Math.* **176** (1996), *no.* 2, 171-243.

[78] H. P. Schlickewei, The multiplicity of binary recurrences, *Invent. Math.* **129** (1997), 11-36.

[79] W. M. Schmidt, The subspace theorem in diophantine approximations, *Compos. Math.* **69** (1989), 121-173.

[80] W. M. Schmidt, "Diophantine Approximation", Springer Verlag, LN **785**, 1980.

[81] W. M. Schmidt, "Diophantine Approximations and Diophantine Equations", Springer Verlag, LN **1467**, 1991.

[82] W. M. Schmidt, The zero multiplicity of linear recurrence sequences, *Acta Math.* **182** (1999), 243-282.

[83] T. N. Shorey and C. L. Stewart, On the Diophantine equation $ax^{2t}+bx^ty+cy^2=d$ and pure powers in recurrence sequences, *Math. Scand.* **52** (1983), 24-36.

[84] T. N. Shorey and C. L. Stewart, Pure Powers in Recurrence Sequences and Some Related Diophantine Equations, *J. Number Theory* **27** (1987), 324-352.

[85] T. N. Shorey and R. Tijdeman, "Exponential Diophantine Equations", Cambridge University Press, Cambridge, 1986.

[86] N. P. Smart, "The Algorithmic Resolution of Diophantine Equations", Cambridge University Press, Cambridge, 1998.

[87] R. Steiner, On nth powers in the Lucas and Fibonacci series, *Fibonacci Quart.* **16** (1978), 451-458.

[88] R. Steiner, On Fibonacci numbers of the form x^2+1, *A Collection of Manuscripts related to the Fibonacci Sequence* (1980), Fibonacci Association, Santa Clara, California, 208-210.

[89] C. L. Stewart, "On Some Diophantine Equations and Related Linear Recurrence Sequences", Sém. de Théorie des Nombres, Paris, 1980-1981, Birkhauser, Boston, 1982.

[90] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer Verlag, Berlin, 1993.

[91] G. Szegő, *Orthogonal Polynomials*, American Mathematical Society Colloquium Publications Vol. 23, Providence, Rhode Island, 1939.

[92] R. Tijdeman, On the equation of Catalan, *Acta. Arith.* **29** (1976), *no.* 2, 197-209.

[93] P. Vojta, A refinement of Schmidt's Subspace Theorem, *Am. J. Math.* **111** (1989), 489-518.

[94] J. F. Voloch, Diagonal equations over function fields, *Bol. Soc. Bras. Mat.* **16** (1985), *no.* 2, 29-39.

[95] M. Waldschmidt, *Diophantine Approximation On Linear Algebraic Groups*, Springer-Verlag, Berlin, 2000.

[96] H. C. Williams, On Fibonacci numbers of the form k^2+1, *Fibonacci Quart.* **13** (1975), 213-214.

[97] O. Wyler, Squares in the Fibonacci series, *Am. Math. Monthly* **71** (1964), 220-222.

[98] U. Zannier, A proof of Pisot's dth root conjecture, *Ann. of Math. (2)* **151**, no. 1 (2000), 375-383.