Functiones et Approximatio
XXXIX.2 (2008), 289–314

ON CERTAIN ARITHMETIC GRAPHS AND THEIR APPLICATIONS TO DIOPHANTINE PROBLEMS

Kálmán Győry

To Professor Władysław Narkiewicz
on his 70th birthday

Abstract: In this paper we continue our investigations concerning arithmetic graphs associated with integral domains and their applications to diophantine problems. We establish some general quantitative theorems for these graphs considered over finitely generated integral domains and prove some effective analogues over number fields and function fields. Further, we apply our results to resultant equations and discriminant equations. In a separate paper, further applications will be given to decomposable form equations, algebraic numbers and irreducible polynomials.
Keywords: Arithmetic graphs, unit equations, polynomials, resultants, discriminants, diophantine finiteness theorems.

1. Introduction

Unit equations and their various generalizations play a role of basic importance in number theory. Many diophantine problems concerning classical diophantine equations, algebraic numbers and irreducible polynomials can be reduced to complicated systems of (generalized) unit equations, in which similar, specific linear dependence relations arise among the equations. In the initial diophantine problems the unknowns are usually zeros of polynomials, conjugate algebraic elements over a field or values of bounded norm of given linear forms at integral points. To give a common, unified treatment and resolution of such diophantine problems, it proved useful to introduce the following arithmetic graphs.

Let R be an integral domain of characteristic 0 which contains 1, and suppose that the unit group R^* of R is of finite rank. For a finite, non-empty subset $\mathcal{M}$ of $R \setminus \{0\}$, we denote by $\mathcal{G}(R, \mathcal{M})$ the graph with vertex set R in which the pair $[\alpha, \beta]$ is an edge if

$$\alpha - \beta \notin \mathcal{M}R^*, \ \ \alpha, \beta \in R \, .$$

This graph and its complement are Cayley graphs of the additive group of R. In diophantine applications, the finite induced subgraphs $\mathcal{G}(\mathcal{A}, \mathcal{M})$ of $\mathcal{G}(R, \mathcal{M})$

2000 Mathematics Subject Classification: primary: 11D61, 11C08; secondary: 05C99.
The author was supported in part by grants T67580 from the HNFSR

are utilized, where $\mathcal{A}$, the vertex set of $\mathcal{G}(\mathcal{A}, \mathcal{M})$, is an appropriate finite ordered subset of R with cardinality $|\mathcal{A}| \geq 3$. Usually $\mathcal{A}$ is chosen to be the set of unknowns mentioned above. If $\mathcal{A}'$ is another ordered subset of R such that $\mathcal{A}' = \varepsilon\mathcal{A} + \beta$ for some $\varepsilon \in R^*$ and $\beta \in R$, then the graphs $\mathcal{G}(\mathcal{A}, \mathcal{M})$ and $\mathcal{G}(\mathcal{A}', \mathcal{M})$ are isomorphic. Then $\mathcal{A}$ and $\mathcal{A}'$ are called equivalent.

The graphs $\mathcal{G}(\mathcal{A}, \mathcal{M})$, in the special case when R is the ring of integers of a number field, were introduced in 1972 by the author [24] for solving an irreducibility problem. Later we extended the concept of these graphs $\mathcal{G} = \mathcal{G}(\mathcal{A}, \mathcal{M})$ to the case when R is the ring of S-integers in a number field, a finitely generated integral domain over $\mathbb{Z}$ or the ring of integers of a function field. It turned out that the connectedness properties of $\mathcal{G}$ and its complement $\overline{\mathcal{G}}$, for example the number of connected components of $\mathcal{G}$, the completeness of $\overline{\mathcal{G}}$ or the existence of a large complete subgraph of $\overline{\mathcal{G}}$ and the connectedness of $\overline{\mathcal{G}}$ as well as of its triangle or quadrangle hypergraph play an important role in the resolution of several diophantine problems. In [27, 33] (number field case), [33] (function field case) and [32, 35, 37] (finitely generated case) we described the structure of the graphs $\mathcal{G}$ and $\overline{\mathcal{G}}$ from the point of view of connectedness. In the number field and the finitely generated cases we showed among others that apart from finitely many equivalence classes of subsets $\mathcal{A}$ of given cardinality, the graph $\mathcal{G}(\mathcal{A}, \mathcal{M})$ has at most two connected components. Further, if $|\mathcal{A}|$ is sufficiently large, $\mathcal{G}(\mathcal{A}, \mathcal{M})$ always has a connected component of order at least $|\mathcal{A}| - 1$.

The connectedness properties of the graphs $\mathcal{G}(\mathcal{A}, \mathcal{M})$ have been used explicitly or implicitly (sometimes as graph method) by many people in their work, including Evertse, Gaál, Leutbecher, Nicklasch, Papp, Schinzel, Shlapentokh, Smart, Stewart, Tijdeman, Wildanger, Yu and the author. By means of these connectedness properties general (qualitative, quantitative and effective) results have been obtained (with or without using graph terminology) on irreducible polynomials (cf. [23, 24, 25, 31, 14, 36, 52]), on triangularly connected decomposable form equations (cf. [41, 26, 28, 30, 32, 54, 55, 56, 22, 21]), on pairs of polynomials of given resultant (cf. [35, 38]), on cliques of exceptional units and Lenstra's construction of Euclidean fields (cf. [27, 46, 45]) and on polynomials and integral elements of given discriminant or on power integral bases (cf. [25, 28, 29, 32, 33, 34, 58, 22, 59, 19, 40]). We note that using our graph method we solved in [25], in effective and more general form, certain unsolved problems proposed by Delone and Faddeev ([9], p. 412, Problem), Nagell ([49], p. 276) and Narkiewicz ([50], p. 541, Problem 19) on polynomials, algebraic integers and algebraic units, respectively, which have given discriminant.

In the present paper we considerably improve and make completely explicit our earlier results on the arithmetic graphs under consideration. In Section 2 we obtain general quantitative theorems over finitely generated domains, while in Section 4 effective results are established over number fields and function fields. As applications, in Sections 3 and 5 we give significant improvements and explicit versions of our earlier theorems on discriminant equations, resultant equations and semi-resultant equations with polynomial unknowns. In Section 5, our theorems concerning resultant equations and semi-resultant equations over function fields

provide the first general effective results on equations of this type. In our proofs we use some deep quantitative as well as effective results on generalized unit equations.

2. Quantitative results in the finitely generated case

Results

Let K be a finitely generated extension field of $\mathbb{Q}$, R a subring of K containing 1, $\mathcal{U}$ a subgroup of finite rank ϱ in the unit group R^* of R with $-1 \in \mathcal{U}$, and $\mathcal{M}$ a finite non-empty subset of $R \setminus \{0\}$. For every pair of distinct positive integers i, j we select an element of $\mathcal{M}$, denoted by δ_{ij}, such that $\delta_{ij} = \delta_{ji}$. For any finite ordered subset $\mathcal{A} = \{\alpha_1, \ldots, \alpha_M\}$ of R, we denote by $\mathcal{G}(\mathcal{A}) = \mathcal{G}_R(\mathcal{A}, \mathcal{U}, \mathcal{M})$ the simple graph with vertex set $\mathcal{A}$ whose edges are the (unordered) pairs $[\alpha_i, \alpha_j]$ for which

$$\alpha_i - \alpha_j \notin \delta_{ij}\mathcal{U} .$$

The ordered subsets $\mathcal{A} = \{\alpha_1, \ldots, \alpha_M\}$ and $\mathcal{A}' = \{\alpha'_1, \ldots, \alpha'_M\}$ of R are called *$\mathcal{U}$-equivalent over R* if

$$\alpha'_i = \varepsilon\alpha_i + \beta \text{ for some } \varepsilon \in \mathcal{U} \text{ and } \beta \in R,\ i = 1, \ldots, M .$$

In this case the graphs $\mathcal{G}(\mathcal{A})$ and $\mathcal{G}(\mathcal{A}')$ are isomorphic. If R is finitely generated over $\mathbb{Z}$, then R^* is also finitely generated (cf. [51]). Then, in the case $\mathcal{U} = R^*$ way say that $\mathcal{A}$ and $\mathcal{A}'$ are *R-equivalent*.

Let $\overline{\mathcal{G}(\mathcal{A})}$ denote the complement of $\mathcal{G}(\mathcal{A})$. Further, denote by $\overline{\mathcal{G}(\mathcal{A})}^{\triangle}$, resp. by $\overline{\mathcal{G}(\mathcal{A})}^{\square}$, the *triangle hypergraph*, resp. the *quadrangle hypergraph* of $\overline{\mathcal{G}(\mathcal{A})}$ whose vertices are the edges of $\overline{\mathcal{G}(\mathcal{A})}$ and whose edges are the cycles[1] $[\alpha_{i_1}, \alpha_{i_2}], \ldots, [\alpha_{i_{k-1}}, \alpha_{i_k}], [\alpha_{i_k}, \alpha_{i_1}]$ in $\overline{\mathcal{G}(\mathcal{A})}$ with $k = 3$, resp. with $k \le 4$, such that

$$\sum_{j \in \mathcal{J}} \left(\alpha_{i_j} - \alpha_{i_{j+1}}\right) \neq 0 \text{ for each non-empty subset } \mathcal{J} \text{ of } \{1, \ldots, k-1\} . \tag{2.1}$$

We note that for $k = 3$, (2.1) automatically holds.

Theorem 2.1. *Let $M \ge 3$ be an integer. Then for all but at most*

$$\left((M+1)^4 e^{18^9(3\varrho+1)}\right)^{M-2} \tag{2.2}$$

$\mathcal{U}$-equivalence classes over R of ordered subsets $\mathcal{A} = \{\alpha_1, \ldots, \alpha_M\}$ of R, one of the following cases holds:

(i) $\mathcal{G}(\mathcal{A})$ is connected and at least one of $\overline{\mathcal{G}(\mathcal{A})}$ and $\overline{\mathcal{G}(\mathcal{A})}^{\square}$ is not connected;

[1] In other words, $\alpha_{i_1}, \ldots, \alpha_{i_k}$ ($k \ge 3$) are distinct elements of $\mathcal{A}$ such that $[\alpha_{i_1}, \alpha_{i_2}]$, …, $[\alpha_{i_{k-1}}, \alpha_{i_k}]$, $[\alpha_{i_k}, \alpha_{i_1}]$ are all edges in $\overline{\mathcal{G}(\mathcal{A})}$.

(ii) $\mathcal{G}(\mathcal{A})$ *has two connected components,* $\mathcal{G}_1$ *and* $\mathcal{G}_2$ *say, such that*[2] $|\mathcal{G}_1| = 1$ *and* $\overline{\mathcal{G}_2}$ *is not connected;*
and, if $M = 4$,

(iii) $\mathcal{G}(\mathcal{A})$ *has two connected components of order* 2 *and* $\overline{\mathcal{G}(\mathcal{A})}^{\square}$ *is not connected.*

This is an explicit version of Theorem 1 in Győry [37]. In [37] our proof did not make it possible to compute the bound corresponding to (2.2). We note that the proof of Theorem 2.1 does not provide any algorithm for determining those $\mathcal{U}$-equivalence classes which do not satisfy (i), (ii), (iii).

In some applications we shall get better results by using the following version of Theorem 2.1.

Theorem 2.2. *Let* $M \geq 3$ *be an integer. Then for all but at most*

$$\left((M+1)^4 2^{16(\varrho+1)}\right)^{M-2} \tag{2.3}$$

$\mathcal{U}$*-equivalence classes over* R *of ordered subsets* $\mathcal{A} = \{\alpha_1, \ldots, \alpha_M\}$ *of* R*, one of the following cases holds:*

(i) $\mathcal{G}(\mathcal{A})$ *is connected and at least one of* $\overline{\mathcal{G}(\mathcal{A})}$ *and* $\overline{\mathcal{G}(\mathcal{A})}^{\triangle}$ *is not connected;*

(ii) $\mathcal{G}(\mathcal{A})$ *has two connected components,* $\mathcal{G}_1$ *and* $\mathcal{G}_2$ *say, such that* $|\mathcal{G}_1| = 1$ *and* $\overline{\mathcal{G}_2}$ *is not connected;*

(iii) $\mathcal{G}(\mathcal{A})$ *has two connected components of order* ≥ 2.

This was earlier proved with (2.3) replaced by a weaker bound which depends, however, on the choice of a transcendence basis of K over $\mathbb{Q}$; see the remark on p. 367 in [37] and Theorem 6 in [35].

Except for certain trivial situations, each of the cases listed in Theorems 2.1 and 2.2 can occur.

In contrast with Theorem 2.1, the case (iii) in Theorem 2.2 cannot be excluded, but the bound in (2.3) is smaller than that in (2.2). Finally we note that our theorems do not remain valid if $\mathcal{U}$ is not of finite rank or if $\mathcal{M}$ is not finite (cf. [32, 35]).

For large M, we obtain the following.

Theorem 2.3. *Let* $\mathcal{A} = \{\alpha_1, \ldots, \alpha_M\}$ *be a finite ordered subset of* R*. If*

$$M > 3 \cdot 2^{16(\varrho+1)} |\mathcal{M}|^2, \tag{2.4}$$

then $\mathcal{G}(\mathcal{A})$ *has at most two connected components, and one of them is of order at least* $M - 1$.

This theorem can be compared with Theorem 11 of [14] and Theorem 2 of [35]. It should be remarked that in [35] the lower bound on M depends also on the choice of a transcendence basis of K over $\mathbb{Q}$.

[2] $|\mathcal{G}|$ denotes the order (number of vertices) of a graph $\mathcal{G}$. Further, $|\mathcal{A}|$ will denote the cardinality of a finite set $\mathcal{A}$.

It is clear that if $\mathcal{A}$ runs through the ordered subsets of cardinality M in R, then among the graphs $\mathcal{G}(\mathcal{A})$ there can be only finitely many non-isomorphic ones. However, our results show that apart from finitely many $\mathcal{U}$-equivalence classes of such subsets $\mathcal{A}$, only certain, well-characterized types of possible graphs of order M can be realized as $\mathcal{G}(\mathcal{A})$. From the point of view of connectedness our Theorems 2.1, 2.2 and 2.3 provide a well-utilizable description of the graphs $\mathcal{G}(\mathcal{A})$.

As will be seen, our above results depend among other things on some quantitative results concerning linear equations with unknowns from a multiplicative subgroup of finite rank of K^*. We note that some function field analogues of our theorems could also be established by means of some recent results of Evertse and Zannier [16] obtained over function fields. We shall not work these out here.

In the following section we give some applications of Theorems 2.1 to 2.3 to discriminant equations and resultant equations. Our theorems have other applications as well, for example to decomposable form equations and irreducible polynomials. These will be the subject of a separate paper.

Proofs

We may and we shall assume in the remaining part of this section that the field K is embedded in $\mathbb{C}$.

Let $q \geq 2$ be an integer, and $(\mathbb{C}^*)^q$ the q-fold direct product of $\mathbb{C}^*$ with coordinatewise multiplication. We say that a subgroup Γ of $(\mathbb{C}^*)^q$ has *rank* r if Γ has a free subgroup Γ_0 of rank r such that for every $\mathbf{u} \in \Gamma$ there is $n \in \mathbb{Z}_{>0}$ with $\mathbf{u}^n \in \Gamma_0$.

To prove our theorems, we shall need the following deep results.

Theorem 2.A. *Let $a_1, \ldots, a_q \in \mathbb{C}^*$, and let Γ be a subgroup of $(\mathbb{C}^*)^q$ of rank r. Then the equation*

$$a_1 u_1 + \cdots + a_q u_q = 1 \quad \text{in } (u_1, \ldots, u_q) \in \Gamma \tag{2.5}$$

has at most $e^{(6q)^{3q}(r+1)}$ solutions with

$$\sum_{i \in I} a_i u_i \neq 0 \quad \text{for each non-empty subset } I \text{ of } \{1, 2, \ldots, q\}. \tag{2.6}$$

Proof. See Theorem 1.1 in [15]. Its proof depends on the Subspace Theorem and hence is ineffective. ■

Let $\mathcal{M}$ and $\mathcal{U}$ be as above.

Theorem 2.B. *For $q = 2$, equation (2.5) has at most*

$$2^{16(\varrho+1)} |\mathcal{M}|^2 \tag{2.7}$$

solutions in u_1, $u_2 \in \mathcal{M}\mathcal{U}$.

Proof. For $q = 2$, every solution u_1, $u_2 \in \mathcal{MU}$ of (2.5) can be written in the form $\delta_1 v_1$, $\delta_2 v_2$, where δ_1, $\delta_2 \in \mathcal{M}$, $(v_1, v_2) \in \mathcal{U}^2$ and

$$(a_1\delta_1)v_1 + (a_2\delta_2)v_2 = 1. \tag{2.8}$$

The number of such equations is at most $|\mathcal{M}|^2$. Further, for fixed δ_1, δ_2, Theorem 1.1 of [3] implies that the number of solutions $(v_1, v_2) \in \mathcal{U}^2$ of (2.8) is at most $2^{16(\varrho+1)}$. This completes the proof. ■

Proof of Theorems 2.1 and 2.2. First consider the case when $\mathcal{U}$ is finitely generated. Denote by $C(q, \mathcal{U})$ the number of solutions of (2.5) with (2.6) in $u_1, \ldots, u_q \in \mathcal{U}$. We proved with Evertse [11] that such a number $C(q, \mathcal{U})$ which is independent of the coefficients $a_1, \ldots, a_q$ exists. Then our Theorem 2.1 was proved in ([37], Theorem 1) with $C(3, \mathcal{U})$ instead of $e^{18^9(3\varrho+1)}$. Further, as was pointed out in Section 2 of [37], the statement of our Theorem 2.2 is true with $C(2, \mathcal{U})$ in place of $2^{16(\varrho+1)}$. But our proofs in [37] remain valid for $\mathcal{U}$ of finite rank as well. Hence Theorems 2.1 and 2.2 immediately follow from the results of [37], Remark 5 of [38] and Theorems 2.A and 2.B above. ■

Proof of Theorem 2.3. We combine the proof of Theorem 2 of [35] with Theorem 2.B. Let $\mathcal{A} = \{\alpha_1, \ldots, \alpha_M\}$ be a finite ordered subset of R, and let $\mathcal{G}_1, \ldots, \mathcal{G}_l$ be the connected components of $\mathcal{G}(\mathcal{A})$ such that $|\mathcal{G}_1| \leq \ldots \leq |\mathcal{G}_l|$. Suppose that $l \geq 3$ or $l = 2$ and $|\mathcal{G}_1| \geq 2$. For $l = 3$, let α_{i_1}, α_{i_2} be vertices of $\mathcal{G}_1$ and $\mathcal{G}_2$, respectively, while for $l = 2$, let α_{i_1}, α_{i_2} be vertices of $\mathcal{G}_1$. Then we have

$$\alpha_{i_2} - \alpha_{i_1} = (\alpha_{i_2} - \alpha_j) + (\alpha_j - \alpha_{i_1})$$

for every vertex α_j from $\mathcal{G}_3, \ldots, \mathcal{G}_l$ if $l \geq 3$, and from $\mathcal{G}_2$ if $l = 2$. Further, $\alpha_{i_2} - \alpha_j$, $\alpha_j - \alpha_{i_1} \in \mathcal{MU}$ for each j. Hence, by Theorem 2.B, the number of α_j under consideration is at most $2^{16(\varrho+1)}|\mathcal{M}|^2$. On the other hand, the number of α_j in question is at least $\frac{1}{3}M$. This implies that if (2.4) holds, then $l = 1$ or $l = 2$ and $|\mathcal{G}_1| = 1$ which proves Theorem 2.3. ■

3. Applications of Theorems 2.1, 2.2 and 2.3 to discriminant equations and resultant equations

Results

Let K be a finitely generated extension field of $\mathbb{Q}$, G a finite normal extension of K, and A an integrally closed subring of K with 1 which has K as its quotient field and which is finitely generated over $\mathbb{Z}$. Then A^*, the unit group of A is finitely generated.

Many diophantine problems can be reduced to *discriminant equations* of the form

$$D(f) \in aA^* \text{ in monic } f \in A[x] \text{ having all their zeros in } G, \tag{3.1}$$

and *resultant equations* of the shape

$$R(f,g) \in aA^* \text{ in monic } f,g \in A[x] \text{ having all their zeros in } G. \tag{3.2}$$

Here $D(\ )$ denotes discriminant, $R(\ ,\ )$ resultant and a is a fixed non-zero element of A.

In this section we deduce from Theorems 2.1, 2.2 and 2.3 some quantitative finiteness results for (3.1) and (3.2). For this we shall need some notation and definitions. Since A is integrally closed and finitely generated over $\mathbb{Z}$, the integral closure $\widehat{A}$ of $A\left[a^{-1}\right]$ in G and its unit group $\widehat{A}^*$ are finitely generated (cf. [48, 44]). Denote by ϱ the rank of $\widehat{A}^*$.

First consider equation (3.1). The monic polynomials f, f' in $A[x]$ are called A-*equivalent* if $f'(x) = \varepsilon^{\deg(f)} f(x/\varepsilon + b)$ for some $\varepsilon \in A^*$ and $b \in A$. If f is a solution of (3.1) then so is every f' which is A-equivalent to f. It was proved in [32] that there are only finitely many A-equivalence classes of monic polynomials $f \in A[x]$ which satisfy (3.1). Later some quantitative versions and an effective variant were established in [10], [38] and in [34], respectively. In the special case when A is a ring of S-integers of a number field, see also [29] and the references given there. Analogous results concerning binary forms with S-integer coefficients are given in [4], [12], [1] and [40].

Theorem 3.1. *Let $m \geq 2$ be an integer. If $f(x)$ is a solution of (3.1) with degree m, then*

$$m \leq 3 \cdot 2^{16(\varrho+1)}. \tag{3.3}$$

Further, the number of A-equivalence classes of solutions $f(x)$ of (3.1) with degree m is at most

$$\left((m+1)^4 2^{17(\varrho+1)}\right)^{m-1}. \tag{3.4}$$

Theorem 3.1 can be compared with the corresponding results of [10] and [38]. In contrast with the bounds established in [10] and [38], our bounds in (3.3) and (3.4) are independent of the choice of the transcendence basis of K over $\mathbb{Q}$.

Similarly to the earlier versions, Theorem 3.1 has many applications in algebraic number theory (cf. [32], [34] and [10]). We present here an application to the equation

$$D_{L/K}(\alpha) \in aA^* \quad \text{in } \alpha \in B, \tag{3.5}$$

where L is an extension of K of degree $m \geq 2$, B denotes the integral closure of A in L, and we assume that G is the normal closure of L over K.

Two elements α, α' of B are said to be A-*equivalent* if $\alpha' = \varepsilon\alpha + b$ for some $\varepsilon \in A^*$ and $b \in A$. In this case, if α is a solution of (3.5) then so is α' as well. It was proved in [32] in a qualitative form and in [25, 34] in an effective form that there are only finitely many A-equivalence classes of elements $\alpha \in B$ satisfying (3.5). Applying Theorem 3.1 to the minimal polynomials over K of the solutions α of (3.5) and following the proof of Theorem 5 of [32], we obtain at once the following.

Theorem 3.2. *The number of A-equivalence classes of $\alpha \in B$ which satisfy* (3.5) *can be estimated from above by an effectively computable constant depending only on m and ϱ.*

This may be compared with Theorem 3 of [10] where the bound depends also on the choice of a transcendence basis of $K/\mathbb{Q}$.

From (3.4) it is easy to deduce an explicit version of Theorem 3.2. We note that a slightly better bound can be obtained by applying Theorem 2.B in a direct way to equation (3.5). Such an improvement will be given in a forthcoming work.

Consider now equation (3.2). We call the pairs (f, g) and (f', g') of monic polynomials in $A[x]$ *A-equivalent* if $f'(x) = \varepsilon^{\deg(f)} f\,(x/\varepsilon + b)$, $g'(x) = \varepsilon^{\deg(g)} g\,(x/\varepsilon + b)$ for some $\varepsilon \in A^*$ and $b \in A$. If (f, g) is a solution of (3.2) then so is every (f', g') which is A-equivalent to (f, g). We proved in [38] (see also [35] and [13]) in a quantitative form that there are only finitely many A-equivalence classes of pairs (f, g) with (3.2) for which $\deg(f)$ and $\deg(g)$ are fixed and

$$\omega(f) \geq 2,\ \omega(g) \geq 2 \text{ and } \omega(f) + \omega(g) \geq 5. \tag{3.6}$$

Here $\omega(f)$ resp. $\omega(g)$ denote the number of distinct zeros of f resp. of g. We note that the assumption (3.6) is necessary for the finiteness. In the special case when A is a ring of S-integers of a number field, the quantitative results of [38] were improved and extended in [2] to the case of binary forms.

The results of [35], [38] and [2] as well as the following Theorem 3.3 are ineffective. Some special but effective related results concerning (3.2) over $\mathbb{Z}$ can be found in [20] and [43].

Theorem 3.3. *If (f, g) is a solution of (3.2) with (3.6), then*

$$\omega(f) + \omega(g) \leq 3 \cdot 2^{17(\varrho+1)}. \tag{3.7}$$

Further, for given integers $m \geq 2$, $n \geq 2$ with $m + n \geq 5$, the number of A-equivalence classes of solutions (f, g) of (3.2) with (3.6) and with $\deg(f) = m$, $\deg(g) = n$ is at most

$$\left((m+n)^4\, e^{4 \cdot 18^9 (\varrho+1)}\right)^{m+n-2}. \tag{3.8}$$

This can be compared with the corresponding results of [35], [38] where the upper bounds depend on the choice of a transcendence basis of $K/\mathbb{Q}$. Further, those bounds contain certain unspecified factors which, at that time, were not effectively computable.

We consider now a common generalization of equations (3.1) and (3.2). For monic polynomials $f,\ g \in K[x]$ with zeros $\alpha_1, \ldots, \alpha_m$ and $\beta_1, \ldots, \beta_n$, respectively, the *semi-resultant* $R^*(f, g)$ of f and g is defined by

$$R^*(f, g) = \widetilde{\prod}_{i,j} (\alpha_i - \beta_j)\ ,$$

where the product $\widetilde{\prod}$ is over all pairs i, j such that $\alpha_i - \beta_j \neq 0$. Then (cf. e.g. [38]) $R^*(f,g) \in K \setminus \{0\}$ and, for $f,\ g \in A[x]$, $R^*(f,g) \in A \setminus \{0\}$. If f and g have no common zero then $R^*(f,g) = R(f,g)$. Further, if f has no multiple zero then $R^*(f,f) = (-1)^{\binom{m}{2}} D(f)$, where $m = \deg(f)$. Hence the semi-resultant is a common generalization of the resultant and of the discriminant. Similarly, the *semi-resultant equation*

$$R^*(f,g) \in aA^* \text{ in monic } f,g \in A[x] \text{ having all their zeros in } G \tag{3.9}$$

is a common generalization of (3.1) and (3.2). Semi-resultants have applications not only in diophantine number theory but also in transcendental number theory; see e.g. [8] and [5].

As was seen in [38], we can obtain finiteness results for the solutions of (3.9) only if we restrict ourselves to those solutions (f,g) for which

$$\omega(f) \geq 2, \omega(g) \geq 2 \text{ and if } f,g \text{ have no common zero then } \omega(f) + \omega(g) \geq 5. \tag{3.10}$$

Quantitative finiteness theorems on the solutions of (3.9) with (3.10) were given in [38]. In the special case when A is a ring of S-integers of a number field, qualitative versions were obtained in [39] for binary forms with S-integer coefficients.

The following theorem is an explicit and improved version of the main results (Theorems 1 and 2) of [38].

Theorem 3.4. *If (f,g) is a solution of (3.9) with (3.10), then (3.7) holds. Further, for given integers $m \geq 2$, $n \geq 2$, the number of A-equivalence classes of solutions (f,g) of (3.9) with (3.10) and with $\deg(f) = m$, $\deg(g) = n$ does not exceed the bound occurring in (3.8).*

Theorems 3.1 and 3.3 are immediate consequences of Theorem 3.4, except for (3.4) which is better than that implied by (3.8). However, as we shall see, following the proof of Theorem 3.4 in the special situation considered in Theorem 3.1 and using Theorem 2.2 in place of Theorem 2.1, (3.4) follows in a straightforward way.

Remark 1. Of particular interest are Theorems 3.1 to 3.4 in the special case when K is a number field and A is the ring of S-integers of K for some finite set S of places of K containing all infinite places. If G is a finite normal extension of K with degree $\delta \geq 1$, s denotes the cardinality of S and $\omega_S(a)$ is the number of distinct prime ideal divisors of a in A, then the parameter ϱ occurring in our theorems satisfies

$$\varrho \leq (s + \omega_S(a) - 1)\,\delta\ .$$

In this special situation our Theorems 3.1 to 3.4 can be compared with the corresponding results of [10], [38], [1] and [2]. ■

Proofs

Proof of Theorem 3.4. We follow the proofs of Theorems 1 and 2 of [38]. Only those steps will be detailed which differ from those in [38].

For a solution (f, g) of (3.9) with (3.10) we denote by $\alpha_1, \dots, \alpha_k$ $(k \geq 0)$ the distinct zeros of f which differ from the zeros of g, by $\beta_1, \dots, \beta_l$ $(l \geq 0)$ the distinct zeros of g which are not zeros of f, and by $\gamma_1, \dots, \gamma_p$ $(p \geq 0)$ the distinct zeros of $\gcd(f, g)$. Let $\mathcal{A} = \{\alpha_1, \dots, \alpha_k, \beta_1, \dots, \beta_l, \gamma_1, \dots, \gamma_p\}$. Then each element of $\mathcal{A}$ is contained in $\widehat{A}$ and, by (3.9),

$$R^*(f, g) \in \widehat{A}^*. \tag{3.11}$$

Consider the graph $\mathcal{G}(\mathcal{A}) = \mathcal{G}_R(\mathcal{A}, \mathcal{U}, \mathcal{M})$ with the choice $R = \widehat{A}$, $\mathcal{U} = \widehat{A}^*$ and $\mathcal{M} = \{1\}$. Then (3.11) implies that the subgraphs of $\mathcal{G}(\mathcal{A})$ having vertex sets $\{\alpha_1, \dots, \alpha_k\}$, $\{\beta_1, \dots, \beta_l\}$, $\{\gamma_1\}, \dots, \{\gamma_p\}$, respectively, are disconnected. Put $M = k + l + p$. If $M > 3 \cdot 2^{16(\varrho+1)}$, then using (3.10) we infer that $\mathcal{G}(\mathcal{A})$ has either at least three connected components or two connceted components of order ≥ 2. However, this contradicts Theorem 2.3. Thus $M \leq 3 \cdot 2^{16(\varrho+1)}$. But $\omega(f) + \omega(g) \leq 2M$, hence (3.7) follows.

To derive the bound (3.8), fix the degrees $\deg(f) = m$ and $\deg(g) = n$. As in [38], it suffices to deal with the number of tuples $\mathcal{A} = \{\alpha_1, \dots, \alpha_k, \beta_1, \dots, \beta_l, \gamma_1, \dots, \gamma_p\}$ for fixed k, l, p and fixed multiplicities of the zeros. Then later, the bound obtained for the number of tuples under consideration must be multiplied by 2^{m+n-2}.

For simplicity, denote by $\{x_1, \dots, x_M\}$ the tuple $\mathcal{A}$. Then (3.9) may be written as

$$\widetilde{\prod} (x_i - x_j)^{a_{ij}} \in aA^* \subset \widehat{A}^* \tag{3.12}$$

with fixed positive integers a_{ij}, where the x_i are zeros of f and x_j are zeros of g. Since each factor $x_i - x_j \in \widehat{A}$, this implies that $x_i - x_j \in \widehat{A}^*$ for all pairs under consideration.

If $M \geq 3$, we can apply Theorem 2.1 with $R = \widehat{A}$, $\mathcal{U} = \widehat{A}^*$, $\mathcal{M} = \{1\}$. Then it is easy to check that, by (3.10), none of the cases (i), (ii), (iii) of Theorem 2.1 can hold for $\mathcal{G}(\mathcal{A})$. Hence Theorem 2.1 implies that

$$x_i = \tau x_i' + \beta \text{ for } i = 1, \dots, M, \tag{3.13}$$

where $\tau \in \widehat{A}^*$, $\beta \in \widehat{A}$, and where the number of possible tuples $\mathcal{A}' = \{x_1', \dots, x_M'\}$ is at most

$$C_1 := \left\{ (M+1)^4 e^{18^9(3\varrho+1)} \right\}^{M-2}.$$

Further, $M \leq m + n$. If $M = 2$, then (3.13) immediately follows from (3.12) with $C_1 = 1$.

It remains to show that any two $\widehat{A}$-equivalent tuples $(x_1, \dots, x_M)$, $(x_1', \dots, x_M')$ satisfying (3.9) or (3.12) (with the same multiplicities) are in fact A-equivalent. So

assume that (3.13) holds for these tuples. Then $(x_i - x_j) = \tau\left(x'_i - x'_j\right)$ for all i, j. This determines τ uniquely. On the other hand by applying any σ from $\mathrm{Gal}(G/K)$ and observing that $(x_1, \ldots, x_M)$ and $(x'_1, \ldots, x'_M)$ are permuted in the same way by σ it follows that $\sigma(\tau) = \tau$. Hence $\tau \in K$. In view of (3.12) we obtain $\tau^b \in A^*$ where $b = \sum_{i,j} a_{ij}$. Since A is integrally closed this implies $\tau \in A^*$. Again by conjugation, it follows that $\beta = x_i - \tau x'_i \in K$ for $i = 1, \ldots, M$ and then $\beta \in A$ since β is integral over A and A is integrally closed. So the tuples in question are A-equivalent, and after some computation (3.8) follows. ■

Proof of Theorems 3.1 and 3.3. As was mentioned after the enunciation of Theorem 3.4, Theorem 3.3 and (3.3) of Theorem 3.1 immediately follow from Theorem 3.4. The bound in (3.4) can be easily derived by combining the proof of Theorem 3.4 with Theorem 2.2. ■

4. Effective results concerning the graphs $\mathcal{G}(\mathcal{A})$ in the number field and function field cases

Results

Let K be an algebraic number field (number field case) or a function field of one variable (function field case) over an algebraically closed field $\mathbf{k}$ of characteristic 0. Then K is a finite extension of $\mathbb{Q}$, resp. of the rational function field $\mathbf{k}(z)$. Denote by d the degree of this extension.

In order to make effective computations in the function field case, it is necessary to assume that $\mathbf{k}$ is explicitly presented in the sense of [17]. This means in our situation that we can perform all the field operations with elements of $\mathbf{k}$ and that there is an algorithm to determine the zeros of any polynomial with coefficients in $\mathbf{k}$.

In the number field case let M_K denote the set of places on K, while in the function field case the set of valuations of $K/\mathbf{k}$ with value group $\mathbb{Z}$. In the number field case

$$h(\alpha) = \frac{1}{d} \sum_{v \in M_K} \log \max\left(1, |\alpha|_v\right)$$

will denote the absolute logarithmic height of $\alpha \in K$, where the absolute value $|\alpha|_v$ is normalized in the usual way. In the function field case we denote by

$$h_K(\alpha) = \sum_{v \in M_K} \max\left(v(\alpha), 0\right)$$

the height of $\alpha \in K \setminus \{0\}$, and we put $h_K(0) = 0$. In what follows, $h(\,)$ and $h_K(\,)$ will be called simply (additive) heights. For their properties, see e.g. [57], [34], [47].

Let S be a finite subset of M_K which contains in the number field case the set of infinite places of K, and in the function field case the infinite valuations v of K for which $v(z) < 0$. The element $\alpha \in K$ is called S-integer if for every $v \in M_K \setminus S$,

$|\alpha|_v \le 1$ in the number field case, and $v(\alpha) \ge 0$ in the function field case. The ring of S-integers and its unit group will be denoted by O_S and O_S^*, respectively.

For $\alpha \in K \setminus \{0\}$, the (additive) *$S$-norm* is defined by

$$N_S(\alpha) = \begin{cases} \sum_{v \in S} \log |\alpha|_v & \text{in the number field case,} \\ \\ -\sum_{v \in S} v(\alpha) & \text{in the function field case.} \end{cases}$$

We note that in both cases $N_S(\alpha) \ge 0$ if $\alpha \in O_S$. Further, for $\alpha \in O_S$, $N_S(\alpha) = 0$ if and only if $\alpha \in O_S^*$.

For a finite subset $\mathcal{A} = \{\alpha_1, \dots, \alpha_M\}$ of O_S and for $N \ge 0$, we denote by $\mathcal{G}(\mathcal{A}) = \mathcal{G}_K(\mathcal{A}, S, N)$ the graph with vertex set $\mathcal{A}$ whose edges are the (unordered) pairs $[\alpha_i, \alpha_j]$ such that

$$N_S(\alpha_i - \alpha_j) > N \, .$$

In the special case when K is a number field, $R = O_S$, $\mathcal{U} = O_S^*$ and $\mathcal{M}$ is a maximal set of pairwise non-associate elements of O_S with S-norm $\le N$, the graph $\mathcal{G}_R(\mathcal{A}, \mathcal{U}, \mathcal{M})$ defined in Section 1 is just the graph $\mathcal{G}_K(\mathcal{A}, S, N)$. With the terminology of Section 1 we say that the ordered subsets $\mathcal{A}$, $\mathcal{A}'$ of O_S are *O_S-equivalent* if $\mathcal{A}' = \varepsilon\mathcal{A} + \beta$ with some $\varepsilon \in O_S^*$ and $\beta \in O_S$. Then $\mathcal{G}(\mathcal{A})$ and $\mathcal{G}(\mathcal{A}')$ are isomorphic.

To state our results, we need some further notation. Let s denote the cardinality of S. Further, in the number field case let r, R_K and h_K denote the unit rank, regulator and class number of K, R_S the S-regulator of K (for its definition see e.g. [7]), and P and Q the maximum and the product of the norms of the prime ideals corresponding to the finite places in S (with the convention that $P = Q = 1$ if S consists only of infinite places). Put

$$E := 160 r^{r+1} R_K + \frac{h_K}{d} \log Q + \frac{1}{d} N \, .$$

In the function field case we denote by g^* the genus of $K/\mathbf{k}$. We use the notation $\log^* a$ for $\max(1, \log a)$.

Theorem 4.1. *For given $M \ge 3$, let $\mathcal{A} = \{\alpha_1, \dots, \alpha_M\}$ be a subset of O_S. Then at least one of the following cases holds:*

(i) $\mathcal{G}(\mathcal{A})$ is connected and at least one of $\overline{\mathcal{G}(\mathcal{A})}$ and $\overline{\mathcal{G}(\mathcal{A})}^{\triangle}$ is not connected;

(ii) $\mathcal{G}(\mathcal{A})$ has two connected components, $\mathcal{G}_1$ and $\mathcal{G}_2$ say, such that $|\mathcal{G}_1| = 1$ and $\overline{\mathcal{G}_2}$ is not connected;

(iii) $\mathcal{G}(\mathcal{A})$ has two connected components of order ≥ 2;

(iv) there exists $\sigma \in O_S \setminus \{0\}$ such that in the number field case

$$\max_{1 \le i,j \le M} h\left((\alpha_i - \alpha_j)/\sigma\right) < 2^{15} M^3 (16ds)^{2(s+2)} P R_S \left(\log^* R_S\right) E, \qquad (4.1)$$

while in the function field case

$$\max_{1\le i,j\le M} h_K\left((\alpha_i-\alpha_j)/\sigma\right) < M^3\left(s+3N+2g^*-2\right). \tag{4.2}$$

Furthermore, σ can be chosen so that in the number field case $\sigma \in O_S^*$, and in the function field case $\sigma = \alpha_k - \alpha_l$ for some edge $[\alpha_k, \alpha_l]$ of $\overline{\mathcal{G}(\mathcal{A})}$ [3].

In the number field case this furnishes an effective version of our Theorem 2.2. In this case Theorem 4.1 implies that for given $M \ge 3$, there are only finitely many O_S-equivalence classes of subsets $\mathcal{A} = \{\alpha_1, \dots, \alpha_M\}$ in O_S for which neither of (i), (ii) and (iii) holds, and a representative in each class can be effectively determined. We note that this finiteness result does not remain valid in the function field case even for $N = 0$. Indeed, in this case fix an element ε of $O_S^*/\mathbf{k}$ such that $1-\varepsilon \in O_S^*$, and let $\eta_4, \dots, \eta_{M-1}$ be distinct fixed elements of $\mathbf{k}$ which differ from 0 and 1. If η_M runs through the elements of $\mathbf{k}$, the subsets $\mathcal{A} = \{0, 1, \varepsilon, \eta_4, \dots, \eta_{M-1}, \eta_M\}$ are pairwise O_S-inequivalent. Further, it is easy to see that our Theorem 2.3 has no analogue in the function field case.

Our Theorem 4.1 and its complement Proposition 4.3 can be compared with Theorem 1 of [27] (number field case) and Theorem 1.1 of [33] (number field and function field cases). The bounds in Theorem 4.1 and Proposition 4.3 are much better in terms of most parameters than the corresponding ones in [27, 33]. My thesis [33] was written in Hungarian and is available in Hungary only. In the function field case Theorem 4.1 and Propositions 4.2 and 4.3 below are the first results on the graphs under consideration which are published in an international periodical.

The following result which is of independent interest will be used in the proof of Theorem 4.1. In the important special case when $\overline{\mathcal{G}(\mathcal{A})}$ is complete, Proposition 4.2 gives much better bounds than (4.1) and (4.2).

Proposition 4.2. *Under the notation and assumptions of Theorem 4.1, suppose that both $\overline{\mathcal{G}(\mathcal{A})}$ and $\overline{\mathcal{G}(\mathcal{A})}^{\triangle}$ are connected. Then the case* (iv) *of Theorem 4.1 holds. If in particular $\overline{\mathcal{G}(\mathcal{A})}$ is complete then, in (4.1) and (4.2), M^3 can be replaced by* 5. *Further, if $N = 0$, in the function field case either $(\alpha_i - \alpha_j)/\sigma$ lies in $\mathbf{k}$ for each i, j, or it has only finitely many possibilities in K for each i, j, which may be determined effectively.*

In terms of certain parameters this Proposition can be regarded as a significant improvement of Lemma 3 of [27] and Lemma 1.9 of [33]. These weaker versions were applied in [30] to decomposable form equations and in [29] to polynomials of given discriminant.

The next proposition makes more precise the statement in (iii) of Theorem 4.1, at the price of replacing the bounds in (4.1) and (4.2) by larger ones.

Proposition 4.3. *Under the notation and assumptions of Theorem 4.1, suppose that $\mathcal{G}(\mathcal{A})$ has two connected components of order ≥ 2. Then at least one of the following cases holds:*

[3] This implies that $N_S(\sigma) \le N$.

(i) both components of $\mathcal{G}(\mathcal{A})$ are complete, and in the function field case $M = 4$;
(ii) there exists $\sigma \in O_S \setminus \{0\}$ such that in the number field case

$$\max_{1\le i,j\le M} h\left((\alpha_i - \alpha_j)/\sigma\right) < 2^{31} M^6 (16ds)^{4(s+2)} \left(PR_S \left(\log^* R_S\right)\right)^2 E, \tag{4.3}$$

and in the function field case

$$\max_{1\le i,j\le M} h_K\left((\alpha_i - \alpha_j)/\sigma\right) < 3M^3 \left(s + 4N + \max(2g-2, 0)\right). \tag{4.4}$$

Further, σ can be chosen as in Theorem 4.1.

As we shall see, the proofs of Theorem 4.1 and Propositions 4.2, 4.3 are based on some profound effective results on S-unit equations.

Our results presented in this section have several applications, among other things to discriminant equations, resultant equations, decomposable form equations and irreducible polynomials. Some applications will be given in the next section. Other applications will be published in a separate paper.

Proofs

We keep the notation of the first part of this section. We shall deal simultaneously with the number field and the function field cases.

For $q \ge 3$, consider the equation

$$u_1 + \cdots + u_q = 0 \text{ in } u_i \in O_S \setminus \{0\} \text{ with } N_S(u_i) \le N \text{ for } i = 1, \ldots, q. \tag{4.5}$$

If $N = 0$, this is just an S-unit equation.

The following theorems will play a crucial role in our proofs. They are of fundamental importance for many other applications. In the number field case, the proof of Theorem 4.A involves the theory of logarithmic forms.

Theorem 4.A. *In the number field case, let $q = 3$ and let u_1, u_2, u_3 be a solution of (4.5). Then there is a $\sigma \in O_S^*$ such that*

$$\max_{1\le i\le 3} h\left(u_i/\sigma\right) < 2^{15} \left(16ds\right)^{2(s+2)} PR_S \left(\log^* R_S\right) E. \tag{4.6}$$

In the function field case, let $q \ge 3$ and let $u_1, \ldots, u_q$ be a solution of (4.5) for which $u_1 + u_2 + \cdots + u_q$ has no proper vanishing subsum. Then with the choice $\sigma = u_q$ we have

$$\max_{1\le i\le q} h_K\left(u_i/\sigma\right) < \frac{1}{2}(q-1)(q-2)\left(s + qN + \max(2g^* - 2, 0)\right). \tag{4.7}$$

Remark 2. As will be apparent from the proof of the function field case, for $q = 3$ $\max(2g^* - 2, 0)$ may be replaced by $2g^* - 2$ in (4.7). ■

Proof of Theorem 4.A. In the number field case, Theorem 4.A is an immediate consequence of Corollary 1 of Győry and Yu [42]. In fact, in terms of n and s a slightly better bound can be deduced from that result of [42] by a careful computation.

Next consider equation (4.5) in the function field case. Let $u_1, \dots, u_q$ be a solution of (4.5) for which $u_1 + \cdots + u_q$ has no proper vanishing subsum. Then $v(u_i) \geq 0$ for every i and every $v \in M_K \setminus S$. Let S_1 denote the smallest subset of M_K such that $S_1 \supseteq S$ and that $u_1, \dots, u_q$ are already S_1-units, i.e. $v(u_i) = 0$ for each i and for every $v \in M_K \setminus S_1$. It follows from the sum formula that

$$N \geq N_S(u_i) = \sum_{v \in M_K \setminus S} v(u_i), \quad i = 1, \dots, q \,,$$

whence

$$\sum_{v \in M_K \setminus S} (v(u_1) + \cdots + v(u_q)) \leq qN \,.$$

By the minimal choice of S_1 we have

$$v(u_1) + \cdots + v(u_q) \geq 1 \text{ for every } v \in S_1 \setminus S \,,$$

hence $|S_1 \setminus S| \leq qN$. This gives that

$$|S_1| \leq s + qN. \tag{4.8}$$

Since in (4.5) $u_1/u_q, \dots, u_{q-1}/u_q$ are S_1-units, Theorem B of Brownawell and Masser [6] implies that

$$\max_{1 \leq i \leq q} h_K(u_i/u_q) < \frac{1}{2}(q-1)(q-2)\,(|S_1| + \max(2g^* - 2, 0))\,. \tag{4.9}$$

Further, if $q = 3$ then by Theorem 4.B below, $\max(2g^* - 2, 0)$ can be replaced by $2g^* - 2$. Together with (4.8), (4.9) implies (4.7) with the choice $\sigma = u_q$. ■

For $q = 3$, Theorem 4.A implies in the number field case that $u_1/\sigma, u_2/\sigma$ and u_3/σ may be effectively determined. The same is true in the function field case if $N = 0$.

Theorem 4.B. *Consider equation (4.5) in the function field case with $q = 3$, $N = 0$, and let u_1, u_2, u_3 be a solution of this equation. Then we have*

$$\max_{1 \leq i \leq 3} h_K(u_i/\sigma) \leq s + 2g^* - 2 \tag{4.10}$$

with the choice $\sigma = u_3$. Further, u_1/σ and u_2/σ either lie in $\mathbf{k}$, or they have only finitely many possibilities in K, which may be determined effectively.

Proof. This is a special case of Lemma 2 and its Corollary of Mason [47], Chapter 1. ■

Proof of Proposition 4.2. We use an idea which was applied several times in our earlier papers; see e.g. Lemma 2 in [27] and the references given there.

We shall apply repeatedly Theorems 4.A and 4.B. Denote by C_2 the upper bound occurring in (4.6), resp. in (4.7) with $q = 3$, according as we are concerned with the number field or function field case. Let $\mathcal{A} = \{\alpha_1, \dots, \alpha_M\}$ be a finite subset of O_S with $M \geq 3$, and assume that both $\overline{\mathcal{G}(\mathcal{A})}$ and $\overline{\mathcal{G}(\mathcal{A})}^{\triangle}$ are connected. We first prove (4.1) and (4.2) for those pairs α_i, α_j for which $[\alpha_i, \alpha_j]$ is an edge in $\overline{\mathcal{G}(\mathcal{A})}$. We may assume without loss of generality that α_1, α_2, α_3 is a triangle in $\overline{\mathcal{G}(\mathcal{A})}$. Using the identity

$$(\alpha_1 - \alpha_2) + (\alpha_2 - \alpha_3) + (\alpha_3 - \alpha_1) = 0 \ ,$$

Theorem 4.A implies that there is a σ with the required properties such that the heights of $(\alpha_1 - \alpha_2)/\sigma$, $(\alpha_2 - \alpha_3)/\sigma$ and $(\alpha_3 - \alpha_1)/\sigma$ are bounded above by C_2. By Remark 2, in the function field case we can take in C_2 $2g^* - 2$ in place of $\max(2g^* - 2, 0)$.

For $M = 3$ we are done. Suppose now that $M \geq 4$, and let $[\alpha_u, \alpha_v]$ be a further edge in $\overline{\mathcal{G}(\mathcal{A})}$ with u or v not contained in $\{1, 2, 3\}$. Starting from the edge $[\alpha_2, \alpha_3]$ of $\overline{\mathcal{G}(\mathcal{A})}$ we can get the edge $[\alpha_u, \alpha_v]$ through a sequence of triangles in $\overline{\mathcal{G}(\mathcal{A})}$ such that $[\alpha_2, \alpha_3]$ is side of the first triangle, $[\alpha_u, \alpha_v]$ is side of the last triangle, and two consecutive triangles have a common side. Further, we may assume that the number of triangles in question is at most $\binom{M}{2}$. Let

$$\beta_1 = \alpha_1 - \alpha_2, \ \beta_2 = \beta_{i_1} = \alpha_2 - \alpha_3, \ \beta_{i_w} = \alpha_u - \alpha_v \ ,$$

and denote by $\beta_{i_2}, \dots, \beta_{i_{w-1}}$ the sequence of the differences corresponding to common sides of the triangles under consideration. By the above assumption, we have $w \leq \binom{M}{2}$.

Applying Theorem 4.A as above, we infer that there are $\sigma_1 = \sigma, \sigma_2, \dots, \sigma_{w-1}$ in $O_S \setminus \{0\}$ with the properties described in Theorem 4.A such that $\beta_{i_t}/\sigma_t, \beta_{i_{t+1}}/\sigma_t$ have heights at most C_2 for $t = 1, \dots, w-1$. In the number field case $\sigma \in O_S^*$, while in the function field case we may choose $\sigma = \alpha_1 - \alpha_2$. The height of σ_{t+1}/σ_t is at most $2C_2$. Then it follows that

$$\beta_{i_w}/\sigma = (\alpha_u - \alpha_v)/\sigma$$

is of height at most $M^2 C_2$.

By the connectedness of $\overline{\mathcal{G}(\mathcal{A})}$ there exists, for any distinct α_i, $\alpha_j \in \mathcal{A}$, a path $\alpha_i = \alpha_{j_1}, \dots, \alpha_{j_l} = \alpha_j$ of length at most $M - 1$ in $\overline{\mathcal{G}(\mathcal{A})}$. Further, we have

$$\alpha_i - \alpha_j = (\alpha_{j_1} - \alpha_{j_2}) + \cdots + \left(\alpha_{j_{l-1}} - \alpha_{j_l}\right) \ .$$

But the height of $\left(\alpha_{j_k} - \alpha_{j_{k+1}}\right)/\sigma$ is at most $M^2 C_2$ for each k, hence the height of $(\alpha_i - \alpha_j)/\sigma$ does not exceed $M^3 C_2$.

In what follows, we assume that $\overline{\mathcal{G}(\mathcal{A})}$ is complete. Consider the edge $[\alpha_1, \alpha_2]$, $[\alpha_2, \alpha_3]$, $[\alpha_3, \alpha_1]$ and $[\alpha_u, \alpha_v]$ as above. Applying the above argument to the triangles α_2, α_3, α_u and α_3, α_u, α_v, we get in a similar way as above that for

appropriate σ', σ'' having the properties specified in the Proposition, the heights of $(\alpha_2-\alpha_3)/\sigma$, $(\alpha_2-\alpha_3)/\sigma'$, $(\alpha_3-\alpha_u)/\sigma'$, $(\alpha_3-\alpha_v)/\sigma''$, $(\alpha_u-\alpha_v)/\sigma''$ are bounded above by C_2. However this implies that the height of $(\alpha_u-\alpha_v)/\sigma$ is at most $5C_2$.

Finally, consider the function field case with $N=0$. First suppose that there are three different indices, say 1, 2, 3 such that $(\alpha_1-\alpha_3)/(\alpha_1-\alpha_2)\notin\mathbf{k}$. Then applying Theorem 4.B to the equation

$$(\alpha_1-\alpha_2)+(\alpha_2-\alpha_3)+(\alpha_3-\alpha_1)=0$$

we infer that both $(\alpha_1-\alpha_3)/(\alpha_1-\alpha_2)$ and $(\alpha_2-\alpha_3)/(\alpha_1-\alpha_2)$ may have only finitely many possibilities in K, which may be determined effectively. For $M=3$ we are done. Suppose that $M>3$ and let $i>3$ with $i\le M$. We have

$$(\alpha_1-\alpha_i)+(\alpha_i-\alpha_2)+(\alpha_2-\alpha_1)=0 \tag{4.11}$$

and

$$(\alpha_1-\alpha_i)+(\alpha_i-\alpha_3)+(\alpha_3-\alpha_1)=0. \tag{4.12}$$

We apply now Theorem 4.B to (4.11) and (4.12). Then it follows from (4.11) that either $(\alpha_1-\alpha_i)/(\alpha_1-\alpha_2)\in\mathbf{k}$ or it has only finitely many and effectively determinable possibilities. The same assertion follows from (4.12) for $(\alpha_1-\alpha_i)/(\alpha_1-\alpha_3)$. But both quotients cannot be contained in $\mathbf{k}$ because their quotient $(\alpha_1-\alpha_3)/(\alpha_1-\alpha_2)\notin\mathbf{k}$. If $(\alpha_1-\alpha_i)/(\alpha_1-\alpha_3)$ may have only finitely many and effectively determinable possibilities in K, the same is true for $(\alpha_1-\alpha_i)/(\alpha_1-\alpha_2)$, since this is the product of $(\alpha_1-\alpha_i)/(\alpha_1-\alpha_3)$ and $(\alpha_1-\alpha_3)/(\alpha_1-\alpha_2)$. Therefore in every case $(\alpha_1-\alpha_i)/(\alpha_1-\alpha_2)$ may have only finitely many and effectively determinable possibilities in K. The same holds for $(\alpha_1-\alpha_j)/(\alpha_1-\alpha_2)$ if $j\ge 2$, $j\ne i$, and hence for every $(\alpha_i-\alpha_j)/(\alpha_1-\alpha_2)$ as well.

It remains the case when $(\alpha_1-\alpha_i)/(\alpha_1-\alpha_2)\in\mathbf{k}$ for each i. But then $(\alpha_i-\alpha_j)/(\alpha_1-\alpha_2)\in\mathbf{k}$ for each i and j. This completes the proof with the choice $\sigma=\alpha_1-\alpha_2$. ∎

Proof of Theorem 4.1. Denote by $\mathcal{G}_1,\dots,\mathcal{G}_l$ the connected components of $\mathcal{G}(\mathcal{A})$ with $|\mathcal{G}_1|\le\cdots\le|\mathcal{G}_l|$. First assume that $l=1$. If at least one of $\overline{\mathcal{G}(\mathcal{A})}$ and $\overline{\mathcal{G}(\mathcal{A})}^{\triangle}$ is not connected, then the case (i) holds. On the other hand, if both $\overline{\mathcal{G}(\mathcal{A})}$ and $\overline{\mathcal{G}(\mathcal{A})}^{\triangle}$ are connected, in view of Proposition 4.2 we arrive at the case (iv).

If $l\ge 3$, then $\overline{\mathcal{G}(\mathcal{A})}$ and $\overline{\mathcal{G}(\mathcal{A})}^{\triangle}$ are again connected and the case (iv) follows as above. Suppose now that $l=2$. First consider the case when $|\mathcal{G}_1|=1$. If $\overline{\mathcal{G}_2}$ is connected then both $\overline{\mathcal{G}(\mathcal{A})}$ and $\overline{\mathcal{G}(\mathcal{A})}^{\triangle}$ are connected, and Proposition 4.2 implies again the case (iv). Otherwise, if $\overline{\mathcal{G}_2}$ is not connected than we have the case (ii). Finally, it remains the case (iii) and the proof is completed. ∎

In the next proof we shall use the fact that for $\alpha\in O_S\setminus\{0\}$,

$$N_S(\alpha)\le\begin{cases} dh(\alpha) & \text{in the number field case,}\\ h_K(\alpha) & \text{in the function field case.}\end{cases} \tag{4.13}$$

Proof of Proposition 4.3. First consider the number field case. Let $\mathcal{G}_1$, $\mathcal{G}_2$ be the connected components of $\mathcal{G}(\mathcal{A})$, and assume that at least one of them, say $\mathcal{G}_2$ is not complete. Let $[\alpha_u, \alpha_v]$ be an edge of $\overline{\mathcal{G}_2}$, and $\mathcal{A}'$ the union of the set $\{\alpha_u, \alpha_v\}$ and the set of vertices of $\mathcal{G}_1$. Consider the graph $\mathcal{G}(\mathcal{A}') = \mathcal{G}_K(\mathcal{A}', S, N)$. It is easy to see that both $\overline{\mathcal{G}(\mathcal{A}')}$ and $\overline{\mathcal{G}(\mathcal{A}')}^{\triangle}$ are connected. Hence by Proposition 4.2 there is a $\sigma' \in O_S^*$ such that for any distinct vertices α_i, α_j of $\mathcal{G}(\mathcal{A}')$, the height of $(\alpha_i - \alpha_j)/\sigma'$ is at most C_3, where C_3 denotes the bound occurring in (4.1). Then, using (4.13), we infer that

$$N_S(\alpha_i - \alpha_j) = N_S((\alpha_i - \alpha_j)/\sigma') \le nh((\alpha_i - \alpha_j)/\sigma') \le nC_3 =: C_4 .$$

In view of the lower bound (25) of [42] concerning R_S, we have $C_4 \ge N$. The graph $\mathcal{G}'(\mathcal{A}) = \mathcal{G}_K(\mathcal{A}, S, C_4)$ satisfies the assumptions of Proposition 4.2. Therefore, using Proposition 4.2 with N replaced by C_4 we infer that there is a $\sigma \in O_S^*$ such that (4.3) holds for each α_i, $\alpha_j \in \mathcal{A}$.

Next consider the function field case. Assume that $\overline{\mathcal{G}(\mathcal{A})}$ is of order ≥ 5. Then one can prove by using the same arguments as in the proof of Theorem 1 of [37] that both $\overline{\mathcal{G}(\mathcal{A})}$ and $\overline{\mathcal{G}(\mathcal{A})}^{\square}$ are connected. We can now proceed as in the proof of Proposition 4.2, but with $\overline{\mathcal{G}(\mathcal{A})}^{\square}$ instead of $\overline{\mathcal{G}(\mathcal{A})}^{\triangle}$. If e.g. $[\alpha_1, \alpha_2], [\alpha_2, \alpha_3], [\alpha_3, \alpha_4], [\alpha_4, \alpha_1]$ is a quadrangle in $\overline{\mathcal{G}(\mathcal{A})}$, then by Theorem 4.A there is a $\sigma \in O_S \setminus \{0\}$, say $\sigma = \alpha_1 - \alpha_2$, such that the heights of $(\alpha_1 - \alpha_2)/\sigma$, $(\alpha_2 - \alpha_3)/\sigma$, $(\alpha_3 - \alpha_4)/\sigma$, $(\alpha_4 - \alpha_1)/\sigma$ are at most C_5, where C_5 denotes the bound occurring in (4.7) with the choice $q = 4$. Let now $[\alpha_u, \alpha_v]$ be a further edge in $\overline{\mathcal{G}(\mathcal{A})}$ such that at least one of u and v is not contained in the set $\{1, 2, 3, 4\}$. Then working with quadrangles in place of triangles, one can prove in the same way as in the proof of Proposition 4.2 that $(\alpha_u - \alpha_v)/\sigma$ is of height at most M^2C_5. This implies as in the proof of Proposition 4.2 that for each pair α_i, $\alpha_j \in \mathcal{A}$, the height of $(\alpha_i - \alpha_j)/\sigma$ is bounded above by M^3C_5. Since by assumption both $\mathcal{G}_1$ and $\mathcal{G}_2$ have order ≥ 2, it remains the case $M = 4$, when both $\mathcal{G}_1$ and $\mathcal{G}_2$ must be complete. ■

5. Applications of the results of Section 4 to resultant equations and discriminant equations over function fields

Results

Keeping the notation of the preceding section, let K be a finite extension of the rational function field $\mathbf{k}(z)$ over $\mathbf{k}$, where $\mathbf{k}$ is an algebraically closed field of characteristic 0. We assume as in Section 4 that $\mathbf{k}$ is explicitly presented. Let M_K denote the set of valuations of $K/\mathbf{k}$ with value group $\mathbb{Z}$. Let S be a finite subset of M_K with cardinality s which contains the infinite valuations, O_S the ring of S-integers and O_S^* the group of S-units in K. Further, let G be a normal extension of degree δ of K with genus g^*.

Using our Theorem 4.1 and Propositions 4.2 and 4.3 we shall give effective function field analogues of some results of Section 3. For simplicity, we restrict ourselves here to polynomials without multiple zeros.

Let a be a non-zero element of O_S, and consider the semi-resultant equation

$$R^*(f,g) \in aO_S^* \text{ in squarefree monic } f,g \in O_S \text{ having all their zeros in } G. \tag{5.1a}$$

According to (3.10), we consider only those solutions (f,g) for which

$$\begin{aligned} &\deg(f) \geq 2, \ \ \deg(g) \geq 2 \\ &\text{and if } f,g \text{ have no common zero then} \\ &\deg(f) + \deg(g) \geq 5. \end{aligned} \tag{5.2}$$

As in Section 3, the pairs (f,g) and (f',g') of monic polynomials in $O_S[x]$ are called *O_S-equivalent* if $f'(x) = \varepsilon^{\deg(f)} f\,(x/\varepsilon + b)$ and $g'(x) = \varepsilon^{\deg(g)} g\,(x/\varepsilon + b)$ for some $\varepsilon \in O_S^*$ and $b \in O_S$. If (f,g) is a solution of (5.1a) then so is (f',g').

As is known (see e.g. [10]), $O_S^*/\mathbf{k}^*$ is finitely generated, and its rank, say r, is at most $s-1$. Let $\eta_1, \ldots, \eta_r$ be a basis of $O_S^*/\mathbf{k}^*$ and denote by E the maximum of their heights.

Apart from (3.7), the following theorem can be regarded as an effective function field analogue of our Theorem 3.4.

Theorem 5.1a. *If (f,g) is a solution of (5.1a) with (5.2) and with $\deg(f) = m$, $\deg(g) = n$, then it is O_S-equivalent to a solution (f',g') such that the heights (in G) of the zeros of f' and g' do not exceed*

$$6(m+n)^4 \left(\delta(s + h_K(a) + (s-1)mnE) + \max(2g^* - 2, 0)\right). \tag{5.3a}$$

Consider now the equation

$$R^*(f,g) = a \text{ in squarefree monic } f,g \in O_S[x] \text{ having all their zeros in } G. \tag{5.1b}$$

If (f,g) is a solution of (5.1b) then so is every pair (f',g') for which $f'(x) = f(x+b)$, $g'(x) = g(x+b)$ for some $b \in O_S$. Such pairs will be called *strongly O_S-equivalent.*

Apart from the form of the bounds, Theorem 5.1a and the following theorem can be deduced from each other. It will be more convenient to deduce Theorem 5.1a from Theorem 5.1b.

Theorem 5.1b. *If (f,g) is a solution of (5.1b) with (5.2) and with $\deg(f) = m$, $\deg(g) = n$, then it is strongly O_S-equivalent to a solution (f',g') such that the heights (in G) of the zeros of f' and g' do not exceed*

$$6(m+n)^4 \left(\delta(s + h_K(a)) + \max(2g^* - 2, 0)\right). \tag{5.3b}$$

The above theorems can be applied to resultant equations and discriminant equations as in Section 3.

Theorem 5.2. *Let (f,g) be a solution of the resultant equation*

$$R(f,g) \in aO_S^* \text{ in squarefree monic } f,g \in O_S[x] \text{ having all their zeros in } G \tag{5.4}$$

such that

$$\deg(f) = m \geq 2, \deg(g) = n \geq 2 \text{ and } m + n \geq 5 .$$

Then (f, g) is O_S-equivalent to a solution (f', g') such that the heights (in G) of the zeros of f' and g' do not exceed the bound occurring in (5.3a).

Theorem 5.1b has a similar consequence for the resultant equation $R(f, g) = a$.

From the bounds obtained in (5.3a) and (5.3b) it is easy to derive bounds for the maximum height of the coefficients of f' and g'.

In contrast with Theorems 3.3 and 3.4, Theorems 5.1a, 5.1b and 5.2 do not imply the finiteness of the (strong) O_S-equivalence classes of solutions (f, g). For example, let

$$f(x) = x(x-1),\ g(x) = (x-\varepsilon)(x-\eta_2)\cdots(x-\eta_{n-1})(x-\eta_n) ,$$

where $n \geq 3$, $\varepsilon \in O_S^* \setminus \mathbf{k}^*$ such that $1 - \varepsilon \in O_S^*$, and $\eta_2, \ldots, \eta_{n-1}$ are distinct elements of $\mathbf{k}$, different from 0 and 1. If η_n runs through the elements of $\mathbf{k}$, then the pairs (f, g) satisfy both (5.1a) and (5.4) with $m = 2$, and they are pairwise O_S-inequivalent. Further, it is easy to show that in our above theorems $m + n$ cannot be bounded above.

Finally, consider the discriminant equations

$$D(f) \in aO_S^* \text{ in monic } f \in O_S[x] \text{ having all their zeros in } G , \tag{5.5a}$$

and

$$D(f) = a \text{ in monic } f \in O_S[x] \text{ having all their zeros in } G . \tag{5.5b}$$

The monic polynomials f, $f' \in O_S[x]$ are called *O_S-equivalent*, resp. *strongly O_S-equivalent*, if $f'(x) = \varepsilon^{\deg(f)} f\,(x/\varepsilon + b)$, resp. if $f'(x) = f(x + b)$ for some $\varepsilon \in O_S^*$ and $b \in O_S$. If f is a solution of (5.5a), resp. of (5.5b), then so is every f' which is O_S-equivalent, resp. strongly O_S-equivalent to f.

If $f(x)$ is an arbitrary monic polynomial in $\mathbf{k}[\mathbf{x}]$ with degree $n \geq 3$ and discriminant $D(f) \neq 0$, then every monic $f' \in O_S[x]$ which is strongly O_S-equivalent to $\sigma^n f\,(x/\sigma)$ with some $\sigma \in G^*$ is called *special*. Notice that all polynomials which are O_S-equivalent to a special polynomial in $O_S[x]$ must be special in $O_S[x]$ themselves.

It is easy to see that equations (5.5a) and (5.5b) may have infinitely many (strong) O_S-equivalence classes of special polynomial solutions. On the other hand, it follows from Theorem 1 of [10] (which was established more generally, over function fields of several variables[4]) that the numbers of (strong) O_S-equivalence classes of non-special polynomial solutions of equations (5.5a) and (5.5b) are finite and can be estimated from above by explicit bounds depending only on n, δ, a and the degree of $K/\mathbf{k}(z)$. We give now effective versions of these finiteness results.

Theorems 5.1a and 5.1b give as immediate consequences results for (5.5a) and (5.5b) with the choice $g = f$. However, we can deduce better bounds and effective finiteness results from Proposition 4.2.

[4]Further, in [10] it is only assumed that $\mathbf{k}$ is algebraically closed in K.

Theorem 5.3a. *If $f \in O_S[x]$ is a solution of (4.5a) with degree $n \geq 3$, then it is O_S-equivalent to a monic polynomial $f' \in O_S[x]$ whose zeros have heights (in G) not exceeding*

$$5(2n-1)\left(\delta\left(s + h_K(a) + (s-1)n^2E\right) + 2g^* - 2\right). \tag{5.6a}$$

Further,

(i) f is special, or
(ii) f' belongs to a finite, effectively determinable subset of $O_S[x]$ depending only on K, S, G, a, n and $\eta_1, \ldots, \eta_r$.

Theorem 5.3a will be deduced from the following.

Theorem 5.3b. *If $f \in O_S[x]$ is a solution of (5.5b) with degree $n \geq 3$, then it is strongly O_S-equivalent to a monic $f' \in O_S[x]$ whose zeros have heights (in G) not exceeding*

$$5(2n-1)\left(\delta\left(s + h_K(a)\right) + 2g^* - 2\right). \tag{5.6b}$$

Further,

(i) f is special, or
(ii) $f'(x)$ belongs to a finite, effectively determinable subset of $O_S[x]$ depending only on K, S, G, a and n.

From the bounds (5.6a) and (5.6b) one can easily derive bounds for the heights of the coefficients of the polynomials f' under considerations.

The bound (5.6b) can be compared with the bound (2.17) of Theorem 2 in [34], which was obtained over function fields of several variables. Theorem 2 of [34] led in that paper to applications to integral elements of given discriminant and power integral bases. Our Theorems 5.3a and 5.3b have similar applications. In the special case when the polynomials $f \in O_S[x]$ are irreducible a result similar to our Theorem 5.3b can be deduced from Theorem 1 of Gaál [18] concerning integral elements of given discriminant. We note that in this special situation only the cases (ii) can occur in our Theorems 5.3a and 5.3b.

Proofs

We first prove Theorem 5.1b.

Proof of Theorem 5.1b. We follow the proof of Theorem 3.4. Let (f, g) be a solution of (5.1b) with (5.2) and with $\deg(f) = m$, $\deg(g) = n$. Further, let $\alpha_1, \ldots, \alpha_k$ $(k \geq 0)$, $\beta_1, \ldots, \beta_l$ $(l \geq 0)$, $\gamma_1, \ldots, \gamma_p$ $(p \geq 0)$ and $\mathcal{A} = \{\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_l, \gamma_1, \ldots, \gamma_p\} = \{x_1, \ldots, x_M\}$ be as in the proof of Theorem 3.4. Then we can write (5.1b) in the form

$$\widetilde{\prod}(x_i - x_j) = a, \tag{5.7}$$

where the x_i are zeros of f and x_j are zeros of g.

Let S_1 denote the smallest subset of M_K such that $S \subseteq S_1$ and $a \in O_{S_1}^*$. Using (4.13), we infer as in the proof of Theorem 4.A that $|S_1| \leq s + h_K(a)$. Let T be the set of continuations to G of the valuations in S_1, O_T the ring of T-integers and O_T^* the group of T-units in G. We have $|T| \leq \delta|S_1|$. Since by assumption f, $g \in O_S[x]$, it follows that x_i, $x_j \in O_T$, and hence (5.7) implies that $x_i - x_j \in O_T^*$. Then, for $N = 0$, the graph $\mathcal{G}(\mathcal{A}) = \mathcal{G}_G(\mathcal{A}, T, N)$ has either at least 3 components or 2 components of order ≥ 2. We can now apply in the first case Theorem 4.1 and in the second case Proposition 4.3 with $N = 0$ and with O_S replaced by O_T. We observe that the bound in (4.4) is larger than that in (4.2). Thus it follows that there is $\sigma \in O_T^*$ such that for each pair of distinct x_u, x_v of $f \cdot g$

$$h_G((x_u - x_v)/\sigma) \leq 3(m+n)^3(\delta(s + h_K(a)) + \max(2g^* - 2, 0)) =: C_1, \quad (5.8)$$

where $h_G(\,)$ denotes the height in G. Denote by w the number of factors on the left hand side of (5.7). Using now (5.8) and multiplying (5.7) by σ^{-w}, the height in G of the right hand side so obtained can be estimated from above. We note that $h_G(a) = \delta h_K(a)$. So we infer that

$$h_G(\sigma) \leq \delta h_K(a) + C_1. \quad (5.9)$$

Thus (5.8) and (5.9) imply that

$$h_G(x_u - x_v) \leq \delta h_K(a) + 2C_1 =: C_2\ .$$

Fix a zero x_u of $f \cdot g$ and add the differences $x_u - x_v$ for each zero x_v of $f \cdot g$. Since the sum of the zeros of $f \cdot g$ is an element of O_S, we obtain that

$$x_u = \tau_u - b$$

with some $b \in O_S$ and $\tau_u \in O_T$ such that

$$h_G(\tau_u) \leq (m + n - 1)C_2.$$

Finally, we set $f'(x) = \prod(x - \tau_u)$, resp. $g'(x) = \prod(x - \tau_u)$, for each u for which x_u is a zero of f, resp. of g. Then f', g' are monic polynomials with coefficients in O_S, and the pair (f, g) is strongly O_S-equivalent to the pair (f', g'). ■

Proof of Theorem 5.1a. Suppose that (f, g) is a solution of (5.1a). Then $R^*(f, g) = a\varrho$ with some $\varrho \in O_S^*$. Representing ϱ in the basis $\eta_1, \ldots, \eta_r$ of $O_S^*/\mathbf{k}^*$, we can write $\varrho = \varepsilon^w \eta$, where w is as above, ε, $\eta \in O_S^*$ and $h_K(\eta) \leq r(w-1)E$. We have $r \leq s-1$ and $w \leq mn$. Putting $f_1(x) = \varepsilon^{-m} f(\varepsilon x)$ and $g_1(x) = \varepsilon^{-n} g(\varepsilon x)$, these are monic polynomials with coefficients in O_S and

$$R^*(f_1, g_1) = a\eta.$$

Now applying Theorem 5.1b to this equation in f_1, g_1, we get that $f(x) = \varepsilon^m f'(x/\varepsilon + b)$, $g(x) = \varepsilon^n g'(x/\varepsilon + b)$ with monic f', $g' \in O_S[x]$ whose zeros have heights not exceeding the bound occurring in (5.3a). ■

Proof of Theorem 5.3b. Let f be a solution of (5.5b) with zeros $\alpha_1, \ldots, \alpha_n$ in G, let $\mathcal{A} = \{\alpha_1, \ldots, \alpha_n\}$, and let S_1, T, O_T and O_T^* be as in the proof of Theorem 5.1b. As was seen there, $|T| \leq \delta(s + h_K(a))$. Equation (5.5b) implies that $\alpha_i - \alpha_j \in O_T^*$ for each distinct i, j with $1 \leq i, j \leq n$. Then, for $N = 0$, the graph $\mathcal{G}(\mathcal{A}) = \mathcal{G}_G(\mathcal{A}, T, N)$ has only isolated vertices. Applying Proposition 4.2 to this graph, it follows that for some $\sigma \in O_T^*$,

$$h_G\left((\alpha_i - \alpha_j)/\sigma\right) \leq 5\left(\delta(s + h_K(a)) + 2g^* - 2\right) =: C_3. \tag{5.10}$$

Further, either

i) $(\alpha_i - \alpha_j)/\sigma \in \mathbf{k}$ for each i, j, or

ii) $(\alpha_i - \alpha_j)/\sigma$ has only finitely many and effectively determinable possibilities in G.

Using (5.10) and $h_G(a) = \delta h_K(a)$, one can easily deduce from (5.5b) that

$$h_G(\sigma) \leq \delta h_K(a)/(n(n-1)) + C_3\ ,$$

and so

$$h_G(\alpha_i - \alpha_j) \leq \delta h_K(a)/(n(n-1)) + 2C_3\ .$$

Fix i, and add the differences $\alpha_i - \alpha_j$ for each j. Then we infer that $\alpha_i = \alpha_i' - b$ for some $b \in O_S$ and $\alpha_i' \in O_T$ such that

$$h_G(\alpha_i') \leq \delta h_K(a)/n + 2(n-1)C_3 \leq (2n-1)C_3\ .$$

Further, the polynomial $f'(x)$ having zeros $\alpha_1', \ldots, \alpha_n'$ is strongly O_S-equivalent to $f(x)$.

We now return to the cases i) and ii).
In the case i) we infer that $\alpha_i' = \sigma\gamma_i$ with some $\gamma_i \in \mathbf{k}$ for $i = 1, \ldots, n$. Putting $f''(x) = \prod_{i=1}^{n}(x - \gamma_i)$, $f'(x) = \sigma^n f''(x/\sigma)$ is strongly O_S-equivalent to $f(x)$. Hence f is special in $O_S[x]$.

In case ii), it follows from (5.5b) that σ may have only finitely many and effectively computable possibilities in G. Hence the same holds for the differences $\alpha_i - \alpha_j$, and for the above α_i' as well. This implies (ii). ■

Proof of Theorem 5.3a. Theorem 5.3a can be deduced from Theorem 5.3b in the same way as Theorem 5.1a from Theorem 5.1b. ■

Acknowledgements. The author would like to thank the referee for his/her useful remarks and for the improvement proposed in the former bound occurring in (3.8).

References

[1] A. Bérczes, J. H. Evertse, K. Győry, *On the number of equivalence classes of binary forms of given degree and given discriminant*, Acta. Arith. **113** (2004), 363–399.

[2] A. Bérczes, J. H. Evertse, K. Győry, *On the number of pairs of binary forms with given degree and given resultant*, Acta. Arith. **128** (2007), 19–54.

[3] F. Beukers, H. P. Schlickewei, *The equation $x + y = 1$ in finitely generated groups*, Acta. Arith. **78** (1996), 189–199.

[4] B. J. Birch, J. R. Merriman, *Finiteness theorems for binary forms with given discriminant*, Proc. London Math. Soc. **25** (1972), 385-394.

[5] W. D. Brownawell, *Some remarks on semi-resultants*, in: Transcendence Theory, Advances and Applications, Acad. Press 1977, pp. 205–210.

[6] W. D. Brownawell, D. W. Masser, *Vanishing sums in function fields*, Math. Proc. Camb. Phil. Soc. **100** (1986), 427–434.

[7] Y. Bugeaud, K. Győry, *Bounds for the solutions of unit equations*, Acta Arith. **74** (1996), 67–80.

[8] G. V. Chudnovsky, *Analytic methods in diophantine approximations* (Russian), Inst. Math. Ukrainian Acad. of Science, Preprint IM-74-9, Kiev, 1974.

[9] B. N. Delone, D. K. Faddeev, *The theory of irrationalities of the third degree*, Amer. Math. Soc., Providence, 1964 (Translated from the Russian).

[10] J. H. Evertse, K. Győry, *On the number of polynomials and integral elements of given discriminant*, Acta. Math. Hung. **51** (1988), 341–362.

[11] J. H. Evertse, K. Győry, *On the numbers of solutions of weighted unit equations.* Compositio Math. **66** (1988), 329–354.

[12] J. H. Evertse, K. Győry, *Effective finiteness results for binary forms with given discriminant*, Compositio Math. **79** (1991), 169–204.

[13] J. H. Evertse, K. Győry, *Lower bounds for resultants I.* Compositio Math. **88** (1993), 1–23.

[14] J. H. Evertse, K. Győry, C. L. Stewart and R. Tijdeman, *S-unit equations and their applications.* in: New Advances in Transcendence Theory, Cambridge, 1988. pp. 110–174.

[15] J. H. Evertse, H. P. Schlickewei and W. M. Schmidt, *Linear equations in variables which lie in a multiplicative group*, Annals of Math. **155** (2002), 1–30.

[16] J. H. Evertse, U. Zannier, *Linear equations with unknowns from a multiplicative group in a function field*, Acta Arith. **133** (2008), 159–170.

[17] A. Fröhlich, J. C. Shepherdson, *Effective procedures in field theory*, Philos. Trans. Roy. Soc. London, Ser **A**, **248** (1956), 407–432.

[18] I. Gaál, *Integral elements with given discriminant over function fields*, Acta. Math. Hung. **52** (1988), 133–146.

[19] I. Gaál, *Diophantine equations and power integral bases*, Birkhäuser, 2002.

[20] I.Gaál, *On the resolution of resultant type equations*, J.Symbolic Comp. **34** (2002), 137–144.

[21] I. Gaál, *Solving explicitly decomposable form equations over global function fields*, J. Algebra, Number Theory and Appl. **6** (2006), 425–434.

[22] I. Gaál, K. Győry, *Index form equations in quintic fields.* Acta Arith. **89** (1999), 379–396.

[23] K. Győry, *Sur l'irréductibilité d'une classe des polynômes I.* Publ. Math. Debrecen **18** (1971), 289–307.

[24] K. Győry, *Sur l'irréductibilité d'une classe des polynômes II.* Publ. Math. Debrecen **19** (1972), 293–326.

[25] K. Győry, *On polynomials with integer coefficients and given discriminant I, II, III, IV, V*; Acta Arith. **23** (1973), 419–426; Publ. Math. Debrecen **21** (1974), 125–144; ibid. **23** (1976), 141–165; ibid. **25** (1978), 155–167; Acta Math. Acad. Sci. Hungar. **32** (1978), 175–190.

[26] K. Győry, *On the greatest prime factors of decomposable forms at integer points*, Ann. Acad. Sci. Fenn., Ser. A I, Math. **4** (1978/1979), 341–355.

[27] K. Győry, *On certain graphs composed of algebraic integers of a number field and their applications I.* Publ. Math. Debrecen **27** (1980), 229–242.

[28] K. Győry, *Résultats effectifs sur la représentation des entiers par des formes décomposables*, Queen's Papers in Pure and Applied Math., No 56, Kingston, Canada, 1980.

[29] K. Győry, *On discriminants and indices of integers of an algebraic number field.* J. Reine Angew. Math. **324** (1981), 114–126.

[30] K. Győry, *On the representation of integers by decomposable forms in several variables.* Publ. Math. Debrecen **28** (1981), 89–98.

[31] K. Győry, *On the irreducibility of a class of polynomials III.* J. Number Theory **15** (1982), 164–181.

[32] K. Győry, *On certain graphs associated with an integral domain and their applications to diophantine problems.* Publ. Math. Debrecen **29** (1982), 79–94.

[33] K. Győry, *Effective finiteness theorems for diophantine problems and their applications* (in Hungarian). Academic doctor's thesis, Debrecen, 1983.

[34] K. Győry, *Effective finiteness theorems for polynomials with given discriminant and integral elements with given discriminant over finitely generated domains.* J. Reine Angew. Math. **346** (1984), 54–100.

[35] K. Győry, *On arithmetic graphs associated with integral domains.* A Tribute to Paul Erdős. Cambridge University Press, 1990. pp. 207–222.

[36] K. Győry, *On the irreducibility of a class of polynomials IV.* Acta Arith. **62** (1992), 399–405.

[37] K. Győry, *On arithmetic graphs associated with integral domains II.* Sets, Graphs and Numbers. Coll. Math. Soc. J. Bolyai **60**, North-Holland Publ. Comp.,1992. pp. 365–374.

[38] K. Győry, *On the number of pairs of polynomials with given resultant or given semi-resultant.* Acta. Sci. Math. **57** (1993), 515–529.

[39] K. Győry, *On pairs of binary forms with given resultant or given semi-resultant.* Math. Pannon. **4** (1993), 169–180.

[40] K. Győry, *Polynomials and binary forms with given discriminant*, Publ. Math. Debrecen **69** (2006), 473–499.

[41] K. Győry and Z. Z. Papp, *Effective estimates for the integer solutions of norm form and discriminant form equations.* Publ. Math. Debrecen **25** (1978), 311–325.
[42] K. Győry, K. Yu, *Bounds for the solutions of S-unit equations and decomposable form equations*, Acta Arith. **123** (2006), 9–41.
[43] I. Járási, *Computing small solutions of unit equations in three variables II, Applications to resultant form equations*, Publ. Math. Debrecen **65** (2004), 399–408.
[44] S. Lang, *Fundamentals of diophantine geometry*, Springer, 1983.
[45] A. Leutbecher, *New Euclidean fields by Lenstra's method of exceptional units*, Proc. Conf. on Number Thoery and Arithmetic Geometry, Essen, 1991. pp. 79–80.
[46] A. Leutbecher, G. Niklasch, *On cliques of exceptional units and Lenstra's construction of Euclidean fields*, in: Number Theory, Lecture Notes in Math. **1380**, Springer, 1989. pp. 150–178.
[47] R. C. Mason, *Diophantine equations over function fields*, Cambridge, 1984.
[48] M. Nagata, *A general theory of algebraic geometry over Dedekind domains I*, Amer. J. Math. **78** (1956), 78–116.
[49] T. Nagell, *Sur les discriminants des nombres algébriques*, Arkiv för Mat. **7** (1967), 265–282.
[50] W. Narkiewicz, Elementary and analytic theory of algebraic numbers (2nd ed.), Springer, 1990.
[51] P. Roquette, *Einheiten und Divisorenklassen in eudlich erzeugbar Körpern*, J. Deutsch. Math. Verein. **60** (1957), 1–21.
[52] A. Schinzel, *Polynomials with special regard to irreducibility*, Cambridge, 2000.
[53] A. Shlapentokh, *Polynomials with a given discriminant over fields of algebraic functions of positive characteristic.* Pacific J. Math. **173** (1996), 533–555.
[54] N. P. Smart, *The solutions of triangularly connected decomposable form equations.* Math. Comp. **64** (1995), 819–840.
[55] N. P. Smart, *Solving discriminant form equations via unit equations.* J. Symbolic. Comp. **21** (1996), 367–374.
[56] N. P. Smart, *The algorithmic resolution of diophantine equations*, Cambridge, 1998.
[57] M. Waldschmidt, *Diophantine approximation on linear algebraic groups*, Springer, 2000.
[58] K. Wildanger, *Über das Lösen von Einheiten-und Indexformgleichungen in algebraischen Zahlkörpern mit einer Anwendung auf die Bestimmung aller ganze Punkte einer Mordellschen Kurve*, Dissertation, Berlin, 1997.
[59] K. Wildanger, *Über das Lösen von Einheiten-und Indexformgleichungen in algebraischen Zahlkörpern*, J. Number Theory **82** (2000), 188–224.

Address: Institute of Mathematics, Number Theory Research Group of the Hungarian Academy of Sciences, University of Debrecen H-4010 Debrecen, P.O.B. 12 Hungary

E-mail: gyory@math.klte.hu

Received: 11 January 2008; **revised:** 18 March 2008