Effective results for unit points on curves over finitely generated domains

By Attila Bérczes†

Institute of Mathematics, University of Debrecen

H-4010 Debrecen, P.O. Box 12, Hungary

e-mail: berczesa@science.unideb.hu

(*Received*)

Abstract

Let A be a commutative domain of characteristic 0 which is finitely generated over $\mathbb{Z}$ as a $\mathbb{Z}$-algebra. Denote by A^* the unit group of A and by $\overline{K}$ the algebraic closure of the quotient field K of A. We shall prove effective finiteness results for the elements of the set

$$\mathcal{C} := \{(x, y) \in (A^*)^2 | F(x, y) = 0\}$$

where $F(X, Y)$ is a non-constant polynomial with coefficients in A which is not divisible over $\overline{K}$ by any polynomial of the form $X^m Y^n - \alpha$ or $X^m - \alpha Y^n$, with $m, n \in \mathbb{Z}_{\geq 0}$, $\max(m, n) > 0$, $\alpha \in \overline{K}^*$. This result is a common generalization of effective results of Evertse and Győry (2013) on S-unit equations over finitely generated domains, of Bombieri and Gubler (2006) on the equation $F(x, y) = 0$ over S-units of number fields, and it is an effective version of Lang's general but ineffective theorem (1960) on this equation over finitely generated domains. The conditions that A is finitely generated and F is not divisible by any polynomial of the above type are essentially necessary.

† The research was supported in part by the University of Debrecen, and by grants K100339 and NK104208 of the Hungarian National Foundation for Scientific Research. This work was partially supported by the European Union and the European Social Fund through project Supercomputer, the national virtual lab (grant no.: TAMOP-4.2.2.C-11/1/KONV-2012-0010).

1. *Introduction.*

Let A be a commutative domain of characteristic 0 which is finitely generated over $\mathbb{Z}$, K the quotient field of A and A^* the unit group (multiplicative group of invertible elements) of A.

Let $F \in A[X,Y]$ be a non-constant polynomial. By a result of Lang [**20**] from 1960, the equation

$$F(x,y) = 0 \quad \text{in } x, y \in A^* \tag{1.1}$$

has only finitely many solutions, provided F is not divisible by any polynomial of the form

$$X^m Y^n - \alpha \qquad \text{or} \qquad X^m - \alpha Y^n \tag{1.2}$$

for any non-negative integers m, n, not both zero, and any $\alpha \in A^*$. Lang's proof is ineffective. The conditions imposed in Lang's theorem, i.e., that A be finitely generated and F not be divisible by any polynomial of type (1.2), are essentially necessary. Bombieri and Gubler [**5**] (Theorem 5.4.5) gave an effective proof of Lang's result in the case that A is the ring of S-integers in a number field, and this was made more precise, with explicit upper bounds for the heights of x, y, by Bérczes, Evertse, Győry and Pontreau [**4**].

Using the method developed by Győry [**15**], [**16**] and Evertse and Győry [**12**], we give an effective proof of Lang's result for arbitrary finitely generated domains A, i.e. we show that given suitable representations for A and the coefficients of F, one can in principle effectively determine the solutions of (1.1) under a slightly stronger condition then (1.2), namely in (1.2) we allow $\alpha \in \overline{K}^*$ instead of $\alpha \in A^*$. In fact, we give a quantitative version of this, with upper bounds for the sizes of x and y.

The precise statement of our result, together with the necessary definitions, is given in Section 2. Below, we give a brief overview of further earlier work related to our result.

With the choice $F(X,Y) = aX + bY - c$ our equation contains as a special case the unit equation

$$ax + by = c \quad \text{in } x, y \in A^*. \tag{1.3}$$

The investigation of unit equations is one of the classical topics in diophantine number theory. For the unit equation (1.3) over the unit group of a domain A, the first general finiteness result is due to Siegel [**24**], who proved finiteness of the number of solutions over the unit group of the ring of integers of a number field. Building further on results of Mahler [**22**] and Parry [**23**] in 1960 Lang [**20**] extended the finiteness result to the case when A is a finitely generated domain over $\mathbb{Z}$. However, all these results were ineffective. The first general effective finiteness result for S-unit equations is due to Győry [**13**], [**14**]. His proof depends on Baker's method, i.e. on estimates for linear forms in logarithms.

Later Győry [**15**], [**16**] introduced an effective specialization method and proved effective finiteness theorems for unit equations over finitely generated domains from a restricted class that have transcendental elements. Recently, Evertse and Győry [**12**] improved the method of Győry and extended these finiteness results for the case when A is an arbitrary domain which is finitely generated over $\mathbb{Z}$. The main result of the present paper is a common generalization of this result of Evertse and Győry [**12**], and the above mentioned result of Bombieri and Gubler [**5**] (Theorem 5.4.5) and of Bérczes, Evertse, Győry and Pontreau [**4**] (Theorem 2.1).

It is also worth recalling some historical facts on effective finiteness results for diophantine equations over finitely generated domains. The first effective results for diophantine equations over finitely generated domains date back to the 1980's, when Győry ([**15**], [**16**]) developed an effective specialization method and proved effective results for norm form, index form and discriminant form equations, unit equations, and for polynomials and integral elements of given discriminant over a wide class of finitely generated integral domains. Using the method of Győry other types of equations have been studied in this generality by Brindza, Pintér, Végső and others (see [**6**], [**7**], [**9**], [**8**]).

Recently, using results of Aschenbrenner [**1**], Evertse and Győry [**12**] extended the specialization method of Győry, and proved effective finiteness results for unit equations over arbitrary finitely generated domains. Later Bérczes, Evertse and Győry [**3**] proved effective results for Thue equations, hyper- and super-elliptic equations, and the Schinzel-Tijdeman equation over arbitrary finitely generated domains.

The organization of the paper is as follows. In Section 2 we present our main result. The other sections are devoted to the proof of our main theorem. In Section 3 we present preparatory results for the proof: on the one hand we reformulate condition (1.2) in a form which can be easily checked effectively, on the other hand we prove effective estimates for the gcd of polynomials. In Section 4 we construct a domain $B \supseteq A$ that is easier to handle and show that our result, proved for the domain B instead of A, implies our result for A. Finally Sections 5 and 6 contain the proof of the above mentioned extended result.

2. *Results*

2·1. *Notation*

Let $r > 0$ and let $A := \mathbb{Z}[z_1, \dots, z_r]$ be a domain of characteristic 0 which is finitely generated over $\mathbb{Z}$. Clearly, A can be expressed as a factor ring

$$A \cong \mathbb{Z}[X_1, \dots, X_r]/\mathcal{I}, \tag{2.1}$$

where $\mathcal{I}$ is the ideal of $R := \mathbb{Z}[X_1, \dots, X_r]$ which consists of all polynomials $f \in R$ with the property $f(z_1, \dots, z_r) = 0$. The ideal $\mathcal{I}$ is finitely generated, so we may write

$$\mathcal{I} = (f_1, \dots, f_t) \qquad \text{with} \quad f_1, \dots, f_t \in \mathbb{Z}[X_1, \dots, X_r]. \tag{2.2}$$

In fact in this way the polynomials $f_1, \dots, f_t$ fix a representation for the domain A. Recall that A is a domain of characteristic 0 if and only if $\mathcal{I}$ is a prime ideal, and $\mathcal{I} \cap \mathbb{Z} = \emptyset$. Given a set of generators $f_1, \dots, f_t$ for I this property can be checked effectively (see [**1**] and [**18**]).

Let K denote the quotient field of A. We say that the polynomial $f \in R$ *represents* $\alpha \in A$ if we have $f(z_1, \dots, z_r) = \alpha$. Further we say that the pair $(f, g) \in R^2$ *represents* $\beta \in K$ if $g \notin \mathcal{I}$ (i.e. $g(z_1, \dots, z_r) \neq 0$) and $\frac{f(z_1,\dots,z_r)}{g(z_1,\dots,z_r)} = \beta$. We will also use the terminology that f is a *representative* for α, or (f, g) is a *pair of representatives* for β. Clearly, any element $\alpha \in A$ has infinitely many representatives, and any $\beta \in K$ has infinitely many pairs of representatives. However, since one can effectively decide whether a given polynomial of R belongs to a given ideal of R or not (see [**1**]), one can also effectively decide if two polynomials represent the same element of A, or if two pairs of polynomials of R represent the same element of K. Indeed, two polynomials $f, f' \in R$ represent the same element $\alpha \in A$ if and only if $f - f' \in \mathcal{I}$, and two pairs of polynomials $(f, g), (f', g') \in R^2$ represent the same element $\beta \in K$ if and only if $fg' - f'g \in \mathcal{I}$.

We shall measure elements of A by their representatives. For a non-zero polynomial $f \in R$ let us denote by $\deg f$ the total degree of f and by $h(f)$ the absolute logarithmic height of f, i.e. the logarithm of the maximum of the absolute values of its coefficients. Further we define the size of f by

$$s(f) := \max(1, \deg f, h(f)).$$

For the constant 0 polynomial we define $s(0) := 1$.

Throughout the paper we shall use the notation $O(\cdot)$ to denote a quantity which is c times the expression between the parentheses, where c is an effectively computable positive absolute constant which may be different at each occurrence of the O-symbol. Further, throughout the paper we write $\log^* a := \max(1, \log a)$ for $a > 0$, and $\log^* 0 := 1$.

2·2. *Results*

Let A be a finitely generated domain given in the form (2.1), where the ideal $\mathcal{I}$ is generated by the polynomials $f_1, \dots, f_t \in \mathbb{Z}[X_1, \dots, X_r]$. Let K denote the quotient field of A and denote by $\overline{K}$ the algebraic closure of K.

Let $F(X, Y) = \sum_{(i,j)\in I} a_{ij} X^i Y^j \in A[X, Y]$ be a polynomial of total degree $N :=$

$\deg F$, and suppose that F fulfils the following condition:

$$\begin{gathered} F \textbf{ is not divisible by} \text{ any non-constant polynomial of the form} \\ X^m Y^n - \alpha \quad \text{or} \quad X^m - \alpha Y^n, \text{where } m, n \in \mathbb{Z}_{\geq 0} \text{ and } \alpha \in \overline{K}^*. \end{gathered} \tag{2.3}$$

Further, suppose that we are given representatives $\tilde{a}_{ij} \in \mathbb{Z}[X_1, \ldots, X_r]$ of $a_{ij} \in A$, respectively. Put $\tilde{F}(X, Y) := \sum_{(i,j)\in I} \tilde{a}_{ij} X^i Y^j$. We assume that

$$\begin{cases} \deg f_1, \ldots, \deg f_t, \deg \tilde{a}_{ij} \leq d \ \text{ for every } \ (i,j) \in I \\ h(f_1), \ldots, h(f_t), h(\tilde{a}_{ij}) \leq h \ \text{ for every } \ (i,j) \in I, \end{cases} \tag{2.4}$$

where d, h are real numbers with $d > 1$ and $h > 1$. In Section 3 we show that condition (2.3) is effectively decidable in terms of $f_1, \ldots, f_t$ and the $\tilde{a}_{ij}$.

THEOREM 2·1. *If A is a finitely generated domain as above, and F fulfils the condition (2.3) then for all elements (x, y) of the set*

$$\mathcal{C} := \{(x, y) \in (A^*)^2 | F(x, y) = 0\} \tag{2.5}$$

there exist representatives $\tilde{x}$, $\tilde{y}$, $\tilde{x}'$ and $\tilde{y}'$ of x, y, x^{-1} and y^{-1}, respectively, such that

$$s(\tilde{x}), s(\tilde{y}), s(\tilde{x}'), s(\tilde{y}') \leq \exp\left\{(2d)^{\exp O(r)} (2N)^{(\log^* N)\cdot \exp O(r)} \cdot (h+1)^3\right\}. \tag{2.6}$$

We mention that the above result is effective in the sense that it provides an algorithm to determine, at least in principle, all elements of the set (2.5). Indeed, there are only finitely many polynomials of $\mathbb{Z}[X_1, \ldots, X_r]$ below the bound in (2.6) and these can be effectively enumerated. Further, $(x, y) \in \mathcal{C}$ is clearly fulfilled if and only if there are polynomials $\tilde{x}, \tilde{y}, \tilde{x}', \tilde{y}' \in \mathbb{Z}[X_1, \ldots, X_r]$ with their sizes below the bound (2.6), which fulfil

$$\tilde{x} \cdot \tilde{x}' - 1, \ \tilde{y} \cdot \tilde{y}' - 1, \ \tilde{F}(\tilde{x}, \tilde{y}) \in \mathcal{I}. \tag{2.7}$$

So we can enlist all 4-tuples $(\tilde{x}, \tilde{y}, \tilde{x}', \tilde{y}')$ with $s(\tilde{x}), s(\tilde{y}), s(\tilde{x}'), s(\tilde{y}')$ being smaller than our bound, then (using an ideal membership algorithm) check if (2.7) is fulfilled. Finally, we have to group all the tuples in which $(\tilde{x}, \tilde{y})$ represent the same pair $(x, y) \in (A^*)^2$ and pick out one pair from each group. So we get a list consisting of one representative for each element of the set (2.5).

3. *Preparations for the proof of Theorem* 2·1

3·1. *Analyzing the condition (*2.3*) posed on* F

Let $A, K, \overline{K}$ be as in Section 2·2 and let $F(X,Y) \in A[X,Y]$ be a bivariate polynomial given by

$$F(X,Y) = \sum_{(i,j)\in I} a_{ij} X^i Y^j,$$

where $I \subset \mathbb{Z}^2_{\geq 0}$ is a finite set, and $0 \neq a_{ij} \in A$ are fixed for $(i,j) \in I$. Denote by N the total degree of F and by $n(F)$ the number of non-zero coefficients of F.

For any partition $\mathcal{P} = (I_1, \dots, I_k)$ of I with $|I_l| \geq 2$ for $l = 1, \dots, k$ we define the $\mathbb{Z}$-module

$$\Lambda(F,\mathcal{P}) := \langle \{(i_1,j_1) - (i_2,j_2) \mid (i_1,j_1),(i_2,j_2) \in I_l \text{ for some } l = 1,\dots,k\} \rangle$$

i.e. the $\mathbb{Z}$-module defined by all differences of pairs of exponents (i,j) belonging to the same set in the partition $\mathcal{P}$. Let $r(F,\mathcal{P})$ denote the rank of the $\mathbb{Z}$-module $\Lambda(F,\mathcal{P})$.

In the sequel, for any solution (x,y) of the equation

$$F(x,y) = 0 \qquad \text{in} \quad x,y \in A^* \tag{3.1}$$

we say that a partition $\mathcal{P}$ of I corresponds to F and (x,y) if $\mathcal{P} = (I_1,\dots,I_k)$ such that

(i) $I_1 \cup I_2 \cup \cdots \cup I_k = I$, $I_i \cap I_j = \emptyset$ for $i \neq j$, $I_l \neq \emptyset$ for $l = 1,\dots,k$
(ii) x,y is a solution of the following system

$$\sum_{(i,j)\in I_l} a_{ij} x^i y^j = 0 \qquad \text{for} \quad l = 1,\dots,k. \tag{3.2}$$

(iii) $\sum_{(i,j)\in I_0} a_{ij} x^i y^j \neq 0$ for any proper subset I_0 of any of the sets I_l for $l = 1,\dots,k$.

In this case we shall also say that (x,y) is associated with the partition $\mathcal{P}$. We mention that $a_{ij} \neq 0$, $x,y \in A^*$ and (3.2) imply $|I_l| \geq 2$ for $l = 1,\dots,k$.

Let us analyze now the case when for a given partition $\mathcal{P}$ the rank of $\Lambda := \Lambda(F,\mathcal{P})$ is 1. This means that there exists a pair $(m,n) \in \mathbb{Z}^2$ with $\gcd(m,n) = 1$ such that for any two elements $(i,j),(i',j') \in I_l$ for $l = 1,\dots,k$ we have $(i,j) - (i',j') = t \cdot (m,n)$ with $t \in \mathbb{Z}$, $|t| \leq N$. Fixing an element $(i_l,j_l) \in I_l$ for $l = 1,\dots,k$ we get that every $(i,j) \in I_l$ can be written as $(i,j) = (i_l,j_l) + t_{ij}(m,n)$, for $l = 1,\dots,k$, with some $t_{ij} \in \mathbb{Z}$, $|t_{ij}| \leq N$. Thus the system (3.2) is equivalent to the system

$$X^{i_l} Y^{j_l} \sum_{(i,j)\in I_l} a_{ij} (X^m Y^n)^{t_{ij}} = 0 \qquad \text{for} \quad l = 1,\dots,k.$$

By multiplying these equations by suitable powers of $X^m Y^n$ we see that it is equivalent to a system

$$g_l(X^m Y^n) = 0 \qquad \text{for} \quad l = 1,\dots,k, \tag{3.3}$$

where $g_l \in A[X]$, $g_l(0) \neq 0$ for $l = 1, \ldots, k$ and

$$g_l(X) := \sum_{(i,j)\in I_l} a_{ij} X^{s_{ij}}, \tag{3.4}$$

where $0 \leq s_{ij} \leq 2N$. We shall call $(g_1, \ldots, g_k)$ the polynomial system corresponding to the partition $\mathcal{P}$. Now the fact that (3.1) has a solution associated with $\mathcal{P}$ is equivalent to the system (3.3) having a solution $x, y \in A^*$ which can happen only if the polynomials $g_k(X)$ have a common root $\alpha \in A^*$, i.e. $X - \alpha$ divides g_l for all $l = 1, \ldots, k$, which contradicts the assumption (2.3). Now we are ready to state two Propositions:

PROPOSITION 3·1. *Let $F(X, Y) \in A[X, Y]$ be a polynomial. Then F satisfies condition (2.3) if and only if for any partition $\mathcal{P} = (I_1, \ldots, I_k)$ of I we have one of the following:*

(i) *$r(\mathcal{P}) = 2$, or*

(ii) *$r(\mathcal{P}) = 1$, and the polynomial system $(g_1, \ldots, g_k) \in A[X]^k$ corresponding to $\mathcal{P}$ has the property*

$$\gcd(g_1, \ldots, g_k) = 1 \qquad \text{in} \quad K[X].$$

Proof. First suppose that (2.3) holds. Let $\mathcal{P}$ be any partition of rank 1 and assume $\gcd(g_1, \ldots, g_k) \neq 1$ over K. Thus there exists $\alpha \in \overline{K}$ with $g_i(\alpha) = 0$ for $i = 1, \ldots, k$, thus $X^m Y^n - \alpha$ or $X^m - \alpha Y^n$ divides F for some $m, n \in \mathbb{Z}_{\geq 0}$, which contradicts (2.3).

Conversely, we show that if F has a factor of the form $X^m Y^n - \alpha$ or $X^m - \alpha Y^n$ with $m, n \in \mathbb{Z}_{\geq 0}$ and $\alpha \in \overline{K}$ then there exists a partition $\mathcal{P}$ of I such that $r(\mathcal{P}, F) = 1$ and $\gcd(g_1, \ldots, g_k) \neq 1$ over K. To simplify the proof we consider F as a Laurent polynomial. Then an equivalent formulation of our assumption is that F has a non-constant divisor of the form $X^m Y^n - \alpha$ with $m, n \in \mathbb{Z}$ and $\alpha \in \overline{K}$. Clearly, we may suppose $(m, n) = 1$, thus there exist $m', n' \in \mathbb{Z}$ with $mn' - nm' = 1$. Put $U = X^m Y^n$ and $V = X^{m'} Y^{n'}$, and define the Laurent polynomial F' by $F'(U, V) = F(X, Y)$. Now F' is divisible by $U - \alpha$, thus we have $F'(\alpha, V) \equiv 0$. If we write

$$F'(U, V) = \sum_{i=0}^{k} V^i g_i(U)$$

then by $F'(\alpha, V) \equiv 0$ we must have $g_i(\alpha) = 0$ for all $i = 1, \ldots, k$, and thus $\gcd(g_1, \ldots, g_k) \neq 1$ in $K[U]$. Writing F in the form

$$F(X, Y) = \sum_{i=0}^{k} X^{im'} Y^{in'} g_i(X^m Y^n)$$

induces a partition $\mathcal{P} = (I_1, \ldots, I_k)$, with $r(\mathcal{P}, F) = 1$ and $\gcd(g_1, \ldots, g_k) \neq 1$ over K. This concludes the proof of the proposition. □

PROPOSITION 3·2. *Let $F(X, Y)$ be a polynomial satisfying (2.3) and fix a solution (x, y) of (3.1). Let $\mathcal{P} = (I_1, \ldots, I_k)$ be a partition of I corresponding to F and (x, y) and*

let $\Lambda := \Lambda(F, \mathcal{P})$ *be the* $\mathbb{Z}$*-module corresponding to the solution* (x, y) *and the partition* $\mathcal{P}$*. Then we have*

$$r(\mathcal{P}) = 2.$$

Proof. This is a direct consequence of Proposition 3·1, since for a solution (x, y) and a partition $\mathcal{P}$ associated with it, with $r(\Lambda(F, \mathcal{P})) = 1$ the corresponding polynomial system must consist of co-prime elements, which contradicts (ii) of Proposition 3·1, i.e. only $r(\Lambda(F, \mathcal{P})) = 2$ is possible. □

The above two propositions mean in fact, that for a polynomial fulfilling condition (2.3) there might exist partitions of I of rank 1, but these are never partitions corresponding to a solution.

3·2. *Effective estimates for the* gcd *of polynomials*

For a polynomial $P \in \mathbb{C}[X]$ let $||P||_1$ denote the sum of the absolute values of the coefficients of P.

PROPOSITION 3·3. *Let* A *be a finitely generated domain as in Section* 2·2 *and* K *its quotient field. Let* $k, \rho \in \mathbb{N}$ *be with* $2^{k-1} \leq \rho \leq 2^k$ *and let*

$$g_i(X) := \sum_{j=0}^{\delta} x_{ij} X^j \in A[X] \qquad \text{for} \quad i = 1, \dots, \rho$$

be non-zero polynomials such that $\gcd(g_1, \dots, g_\rho)$ *in* $K[X]$ *has degree* δ_0*. Let* $\mathbf{x} := (x_{ij} : i = 1, \dots, \rho, j = 0, \dots, \delta)$ *be the vector consisting of the coefficients of the polynomials* $g_1, \dots, g_\rho$*.*

Then there exist polynomials $P_0, \dots, P_{\delta_0}$ *with integer coefficients, in* $\rho(\delta + 1)$ *variables with the following properties:*

(i) $\deg P_i \leq (2\delta)^k$*, and* $||P_i||_1 \leq (2\delta)^{2\delta + (2\delta)^2 + \dots + (2\delta)^k}$*;*

(ii) *There are polynomials* $u_1, \dots, u_\rho \in A[X]$ *such that*

$$u_1 g_1 + \dots + u_\rho g_\rho = \sum_{j=0}^{\delta_0} P_j(\mathbf{x}) X^j,$$

where not all $P_j(\mathbf{x})$ *are* 0*.*

For the proof of Proposition 3·3 we need the following:

LEMMA 3·4. *Let* A *be a finitely generated domain as in Section* 2·2 *and* K *its quotient field. Let* $g_1, g_2 \in A[X]$ *be non-zero polynomials with* $\deg g_1 = n_1$*,* $\deg g_2 = n_2$*, and such that* $\gcd(g_1, g_2)$ *in* $K[X]$ *has degree* δ_0*. Then there exist polynomials* $u_1, u_2, g \in A[X]$ *with*

$$u_1 g_1 + u_2 g_2 = g, \tag{3.5}$$

with $\deg u_1 \le n_2-\delta_0-1$, $\deg u_2 \le n_1-\delta_0-1$, $\deg g = \delta_0$, *and such that the coefficients of* g *are determinants of order* $n_1+n_2-2\delta_0$ *of which* $n_2-\delta_0$ *columns consist of coefficients of* g_1 *and* $n_1-\delta_0$ *columns consist of coefficients of* g_2. *Further, in this case we have automatically* $g = \gcd(g_1, g_2)$ *in* $K[X]$.

Proof. By properties of the gcd of polynomials over a field there exist $g = \gcd(g_1, g_2) \in K[X]$ and $u_1, u_2 \in K[X]$ with (3.5), and reducing u_1 modulo g_2/g, and u_2 modulo g_1/g it is clear that we may choose u_1, u_2 such that $\deg u_1 \le n_2 - \delta_0 - 1$ and $\deg u_2 \le n_1 - \delta_0 - 1$. Further the triple (u_1, u_2, g) is unique up to a common constant factor from K. Multiplying the identity by a common multiple of all the denominators of the coefficients of g, u_1, u_2 we can guarantee also $g, u_1, u_2 \in A[X]$. Write

$$u_1 := \sum_{i=0}^{n_2-\delta_0-1} x_i X^i, \qquad u_2 := \sum_{i=0}^{n_1-\delta_0-1} y_i X^i \qquad g = \sum_{i=0}^{\delta_0} z_i X^i.$$

Then by equating coefficients, the polynomial identity

$$u_1 g_1 + u_2 g_2 - g = 0$$

is equivalent to a system of linear equations

$$\begin{pmatrix} -I & F_{11} & F_{12} \\ \mathbf{0} & F_{21} & F_{22} \end{pmatrix} \cdot \begin{pmatrix} \mathbf{z} \\ \mathbf{x} \\ \mathbf{y} \end{pmatrix} = \underline{0}.$$

in the variables x_i, y_i, z_i, consisting of $n_1 + n_2 - \delta_0$ linearly independent equations. In this system the block $-I$ is the negative of a unit matrix of order $\delta_0 + 1$, F_{11} and F_{21} are blocks (of $n_2 - \delta_0$ columns) consisting of coefficients of g_1 and F_{12} and F_{22} blocks (of $n_1 - \delta_0$ columns) consisting of coefficients of g_2.

The solution subspace of this system of equations is one-dimensional, and we have one more unknown than the number of equations. Hence the equations in the system are linearly independent. Further, this system of equations has the non-zero solution $(\Delta_1, -\Delta_2, \ldots, \pm\Delta_{n_1+n_2-\delta_0+1})^{\mathrm{T}}$, where Δ_i denotes the determinant of the matrix obtained from the matrix of our system by removing the ith column. So we may take

$$g(X) = \Delta_1 - \Delta_2 X + \Delta_3 X^2 + \cdots \pm \Delta_{\delta_0+1} X^{\delta_0}.$$

This concludes the proof of our lemma. □

Proof of Proposition 3·3 We may assume without loss of generality that $\rho = 2^k$, otherwise we copy some of the polynomials $g_1, \ldots, g_\rho$ to have 2^k polynomials.

Now we use induction on k. For $k = 1$ the statement is true by Lemma 3·4. So we assume that the statement of our proposition is true for $k-1$ and we prove it for k. Suppose that

$$\deg \gcd(g_1, \ldots, g_{2^{k-1}}) = d_1, \qquad \deg \gcd(g_{2^{k-1}+1}, \ldots, g_{2^k}) = d_2 \quad \text{in } K[X].$$

Then by the inductive assumption there are polynomials $v_1, \dots, v_{2^{k-1}} \in A[X]$ with

$$\sum_{i=1}^{2^{k-1}} v_i g_i = \sum_{j=0}^{d_1} Q_{1j}(\mathbf{x}_1) X^j,$$

where not all Q_{1j} are zero and where $\mathbf{x}_1$ is the vector consisting of all coefficients of the polynomials $g_1, \dots, g_{2^{k-1}}$, and there also exist polynomials $v_{2^{k-1}+1}, \dots, v_{2^k} \in A[X]$ with

$$\sum_{i=2^{k-1}+1}^{2^k} v_i g_i = \sum_{j=0}^{d_2} Q_{2j}(\mathbf{x}_2) X^j,$$

where not all Q_{2j} are zero and where $\mathbf{x}_2$ is the vector consisting of all coefficients of the polynomials $g_{2^{k-1}+1}, \dots, g_{2^k}$. Further, by the induction hypothesis we may assume

$$\deg Q_{ij} \le (2\delta)^{k-1}, \qquad ||Q_{ij}||_1 \le (2\delta)^{2\delta + \dots + (2\delta)^{k-1}} := c(\delta)$$

for $i = 1, 2$ and $j = 0, \dots, d_i$. By Lemma 3·4 there are $w_1, w_2 \in A[X]$ such that

$$w_1 \sum_{j=0}^{d_1} Q_{1j}(\mathbf{x}_1) X^j + w_2 \sum_{j=0}^{d_2} Q_{2j}(\mathbf{x}_2) X^j = \sum_{j=0}^{\delta_0} P_j(\mathbf{x}) X^j,$$

with $P_{\delta_0} \neq 0$, and where P_j is a determinant of order $d_1 + d_2 - 2\delta_0$ of which $d_2 - \delta_0$ columns consist of polynomials Q_{1j} $(j = 1, \dots, d_1)$ and $d_1 - \delta_0$ columns of polynomials Q_{2j} $(j = 1, \dots, d_2)$. This implies

$$\deg P_j(\mathbf{x}) \le (d_2 - \delta_0)(2\delta)^{k-1} + (d_1 - \delta_0)(2\delta)^{k-1} \le \delta(2\delta)^{k-1} + \delta(2\delta)^{k-1} \le (2\delta)^k,$$

and

$$\begin{aligned} ||P_j||_1 &\le \{(d_1 + d_2 - 2\delta_0) \cdot c(\delta)\}^{d_2 - \delta_0} \cdot \{(d_1 + d_2 - 2\delta_0) \cdot c(\delta)\}^{d_1 - \delta_0} \\ &\le \left\{(2\delta)^{\delta} \cdot (2\delta)^{\delta \cdot (2\delta + \dots + (2\delta)^{k-1})}\right\}^2 \le (2\delta)^{2\delta + \dots + (2\delta)^k}. \end{aligned}$$

This concludes the proof of Proposition 3·3. □

COROLLARY 3·1. *Let A be a finitely generated domain as in Section 2·2 and K its quotient field. Let $k, \rho \in \mathbb{N}$ be with $2^{k-1} \le \rho \le 2^k$ and define the polynomials*

$$g_i(X) := \sum_{j=0}^{\delta} x_{ij} X^j \in A[X] \qquad \text{for} \quad i = 1, \dots, \rho.$$

Further, suppose that the coefficients $x_{ij} \in A$ have representatives $\tilde{x}_{ij}$ with

$$\deg \tilde{x}_{ij} \le d, \qquad h(\tilde{x}_{ij}) \le h,$$

where $d > 1$ and $h > 1$ are given real numbers. Suppose that

$$\gcd(g_1, \dots, g_\rho) = 1 \quad \text{in } K[X].$$

Then there exist polynomials $u_1, \dots, u_\rho \in A[X]$ such that

$$u_1 g_1 + \dots + u_\rho g_\rho = R,$$

where $R \in A$, $R \neq 0$, and R has a representative $\tilde{R}$ with

$$\deg \tilde{R} \leq d(2\delta)^k, \qquad h(\tilde{R}) \leq (2\delta)^{k+2}(d+1)rh.$$

Proof. Put $\mathbf{x} := (x_{ij} \ : \ i = 1, \ldots, \rho, j = 0, \ldots, \delta)$ be the vector consisting of the coefficients of the polynomials $g_1, \ldots, g_\rho$. By Proposition 3·3 there exist polynomials $u_1, \ldots, u_\rho \in A[X]$ such that

$$u_1 g_1 + \cdots + u_\rho g_\rho = P_0(\mathbf{x}),$$

where $P_0(\mathbf{X})$ is a polynomial in $\rho(\delta+1)$ variables with integer coefficients and with

$$\deg P_0 \leq (2\delta)^k, \qquad ||P_0||_1 \leq (2\delta)^{2\delta+(2\delta)^2+\cdots+(2\delta)^k}.$$

This together with $\deg \tilde{x}_{ij} \leq d$ proves

$$\deg \tilde{R} \leq d(2\delta)^k.$$

Clearly by the assumptions of the corollary we have

$$||\tilde{x}_{ij}||_1 \leq (d+1)^r h,$$

thus

$$||\tilde{R}||_1 = ||P_0||_1((d+1)^r h)^{(2\delta)^k} \leq (2\delta(d+1)^r h)^{(2\delta)^{k+1}}.$$

and finally we get

$$h(\tilde{R}) \leq \log ||\tilde{R}||_1 \leq (2\delta)^{k+2}(d+1)rh.$$

□

4. *Extending A to a larger ring*

First we shall extend our domain A to a larger domain B and prove an effective result for the set

$$\mathcal{C}' := \{(x, y) \in (B^*)^2 | F(x, y) = 0\}$$

The main advantage of this will be, that we choose the larger domain B such that it will be easier to do effective computations with elements of B then it is with elements of A.

Recall that $A = \mathbb{Z}[z_1, \ldots, z_r]$ is a finitely generated domain, and let us denote by K the quotient field of A. Let $f_1, \ldots, f_t$ be the generators of the ideal $\mathcal{I}$ that defines our domain A (see (2.1), (2.2)) and put

$$d_0 := \max(1, \deg f_1, \ldots, \deg f_t), \qquad h_0 := \max(1, h(f_1), \ldots, h(f_t)). \tag{4.1}$$

Let $q \geq 0$ denote the transcendence degree of K and suppose without loss of generality that $z_1, \ldots, z_q$ is a transcendence basis of $K/\mathbb{Q}$. Put

$$K_0 := \mathbb{Q}(z_1, \ldots, z_q), \qquad A_0 := \mathbb{Z}[z_1, \ldots, z_q], \tag{4.2}$$

with the convention that in the case $q = 0$ we put $K_0 = \mathbb{Q}$ and $A_0 = \mathbb{Z}$. For elements $0 \neq f \in A_0$ we will use the notation $\deg f$ and $h(f)$ for the total degree and logarithmic height of f, respectively, viewed as a polynomial in the unknowns $z_1, \dots, z_q$, with the convention that in the case $q = 0$ we put $\deg f := 0$ and $h(f) := \log |f|$.

The field K is clearly a finite algebraic extension of K_0, so we have $K = K_0(w)$ for some $w \in K$. We shall see that w may be chosen in such a way that it is integral over A_0, the degree of its minimal polynomial, and the degree and height of the coefficients of its minimal polynomial are bounded. Further, there exists an element $f \in A_0$, such that $A \subset A_0[w, f^{-1}] := B$, some "important" elements are units in B, and the degree and height of f is also bounded. This is described more precisely in the following proposition. Recall that a_{ij} denote the coefficients of F and N is the total degree of F in Theorem 2·1. Let us use the notation $\log_2^* x := \max(1, \log_2 x)$.

PROPOSITION 4·1. *(i) There exists an element $w \in A$ which is integral over A_0 such that $K = K_0(w)$ and having minimal polynomial*

$$\mathcal{F}(X) = X^D + \mathcal{F}_1 X^{D-1} + \cdots + \mathcal{F}_D \in A_0[X]$$

over K_0 of degree $D \leq d_0^{r-q}$, such that

$$\deg \mathcal{F}_k \leq (2d_0)^{\exp O(r)}, \qquad h(\mathcal{F}_k) \leq (2d_0)^{\exp O(r)}(h_0 + 1) \tag{4.3}$$

for $k = 1, \dots, D$.

(ii) Let $R \in A$ and suppose that R has a representative $\tilde{R}$ with

$$\deg \tilde{R} \leq d(4N)^{\log_2^* N}, \qquad h(\tilde{R}) \leq (4N)^{\log_2^* N + 2}(d+1)rh. \tag{4.4}$$

Then there exists a non-zero $f \in A_0$ such that

$$\begin{aligned} &A \subseteq A_0[w, f^{-1}], \\ &a_{ij} \in A_0[w, f^{-1}]^* \qquad \text{for } (i,j) \in I \\ &R \in A_0[w, f^{-1}]^* \end{aligned} \tag{4.5}$$

and

$$\begin{aligned} &\deg f \leq (2d)^{\exp O(r)} \cdot (2N)^{\log^* N \cdot \exp O(r)}, \\ &h(f) \leq (2d)^{\exp O(r)} \cdot (2N)^{\log^* N \cdot \exp O(r)} \cdot h. \end{aligned} \tag{4.6}$$

Remark. The element R above for the moment may be any $R \in A$ with (4.4), and it will be specified at the very end of our proof in equation (6.18).

Proof of Proposition 4·1 In the proof for convenience we shall use Proposition 3.1 of [**3**]. However, this proposition is just a suitable reformulation and combination of Proposition 3.4, Lemma 3.2, (i), and Lemma 3.6. of Evertse and Győry [**12**]. In principle (i) of the present proposition is exactly (i) of Proposition 3.1 of [**12**].

To prove (ii) we will use (ii) of Proposition 3.1 of [**3**] with the choice

$$\{\alpha_1, \dots, \alpha_k\} = \{a_{ij}, \quad \text{for } (i,j) \in I\} \cup \{R\}.$$

Thus we have $k = n(F) + 1 < O(N^2)$, where $n(F)$ denotes the number of non-zero coefficients of F. Further, we may choose v_l to be 1, and u_l to be one of the polynomials $\tilde{a}_{ij}$ for $l = 1, \dots, k-1$, and we also may choose $v_k = 1$ and $u_k = \tilde{R}$ which gives the estimates

$$d^{**} = d(4N)^{\log_2^* N} \quad \text{and} \quad h^{**} = (4N)^{\log_2^* N + 2}(d+1)rh.$$

Now we use statement (ii) of Proposition 3.1 of [**3**] and we choose a larger constant in the $O(\cdot)$ symbol to simplify the expressions in the bounds. This concludes the proof of our Proposition 4·1. □

Next we introduce a new representation for the elements of the field K. As in Proposition 4·1 we denote the degree of K over K_0 by D. Since $K = K_0(w)$ every element $\alpha \in K$ can be written uniquely in the form $\sum_{j=0}^{D-1} R_{\alpha,j} w^j$, where $R_{\alpha,j} \in K_0$. Since K_0 is the fraction field of A_0, and A_0 is a unique factorization domain (indeed, $z_1, \dots, z_q$ are algebraically independent), there exist $P_{\alpha,0}, \dots, P_{\alpha,D-1}, Q_\alpha \in A_0$ such that the above representation can be rewritten in the form

$$\alpha = Q_\alpha^{-1} \sum_{j=0}^{D-1} P_{\alpha,j} w^j \quad \text{with} \quad Q_\alpha \neq 0, \quad \gcd(P_{\alpha,0}, \dots, P_{\alpha,D-1}, Q_\alpha) = 1. \tag{4.7}$$

Further, the tuple $(P_{\alpha,0}, \dots, P_{\alpha,D-1}, Q_\alpha)$ in the representation (4.7) of α is up to sign uniquely determined.

Using this representation we introduce two new concepts which will turn out to be useful to measure elements of K. Let us define

$$\begin{cases} \overline{\deg}\,\alpha := \max(\deg P_{\alpha,0}, \dots, \deg P_{\alpha,D-1}, \deg Q_\alpha) \\ \overline{h}(\alpha) := \max(h(P_{\alpha,0}), \dots, h(P_{\alpha,D-1}), h(Q_\alpha)), \end{cases} \tag{4.8}$$

with the convention that for $q = 0$ we define $\overline{\deg}\,\alpha = 0$ and $\overline{h}(\alpha) = \log \max(|P_{\alpha,0}|, \dots, |P_{\alpha,D-1}|, |Q_\alpha|)$.

The following Lemma shows that $\overline{\deg}\,\alpha$ and $\overline{h}(\alpha)$ may be bounded by the height and degree of representatives for α, the bound being dependent also on parameters of A, and conversely, $\alpha \in A$ has a representative whose height and degree are bounded by $\overline{\deg}\,\alpha$ and $\overline{h}(\alpha)$, the bound again being dependent also on parameters of A.

LEMMA 4·2. *(i) Let $\alpha \in K^*$ and let (a, b) be a pair of representatives for α with $a, b \in \mathbb{Z}[X_1, \dots, X_r]$, $b \notin I$. Put*

$$d^* = \max(d_0, \deg a, \deg b) \quad \textit{and} \quad h^* := \max(h_0, h(a), h(b)).$$

Then

$$\overline{\deg}\,\alpha \le (2d^*)^{\exp O(r)}, \qquad \overline{h}(\alpha) \le (2d^*)^{\exp O(r)}(h^*+1). \tag{4.9}$$

(ii) Let α be a nonzero element of A, and put

$$\widehat{d} := \max(d_0, \overline{\deg}\,\alpha), \qquad \widehat{h} := \max(h_0, \overline{h}(\alpha)).$$

Then α has a representative $\tilde{\alpha} \in \mathbb{Z}[X_1, \dots, X_r]$ such that

$$\begin{cases} \deg \tilde{\alpha} \le (2\widehat{d})^{\exp O(r \log^* r)}(\widehat{h}+1), \\ h(\tilde{\alpha}) \le (2\widehat{d})^{\exp O(r \log^* r)}(\widehat{h}+1)^{r+1}. \end{cases} \tag{4.10}$$

Moreover, if $\alpha \in A^*$ then α^{-1} has a representative $\tilde{\alpha}' \in \mathbb{Z}[X_1, \dots, X_r]$ with

$$\begin{cases} \deg \tilde{\alpha}' \le (2\widehat{d})^{\exp O(r \log^* r)}(\widehat{h}+1), \\ h(\tilde{\alpha}') \le (2\widehat{d})^{\exp O(r \log^* r)}(\widehat{h}+1)^{r+1}. \end{cases} \tag{4.11}$$

Proof. Statement (i) is Lemma 3.5 in Evertse and Győry [**12**], while (ii) is a special case of Lemma 3.7 of Evertse and Győry [**12**] with the choice $\lambda = 1$ and $a = b = 1$. See also Lemma 3.4 and Lemma 3.5 of [**3**]. □

In the following proposition we shall state a generalization of our Theorem 2·1 and then we show how our Theorem 2·1 follows from that. Then the rest of the paper will be devoted to the proof of this more general proposition.

PROPOSITION 4·3. *Let w and f be as in Proposition 4·1 and put*

$$B := A_0[f^{-1}, w].$$

Then for every element (x, y) of the set

$$\mathcal{C}' := \{(x, y) \in (B^*)^2 | F(x, y) = 0\}$$

we have

$$\overline{\deg}\,x,\ \overline{\deg}\,y \le (2d)^{\exp O(r)} \cdot (2N)^{\log^* N \cdot \exp O(r)}, \tag{4.12}$$

$$\overline{h}(x),\ \overline{h}(y) \le \exp\left\{\cdot (2d)^{\exp O(r)}(2N)^{\log^* N \cdot \exp O(r)} \cdot (h+1)^3\right\}. \tag{4.13}$$

Now we give the proof of Theorem 2·1 using Proposition 4·3, which will be proved in the next two sections.

Proof of Theorem 2·1 Let $(x, y) \in \mathcal{C}$. Since $A \subseteq B$ we also have $(x, y) \in \mathcal{C}'$ where $B = A_0[f^{-1}, w]$, with f, w satisfying the conditions specified in Proposition 4·1. Then we use Proposition 4·3, to infer (4.12) and (4.13), and then we apply Lemma 4·2 (ii) to x and y, to show that x, y, x^{-1} and y^{-1} have representatives $\tilde{x}, \tilde{y}, \tilde{x}', \tilde{y}' \in \mathbb{Z}[X_1, \dots, X_r]$ with (2.6). □

5. *Bounding the degree in Proposition* 4·3

In this section we shall consider K as a function field in one variable, and we shall prove (4.12) using earlier results of Brownawell and Masser [**10**] for function fields.

We recall the definition of valuations and height on function fields in one variable. Let $\Bbbk$ be an algebraically closed field of characteristic 0, z a transcendental element over $\Bbbk$ and M a finite extension of $\Bbbk(z)$. Denote by $g_{M/\Bbbk}$ the genus of M, and by $\mathcal{M}_M$ the collection of valuations of $M/\Bbbk$, which are the discrete valuations of M with value group $\mathbb{Z}$ which are trivial on $\Bbbk$. Recall that these valuations satisfy the sum formula

$$\sum_{v\in\mathcal{M}_M} v(\alpha) = 0 \qquad \text{for} \quad \alpha \in M^*.$$

For a finite subset S of $\mathcal{M}_M$, an element $\alpha \in M$ is called an S-integer if $v(\alpha) \geq 0$ for all $v \in \mathcal{M}_M \setminus S$. The S-integers form a ring in M, denoted by $\mathcal{O}_S$. The (homogeneous) height of $\mathbf{a} = (\alpha_1, \ldots, \alpha_l) \in M^l$ relative to $M/\Bbbk$ is defined by

$$H_M^*(\mathbf{a}) = H_M^*(\alpha_1, \ldots, \alpha_l) := -\sum_{v\in\mathcal{M}_M} \min(v(\alpha_1), \ldots, v(\alpha_l)).$$

The height of $\alpha \in M$ relative to $M/\Bbbk$ is defined by

$$H_M(\alpha) := H_M^*(1, \alpha) = -\sum_{v\in\mathcal{M}_M} \min(0, v(\alpha)).$$

We have $H_M(\alpha) = 0$ if and only if $\alpha \in \Bbbk$.

First we recall a Lemma of [**3**] which will be useful for bounding the genus:

LEMMA 5·1. *Let $\Bbbk$ be an algebraically closed field, z a transcendental element over $\Bbbk$ and put $M = \Bbbk(z)$. Let*

$$F = f_0X^l + f_1X^{l-1} + \cdots + f_l \in M[X]$$

be a polynomial with $f_0 \neq 0$ and with non-zero discriminant. Let L be the splitting field of F over M. Then we have

$$g_{L/\Bbbk} \leq [L : M] \cdot l \max(\deg f_0, \ldots, \deg f_l).$$

Proof. This is a special case of Lemma 4.2 of [**3**]. □

PROPOSITION 5·2. *Let $\Bbbk$ be an algebraically closed field of characteristic 0, z a transcendental element over $\Bbbk$ and M a finite extension of $\Bbbk(z)$. Denote by $g_{M/\Bbbk}$ the genus of M and let S be a finite set of valuations of M. Denote by $\mathcal{O}_S$ the ring of S-integers of M, and by $\mathcal{O}_S^*$ its unit group. Consider the equation*

$$u_1 + \cdots + u_n = 0 \qquad \text{in} \qquad u_1, \ldots, u_n \in \mathcal{O}_S^*. \tag{5.1}$$

For every non-degenerate solution $u_1, \dots, u_n$ of the above equation we have

$$H_M^*(u_1, \dots, u_n) \leq \frac{1}{2}(n-1)(n-2)(|S| + g_{M/\Bbbk}).$$

Proof. This is in fact a variant of Corollary I of Brownawell and Masser [**10**], modified according to the remark after Theorem B of [**10**]. □

PROPOSITION 5·3. *Let $\Bbbk$ be an algebraically closed field of characteristic 0, z a transcendental element over $\Bbbk$, M a finite extension of $\Bbbk(z)$, and $\overline{M}$ the algebraic closure of M. Denote by $g_{M/\Bbbk}$ the genus of M and let S be a finite set of valuations of M. Denote by $\mathcal{O}_S$ the ring of S-integers of M, and by $\mathcal{O}_S^*$ its unit group. Let $F(X,Y) = \sum_{(i,j)\in I} a_{ij}X^iY^j \in \mathcal{O}_S[X,Y]$ with $a_{ij} \in \mathcal{O}_S^*$ for $(i,j) \in I$, be a polynomial which fulfils the condition that*

$$\begin{gathered} F \textbf{ is not divisible by } \text{any non-constant polynomial of the form} \\ X^mY^n - \alpha \quad \text{or} \quad X^m - \alpha Y^n, \text{where } m,n \in \mathbb{Z}_{\geq 0} \text{ and } \alpha \in \overline{M}. \end{gathered} \tag{5.2}$$

Assume that $H_M(a_{ij}) \leq H_0$ for all $(i,j) \in I$. Then for every $x, y \in \mathcal{O}_S^*$ with

$$F(x,y) = 0$$

we have

$$H_M(x), H_M(y) \leq 2 \deg F \left(n(F)^2 \cdot \left(|S| + g_{M/\Bbbk}\right) + 2H_0\right), .$$

where $n(F)$ denotes the number of non-zero terms of F.

Proof. Since the coefficients of the polynomial F are S-units, we may consider the equation

$$\sum_{(i,j)\in I} a_{ij}x^iy^j = 0 \qquad \text{in} \quad x, y \in \mathcal{O}_S^* \tag{5.3}$$

as an equation of type (5.1). Let us fix a solution x, y of the equation. If there are vanishing sub-sums in the left hand side of (5.3) then all these vanishing sub-sums form individually an equation of type (5.1), and we get a system of the form

$$\begin{cases} \sum_{(i,j)\in I_1} a_{ij}x^iy^j = 0 & \text{in} \quad x, y \in \mathcal{O}_S^* \\ \dots\dots\dots\dots\dots & \\ \sum_{(i,j)\in I_k} a_{ij}x^iy^j = 0 & \text{in} \quad x, y \in \mathcal{O}_S^*, \end{cases} \tag{5.4}$$

such that none of these equations has a proper vanishing subsum. Let $\mathcal{P} = (I_1, \dots, I_k)$. As explained in Section 3 condition (5.2) implies that $\operatorname{rank} \Lambda(F, \mathcal{P}) = 2$. By dividing each

equation of (5.4) by one of its terms we get

$$\begin{cases} 1+\sum\limits_{(i,j)\in I_1\setminus\{(i_1,j_1)\}} \frac{a_{ij}}{a_{i_1j_1}}x^{i-i_1}y^{j-j_1}=0 & \text{in} \quad x,y\in\mathcal{O}_S^* \\ \cdots\cdots\cdots\cdots\cdots & \\ 1+\sum\limits_{(i,j)\in I_k\setminus\{(i_k,j_k)\}} \frac{a_{ij}}{a_{i_kj_k}}x^{i-i_k}y^{j-j_k}=0 & \text{in} \quad x,y\in\mathcal{O}_S^*, \end{cases} \tag{5.5}$$

where we have $(i_l,j_l)\in I_l$ for $l=1,\dots,k$. Now we apply Proposition 5·2 to these equations. The number of terms of each equation is bounded above by $n(F)$, so we get

$$\begin{aligned} H_M\left(\frac{a_{ij}}{a_{i_lj_l}}x^{i-i_l}y^{j-j_l}\right) &\le H_M^*\left(\left(1,\frac{a_{ij}}{a_{i_lj_l}}x^{i-i_l}y^{j-j_l}\ :\ (i,j)\in I_l\setminus\{(i_l,j_l)\}\right)\right) \\ &\le H_M^*((a_{ij}x^iy^j\ :\ (i,j)\in I_l)) \le n(F)^2\cdot\left(|S|+g_{M/\Bbbk}\right) \end{aligned}$$

for every $l=1,\dots,k$ and every $(i,j)\in I_l\setminus\{(i_l,j_l)\}$. Thus we have

$$\begin{aligned} H_M\left(x^{i-i_l}y^{j-j_l}\right) &\le n(F)^2\cdot\left(|S|+g_{M/\Bbbk}\right)+H_M\left(\frac{a_{ij}}{a_{i_0j_0}}\right) \\ &\le n(F)^2\cdot\left(|S|+g_{M/\Bbbk}\right)+2H_0, \end{aligned}$$

which means that we have

$$H_M\left(x^ay^b\right)\le n(F)^2\cdot\left(|S|+g_{M/\Bbbk}\right)+2H_0,$$

for every $(a,b)=(u_1-u_2,v_1-v_2)$ with $(u_1,v_1),(u_2,v_2)\in I_l$ for some $l=1,\dots,k$. However $\Lambda(F,\mathcal{P}_{(x,y)}(F))$ is the $\mathbb{Z}$-module generated by these elements, and it has rank 2. Thus among these generators there exist $(a_1,b_1),(a_2,b_2)$ with $a_1b_2-a_2b_1\neq 0$. By putting $z_1:=x^{a_1}y^{b_1}$ and $z_2:=x^{a_2}y^{b_2}$ we have

$$x^{a_1b_2-a_2b_1}=z_1^{b_2}z_2^{-b_1}\qquad y^{a_1b_2-a_2b_1}=z_2^{a_1}z_1^{-a_2},$$

and we get the estimate

$$\begin{aligned} H_M(x) &\le \frac{1}{|a_1b_2-a_2b_1|}H_M(z_1^{b_2}z_2^{-b_1}) \le \frac{|b_2|H_M(z_1)+|b_1|H_M(z_2)}{|a_1b_2-a_2b_1|} \\ &\le 2\deg F\left(n(F)^2\cdot\left(|S|+g_{M/\Bbbk}\right)+2H_0\right), \end{aligned}$$

and similarly

$$H_M(y)\le 2\deg F\left(n(F)^2\cdot\left(|S|+g_{M/\Bbbk}\right)+2H_0\right).$$

This concludes the proof of the proposition. □

Recall that $A=\mathbb{Z}[z_1,\dots,z_r]$, K denotes the quotient field of A, $z_1,\dots,z_q$ form a transcendence basis for K, $A_0:=\mathbb{Z}[z_1,\dots,z_q]$, and $K_0:=\mathbb{Q}(z_1,\dots,z_q)$. Further, let w be a primitive element of the extension K/K_0, which is integral over A_0 and has the properties specified in (i) of Proposition 4·1, and let $f\in A_0$ be an element with the properties specified in (ii) of Proposition 4·1. As above, put $B:=A_0[w,f^{-1}]$.

Now let us fix $i \in \{1, \dots, q\}$ and for each such fixed i put

$$\Bbbk_i := \mathbb{Q}(z_1, \dots, z_{i-1}, z_{i+1}, \dots, z_q).$$

Clearly, we shall have $A_0 \subseteq \overline{\Bbbk_i}[z_i]$, where $\overline{\Bbbk_i}$ denotes the algebraic closure of $\Bbbk_i$. Let $w^{(1)} = w, \dots, w^{(D)}$ denote the conjugates of w over K_0, and put

$$M_i := \overline{\Bbbk_i}\left(z_i, w^{(1)}, \dots, w^{(D)}\right),$$
$$B_i := \overline{\Bbbk_i}\left[z_i, w^{(1)}, \dots, w^{(D)}, f^{-1}\right].$$

Then clearly M_i is the splitting field of the polynomial

$$\mathcal{F}(X) = X^D + \mathcal{F}_1 X^{D-1} + \cdots + \mathcal{F}_D \in A_0[X]$$

over $\overline{\Bbbk_i}[z_i]$, where $\mathcal{F}(X)$ is the minimal polynomial of w over K_0. Further, we have

$$B \subset B_i.$$

Let $\Delta_i := [M_i : \overline{\Bbbk}_i(z_i)]$ and denote by $g_{M_i/\overline{\Bbbk}_i}$ the genus of $M_i/\overline{\Bbbk}_i$, and by H_{M_i} the height taken with respect to $M_i/\overline{\Bbbk}_i$. In the following lemma we shall use the quantity

$$d_1 := \max(d_0, \deg f, \deg \mathcal{F}_1, \dots, \deg \mathcal{F}_D), \tag{5.6}$$

and later we will use that by Proposition 4·1 we have the estimate

$$d_1 \leq (2d)^{\exp O(r)} \cdot (2N)^{\log^* N \cdot \exp O(r)}. \tag{5.7}$$

To bound the $\overline{\deg}$ of an element of K we shall use the following:

LEMMA 5·4. *Let $\alpha \in K^*$ and let by $\alpha^{(1)}, \dots, \alpha^{(D)}$ be the conjugates of α corresponding to $w^{(1)}, \dots, w^{(D)}$, respectively. Then we have:*

$$\overline{\deg}\, \alpha \leq qDd_1 + \sum_{i=1}^{q} \Delta_i^{-1} \sum_{j=1}^{D} H_{M_i}(\alpha^{(j)}).$$

Proof. This is Lemma 4.4 in Evertse and Győry [**12**]. □

Conversely, we have the following:

LEMMA 5·5. *Let $\alpha \in K^*$ and $\alpha^{(1)}, \dots, \alpha^{(D)}$ be as in Lemma 5·4. Then we have*

$$\max_{i,j} H_{M_i}(\alpha^{(j)}) \leq \Delta_i \left(2D\overline{\deg}\, \alpha + (2d_0)^{\exp O(r)}\right). \tag{5.8}$$

Proof. This is Lemma 4.4 of [**3**]. □

Now we use Proposition 5·3 and Lemma 5·4 to prove statement (4.12) of Proposition 4·3:

Proof of (4.12). We denote by $w^{(1)} := w, \dots, w^{(D)}$ the conjugates of w over K_0, and for $\alpha \in K$ we denote by $\alpha^{(1)}, \dots, \alpha^{(D)}$ the conjugates of α corresponding to $w^{(1)}, \dots, w^{(D)}$. For $i = 1, \dots, n$ let $\Bbbk_i$, $\overline{\Bbbk}_i$, M_i, Δ_i have the same meaning as above. Let

$$S_i := \{v \in \mathcal{M}_{M_i} \ : \ v(z_i) < 0 \text{ or } v(f) > 0\}.$$

Since $w^{(j)} \in M_i$ and is integral over $\Bbbk_i[z_i]$, we have $w^{(j)} \in \mathcal{O}_{S_i}$ for $j = 1, \dots, D$. Since also $f^{-1} \in \mathcal{O}_{S_i}$ thus we have $\alpha^{(j)} \in \mathcal{O}_{S_i}$ for $\alpha \in B = A_0[f^{-1}, w]$, $j = 1, \dots, D$, $i = 1, \dots, q$.

Let $(x, y) \in \mathcal{C}'$. Then $x^{(j)}, y^{(j)}$ is a solution of the equation

$$F^{(j)}(x^{(j)}, y^{(j)}) = 0 \qquad \text{in} \quad x^{(j)}, y^{(j)} \in \mathcal{O}_{S_i}^*$$

for every $j = 1, \dots, D$, $i = 1, \dots, q$. Clearly the non-zero coefficients of $F^{(j)}(X, Y)$ are in $\mathcal{O}_{S_i}^*$, so by Proposition 5·3 we obtain that

$$\max(H_{M_i}(x^{(j)}), H_{M_i}(y^{(j)})) \le 2N \left(n(F)^2 \left(|S_i| + g_{M_i/\overline{\Bbbk}_i}\right) + 2H_0\right), \tag{5.9}$$

where $H_0 := \max\limits_{i,j,u,v} H_{M_i}(a_{uv}^{(j)})$. By $\deg \tilde{a}_{uv} \le d$ and Lemma 4·2 we have $\overline{\deg}\, a_{uv} \le (2d)^{\exp O(r)}$, which together with Lemma 5·5 gives

$$H_0 \le \Delta_i (2d)^{\exp O(r)}. \tag{5.10}$$

Now we have to estimate the genus of $M_i/\overline{\Bbbk}_i$ and the cardinality of S_i. First, using Lemma 5·1 for $\overline{\Bbbk}_i[z_i]$ and the polynomial $\mathcal{F}(X) = X^D + \mathcal{F}_1 X^{D-1} + \cdots + \mathcal{F}_D$, in view of the bounds in (i) of Proposition 4·1 we get

$$g_{M_i/\overline{\Bbbk}_i} \le \Delta_i D \max_{1 \le k \le D} \deg_{z_i} \mathcal{F}_k \le \Delta_i D (2d_0)^{\exp O(r)} \le \Delta_i (2d)^{\exp O(r)}. \tag{5.11}$$

To bound $|S_i|$ we mention that every valuation of $\overline{\Bbbk}_i(z_i)$ can be extended to at most $[M_i : \overline{\Bbbk}_i(z_i)] = \Delta_i$ valuations of M_i. Thus the number of valuations v of M_i with $v(z_i) < 0$ is bounded by Δ_i and similarly, the number of valuations v of M_i with $v(f) > 0$ is bounded above by $\Delta_i \deg_{z_i} f$. Hence altogether we have

$$\begin{aligned} |S_i| &\le \Delta_i + \Delta_i \deg_{z_i} f \le \Delta_i (1 + \deg f) \\ &\le \Delta_i (2d)^{\exp O(r)} \cdot (2N)^{\log^* N \cdot \exp O(r)}, \end{aligned} \tag{5.12}$$

where in the estimates we have used (ii) of Proposition 4·1.

Now turning again our attention to the estimate (5.9), and using (5.11) and (5.12) we get

$$\max(H_{M_i}(x^{(j)}), H_{M_i}(y^{(j)})) \le \Delta_i (2d)^{\exp O(r)} \cdot (2N)^{\log^* N \cdot \exp O(r)}. \tag{5.13}$$

Now it is the time to use Lemma 5·4, which together with (5.13), $D \le d^r$, $q \le r$ and

(5.7) proves that

$$\begin{aligned}\overline{\deg}\, x, \overline{\deg}\, y &\le qDd_1 + \sum_{i=1}^{q} \Delta_i^{-1} \sum_{j=1}^{D} H_{M_i}(x^{(j)}) \\ &\le (2d)^{\exp O(r)} \cdot (2N)^{\log^* N \cdot \exp O(r)}.\end{aligned}$$

This concludes the proof of (4.12) of Proposition 4·3. □

6. *Bounding the height in Proposition* 4·3

For a number field K the set of places of K is denoted by M_K. For every place $v \in M_K$ we choose an absolute value $|\cdot|_v$ in such a way that for $x \in \mathbb{Q}$ we have

$$|x|_v = |x|^{[K_v:\mathbb{R}]/[K:\mathbb{Q}]} \text{ if } v \text{ is infinite}, \qquad |x|_v = |x|_p^{[K_v:\mathbb{Q}_p]/[K:\mathbb{Q}]} \text{ if } v \text{ is finite},$$

where p is the prime below v.

For any finite set of places S of K, containing all infinite places, we define the ring of S-integers and group of S-units by

$$\begin{aligned}\mathcal{O}_S &= \{x \in K : |x|_v \le 1 \text{ for } v \in M_K \setminus S\}, \\ \mathcal{O}_S^* &= \{x \in K : |x|_v = 1 \text{ for } v \in M_K \setminus S\},\end{aligned}$$

respectively.

The (absolute logarithmic Weil) height of $x \in \overline{\mathbb{Q}}$ is defined by picking any number field K such that $x \in K$ and putting

$$h(x) := \sum_{v \in M_K} \max(0, \log |x|_v);$$

this does not depend on the choice of K. For a polynomial f we put $K := \mathbb{Q}(a_1, \dots, a_g)$ where $a_1, \dots, a_g$ are the non-zero coefficients of f, and we define the height of f by

$$h(f) := \sum_{v \in M_K} \log \max_{1 \le i \le g} |a_i|_v.$$

6·1. *The result for the number field case*

In this section we present a version of Theorem 2.1 of [**4**]. Let Γ be a finitely generated subgroup of $(\overline{\mathbb{Q}}^*)^2$. Let $\{\mathbf{w}_1, \dots, \mathbf{w}_r\}$ be a basis of Γ modulo Γ_{tors}. Put

$$h_w := \max\big(1, h(\mathbf{w}_1), \dots, h(\mathbf{w}_r)\big).$$

Denote by K the smallest number field such that $\Gamma \subset (K^*)^2$, and put $d := [K : \mathbb{Q}]$. Let S be the minimal finite set of places of K containing all the infinite places of K and having the property that $\Gamma \subset (\mathcal{O}_S^*)^2$ and denote by s the cardinality of S. Define

$$P(v) := 2 \text{ if } v \text{ is infinite}, \qquad P(v) := \#\mathcal{O}_K/\mathfrak{p}_v \text{ if } v \text{ is finite}, \tag{6.1}$$

where $\mathfrak{p}_v$ is the prime ideal of $\mathcal{O}_K$ corresponding to v, and put

$$\mathbf{P} := \max_{v \in S} P(v). \tag{6.2}$$

The discriminant of the field K is denoted by D_K.

Let $f(X,Y) \in \overline{\mathbb{Q}}[X,Y]$ be a polynomial which is not divisible by any non-constant polynomial of the shape $aX^mY^n - b$ or $aX^m - bY^n$ for some $a, b \in \overline{\mathbb{Q}}$, $m, n \in \mathbb{Z}_{\geq 0}$. We mention that in this case f is also not divisible by any polynomial which depends on exactly one of the variables X, Y, since then it would be divisible by a polynomial of the shape $aX - b$ or $aY - b$, respectively. Put $N := \deg f$ for the total degree of f. Let L be the field extension of K generated by the coefficients of f. Put

$$\begin{aligned}
&\delta := \deg_X f + \deg_Y f, \quad H := \max(1, h(f)),\\
&C_0 := \left(e^{13}\delta^7 d^3 r\right)^{r+3} s \cdot \frac{\mathbf{P}^{2\delta^2}}{\log \mathbf{P}} h_w^r \cdot \log^* \left(\max(\delta d s \mathbf{P}, \delta h_w)\right)..\\
&C_1 := \left(\delta \cdot d \cdot s \cdot \log \mathbf{P} \cdot D_K (\log^* D_K)^{d-1}\right)^{O(s^2)} \cdot \mathbf{P}^{2\delta^2}.
\end{aligned}$$

Let $\mathcal{C} \subset (\overline{\mathbb{Q}}^*)^2$ be the curve defined by $f(x,y) = 0$.

PROPOSITION 6·1. *Assume that f is absolutely irreducible. Then for every point $\mathbf{x} = (x,y) \in \mathcal{C} \cap \Gamma$ we have*

$$h(x) + h(y) \leq C_0 H.$$

Proof. This is just Theorem 2.1 of [**4**] □

PROPOSITION 6·2. *Assume that $\Gamma = \mathcal{O}_S^*$. Then for every point $\mathbf{x} = (x,y) \in \mathcal{C} \cap \Gamma$ we have*

$$h(x) + h(y) \leq C_1 (H + 2N).$$

Proof. This is a weaker version of Proposition 6·1. We shortly explain how this result is deduced from Proposition 6·1. If $f(x,y) = 0$ then there exists an absolutely irreducible factor $g(X,Y)$ of f, which then fulfils the conditions of Proposition 6·1, thus we may apply that for g. Further, since g divides f it is also well known that $h(g) \leq h(f) + 2N$ (see Proposition B.7.3 of [**19**]).

We also have to take care of the dependence on h_w and r, more precisely to estimate h_w and r in the case $\Gamma = \mathcal{O}_S^*$. If we take $\Gamma := (\mathcal{O}_S^*)^2$ then one can bound the number of generators r of Γ by $2s - 2$ and we may choose a system of fundamental S-units to get a set of generators for $(\mathcal{O}_S^*)^2$, so that the height of these elements in this fundamental system is bounded. More precisely by Lemma 2 of [**17**] we can choose the generators such that

$$h_0 \leq c_1 R_S,$$

where $c_1 := 29e\sqrt{s-2}d^{s-1}(\log^* d)\cdot((s-1)!)^2/(2^{s-2}d^{s-1})$, and R_S is the S-regulator of K. For the S-regulator by using Lemma 3 of [**11**] and Lemma 2.1 of [**2**] (for the original result see Louboutin [**21**]) we can derive the bound

$$R_S \leq |D_K|^{\frac{1}{2}}(\log^* |D_K|)^{d-1}\cdot(\log P)^s.$$

Combining these estimates the bound of our proposition follows by a simple computation. We mention that a much sharper bound could have been deduced, but this estimate is more than enough for our purpose. □

6·2. *Specializations*

In this section we shall use many specializations which map K to a number field, in order to be able to profit from our results from Section 6·1. The main feature of these specializations, called Győry-Kronecker specializations is that using sufficiently many of them, there will be at least one, which makes possible to extend effective results over number fields to similar results over finitely generated domains. Such specializations were first used by Győry [**15**] and [**16**], however, here we introduce and use the refined version of this specialization method due to Evertse and Győry [**12**].

First for every $\mathbf{u}\in\mathbb{Z}^q$ we may replace z_i by u_i for $i=1,\dots,q$. This defines a homomorphism from a subring of K_0 to $\mathbb{Q}$. More precisely, for fixed $\mathbf{u}\in\mathbb{Z}^q$ we consider the homomorphism $\varphi_{\mathbf{u}}: K_0\to\mathbb{Q}$ defined by

$$\varphi_{\mathbf{u}}(\alpha) := \alpha(\mathbf{u}) = \frac{g_1(\mathbf{u})}{g_2(\mathbf{u})}$$

for every $\alpha=\frac{g_1}{g_2}\in K_0$ with $g_1,g_2\in A_0$, and with the additional property $g_2(\mathbf{u})\neq 0$. Now we wish to extend this to a ring homomorphism from B to $\overline{\mathbb{Q}}$. Thus we will impose some restrictions on $\mathbf{u}$. Recall that $K=K_0(w)$, $B=A_0[f^{-1},w]$, and $\mathcal{F}$ is the minimal polynomial of w, and $f\in A_0$, both with properties specified in Proposition 4·1. Let $\Delta_{\mathcal{F}}$ denote the discriminant of $\mathcal{F}$ with the convention $\Delta_{\mathcal{F}}=1$ if $\mathcal{F}$ is a linear polynomial. Put

$$\mathcal{H} := \Delta_{\mathcal{F}}\cdot\mathcal{F}_D\cdot f,$$

observe that $\mathcal{H}\in A_0$ and assume that $\mathbf{u}$ is chosen such that $\mathcal{H}(\mathbf{u})\neq 0$. Put

$$\begin{cases} d_0^* = \max(\deg\mathcal{F}_1,\dots,\deg\mathcal{F}_D) \\ h_0^* = \max(h(\mathcal{F}_1),\dots,h(\mathcal{F}_D)) \end{cases} \qquad \begin{cases} d_1^* = \max(d_0^*,\deg f) \\ h_1^* = \max(h_0^*,h(f)). \end{cases}$$

By Proposition 4·1 we infer that

$$\begin{cases} d_0^* \le (2d_0)^{\exp O(r)} \le (2d)^{\exp O(r)} \\ h_0^* \le (2d_0)^{\exp O(r)}(h_0+1) \le (2d)^{\exp O(r)}(h+1) \\ d_1^* \le (2d)^{\exp O(r)} \cdot (2N)^{\log^* N \cdot \exp O(r)} \\ h_1^* \le (2d)^{\exp O(r)} \cdot (2N)^{\log^* N \cdot \exp O(r)} \cdot (h+1). \end{cases} \tag{6.3}$$

Thus we clearly have

$$\deg \mathcal{H} \le (2D-2) \cdot d_0^* + d_0^* + d_1^* \le (2d)^{\exp O(r)} \cdot (2N)^{\log^* N \cdot \exp O(r)}. \tag{6.4}$$

Now let $\mathbf{u} \in \mathbb{Z}^q$ be fixed such that $\mathcal{H}(\mathbf{u}) \neq 0$. Thus the polynomial

$$\mathcal{F}_{\mathbf{u}} := X^D + \mathcal{F}_1(\mathbf{u})X^{D-1} + \cdots + \mathcal{F}_D(\mathbf{u})$$

has non-zero discriminant, and since $\mathcal{F}_D(\mathbf{u}) \neq 0$ it has D distinct non-zero roots. Let us denote these numbers by $w^{(1)}(\mathbf{u}), \ldots, w^{(D)}(\mathbf{u})$.

To extend our map $\varphi_{\mathbf{u}}$ to B we use the representation (4.7) of elements $\alpha \in B$. Namely, for each $j = 1, \ldots, D$ we may define the function $\varphi_{\mathbf{u},j}$ such that for $\alpha \in B$ written as

$$\alpha = \sum_{i=1}^{D-1} (P_i/Q)\, w^i, \qquad \text{where } P_0, \ldots, P_{D-1}, Q \in A_0,\ \gcd(P_0, \ldots, P_{D-1}, Q) = 1, \tag{6.5}$$

we define

$$\varphi_{\mathbf{u},j}(\alpha) := \sum_{i=1}^{D-1} (P_i(\mathbf{u})/Q(\mathbf{u})) \left(w^{(j)}(\mathbf{u})\right)^i. \tag{6.6}$$

This is well-defined, since for $\alpha \in B$ the polynomial Q must divide a power of f, hence $Q(\mathbf{u}) \neq 0$. By this we described exactly D ways to extend $\varphi_{\mathbf{u}}$ from K_0 to B. Clearly, the map $\varphi_{\mathbf{u},j}$ defined above is a ring homomorphism from B to $\overline{\mathbb{Q}}$, thus any unit of B is mapped to a non-zero element of $\overline{\mathbb{Q}}$ by any of the above defined specializations. Put

$$K_{\mathbf{u},j} := \mathbb{Q}(w^{(j)}(\mathbf{u})) \qquad \text{for} \qquad j = 1, \ldots, D, \tag{6.7}$$

and denote by $\Delta_{K_{\mathbf{u},j}}$ the discriminant of the algebraic number field $K_{\mathbf{u},j}$.

In the sequel we recall three lemmas of Evertse and Győry [**12**], which are necessary for our proof.

LEMMA 6·3. *Let $\mathbf{u} \in \mathbb{Z}^q$ with $\mathcal{H}(\mathbf{u}) \neq 0$. Then for $j = 1, \ldots, D$ we have $[K_{\mathbf{u},j} : \mathbb{Q}] \le D$ and*

$$|\Delta_{K_{\mathbf{u},j}}| \le D^{2D-1} \left((d_0^*)^q e^{h_0^*} \max(1, |\mathbf{u}|^{d_0^*})\right)^{2D-2}.$$

Proof. This is Lemma 5.5 in Evertse and Győry [**12**]. □

The following lemma bounds the height of $\alpha^{(j)}(\mathbf{u}) := \varphi_{\mathbf{u},j}(\alpha)$ for $\mathbf{u} \in \mathbb{Z}^q$ in terms of the size of $\alpha \in B$ and some parameters of B.

LEMMA 6·4. *Let $\mathbf{u} \in \mathbb{Z}^q$ with $\mathcal{H}(\mathbf{u}) \neq 0$, and let $\alpha \in B$. Then for $j = 1, \dots, D$,*

$$h(\alpha^{(j)}(\mathbf{u})) \leq D^2 + q(D \log d_0^* + \log \overline{\deg}\, \alpha) + \\ + Dh_0^* + \overline{h}(\alpha) + (Dd_0^* + \overline{\deg}\, \alpha) \log \max(1, |\mathbf{u}|).$$

Proof. This is Lemma 5.6 in Evertse and Győry [**12**]. □

The following lemma shows that if we take a large enough number of specializations, then there is at least one specialization among them (say corresponding to $\mathbf{u} \in \mathbb{Z}^q$), such that $\overline{h}(\alpha)$ for $\alpha \in B$ can be bounded by the heights of the images of α by the specializations $\varphi_{\mathbf{u},j}$ for $j = 1, \dots, D$.

LEMMA 6·5. *Let $\alpha \in B$, $\alpha \neq 0$, and let N_0 be an integer with*

$$N_0 \geq \max(\overline{\deg}\, \alpha, 2Dd_0^* + 2(q+1)(d_1^* + 1)). \tag{6.8}$$

Then the set

$$\mathcal{S} := \{\mathbf{u} \in \mathbb{Z}^q \ : \ |\mathbf{u}| \leq N_0, \mathcal{H}(\mathbf{u}) \neq 0\}$$

is non-empty, and

$$\overline{h}(\alpha) \leq 5N_0^4(h_1^* + 1)^2 + 2D(h_1^* + 1)H, \tag{6.9}$$

where $H := \max\{h(\alpha^{(j)}(\mathbf{u})) \ : \ \mathbf{u} \in \mathcal{S}, \ j = 1, \dots, D\}$.

Proof. This is Lemma 5.7 in Evertse and Győry [**12**]. □

6·3. *Conclusion of the proof of Proposition* 4·3

In this subsection we combine the specialization method and the result for the number field case presented in the first two subsections of this section, in order to prove (4.13).

*Proof of (*4.13*) of Proposition* 4·3 Since in the case $q = 0$ we are in the number field case our Theorem 2.1 of [**4**] will give a much better bound than stated in Proposition 4·3. So we may consider the case $q > 0$. Let $\mathcal{P}$ be a fixed partition of I and $(x, y) \in \mathcal{C}'$ be a fixed solution associated with $\mathcal{P}$. Choose $\mathbf{u} \in \mathbb{Z}^q$ with $\mathcal{H}(\mathbf{u}) \neq 0$ and $k \in \{1, \dots, D\}$, and consider the corresponding specialization $\varphi_{\mathbf{u},k}$ defined in (6.6), where later we shall specify some further requirements on $\mathbf{u}$ and k when we shall apply Lemma 6·5. Then we have the notation

$$\begin{aligned} &\varphi_{\mathbf{u},k}(x) = x^{(k)}(\mathbf{u}), \qquad \varphi_{\mathbf{u},k}(y) = y^{(k)}(\mathbf{u}), \\ &\varphi_{\mathbf{u},k}(a_{ij}) = a_{ij}^{(k)}(\mathbf{u}) \qquad \text{for} \quad (i,j) \in I. \end{aligned} \tag{6.10}$$

Put $F_{\mathbf{u},k}(X,Y) := \sum_{(i,j)\in I} a_{ij}^{(k)}(\mathbf{u})X^iY^j$, let $K_{\mathbf{u},k}$ be the field defined in (6.7), $S_{\mathbf{u},k}$ be the set of places of $K_{\mathbf{u},k}$ containing all infinite places and those finite places which lie above prime ideals dividing $f(\mathbf{u})$. Since we clearly have

$$\varphi_{\mathbf{u},k}(B) \subseteq \mathcal{O}_{S_{\mathbf{u},k}},$$

thus from $(x,y) \in \mathcal{C}'$ we get

$$F_{\mathbf{u},k}\left(x^{(k)}(\mathbf{u}), y^{(k)}(\mathbf{u})\right) = 0 \qquad \text{in} \quad x^{(k)}(\mathbf{u}), y^{(k)}(\mathbf{u}) \in \mathcal{O}^*_{S_{\mathbf{u},k}}. \tag{6.11}$$

Now we shall apply Lemma 6·5. Since in the previous section we have proved (4.12), i.e.

$$\overline{\deg}\, x, \overline{\deg}\, y \le (2d)^{\exp O(r)} \cdot (2N)^{\log^* N \cdot \exp O(r)},$$

now in view of (6.3) we may apply Lemma 6·5 with some

$$N_0 \le (2d)^{\exp O(r)} \cdot (2N)^{\log^* N \cdot \exp O(r)}$$

to infer that the set

$$\mathcal{S} := \{\mathbf{u} \in \mathbb{Z}^q \ : \ |\mathbf{u}| \le N_0, \ \mathcal{H}(\mathbf{u}) \neq 0\}$$

is non-empty. Taking also (6.3) in account we have

$$\begin{aligned} \overline{h}(x) &\le (2d)^{\exp O(r)} \cdot (2N)^{\log^* N \cdot \exp O(r)} (h+1)^2 H_x, \\ \overline{h}(y) &\le (2d)^{\exp O(r)} \cdot (2N)^{\log^* N \cdot \exp O(r)} (h+1)^2 H_y, \end{aligned} \tag{6.12}$$

where $H_x := \max\{h(x^{(k)}(\mathbf{u})) \ : \ \mathbf{u} \in \mathcal{S}, \ k = 1, \dots, D\}$ and $H_y := \max\{h(y^{(k)}(\mathbf{u})) \ : \ \mathbf{u} \in \mathcal{S}, \ k = 1, \dots, D\}$.

To finish the proof, the last step is to estimate H_x and H_y using Proposition 6·2 for equation (6.11). We fix any $\mathbf{u} \in \mathcal{S}$ and $k = 1, \dots, D$. By Lemma 6·3 and in view of (6.3) we get that

$$\begin{aligned} |\Delta_{K_{\mathbf{u},k}}| &\le D^{2D-1} \left((d_0^*)^q e^{h_0^*} \max(1, |\mathbf{u}|^{d_0^*})\right)^{2D-2} \\ &\le \exp\left\{(2d)^{\exp O(r)} \cdot (h+1) \cdot (\log^* N)^2\right\}, \end{aligned} \tag{6.13}$$

and $[K_{\mathbf{u},k} : \mathbb{Q}] \le D$.

To estimate $h(F_{\mathbf{u},k})$ we bound the height of its coefficients, i.e. $h(a_{ij}^{(k)}(\mathbf{u}))$ for $(i,j) \in I$. For this we use first Lemma 4·2, which in view of $\deg \tilde{a}_{ij} < d$ and $h(\tilde{a}_{ij}) < h$ gives

$$\overline{\deg}\, a_{ij} \le (2d)^{\exp O(r)} \qquad \overline{h}(a_{ij}) \le (2d)^{\exp O(r)}(h+1).$$

This together with Lemma 6·4 gives for every $(i,j) \in I$ the estimate

$$h\left(a_{ij}^{(k)}(\mathbf{u})\right) \le (\log^* N)^2 (2d)^{\exp O(r)}(h+1),$$

which in turn proves

$$h(F_{\mathbf{u},k}) \le n(F) \cdot \max h\left(a_{ij}^{(k)}(\mathbf{u})\right) \le N^2 (\log^* N)^2 (2d)^{\exp O(r)}(h+1). \tag{6.14}$$

We also have to estimate the cardinality of $S_{K_{\mathbf{u},k}}$. For this, we first bound the absolute value of $f(\mathbf{u})$ by the elementary computation

$$\begin{aligned}|f(\mathbf{u})| &\le (\deg f)^q \cdot e^{h(f)} \cdot (\max(1,|\mathbf{u}|))^{\deg f} \le (d_1^*)^q \cdot e^{h_1^*} \cdot (\max(1,|\mathbf{u}|))^{d_1^*} \\ &\le \exp\left\{(2d)^{\exp O(r)} \cdot (2N)^{\log^* N \cdot \exp O(r)} \cdot (h+1)\right\}.\end{aligned}$$

Clearly we have $s := |S_{K_{\mathbf{u},j}}| \le D(1+\omega(f(\mathbf{u})))$, where $\omega(f(\mathbf{u}))$ denotes the number of distinct prime factors of $f(\mathbf{u})$. Thus we get

$$\begin{aligned}s &\le O\left(d^r \log^* |f(\mathbf{u})| / \log^* \log^* |f(\mathbf{u})|\right) \\ &\le (2d)^{\exp O(r)} \cdot (2N)^{\log^* N \cdot \exp O(r)} \cdot (h+1).\end{aligned} \tag{6.15}$$

Further, for the maximum of the norm of the prime ideals belonging to $S_{K_{\mathbf{u},k}}$ we have the estimate

$$\mathbf{P} \le |f(\mathbf{u})|^D \le \exp\left\{(2d)^{\exp O(r)} \cdot (2N)^{\log^* N \cdot \exp O(r)} \cdot (h+1)\right\}. \tag{6.16}$$

Now we shall show that for the polynomial $F_{\mathbf{u},l}$ we have

$$\begin{aligned}&F_{\mathbf{u},l} \textbf{ is not divisible by} \text{ any non-constant polynomial of the form} \\ &\quad X^m Y^n - \alpha \quad \text{or} \quad X^m - \alpha Y^n, \text{where } m,n \in \mathbb{Z}_{\ge 0} \text{ and } \alpha \in \overline{K}_{\mathbf{u},l}.\end{aligned} \tag{6.17}$$

The coefficients a_{ij} of F are units in B, thus all these coefficients are mapped to non-zero elements $a_{ij}^{(l)}(\mathbf{u})$ by the specialization $\varphi_{\mathbf{u},l}$, so the partitions of the polynomial F are just the same as the partitions of the polynomial $F_{\mathbf{u},l}$. If $\operatorname{rank}\Lambda(F,\mathcal{P}) = 2$ then we also have $\operatorname{rank}\Lambda(F_{\mathbf{u},l},\mathcal{P}) = 2$. Further, if $\operatorname{rank}\Lambda(F,\mathcal{P}) = 1$ then we also have $\operatorname{rank}\Lambda(F_{\mathbf{u},l},\mathcal{P}) = 1$ and by Proposition 3·1 the corresponding system of polynomials $g_1,\dots,g_k$ (see Section 3) has the property $\gcd(g_1,\dots,g_k) = 1$ in $K[X]$. Thus there exist polynomials $u_1,\dots,u_k \in A[X]$ and a constant $R \in A$ with

$$u_1 g_1 + \cdots + u_k g_k = R, \tag{6.18}$$

and by Proposition 3·3 we see that R can be chosen such that it has a representative $\tilde{R}$ with

$$\deg \tilde{R} \le d(4N)^{\log_2^* N}, \qquad h(\tilde{R}) \le (4N)^{\log_2^* N + 2}(d+1)rh.$$

This R fulfils all assumptions made for R in Proposition 4·1, so assume that f and B have been chosen in Proposition 4·1 such that $R \in B^*$. Now we apply the specialization $\varphi_{\mathbf{u},l}$ to (6.18) to infer that

$$(u_1)_{\mathbf{u},l}(g_1)_{\mathbf{u},l} + \cdots + (u_k)_{\mathbf{u},l}(g_k)_{\mathbf{u},l} = R_{\mathbf{u}}^{(l)}.$$

Since $R \in B^*$ we have $R_{\mathbf{u}}^{(l)} \ne 0$ hence $\gcd((g_1)_{\mathbf{u},l},\dots,(g_k)_{\mathbf{u},l}) = 1$ in $K_{\mathbf{u},l}$. By Proposition 3·1 this proves (6.17). So the polynomial $F_{\mathbf{u},l}$ cannot have any non-constant factor of the shape $aX^mY^n - b$ or $aX^m - bY^n$ for some $a,b \in \overline{\mathbb{Q}}$, $m,n \in \mathbb{Z}_{\ge 0}$. Thus the solution set of equation (6.11) fulfills the conditions of Proposition 6·2, so combining this by statements

(6.14), (6.15), (6.16), (6.13) and $[K_{\mathbf{u},k} : \mathbb{Q}] \leq D$ we get the estimate

$$h(x^{(k)}(\mathbf{u})), h(y^{(k)}(\mathbf{u})) \leq \exp\left\{(2d)^{\exp O(r)}(2N)^{\log^* N \cdot \exp O(r)} \cdot (h+1)^3\right\},$$

for every $\mathbf{u} \in \mathcal{S}$ and $k = 1, \ldots, D$, which provides the same upper bound for H_x and H_y. Now combining this latter estimate with (6.12) we get the desired bound (4.13). This concludes the proof of Proposition 4·3. □

Acknowledgements. The author would like to thank Jan-Hendrik Evertse for his help and useful comments, and the anonymous referee for her/his substantial work.

REFERENCES

[**1**] M. Aschenbrenner, Ideal membership in polynomial rings over the integers, *J. Amer. Math. Soc.*, **17** (2004), 407–442.

[**2**] A. Bérczes, J.-H. Evertse and K. Győry, Effective results for hyper- and superelliptic equations over number fields, *Publ. Math. Debrecen*, **82** (2013), 727–756.

[**3**] A. Bérczes, J.-H. Evertse and K. Győry, Effective results for Diophantine equations over finitely generated domains, *Acta Arith.*, **163** (2014), 71–100.

[**4**] A. Bérczes, J.-H. Evertse, K. Győry and C. Pontreau, Effective results for points on certain subvarieties of tori, *Math. Proc. Cambridge Phil. Soc.*, **147** (2009), 69–94.

[**5**] E. Bombieri and W. Gubler, *Heights in Diophantine geometry*, Cambridge University Press, Cambridge, 2006.

[**6**] B. Brindza, On the equation $f(x) = y^m$ over finitely generated domains, *Acta Math. Hungar.*, **53** (1989), 377–383.

[**7**] B. Brindza, The Catalan equation over finitely generated integral domains, *Publ. Math. Debrecen*, **42** (1993), 193–198.

[**8**] B. Brindza and Á. Pintér, On equal values of binary forms over finitely generated fields, *Publ. Math. Debrecen*, **46** (1995), 339–347.

[**9**] B. Brindza, A. Pintér and J. Végső, The Schinzel-Tijdeman equation over function fields, *C.R. Math. Rep. Acad. Sci. Canada*, **16** (1994), 53–57.

[**10**] W. D. Brownawell and D. W. Masser, Vanishing sums in function fields, *Math. Proc. Cambridge Philos. Soc.*, **100** (1986), 427–434.

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

[**12**] J.-H. Evertse and K. Győry, Effective results for unit equations over finitely generated integral domains, *Math. Proc. Camb. Phil. Soc.*, **154** (2013), 351–380.

[**13**] K. Győry, Sur les polynômes à coefficients entiers et de dicriminant donné II, *Publ. Math. Debrecen*, **21** (1974), 125–144.

[**14**] K. Győry, On the number of solutions of linear equations in units of an algebraic number field, *Comment. Math. Helv.*, **54** (1979), 583–600.

[**15**] K. Győry, Bounds for the solutions of norm form, discriminant form and index form equations in finitely generated integral domains, *Acta Math. Hungar.*, **42** (1983), 45–80.

[**16**] 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.

[**17**] K. Győry and K. Yu, Bounds for the solutions of S-unit equations and decomposable form equations, *Acta Arith.*, **123** (2006), 9–41.

[**18**] G. Hermann, Die Frage der endlich vielen Schritte in der Theorie der Polynomideale, *Math. Ann.*, **95** (1926), 736–788.

[**19**] M. HINDRY and J. H. SILVERMAN, *Diophantine geometry*, vol. 201 of *Graduate Texts in Mathematics*, Springer-Verlag, New York, 2000.
[**20**] S. LANG, Integral points on curves, *Inst. Hautes Études Sci. Publ. Math.*, (1960), 27–43.
[**21**] S. LOUBOUTIN, Explicit bounds for residues of Dedekind zeta functions, values of L-functions at $s = 1$, and relative class numbers, *J. Number Theorey*, **85** (2000), 263–282.
[**22**] K. MAHLER, Zur Approximation algebraischer Zahlen. I, *Math. Ann.*, **107** (1933), 691–730.
[**23**] C. J. PARRY, The $\mathfrak{p}$-adic generalisation of the Thue-Siegel theorem, *Acta Math.*, **83** (1950), 1–100.
[**24**] C. SIEGEL, Approximation algebraischer Zahlen, *Math. Z.*, **10** (1921), 173–213.