Attila BÉRCZES

**Effective results for division points on curves in** $\mathbb{G}_m^2$


<http://jtnb.cedram.org/item?id=JTNB_2015__27_2_405_0>
Effective results for division points
on curves in $\mathbb{G}_m^2$

par Attila BÉRCZES

To the memory of Professor Pierre Liardet

Abstract. Let $A := \mathbb{Z}[z_1, \ldots, z_r] \supset \mathbb{Z}$ be a finitely generated integral domain over $\mathbb{Z}$, let $K$ denote its quotient field, and $K^*$ the multiplicative group of non-zero elements of $K$. Let $\Gamma$ be a finitely generated subgroup of $K^*$, and let $\overline{\Gamma}$ denote the division group of $\Gamma$. Let $F(X,Y) \in A[X,Y]$ be a polynomial. In 1974, P. Liardet proved that under some natural conditions on $F$ the equation

$$F(x, y) = 0 \text{ with } x, y \in \overline{\Gamma}$$

has only finitely many solutions. The proof of Liardet was ineffective. In 2009, an effective version of Liardet’s Theorem has been proved by Bérczes, Evertse, Győry and Pontreau in the case when $\Gamma \subset \overline{\mathbb{Q}}$. In the present paper an effective version of Liardet’s Theorem is proved in the general case.
1. Introduction

Let $A := \mathbb{Z}[z_1, \ldots, z_r] \supset \mathbb{Z}$ be a finitely generated integral domain over $\mathbb{Z}$. In the rest of the paper under finitely generated domain we mean an integral domain $\mathbb{Z}[z_1, \ldots, z_r] \supset \mathbb{Z}$. Finiteness results for several kinds of Diophantine equations over $A$ date back to the middle of the last century. In his book [16] and paper [15] S. Lang generalized several earlier results on Diophantine equations over the integers to results over $A$, including results concerning unit equations, Thue-equations and integral points on curves. However, all his results were ineffective. The first effective results for Diophantine equations over finitely generated domains were published in the 1980’s, when Győry [13], [14] developed his new effective specialization method. This enabled him to prove effective results over finitely generated domains of a special type. He proved such results for unit equations, norm form equations, index form equations, discriminant form equations [13] and for polynomials and integral elements of given discriminant [14]. Later Brindza proved such results for superelliptic equations [8] and the generalized Catalan equation [9], Brindza and Pintér obtained such results for equal values of binary forms [10], and Brindza, Pintér and Végső [11] for the Schinzel-Tijdeman equation.

In 2011 Evertse and Győry [12] refined the method of Győry such that they were able to prove effective results for unit equations $ax + by = 1$ in $x, y \in A^*$ over arbitrary finitely generated domains $A$ of characteristic 0. Later Bérczes, Evertse and Győry [4] obtained effective results for Thue equations, hyper- and superelliptic equations and for the Schinzel-Tijdeman equation over arbitrary finitely generated domains. Lastly Bérczes in [2] proved an effective result for equations $F(x, y) = 0$ in $x, y \in A^*$ for arbitrary finitely generated domains $A$, thus giving an effective version of the below result of Lang [15].

Let $K$ denote the quotient field of the domain $A$, and denote by $K^*$ the multiplicative group of non-zero elements of $K$. Denote by $\overline{K}$ the algebraic closure of $K$ and by $\overline{K}^*$ its unit group. Let $\Gamma$ be a finitely generated subgroup of $K^*$. Let $F(X,Y) \in A[X,Y]$ be a polynomial. In 1960 Lang [15] proved that the equation

(1.1) \[ F(x, y) = 0 \quad \text{in } x, y \in \Gamma \]

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

(1.2) \[ X^m Y^n - \alpha \quad \text{or} \quad X^m - \alpha Y^n \]

where $m, n$ are non-negative integers, not both zero, and any $\alpha \in \Gamma$. Lang’s proof of this result is ineffective. The first effective versions of this result of Lang have been proved by Bombieri and Gubler [7, p. 147, Theorem 5.4.5] (see Bérczes, Evertse Győry and Pontreau [5] for an explicit version) for
the number field case and by Bérczes [2] in its full generality, over finitely generated domains. We mention that the effective results are proved under a slightly stronger condition than (1.2), namely in (1.2) $\alpha \in K$ is assumed instead of $\alpha \in \Gamma$.

Denote by $\Gamma$ the division group of $\Gamma$, i.e. the group defined by

$$\Gamma := \left\{ x \in K^* \mid \exists m \in \mathbb{N}, x^m \in \Gamma \right\}.$$

Lang also conjectured ([17], [18], see also [19]) that the above equation has finitely many solutions in $x, y \in \Gamma$ under the same condition (1.2). Liardet [20], [21] proved this conjecture of Lang. However, this famous result of Liardet is also ineffective.

An effective version of Liardet’s Theorem in the number field case is due to Bérczes, Evertse, Győry and Pontreau [5], however, in the general case no effective result had been proved.

In the present paper we make effective the above-mentioned finiteness theorem of Liardet in the general case. Our result is not only effective, but also quantitative in the sense that an upper bound for the sizes of the solutions $x, y \in \Gamma$ is provided. The presented result is a common generalization of the results of Bombieri and Gubler [7, p. 147, Theorem 5.4.5], Bérczes, Evertse, Győry and Pontreau [5] and that of Bérczes [2]. Further, our result is also a generalization of the result of Bérczes, Evertse and Győry [3] and of Evertse and Győry [12] on unit equations, since taking $F(X,Y) = aX + bY - 1$ in the main result of the present paper we just get an effective finiteness result for generalized unit equations in two unknowns over the division group of an arbitrary finitely generated group. The main tool of the proof is an effective specialization method introduced by Győry in the 1980’s (see [13], [14]), and improved by Evertse and Győry [12] in 2011. The main difficulty of the proof is that on one hand we have to bound also the degrees over $K$ of the solutions from $\Gamma$, on the other hand we do not have any convenient representation for the elements of $\Gamma$. We also mention that this is the first effective result for Diophantine equations over the division group of an arbitrary finitely generated group.

The plan of the paper is as follows. Section 2 contains our main result, while in Section 3 we reduce our main theorem to two propositions. The rest of the paper is devoted to the proof of these propositions. Section 4 contains auxiliary results, while Section 5 is devoted to a general description of the specialization method of Evertse and Győry. The last two Sections contain the proofs of our two propositions stated in Section 3.

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
\[
\log^* a := \max(1, \log a) \text{ for } a > 0, \text{ and } \log^* 0 := 1.
\]

2. Results

Let $A := \mathbb{Z}[z_1, \ldots, z_r]$ be a finitely generated domain over $\mathbb{Z}$, and let $K$ denote its quotient field. Then
\[
A \cong \mathbb{Z}[X_1, \ldots, X_r]/\mathcal{I},
\]
where $\mathcal{I}$ denotes the ideal of the polynomial ring $R = \mathbb{Z}[X_1, \ldots, X_r]$ which consists of those polynomials $f \in R$ for which $f(z_1, \ldots, z_r) = 0$. This ideal is finitely generated, i.e. we can write $\mathcal{I} = (f_1, \ldots, f_t)$ with suitable polynomials $f_1, \ldots, f_t \in R$. We may view such a set of generators for $\mathcal{I}$ as a representation for the finitely generated domain $A$. Recall that $A$ is a domain of characteristic 0 if and only if $\mathcal{I}$ is a prime ideal, and $\mathcal{I}\cap\mathbb{Z} = \emptyset$, and this property can be checked effectively, given a set of generators for $\mathcal{I}$.

We say that a polynomial $f \in R$ represents $\alpha \in A$ if $\alpha = f(z_1, \ldots, z_r)$. Such a polynomial $f$ is called a representation for $\alpha$. Similarly, we say that a pair of polynomials $(f, g) \in R^2$ represents $\beta \in K$ if $g \notin \mathcal{I}$ (i.e. $g(z_1, \ldots, z_r) \neq 0$) and $\beta = \frac{f(z_1, \ldots, z_r)}{g(z_1, \ldots, z_r)}$. Such a pair $(f, g)$ is also called a representation pair for $\beta$.

For a non-zero polynomial $f \in R$ we 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. It is convenient for effective computations to measure an element of $A$ by the degree and height of a representative of it, since there are only finitely many polynomials in $R$ with both degree and height below a given bound.

Let $\gamma_1, \ldots, \gamma_s \in K^*$ be arbitrary non-zero elements of $K$ given by corresponding representation pairs $(g_1, h_1), \ldots, (g_s, h_s)$. Define the finitely generated group
\[
\Gamma := \left\{ \gamma_1^{l_1} \cdots \gamma_s^{l_s} \mid l_1, \ldots, l_s \in \mathbb{Z} \right\},
\]
and its division group
\[
\overline{\Gamma} := \left\{ \delta \in K \mid \exists m \in \mathbb{Z}_{>0} : \delta^m \in \Gamma \right\}.
\]

Let $I \subset \mathbb{Z}_{\geq 0}^2$ be a non-empty set, and let $F(X, Y) = \sum_{(i,j) \in I} a_{ij} X^i Y^j \in A[X,Y]$ be a polynomial which fulfils the following condition:

\[
F \text{ is not divisible by any non-constant polynomial of the form } X^m Y^n - \alpha \text{ or } X^m - \alpha Y^n, \text{ where } m, n \in \mathbb{Z}_{\geq 0} \text{ and } \alpha \in K^*.
\]

We mention that this condition is effectively decidable, as is explained in Section 3.1 of [2]. Let $N := \deg F$ denote the total degree of $F$, and assume
that $F$ is given by specifying a representative $\tilde{a}_{ij}$ of its coefficient $a_{ij}$ for each $(i,j) \in I$.

Further, we assume that

\begin{equation}
\deg f_1,\ldots, \deg f_t, \deg g_1,\ldots, \deg g_s, \deg h_1,\ldots, \deg h_s, \deg \tilde{a}_{ij} \leq d \\
h(f_1),\ldots, h(f_t), h(g_1),\ldots, h(g_s), h(h_1),\ldots, h(h_s), h(\tilde{a}_{ij}) \leq h,
\end{equation}

where $(i,j) \in I$ and $d, h$ are real numbers with $d > 1$ and $h > 1$.

**Theorem 2.1.** Let $A$ be a finitely generated domain as above, $\overline{\Gamma}$ the above-defined division group and $F(X,Y) \in A[X,Y]$ a polynomial which fulfils the condition (2.4). Define the set

\begin{equation}
C := \{(x,y) \in (\overline{\Gamma})^2 | F(x,y) = 0\}.
\end{equation}

(i) Then there exists a positive integer $m$ with

\begin{equation}
m \leq \exp \left\{ N^6(2d)^{\exp\left\{C_1(r+s)\right\}}(h+1)^4s \right\}
\end{equation}

with $C_1$ an effectively computable absolute constant such that

$x^m \in \Gamma$ and $y^m \in \Gamma$, for every $(x,y) \in C$.

(ii) More precisely, there exists an effectively computable absolute constant $C_2$, such that for all $(x,y) \in C$ there are integers $t_{1,x},\ldots, t_{s,x}, t_{1,y},\ldots, t_{s,y}$ with

\begin{equation}
t_{i,x}, t_{i,y} \leq \exp \left\{ \exp \left\{ N^{12}(2d)^{\exp\left\{C_2(r+s)\right\}}(h+1)^8s \right\} \right\}
\end{equation}

for $i = 1,\ldots, s$, such that

\begin{equation}
x^m = \gamma_1^{t_{1,x}} \cdots \gamma_s^{t_{s,x}}, \quad y^m = \gamma_1^{t_{1,y}} \cdots \gamma_s^{t_{s,y}}.
\end{equation}

3. A reduction

In this section we reduce Theorem 2.1 to two propositions and using a result of Everste and Györy [12] we show how Theorem 2.1 can be deduced from these propositions.

**Proposition 3.1.** Let $A$ be a finitely generated domain as above, $\overline{\Gamma}$ the above-defined division group and $F(X,Y) \in A[X,Y]$ a polynomial which fulfils the condition (2.4). Then there exists a suitably large effectively computable constant $C_3$ such that for every $(x,y) \in C$ there exists an exponent

$m_0 < N^6(2d)^{\exp\left\{C_3(r+s)\right\}}(h+1)^4s$

for which we have

$x^{m_0} \in \Gamma, \quad y^{m_0} \in \Gamma.$
We remark that in this proposition the value of the exponent $m_0$, although bounded by (3.1), it may depend on the choice of the pair $(x,y) \in C$. In contrast, in the statement (i) of Theorem 2.1 the exponent $m$ is uniform, i.e. it does not depend on the pair $(x,y) \in C$.

Now we deduce statement (i) of Theorem 2.1 from the above Proposition 3.1.

Proof of Theorem 2.1 (i). Let $C_3$ be the constant specified in Proposition 3.1 and define

$$M_0 := \left[ N^6 (2d)^{\exp \{ C_3 (r+s) \} } (h+1)^{4s} \right].$$

Put

$$m := \text{lcm}(1, \ldots, M_0).$$

Then by Proposition 3.1 we clearly have

$$x^m, y^m \in \Gamma$$

for every $(x,y) \in C$.

Using the estimate

$$\pi(M) \leq \frac{4}{3} \frac{M}{\log M}$$

of Rosser and Schönfeld [22] for the number $\pi(M)$ of primes up to $M$ we get

$$\text{lcm}(1, \ldots, M) \leq \prod_{p \leq M} p^{\log M / \log p} \leq \prod_{p \leq M} p^{\log M / \log p}$$

$$= \prod_{p \leq M} M^{\exp \{ C_3 (r+s) \} } \leq e^{\frac{4}{3} M}.$$ 

Thus we have the estimate

$$m \leq \exp \left\{ N^6 (2d)^{\exp \{ C_3 (r+s) \} } (h+1)^{4s} \right\},$$

which concludes the proof of (i) of Theorem 2.1. \qed

Next let us fix $m$ to be the integer specified in (i) of Theorem 2.1 and consider the set

$$C_1 := \left\{ (x_0, y_0) \in \Gamma^2 \mid \exists x,y \in \Gamma : x^m = x_0, y^m = y_0, F(x,y) = 0 \right\}.$$

Proposition 3.2. Let $(x_0, y_0) \in C_1$. Then there exist representatives $\tilde{x}_0$ and $\tilde{y}_0$ for $x_0$ and $y_0$, respectively, with the property

$$\deg \tilde{x}_0, \deg \tilde{y}_0 \leq \exp \left\{ N^6 (2d)^{\exp \{ C_3 (r+s) \} } (h+1)^{4s} \right\}$$

$$h(\tilde{x}_0), h(\tilde{y}_0) \leq \exp \left\{ \exp \left\{ N^6 (2d)^{\exp \{ C_3 (r+s) \} } (h+1)^{4s} \right\} \right\}.$$ 

To deduce (ii) of Theorem 2.1 from the above proposition we need the following result of Evertse and Győry [12].
Lemma 3.3. Let $\gamma_1, \ldots, \gamma_s \in K^*$ be multiplicatively independent elements, and assume that for $\gamma_0 \in K^*$ we have

$$\gamma_0 = \gamma_1^{k_1} \cdots \gamma_s^{k_s}.$$  

Further, assume that for $i = 0, \ldots, s$ we have pairs of representatives $(g_{i1}, g_{i2})$ for $\gamma_i$ such that

$$\{ \deg f_1, \ldots, \deg f_t, \deg g_0, \deg g_1, \ldots, \deg g_s, \deg g_{s,1}, \ldots, \deg g_{s,2} \leq d_2$$
$$h(f_1), \ldots, h(f_t), h(g_0,1), h(g_0,2), \ldots, h(g_s,1), h(g_s,2) \leq h_2,$$

for some real numbers $d_2, h_2 > 1$. Then we also have

$$|k_i| \leq (2d_2)^{\exp O(r+s)}(h_2 + 1)^{2s}, \quad \text{for } i = 1, \ldots, s.$$  

Proof. This is Corollary 7.3 of Evertse and Győry [12]. □

Proof of (ii) of Theorem 2.1. Let $m$ be the exponent specified in (i) of Theorem 2.1. Then by $x^m \in \Gamma$ and $y^m \in \Gamma$ we have

$$x^m = \gamma_1^{t_{1,x}} \cdots \gamma_s^{t_{s,x}}, \quad y^m = \gamma_1^{t_{1,y}} \cdots \gamma_s^{t_{s,y}}$$

with certain integer exponents $t_{1,x}, \ldots, t_{s,x}$ and $t_{1,y}, \ldots, t_{s,y}$. Now by our assumption on $\gamma_1, \ldots, \gamma_s$ and by Proposition 3.2 we see that $x^m, y^m, \gamma_1, \ldots, \gamma_s$ have representatives with degrees and heights below the bound

$$\exp \left\{ \exp \left\{ N^{12}(2d)^{\exp O(r+s)}(h + 1)^{8s} \right\} \right\},$$

which together with Lemma 3.3 applied to the relations (3.5) concludes the proof of statement (ii) of Theorem 2.1. □

4. Auxiliary results

4.1. Results in the function field case. We recall some definitions and results concerning function fields in one variable, that are needed in our proofs.

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

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

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 subring of $M$, denoted by $O_S$. The (homogeneous) height of $a = (\alpha_1, \ldots, \alpha_l) \in M^l$ relative to $M/k$ is defined by

$$H^*_{M/k}(a) = H^*_{M/k}(\alpha_1, \ldots, \alpha_l) := \sum_{v \in \mathcal{M}_M} \min(v(\alpha_1), \ldots, v(\alpha_l)).$$
The height of $\alpha \in M$ relative to $M/\mathbb{k}$ is defined by 
\[ H_{M/\mathbb{k}}(\alpha) := H^*_M(1, \alpha) = -\sum_{v \in \mathcal{M}} \min(0, v(\alpha)). \]

It is clear that $H_{M/\mathbb{k}}(\alpha) = 0$ if and only if $\alpha \in \mathbb{k}$.

First we recall a Lemma of [4] which will be useful for bounding the genus:

**Lemma 4.1.** Let $\mathbb{k}$ be an algebraically closed field, $z$ a transcendental element over $\mathbb{k}$ and put $M = \mathbb{k}(z)$. Let 
\[ F = f_0 X^l + f_1 X^{l-1} + \cdots + f_l \in M[X] \]
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 
\[ g_{L/\mathbb{k}} \leq [L : M] \cdot l \max(\deg f_0, \ldots, \deg f_l). \]

**Proof.** This is a special case of Lemma 4.2 of [4]. \hfill \Box

**Proposition 4.2.** Let $\mathbb{k}$ be an algebraically closed field of characteristic 0, $z$ a transcendental element over $\mathbb{k}$, $M$ a finite extension of $\mathbb{k}(z)$, and $\overline{M}$ the algebraic closure of $M$. Denote by $g_{M/\mathbb{k}}$ 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 
\[ F(X, Y) = \sum_{(i,j) \in I} a_{ij} X^i Y^j \in \mathcal{O}_S[X, Y] \]
with $a_{ij} \in \mathcal{O}_S^*$ for $(i, j) \in I$, be a polynomial which fulfils the condition that
\[ F \text{ is not divisible by any non-constant polynomial of the form} \]
\[ X^m Y^n - \alpha \quad \text{or} \quad X^m - \alpha Y^n, \quad \text{with} \quad m, n \in \mathbb{Z}_{\geq 0}, \quad \alpha \in \overline{M}. \]

Assume that $H_{M/\mathbb{k}}(a_{ij}) \leq H_0$ for all $(i, j) \in I$. Then for every $x, y \in \mathcal{O}_S^*$ with
\[ F(x, y) = 0 \]
we have 
\[ H_{M/\mathbb{k}}(x), H_{M/\mathbb{k}}(y) \leq 2 \deg F \left( n(F)^2 \cdot \left( |S| + g_{M/\mathbb{k}} \right) + 2H_0 \right), \]
where $n(F)$ denotes the number of non-zero terms of $F$.

**Proof.** This is Proposition 5.3 of [2]. \hfill \Box

### 4.2. Results in the number field case.

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

$$O_S = \{ x \in K : |x|_v \leq 1 \text{ for } v \in M_K \setminus S \},$$
$$O_S^* = \{ x \in K : |x|_v = 1 \text{ for } v \in M_K \setminus S \},$$

respectively.

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

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

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

$$h_{\text{abs}}(f) := \sum_{v \in M_K} \log \max_{1 \leq i \leq g} |a_i|_v.$$

Let $\Gamma$ be a finitely generated subgroup of $(\mathbb{Q}^*)^2$. 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 $\Gamma \subset (O_S^*)^2$. Denote by $s$ the cardinality of $S$. Define

(4.2) \quad P(v) := 2 \text{ if } v \text{ is infinite, } \quad P(v) := \#O_K/p_v \text{ if } v \text{ is finite,}

where $p_v$ is the prime ideal of $O_K$ corresponding to $v$, and put

(4.3) \quad P := \max_{v \in S} P(v).

The discriminant of the field $K$ is denoted by $D_K$.

Let $f(X,Y) \in \mathbb{Q}[X,Y]$ be a polynomial which is not divisible by any non-constant polynomial of the shape $\alpha X^m Y^n - \beta$ or $\alpha X^m - \beta Y^n$ for some $\alpha, \beta \in \mathbb{Q}$, $m, n \in \mathbb{Z}_{\geq 0}$. 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 $(\alpha X - \beta)$ or $\alpha Y - \beta$, respectively. Write $N := \deg f$ for the total degree of $f$. Let $L$ be the field extension of $K$ generated by the coefficients of $f$. Put

$$\delta := \deg_X f + \deg_Y f, \quad H := \max(1, h_{\text{abs}}(f)),
$$
$$c_1 := (\delta \cdot d \cdot s \cdot \log P \cdot D_K (\log^* D_K)^{d-1})^{O(s^2)} \cdot P^{2s^2}.$$

Let $C_0 \subset (\mathbb{Q}^*)^2$ be the curve defined by $f(x, y) = 0$.

**Proposition 4.3.** For every point $x = (x, y) \in C_0 \cap \Gamma$ we have

$$h_{\text{abs}}(x) + h_{\text{abs}}(y) \leq c_1(H + 2N).$$
4.3. Analyzing the condition (2.4) posed on $F$. Let $A, K, \overline{K}$ be as in Section 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 $I \subset \mathbb{Z}_{\geq 0}^2$ is a finite set, and $0 \neq a_{ij} \in A$ are fixed. Denote by $N$ the total degree of $F$ and by $n(F)$ the number of non-zero coefficients of $F$.

A partition of the set $I$ is just a tuple $\mathcal{P} = (I_1, \ldots, I_k)$ of subsets of $I$ with the properties $I_1 \cup I_2 \cup \cdots \cup I_k = I$, $I_i \cap I_j = \emptyset$ for $i \neq j$, and $I_i \neq \emptyset$ for $l = 1, \ldots, k$.

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

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

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

$$(4.4) \quad F(x,y) = 0 \quad \text{in} \quad x,y \in A^*$$

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

1. $x,y$ is a solution of the following system

$$(4.5) \quad \sum_{(i,j) \in I_l} a_{ij} x^i y^j = 0 \quad \text{for} \quad l = 1, \ldots, k,$$

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

In this case we shall also say that $(x,y)$ is associated with the partition $\mathcal{P}$. We mention that $a_{ij} \neq 0$ for $(i,j) \in I_l$, $x,y \in A^*$ and (4.5) imply $|I_l| \geq 2$ for $l = 1, \ldots, k$.

In the case when for a given partition $\mathcal{P}$ the rank of $\Lambda := \Lambda(F, \mathcal{P})$ is 1 then we associate a system of polynomials to $\mathcal{P}$ as follows: if $r(F, \mathcal{P}) = 1$ then 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 $l = 1, \ldots, k$ 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 $l = 1, \ldots, k$ we get that every $(i,j) \in I_l$ can be written as $(i,j) = (i_l,j_l) + t_{ij}(m,n)$, for $l = 1, \ldots, k$, with some $t_{ij} \in \mathbb{Z}$, $|t_{ij}| \leq N$. Thus the system (4.5) is equivalent to the system

$$X^{i_l}Y^{j_l} \sum_{(i,j) \in I_l} a_{ij} (X^m Y^n)^{t_{ij}} = 0 \quad \text{for} \quad l = 1, \ldots, k.$$
By multiplying these equations by suitable powers of $X^mY^n$ we see that (4.5) is equivalent to a system
\begin{equation}
g_l(X^mY^n) = 0 \quad \text{for} \quad l = 1, \ldots, k,
\end{equation}
where
\begin{equation}
g_l(X) := \sum_{(i,j) \in I_l} a_{ij}X^{s_{ij}} \in A[X], \quad g_l(0) \neq 0 \quad \text{for} \quad l = 1, \ldots, k
\end{equation}
and $0 \leq s_{ij} \leq 2N$ for all $(i,j)$. We shall call $(g_1, \ldots, g_k)$ the polynomial system corresponding to the partition $\mathcal{P}$.

**Proposition 4.4.** Let $F(X,Y) \in A[X,Y]$ be a polynomial. Then $F$ satisfies condition (2.4) if and only if for each partition $\mathcal{P} = (I_1, \ldots, I_k)$ of $I$ we have one of the following:

1. $r(F, \mathcal{P}) = 2$, or
2. $r(F, \mathcal{P}) = 1$, and the polynomial system $(g_1, \ldots, g_k) \in A[X]^r$ corresponding to $\mathcal{P}$ has the property
   \[ \gcd(g_1, \ldots, g_r) = 1 \quad \text{in} \quad K[X]. \]

**Proof.** This is Proposition 3.1 of [2]. □

**Proposition 4.5.** Let $F(X,Y)$ be a polynomial satisfying (2.4) and fix a solution $(x,y)$ of (4.4). 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 $\mathcal{P}$. Then we have
\[ r(F, \mathcal{P}) = 2. \]

**Proof.** This is Proposition 3.2 of [2]. □

The above two propositions mean in fact, that for a polynomial fulfilling condition (2.4) there might exist partitions of $I$ of rank 1, but these are never partitions corresponding to a solution.

### 4.4. Effective estimates for the gcd of polynomials.

**Lemma 4.6.** Let $A$ be a finitely generated domain as in Section 2 and $K$ its quotient field. Let $k, \rho \in \mathbb{N}$ with $2^{k-1} \leq \rho \leq 2^k$ and define the polynomials
\[ g_i(X) := \sum_{j=0}^d x_{ij}X^j \in A[X] \quad \text{for} \quad i = 1, \ldots, \rho. \]
Further, suppose that the coefficients $x_{ij} \in A$ have representatives $\tilde{x}_{ij}$ with
\[ \deg \tilde{x}_{ij} \leq d, \quad h(\tilde{x}_{ij}) \leq h, \]
where $d > 1$ and $h > 1$ are given real numbers. Suppose that
\[ \gcd(g_1, \ldots, g_\rho) = 1 \quad \text{in} \quad K[X]. \]
Then there exist polynomials $u_1, \ldots, u_\rho \in A[X]$ and non-zero $R \in A$, such that
$$u_1g_1 + \cdots + u_\rho g_\rho = R,$$
and that $R$ has a representative $\tilde{R}$ with
$$\deg \tilde{R} \leq d(2\delta)^k, \quad h(\tilde{R}) \leq (2\delta)^{k+2}(d+1)rh.$$  

**Proof.** This is Corollary 3.1 in [2]. \qed

5. General description of the method for proving effective results over finitely generated domains

5.1. Extending the domain $A$. In this section we extend the domain $A$ to a larger finitely generated domain $B$ in which it will be more convenient to do effective computations, and which can be chosen in such a way that several elements of $K$ (chosen according to our needs) will be units in this extended domain. This latter property will have special importance when we define our specializations. We also introduce a new representation for elements of $K$, which gives rise to a different way of measuring elements of $K$ than the one using the size of representatives, and this way of measuring will be more convenient in our proofs.

Let $A = \mathbb{Z}[z_1, \ldots, z_r]$ be a finitely generated domain given by (2.1), and let $K$ be its quotient field. Let $q \geq 0$ denote the transcendence degree of $K$. We may assume without loss of generality that $z_1, \ldots, z_q$ is a transcendence basis of $K/\mathbb{Q}$. Put

$$K_0 := \mathbb{Q}(z_1, \ldots, z_q), \quad A_0 := \mathbb{Z}[z_1, \ldots, z_q].$$

For elements $f \in A_0 \setminus \{0\}$ let $\deg f$ and $h(f)$ denote the total degree and logarithmic height of $f$, respectively, viewed as a polynomial in the unknowns $z_1, \ldots, z_q$. In the case $q = 0$ we define $\deg f := 0$ and $h(f) := \log |f|$. Put

$$d_0 := \max(1, \deg f_1, \ldots, \deg f_t), \quad h_0 := \max(1, h(f_1), \ldots, h(f_t)),$$

where $f_1, \ldots, f_t$ are the generators of the ideal $\mathcal{I}$ in (2.1).

Since the field $K$ is a finite algebraic extension of $K_0$, we can write $K = K_0(w)$ for some $w \in K$. We recall the following result of Evertse and Györy.

**Proposition 5.1.** (i) There exists $w \in A$ such that $K = K_0(w)$, $w$ is integral over $A_0$ and $w$ has minimal polynomial
$$\mathcal{F}(X) = X^D + \mathcal{F}_1 X^{D-1} + \cdots + \mathcal{F}_D \in A_0[X]$$
over $K_0$ such that $D \leq d_0^{-q}$ and

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

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

(ii) Let $\alpha_1, \ldots, \alpha_k \in K^*$ and suppose that $\alpha_i$ has representation pair $(u_i, v_i)$ with $u_i, v_i \in \mathbb{Z}[X_1, \ldots, X_r]$, $v_i \not\in I$, for $i = 1, \ldots, k$. Put
\[
d^{**} := \max(d_0, \deg u_1, \deg v_1, \ldots, \deg u_k, \deg v_k),
\]
\[
h^{**} := \max(h_0, h(u_1), h(v_1), \ldots, h(u_k), h(v_k)).
\]
Then there is a non-zero $f \in A_0$ such that with $B := A_0[w, f^{-1}]$ we have
\[
A \subseteq B,
\]
\[
\alpha_1, \ldots, \alpha_k \in B^*.
\]
Further, $f$ can be chosen such that it fulfils
\[
\deg f \leq (k + 1)(2d^{**})^{\exp O(r)}, \quad h(f) \leq (k + 1)(2d^{**})^{\exp O(r)}(h^{**} + 1).
\]

Proof. These versions of (i) and (ii) are stated in Proposition 3.1 in [2], however originally (i) is proved in Evertse and Győry [12], Proposition 3.4 and Lemma 3.2, (i), while (ii) is proved in [12], Lemma 3.6. □

Now let us describe the above-mentioned representation for the elements of the field $K$. Recall that $D$ denotes the degree of $K$ over $K_0$. Since $K = K_0(w)$ for every element $\alpha \in K$ there exists a unique representation $\sum_{j=0}^{D-1} R_{\alpha,j} w^j$, where $R_{\alpha,j} \in K_0$. Since $A_0$ is a unique factorization domain (indeed, $z_1, \ldots, z_q$ are algebraically independent) and $K_0$ is its quotient field, thus there exist $P_{\alpha,0}, \ldots, P_{\alpha,D-1}, Q_\alpha \in A_0$ such that
\[
\alpha = Q_\alpha^{-1} \sum_{j=0}^{D-1} P_{\alpha,j} w^j \quad \text{with} \quad Q_\alpha \neq 0, \quad \gcd(P_{\alpha,0}, \ldots, P_{\alpha,D-1}, Q_\alpha) = 1.
\]
Further, the tuple $(P_{\alpha,0}, \ldots, P_{\alpha,D-1}, Q_\alpha)$ is up to sign uniquely determined. Now we define
\[
\begin{aligned}
\overline{\deg} \alpha &:= \max(\deg P_{\alpha,0}, \ldots, \deg P_{\alpha,D-1}, \deg Q_\alpha) \\
\overline{h}(\alpha) &:= \max(h(P_{\alpha,0}), \ldots, h(P_{\alpha,D-1}), h(Q_\alpha)),
\end{aligned}
\]
if $q > 0$, and $\overline{\deg} \alpha = 0$ and $\overline{h}(\alpha) = \log \max(|P_{\alpha,0}|, \ldots, |P_{\alpha,D-1}|, |Q_\alpha|)$ if $q = 0$. These two concepts provide a convenient way to measure elements of $K$.

**Proposition 5.2.** Let $\alpha_1, \ldots, \alpha_k \in K^*$ and suppose that there are $\bar{d} > 1$ and $\bar{h} > 1$ such that $\overline{\deg} \alpha_i \leq \bar{d}$ and $\overline{h}(\alpha_i) \leq \bar{h}$ for $i = 1, \ldots, k$. Then there is a non-zero $f \in A_0$ such that with $B := A_0[w, f^{-1}]$ we have
\[
A \subseteq B,
\]
\[
\alpha_1, \ldots, \alpha_k \in B^*.
\]
Further, $f$ can be chosen such that it fulfills
\begin{align}
\deg f &\leq (2d_0)^{\exp O(r)} + 2kd, \\
h(f) &\leq (2d_0)^{\exp O(r)}(h_0 + 1) + 2k\hat{h} + 2rkd.
\end{align}

Proof. This proposition is just a variant of (ii) of Propositions 5.1. To prove it we only need to slightly modify the proof of Lemma 3.6. in [12]. In principle, the element $f$ is chosen to be the same as in (ii) of Propositions 5.1 (as constructively given in the proof of Lemma 3.6. in [12]), just the estimate for the degree and height of $f$ is computed in terms of $d_0, \tilde{d}, \hat{h}$ instead of $d^*, h^*.$

The following two lemmas describe how $\overline{\deg} \alpha$ and $\overline{h}(\alpha)$ and the height and degree of representatives for $\alpha$ may be bounded in terms of each other.

**Lemma 5.3.** Let $\alpha \in K^*$ and let $(a, b)$ be a pair of representatives for $\alpha$ with $a, b \in \mathbb{Z}[X_1, \ldots, X_r], b \notin I.$ Put
\[
d^* := \max(d_0, \deg a, \deg b) \quad \text{and} \quad h^* := \max(h_0, h(a), h(b)).
\]

Then
\begin{align}
\overline{\deg} \alpha &\leq (2d^*)^{\exp O(r)}, \\
\overline{h}(\alpha) &\leq (2d^*)^{\exp O(r)}(h^* + 1).
\end{align}

Proof. This is Lemma 3.5 in Evertse and Győry [12].

**Lemma 5.4.** Let $\alpha$ be a nonzero element of $A,$ and put
\[
\hat{d} := \max(d_0, \overline{\deg} \alpha), \quad \hat{h} := \max(h_0, \overline{h}(\alpha)).
\]

Then $\alpha$ has a representative $\tilde{\alpha} \in \mathbb{Z}[X_1, \ldots, X_r]$ such that
\begin{align}
\overline{\deg} \tilde{\alpha} &\leq (2\hat{d})^{\exp O(r \log^* r)}(\hat{h} + 1), \\
\overline{h}(\tilde{\alpha}) &\leq (2\hat{d})^{\exp O(r \log^* r)}(\hat{h} + 1)^{r+1}.
\end{align}

Proof. This is a special case of Lemma 3.7 of Evertse and Győry [12] with the choice $\lambda = 1$ and $a = b = 1.$ The proof of this lemma is based on work of Aschenbrenner [1].

Using Lemma 5.3 and (2.5) we have the estimates
\begin{align}
\overline{\deg} \gamma_i &\leq (2d)^{\exp(O(r))}, \\
\overline{h}(\gamma_i) &\leq (2d)^{\exp(O(r))}(h + 1)
\end{align}
for $i = 1, \ldots, s,$ and
\begin{align}
\overline{\deg} a_{ij} &\leq (2d)^{\exp(O(r))}, \\
\overline{h}(a_{ij}) &\leq (2d)^{\exp(O(r))}(h + 1)
\end{align}
for $(i, j) \in I.$ These estimates will be frequently used in the rest of the paper.
5.2. Using function field results for bounding the degree \( \overline{\deg} \) of elements of \( B \). In this subsection we collect the main tools needed to use results over function fields to bound the \( \overline{\deg} \) of elements of \( B \). Recall that \( A = \mathbb{Z}[z_1, \ldots, z_r] \) and \( K \) denotes the quotient field of \( A \). We keep our assumption that \( z_1, \ldots, z_q \) is a transcendence basis of \( \mathbb{Q}(w) \). Let \( w \in A_0 \) and \( f \in A_0 \) be the elements specified in Proposition 5.1 and put \( B := A_0[z_1, \ldots, z_q] \). Then \( K = \mathbb{Q}(w) \) and \( A \subseteq B \subseteq K \). Further, let us denote by \( w^{(1)} = w, \ldots, w^{(D)} \) the conjugates of \( w \) over \( K_0 \).

Now we fix \( i \in \{1, \ldots, q\} \) and introduce the following notation:

\[
\begin{align*}
k_i &:= \mathbb{Q}(z_1, \ldots, z_i-1, z_{i+1}, \ldots, z_q), \\
\overline{k}_i &\text{ denotes the algebraic closure of } k_i, \\
M_i &:= \overline{k}_i(z_i, w^{(1)}, \ldots, w^{(D)}), \\
B_i &:= k_i[z_i, f^{-1}, w^{(1)}, \ldots, w^{(D)}].
\end{align*}
\]

Clearly, \( M_i \) is the splitting field of the minimal polynomial \( F(X) \) of \( w \) over the field \( \overline{k}_i(z_i) \), and \( B_i \) is a subring of \( M_i \) containing \( B \). Further, we use the following notation:

\[
\Delta_i := [M_i : \overline{k}_i(z_i)], \\
g_{M_i} \text{ denotes the genus of } M_i/\overline{k}_i, \\
H_{M_i} \text{ denotes the height with respect to } M_i/\overline{k}_i.
\]

Put

\[
d_1 := \max\{d_0, \deg f, \deg F_1, \ldots, \deg F_D\}.
\]

The following Lemma gives an upper bound for the \( \overline{\deg} \) of an element of \( K^* \) depending on the function field heights with respect to \( M_i/\overline{k}_i \) of its conjugates.

**Lemma 5.5.** Let \( \alpha \in K^* \) and denote by \( \alpha^{(1)}, \ldots, \alpha^{(D)} \) the conjugates of \( \alpha \) corresponding to \( w^{(1)}, \ldots, w^{(D)} \). Then

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

**Proof.** This is Lemma 4.4 in Evertse and Győry [12]. \( \square \)

Conversely, we have the following:

**Lemma 5.6.** Let \( \alpha \in K^* \) and \( \alpha^{(1)}, \ldots, \alpha^{(D)} \) be as in Lemma 5.5. Then we have

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

**Proof.** This is Lemma 4.4 of [4]. \( \square \)
5.3. Specializations. Recall again that
\[ K_0 = \mathbb{Q}(z_1, \ldots, z_q), \quad K = \mathbb{Q}(z_1, \ldots, z_q), \]
where \( w, f \) are the elements specified in Proposition 5.1, and the minimal polynomial of \( w \) has the form \( \mathcal{F}(X) = X^D + \mathcal{F}_1 X^{D-1} + \cdots + \mathcal{F}_D \in A_0[X] \), with degree and coefficients bounded as described in Proposition 5.1.

For every \( \mathbf{u} \in \mathbb{Z}^q \) the substitution \( z_i \to u_i \) for \( i = 1, \ldots, q \) defines a mapping from a subring of \( K_0 \) to \( \overline{\mathbb{Q}} \). More precisely, we fix \( \mathbf{u} \) and we consider the ring homomorphism \( \varphi_{\mathbf{u}} \) from a subring of \( K_0 \) to \( \overline{\mathbb{Q}} \) defined by
\[
\varphi_{\mathbf{u}}(\alpha) := \alpha(\mathbf{u}) = \frac{g_1(\mathbf{u})}{g_2(\mathbf{u})}
\]
for every \( \alpha = g_1 g_2 \in K_0 \) with \( g_1, g_2 \in A_0 \), and with the additional property \( g_2(\mathbf{u}) \neq 0 \). To extend this map to a ring homomorphism from \( B \) to \( \overline{\mathbb{Q}} \) we will impose some restrictions on \( \mathbf{u} \). 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
\[
\mathcal{H} := \Delta_{\mathcal{F}} \cdot \mathcal{F}_D \cdot f \in A_0,
\]
and assume that \( \mathbf{u} \) is chosen such that \( \mathcal{H}(\mathbf{u}) \neq 0 \). Put
\[
(5.19) \begin{cases} d_0^* = \max(\deg \mathcal{F}_1, \ldots, \deg \mathcal{F}_D) \\ h_0^* = \max(h(\mathcal{F}_1), \ldots, h(\mathcal{F}_D)) \end{cases} \quad \begin{cases} d_1^* = \max(d_0^*, \deg f) \\ h_1^* = \max(h_0^*, h(f)) \end{cases}
\]
Thus we clearly have
\[
(5.20) \quad \deg \mathcal{H} \leq (2D - 2) \cdot d_0^* + d_1^* \leq (2D - 1) \cdot d_0^* + d_1^*.
\]

Let us fix a tuple \( \mathbf{u} \in \mathbb{Z}^q \) with \( \mathcal{H}(\mathbf{u}) \neq 0 \). Since \( \mathcal{H}(\mathbf{u}) \neq 0 \) implies \( \Delta_{\mathcal{F}} \neq 0 \) and \( \mathcal{F}_D(\mathbf{u}) \neq 0 \), the polynomial
\[
\mathcal{F}_\mathbf{u} := X^D + \mathcal{F}_1(\mathbf{u}) X^{D-1} + \cdots + \mathcal{F}_D(\mathbf{u})
\]
has \( D \) distinct non-zero roots, say \( w^{(1)}(\mathbf{u}), \ldots, w^{(D)}(\mathbf{u}) \).

Now we extend the map \( \varphi_{\mathbf{u}} \) to the ring \( B \) in \( D \) different ways. Namely, for each \( j = 1, \ldots, D \) we shall define the function \( \varphi_{\mathbf{u},j} \) on \( B \) such that if \( \alpha \in B \) is written as
\[
(5.21) \quad \alpha = \sum_{i=1}^{D-1} (P_i/Q) w^i,
\]
where \( P_0, \ldots, P_{D-1}, Q \in A_0, \gcd(P_0, \ldots, P_{D-1}, Q) = 1 \), then
\[
(5.22) \quad \varphi_{\mathbf{u},j}(\alpha) = \alpha^{(j)}(\mathbf{u}) := \sum_{i=1}^{D-1} (P_i(\mathbf{u})/Q(\mathbf{u})) (w^{(j)}(\mathbf{u}))^i.
\]
Since $\alpha \in B$, the polynomial $Q$ must divide a power of $f$ and hence $Q(u) \neq 0$, so $\varphi_{u,j}(\alpha)$ is well-defined. Clearly, $\varphi_{u,j}$ is a ring homomorphism from $B$ to $\mathbb{Q}$, thus any of the specializations $\varphi_{u,j}$ maps any unit of $B$ to a non-zero element of $\mathbb{Q}$. We mention that $\varphi_{u,j}$ is the identity on $B \cap \mathbb{Q}$. Further, if $\alpha \in B \cap \mathbb{Q}$ then $\varphi_{u,j}(\alpha)$ is a conjugate of $\alpha$.

For $u = (u_1, \ldots, u_q) \in \mathbb{Z}^q$, put $|u| := \max(|u_1|, \ldots, |u_q|)$. Then for any $g \in A_0$, $u \in \mathbb{Z}^q$,

\begin{equation}
\log |g(u)| \leq q \log \deg g + h(g) + \deg g \log \max(1, |u|). \tag{5.23}
\end{equation}

Thus, we have

\begin{equation}
h(F_u) \leq q \log d_0^* + h_0^* + d_0^* \log \max(1, |u|) \tag{5.24}
\end{equation}

and so by Lemma 5.1 of Evertse and Győry [12]

\begin{equation}
\sum_{j=1}^{D} h(w^{(j)}(u)) \leq D + 1 + q \log d_0^* + h_0^* + d_0^* \log \max(1, |u|). \tag{5.25}
\end{equation}

Define the algebraic number fields

\begin{equation}
K_{u,j} := \mathbb{Q}(w^{(j)}(u)) \quad \text{for} \quad j = 1, \ldots, D,
\end{equation}

and denote by $\Delta_{K_{u,j}}$ their discriminant.

The following lemmas of Evertse and Győry [12] summarize important properties of the above-defined specializations.

**Lemma 5.7.** Let $u \in \mathbb{Z}^q$ with $\mathcal{H}(u) \neq 0$. Then for $j = 1, \ldots, D$ we have $[K_{u,j} : \mathbb{Q}] \leq D$ and

\[ |\Delta_{K_{u,j}}| \leq D^{2D-1} \left((d_0^*)^{q_0} e^{h_0^* \max(1, |u|)}\right)^{2D-2}. \]

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

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

**Lemma 5.8.** Let $u \in \mathbb{Z}^q$ with $\mathcal{H}(u) \neq 0$, and let $\alpha \in B$. Then for $j = 1, \ldots, D$,

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

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

The below lemma shows that if we take a sufficiently large number of specializations, then there is at least one specialization among them (say corresponding to $u \in \mathbb{Z}^q$), such that $\overline{h}(\alpha)$ for $\alpha \in B$ can be bounded by the heights of the images of $\alpha$ by the specializations $\varphi_{u,j}$ for $j = 1, \ldots, D$. 
Lemma 5.9. Let $\alpha \in B$, $\alpha \neq 0$, and let $N_0$ be an integer with
\begin{equation}
N_0 \geq \max(\deg \alpha, 2Dd_0^* + 2(q + 1)(d_1^* + 1)).
\end{equation}
Then the set
\[ S := \{ u \in \mathbb{Z}^q : |u| \leq N_0, \mathcal{H}(u) \neq 0 \} \]
is non-empty, and
\begin{equation}
\overline{h}(\alpha) \leq 5N_0^4(h_1^* + 1)^2 + 2D(h_1^* + 1)H,
\end{equation}
where $H := \max\{h(\alpha^{(j)}(u)) : u \in S, j = 1, \ldots, D\}$.

Proof. This is Lemma 5.7 in Evertse and Győry [12]. \qed

6. Proof of Proposition 3.1

We split the proof of Proposition 3.1 into several steps, each being presented in a separate subsection:

- for $(x, y) \in C$ we bound the degree of the field $K(x, y)$ over $K$;
- we estimate the smallest positive integer exponent $M$ such that for $(x, y) \in C$ we have $x^M, y^M \in \Gamma_K$, where $\Gamma_K$ denotes the $K$-closure of $\Gamma$, i.e. the largest subgroup of $\Gamma$ which belongs to $K^*$;
- for $\gamma \in \Gamma_K$ we estimate the smallest positive integer exponent $m(\gamma)$ such that $\gamma^{m(\gamma)} \in \Gamma$;
- we conclude the proof of Proposition 3.1.

6.1. Bounding the degree of $K(x, y)$. Let $(x, y) \in C$. We shall give a bound on the degree of the field $L := K(x, y)$ over $K$. Since $x, y \in \Gamma$, there exist $m_x, m_y \in \mathbb{Z}_{>0}$ such that $x^{m_x}, y^{m_y} \in \Gamma$. Take the least common multiple of $m_x$ and $m_y$ and denote it by $m_{xy}$. Then $x^{m_{xy}}, y^{m_{xy}} \in \Gamma \subset K$, so we have
\[ [K(x, y) : K] \leq m_{xy}. \]

In order to estimate $m_{xy}$ put $F_{x,y}(X, Y) := F(xX, yY)$. Then for any embedding $\sigma : L \hookrightarrow \overline{K}$, we have $F(\sigma(x), \sigma(y)) = 0$, hence
\[ F_{x,y} \left( \frac{\sigma(x)}{x}, \frac{\sigma(y)}{y} \right) = 0. \]

Since $x^{m_x} \in K$ we also have $\sigma(x)^{m_x} \in K$, hence
\[ \left( \frac{\sigma(x)}{x} \right)^{m_{xy}} = 1, \]
and similarly,
\[ \left( \frac{\sigma(y)}{y} \right)^{m_{xy}} = 1. \]
Thus the distinct embeddings $\sigma : K(x, y) \hookrightarrow K$ give rise to distinct solutions $\left(\frac{\sigma(x)}{x}, \frac{\sigma(y)}{y}\right)$ of the equation

$$F_{x, y}(\rho_1, \rho_2) = 0 \quad \text{in} \quad \rho_1, \rho_2 \quad \text{roots of unity}.$$  

However, by the result of Beukers and Smyth [6] this equation has at most $22(\deg F)^2$ solutions in roots of unity. Thus we have proved that

$$(6.1) \quad [K(x, y) : K] \leq 22(\deg F)^2 = 22N^2.$$  

6.2. Bounding the exponent $M$. Let again $x, y \in \mathbb{C}$. Let us denote by $\Gamma_K$ the $K$-closure of $\Gamma$, i.e. the largest subgroup of $\Gamma$ belonging to $K^*$. Then we have $\Gamma \subseteq \Gamma_K \subseteq \Gamma$. Now we shall give an upper bound for the minimal exponent $M$ such that

$$x^M, y^M \in \Gamma_K.$$  

Let $d_x := [K(x) : K]$. Then we have $d_x \leq 22N^2$. By $x \in \Gamma$ there exists $m_x \in \mathbb{N}$ with $x^{m_x} \in \Gamma$. Put $\gamma := x^{m_x}$. Then the minimal polynomial $f_x(X)$ of $x$ over $K$ divides

$$X^{m_x} - \gamma = \prod_{i=1}^{m_x} (X - \rho^i x),$$  

where $\rho$ is a primitive root of unity of order $m_x$. Thus

$$f_x(X) = \prod_{j=1}^{d_x} \left( X - \rho^{i_j} x \right) \in K[X]$$  

with suitable distinct choices of $i_j \in \{1, \ldots, m_x\}$. Hence there exists a root of unity $\rho$ such that

$$\rho x^{d_x} \in K^*.$$  

Now let us estimate the order $l$ of $\rho$. Clearly, $\rho \in K(x)$. Further, since $[K : K_0] \leq d^r - q$ (see Proposition 5.1 (i)) we have $[K(x) : K_0] \leq d_x \cdot d^r - q$, and by $\rho \in K(x)$ this gives the estimate $[K(\rho) : K_0] \leq d_x \cdot d^r - q$, which gives $[K_0(\rho) : K_0] \leq d_x \cdot d^r - q$. However, since $K_0 = \mathbb{Q}(z_1, \ldots, z_q)$, with algebraically independent elements $z_1, \ldots, z_q$, we have $[K_0(\rho) : K_0] = [\mathbb{Q}(\rho) : \mathbb{Q}]$, hence

$$[\mathbb{Q}(\rho) : \mathbb{Q}] \leq d_x \cdot d^r - q.$$  

On the other hand $\rho$ is a root of unity of order $l$, so

$$[\mathbb{Q}(\rho) : \mathbb{Q}] = \varphi(l),$$  

which gives the estimate

$$\varphi(l) \leq d_x \cdot d^r - q.$$  

Now using the estimate

$$\varphi(l) \gg \frac{l}{\log \log l}$$
of Rosser and Schönfeld [22] we infer
\[ l \ll (d_x d_r^q)^2, \]
where the constants implied by \( \ll \) and \( \gg \) are absolute constants. However, since \( \rho x^d_x \in K^* \) we have \( (\rho x^d_x)^l \in K^* \) hence \( x^{d_x-l} \in K^* \), which by \( d_x \leq 22N^2 \) proves that
\[ (6.2) \quad M \leq d_x \cdot l \ll d_x^3 d_r^{2(r-q)} \ll N^6 d_r^{2(r-q)}. \]

6.3. Bounding the exponent \( m(\gamma) \). The next step is to take an arbitrary element
\[ \gamma \in \Gamma_K \setminus \Gamma. \]
Since \( \gamma \in \Gamma_K \subseteq \bar{\Gamma} \) there exists a minimal natural number \( m(\gamma) \) such that
\[ \gamma^{m(\gamma)} \in \Gamma. \]
We now estimate \( m(\gamma) \). Clearly, for such an \( m(\gamma) \) we have
\[ (6.3) \quad \gamma^{m(\gamma)} = \gamma_1^{t_1} \cdots \gamma_s^{t_s}, \]
and without loss of generality we may suppose that \( 0 \leq t_i < m(\gamma) \) for \( i = 1, \ldots, s \). Indeed, if we take \( v_i \) with \( v_i \equiv t_i \pmod{m(\gamma)} \) and \( 0 \leq v_i < m(\gamma) \) for \( i = 1, \ldots, s \), then considering \( \gamma' := \gamma_1^{v_1} \cdots \gamma_s^{v_s} \) we have \( m(\gamma) = m(\gamma') \), and for bounding \( m(\gamma) \) we may just replace \( \gamma \) by \( \gamma' \). So we start with the relation
\[ (6.4) \quad \gamma^{m(\gamma)} = \gamma_1^{t_1} \cdots \gamma_s^{t_s}, \quad 0 \leq t_i < m(\gamma). \]
Now we first bound \( \deg \gamma \) and \( h(\gamma) \).

6.3.1. Bounding \( \deg \gamma \).

Recall that \( \gamma_1, \ldots, \gamma_s \in K^* \) are given by corresponding representation pairs \((g_1, h_1), \ldots, (g_s, h_s)\), which fulfil (2.5). First we extend the domain \( A \) to a larger domain \( B \) such that the 'numerator' and 'denominator' of \( \gamma_1, \ldots, \gamma_s \) are all units of \( B \). More precisely, let \( \gamma_{i1} := g_i(z_1, \ldots, z_r) \) and \( \gamma_{i2} := h_i(z_1, \ldots, z_r) \) for \( i = 1, \ldots, s \). Then we have the following:

Proposition 6.1. There exists a non-zero \( f \in A_0 \) such that
\[ (6.5) \quad A \subseteq A_0[w, f^{-1}] =: B, \quad \gamma_{i1}, \gamma_{i2} \in A_0[w, f^{-1}]^* \quad \text{for} \quad i = 1, \ldots, s \]
and
\[ (6.6) \quad \deg f \leq (2s + 1)(2d)^{\exp O(r)}, \quad h(f) \leq (2s + 1)(2d)^{\exp O(r)}(h + 1). \]

Proof. This is a simple consequence of (ii) of Proposition 5.1. Indeed, we have \( k = 2s \), and in view of (2.5) we may take \( d^{**} = d \) and \( h^{**} = h \). \( \square \)
We use the notation of Section 5.2.
By (5.16), (2.5), (5.3) and (6.6) we have the estimate
\begin{equation}
d_1 \leq (2s + 1)(2d)^{\exp O(r)}.
\end{equation}
By Lemma 5.6 we have
\begin{equation}
\max_{i,j} H_{M_i} \left( \gamma_k^{(i)} \right) \leq \Delta_i \left( 2D \deg \gamma_k + (2d_0)^{\exp O(r)} \right) \leq \Delta_i (2d)^{\exp O(r)}.
\end{equation}
Further, by (6.4) we have
\begin{equation}
mH_{M_i} \left( \gamma^{(j)} \right) \leq \sum_{k=1}^s t_k H_{M_i} \left( \gamma_k^{(j)} \right)
\end{equation}
which means
\begin{equation}
H_{M_i} \left( \gamma^{(j)} \right) \leq \sum_{k=1}^s \frac{t_k}{m} H_{M_i} \left( \gamma_k^{(j)} \right) \leq \sum_{k=1}^s H_{M_i} \left( \gamma_k^{(j)} \right) \leq s \Delta_i (2d)^{\exp O(r)}.
\end{equation}
Thus by Lemma 5.5 we get
\begin{equation}
\deg \gamma \leq qDd_1 + \sum_{i=1}^q \Delta_i^{-1} \sum_{j=1}^D H_{M_i} \left( \gamma^{(j)} \right)
\end{equation}
\begin{equation}
\leq qD(2s + 1)(2d)^{\exp O(r)} + \sum_{i=1}^q \Delta_i^{-1} Ds \Delta_i (2d)^{\exp O(r)}
\leq s(2d)^{\exp O(r)}.
\end{equation}

6.3.2. **Bounding** \( \overline{h}(\gamma) \).

We shall use the notation of Section 5.3. Let \( \varphi_{u,j} \) be a specialization map on the domain \( B \) as defined in Section 6.3.1. Then applying \( \varphi_{u,j} \) to the relation (6.4) we get
\begin{equation}
\gamma^{(j)}(u)^{m(\gamma)} = \gamma_1^{(j)}(u)t_1 \ldots \gamma_s^{(j)}(u)t_s,
\end{equation}
which gives
\begin{equation}
m(\gamma)h_{\text{abs}}(\gamma^{(j)}(u)) \leq \sum_{i=1}^s t_i h_{\text{abs}}(\gamma_i^{(j)}(u))
\end{equation}
leading to the estimate
\begin{equation}
h_{\text{abs}}(\gamma^{(j)}(u)) \leq \sum_{i=1}^s \frac{t_i}{m(\gamma)} h_{\text{abs}}(\gamma_i^{(j)}(u)) \leq \sum_{i=1}^s h_{\text{abs}}(\gamma_i^{(j)}(u)).
\end{equation}
By Lemma 5.8 and (5.12) we have
\begin{equation}
h_{\text{abs}}(\gamma_i^{(j)}(u)) \leq (2d)^{\exp O(r)} (h + 1 + \log \max(1, |u|)).
\end{equation}
Using the domain $B$ specified in Section 6.3.1 by (6.5) we have
\[ (6.13) \quad d_1^* \leq (2s + 1)(2d)^{\exp(O(r))}, \quad h_1^* \leq (2s + 1)(2d)^{\exp(O(r))}(h + 1). \]
Now in order to use Lemma 5.9 we may choose $N_0 := (2s + 1)(2d)^{\exp(O(r))}$ providing the bound
\[ h_{abs}(\gamma^{(j)}_i(u)) \leq (2d)^{\exp(O(r))}(h + 1)s, \]
which together with (6.11) gives
\[ h_{abs}(\gamma^{(j)}_i(u)) \leq s^2(2d)^{\exp(O(r))}(h + 1), \]
and the use of Lemma 5.9 leads to the estimate
\[ (6.14) \quad \overline{h}(\gamma) \leq s^6(2d)^{\exp(O(r))}(h + 1)^2. \]

6.3.3. Bounding the exponents in (6.4).

Lemma 6.2. Let $\gamma_0, \gamma_1, \ldots, \gamma_s \in K^*$ be multiplicatively dependent elements, and assume that for $i = 0, \ldots, s$ we have
\[ (6.15) \quad \deg \gamma_i \leq (2d)^{\exp(O(r+s))}, \quad \overline{h}(\gamma_i) \leq (2d)^{\exp(O(r+s))}(h + 1)^2. \]
Then there exist integers $k_0, \ldots, k_s$ not all equal to 0 such that
\[ \gamma_0^{k_0} \ldots \gamma_s^{k_s} = 1 \]
and
\[ (6.16) \quad |k_i| \leq (2d)^{\exp(O(r+s))}(h + 1)^{2s}, \quad \text{for } i = 0, \ldots, s. \]

Proof. This is a variant of Lemma 7.2 of Evertse and Győry in [12]. To prove this result it would be necessary to redo the long proof of Lemma 7.2 of [12], with most part of it completely unchanged. So here we only indicate those points which should be changed in the proof of Lemma 7.2 of [12] to get our Lemma 6.2. The first point is, that after defining the elements $\gamma_\nu$ we have to estimate their $\deg$, i.e. we get
\[ \deg \gamma_\nu \leq \sum_{i=0}^s v_i \deg \gamma_i \leq V \cdot (2d)^{\exp(O(r+s))}. \]
Thus using our Proposition 5.2 we get the same estimate
\[ \deg f \leq V^{\exp(O(r+s))} \]
as in [12]. From this point we have to redo identically the computation of the proof of Lemma 7.2 of [12], just with the bounds (6.15) instead of the bounds given in the proof of Evertse and Győry for $\deg \gamma_i$ and $\overline{h}(\gamma_i)$, and finally we get the estimate (6.16). \qed

Now applying Lemma 6.2 to our identity (6.4) we get the desired bound
\[ (6.17) \quad |m(\gamma)|, |t_i| \leq (2d)^{\exp(O(r+s))}(h + 1)^{2s}. \]
6.4. Concluding the proof of Proposition 3.1. In Section 6.2 we proved that for a given \((x, y) \in C\) there exists an exponent \(M\) with (6.2) such that \(x^M, y^M \in \Gamma_K\).

Further, by Section 6.3 there exist exponents \(m(x^M)\) and \(m(y^M)\) with

\[
m(x^M), m(y^M) \leq (2d)^{\exp(O(r+s))}(h + 1)^{2s},
\]

such that

\[
(x^M)^{m(x^M)}, (y^M)^{m(y^M)} \in \Gamma.
\]

Put \(m_0 := M \cdot m(x^M) \cdot m(y^M)\). Then we have

\[
m_0 \leq N^6(2d)^{\exp(O(r+s))}(h + 1)^{4s}.
\]

Denoting by \(C_3\) the constant implied by the \(O(\cdot)\) symbol in the last inequality the proof of Proposition 3.1 is concluded.

7. Proof of Proposition 3.2

7.1. Bounding the degree. We shall use the notation of Section 5.1 however we shall extend our domain \(A\) to a larger domain \(B\) in a different way than we did in Section 6. More precisely, we choose \(f\) and thus \(B\) as described in the following proposition:

**Proposition 7.1.** There exists a non-zero \(f \in A_0\) with

\[
\begin{align*}
\deg f &\leq sN^2(2d)^{\exp O(r)}, \\
h(f) &\leq sN^2(2d)^{\exp O(r)}(h + 1),
\end{align*}
\]

such that with \(B := A_0[f^{-1}, w]\)

\[
A \subseteq B,
\]

\[
\gamma_{i1}, \gamma_{i2} \in B^* \quad \text{for } i = 1, \ldots, s,
\]

\[
a_{ij} \in B^* \quad \text{for } (i, j) \in I.
\]

**Proof.** This is a simple consequence of (ii) of Proposition 5.1. Indeed, we have \(k := 2s + |I| \leq O(sN^2)\), and in view of (2.5) we may take \(d^{**} = d\) and \(h^{**} = h\). \(\square\)

Put \(B := A_0[w, f^{-1}]\). Then we clearly have \(A \subseteq B \subseteq K\). Recall that for a fixed \(i \in \{1, \ldots, q\}\) in Section 5.2 we introduced the notation

\[
\begin{align*}
k_i &:= \mathbb{Q}(z_1, \ldots, z_{i-1}, z_{i+1}, \ldots, z_q), \\
\mathbb{K}_i &:= \text{the algebraic closure of } \mathbb{K}_i, \\
M_i &:= \mathbb{K}_i(z_i, w^{(1)}, \ldots, w^{(D)}), \\
B_i &:= \mathbb{K}_i[z_i, f^{-1}, w^{(1)}, \ldots, w^{(D)}],
\end{align*}
\]

(7.3)
where \( w \) is the element specified in Proposition 5.1 and \( w^{(1)}, \ldots, w^{(D)} \) denote the conjugates of \( w \) over \( K_0 \). Further, we used the notation

\[
\Delta_i := [M_i : \bar{K}_i(z_i)],
\]

\[
g_{M_i} := \text{the genus of } M_i/\bar{K}_i,\]

\[
H_{M_i} := \text{the height with respect to } M_i/\bar{K}_i.
\]

Let \( \mathcal{M}_{M_i} \) denote the set of places of \( M_i \) and define

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

Then we have the estimates

\[
|S_i| \leq \Delta_i + \Delta_i \deg_{z_i} f \leq \Delta_i(1 + \deg f)
\]

\[
\leq \Delta_i sN^2(2d)^{\exp O(r)},
\]

and

\[
g_{M_i} \leq \Delta_i D \max_{1 \leq k \leq D} \deg_{z_i} F_k \leq \Delta_i D(2d_0)^{\exp O(r)} \leq \Delta_i(2d)^{\exp O(r)}.
\]

Let \( x, y \) be such that \( F(x, y) = 0 \) and \( x^m, y^m \in \Gamma \) and put \( \tilde{M}_i := M_i(x, y) \). Denote by \( \tilde{S}_i \) the set of places of \( M_i \) lying above places of \( S_i \) and denote by \( g_{\tilde{M}_i} \) the genus of the extension \( \tilde{M}_i/k_i \). By (6.1) we clearly have

\[
[\tilde{M}_i : M_i] \leq 22N^2.
\]

Now we wish to bound \( g_{\tilde{M}_i} \) and \( |\tilde{S}_i| \). By the Riemann-Hurwitz formula we have

\[
2g_{\tilde{M}_i} - 2 = [\tilde{M}_i : M_i] \cdot (2g_{M_i} - 2) + \sum_{v \in \mathcal{M}_{\tilde{M}_i}} \sum_{V \mid v} (e(V \mid v) - 1).
\]

The valuations \( v \not\in S_i \) do not ramify, i.e. \( e(V \mid v) = 1 \) for \( V \) above \( v \), hence

\[
2g_{\tilde{M}_i} - 2 = [\tilde{M}_i : M_i] \cdot (2g_{M_i} - 2) + \sum_{v \in S_i} \sum_{V \mid v} (e(V \mid v) - 1)
\]

\[
= [\tilde{M}_i : M_i] \cdot (2g_{M_i} - 2) + \sum_{v \in S_i} [\tilde{M}_i : M_i] - |\tilde{S}_i|
\]

\[
= [\tilde{M}_i : M_i] \cdot (2g_{M_i} - 2) + |S_i|[\tilde{M}_i : M_i] - |\tilde{S}_i|.
\]

This gives us

\[
2g_{\tilde{M}_i} + |\tilde{S}_i| = [\tilde{M}_i : M_i] \cdot (2g_{M_i} - 2 + |S_i|) + 2,
\]

which provides at the same time the upper bounds for \( g_{\tilde{M}_i} \) and \( |\tilde{S}_i| \) given below:

\[
g_{\tilde{M}_i} \leq 22N^2(2g_{M_i} + |S_i|) \leq \Delta_i sN^4(2d)^{\exp O(r)},
\]
and similarly,
\[(7.9) \quad |\tilde{S}_i| \leq \Delta_i s N^4 (2d)^{\exp O(r)}.
\]

We will use Proposition 4.2 to bound \(H_{\tilde{M}_i}(x)\) and \(H_{\tilde{M}_i}(y)\) by
\[(7.10) \quad H_{\tilde{M}_i}(x), H_{\tilde{M}_i}(y) \leq 2N \left[ (N + 1)^4 (|\tilde{S}_i| + g_{\tilde{M}_i}) + 2H_0 \right],
\]
where \(H_0\) is an upper bound for \(H_{\tilde{M}_i}(a^{(j)}_{uv})\). By Lemma 5.6 and by (5.13) we get
\[
H_{\tilde{M}_i}(a^{(j)}_{uv}) \leq [\tilde{M}_i : M_i] \cdot \left( 2D \deg a_{uv} + (2d_0)^{\exp O(r)} \right)
\leq 22N^2 \Delta_i (2d)^{\exp O(r)} \leq N^2 \Delta_i (2d)^{\exp O(r)} =: H_0
\]
This together with (7.10) provides the estimate
\[(7.11) \quad H_{\tilde{M}_i}(x), H_{\tilde{M}_i}(y) \leq \Delta_i s N^9 (2d)^{\exp O(r)},
\]
which together with (2.7) proves
\[
H_{\tilde{M}_i}(x_0) = H_{\tilde{M}_i}(x^m) \leq mH_{\tilde{M}_i}(x) \leq \Delta_i \exp \left\{ N^6 (2d)^{\exp O(r+s)} (h + 1)^{4s} \right\},
\]
and the same bound for \(H_{\tilde{M}_i}(y_0)\). Now using \(H_{\tilde{M}_i}(x_0) = [\tilde{M}_i : M_i] \cdot H_{M_i}(x_0)\) and \(H_{\tilde{M}_i}(y_0) = [\tilde{M}_i : M_i] \cdot H_{M_i}(y_0)\) we obtain
\[
H_{M_i}(x_0), H_{M_i}(y_0) \leq \Delta_i \exp \left\{ N^6 (2d)^{\exp O(r+s)} (h + 1)^{4s} \right\},
\]
which together with Lemma 5.5 proves the desired estimate
\[(7.12) \quad \overline{\deg} x_0, \overline{\deg} y_0 \leq \exp \left\{ N^6 (2d)^{\exp O(r+s)} (h + 1)^{4s} \right\}.
\]

7.2. Preparations for bounding the height.

**Lemma 7.2.** Let \(\mathcal{R}\) be an integral domain, \(H(X) := \sum_{i=0}^n c_i X^i \in \mathcal{R}[X]\) be a polynomial, and \(\rho\) a primitive \(m^{th}\) root of unity. Then we have
\[
\prod_{j=1}^m H(\rho^j X) \in \mathcal{R}[X^m].
\]

**Proof.** There is no loss of generality, to assume that \(\mathcal{R} = \mathbb{Z}[c_0, \ldots, c_n]\), where \(c_0, \ldots, c_n\) are independent variables. Let \(K_c := \overline{\mathbb{Q}}(c_0, \ldots, c_n)\) and \(\overline{K}_c\) the algebraic closure of \(K_c\). We may write
\[
H(X) = c_n \prod_{k=1}^n (X - \alpha_k),
\]
where \( \alpha_1, \ldots, \alpha_n \in \overline{K}_c \). Thus
\[
\prod_{j=0}^{m-1} H(\rho^j X) = c_n^m \prod_{k=1}^n \prod_{j=0}^{m-1} (\rho^j X - \alpha_k) = c_n^m \rho^{nm(m-1)/2} \prod_{k=1}^n (X^m - \rho^{-j} \alpha_k^m)
= c_n^m (-1)^{n(m-1)} \prod_{k=1}^n (X^m - \alpha_k^m).
\]
Since the coefficients of \( \prod_{k=1}^n (X^m - \alpha_k^m) \) are elementary symmetric polynomials with integral coefficients in \( \alpha_i \)'s, they are in fact elements of \( \mathbb{Z}[c_0/c_n, \ldots, c_{n-1}/c_n] \). Hence \( \prod_{j=0}^{m-1} H(\rho^j X) =: G(X^m) \) with \( G \in K_c[X] \).
But the coefficients of \( G \) are integral over \( \mathcal{R} \), and \( \mathcal{R} \) is integrally closed, hence they belong to \( \mathcal{R} \).

**Proposition 7.3.** Let \( \rho \) be a primitive \( m \)th root of unity. Then there exists a polynomial \( G(U, V) = \sum_{(i, j) \in J} b_{ij} U^i V^j \in A[U, V] \) with \( b_{ij} \neq 0 \) for \( (i, j) \in J \), such that
\[
(7.13) \quad G(X^m, Y^m) = \prod_{k=0}^{m-1} \prod_{l=0}^{m-1} F(\rho^k X, \rho^l Y),
\]
and such that the coefficients \( b_{ij} \) of \( G \) have representatives \( \tilde{b}_{ij} \) with
\[
(7.14) \quad \deg \tilde{b}_{ij} \leq m^2 d, \quad h(\tilde{b}_{ij}) \leq m^2 (h + 2 \log(N + 1))
\]

**Proof.** Put \( R_0 := \mathbb{Z}[a_{pq} : (p, q) \in I] \), where we adjoin all coefficients \( a_{pq} \) of \( p, q \in I \) to \( \mathbb{Z} \). First we consider the polynomial \( H(X, Y) := \prod_{l=0}^{m-1} F(X, \rho^l Y) \) as a polynomial in one variable (namely in \( Y \)) over the integral domain \( R := R_0[X] \). Then by Lemma 7.2 we see that \( H(X, Y) \in R[Y^m] \). Using again Lemma 7.2 for the polynomial
\[
\prod_{k=0}^{m-1} \prod_{l=0}^{m-1} F(\rho^k X, \rho^l Y) = \prod_{k=0}^{m-1} H(\rho^k X, Y),
\]
and the ring \( R_1 := R_0[Y^m] \) we infer that
\[
\prod_{k=0}^{m-1} \prod_{l=0}^{m-1} F(\rho^k X, \rho^l Y) \in R_0[X^m, Y^m],
\]
so we clearly have \( \prod_{k=0}^{m-1} \prod_{l=0}^{m-1} F(\rho^k X, \rho^l Y) \in A[X^m, Y^m] \), thus the existence of a polynomial \( G(U, V) \in A[U, V] \) with (7.13) is proved.

Now we have to prove the estimates for the coefficients of \( G \). Recall that \( F(X, Y) = \sum_{(p, q) \in I} a_{pq} X^p Y^q \), and by assumption (see (2.5)) we are given representatives \( \tilde{a}_{pq} \) such that
\[
\deg \tilde{a}_{pq} \leq d, \quad h(\tilde{a}_{pq}) \leq h.
\]
Put
\[
\tilde{F}_{kl} := \tilde{F}(\rho^k X, \rho^l Y).
\]
For a polynomial $F$ with complex coefficients let us denote by $||F||_1$ the one-norm of $F$, i.e. the sum of the absolute values of the coefficients of $F$.

Then we have

$$||\tilde{F}_{kl}||_1 = ||\tilde{F}||_1 = \sum_{(p,q) \in I} ||\tilde{a}_{pq}||_1$$

and

$$||\tilde{G}||_1 \leq \prod_{k=0}^{m-1} \prod_{l=0}^{m-1} ||\tilde{F}_{kl}||_1 \leq ||\tilde{F}||_1^m.$$ 

This shows that

$$h(\tilde{G}) \leq m^2 \log ||F||_1 \leq m^2(h(\tilde{F}) + \log |I|) \leq m^2(h + 2 \log(N + 1)),$$

and this proves

$$h(\tilde{b}_{ij}) \leq m^2(h + 2 \log(N + 1)).$$

Further, the coefficient $b_{kl}$ is a sum of products of the terms $a_{pq}$, each summand consisting of at most $m^2$ multiplicands, so we have

$$\deg \tilde{b}_{ij} \leq m^2d.$$ 

□

**Lemma 7.4.** Let $G(X,Y)$ be the polynomial defined in Proposition 7.3. Then $G(X,Y)$ is divisible by a non-constant polynomial of the form $X^aY^b - \alpha$ or $X^a - \alpha Y^b$ with $\alpha \in \mathbb{K}^*$, $a, b \in \mathbb{Z}_{\geq 0}$ if and only if $F(X,Y)$ is divisible by a non-constant polynomial of the form $X^uY^v - \beta$ or $X^u - \beta Y^v$ with $\beta \in \mathbb{K}^*$, $u, v \in \mathbb{Z}_{\geq 0}$.

**Proof.** Clearly we may assume $\gcd(a, b) = 1$, otherwise we factorize $X^aY^b - \alpha$ or $X^a - \alpha Y^b$ and we get a similar factor of $G$ with the property $(a, b) = 1$. Then $X^a Y^b - \alpha$ or $X^a - \alpha Y^b$ divides $G(X^m, Y^m)$, which also means that $X^aY^b - \alpha'$ or $X^a - \alpha' Y^b$ divides $G(X^m, Y^m)$ with a suitable $\alpha' \in \mathbb{K}^*$. However, by $\gcd(a, b) = 1$ we know that $X^aY^b - \alpha'$ or $X^a - \alpha' Y^b$ is absolutely irreducible, so if it divides $G(X^m, Y^m)$ then it divides one of $F_{kl}(X,Y)$, but this means that $\rho^{-ka} X \rho^{-lb} Y - \alpha'$ or $\rho^{-ka} X - \alpha' \rho^{-lb} Y$ divides $F(X,Y)$. The converse is trivial, so this concludes the proof of the Lemma.

□

**Lemma 7.5.** The set $C_1$ defined in (3.1) is equal to the set

$$(7.15) \quad \{ (x_0, y_0) \in \Gamma^2 \mid G(x_0, y_0) = 0 \}.$$

**Proof.** Denote the set in (7.15) by $C_2$. If $(x_0, y_0) \in C_1$ then there exist $x, y \in \Gamma$ with $x^m = x_0$, $y^m = y_0$ such that $F(x, y) = 0$. So clearly

$$0 = \prod_{k=0}^{m-1} \prod_{l=0}^{m-1} F(\rho^k x, \rho^l y) = G(x^m, y^m) = G(x_0, y_0),$$

thus $(x_0, y_0) \in C_2$. 

□
Conversely, if \((x_0, y_0) \in C_2\) then we have \(G(x_0, y_0) = 0\). All the \(m\)th roots of \(x_0\) and \(y_0\) are zeros of the polynomials

\[
X^m - x_0 = \prod_{k=0}^{m-1} (X - \rho^k x_0^{1/m})
\]

and

\[
X^m - y_0 = \prod_{l=0}^{m-1} (X - \rho^l y_0^{1/m}),
\]

respectively, with any fixed choice \(x_0^{1/m}\) and \(y_0^{1/m}\) of an \(m\)th roots of \(x_0\) and \(y_0\). Then we have

\[
\prod_{k=0}^{m-1} \prod_{l=0}^{m-1} F_{kl} \left( x_0^{1/m}, y_0^{1/m} \right) = G \left( (x_0^{1/m})^m, (y_0^{1/m})^m \right) = 0,
\]

so there exist \(k, l \in \{0, \ldots, m-1\}\) with

\[
F_{kl} \left( x_0^{1/m}, y_0^{1/m} \right) = 0,
\]

i.e. we have

\[
F \left( \rho^k x_0^{1/m}, \rho^l y_0^{1/m} \right) = 0.
\]

Thus by the choice \(x = \rho^k x_0^{1/m}\) and \(y = \rho^l y_0^{1/m}\) there exist \(x, y \in \Gamma\) with \(x^m = x_0\), \(y^m = y_0\) and \(F(x, y) = 0\), however these conditions just mean that \((x_0, y_0) \in C_1\). This concludes the proof of our Lemma. \(\square\)

### 7.3. Bounding the height of elements of \(C_1\).

Now we will use the specialization method to bound \(h(x_0), h(y_0)\) for any \((x_0, y_0) \in C_1\). More precisely, we prove

**Proposition 7.6.** If \((x_0, y_0) \in C_1\) then we have

\[
(7.16) \quad \overline{\deg} x_0, \overline{\deg} y_0 \leq \exp \left\{ N^6(2d)^{\exp O(r+s)}(h+1)^4s \right\}
\]

\[
(7.17) \quad \overline{h}(x_0), \overline{h}(y_0) \leq \exp \left\{ \exp \left\{ N^{12}(2d)^{\exp O(r+s)}(h+1)^8s \right\}\right\}
\]

This sub-section is devoted to the proof of Proposition 7.6. Recall that the coefficients \(b_{ij}\) of \(G\) have representatives \(\tilde{b}_{ij}\) with

\[
\deg \tilde{b}_{ij} \leq m^2d, \quad h(\tilde{b}_{ij}) \leq m^2(h + 2 \log(N + 1)).
\]

Thus by Lemma 5.3 and by (2.7) we have

\[
(7.18) \quad \overline{\deg} b_{ij}, \overline{h}(b_{ij}) \leq \exp \left\{ N^6(2d)^{\exp O(r+s)}(h+1)^4s \right\}.
\]

Again, we have to extend the domain \(A\) to a larger domain. For this, we use a suitable version of Proposition 5.2. More precisely we have
**Proposition 7.7.** Let \( R \in A \) be an arbitrary non-zero element having a representative \( \bar{R} \) with the property

\[
\deg \bar{R}, h(\bar{R}) \leq \exp \left\{ N^{12}(2d)^{\exp O(r+s)}(h + 1)^{8s} \right\}.
\]

Then there exists a non-zero \( f \in A_0 \) such that for \( B := A_0[w, f^{-1}] \)

\[
A \subseteq B,
\]

\[
\gamma_{i1}, \gamma_{i2} \in B^* \quad \text{for } i = 1, \ldots, s,
\]

\[
b_{ij} \in B^* \quad \text{for } (i, j) \in \mathcal{J},
\]

\[
R \in B^*.
\]

Further, \( f \) can be chosen such that it fulfills

\[
\deg f, h(f) \leq \exp \left\{ N^{12}(2d)^{\exp O(r+s)}(h + 1)^{8s} \right\}.
\]

**Proof.** This is a variant of Proposition 5.2. We clearly know that the \( \deg \) and \( h \) of the elements \( \gamma_{i1}, \gamma_{i2} \in A_0[w, f^{-1}]^* \) for \( i = 1, \ldots, s, b_{ij} \in A_0[w, f^{-1}]^* \) for \( (i, j) \in \mathcal{J}, \) and \( R \in A_0[w, f^{-1}]^* \) are bounded by

\[
\exp \left\{ N^{12}(2d)^{\exp O(r+s)}(h + 1)^{8s} \right\}.
\]

thus by Proposition 5.2 the estimate (7.21) follows at once. \( \square \)

The element \( R \in A \) in the above Proposition will be specified later during the proof, and will be chosen such that it fulfills condition (7.19).

**Proof of Proposition 7.6.** For the case \( q = 0 \) we are in the number field case, and for this case much better bounds are provided by [5], so we may assume \( q > 0. \)

Estimate (7.16) is the same as (7.12). Now we prove the estimate (7.17) using the specialization method described in Section 5.3.

Let \( \mathcal{P} \) be a fixed partition of \( \mathcal{J} \) and \( (x_0, y_0) \in C_2 \) be a fixed solution associated with \( \mathcal{P}. \)

Put \( B := A_0[w, f^{-1}] \). Then for the quantities \( d_0^*, d_1^*, h_0^*, h_1^* \) defined in (5.19) we have the following estimates:

\[
d_0^* \leq (2d)^{\exp O(r)},
\]

\[
h_0^* \leq (2d)^{\exp O(r)}(h + 1),
\]

\[
d_1^*, h_1^* \leq \exp \left\{ N^{12}(2d)^{\exp O(r+s)}(h + 1)^{8s} \right\}.
\]

Thus for \( \mathcal{H} := \Delta_{\mathcal{F}} \cdot \mathcal{F}_D \cdot f \in A_0 \) we have

\[
\deg \mathcal{H} \leq (2D - 2)d_0^* + d_0^* + d_1^* \leq \exp \left\{ N^{12}(2d)^{\exp O(r+s)}(h + 1)^{8s} \right\}.
\]
We shall choose \( u \in \mathbb{Z}^q \) such that \( H(u) \neq 0 \) and consider the extended specializations \( \varphi_{u,k} \) defined in (5.22). Then we have

\[
\varphi_{u,k}(x_0) = x_0^{(k)}(u), \quad \varphi_{u,k}(y_0) = y_0^{(k)}(u),
\]

(7.23)

\[ \varphi_{u,k}(b_{ij}) = b_{ij}^{(k)}(u) \quad \text{for } (i,j) \in I. \]

Later we shall specify some further requirements on \( u \) and \( k \) to be able to apply Lemma 5.9.

The polynomial \( G(X,Y) \) is mapped by \( \varphi_{u,k} \) to the polynomial

\[
G_{u,k}(X,Y) := \sum_{(i,j) \in J} b_{ij}^{(k)}(u)X^iY^j.
\]

(7.24) Let \( K_{u,k} \) be the field defined in (5.26), and \( S_{u,k} \) the set of places of \( K_{u,k} \) containing all infinite places and those finite places which lie above prime ideals dividing \( f(u) \). Since we clearly have

\[
\varphi_{u,k}(\Gamma) \subseteq \varphi_{u,k}(B^*) \subseteq O_{S_{u,k}}^*,
\]

from (7.22) in Lemma 5.9 we may choose

\[
N_0 \leq \exp \left\{ N^{12}(2d)^{\exp O(r+s)}(h+1)^{8s} \right\}
\]

to infer that the set

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

is non-empty. Put

\[
H_1 := \max\{ h_{\text{abs}}(x_0^{(k)}(u)), h_{\text{abs}}(y_0^{(k)}(u)) : u \in S, \ k = 1, \ldots, D \}.
\]

Then using (7.22) and Lemma 5.9 we infer

\[
\overline{h}(x_0), \overline{h}(y_0) \leq \exp \left\{ N^{12}(2d)^{\exp O(r+s)}(h+1)^{8s} \right\} H_1.
\]

(7.25) The last step is to estimate \( H_1 \). Fix any \( u \in S \) and \( k = 1, \ldots, D \). First using Lemma 5.7 and (7.22) we can estimate the parameters of the field \( K_{u,k} \):

\[
|\Delta_{K_{u,k}}| \leq D^{2D-1} \left( (d_0^*)^q e^{h_0^*} \max(1, |u|^{d_0^*}) \right)^{2D-2}
\]

(7.26)

\[
\leq \exp \left\{ N^{12}(2d)^{\exp O(r+s)}(h+1)^{8s} \right\},
\]

and \([K_{u,k} : \mathbb{Q}] \leq D\).

To bound \( h_{\text{abs}}(G_{u,k}) \) we first have to estimate the height of its coefficients. Lemma 5.8 together with (7.18) gives

\[
h_{\text{abs}} \left( b_{ij}^{(k)}(u) \right) \leq \exp \left\{ N^{6}(2d)^{\exp O(r+s)}(h+1)^{4s} \right\}.
\]
This leads to the estimate
\[
    h_{\text{abs}}(G_{u,k}) \leq n(G) \cdot \max h\left(b_{ij}^{(k)}(u)\right) \\
    \leq \exp\left\{N^6(2d)^{\exp O(r+s)}(h+1)^{4s}\right\}.
\]
(7.27)

To bound the cardinality of $S_{K_{u,k}}$ first we estimate
\[
    |f(u)| \leq (\deg f)^q \cdot e^{h(f)} \cdot (\max(1, |u|))^{\deg f} \leq (d_1^* q)^i \cdot e^{h_1^*} \cdot (\max(1, |u|))^{d_1^*} \\
    \leq \exp\left\{\exp\left\{N^{12}(2d)^{\exp O(r+s)}(h+1)^{8s}\right\}\right\}.
\]
(7.28)

Since $s := |S_{K_{u,j}}| \leq D(1 + \omega(f(u)))$, where $\omega(f(u))$ denotes the number of distinct prime factors of $f(u)$, we get
\[
    s \leq O \left( d^r \log^* |f(u)|/\log^* \log^* |f(u)| \right) \\
    \leq \exp\left\{\exp\left\{N^{12}(2d)^{\exp O(r+s)}(h+1)^{8s}\right\}\right\}.
\]
(7.29)

For the maximum of the norm of the prime ideals belonging to $S_{K_{u,k}}$ we have
\[
    P \leq |f(u)|^D \leq \exp\left\{\exp\left\{N^{12}(2d)^{\exp O(r+s)}(h+1)^{8s}\right\}\right\}.
\]
(7.30)

Now in order to be able to use Proposition 4.3 for the equation (7.24) we have to prove that the polynomial $G_{u,k}$ fulfills the condition
\[
    G_{u,l} \text{ is not divisible by } \text{any non-constant polynomial of the form } X^mY^n - \alpha \quad \text{or} \quad X^m - \alpha Y^n, \quad \text{where} \ m, n \in \mathbb{Z}_{\geq 0} \quad \text{and} \quad \alpha \in K_{u,l}.
\]

The coefficients $b_{ij}$ of $G$ are units in $B$, thus all these coefficients are mapped to non-zero elements $b_{ij}^{(l)}(u)$ by the specialization $\varphi_{u,l}$. Thus the partitions of the polynomial $G$ are just the same as the partitions of the polynomial $G_{u,l}$.

If $r(G, \mathcal{P}) = 2$ then we also have $r(G_{u,k}, \mathcal{P}) = 2$. Further, if $r(G, \mathcal{P}) = 1$ then we also have $r(G_{u,k}, \mathcal{P}) = 1$, and by Proposition 4.4 the corresponding system of polynomials $g_1, \ldots, g_k$ (see Section 4.3) has the property $\gcd(g_1, \ldots, g_k) = 1$ in $K[X]$. Thus there exist polynomials $u_1, \ldots, u_k$ and a non-zero constant $R \in A$ with
\[
    u_1g_1 + \cdots + u_kg_k = R,
\]
(7.31)

and by Lemma 4.6 we see that $R$ can be chosen such that it has a representative $\tilde{R}$ with
\[
    \deg \tilde{R}, h(\tilde{R}) \leq \exp\left\{N^{12}(2d)^{\exp O(r+s)}(h+1)^{8s}\right\}.
\]

Assume that $f \in A_0$ and the domain $B$ are chosen in Proposition 7.7 such that $R \in B^*$. Now apply the specialization $\varphi_{u,k}$ to the relation (7.31)
to infer that
\[(u_1)_{u,k}(g_1)_{u,k} + \cdots + (u_k)_{u,k}(g_k)_{u,k} = R^{(k)}_{u}\].

Since \(R \in B^*\) we have \(R^{(k)}_{u} \neq 0\), and we see that \(\gcd((g_1)_{u,k}, \ldots, (g_k)_{u,k}) = 1\) in \(K_{u,k}[X]\). However, the above argument by Proposition 4.4 implies that \(G_{u,k}\) fulfills (7.30).

So the polynomial \(G_{u,k}\) cannot have any non-constant factor of the shape \(aX^mY^n - b\) or \(aX^m - bY^n\) for some \(a, b \in \mathbb{Q}\), \(m, n \in \mathbb{Z}_{\geq 0}\). Thus the solution set of equation (7.24) fulfills the conditions of Proposition 4.3, so combining this by statements (7.27), (7.28), (7.29), (7.26) and \([K_{u,k} : \mathbb{Q}] \leq D\) we get the estimate
\[h_{\text{abs}}(x_0^{(k)}(u), h_{\text{abs}}(y_0^{(k)}(u)) \leq \exp\left\{ \exp\left\{ N^{12}(2d)\exp \left( O(r+s) (h+1)^9s \right) \right\} \right\},\]
for every \(u \in S\) and \(k = 1, \ldots, D\), which provides the same upper bound for \(H_1\). Now combining this latter estimate with (7.25) we get the desired bound (7.17). This concludes the proof of Proposition 7.6.

\[\square\]

7.4. Concluding the proof of Proposition 3.2. Now Proposition 7.6 also provides upper bounds for the heights of elements of the set \(C_1\). So for any \((x_0, y_0) \in C_1\) we have
\[\overline{\deg} x_0, \overline{\deg} y_0 \leq \exp\left\{ N^6(2d)\exp \left( O(r+s) (h+1)^9s \right) \right\},\]
and
\[\overline{h}(x_0), \overline{h}(y_0) \leq \exp\left\{ \exp\left\{ N^{12}(2d)\exp \left( O(r+s) (h+1)^9s \right) \right\} \right\},\]
which by Lemma 5.4 concludes the proof of our Proposition 3.2.

Acknowledgements. The author would like to thank Jan-Hendrik Evertse for his kind help and useful comments.

References


Attila Bérczes
Institute of Mathematics
University of Debrecen
H-4010 Debrecen P.O. Box 12, Hungary
E-mail: berczes@science.unideb.hu