Heights and logarithmic gcd on algebraic curves

Mourad Abouzaid (Université Bordeaux 1)

December 22, 2006

Abstract

Let $F(x,y)$ be an irreducible polynomial over $\mathbb{Q}$, satisfying $F(0,0)=0$. Skolem (1929) proved that the integral solutions of $F(x,y)=0$ with fixed gcd are bounded and Walsh (1992) gave an explicit bound in terms of $d=\gcd(x,y)$ and F. Assuming that $(0,0)$ is a non-singular point of the plane curve $F(x,y)=0$, we extend this result to **algebraic** solution, and obtain an **asymptotic equality** instead of inequality. We show that for any algebraic solution (α,β), the quotient $h(\alpha)/\log d$ is approximatively equal to $\deg_y F$ and the quotient $h(\beta)/\log d$ to $\deg_x F$; here $h(\cdot)$ is the absolute logarithmic height and d is the (properly defined) "greatest common divisor" of α and β.

1 Introduction

In 1929, Skolem [13] (see also [12, page 90]) proved, using a method of Runge that if $F(x,y)$ is an irreducible polynomial with integral coefficients satisfying $F(0,0)=0$, the equation $F(x,y)=0$ has only finitely many solutions $(x,y)\in\mathbb{Z}$ with bounded $\gcd(x,y)$. Unfortunately, Skolem's result was overshadowed by the seminal theorem of Siegel [11], proved the same year: the equation $F(x,y)=0$ has only finitely many solutions unless the plane curve defined by this equation is rational.

Still, Skolem's approach, when it applies, has an important advantage. While the argument of Siegel is ineffective, that is, it does not imply any explicit bound for the solutions of our equation, the method of Skolem allows one, in principle, to bound the solutions with $\gcd(x,y)=d$ explicitly in terms of the polynomial F and the number d.

Indeed, in 1992, P. G. Walsh [16, Theorem 2, p. 159] gave an explicit version of Skolem's result. He proved that if F is a polynomial as above, then the solutions of $F(x,y)=0$ with $\gcd(x,y)=d$ satisfy

$$|x|\leqslant (m^6n^6(m+1)^{n-1}d^{mn}H^n)^{2m^6n^6}$$

and similarly for y. Here m and n are the degrees of F in x and y, respectively, and H is the maximum of absolute values of the coefficients of F. In the special case when F defines a plane curve of genus 0 and $(0,0)$ is a non-singular point of this curve, D. Poulakis [9] slightly refined the estimate of Walsh, proving that the solutions were bounded by $c(m,n)d^{2n}H^{230m^2n^6}$,

In this paper, we improve on the work of Walsh and Poulakis in two directions. First of all, we show that, with a suitable generalization of the notion of gcd, the assertion holds for a polynomial with any algebraic coefficients and for algebraic solutions x,y, not just for the solutions in rational integers. (In [2, p. 305], Bombieri gives such a generalization of Runge's Theorem about homogeneous polynomials in $\mathbb{Z}[x,y]$.)

Second, we not only estimate x and y in terms of d (and F), but we obtain a sort of asymptotic equality when $h(\alpha)$ tends to infinity. For instance, our Theorem 1.3 implies that in the particular case $x,y\in\mathbb{Z}$ we have $\log|x|$ approximately equal to $n\log d$ and $\log|y|$ to $m\log d$.

We do not make any restriction on the genus of the curve given by F but, to simplify some arguments, we assume that $(0,0)$ is a non-singular point of our curve. But this assumption is purely technical: a suitable refinement of our method allows one to drop it, see the end of Subsection 1.2.

Skolem and Walsh used the methods of Runge. Poulakis used a rational parametrization of the genus 0 curve. Our argument is based on the method of Sprindzhuk [14, 15] in the simplified form due to Bilu and Masser [1].

1.1 Definitions

To state our results, we need some definitions. For a number field K we denote by $\mathcal{M}_K$ the set of valuations of K, normalized to extend the standard valuations of $\mathbb{Q}$. That is, if $v \in \mathcal{M}_K$ is an infinite valuation corresponding to a real embedding σ or to a pair of complex conjugate embeddings $\sigma, \overline{\sigma}$, then $|\alpha|_v = |\sigma(\alpha)|$ for $\alpha \in K$, while if v is a finite valuation extending the p-adic valuation of $\mathbb{Q}$, then $|p|_v = 1/p$. With this normalization, we have, for $\alpha \in K^*$, the *product formula*

$$\prod_{v \in \mathcal{M}_K} |\alpha|_v^{[K_v:\mathbb{Q}_v]} = 1$$

where K_v is the completion of K in the v-metric. We will also denote by $\mathcal{M}_K^\infty$ the set of infinite valuations of K and we will denote by $\mathcal{M}_K^0$ the set of finite valuations of K.

Recall the definition of the *Weil height* of an algebraic number. Let α be an algebraic number, and let K be a number field containing α. We define the Weil height of α by

$$h(\alpha) = \sum_{v \in \mathcal{M}_K} \frac{[K_v : \mathbb{Q}_v]}{[K : \mathbb{Q}]} \log \max\{1, |\alpha|_v\}.$$

A standard verification shows that $h(\alpha)$ does not depend on the choice of the field K. Also, the product formula implies that for any $\alpha \in K^*$ we have $h(\alpha) = h(\alpha^{-1})$, that is,

$$h(\alpha) = -\sum_{v \in \mathcal{M}_K} \frac{[K_v : \mathbb{Q}_v]}{[K : \mathbb{Q}]} \log \min\{1, |\alpha|_v\}.$$

For every $v \in \mathcal{M}_K$ we define the "local height" $h_v(\alpha)$ by

$$h_v(\alpha) = -\frac{[K_v : \mathbb{Q}_v]}{[K : \mathbb{Q}]} \log \min\{1, |\alpha|_v\}$$

(with the convention $h_v(0) = -\infty$), so that

$$h(\alpha) = \sum_{v \in \mathcal{M}_K} h_v(\alpha).$$

for $\alpha \in K^*$. We can also define the local height of α associated to a subset S of $\mathcal{M}_K$ by

$$h_S(\alpha) = \sum_{v \in S} h_v(\alpha).$$

Next, we want to extend to arbitrary algebraic numbers the notion of the greatest common divisor. Let α and β be algebraic numbers, and let K be a number field containing them both. We define the *logarithmic gcd* of α and β by

$$\operatorname{lgcd}(\alpha, \beta) = \sum_{v \in \mathcal{M}_K} \min\{h_v(\alpha), h_v(\beta)\}.$$

An easy verification shows that $\operatorname{lgcd}(\alpha, \beta)$ does not depend on the choice of the field K, and that, in the case when α and β are non zero rational integers, it is equal to the logarithm of the usual greatest common divisor:

$$\operatorname{lgcd}(\alpha, \beta) = \log |\gcd(\alpha, \beta)| \qquad (\alpha, \beta \in \mathbb{Z} \backslash \{0\}).$$

To state our main result, we also need the notion of the Weil height of a polynomial. Let $F(x,y)$ be a polynomial with algebraic coefficients, and let K be a number field containing these coefficients. We define the *Weil height* of F by

$$h(F) = \sum_{v \in \mathcal{M}_K} \frac{[K_v : \mathbb{Q}_v]}{[K : \mathbb{Q}]} \log |F|_v,$$

where $|F|_v$ is the maximum of v-absolute values of the coefficients of F. Again, $h(F)$ is independent of the choice of the field K.

1.2 The main theorems

Our main result is the following theorem.

Theorem 1.1 *Let $F(x,y) \in \overline{\mathbb{Q}}[x,y]$ be an absolutely irreducible polynomial with $m = \deg_x F$ and $n = \deg_y F$. Assume that*

$$F(0,0) = 0, \qquad \partial_y F(0,0) \neq 0. \tag{1}$$

Let ε satisfy $0 < \varepsilon \leqslant 1$. Then for all $(\alpha,\beta) \in \overline{\mathbb{Q}}^* \times \overline{\mathbb{Q}}$ such that $F(\alpha,\beta) = 0$ we have either

$$h(\alpha) \leqslant 27mn^5\varepsilon^{-2}h(F) + 171mn^5\varepsilon^{-2}\log(2m+2n) \tag{2}$$

or

$$|h(\alpha) - n\,\mathrm{lgcd}(\alpha,\beta)| \leqslant \varepsilon h(\alpha) + 41n^3\varepsilon^{-1}h(F) + 275n^3\varepsilon^{-1}\log(2m+2n). \tag{3}$$

Let $F(x,y) \in \overline{\mathbb{Q}}[x,y]$ be an absolutely irreducible polynomial and let (α_k,β_k) be a sequence of algebraic points on the plane curve $F(x,y) = 0$. It is well known that, when $h(\alpha_k)$ tends to infinity, we have an asymptotic equality $mh(\alpha_k) \sim nh(\beta_k)$. This property is called **the quasi-equivalence of heights**. As a consequence of Theorem 1.1 we obtain a quantitative version of this property.

Corollary 1.2 *Let $F(x,y) \in \overline{\mathbb{Q}}[x,y]$ be an absolutely irreducible polynomial and let m, n and ε be as in Theorem 1.1. Then for any couple $(\alpha,\beta) \in \overline{\mathbb{Q}}^2$ such that $F(\alpha,\beta) = 0$, we have either*

$$\max\{h(\alpha), h(\beta)\} \leqslant 56M^8\varepsilon^{-2}h(F) + 420M^{10}\varepsilon^{-2}\log(4M), \tag{4}$$

or

$$\left|\frac{h(\alpha)}{n} - \frac{h(\beta)}{m}\right| \leqslant \varepsilon h(\alpha) + 330M^5\varepsilon^{-1}h(F) + 2606M^7\varepsilon^{-1}\log(4M), \tag{5}$$

where $M = \max\{m,n\}$.

Habegger [5] recently suggested another explicit version of quasi-equivalence of heights on a curve.

An obvious disadvantage of Theorem 1.1 is that it is non-symmetric in x and y. Using Corollary 1.2, we obtain the following symmetric statement.

Theorem 1.3 *Let $F(x,y) \in \overline{\mathbb{Q}}[x,y]$ be an absolutely irreducible polynomial such that $(0,0)$ is a non-singular point of the curve $F(x,y) = 0$. Then for any solution $(\alpha,\beta) \in \overline{\mathbb{Q}}^* \times \overline{\mathbb{Q}}$ of $F(x,y) = 0$, we have either (4) holds or*

$$\max\{|h(\alpha) - n\Delta|, |h(\beta) - m\Delta|\} \leqslant \varepsilon h(\alpha) + 742M^7\varepsilon^{-1}h(F) + 5762M^9\varepsilon^{-1}\log(2m+2n), \tag{6}$$

where $\Delta = \mathrm{lgcd}(\alpha,\beta)$ and $M = \max\{m,n\}$.

Remark that by specifying the parameter ε, one can obtain the familiar square root form for the error term in the asymptotic estimates (3), (5) and (6). For instance, in Theorem 1.1, taking

$$\varepsilon = 15\sqrt{\frac{mn^5(h(F)+\log(2m+2n))}{h(\alpha)}},$$

we obtain the following.

Corollary 1.4 *In the set-up of Theorem 1.1, we have either*

$$h(\alpha) \leqslant 225mn^5(h(F)+\log(2m+2n)),$$

or

$$|h(\alpha) - n\mathrm{lgcd}(\alpha,\beta)| \leqslant 40m^{1/2}n^{5/2}\sqrt{h(\alpha)(h(F)+\log(2m+2n))}.$$

One can do similarly for Corollary 1.2 and Theorem 1.3.

We remark in conclusion that the non-singularity assumption can be dropped. In this case $|h(\alpha) - n\mathrm{lgcd}(\alpha,\beta)|$ and $|h(\beta) - m\mathrm{lgcd}(\alpha,\beta)|$ should be replaced by $|rh(\alpha) - n\mathrm{lgcd}(\alpha,\beta)|$ and $|rh(\beta) - m\mathrm{lgcd}(\alpha,\beta)|$ where

$$r = \sum_P \min\left\{\mathrm{ord}_P(x), \mathrm{ord}_P(y)\right\}.$$

Here the sum extends to the algebraic points P of the plain curve $F(x,y) = 0$ with $x(P) = y(P) = 0$. (We have $r = 1$ if and only if $(0,0)$ is a non-singular point.) We plan to pursue this in a forthcoming article.

In Section 2, we recall some classical properties for heights, and some auxiliary results that we will use in the several proofs. In Section 3 we prove Theorem 1.1, and in finale Section 4 we we show how Theorem 1.1 implies a quantitative version of quasi-equivalence of heights (Corollary 1.2) and we obtain a symmetric version of Theorem 1.1 (Theorem 1.3).

2 Auxiliary facts

In this section we state several facts, to be used in the proof of the main theorem.

2.1 Estimates for heights

We begin with the classical property of polynomials, known as *Gauss lemma* in the finite case and *Gelfond's inequality* in the infinite case.

Proposition 2.1 *Let $f_1(x), \dots, f_r(x)$ be polynomials with coefficients in a number field K. Then for any finite valuation $v \in \mathcal{M}_K$ we have*

$$|f_1 \cdots f_r|_v = |f_1|_v \cdots |f_r|_v,$$

and for any infinite $v \in \mathcal{M}_K$ we have

$$e^{-(d_1+\cdots+d_r)}|f_1|_v \cdots |f_r|_v \leqslant |f_1 \cdots f_r|_v \leqslant 2^{d_1+\cdots+d_r}|f_1|_v \cdots |f_r|_v, \tag{7}$$

where $d_i = \deg f_i \qquad (i = 1, \dots, r)$.

Proof The case of finite v is classical; see, for instance, [8, III, Section 2]. For the infinite v, the left-hand side of (7) is the inequality $(*)$ in the proof of Proposition B.7.3 of [6] with $m = 1$ (note that integers d_i in [6] are not exactly the d_i of our proposition). The right-hand side is Proposition B.7.4 (a) in [6] with $n = 1$. □

An easy consequence of Proposition 2.1 is the following estimate for the height of the product of polynomials.

Proposition 2.2 *Let $f_1(x), \dots, f_r(x)$ be polynomials with algebraic coefficients. Then*

$$h(f_1) + \cdots + h(f_r) - (d_1 + \cdots + d_r) \leqslant h(f_1 \cdots f_r) \leqslant h(f_1) + \cdots + h(f_r) + (d_1 + \cdots + d_r) \log 2,$$

where $d_i = \deg f_i$ for $i = 1, \dots, r$).

In particular, if a polynomial $g(x)$ divides a polynomial $f(x)$ then

$$h(g) \leqslant h(f) + \deg f$$

Proof Taking the logarithm, summing up over all the valuations of K, and using the identity

$$\sum_{v \in \mathcal{M}_K^\infty} \frac{[K_v : \mathbb{Q}_v]}{[K : \mathbb{Q}]} = 1,$$

we obtain the result. □

Since the height of an algebraic number α is equal to the height of the polynomial $x - \alpha$, we deduce from Proposition 2.2 the following statement.

Proposition 2.3 *Let $f(x)$ be a polynomial of degree d with algebraic coefficients and let α be a root of f. Then*

$$h(\alpha) \leqslant h(f) + d.$$

In this paper, we will also need to estimate the height of the resultant of two polynomials.

Proposition 2.4 *Let $F_1(x, y)$ and $F_2(x, y)$ be polynomials with algebraic coefficients, and let $R(x)$ be their resultant with respect to the variable y. Put*

$$m_i = \deg_x F_i, \quad n_i = \deg_y F_i \qquad (i = 1, 2).$$

Then

$$h(R) \leqslant n_1 h(F_2) + n_2 h(F_1) + (m_1 n_2 + m_2 n_1) + (n_1 + n_2) \log(n_1 + n_2).$$

Proof Let K be a number field containing the coefficients of F_1 and of F_2, and write

$$F_i(x, y) = a_{in_i}(x) y^{n_i} + \cdots + a_{i1}(x) y + a_{i0}(x) \qquad (i = 1, 2),$$

where $a_{ik}(x) \in K[x]$. The determinant representation of the resultant (see [7, Chapter IV, Section 8]) implies that $R(x)$ can be written as a sum of $(n_1 + n_2)!$ polynomials in x, each being either 0 or $\pm$ product of n_2 polynomials taken among $a_{1k}(x)$ and n_1 polynomials taken among $a_{2k}(x)$. If, say, $u(x)$ is one such term then Proposition 2.1 implies that

$$|u|_v \leqslant |F_1|_v^{n_2} |F_2|_v^{n_1}$$

for a finite $v \in \mathcal{M}_K$ and

$$|u|_v \leqslant 2^{m_1 n_2 + m_2 n_1} |F_1|_v^{n_2} |F_2|_v^{n_1}$$

for an infinite $v \in \mathcal{M}_K$. It follows that

$$|R|_v \leqslant |F_1|_v^{n_2} |F_2|_v^{n_1}$$

for a finite $v \in \mathcal{M}_K$ and

$$|R|_v \leqslant (n_1+n_2)!2^{m_1n_2+m_2n_1}|F_1|_v^{n_2}|F_2|_v^{n_1}$$

for an infinite $v \in \mathcal{M}_K$. Taking the logarithm and summing up over $v \in \mathcal{M}_K$, we get

$$\begin{aligned} h(R) \leqslant & n_2h(F_1) + n_1h(F_2) + \log((n_1+n_2)!2^{m_1n_2+m_2n_1}) \\ \leqslant & n_2h(F_1) + n_1h(F_2) + (m_1n_2+m_2n_1) + (n_1+n_2)\log(n_1+n_2). \end{aligned}$$ □

Proposition 2.5 *Let $F(x,y) \in \overline{\mathbb{Q}}[x,y]$ be a polynomial with $m = \deg_x F$ and $n = \deg_y F$ and let α, β be two algebraic numbers.*

1. *We have $h(F(\alpha,\beta)) \leqslant h(F) + mh(\alpha) + nh(\beta) + \log((m+1)(n+1))$.*
2. *If $F(\alpha,\beta) = 0$ with $F(\alpha,y)$ not vanishing, then*

$$h(\beta) \leqslant h(F) + mh(\alpha) + n + \log(m+1).$$

3. *Let $F_1(x,y) = F(x+\alpha, y+\beta)$. Then*

$$h(F_1) \leqslant h(F) + mh(\alpha) + nh(\beta) + m + n + \log(m+1) + \log(n+1).$$

Proof Below, we let K be a number field containing the coefficients of F, as well as the numbers α and β.

1. For any $v \in \mathcal{M}_K$ we have

$$|F(\alpha,\beta)|_v \leq |F|_v \max\{1, |\alpha|_v^m\} \max\{1, |\beta|_v^n\}$$

if v is finite, and

$$|F(\alpha,\beta)|_v \leqslant (m+1)(n+1)|F|_v \max\{1, |\alpha|_v^m\} \max\{1, |\beta|_v^n\}$$

if v is infinite. Taking the logarithm and summing up over $\mathcal{M}_K$, we obtain the result.

2. Put $f(y) = F(\alpha, y)$. Then

$$|f|_v \leqslant \begin{cases} |F|_v \max\{1, |\alpha|_v\}^m & \text{if } v \text{ is finite,} \\ (m+1)|F|_v \max\{1, |\alpha|_v\}^m & \text{if } v \text{ is infinite.} \end{cases}$$

This implies that $h(f) \leqslant h(F) + mh(\alpha) + \log(m+1)$. Since β is a root of f, the result follows by Proposition 2.3.

3. Expanding the polynomial F_1, we get

$$F_1(x,y) = \sum_{\substack{0 \leqslant k \leqslant m \\ 0 \leqslant \ell \leqslant n}} \sum_{\substack{k \leqslant i \leqslant m \\ \ell \leqslant j \leqslant n}} a_{ij} \binom{i}{k} \binom{j}{\ell} \alpha^{i-k} \beta^{j-\ell} x^k y^\ell$$

where (a_{ij}) are the coefficients of F. Then

$$|F_1|_v \leqslant \begin{cases} |F|_v \max\{1, |\alpha|_v^m\} \max\{1, |\beta|_v^n\} & \text{if } v \text{ is finite,} \\ (m+1)(n+1)2^{m+n}|F|_v \max\{1, |\alpha|_v^m\} \max\{1, |\beta|_v^n\} & \text{otherwise.} \end{cases}$$

Taking the log and summing over all the places of K, the result follows.

2.2 Eisenstein's theorem

Let K be a number field, and let $F(x,y) \in K[x,y]$ be a polynomial satisfying

$$F(0,0) = 0, \qquad \partial_y F(0,0) \neq 0. \tag{8}$$

By the Theorem of Puiseux, there exists a single power series $Y(x) \in K[[x]]$ satisfying $Y(0) = 0$ and $F(x, Y(x)) = 0$. The coefficients of this series can be estimated using modern numerical versions of Eisenstein's theorem (see, for instance [4]). However, in our special case, much sharper estimates hold than those from [4]. The following statement is the case $a = 0$ of [6, Proposition E.9.1].

Theorem 2.6 *Let K be a number field, and let $F(x,y) \in K[x,y]$ be a polynomial satisfying (8). Put $m = \deg_x F$ and $n = \deg_y F$. Let $Y(x) = \sum_{k\geqslant 1} a_k x^k \in K[[x]]$ be the power series satisfying $F(x, Y(x)) = 0$. Then for each place v of K and for all $k \geqslant 1$, we have*

$$|a_k|_v \leqslant \begin{cases} \dfrac{|F|_v^{2k}}{|\partial_y F(0,0)|_v^{2k}} & \text{if } v \text{ is finite,} \\ (2m+2n)^{11k} \dfrac{|F|_v^{2k}}{|\partial_y F(0,0)|_v^{2k}} & \text{otherwise.} \end{cases} \tag{9}$$

In the set-up of Theorem 2.6, put

$$A_v = \begin{cases} \left(\frac{|F|_v}{|\partial_y F(0,0)|_v}\right)^2 & \text{if } v \text{ is finite,} \\ (2m+2n)^{11} \left(\frac{|F|_v}{|\partial_y F(0,0)|_v}\right)^2 & \text{otherwise,} \end{cases}$$

so that according to Theorem 2.6 for all $k \geqslant 0$ and for all valuation v in $\mathcal{M}_K$ we have

$$|a_k|_v \leqslant A_v^k. \tag{10}$$

Notice that $A_v = 1$ for all place outside of a finite set and that $A_v \geq 1$ for all $v \in \mathcal{M}_K$ (because $\partial_y F(0,0)$ is one of the coefficients of F). Also,

$$\begin{aligned} \sum_{v\in\mathcal{M}_K} \frac{[K_v:\mathbb{Q}_v]}{[K:\mathbb{Q}]} \log A_v =& 2 \sum_{v\in M_k} \frac{[K_v:\mathbb{Q}_v]}{[K:\mathbb{Q}]} \log |F|_v - 2 \sum_{v\in M_k} \frac{[K_v:\mathbb{Q}_v]}{[K:\mathbb{Q}]} \log |\partial_y F(0,0)|_v \\ &+ 11 \log(2m+2n) \\ =& 2h(F) + 11\log(2m+2n). \end{aligned} \tag{11}$$

(The second sum vanishes due to the product formula.) We shall frequently use this relation in the present article, sometimes without special reference.

Proposition 2.7 *Let K be a number field and let $Y(x) = \sum_{k\geqslant 0} a_k x^k$ be a series with coefficients in K. For all $r \in \mathbb{N}^*$, put $Z_r(x) = Y(x)^r = \sum_{k\geqslant 0} b_k^{(r)} x^k$. Assume that for any valuation $v \in \mathcal{M}_K$ there is a real number $A_v \geqslant 1$ such that for all index $k \geqslant 0$ we have $|a_k|_v \leqslant A_v^k$. Then for any valuation v of K and for all index $k \geqslant 0$ we have*

$$|b_k^{(r)}|_v \leqslant \begin{cases} A_v^k & \text{if } v \text{ is finite,} \\ \binom{r+k-1}{k} A_v^k & \text{otherwise.} \end{cases} \tag{12}$$

Proof We prove this by induction in r. For $r = 1$ this is clear. Assume that (12) is true for some $r \in \mathbb{Z}^{\geqslant 1}$. Then

$$Z_{r+1}(x) = Y(x)^{r+1} = \sum_{k \geqslant 0} \left(\sum_{i=0}^{k} a_i b_{k-i}^{(r)} \right) x^k.$$

Then for any finite valuation v we have

$$|b_k^{(r+1)}|_v \leqslant A_v^k$$

and for any infinite valuation v we have

$$|b_k^{(r+1)}|_v \leqslant \sum_{i=0}^{k} |a_i|_v |b_{k-i}^{(r)}|_v \leqslant A_v^k \sum_{i=0}^{k} \binom{r+k-1}{r-1} = \binom{r+k}{r} A_v^k,$$

which is (12) for $r+1$. □

2.3 Absolute Siegel's lemma

We shall also need the *Absolute Siegel's lemma*, due to Roy and Thunder [10]. The following is an adaptation of Theorem 2.2 from [10].

Theorem 2.8 *Let $L_1, ..., L_\mu \in \overline{\mathbb{Q}}[x_1, ..., x_\nu]$ be μ linear forms. There exists a nonzero $\underline{c} \in \overline{\mathbb{Q}}^\nu$ such that*

$$L_1(\underline{c}) = ... = L_\mu(\underline{c}) = 0 \tag{13}$$

and

$$h(\underline{c}) \leqslant (\nu - \mu)^{-1}(h(L_1) + ... + h(L_\mu)) + (\nu - \mu)\log 2.$$

Proof Let V be the subspace of $\overline{\mathbb{Q}}^\nu$ of dimension $d = \nu - \mu$ defined by (13). According to Section 1 of [10], we can define the height of V as follows: if $\dim V = 1$, then $h(V)$ is the height of any non zero element of V. If $\dim V = d > 1$, then $h(V)$ is the height of the d-th exterior power $\bigwedge^d(V)$ which is a one-dimensional space. According to Theorem 1.1 of [10] we have $h(V) = h(V^\perp)$ and lemma 4.7 implies that $h(V^\perp) \leqslant h(L_1) + \cdots + h(L_\mu)$. Theorem 2.2 from [10] then implies that V contains a non-zero vector $\underline{c}$ satisfying

$$h(\underline{c}) \leqslant d^{-1}h(V) + d\log 2 \leqslant d^{-1}(h(L_1) + \cdots + h(L_\mu)) + d\log 2.$$

□

A more precise version of this absolute Siegel's lemma can be deduced from a result of Zhang (see [3, Lemma 4.7.]) but using it would not imply any substantial refinement of our result.

3 Proof of Theorem 1.1

3.1 An auxiliary polynomial

First, with Absolute Siegel's lemma (Theorem 2.8), we construct an auxiliary polynomial with controlled height which order of vanishing at the point $(0, 0)$ is high.

Proposition 3.1 *Let N be a positive integer, and let δ be a real number satisfying $0 < \delta \leq 1$. Then there exists a non-zero polynomial $G(x, y) \in \overline{\mathbb{Q}}$ with $\deg_x G \leqslant N$ and $\deg_y G \leqslant n - 1$ satisfying the following properties:*

$$\mathrm{ord}_x G(x, Y(x)) \geqslant nN(1 - \delta), \tag{14}$$

$$h(G) \leqslant 2nN\delta^{-1}h(F) + 15nN\delta^{-1}\log(2m + 2n). \tag{15}$$

Here $Y(x)$ is the Puiseux expansion defined in Section 2.2.

Proof Write

$$G(x,y) = \sum_{\substack{0\leq i\leq N\\ 0\leq j\leq n-1}} G_{ij}x^i y^j$$

with yet unknown algebraic coefficients G_{ij}. Denote by $\underline{c}$ the $n(N+1)$-dimensional vector of these coefficients, ordered somehow. Then

$$G(x,Y(x)) = \sum_{r=0}^{\infty} L_r(\underline{c})x^r,$$

where

$$L_r = G_{r0} + \sum_{i=0}^{\min\{N,r\}} \sum_{j=1}^{n-1} b_{r-i}^{(j)} G_{ij},$$

the algebraic numbers $b_{r-i}^{(j)}$ being those defined in Proposition 2.7. We view L_r as linear forms in variables G_{ij} with algebraic coefficients. Condition (14) can be stated as

$$L_r(\underline{c}) = 0 \qquad (0 \leqslant r \leqslant nN(1-\delta)). \tag{16}$$

We wish to apply Theorem 2.8 to this system of linear equations in $\underline{c}$. Using Proposition 2.7, we find that for any finite valuation v, we have

$$|L_r|_v = \max_{i,j}\{1, |b_{r-i}^{(j)}|_v\} \leqslant A_v^r \leqslant A_v^{nN},$$

and for any infinite valuation v, we have

$$|L_r|_v = \max_{i,j}\{1, |b_{r-i}^{(j)}|_v\} \leqslant \max_{i,j} \binom{r-i+j-1}{r-i} A_v^r \leqslant 2^{2nN} A_v^{nN},$$

so that by (11) we have

$$h(L_r) \leqslant 2nNh(F) + 13nN\log(2m+2n),$$

for all $0 \leqslant r \leqslant nN(1-\delta) - 1$.

Applying Theorem 2.8, we find a non-zero solution $\underline{c}$ of (16) satisfying

$$h(\underline{c}) \leqslant (n(1+N\delta))^{-1}(h(L_1) + ... + h(L_{\lfloor nN(1-\delta)\rfloor})) + n(1+N\delta)\log 2.$$

This proves the proposition. □

3.2 v-adic convergence and partial height

Let K be a number field containing all the algebraic numbers of the problem and $\mathcal{M}_K$ the set of all the places of K. Let $Y(x) = \sum_{i\geqslant 1} a_k x^k \in K[[x]]$ be The Puiseux series satisfying $F(x,Y(x)) = 0$. Recall that according to Theorem 2.6 we have $|a_k|_v \leqslant A_v^k$ for all $v \in \mathcal{M}_K$ and for all $k \geqslant 1$. Let S be the subset of $\mathcal{M}_K$ defined by

$$S = \left\{ v \in \mathcal{M}_K \ : \ |\alpha|_v \begin{array}{ll} \leqslant & (2A_v)^{-1} \quad \text{if } v \text{ is infinite,} \\ < & A_v^{-1} \quad \text{otherwise.} \end{array} \right\}$$

By (10), for each $v \in S$ the series $\sum a_k \alpha^k$ converges for the v-metric. We will denote by $Y_v(\alpha)$ its sum and set

$$T = \{v \in S, \ Y_v(\alpha) = \beta\}.$$

Lemma 3.2 *We have*

$$h_S(\alpha) \leqslant h(\alpha) \leqslant h_S(\alpha) + 2h(F) + 12\log(2m+2n).$$

Proof By inclusion the first inequality is clear. For the second one, an explicit calculus of $h_{\mathcal{M}_k\setminus S}(\alpha)$ gives us

$$\begin{aligned}
h_{\mathcal{M}_K\setminus S}(\alpha) &= -\sum_{v\in\mathcal{M}_K\setminus S}\frac{[K_v:\mathbb{Q}_v]}{[K:\mathbb{Q}]}\log\min\{1,|\alpha|_v\}\\
&\leqslant \sum_{v\in\mathcal{M}_K^\infty\setminus S}\frac{[K_v:\mathbb{Q}_v]}{[K:\mathbb{Q}]}\log A_v+\sum_{v\in\mathcal{M}_K^0\setminus S}\frac{[K_v:\mathbb{Q}_v]}{[K:\mathbb{Q}]}\log 2A_v\\
&\leqslant \sum_{v\in\mathcal{M}_K}\frac{[K_v:\mathbb{Q}_v]}{[K:\mathbb{Q}]}\log A_v+\log 2\\
&\leqslant 2h(F)+12\log(2m+2n). \qquad \square
\end{aligned}$$

3.3 A bound for $|h(\alpha)-nh_T(\alpha)|$

Proposition 3.3 *Either*

$$h(\alpha)\leqslant 27mn^3\varepsilon^{-2}h(F)+171mn^3\varepsilon^{-2}\log(2m+2n), \tag{17}$$

or

$$nh_T(\alpha)\leqslant(1+\varepsilon)h(\alpha)+32n\varepsilon^{-1}h(F)+230n\varepsilon^{-1}\log(2m+2n). \tag{18}$$

Proof Let N be a positive integer satisfying

$$N\geqslant\max\{m,n\}$$

and let δ satisfy $0<\delta\leqslant 1$, both N and δ to be specified latter. Let $G(x,y)$ be the auxiliary polynomial constructed in Proposition 3.1. By extending the field K we may assume that it contains the coefficients of G. The rest of the proof split into two cases.

The case $G(\alpha,\beta)=0$. Since $F(\alpha,\beta)=0$ as well, the polynomials $F(\alpha,y)$ and $G(\alpha,y)$ have a common root β. Then α is a root of the resultant $R(x)=\mathrm{Res}_y(F(x,y),G(x,y))$ and by Propositions 2.3 and 2.4 we have

$$\begin{aligned}
h(\alpha)\leqslant& h(R)+m(n-1)+nN\\
\leqslant& n(h(F)+h(G))+2(m(n-1)+nN)+(2n-1)\log(2n-1)\\
\leqslant& n(1+2nN\delta^{-1})h(F)+13n^2N\delta^{-1}\log(2m+2n)+4nN+2n\log(2n) \qquad (19)\\
\leqslant& 3n^2N\delta^{-1}h(F)+19n^2N\delta^{-1}\log(2m+2n).
\end{aligned}$$

(We used the condition $N\geqslant m$ for (19)).

The case $G(\alpha,\beta)=\gamma\neq 0$. In this case Proposition 2.5 implies that

$$\begin{aligned}
h(\gamma)\leqslant& h(G)+Nh(\alpha)+(n-1)h(\beta)+\log((N+1)n)\\
\leqslant& (N+(n-1)m)h(\alpha)+3nN\delta^{-1}h(F)+19nN\delta^{-1}\log(2m+2n). \qquad (20)
\end{aligned}$$

On the other side, write

$$Z(x)=G(x,Y(x))=\sum_{k\geqslant nN(1-\delta)}b_kx^k.$$

By Proposition 2.7, for any finite valuation v of K we have

$$|b_k|_v\leqslant|G|_vA_v^k,$$

for all $k \geqslant nN(1-\delta)$. Moreover, if v is a place of S, we have $A_v|\alpha|_v < 1$ so that the series $\sum b_k \alpha^k$ converges in v-metric and its sum $Z_v(\alpha)$ satisfies

$$|Z_v(\alpha)|_v \leqslant |G|_v (A_v|\alpha|_v)^{nN(1-\delta)}$$

and for any infinite valuation v, while $N \geqslant n$ we have

$$|b_k|_v \leqslant |G|_v \sum_{i=0}^{N} \sum_{j=1}^{n-1} |b_{k-i}^{(j)}|_v \leqslant \left(\begin{array}{c} n+k \\ n-1 \end{array} \right) |G|_v A_v^k$$

for all $k \geqslant nN(1-\delta)$. A short computation shows that for any positive integers n and $k \geqslant n$ we have $\left(\begin{array}{c} n+k \\ n-1 \end{array} \right) \leqslant (6k)^n$.

By the definition of the set S, for any infinite $v \in S$ we have $A_v|\alpha|_v \leqslant 1/2$. Hence the series $\sum b_k \alpha^k$ converges in the v-metric and its sum $Z_v(\alpha)$ satisfies

$$\begin{aligned} |Z_v(\alpha)|_v \leqslant & \sum_{k \geqslant nN(1-\delta)} (6k)^n |G|_v (A_v|\alpha|_v)^k \leqslant 6^n |G|_v (A_v|\alpha|_v)^{nN(1-\delta)} \sum_{k \geqslant 0} (k+nN)^n 2^{-k} \\ \leqslant & 4(24n^2N)^n |G|_v (A_v|\alpha|_v)^{nN(1-\delta)}. \end{aligned}$$

Furthermore, for v in the set T defined in Section 3.2, we have $Z_v(\alpha) = G(\alpha, \beta) = \gamma$. Then

$$\begin{aligned} h(\gamma) \geqslant h_T(\gamma) \geqslant & Nn(1-\delta)(h_T(\alpha) - 2h(F)) - h(G) \\ & - 11nN(1-\delta)\log(2m+2n) - \log(4(24n^2N)^n) \\ \geqslant & Nn(1-\delta)h_T(\alpha) - 4nN\delta^{-1}h(F) - 32nN\delta^{-1}\log(2m+2n). \end{aligned}$$

Combining this with (20), we get

$$nh_T(\alpha) \leqslant \frac{1}{1-\delta}\left(1 + \frac{m(n-1)}{N}\right) h(\alpha) + \frac{7n}{\delta(1-\delta)} h(F) + \frac{51n}{\delta(1-\delta)} \log(2m+2n).$$

We can now choose N and δ in order to get the expected bounds. First we choose $\delta = \varepsilon/3$ so that $\delta < 1/3$ and $1 - \delta \geqslant 2/3$. Secondly, to have $\frac{1}{1-\delta}\left(1 + \frac{m(n-1)}{N}\right) \leqslant (1+\varepsilon)$, we must choose $N \geqslant \frac{m(n-1)}{\delta(2-3\delta)}$ so that $n/(N(1-\delta)) \leqslant 2\delta < 1$. Then, if $G(\alpha, \beta) \neq 0$, we have

$$nh_T(\alpha) \leqslant (1+3\delta)h(\alpha) + 21n(2\delta)^{-1}h(F) + 153n(2\delta)^{-1}\log(2m+2n).$$

On the other hand, if $G(\alpha, \beta) = 0$, choosing $N \leqslant mn/\delta$ gives us

$$h(\alpha) \leqslant 27mn^3\varepsilon^{-2}h(F) + 171mn^3\varepsilon^{-2}\log(2m+2n).$$

Note that an integer satisfying the bounds for N is $N = \lfloor mn/\delta \rfloor$ and that it gives the announced bound for $nh_T(\alpha)$. □

Proposition 3.4 *Either* (2) *holds or we have*

$$nh_T(\alpha) \geqslant (1-\varepsilon)h(\alpha) - 34n^3\varepsilon^{-1}h(F) - 242n^3\varepsilon^{-1}\log(2m+2n). \tag{21}$$

Proof Let $\rho(x)$ be the resultant $\mathrm{Res}_y(F(x,y), \partial_y F(x,y))$. If $\rho(\alpha) = 0$, then by Propositions 2.3 et 2.4, we have $h(\alpha) \leqslant n(h(F) + h(\partial_y F)) + 2mn\log 2$. But $h(\partial_y F) \leqslant h(F) + \log n$, so that

$$h(\alpha) \leqslant 2nh(F) + n\log n$$

which is better than (2). We can now assume that $\rho(\alpha)$ is nonzero and we can enlarge the field K so tha the polynomial $F(\alpha, y)$ splits into linear factors. Let us put

$$F(\alpha, y) = A\prod_{i=1}^{n}(y - \beta_i).$$

We can now apply Proposition 3.3 with ε/n instead of ε: let $\beta = \beta_1$ and for i from 1 to n, we put $T_i = \{v \in S,\ \ Y_v(\alpha) = \beta_i\}$. The set T_i form a partition of S so that

$$h_S(\alpha) = h_{T_1}(\alpha) + \cdots + h_{T_n}(\alpha).$$

If (2) is not true then Proposition 3.3 gives

$$nh_{T_i}(\alpha) \leqslant \left(1 + \frac{\varepsilon}{n}\right) h(\alpha) + 32n^2\varepsilon^{-1}h(F) + 230n^2\varepsilon^{-1}\log(2m + 2n)$$

so that by Lemma 3.2 we have

$$\begin{aligned} h_T(\alpha) =& h_S(\alpha) - h_{T_2}(\alpha) - \cdots - h_{T_n}(\alpha) \\ \geqslant& \frac{1-\varepsilon}{n}h(\alpha) - 34n^2\varepsilon^{-1}h(F) - 242n^2\varepsilon^{-1}\log(2m + 2n) \end{aligned}$$

which gives us the wanted bound. □

Combining Propositions 3.3 and 3.4 we get the following propotion:

Proposition 3.5 *Either* (2) *holds or we have*

$$|h(\alpha) - nh_T(\alpha)| \leqslant \varepsilon h(\alpha) + 34n^3\varepsilon^{-1}h(F) + 242n^3\varepsilon^{-1}\log(2m + 2n). \tag{22}$$

3.4 A bound for $|\mathrm{lgcd}(\alpha, \beta) - h_T(\alpha)|$

In this subsection, we prove the following proposition:

Proposition 3.6 *Let F be a polynomial with algebraic coefficients, and let K, m, and n be as in Theorem 1.1. Let also be S and T the subsets of $\mathcal{M}_K$ defined at the begining of Subsection 3.2. Then*

$$|\mathrm{lgcd}(\alpha, \beta) - h_T(\alpha)| \leqslant 7h(F) + 33n\log(2m + 2n).$$

Proof The **lower bound** is relatively easy. Recall first that for every place v in S, we have

$$|\alpha|_v \begin{cases} \leqslant & (2A_v)^{-1} \quad \text{if } v \text{ is infinite,} \\ < & A_v^{-1} \quad \text{if } v \text{ is finite} \end{cases}$$

and the series $\sum a_k\alpha^k$ converges for the v-metric. Hence, if v is infinite, we have

$$|Y_v(\alpha)|_v \leqslant |\alpha|_v \sum_{k\geqslant 1}|a_k|_v|\alpha|_v^{k-1} \leqslant |\alpha|_v \sum_{k\geqslant 1}A_v^k|\alpha|_v^{k-1} \leqslant |\alpha|_v A_v \sum_{k\geqslant 1}2^{1-k} \leqslant 2A_v|\alpha|_v, \tag{23}$$

and

$$|Y_v(\alpha)|_v = |\alpha|_v \left|\sum_{k\geqslant 1}a_k\alpha^{k-1}\right|_v \leqslant |\alpha|_v \max_{k\geqslant 1}|a_k|_v|\alpha|_v^{k-1} \leqslant A_v|\alpha|_v \tag{24}$$

if v is finite. In particular, for any place v in T, we have

$$|\beta|_v \leqslant \begin{cases} 2A_v|\alpha|_v & \text{if } v \text{ is infinite,} \\ A_v|\alpha|_v & \text{otherwise.} \end{cases}$$

Then for any v in T, we have

$$h_v(\beta) \geqslant \begin{cases} h_v(\alpha) - \frac{[K_v:\mathbb{Q}_v]}{[K:\mathbb{Q}]} \log 2A_v & \text{if } v \text{ is infinite,} \\ h_v(\alpha) - \frac{[K_v:\mathbb{Q}_v]}{[K:\mathbb{Q}]} \log A_v & \text{otherwise.} \end{cases}$$

Let us put $\Delta = \operatorname{lgcd}(\alpha, \beta)$. We have

$$\begin{aligned} \Delta &= \sum_{v \in \mathcal{M}_K} \min\{h_v(\alpha), h_v(\beta)\} \geqslant \sum_{v \in T} \min\{h_v(\alpha), h_v(\beta)\} \\ &\geqslant \sum_{v \in T} h_v(\alpha) - \sum_{v \in \mathcal{M}_K^0} \frac{[K_v : \mathbb{Q}_v]}{[K : \mathbb{Q}]} \log(A_v) - \sum_{v \in \mathcal{M}_K^\infty} \frac{[K_v : \mathbb{Q}_v]}{[K : \mathbb{Q}]} \log(2A_v). \end{aligned}$$

This gives us a lower bound for $\Delta - h_T(\alpha)$:

$$\Delta - h_T(\alpha) \geqslant -2h(F) - 12\log(2m + 2n). \tag{25}$$

The upper bound is more advanced. It relies in the following statement.

Proposition 3.7 *In the set-up of Proposition 3.6, there is a partition $S = T \amalg U \amalg V$ such that*

$$\begin{aligned} h_U(\alpha) &\leqslant 4h(F) + 12\log(2m + 2n) + \log(n2^{n+4}) \\ h_V(\beta) &\leqslant h(F) + \log(n2^{n+3}) \end{aligned}$$

To prove this proposition, we need the following lemma.

Lemma 3.8 *Let K be a field with a valuation v and let $f(y) \in K[y]$ be a polynomial of degree n.*

1. *For any root β of f, we have*

$$|\beta|_v \geqslant \begin{cases} \dfrac{|f(0)|_v}{|f|_v} & \text{if } v \text{ is finite,} \\ \dfrac{|f(0)|_v}{n|f|_v} & \text{otherwise.} \end{cases}$$

2. *Let β and γ be two distinct roots of f. Then*

$$\max\{|\beta|_v, |\gamma|_v\} \geqslant c_v(n) \frac{|f'(0)|_v}{|f|_v}$$

where $c_v(n) = \dfrac{1}{(n+1)2^{n+2}}$ if v is infinite, and $c_v(n) = 1$ if v is finite.

Proof

1. Let β be a root of $f(y) = \sum_{i=0}^n b_i y^i$ and let v be a place of K. If $|\beta|_v \geqslant 1$, the result is clear because $f(0)$ is one of the coefficients of f. Let us assume that $|\beta|_v < 1$. Since β is a root of f, we get

$$|f(0)|_v = |b_0|_v = \left| \sum_{i=1}^n b_i \beta^i \right|_v,$$

so that

$$|f(0)|_v \leqslant \begin{cases} |f|_v |\beta|_v & \text{if } v \text{ is finite,} \\ n|f|_v |\beta|_v & \text{otherwise.} \end{cases}$$

2. Let β and γ be two distinct roots of f. If $|\beta|_v \geqslant 1$ this is done. Let us assume that $|\beta|_v < 1$ and let $g(x) = \dfrac{f(x+\beta)}{x}$ which roots are $\beta - \beta_i$ for $i = 2 \dots n$. As in Proposition 2.5, we have

$$|g|_v \leqslant \begin{cases} |f|_v & \text{if } v \text{ is finite,} \\ (n+1)2^n|f|_v & \text{otherwise} \end{cases}$$

Moreover, by the definition of g we have

$$g(0) = f'(0) + \sum_{k=1}^{n-1} \frac{\beta^k}{k!} f^{(k+1)}(0) = f'(0) + \sum_{k=1}^{n-1} (k+1) b_k \beta^k, \tag{26}$$

Let us assume that v is infinite. By (26), we get

$$|f'(0)|_v \leqslant |g(0)|_v + \sum_{k=1}^{n-1} |(k+1)b_k\beta^k|_v \leqslant |g(0)|_v + n^2|f|_v|\beta|_v,$$

so that $|g(0)|_v \geqslant |f'(0)|_v/2$ as soon as $|\beta|_v \leqslant |f'(0)|_v/(2n^2|f|_v)$. Applying the first part of the lemma to polynomial g we get

$$|\gamma - \beta|_v \geqslant \frac{|g(0)|_v}{n|g|_v} \geqslant \frac{1}{(n+1)2^{n+1}} \frac{|f'(0)|_v}{|f|_v}$$

as soon as $|\beta|_v \leqslant |f'(0)|_v/(2n^2|f|_v)$ and

$$|\gamma|_v \geqslant \frac{1}{(n+1)2^{n+2}} \frac{|f'(0)|_v}{|f|_v}$$

if $|\beta|_v \leqslant \dfrac{1}{(n+1)2^{n+2}} \dfrac{|f'(0)|_v}{|f|_v}$.
Similarly, is v is finite, we have

$$|(k+1)\beta^k b_k|_v = |\beta|_v^k |b_k|_v \leqslant |\beta|_v |b_k|_v < |f'(0)|_v \frac{|b_k|_v}{|f|_v} \leqslant |f'(0)|_v,$$

when $|\beta|_v < |f'(0)|_v/|f|_v$. Then $|g(0)|_v = |f'(0)|_v$ and if we apply the first part of the lemma to g once again, we get

$$|\gamma - \beta|_v \geqslant \frac{|g(0)|_v}{|g|_v} \geqslant \frac{|f'(0)|_v}{|f|_v}$$

such that $|\gamma|_v \geqslant |f'(0)|_v/|f|_v$ as soon as $|\beta|_v \leqslant |f'(0)|_v/|f|_v$. □

Proof of Proposition 3.7 . We first define U as the union of two subsets U_1 and U_2 of $S\backslash T$. Let $f(y) = F(\alpha, y)$ and $L = \partial_y F(0,0)$ so that $f'(0) = L + a_{11}\alpha + \cdots + a_{m1}\alpha^m$ and put

$$U_1 = \left\{ v \in S\backslash T \ / \ \begin{array}{ll} |f'(0)|_v \neq |L|_v & \text{if } v \text{ is finite,} \\ |f'(0)|_v \leqslant \frac{|L|_v}{2} & \text{otherwise.} \end{array} \right\}$$

Then for any infinite valuation v in U_1, we have

$$|L|_v = |f'(0) - \sum_{i=1}^{m} a_{i1}\alpha^i|_v \leqslant \frac{|L|_v}{2} + m|\alpha|_v|F|_v,$$

since $|\alpha|_v < 1$. Hence $|L|_v \leqslant 2m|\alpha|_v|F|_v$ and $|\alpha|_v \geqslant \frac{|L|_v}{2m|F|_v}$.

Similarly, for any finite valuation v in U_1, we have

$$|f'(0)|_v \leqslant \max_i\{|L|_v, |a_{i1}\alpha^i|_v\},$$

and this inequality is an equality if the maximum is strict. Since $|f'(0)|_v \neq |L|_v$, for some $i \in \{1,\dots,m\}$, we have $|a_{i1}\alpha^i|_v \geqslant |L|_v$ and then $|\alpha|_v \geqslant \frac{|L|_v}{|F|_v}$. Taking the log and summing up over all the places of U_1 we get

$$h_{U_1}(\alpha) \leqslant h(F) + \log(2m). \tag{27}$$

Furthermore, for any place v in $S\backslash(T\cup U_1)$ we have $|f'(0)|_v = |L|_v$ and $|f|_v \leqslant |F|_v$ if v is finite and $|f'(0)|_v > |L|_v/2$ and $|f|_v \leqslant m|F|_v$ otherwise. We now keep the places of $S\backslash T$ which satisfy $|\beta|_v \leqslant |Y_v(\alpha)|_v$ to build U_2 and we note V the last ones.

By Lemma 3.8, for any place v in U_2 we have $|Y_v(\alpha)|_v \geqslant c_v(n)\frac{|L|_v}{|F|_v}$ and inequalities (23) and (24) give us

$$|\alpha|_v \geqslant \begin{cases} \dfrac{1}{(n+1)2^{n+3}}\dfrac{|L|_v}{A_v|F|_v} & \text{if } v \text{ is infinite,} \\ \dfrac{|L|_v}{A_v|F|_v} & \text{otherwise.} \end{cases}$$

Taking the log and summing up over all the places of U_2 we get

$$h_{U_2}(\alpha) \leqslant h(F) + \sum_{v\in U_2}\frac{[K_v:\mathbb{Q}_v]}{[K:\mathbb{Q}]}\log(A_v) + \log((n+1)2^{n+3}) \leqslant 3h(F) + 15n\log(2m+2n).$$

Similarly, for any place v of V, we have $|\beta|_v \geqslant c_v(n)\frac{|L|_v}{|F|_v}$ and

$$h_V(\beta) \leqslant h(F) + \log(n2^{n+3}) \leqslant h(F) + 5n\log(2m+2n).$$

Writing if $U = U_1 \amalg U_2$ we get

$$h_U(\alpha) = h_{U_1}(\alpha) + h_{U_2}(\alpha) \leqslant 4h(F) + 16n\log(2m+2n),$$

which proves Proposition 3.7. □

Now we are ready to complete the proof of Proposition 3.6. Using the partition $S = T\amalg U\amalg V$, we get:

$$\begin{aligned}\Delta =& \sum_{v\in T}\min\{h_v(\alpha),h_v(\beta)\} + \sum_{v\in U}\min\{h_v(\alpha),h_v(\beta)\} \\ &+ \sum_{v\in V}\min\{h_v(\alpha),h_v(\beta)\} + \sum_{v\in\mathcal{M}_K\backslash S}\min\{h_v(\alpha),h_v(\beta)\} \\ \leqslant& h_T(\alpha) + h_U(\alpha) + h_V(\beta) + h_{\mathcal{M}_K\backslash S}(\alpha) \\ \leqslant& h_T(\alpha) + 7h(F) + 33n\log(2m+2n),\end{aligned}$$

Recall that $h_{\mathcal{M}_K\backslash S}(\alpha)$ was estimated in lemma 3.2. Combined with (25) we get

$$|\Delta - h_T(\alpha)| \leqslant 7h(F) + 33n\log(2m+2n).$$

This proves Proposition 3.6. □

Proof of Theorem 1.1. Combining Propositions 3.5 and 3.6, we obtain that if (2) is not true, then

$$\begin{aligned}|h(\alpha) - n\Delta| \leqslant& |h(\alpha) - nh_T(\alpha)| + n|h_T(\alpha) - \Delta| \\ \leqslant& \varepsilon h(\alpha) + 41n^3\varepsilon^{-1}h(F) + 275n^3\varepsilon^{-1}\log(2m+2n).\end{aligned}$$

Which proves Theorem 1.1. □

4 Quasi-equivalence of heights and symmetrization of Theorem 1.1

4.1 Proof of Corollary 1.2

Let F be as above. We need a "small" solution (α_0, β_0) of $F(x,y)=0$: let $\rho_y(x)$ and $\rho_x(y)$ be respectively the resultants $\mathrm{Res}_y(F, \partial_y F)$ and $\mathrm{Res}_x(F, \partial_x F)$. An algebraic number γ will be called *bad* either if it is a root of $\rho_y(x)$ or if $\rho_x(y)$ and $F(\gamma, y)$ have a common root. There are at most $m(2mn+n+1)$ bad algebraic numbers so that we can choose a good rational integer α_0 with

$$h(\alpha_0) \leqslant \log(m(2mn+n+1)/2+1) \leqslant 2\log(2m+2n). \tag{28}$$

Let $\beta_0 \in \overline{\mathbb{Q}}$ be a root of $F(\alpha_0, y)$. Then by Proposition 2.5, we have

$$h(\beta_0) \leqslant h(F) + mh(\alpha_0) + n + \log(m+1). \tag{29}$$

Now put $F_1(x,y) = F(x+\alpha_0, y+\beta_0)$. By Proposition 2.5, we have

$$\begin{aligned} h(F_1) \leqslant & h(F) + mh(\alpha_0) + nh(\beta_0) + m + n + \log(m+1) + \log(n+1) \\ \leqslant & 2nh(F) + 9mn^2\log(2m+2n). \end{aligned} \tag{30}$$

Now, let $(\alpha, \beta) \in \overline{\mathbb{Q}}^2$ be a solution of the equation $F(x,y)=0$. The polynomial F_1 vanishes in $(\alpha-\alpha_0, \beta-\beta_0)$ and satisfies the hypotheses of Theorem 1.1 with respect both x and y. Then, either one of the two following conditions is satisfied

$$\begin{aligned} h(\alpha-\alpha_0) \leqslant & 27mn^5\varepsilon^{-2}h(F_1) + 171mn^5\varepsilon^{-2}\log(2m+2n) \\ \leqslant & 54mn^6\varepsilon^{-2}h(F) + 414m^2n^7\varepsilon^{-2}\log(2m+2n), \end{aligned} \tag{31}$$

$$\begin{aligned} h(\beta-\beta_0) \leqslant & 27m^5n\varepsilon^{-2}h(F_1) + 171m^5n\varepsilon^{-2}\log(2m+2n) \\ \leqslant & 54m^5n^2\varepsilon^{-2}h(F) + 414m^6n^3\varepsilon^{-2}\log(2m+2n), \end{aligned} \tag{32}$$

or we have

$$\begin{cases} |h(\alpha-\alpha_0) - n\Delta_0| \leqslant \varepsilon h(\alpha-\alpha_0) + 41n^3\varepsilon^{-1}h(F_1) + 275n^3\varepsilon^{-1}\log(2m+2n) \\ |h(\beta-\beta_0) - m\Delta_0| \leqslant \varepsilon h(\beta-\beta_0) + 41m^3\varepsilon^{-1}h(F_1) + 275m^3\varepsilon^{-1}\log(2m+2n), \end{cases} \tag{33}$$

where $\Delta_0 = \mathrm{lgcd}(\alpha-\alpha_0, \beta-\beta_0)$.

But if (32) is true, then by (28), (29) and (30), we get

$$\begin{aligned} h(\beta) \leqslant & h(\beta-\beta_0) + h(\beta_0) + 1 \\ \leqslant & 55m^5n^2\varepsilon^{-2}h(F) + 418m^6n^3\varepsilon^{-2}\log(2m+2n) \end{aligned}$$

and by Proposition 2.5, we have

$$\begin{aligned} h(\alpha) \leqslant & h(F) + nh(\beta) + m + \log(n+1) \\ \leqslant & 56m^5n^3\varepsilon^{-2}h(F) + 420m^6n^4\varepsilon^{-2}\log(2m+2n). \end{aligned}$$

We use the same arguments if (31) holds, in which case the resulting estimates are even slightly better. Thus if one of (31) and (32) holds, then

$$\max\{h(\alpha), h(\beta)\} \leqslant 56M^8\varepsilon^{-2}h(F) + 420M^{10}\varepsilon^{-2}\log(4M),$$

where $M = \max\{m,n\}$.

On the other hand, if (33) is true, then by (28), (29) and (30), we have

$$|h(\alpha-\alpha_0)-n\Delta_0|\leqslant \varepsilon h(\alpha)+82n^4\varepsilon^{-1}h(F)+647mn^5\varepsilon^{-1}\log(2m+2n)$$

and

$$|h(\beta-\beta_0)-m\Delta_0|\leqslant \varepsilon h(\alpha)+82m^3n\varepsilon^{-1}h(F)+647m^4n^2\varepsilon^{-1}\log(2m+2n).$$

Then

$$\begin{aligned}\left|\frac{h(\alpha)}{n}-\frac{h(\beta)}{m}\right|\leqslant&\left|\frac{h(\alpha)}{n}-\frac{h(\alpha-\alpha_0)}{n}\right|+\left|\frac{h(\alpha-\alpha_0)}{n}-\Delta_0\right|+\\&\left|\frac{h(\beta)}{m}-\frac{h(\beta-\beta_0)}{m}\right|+\left|\frac{h(\beta-\beta_0)}{m}-\Delta_0\right|\\\leqslant&2\varepsilon h(\alpha)+165m^2n^3\varepsilon^{-1}h(F)+1303m^3n^4\varepsilon^{-1}\log(2m+2n).\end{aligned}$$

The result follows by taking $\varepsilon/2$ instead of ε. □

4.2 Proof of Theorem 1.3

Let (α,β) be a solution of $F(x,y)=0$. By Theorem 1.2, if (4) is not true, then (5) is satisfied. Moreover, since $(0,0)$ is a non-singular point of $F(x,y)=0$, either $\partial_xF(0,0)$ or $\partial_yF(0,0)$ is non-zero. Without lost of generality, we may assume that so that $\partial_yF(0,0)\neq 0$ and we can apply Theorem 1.1.

If (2) is true, then by Proposition 2.5, we have

$$h(\beta)\leqslant 28m^2n^5\varepsilon^{-2}h(F)+173m^2n^5\varepsilon^{-2}\log(2m+2n),$$

which together with (2) implies (4). And if (3) holds, then Corollary 1.2 implies

$$\begin{aligned}\left|\frac{h(\beta)}{m}-\Delta\right|\leqslant&\left|\frac{h(\beta)}{m}-\frac{h(\alpha)}{n}\right|+\left|\frac{h(\alpha)}{n}-\Delta\right|\\\leqslant&2\varepsilon h(\alpha)+371m^2n^3\varepsilon^{-1}h(F)+2881m^3n^4\varepsilon^{-1}\log(2m+2n).\end{aligned}$$

which together with (3) implies (6) by taking $\varepsilon/(2m)$ instead of ε. □

References

[1] Y. Bilu, D. Masser, *A quick proof of Sprindzhuk's decomposition theorem*, Finite and Infinite Mathematics, to appear.

[2] E. Bombieri, *Weil's "théorème de décomposition"*, Amer. J. Math. **105** (1983), no. 2, 295-308

[3] S.David, P.Philippon, *Minorations des hauteurs normalisées des sous-variétés des tores.* Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **28** (1999), no. 3, 489-543

[4] B. M. Dwork, A. J. Van der Poorten, *The Eisenstein Constant*, Duke Math. J. **65** (1992), 23-43; corrections: **76** (1994), 669-672.

[5] P. Habegger, *Intersecting a variety with algebraic subgroups of multiplicative groups*, in preparation.

[6] M. Hindry, J. Silverman, *Diophantine Geometry, an introduction*, GTM **201**, Springer. (2000).

[7] S. Lang, *Algebra*, GTM **221**, Springer, Revised Third Edition (2002).

[8] S. Lang, *Diophantine Geometry*, Tracts in Mathematics number **11** (1962).

[9] D. Poulakis, *Integer points on rational curves with fixed gcd*, Publ. Math. Debrecen **64/3-4** (2004), 369-379.

[10] D. Roy, J.L. Thunder, *An absolute Siegel's Lemma*, J. reine angew. Math. **476** (1996), 1-26.

[11] C. L. Siegel, *Uber einige Anwendungen Diophantischer Approximationen*, Abh. Preuss. Akad. Wiss. Phys. Math. Kl. (1929), 41-69. Reprinted as pp. 209-266 of his Gesammelte Abhandlungen I, Springer, Berlin (1966).

[12] T. Skolem, *Diophantishe Gleichungen*, J. Springer, Berlin (1938), reprinted by Chelsea, New York (1950).

[13] T. Skolem, *Lösung gewisser Gleichungssysteme in ganzen Zahlen oder ganzzahligen Polynomen mit beschränktem gemeinschaftlichen Teiler*, Oslo Vid. Akar. Skr. I, n°**12** (1929).

[14] V. G. Sprindžuk, *Arithmetic specializations in polynomials*, J. Reine Angew. Math. **340** (1983), 26–52.

[15] V. G. Sprindžuk, *Classical Diophantine equations*, Translated from the 1982 Russian original. Lecture Notes in Mathematics **1559**. Springer-Verlag (1993).

[16] P. G. Walsh, *A quantitative version of Runge's theorem on diophantine equations*, Acta Arithm. **LXII.2** (1992), 157-172.