Michigan Math. J. 51 (2003)

Finiteness Results for Multiplicatively Dependent Points on Complex Curves

E. Bombieri, D. W. Masser, & U. Zannier

1. Introduction

Let n be a positive integer, and let C be a curve in $\mathbf{G}_m^n$ that we suppose (for convenience) is absolutely irreducible. When H is a fixed algebraic subgroup of $\mathbf{G}_m^n$, the intersection of C with H by itself is relatively easy to determine. In [BMZ] we began to study in this context the union of all algebraic subgroups restricted only by dimension. In particular: if $n \geq 2$, and if C is defined over the field $\bar{\mathbf{Q}}$ of all algebraic numbers and satisfies a fairly natural extra hypothesis, then it was shown (Thm. 2, p. 1121) that the intersection of C with the union $\mathcal{H}_{n-2}$ of all H of dimension at most $n-2$ is a finite (possibly empty) set.

The main purpose of the present paper is to generalize this result with regard to the field of definition. More precisely, we shall prove the following.

Theorem. *Let K be a field of characteristic zero, and for $n \geq 2$ let C be an irreducible curve in $\mathbf{G}_m^n$ that is defined over the algebraic closure $\bar{K}$ and is not contained in any translate of an algebraic subgroup of dimension at most $n-1$. Then the intersection of C with the union $\mathcal{H}_{n-2}$ of all algebraic subgroups of dimension at most $n-2$ is a finite (possibly empty) set.*

The restriction to characteristic zero is necessary here. For example, if C is any curve defined over the finite field $K = \mathbf{F}_p$, then the set $C(\bar{K})$ is infinite; on the other hand, any nonzero element of $\bar{K} = \bar{\mathbf{F}}_p$ is a root of unity and so $C(\bar{K})$ lies in the union $\mathcal{H}_0$ of all algebraic subgroups of dimension 0.

We recover Theorem 2 of [BMZ] by taking K as the field $\mathbf{Q}$ of all rational numbers in our Theorem. Our generalization enables us to deduce consequences, however, over the complex field $\mathbf{C}$; thus, if $z_1, \dots, z_n$ are any distinct complex numbers then we see that there are only finitely many complex numbers $z \neq z_1, \dots, z_n$ for which there are two relations,

$$(z-z_1)^{a_1} \cdots (z-z_n)^{a_n} = (z-z_1)^{b_1} \cdots (z-z_n)^{b_n} = 1,$$

where $(a_1, \dots, a_n)$ and $(b_1, \dots, b_n)$ in $\mathbf{Z}^n$ are linearly independent over $\mathbf{Q}$. This follows immediately from our Theorem by considering the line C parameterized by $z-z_1, \dots, z-z_n$ as z varies.

Received January 3, 2002. Revision received June 25, 2003.

We also prove two further results—both of some independent interest—that play a key role in the proof of our Theorem. They concern the union $\mathcal{H}_{n-1}$ of all algebraic subgroups of dimension at most $n-1$. Now $C \cap \mathcal{H}_{n-1}$ is always infinite; this fact was not explicitly proved in [BMZ], but a verification is quite easy. We can recover finiteness in two ways, firstly by considering heights and secondly by considering degrees.

The first situation was treated in [BMZ] over $\bar{\mathbf{Q}}$, but again we need to generalize the field of definition. Because the results involve heights, we shall work (as Lang [L] does) in the context of "fields with a proper set of absolute values satisfying a product formula". Namely, we take (as in [L, pp. 18, 19]) a field F equipped with a set of proper inequivalent valuations $|\cdot|_v$ such that, for each $\xi \neq 0$ in F, only finitely many of these satisfy $|\xi|_v \neq 1$ and then $\prod |\xi|_v = 1$. In this situation, heights can be defined on the algebraic closure $\bar{F}$ or $\bar{F}^n$ or on the projective space $\mathbf{P}_n(\bar{F})$; see [L, p. 52]. Examples include $\mathbf{Q}$ and a rational function field $k(t)$ in one variable over any field k. However, if F has characteristic zero, then by definition a proper valuation restricted to $\mathbf{Q}$ must be either trivial or the standard infinite valuation $|\cdot|_\infty$ or a standard p-adic valuation $|\cdot|_p$. Since we have ruled out multiplicities in the product formula, a number field $\neq \mathbf{Q}$ does not satisfy these conditions.

Our first result on $C \cap \mathcal{H}_{n-1}$ can now be stated as follows.

Proposition 1. *Let F be a field with a proper set of valuations satisfying the product formula. For $n \geq 1$, let C be an irreducible curve in $\mathbf{G}_m^n$ defined over $\bar{F}$ that is not contained in any translate of an algebraic subgroup of dimension at most $n-1$. Then $C \cap \mathcal{H}_{n-1}$ is a set of bounded height in $C(\bar{F}) \subset \bar{F}^n$.*

We recover Theorem 1 of [BMZ, p. 1120] by taking $F = \mathbf{Q}$. In fact, this result refers to different heights defined for $P = (\xi_1, \dots, \xi_n)$ by $h(P) = h(\xi_1) + \cdots + h(\xi_n)$, but it is well known that the particular choice of height is irrelevant in such matters.

The second finiteness result on $C \cap \mathcal{H}_{n-1}$ is a bit easier to state. For P as before, we write $K(P) = K(\xi_1, \dots, \xi_n)$.

Proposition 2. *Let K be a field of characteristic zero that is finitely generated over $\mathbf{Q}$. For $n \geq 1$, let C be an irreducible curve in $\mathbf{G}_m^n$ defined over $\bar{K}$ that is not contained in any translate of an algebraic subgroup of dimension at most $n-1$. Then, for each $D \geq 1$, there are at most finitely many points P in $C \cap \mathcal{H}_{n-1}$ with degree $[K(P) : K] \leq D$.*

This result becomes false without the hypothesis of finite generation; for example, if K is algebraically closed then $[K(P) : K] = 1$ for all P in the infinite set $C \cap \mathcal{H}_{n-1}$.

Each of the three results just stated raises problems from the quantitative standpoint. In the Theorem it would be interesting to estimate the cardinality of the finite set in an efficient way; for example, the finite set corresponding to the line parameterized by $z - z_1, \dots, z - z_n$ should presumably have cardinality bounded by a function depending only on n. If $n = 2$ then this is trivial (two different unit circles can intersect in at most two points), but for $n \geq 3$ the problem appears to be very difficult owing to the use of arithmetic tools in the present proof.

In Proposition 1 we can ask for explicit bounds on the height of the set $C \cap \mathcal{H}_{n-1}$. It is easy to see that these bounds must involve some sort of height $h(C)$ of C and, furthermore, in a dependence that is at least linear if we work logarithmically. It is probably not hard to deduce upper bounds of such a shape, but we do not investigate the problem here. A first result in this direction is contained in the calculations in [BMZ, pp. 1123–1127].

In Proposition 2, we can ask for explicit bounds on the cardinality of the finite set in terms of D; in fact, some lower and upper bounds can be obtained that are nearly asymptotically equal as $D \to \infty$. We will develop this counting aspect in another place.

Finally, let us say a few words about the proofs. Our Theorem for $K = \mathbf{Q}$ was established in [BMZ] by using (among other things) the Amoroso–David theorem [AD] on lower bounds for the product of the heights of r multiplicatively independent elements of $\bar{\mathbf{Q}}$. But we cannot use an analogous method for a field like $K = \mathbf{Q}(t)$, even though this is a field with a product formula and the heights extend to $\overline{\mathbf{Q}(t)}$. The reason is that the Amoroso–David theorem fails if $r \geq 2$. For example, the elements $t^{1/N}$ and $t^{1/N} - 1$ are multiplicatively independent yet both have equally small height as $N \to \infty$, in view of the nonexistence of Archimedean valuations.

Instead, we use a specialization argument to reduce to the case $K = \mathbf{Q}$. To control the possible collapsing under specialization we appeal to Mason's *abc* theorem. Eventually we see that points in $C \cap \mathcal{H}_{n-2}$ must have bounded degree over K, and we conclude using Proposition 2.

This Proposition 2 for $K = \mathbf{Q}$ is an immediate consequence of Proposition 1 together with Northcott's theorem on finiteness. But again for $K = \mathbf{Q}(t)$ this classical result breaks down. For example, the elements $t + N$ ($N = 1, 2, \dots$) all have bounded height and degree; so extra arguments are again required. We argue by induction on the transcendence degree of K, using at each step a lower bound for heights analogous to Dobrowolski's theorem, which is essentially the case $r = 1$ of the Amoroso–David theorem.

Finally, Proposition 1 can be proved with comparative ease by using either of the two methods of [BMZ] (subject to our remarks about Schlickewei's lemma in Section 2). Both of these methods seem to appeal to fairly delicate results on heights due to Siegel and to Néron. But we give another method that avoids such results; this third method is probably the easiest to adapt for explicit upper bounds.

2. Fields with a Proper Set of Valuations Satisfying a Product Formula

We formally state the announced definitions related to fields with a product formula and then prove certain properties of them.

Here we develop some properties of such fields F. Write M_F for the set of valuations.

We define the *zero height group* $Z = Z_F := \{x \in F^* : |x|_v = 1\ \forall v \in M_F\}$ to be the subgroup of F^* made up of elements with trivial valuation everywhere. (When all the valuations in F are ultrametric, the set $Z \cup \{0\}$ is a subfield of F^*.)

We also define a Weil (logarithmic) height on F^* by setting

$$h(\xi) = \sum_{v \in M_F} \max(0, \log|\xi|_v).$$

Plainly, $h(\zeta\xi) = h(\xi)$ for $\zeta \in Z$ and $\xi \in F^*$. Also, we have the usual properties of the height expressed by $h(\xi\eta) \le h(\xi) + h(\eta)$ and $h(\xi^m) = |m|h(\xi)$ (which follows from the product formula for $m < 0$).

We may also define the projective height of a point $P = (a_0 : a_1 : \cdots : a_n) \in \mathbf{P}^n(F)$ by setting, as usual,

$$h(P) = \sum_{v \in M_F} \max_{0 \le i \le n} (\log|a_i|_v).$$

The product formula shows that this is independent of the projective coordinates for P.

The height also may be canonically extended to the algebraic closure $\bar{F}$ of F as in [L]. Namely, if $\xi \in \bar{F}^*$ lies in an extension K of F of degree d, then every valuation v extends to a finite number of valuations $w|v$ on K, and

$$h(\xi) = d^{-1} \sum_{v \in M_K} \sum_{w|v} \max(0, e_w \log|\xi|_w)$$

for appropriate multiplicities e_w (then a product formula with these multiplicities holds in K).

We now have a first lemma on the behavior of the heights in finitely generated subgroups. In the sequel we let F be any field with a proper set of absolute values satisfying a product formula.

LEMMA 2.1. *Given $r \ge 1$ there is $c(r) > 0$ with the following property. Let $\xi_1, \dots, \xi_n$ be $n \ge r$ elements in $\bar{F}^*$ generating a subgroup Γ such that $\Gamma/(Z \cap \Gamma)$ has rank r. Then there exist $g_1, \dots, g_r \in \Gamma$, $\zeta_1, \dots, \zeta_n \in Z$, and $a_{ij} \in \mathbf{Z}$ with*

$$\xi_i = \zeta_i g_1^{a_{i1}} \cdots g_r^{a_{ir}}, \quad i = 1, \dots, n,$$

and

$$\sqrt{\sum_{i=1}^{n} h(\xi_i)^2} \ge c(r) \sum_{j=1}^{r} \Big(\max_{1 \le i \le n} |a_{ij}| \Big) h(g_j).$$

Proof. We first recall from [C] a few useful results from the geometry of numbers. Let $\Lambda \subset \mathbf{R}^r$ be a lattice (i.e., for us, a discrete subgroup of rank r). We denote by $d(\Lambda)$ the absolute value of the determinant whose row vectors are any basis for Λ (this being well-defined). From [C, Thm. V, p. 218], there are linearly independent vectors $\mathbf{b}_1, \dots, \mathbf{b}_r \in \Lambda$ such that

$$\prod_{i=1}^{r} |\mathbf{b}_i| \le c_1(r) d(\Lambda), \tag{2.1}$$

where $|\cdot|$ denotes the Euclidean length and $c_1(r)$ is a positive number depending only on the dimension r.

By [C, Lemma 8, p. 135] we may find a basis $\mathbf{a}_1, \dots, \mathbf{a}_r$ of Λ such that $|\mathbf{a}_j| \le j|\mathbf{b}_j|$ for $j = 1, \dots, r$. Using (2.1), it thus follows that

$$|\det(\mathbf{a}_j)| = d(\Lambda) \ge c_1^{-1}(r) \prod_{j=1}^{r} |\mathbf{b}_j| \ge c_2(r) \prod_{j=1}^{r} |\mathbf{a}_j|, \tag{2.2}$$

where $c_2(r) := (r!\, c_1(r))^{-1}$ is positive and depends only on r.

Fix now $s \in \{1, \dots, r\}$ and write $\mathbf{a}_s = \mathbf{a}_s^* + \mathbf{c}_s$, where $\mathbf{c}_s$ lies in the space spanned over $\mathbf{R}$ by the $\mathbf{a}_j$ ($j \ne s$) and where $\mathbf{a}_s^*$ is orthogonal to that space. Clearly, $\det(\mathbf{a}_j)$ equals the determinant obtained upon replacing $\mathbf{a}_s$ with $\mathbf{a}_s^*$ and leaving the other vectors unchanged. In particular, by the Hadamard inequality we obtain

$$|\det(\mathbf{a}_j)| \le |\mathbf{a}_s^*| \prod_{j \ne s} |\mathbf{a}_j|,$$

which, together with (2.2), implies that

$$|\mathbf{a}_s^*| \ge c_2(r) |\mathbf{a}_s|, \quad s = 1, \dots, r. \tag{2.3}$$

With this in mind, we proceed to prove our lemma. We choose any r elements $\gamma_1, \dots, \gamma_r$ coming from a basis of $\Gamma/(Z \cap \Gamma)$ and write

$$\xi_i = \eta_i \gamma_1^{m_{i1}} \cdots \gamma_r^{m_{ir}}, \quad i = 1, \dots, n, \tag{2.4}$$

with integers m_{ij} and elements $\eta_i \in Z$. For $j = 1, \dots, r$ we let

$$\mathbf{v}_j = (m_{1j}, \dots, m_{nj}) \in \mathbf{Z}^n.$$

The vectors $\mathbf{v}_j$ are linearly independent, since $\Gamma/(Z \cap \Gamma)$ has rank r. Hence they span over $\mathbf{R}$ a vector space V of dimension r, which we identify with $\mathbf{R}^r$ through some Euclidean isometry. We consider the lattice $\Lambda \subset V$ spanned over $\mathbf{Z}$ by $\mathbf{v}_1, \dots, \mathbf{v}_r$ and find a basis $\mathbf{a}_1, \dots, \mathbf{a}_r$ of Λ as before.

Both the $\mathbf{v}_j$ and the $\mathbf{a}_j$ form a basis of Λ, so we may write $\mathbf{v}_j = \sum_{i=1}^{r} t_{ij} \mathbf{a}_i$, with integers t_{ij} forming an invertible matrix over $\mathbf{Z}$ and similarly with the $\mathbf{a}_j$ interchanged with the $\mathbf{v}_j$. In particular, we find that

$$\mathbf{a}_j = (a_{1j}, \dots, a_{nj})$$

for certain integers a_{ij}.

Using these equations, we may substitute in (2.4) to find

$$\xi_i = \zeta_i g_1^{a_{i1}} \cdots g_r^{a_{ir}}, \quad i = 1, \dots, n, \tag{2.5}$$

for suitable elements $\zeta_i \in Z$, where $g_j = \prod_{s=1}^{r} \gamma_s^{t_{js}} \in \Gamma$.

We contend that the inequality of the lemma holds with this choice of the g_j. In fact, pick $s \in \{1, \dots, r\}$ and write

$$\mathbf{a}_s^* = (c_1, \dots, c_n)$$

for suitable rational numbers $c_1, \dots, c_n$. Letting A be a common denominator for them, and taking into account (2.5) and the fact that $\mathbf{a}_s^*$ is orthogonal to the space spanned by the $\mathbf{a}_i$ $(i \neq s)$, we have

$$\prod_{i=1}^{n} \xi_i^{Ac_i} = \zeta g_s^{\sum_{i=1}^{n} Ac_i a_{is}},$$

whence, taking heights, we find

$$\left|\sum_{i=1}^{n} Ac_i a_{is}\right| h(g_s) \le |A| \biggl(\sum_{i=1}^{n} |c_i| h(\xi_i)\biggr).$$

The integer $\sum_{i=1}^{n} Ac_i a_{is}$ is just A times the scalar product $\mathbf{a}_s^* \cdot \mathbf{a}_s$, which equals $|\mathbf{a}_s^*|^2$. In turn, by (2.3) this is bounded below by $c_3(r)|\mathbf{a}_s|^2$, where $c_3(r)$ is positive and depends on r only.

Thus the last displayed estimate implies, by Cauchy's inequality,

$$\begin{aligned}|A| c_3(r) |\mathbf{a}_s|^2 h(g_s) &\le |A| \sum_{i=1}^{n} |c_i| h(\xi_i) \le |A| \sqrt{\sum_{i=1}^{n} |c_i|^2} \sqrt{\sum_{i=1}^{n} h(\xi_i)^2} \\ &= |A| |\mathbf{a}_s^*| \sqrt{\sum_{i=1}^{n} h(\xi_i)^2} \le |A| |\mathbf{a}_s| \sqrt{\sum_{i=1}^{n} h(\xi_i)^2}.\end{aligned}$$

Dividing by the positive number $|A||\mathbf{a}_s|$ yields $\sqrt{\sum_{i=1}^{n} h(\xi_i)^2} \ge c_3(r)|\mathbf{a}_s| h(g_s)$. The right side is bounded below by $c_3(r)(\max_{1\le i\le n} |a_{is}|) h(g_s)$, and now the lemma immediately follows upon taking $c(r) = c_3(r)/r$. □

REMARK. Over number fields a result by Schlickewei [Schl] states that we may find generators $g_1, \dots, g_r$ for $\Gamma/(Z \cap \Gamma)$ and a positive number $c'(r)$ dependent only on r such that, for any integers $a_1, \dots, a_r$, the inequality

$$h(g_1^{a_1} \cdots g_r^{a_r}) \ge c'(r) \sum_{j=1}^{r} |a_j| h(g_j)$$

holds. Such an inequality plainly implies a sharper form of Lemma 2.1 in which the quantities $h(\xi_i)$ are bounded below individually.

However, we note that if $r \ge 2$ then such a sharper result does not hold for any field with a product formula. To produce a counterexample, let $F = \mathbf{C}(x, y)$ be the rational field in two variables over $\mathbf{C}$. We define a set of inequivalent valuations on F as follows. First, for a nonzero polynomial $f(x, y) \in \mathbf{C}[x, y]$ define $\delta(f) = \max\bigl(a + b\sqrt{2}\bigr)$, where the maximum is taken over all monomials $x^a y^b$ appearing in f with a nonzero coefficient. Plainly, $\delta(fg) = \delta(f) + \delta(g)$. Now, define a valuation $|\cdot|_\infty$ by putting $|f|_\infty = 2^{\delta(f)}$. Also, writing $f(x, y) = x^a y^b g(x, y)$, where $g \in \mathbf{C}[x, y]$ is not divisible by x or y, define another valuation

$|\cdot|_0$ by putting $|f|_0 = 2^{-a-b\sqrt{2}}$. Finally, for a principal ideal $I = (p(x, y))$ generated in $\mathbf{C}[x, y]$ by an irreducible polynomial $p(x, y)$ not in $\mathbf{C}x$ or $\mathbf{C}y$, define an associated (discrete) valuation by setting $|f|_I = 2^{-m\delta(p)}$ if $p^m || f$. It is then easy to see that the product formula holds in F for this set of valuations (just check it on the irreducible polynomials) and that $Z = \mathbf{C}^*$. Now the elements x, y are independent modulo Z, but nevertheless $h(x^a y^b) = \left|a + b\sqrt{2}\right| \log 2$ is bounded above if a, b are integers such that $\left|a + b\sqrt{2}\right|$ remains bounded. This easily implies that Schlickewei's result does not hold for the group Γ generated by x and y.

Following the lines of Schlickewei's proof, it may nonetheless be seen that his result holds with the supplementary assumption that all but at most one ultrametric valuations in M_F have rank 1 (i.e., their value group has rank 1). Note that all valuations in our example are discrete and thus have rank 1, except $|\cdot|_\infty$ and $|\cdot|_0$, which have rank 2.

We shall now use Lemma 2.1 to prove another result—crucial to the proof of Proposition 1—about heights in finitely generated groups.

Lemma 2.2. *Given n, there is a number $c'(n)$ with the following property. Let $\xi_1, \dots, \xi_n \in \bar{F}^*$ generate a subgroup Γ such that $\Gamma/(Z \cap \Gamma)$ has rank $\le r$, where $r \ge 1$. Let T be any positive integer. Then there exist integers $b_1, \dots, b_n$, not all zero, such that*

$$|b_i| \le T \quad \textit{and} \quad h(\xi_1^{b_1} \cdots \xi_n^{b_n}) \le c'(n) T^{-(n-r)/r} \max_{1 \le i \le n} h(\xi_i).$$

Proof. We may assume that $\Gamma/(Z \cap \Gamma)$ has rank exactly $r \ge 1$. Let $g_1, \dots, g_r$ be as in Lemma 2.1, so that $\xi_i = \zeta_i \prod_{j=1}^r g_j^{a_{ij}}$. For any integers $b_1, \dots, b_n$, we then obtain

$$\xi_1^{b_1} \cdots \xi_n^{b_n} = \zeta g_1^{L_1} \cdots g_r^{L_r}, \tag{2.6}$$

where $\zeta \in Z$ and $L_j = a_{1j} b_1 + \cdots + a_{nj} b_n$. By a familiar argument involving the pigeonhole principle (see [BMZ, p. 1131] for details), given a positive integer T we may choose $b_1, \dots, b_n \in \mathbf{Z}$ not all zero and such that

$$|b_i| \le T \quad \text{and} \quad |L_j| \le nAh(g_j)^{-1} T^{-(n-r)/r}$$

for all $i = 1, \dots, n$ and all $j = 1, \dots, r$, where we have put $A = \max_{i,j} |a_{ij}| h(g_j)$.

Taking heights in (2.6) and using the inequality for $|L_j|$, we find that

$$h(\xi_1^{b_1} \cdots \xi_n^{b_n}) \le \sum_{j=1}^r h(g_j)|L_j| \le rnAT^{-(n-r)/r}.$$

On the other hand, by Lemma 2.1 we obtain

$$\max_{1 \le i \le n} h(\xi_i) \ge \frac{c(r)}{\sqrt{n}} \sum_{j=1}^r \Bigl(\max_{1 \le i \le n} |a_{ij}| \Bigr) h(g_j) \ge \frac{c(r)}{\sqrt{n}} A,$$

which concludes the proof (here we may choose $c'(n) = \max_{1 \le r \le n} rn\sqrt{n}/c(r)$). □

This lemma is reminiscent of well-known results whose purpose is to find a nontrivial multiplicative relation

$$\xi_1^{b_1} \cdots \xi_n^{b_n} = 1. \tag{$*$}$$

Indeed, if $F = \mathbf{Q}$ and $\xi_1, \dots, \xi_n$ lie in a fixed number field K, we can use the lemma to make $h(\xi_1^{b_1} \cdots \xi_n^{b_n})$ smaller than the minimal positive height of any element of K. Then $(*)$ follows, at least up to roots of unity.

We conclude this section with another lemma, proving known estimates for the height of the root of a polynomial and for the values of rational functions, that is valid in a field F as described previously. As usual, by the height $h(f)$ of a polynomial $f \in F[X]$ we mean the projective height of the vector of its coefficients.

Lemma 2.3. (i) *Let $f(X) = X^d + a_1 X^{d-1} + \cdots + a_d \in \bar{F}[X]$ be a polynomial with a root $\eta \in \bar{F}$. Then $h(\eta) \le h(f) + \log 2$, where the term $\log 2$ can be omitted if there are no Archimedean valuations.*

(ii) *Let $r_0(X), \dots, r_n(X) \in \bar{F}[X]$ be polynomials of maximum degree d. Then there exists a number c, depending only on the r_i, such that $h(r_0(\xi) : \cdots : r_n(\xi)) \le dh(\xi) + c$ for all $\xi \in \bar{F}$ such that the $r_i(\xi)$ are not all zero.*

We recall a short argument for the reader's convenience, for simplicity when F is not a number field (in which case all the valuations are ultrametric).

We may assume that all the relevant elements lie in a finite extension K of F. We let w run through the valuations of K, extending those on F; as explained in Section 2, the height may be expressed in terms of these valuations by using appropriate multiplicities.

To prove (i) we use the equality $\eta^d = -a_1\eta^{d-1} - \cdots - a_d$ to deduce that, for any valuation w, either $|\eta|_w \le 1$ or

$$|\eta|_w = |-a_1 - a_2\eta^{-1} - \cdots - a_d\eta^{-d+1}|_w \le \max_{1 \le i \le d} |a_i|_w,$$

since w is ultrametric. Putting $a_0 = 1$ thus yields

$$\max(1, |\eta|_w) \le \max_{0 \le i \le d} |a_i|_w,$$

and the desired result now follows once we raise to the appropriate power and take the product. (We note that a straightforward adaptation of this argument in the number-field case yields the less precise inequality $h(\eta) \le h(f) + \log d$, which in any case would be sufficient for our purposes; however, one can improve on this by observing that, when $|\cdot|_w$ extends the usual absolute value on $\mathbf{Q}$, we have $|\eta|_w \le \alpha \max(1, |a_1|_w, \dots, |a_d|_w)$, where $\alpha < 2$ is the unique real root > 1 of the equation $x^d = 1 + x + \cdots + x^{d-1}$.)

For (ii), let $\Sigma \subset K$ be the set of coefficients of all the $r_i(X)$. Then, for every valuation w, we clearly have $|r_i(\xi)|_w \le \max_{\sigma \in \Sigma} |\sigma|_w \max(1, |\xi|_w)^d$, whence

$$\max(\log|r_0(\xi)|_w, \dots, \log|r_n(\xi)|_w) \le d \log \max(1, |\xi|_w) + \max_{\sigma \in \Sigma} \log|\sigma|_w.$$

Multiplying by $e_w/[K : F]$ and summing over $w \in M_K$ yields the result, where we may take c to be the projective height of the point whose coordinates are the elements of Σ.

3. Proof of Proposition 1

We shall follow the argument given in [BMZ, Sec. 3] except that, as mentioned in the Introduction, we shall avoid any use of the somewhat delicate results on heights due to Siegel or Néron. Also, the lemma of Schlickewei mentioned in the Remark in Section 2 (i.e., [BMZ, Lemma 2]) will be replaced by our Lemma 2.2. In fact the results of Siegel and Néron do remain valid in our more general context; see for example [L, Prop. 5.4, p. 115]. So the argument of [BMZ, Sec. 2] via [BMZ, Prop. B, p. 1127] could also be used. However, it may be a problem to make these asymptotic results explicit in their dependence on the curve C.

To begin with the proof, let $x_1, \dots, x_n$ be coordinates on $\mathbf{G}_m^n$ that are viewed as rational functions on C. Let $P \in C(\bar{F})$ be such that $(\xi_1, \dots, \xi_n) \in H$, where H is a proper algebraic subgroup of $\mathbf{G}_m^n$ and hence is of dimension $\leq n-1$. Then the ξ_i are multiplicatively dependent, so the group $\Gamma \subset \bar{F}^*$ they generate has rank $r \leq n-1$.

Let i_0 be an index for which $h(\xi_{i_0})$ is maximum, and define the rational function x by $x = x_{i_0}$. We may now apply Lemma 2.2 to Γ. We fix an integer T and obtain the existence of integers $b_1, \dots, b_n$, not all zero, such that

$$|b_i| \leq T,$$
$$h(\xi_1^{b_1} \cdots \xi_n^{b_n}) \leq c'(n) T^{-(n-r)/r} \max_{1 \leq i \leq n} h(\xi_i) = c'(n) T^{-(n-r)/r} h(x(P)). \tag{3.1}$$

Define the rational function y on C by $y = x_1^{b_1} \cdots x_n^{b_n}$. Now y lies in the function field $\bar{F}(x_1, \dots, x_n)$, whose degree over $\bar{F}(x)$ depends only on the curve C. Hence there is an equation

$$s_0(x) y^e + \cdots + s_e(x) = 0$$

with $s_j(x) \in \bar{F}[x]$ not all zero and $e \leq c_1$. These $s_j(x)$ are not all in $\bar{F}$ else y would be constant on C, contrary to our hypothesis. Now the equation can be rewritten as

$$r_0(y) x^d + \cdots + r_d(y) = 0,$$

with $r_i(Y) \in \bar{F}[Y]$ not all zero and of degree at most e. Dividing out by a common factor if necessary, we can suppose that the $r_i(Y)$ have no common zero in $\bar{F}$; they depend only on the curve C and the exponents $b_1, \dots, b_n$ defining y.

Now Lemma 2.3(ii) implies that

$$h(r_0(\xi) : \cdots : r_d(\xi)) \leq c_1 h(\xi) + C_1(T),$$

where $C_1(T)$ is independent of $\xi = y(P) = \xi_1^{b_1} \cdots \xi_n^{b_n}$.

Then, for $\eta = x(P) = \xi_{i_0}$, Lemma 2.3(i) yields

$$h(\eta) \leq c_1 h(\xi) + C_2(T),$$

again with $C_2(T)$ independent of P. It follows that choosing T in (3.1) minimal with $c_1 c'(n) T^{-(n-r)/r} \leq 1/2$ implies $h(\eta) \leq 2C_2(T)$, and this bound depends only on C. The proposition is proved. □

Remark. The same proof yields the sharper result obtained by replacing the set $\mathcal{H}_{n-1}$ with the union $\bigcup_{z\in Z} z\mathcal{H}_{n-1}$ of the set of its translates by elements of Z. In the number-field case Z is just the set of roots of unity, so this gives nothing new.

4. Proof of Proposition 2

We will establish Proposition 2 by using Proposition 1 and induction on n. The starting case $n = 1$ is easy, because then $C = \mathbf{G}_m$ and $C \cap \mathcal{H}_{n-1}$ is the set of roots of unity $\mu \in \bar{K}$. If we bound the degree $[K(\mu) : K]$ by D, then μ is the zero of a monic polynomial over K, irreducible of degree at most D; this polynomial divides some $z^N - 1$ and so all its zeros must be roots of unity. Therefore, its coefficients live in $\bar{\mathbf{Q}} \cap K$. Since every subfield of a finitely generated field is itself finitely generated (see [Schi, proof of Thm. 1, p. 12, and the following Remark]), this intersection is a finitely generated subfield of $\bar{\mathbf{Q}}$ and thus a number field K_0. Hence μ has degree at most D over K_0 and so there are only finitely many possibilities for μ.

We can therefore assume that Proposition 2 holds for curves in $\mathbf{G}_m^{n-1}$ $(n \geq 2)$, and we proceed to deduce it for curves C in $\mathbf{G}_m^n$. By replacing K with a finite extension if necessary, we may assume that C is defined over K.

Since $K/\mathbf{Q}$ is finitely generated, its transcendence degree m is finite, and we will use a further induction on m.

If $m = 0$ then K is a number field. Thus Proposition 1 implies that $C \cap \mathcal{H}_{n-1}$ is a set of bounded height. Now, if we also bound the degree of the point P in this set (by $D[K : \mathbf{Q}]$) then Northcott's theorem (see [L, p. 59]) yields the finiteness required in Proposition 2.

So assume that $m \geq 1$ and that Proposition 2 has been established for fields of transcendence degree strictly less than m. Fix a transcendence basis $\{t_1, \dots, t_m\}$ for K over $\mathbf{Q}$; then K is a finite extension of $\mathbf{Q}(t_1, \dots, t_m)$. Thus $\bar{K}$ naturally embeds into the algebraic closure of $\mathbf{Q}(t_1, \dots, t_m)$, which is $\overline{k(t)}$ for $t = t_m$ and k the algebraic closure of $K_0 := \mathbf{Q}(t_1, \dots, t_{m-1})$.

Observe now that $F = k(t)$ is a field with a proper set of absolute values satisfying a product formula, by virtue of the valuations corresponding to the elements of $\mathbf{P}^1(k)$, with zero-height group $Z = k^*$. Proposition 1 therefore implies that $C \cap \mathcal{H}_{n-1}$ is a set of bounded height in $C(\bar{F}) \subset \bar{F}^n$. We have to prove that there exist only finitely many points $P = (\xi_1, \dots, \xi_n)$ in $C \cap \mathcal{H}_{n-1}$ with $[K(P) : K] \leq D$.

Let $\Gamma = \Gamma(P)$ be the subgroup of $\bar{F}^*$ generated by $\xi_1, \dots, \xi_n$, and let $\tilde{\Gamma} := \Gamma/(k^* \cap \Gamma)$ be the quotient by its zero-height group. Then $\tilde{\Gamma}$ has rank r satisfying $0 \leq r \leq n - 1$.

If $r = 0$ then the argument can be finished as follows. Namely, $\Gamma \subset k^*$, so the coordinates of P are in k. We may assume that there are infinitely many such P and it follows that C is defined over k. So C is also defined over $K' = k \cap K$. This intersection is finitely generated over $\mathbf{Q}$, with transcendence degree at most $m - 1$, and certainly $P \in C(K') \cap \mathcal{H}_{n-1}$. We claim that

$$[K'(P) : K'] \leq D^n. \tag{4.1}$$

This will enable us to apply the induction hypothesis on the transcendence degree.

Consider the monic minimal polynomial Q_i over K of each coordinate ξ_i certainly of degree at most D. Since ξ_i is in the algebraic closure k of $K_0 = \mathbf{Q}(t_1, \ldots, t_{m-1})$, it is a zero of some monic polynomial over K_0. This polynomial splits completely in $k = \bar{K}_0$ and is divisible by Q_i. It follows that all the zeros of Q_i lie in k. Thus the coefficients of Q_i lie in k and so also in $K' = k \cap K$. Hence ξ_i has degree at most D over K' and now (4.1) follows. If required, the exponent n could easily be removed by applying our argument to linear combinations of $\xi_1, \ldots, \xi_n$. In any case, the finiteness of the set of points P with $r = 0$ is now clear by induction on m.

What if $r \geq 1$? We use Lemma 2.1 to find $g_1, \ldots, g_r \in \Gamma$, which are multiplicatively independent modulo elements of zero height in Γ, such that

$$\xi_i = \zeta_i g_1^{a_{i1}} \cdots g_r^{a_{ir}}, \quad i = 1, \ldots, n, \tag{4.2}$$

and

$$\sqrt{\sum_{i=1}^{n} h(\xi_i)^2} \geq c(r) \sum_{j=1}^{r} A_j h(g_j),$$

where $A_j = \max_{1 \leq i \leq n} |a_{ij}|$. If B is the upper bound for the maximum height $\max_{1 \leq i \leq n} h(\xi_i)$ of the coordinates of P provided by Proposition 1, it follows that

$$A_j h(g_j) \leq nB/c(r), \quad j = 1, \ldots, r. \tag{4.3}$$

Thus the heights $h(g_j)$ are “small”.

At a similar point, in [BMZ, p. 1134] we used a result of Dobrowolski type or (if necessary) Amoroso–David type. As already remarked, the latter does not generalize; however, the former does and in an especially simple way. Namely, for any nonconstant $\gamma \in \bar{F} = \overline{k(t)}$ we have the identity

$$h(\gamma) = \frac{[k(\gamma, t) : k(\gamma)]}{[k(\gamma, t) : k(t)]} \tag{4.4}$$

in terms of field degrees (see [Ma, p. 8]). Our g_j are in $\Gamma \subset K(P)$ and $k(t) \supset \mathbf{Q}(t_1, \ldots, t_m)$, so

$$\begin{aligned}[k(g_j, t) : k(t)] &\leq [\mathbf{Q}(g_j, t_1, \ldots, t_m) : \mathbf{Q}(t_1, \ldots, t_m)] \\ &\leq [K(g_j) : K][K : \mathbf{Q}(t_1, \ldots, t_m)] \leq \sigma D\end{aligned}$$

for the constant $\sigma := [K : \mathbf{Q}(t_1, \ldots, t_m)]$.

Now, combining this with (4.4), ignoring the numerator, and comparing with (4.3), we see that

$$A_j \leq (nB/c(r))\sigma D, \quad j = 1, \ldots, r.$$

Therefore, by Proposition 1, the a_{ij} in (4.2) are bounded independently of $P = (\xi_1, \ldots, \xi_n)$. Since P lies in $\mathcal{H}_{n-1}$, there is a multiplicative relation $\xi_1^{b_1} \cdots \xi_n^{b_n} = 1$ with nonzero $(b_1, \ldots, b_n)$ in $\mathbf{Z}^n$. This now forces additive relations

$$\sum_{i=1}^{n} b_i a_{ij} = 0, \quad j = 1, \dots, r,$$

among the $b_1, \dots, b_n$. Since $r \geq 1$ and since the matrix of the a_{ij} has rank r, we have at least one nontrivial relation, say $\sum_{i=1}^{n} b_i a_i = 0$, and this will suffice.

Recall that the a_{ij} are actually bounded, so we get only finitely many possible relations and thus (for our purposes) may suppose that a fixed such relation occurs. We may assume that the a_i are not all zero and coprime. Then, by means of an automorphism of $\mathbf{G}_m^n$, we may assume that our relation is $b_n = 0$. This means that P satisfies $\xi_1^{b_1} \cdots \xi_{n-1}^{b_{n-1}} = 1$. Consider then the projection $\pi(C)$ of C to the first $n-1$ coordinates (a space that we identify with $\mathbf{G}_m^{n-1}$). Because C is not contained in any translate of a proper subgroup, this projection does not reduce to a point, whence its Zariski closure in $\mathbf{G}_m^{n-1}$ is a curve C', also defined over K. It is not contained in any translate of a proper subgroup H' of $\mathbf{G}_m^{n-1}$, for otherwise C would be contained in a translate of the proper subgroup $\pi^{-1}(H')$ of $\mathbf{G}_m^n$. Since $\pi(P) \in C' \cap \mathcal{H}_{n-2}$ still has degree at most D, we may apply the inductive assumption to see that there are only finitely many possibilities for $\pi(P) = (\xi_1, \dots, \xi_{n-1})$. Finally, each equation $x_1 = \xi_1$ has at most finitely many solutions P in C (for otherwise C would be contained in a translate of the subgroup defined by $x_1 = 1$). This completes the proof. □

5. Specializations

Let C and K be as in the Theorem. Our proof strategy is as follows. Suppose for simplicity that K is finitely generated over $\mathbf{Q}$ and that C is defined over K. Now K can be considered as a subfield of $\bar{\mathbf{Q}}(G)$, where G is a $\bar{\mathbf{Q}}$-generic point of some irreducible variety B defined over $\bar{\mathbf{Q}}$. By specializing G to a suitable point Q in $B(\bar{\mathbf{Q}})$, we obtain a curve C_Q over $\bar{\mathbf{Q}}$. It will turn out that a point P in $C \cap \mathcal{H}_{n-2}$ of degree $D = [K(P) : K]$ specializes to almost D different points in $C_Q \cap \mathcal{H}_{n-2}$. If D is sufficiently large then this contradicts the Theorem over $\bar{\mathbf{Q}}$ (Theorem 2 of [BMZ]). Hence D is bounded, and we conclude the proof using Proposition 2 for the curve C.

In fact, we will use the language of intersections as well as that of specializations, and in this section we recall some relevant basic facts, taking some care over small Zariski-closed sets (e.g., the singularities of both C and B cause minor problems in the counting).

As in Section 4, we prefer to work over algebraically closed fields k for the moment. Let $\mathcal{K}$ be a field finitely generated over k and let C in $\mathbf{G}_m^n$ be an absolutely irreducible curve defined over $\mathcal{K}$. In order to describe the totality of all valuations on function fields we need projective nonsingular models, and it suffices to take such a model $\tilde{C}$ of C. We will suppose that both $\tilde{C}$ and a regular map from $\tilde{C}$ to the completion $\hat{C}$ of C in $\mathbf{P}^n$ are defined over $\mathcal{K}$. The coordinates $x_1, \dots, x_n$ on C in $\mathbf{G}_m^n$ induce rational functions on $\tilde{C}$, for which we can use the same symbols, and we further assume that the zeros and poles of $x_1, \dots, x_n$ in $\tilde{C}$ are defined over $\mathcal{K}$. Let S be this set of zeros and poles.

We can find an irreducible affine variety B in $\mathbf{A}^m$, defined over k, such that $\mathcal{K} = k(G)$ for some k-generic point $G = (g_1, \ldots, g_m)$ of B. By clearing denominators in a finite set of defining equations for C, we can assume that their coefficients lie in the ring $k[g_1, \ldots, g_m]$. When we replace $g_1, \ldots, g_m$ by the affine coordinates $y_1, \ldots, y_m$ and then adjoin a finite set of defining equations for B, we obtain a variety C_B in $\mathbf{G}_m^n \times \mathbf{A}^m$ that is defined over k. The projection π to $\mathbf{A}^m$ satisfies $\pi(C_B) = B$, and the projection γ to $\mathbf{G}_m^n$ satisfies $\gamma(C_B \cap \pi^{-1}(G)) = C$.

For any Q in B we can consider the object $C_Q = \gamma(C_B \cap \pi^{-1}(Q))$; this will not always be a curve unless we restrict Q to some nonempty Zariski-open subset B_0 of B. For example, $C_G = C$ itself, and we obtain C_Q by specializing the equations for C.

Likewise, by decreasing B_0 if necessary we can suppose that, for all Q in B_0, the specialized varieties $\hat{C}_Q$ and $\tilde{C}_Q$ are also curves with a regular map f_Q from $\tilde{C}_Q$ to $\hat{C}_Q$. We can even suppose that the curves C_Q, $\hat{C}_Q$, and $\tilde{C}_Q$ are absolutely irreducible (see e.g. [Schi, Thm. 32, p. 201]) and that $\tilde{C}_Q$ is nonsingular (use e.g. the Jacobian criterion). It follows that $\tilde{C}_Q$ is a projective nonsingular model of C_Q.

By further decreasing B_0 we may assume that the genus $g(C_Q) = g(C_G) = g(C)$. Similarly, we may assume that the "singular excess"

$$\varepsilon_Q = \sum_{P \in \hat{C}_Q} (\# f_Q^{-1}(P) - 1)$$

satisfies $\varepsilon_Q = \varepsilon_G = \varepsilon(C)$, say, and that the "number of nonmultiplicative points"

$$\delta_Q = \#(\hat{C}_Q \setminus C_Q)$$

satisfies $\delta_Q = \delta_G = \delta(C)$, say.

Finally, we can suppose that different elements of the set S in $\tilde{C}$ specialize to different elements of $\tilde{C}_Q$, and these make up a set S_Q, which is the set of all zeros and poles of the coordinate functions on C_Q and $\tilde{C}_Q$. We can even suppose that the corresponding orders of zeros and poles remain the same under specialization.

The singularities of B can be dealt with rather more simply: just remove them from B_0.

6. Proof of Theorem

Let C and K be as in the Theorem. We can assume without loss of generality that K is finitely generated over $\mathbf{Q}$ and that C, $\tilde{C}$ and the elements of the set S of zeros and poles of $x_1, \ldots, x_n$ are defined over K. We take $\mathcal{K}$ as the compositum of k and K, with $k = \bar{\mathbf{Q}}$, and we construct B and B_0 as in Section 5. We retain the notation C_Q, $\tilde{C}_Q$, S_Q there.

We start by noting that C is not contained in an algebraic subgroup of $\mathcal{H}_{n-1}$ and so neither is C_Q for every Q in B_0. For if some $x_1^{b_1} \cdots x_n^{b_n}$ (integers $b_1, \ldots, b_n$ not all zero) is constant on C_Q then it is constant on $\tilde{C}_Q$, and this leads to linear relations between the orders of zeros and poles in S_Q. These coincide with the orders in S and thus $x_1^{b_1} \cdots x_n^{b_n}$ would be constant on C, contrary to hypothesis.

Let H be an algebraic subgroup of $\mathbf{G}_m^n$ with dimension exactly $n-1$. Then H is defined by a single relation $x_1^{b_1} \cdots x_n^{b_n} = 1$ with exponents unique up to a common sign. We write $D(H)$ for the degree of $x_1^{b_1} \cdots x_n^{b_n}$ considered as a function on C or $\tilde{C}$; this is then independent of the choice of sign.

We can interpret the equation of H just as well on $\mathbf{G}_m^n \times \mathbf{A}^m$ and thus we can speak of the intersection $C_B \cap H$. We claim now that $C_B \cap H \cap \pi^{-1}(G)$ is finite with cardinality

$$\#(C_B \cap H \cap \pi^{-1}(G)) \leq D(H). \tag{6.1}$$

For γ injects the set of (6.1) into $C \cap H$ and, since $x_1^{b_1} \cdots x_n^{b_n} - 1$ also has degree $D(H)$, these sets certainly contain at most $D(H)$ points.

LEMMA 6.1. *For any H as before and any Q in $B_0(k)$, the set $C_B \cap H \cap \pi^{-1}(Q)$ is finite with cardinality*

$$\#(C_B \cap H \cap \pi^{-1}(Q)) \geq D(H) - c,$$

where $c = 2g(C) - 2 + \varepsilon(C) + \delta(C)$.

Proof. We will use Mason's *abc* theorem [Ma, Lemma 2, p. 14] on the function field $\Lambda = k(C_Q)$. Of course, this is a finite extension of some $F = k(t)$ as in Section 2 and so there is a theory of heights on $\bar{F}$. The nontrivial valuations on $k(C_Q)$ correspond to the points of $\tilde{C}_Q(k)$; however, in [Ma] they are normalized to have value group $\mathbf{Z}$ on $k(C_Q)$, not F. This means that $h(\lambda)$ is just the degree $[\Lambda : k(\lambda)]$ without the denominator in (4.4). Mason's theorem states that if $\lambda_1, \lambda_2, \lambda_3$ are nonzero in Λ with zero sum and if λ_1/λ_2 is not constant, then

$$h(\lambda_1/\lambda_2) \leq N + 2g(C_Q) - 2,$$

where N is the number of valuations v with $|\lambda_1|_v, |\lambda_2|_v, |\lambda_3|_v$ not all equal.

We apply this with $\lambda_1 = x_1^{b_1} \cdots x_n^{b_n}$, $\lambda_2 = -1$, and $\lambda_3 = 1 - \lambda_1$, so that $h(\lambda_1/\lambda_2) = D(H)$. We deduce that there are at least $D(H) - 2g(C_Q) + 2$ valuations v satisfying at least one of $|\lambda_1|_v < 1$, $|\lambda_1|_v > 1$, $|\lambda_3|_v > 1$, or $|\lambda_3|_v < 1$. Throwing away at most $\varepsilon_Q = \varepsilon(C)$ of these, we can restrict attention to points of $\hat{C}_Q$. Throwing away a further $\delta_Q = \delta(C)$ means we are left with points of C_Q. These cannot be zeros or poles of $x_1, \dots, x_n$, so the first three inequalities above are now eliminated; there remains only $|\lambda_3|_v < 1$, so that we have the zeros of $x_1^{b_1} \cdots x_n^{b_n} - 1$ in C_Q. As before, the map γ injects $C_B \cap H \cap \pi^{-1}(Q)$ into this set, and the lemma follows (the finiteness is again clear). $\square$

LEMMA 6.2. *For any H as before, let W be a finite union of irreducible components of $C_B \cap H$. Then, for any Q in $B_0(k)$,*

$$\#(W \cap \pi^{-1}(Q)) \geq \#(W \cap \pi^{-1}(G)) - c.$$

Proof. In general, if $\pi : W \to B$ is a finite map then the two cardinalities of the lemma are actually equal for all Q in some nonempty Zariski-open subset B_W of B; this follows from a standard discriminant argument. However, B_W will usually depend on W and thus on H. The effect of the lemma is to make B_W independent of H at the expense of introducing the constant c.

In fact, some $c > 0$ may be needed. For example, let C be defined over $k(\mathbf{A}) = k(y)$ by

$$x_2 = x_1 + 1, \qquad x_3 = x_1 - y,$$

let H be defined by $x_1^{p+q} = x_2^p x_3^q$, and let $W = C_B \cap H$. Then $\#(W \cap \pi^{-1}(G)) = p + q - 1$, but

$$\#(W \cap \pi^{-1}(Q)) \leq p + q - 2$$

for $Q = p/q$. Thus $\bigcap B_W \subset \mathbf{A} \setminus \mathbf{Q}$, which is far from Zariski-open!

Now to the proof. Let W' be the union of all irreducible components of $C_B \cap H$ not appearing in W, so that $W \cup W' = C_B \cap H$. By Lemma 6.1, the sets $W \cap \pi^{-1}(Q)$ and $W' \cap \pi^{-1}(Q)$ are finite; call their cardinalities $s(Q)$ and $s'(Q)$, respectively. The projections π from W and W' to B have degrees $s(G)$ and $s'(G)$ respectively, and since Q is nonsingular on B we can appeal to [Mu, Thm. 3.25, p. 53] to deduce

$$s(Q) \leq s(G), \qquad s'(Q) \leq s'(G).$$

Also,

$$s(Q) + s'(Q) \geq \#(C_B \cap H \cap \pi^{-1}(Q))$$

and

$$s(G) + s'(G) = \#(C_B \cap H \cap \pi^{-1}(G)),$$

since the sets $W \cap \pi^{-1}(G)$ and $W' \cap \pi^{-1}(G)$ are disjoint. This is because $W \cap W'$ has dimension strictly less than the dimension of B, so no point can project to G. All these inequalities together with (6.1) and Lemma 6.1 lead to $s(Q) \geq s(G) - c$, which is the desired conclusion. $\square$

We can now finish the proof of the Theorem. Since $K \subset \mathcal{K} = k(G)$ is finitely generated over $\mathbf{Q}$, we can find a number field k_0 with $K \subset k_0(G)$. Both of these latter fields are finitely generated over $\mathbf{Q}$ with the same transcendence degree and so the index $[k_0(G) : K] = e$ is finite.

Fix once and for all a point Q on $B_0(k)$, and let q be the cardinality of $C_Q \cap \mathcal{H}_{n-2}$; this is finite by [BMZ, Thm. 2, p. 1121].

Let P be any point of $C \cap \mathcal{H}_{n-2}$ and consider the k_0-Zariski-closure W of (P, G) on C_B in $\mathbf{G}_m^n \times \mathbf{A}^m$. Now P lies in $C \cap H \cap H'$ for two subgroups H, H' of dimension $n-1$ such that $\dim(H \cap H') = n - 2$; hence (P, G) is in $C_B \cap H \cap H'$. The dimension of W is at least the dimension of B, which is also the dimension of $C_B \cap H$. It follows that W (which is irreducible over k_0) is a finite union of $\bar{\mathbf{Q}}$-irreducible components of $C_B \cap H$. Therefore, by Lemma 6.2 we have

$$\#(W \cap \pi^{-1}(Q)) \geq \#(W \cap \pi^{-1}(G)) - c.$$

But $\#(W \cap \pi^{-1}(G))$ is just the degree

$$[k_0(P, G) : k_0(G)] = [k_0(P, G) : K(P)][K(P) : K]/[k_0(G) : K],$$

which is at least $[K(P) : K]/e = D(P)/e$, say. Thus $W \cap \pi^{-1}(Q)$ contains at least $D(P)/e - c$ different points. But these project under γ to different points of $C_Q \cap H \cap H'$, whose cardinality is at most q.

Thus $D(P) \leq e(c + q)$ is bounded independently of P, and we can use Proposition 2 to conclude the finiteness of $C \cap \mathcal{H}_{n-2}$. $\square$

References

[AD] F. Amoroso and S. David, *Le problème de Lehmer en dimension supérieure,* J. Reine Angew. Math. 513 (1999), 145–179.

[ArWh] E. Artin and G. Whaples, *Axiomatic characterization of fields by the product formula for valuations,* Bull. Amer. Math. Soc. 51 (1945), 469–492.

[BMZ] E. Bombieri, D. Masser, and U. Zannier, *Intersecting a curve with algebraic subgroups of multiplicative groups,* Internat. Math. Res. Notices 20 (1999), 1119–1140.

[C] J. W. S. Cassels, *An introduction to the geometry of numbers,* Classics Math., Springer-Verlag, Berlin, 1997.

[L] S. Lang, *Fundamentals of Diophantine geometry,* Springer-Verlag, Berlin, 1983.

[Ma] R. C. Mason, *Diophantine equations over function fields,* Cambridge Univ. Press, Cambridge, U.K., 1984.

[Mu] D. Mumford, *Algebraic geometry I. Complex projective varieties,* Classics Math., Springer-Verlag, Berlin, 1995.

[Schi] A. Schinzel, *Polynomials with special regard to reducibility,* Encyclopedia of mathematics and its applications, vol. 77, Cambridge Univ. Press, Cambridge, U.K., 2000.

[Schl] H. P. Schlickewei, *Lower bounds for heights on finitely generated groups,* Monatsh. Math. 123 (1997), 171–178.

E. Bombieri
School of Mathematics
Institute for Advanced Study
Princeton, NJ 08540

eb@math.ias.edu

D. W. Masser
Mathematisches Institut
Universität Basel
Rheinsprung 21
CH-4051 Basel
Switzerland

masser@math.unibas.ch

U. Zannier
Istituto Universitario di Architettura
D.C.A.
S. Croce 191
30135 Venezia
Italy

zannier@dimi.uniud.it