MÉMOIRES DE LA S. M. F.

YUVAL Z. FLICKER

Linear forms on arithmetic abelian varieties : ineffective bounds

Mémoires de la S. M. F. 2^e série, tome 2 (1980), p. 41-47

<http://www.numdam.org/item?id=MSMF_1980_2_2__41_0>

SOCIÉTÉ MATHÉMATIQUE DE FRANCE
2e série, Mémoire n° 2, 1980, p. 41-47

LINEAR FORMS ON ARITHMETIC ABELIAN VARIETIES : INEFFECTIVE BOUNDS

by

Yuval Z. FLICKER

Using ideas from Baker's method of linear forms in logarithms, Masser, Lang and Coates gave effective lower bounds for linear forms in algebraic points on an abelian variety of CM-type. In [1,3] it was shown that analogous effective bounds hold for the p-adic valuations of such forms for a certain class of primes p (depending on the ring of complex multiplications ; see [1,3]). It would be of interest to obtain such bounds for all abelian varieties, not only of CM-type, and in the p-adic case for all primes unconditionally ; however no-one has yet succeeded in doing this. Confining ourselves to non-effective lower bounds we shall here obtain such bounds for any "arithmetic" abelian variety and all valuations. The first result of the kind which we shall establish was given by Gelfond as a consequence of the Thue-Siegel theory ; hence the ineffective character of the proof. Coates [2] obtained an analogue in the complex elliptic case, applying methods similar to those used by Siegel [7] in the study of integral points on curves of genus 1. Theorem 1 below will depend on the general Thue-Siegel-Mahler-Roth theorem.

Theorem 2 is a geometric reformulation of Theorem 1 ; thus we find a lower bound for the (complex or p-adic) Euclidean distance of a variable point P with algebraic components from a fixed point on the abelian variety, in terms of the height H(P) of the point P. Such reformulation is implicit in Siegel [7] , was made explicit by Lang [4] and later by Masser [5] (see [1,3] for the p-adic case).

This will be applied to deduce a slight improvement of the Siegel(-Mahler) theorem on the finiteness of the number of points on a curve of positive genus which lie in fixed number field K and whose denominator is composed of primes from a finite set. The present variant of the proof of the Siegel-Mahler theorem seems to emphasize more clearly the underlying Diophantine connections.

Applications improving the Siegel-Mahler theorem can be deduced in the same way also from the effective lower bounds for linear forms which can be obtained using the Baker-Masser approach. We note that the sharper but specialized results of [6] and [3] imply a very sharp version of the above theorem in the case of CM-type curves, when the denominator is composed of a special kind of primes. Even in this last case the result is ineffective since we use a base for the K-rational points on A which is given ineffectively by the Mordell-Weil theorem.

§ 1. Let A be an abelian variety with dimension d in a projective space of dimension $d'(\geq d)$. Let K be a number field, and suppose that A, its group law, and its origin e are defined over K. Signify by $\{X_o, X_1, \ldots, X_{d'}\}$ a set of projective coordinates for A, such that $X_o(e) \neq 0$ and $X_i(e) = 0 (1 \leq i \leq d')$; we can always find such set by applying a projective linear transformation. Then $\{x_i = X_i/X_o\}$ is a set of affine coordinates for the affine open subset A_o of the points P on A with $X_o(P) \neq 0$. We shall consider first the points on A_o which are defined over the field of complex numbers, and later the points which are defined over a p-adic completion $K_\wp$ of K.

In the complex case we recall that there is a lattice L in $\mathbb{C}^d$, and a locally injective map $\underline{f} = (f_1, \ldots, f_{d'})$, whose d' components are analytic functions on an open subset of $\mathbb{C}^d$ with periods in L, which parametrizes A_o, and such that $f_i(\underline{0}) = 0 (1 \leq i \leq d')$. Moreover $\underline{f}$ is a local analytic isomorphism at each point in its domain of convergence, and it can be continued as a meromorphic map to the entire space.

In the p-adic case we also have a parametrization of a neighborhood of e on A_o by an injective map $\underline{f} = (f_1, \ldots, f_{d'})$, with d' analytic components, and such that $f_i(\underline{0}) = 0 (1 \leq i \leq d')$; however it is no longer periodic but only locally defined on the neighborhood $|\underline{z}| < p^{-1/(p-1)}$ of the origin in $K_\wp^d$. Moreover we may assume that $\underline{f}$ is an isometry in the p-adic case, see [1], but this will not be needed here. In both cases we say that a vector $\underline{u}$ in $\mathbb{C}^d$ or in $K_\wp^d$, at which $\underline{f}$ converges, is an <u>algebraic point</u>, if each f_i takes an algebraic value at $\underline{u}$.

Now suppose that $\underline{u}_1,\ldots,\underline{u}_m$ are algebraic points which are linearly independent over $\mathbb{Q}$. Since we shall deal simultaneously both with the complex and with the p-adic cases, we shall signify by $|\ |$ any valuation on K. We prove :

Theorem 1 : For any $\varepsilon > 0$ there exists a constant $C > 0$, such that for any set of integers $b_1,\ldots,b_m$, not all 0, with absolute values at most B, we have

$$|b_1\underline{u}_1 +\ldots+ b_m\underline{u}_m| > C \exp(-\varepsilon B^2).$$

The constant C depends on ε, $f_i(\underline{u}_j)$ $(1 \leqslant i \leqslant d', 1 \leqslant j \leqslant m)$, the defining equations of A and on the valuation $|\ |$. As we already remarked C cannot be explicitly computed in these terms, but it will be, once an effective analogue of the Thue-Siegel-Mahler-Roth theorem is established .

§ 2. We shall now proceed to prove Theorem 1 both in the complex and in the p-adic cases. In both cases we shall prove the theorem by deducing a contradiction from the supposition that there are infinitely many sets of integers $b_1,\ldots,b_m$ such that $u = b_1\underline{u}_1 +\ldots+ b_m\underline{u}_m$ does not satisfy the conclusion of Theorem 1. Assuming this, we let n be a natural number, whose value will be specified later, such that the greatest common divisor (p,n) of p and n is 1 in the p-adic case. We write $b_i = nb_i' + q_i$, where b_i' and q_i are rational integers and $0 \leqslant q_i < n$; thus $\underline{u} = n\underline{u}' + \underline{q}$, where

$$\underline{u}' = b_1'\underline{u}_1 +\ldots+ b_m'\underline{u}_m \text{ , and } \underline{q} = q_1\underline{u}_1 +\ldots+ q_m\underline{u}_m .$$

Clearly $\underline{q}$ can take only a finite number of values when n is fixed ; we will restrict our attention in the sequel to a fixed $\underline{q}$ $(= \underline{q}(n))$, and to an infinite sequence of distinct sets $b_1',\ldots,b_m'$, corresponding to $\underline{q}$. On denoting by B' the maximum of the absolute values of b_i' $(1 \leqslant i \leqslant m)$, we have $B \geqslant \frac{1}{2}nB'$, provided that $B' \geqslant 2$. In the sequel the constants implied by << will signify positive numbers which are effectively computable in terms of ε ,n, $f_i(\underline{u}_j)$, the defining equations of A, and the valuation $|\ |$. For the validity of the subsequent arguments, we may assume that $B' >> 1$. Since $|\underline{u}| < e^{-\varepsilon B^2}$ and $(p,n) = 1$ in the p-adic case, we have

$$|\underline{u}' + \underline{q}/n| < e^{-\frac{1}{4}\varepsilon n^2 B'^2} \tag{1}$$

We claim that without loss of generality $\underline{f}$ converges at a sufficiently small (but independent of n) neighborhood of $-\underline{q}/n$. This is easy to show in the p-adic case, since by assumption f converges at $\underline{u}_1,\ldots,\underline{u}_m$, we have $(p,n) = 1$,

and $q_1,\ldots,q_m$ are rational integers ; thus $|q_i/n| \leq 1$ in the p-adic valuation, and it follows that $-\underline{q}/n$ belongs to the domain of convergence of $\underline{f}$. In the complex case we argue similarly . Since $\underline{f}$ is analytic at a sufficiently small neighborhood of $\underline{0}$, and since $|q_i/n| \leq 1$, it suffices to show that for each i the number $|\underline{u}_i|$ is small enough. But this can be assumed without loss of generality, upon replacing $\underline{u}_i$, by $\underline{u}_i/k$, where k is a sufficiently large fixed integer ; note that $\underline{u}_i/k$ are again algebraic points, since the group law on A is defined over K; observing that near $-\underline{q}/n$ the map $\underline{f}$ is an analytic isomorphism, we deduce from (1) that

$$|\underline{f}(\underline{u}') - \underline{f}(-\underline{q}/n)| < e^{-(\varepsilon/5)n^2B'^2} \quad ; \tag{2}$$

also we conclude that there is some $i(1 \leq i \leq d')$ such that $f_i(\underline{u}')$ are distinct for infinitely many $\underline{u}'$.

The height $h(a) = h_K(a)$ of an element a of K is defined to be the product of $\max(1, |a|_v)^{n_v}$ over all valuations $|\ |_v$ of K, where n_v denotes the degree of the completion of K at v over the corresponding completion of the rationals $\mathbb{Q}$. The height h(P) of a point $P = (1,a_1,\ldots,a_{d'})$ is defined by a similar product of the terms $\max_i(1,|a_i|_v)^{n_v}$. On taking a finite extension of K, if necessary, we may assume that any $f_i(\underline{u}_j)$ belongs to K. It follows from the Néron-Tate theorem that the function $\log h(P)$ of P is equal to the sum of a positive definite quadratic form, a linear form and a bounded function. Hence there is a positive constant c which depends on the $f_i(\underline{u}_j)$ and on the defining equations of A only, such that

$$\log h(f_i(\underline{u}')) < \log h(\underline{f}(\underline{u}')) < cB'^2 \ .$$

By virtue of the choice of i, (2) implies that there are infinitely many $\underline{u}'$ with distinct $f_i(\underline{u}')$, such that

$$|f_i(\underline{u}') - f_i(-\underline{q}/n)| < h(f_i(\underline{u}'))^{-\varepsilon'n^2} \tag{3}$$

where $\varepsilon' = \varepsilon/6c$. We note that for any $\underline{u}'$ the number $f_i(\underline{u}')$ lies in K, since the group law of A is defined over K, and the $f_i(\underline{u}_j)$ belong to K . Similarly, since $f_i(-\underline{q}/n)$ is a component of an nth division point of $\underline{f}(-\underline{q})$, we deduce that $f_i(-\underline{q}/n)$ is algebraic. But as soon as n is so large that $\varepsilon'n^2 > 2$, the inequality (3) contradicts the conclusion of the Thue-Siegel-Mahler-Roth theorem, and the proof is complete.

In the case that A is an abelian variety of CM-type, namely, when the tensor product $k = \text{End } A \otimes \mathbb{Q}$, of the ring End A of endomorphisms of A and the rationals $\mathbb{Q}$, has a structure of a quadratic imaginary extension of a totally real field k_1 with $[k_1 : \mathbb{Q}] = d$, a much stronger but specialized result is known. It says that for any archimedean or p-adic valuation of K, where the rational prime p splits completely in k_1 and all of its k-prime divisors have the same splitting type, we have :

Theorem 1' : For any $\varepsilon > 0$ there exists a positive constant C', effectively computable in terms of ε, A, $|\ |$, and $f_i(u_j)$, such that for any set of integers $b_1,\ldots,b_m$, not all 0, with absolute values at most B, we have

$$|b_1u_1+\ldots+ b_mu_m| > C' \exp\{-(\log B)(\log\log B)^{1+dm+\varepsilon}\}.$$

Proof : This is proved in [6] in the archimedean case, and [3] in the non-archimedean case.

In fact the results of [6] and [3] are more general, and Theorem 1' is established there with coefficients b_i which are arbitrary diagonal matrices, not all singular, with algebraic entries. However for the applications that we have in mind it suffices to use only the statement given above.

§ 3. Theorems 1 and 1' have the following geometric reformulations. Let d(e,P) denote the Euclidean distance either in the space $\mathbb{C}^{d'}$ or in the space $K^{d'}$ between the origin e and an arbitrary point P on A_o. We have :

Theorem 2 : For any $\varepsilon > 0$ there exists a positive constant C_1 such that for any point $P(\neq e)$ on A_o with coordinates in K we have

$$d(e,P) > C_1\, h(P)^{-\varepsilon}\ .$$

When A is of CM-type and $|\ |$ satisfies the splitting assumption of theorem 1', we have :

Theorem 2' : For any $\varepsilon > 0$ there exists a positive constant C_1', such that for any point $P(\neq e)$ on A_o with coordinates in K we have

$$d(e,P) > C_1'(\log h(P))^{-(\log\log\log h(P))^{1+dr+\varepsilon}}$$

where r denotes the rank of the Mordell-Weil group A_K.

The constants C_1 and C_1' depend on the (ineffective) determination of a base for the Mordell-Weil group A_K of K-rational points on A, in addition to the parameters on which the constants C and C' (of Theorems 1 and 1') depend (in particular, they depend on the given valuation).

The deduction of Theorem 2 (resp. 2') from Theorem 1 (resp. 1') which is similar to the discussion in [5] , was written out in chapter IV, section 3, of the author's 1978 Cambridge UK thesis, and there is no need to repeat the details here. This comment also applies to the deduction of Theorem 3 (resp. 3') below from Theorem 2 (resp. 2').

Finally the above results can be applied to investigate K-rational points on algebraic curves of positive genus. Thus we consider an affine algebraic plane curve E (of positive genus) such that there exists a non-constant rational map $b : E \to A$, where A is an abelian variety, and E, b and A are defined over K. Let V be a finite set of valuations on K including all of the infinite primes. We define the (generalized) size $S_V(P)$ of a K-rational point $P = (x,y)$ on E to be the product of the terms $M_v = \mathrm{Max}(1, |X|_v, |y|_v)^{n_v}$ over all primes v in V ; similarly we define the (generalized) denominator $D_V(P)$ of P to be the product over all primes v outside V of the terms M_v. We have :

Theorem 3 : For any $\varepsilon > 0$ there exists a positive constant C_2, such that for any K-rational point P on E we have

$$S_V(P) < C_2 D_V(P)^{\varepsilon}$$

The Siegel-Mahler theorem asserts that the number of K-rational points on E whose denominators consist of powers of primes from a finite set W of K-primes is finite. This can be deduced from Theorem 3 on taking A to be the Jacobian variety of the curve and a set V of valuations on K which contains W, and on putting $D_V(P) = 1$.

If A is of CM-type with dimension d and V is a finite set of valuations on K, which in addition to all archimedean valuations, contains only valuations for which Theorems 1' and 2' hold, we have :

Theorem 3' : For any $\varepsilon (0 < \varepsilon < 1)$ there exists a positive constant C_2' such that for any K-rational P on E we have

$$S_V(P) < C_2' (\log D_V(P))^{(\log \log \log D_V(P))^{1+dr+\varepsilon}}$$

The constants C_2 and C_2' depend on ε, V, K and E, and are as ineffective as the constants C_1 and C_1' (respectively).

References

[1] Bertrand D., and Flicker, Y., Linear forms on abelian varieties over local fields, Acta Arith., to appear.

[2] Coates, J. , An application of the Thue-Siegel-Roth theorem to elliptic functions, Proc. Camb. Phil. Soc., 69 (1971) 157-61.

[3] Flicker, Y. , Linear forms on abelian varieties over local fields : a sharpening, preprint.

[4] Lang, S., Diophantine approximations on toruses, Amer. J. Math., 86 (1964), 521-33.

[5] Masser, D.,Linear forms in algebraic points of abelian functions III, Proc. London Math. Soc., 33 (1976), 549-64.

[6] Masser, D., Diophantine approximations and lattices with complex multiplication, Inv. Math., 45 (1978), 61-82.

[7] Siegel, C. , Über einige Anwendungen Diophantischer Approximationen, Abh. Preuss. Akad. Wiss., 1 (1929) ; Ges. Ab. I., 242-66.

Department of Mathematics
Columbia University
New York, New York 10027
U. S. A.