ANNALES

DE

L'INSTITUT FOURIER

Jonathan PILA

Rational points on a subanalytic surface

Tome 55, nº 5 (2005), p. 1501-1516.

<http://aif.cedram.org/item?id=AIF_2005__55_5_1501_0>

Ann. Inst. Fourier, Grenoble
55, 5 (2005), 1501–1516

RATIONAL POINTS ON A SUBANALYTIC SURFACE

by Jonathan PILA

---

1. Introduction.

This paper is concerned with certain diophantine properties of *subanalytic sets* in $\mathbb{R}^n$; specifically the distribution of rational points. A definition of the class of subanalytic sets and derivation of their main properties may be found in [1]; a summary is in [10]. The class of subanalytic sets is larger than the class of semianalytic sets, yet there are strong uniformization and finiteness results. They are a suitable class of nonalgebraic objects in which to study diophantine questions. A *subanalytic surface* will mean a subanalytic set of dimension 2.

Suppose $X \subset \mathbb{R}^n$ is a subanalytic set of dimension $\geqslant 2$. Then X may contain subsets of positive dimension that are semialgebraic, even if X itself is not semialgebraic. Such a subset (e.g. a line) may contain many rational points. Let then X^{a} be the union of all connected semialgebraic subsets of X of positive dimension (note: X^{a} may not be subanalytic [10]). Treating X^{a} in analogy with the *special set* in diophantine geometry [7] I, § 3; [5] § F.5, strong scarcity properties might be expected for the rational points in the complementary subset $X^{\mathrm{t}} = X - X^{\mathrm{a}}$.

Now X^{t} may certainly contain infinitely many rational points (e.g. $X = \{(x, y) \in \mathbb{R}^2, y = 2^x\}$ or, for compact examples, see [10] 7.5), so a natural way to express the scarcity of rational points is by a density

Keywords: Subanalytic set, rational point.
Math. classification: 11D99, 11J99.

estimate relative to a suitable height function. When X is an algebraic variety, it is natural to use the *projective height*

$$H_{\mathrm{proj}}(a_1/b, a_2/b, \ldots, a_n/b) = \max\{|a_i|, b\}$$

when $a_i, b \in \mathbb{Z}, b > 0, (a_1, a_2, \ldots, a_n, b) = 1$. Here the projective height is a less canonical choice, and it will be more natural to use a different height and associated counting function. Thus for $a_i, b_i \in \mathbb{Z}, b_i > 0$, and $\gcd(a_i, b_i) = 1$ for $i = 1, 2, \ldots, n$ set

$$H(a_1/b_1, a_2/b_2, \ldots, a_n/b_n) = \max\{|a_i|, b_i\}.$$

For $X \subset \mathbb{R}^n$ let $X(\mathbb{Q})$ denote the subset of X consisting of points having rational coordinates. Let further $X(\mathbb{Q}, B) = \{P \in X(\mathbb{Q}), H(P) \leqslant B\}$ and set

$$N(X, B) = \# X(\mathbb{Q}, B).$$

Note that $H(P) \leqslant H_{\mathrm{proj}}(P)$. Indeed $\mathbb{R}^n(\mathbb{Q}, B)$ is of order B^{2n} as $B \to \infty$, compared with order B^{n+1} for the projective height.

The following conjecture is made in [10], 7.4.

Conjecture. — *Let $X \subset \mathbb{R}^n$ be a compact subanalytic set and $\epsilon > 0$. There is a constant $c(X, \epsilon)$ such that*

$$N(X^{\mathrm{t}}, B) \leqslant c(X, \epsilon) B^{\epsilon},$$

for all $B \geqslant 1$.

For X of dimension 1, the validity of this conjecture essentially follows from [8], Theorem 9, as noted in [10], Remark 7.4. The aforementioned examples from [10] 7.5, show that, even in dimension 1, such an estimate cannot be much improved in general.

In [10] an analogous conjecture is made for the integer points on the homothetic dilation sX of compact $X \subset \mathbb{R}^n$ for $s \geqslant 1$, namely that $\# sX^{\mathrm{t}}(\mathbb{Z})$ is $O_{X,\epsilon}(s^{\epsilon})$ for all $\epsilon > 0$, and it is proved in dimension 2. (In dimension 1, it follows from results in [3]). This is a somewhat weaker statement: it implies an estimate of the form $O_{X,\epsilon}(B^{\epsilon})$ for rational points of X^{t} with denominator *dividing* B. However it is not strictly weaker, since the dilation parameter s need not be an integer.

The primary goal of this paper is to prove the conjecture on rational points in dimension 2.

Theorem 1.1. — *Let $X \subset \mathbb{R}^n$ be a compact subanalytic surface and let $\epsilon > 0$. There is a constant $c(X, \epsilon)$ such that, for all $B \geqslant 1$,*

$$N(X^{\mathrm{t}}, B) \leqslant c(X, \epsilon) B^{\epsilon}.$$

The proof of this theorem proceeds by showing that the points in question lie on very few intersections of X with hypersurfaces of suitable degree. These intersections will be semianalytic curves. Concluding the proof depends on having an estimate for rational points on such curves (when they are not semialgebraic) that is suitably uniform.

Thus a subsidiary goal is to establish a suitable estimate for rational points on a smooth curve. A prototype of the type of result needed (but for integer points) is the well-known result of Jarnik [6] that a strictly convex plane curve $\Gamma : y = f(x)$ of length $\ell \geqslant 1$ contains at most

$$3(4\pi)^{-1/3}\ell^{2/3} + O(\ell^{1/3})$$

integer points (indeed Jarnik showed that the exponent and constant above are best possible).

The bound for rational points on curves likewise proceeds by showing that the points lie on few algebraic curves of controlled degree. In the following result the hypothesis that $|f'| \leqslant 1$ controls the length of the curve. The point is that the estimate depends only on the nonvanishing of a certain derivative, and is otherwise independent of f.

THEOREM 1.2. — *Let $\epsilon > 0$. There exist $d = d(\epsilon), D = D(\epsilon) \in \mathbb{N}$ and $c(\epsilon) > 0$ with the following property.*

Let $B \geqslant 1, L \geqslant 1/B^2$. Suppose I is a closed interval with $|I| \leqslant L$. Suppose $f \in C^D(I)$ with $|f'| \leqslant 1$ on I and $f^{(D)}$ nonvanishing in the interior of I. Let Γ be the graph of f. Then $\Gamma(\mathbb{Q}, B)$ is contained in the union of at most

$$c(\epsilon)(LB^3)^{\epsilon}$$

real algebraic curves of degree d.

The number of intersections of the graph of a sufficiently smooth function with a curve of given degree can also be controlled by suitable nonvanishing conditions on the function [8].

THEOREM 1.3. — *Let $\epsilon > 0$. There exist $d = d(\epsilon), D = D(\epsilon) \in \mathbb{N}$, $Z = Z_\epsilon \in \mathbb{R}[X_1, \ldots, X_D]$ and $c(\epsilon) > 0$ with the following property.*

Let $B \geqslant 1, L \geqslant 1/B^2$. Suppose I is a closed interval with $|I| \leqslant L$. Suppose $f \in C^D(I)$ with $|f'| \leqslant 1$ on I and $Z(f) = Z(f, f', f'', \ldots, f^{(D)})$ nonvanishing in the interior of I. Let Γ be the graph of f. Then

$$N(\Gamma, B) \leqslant c(\epsilon)(LB^3)^{\epsilon}.$$

Moreover, if f is transcendental analytic then $Z(f)$ has only finitely many zeros on I.

Bounds of this shape for integer points follow from the results of [3], [8]. The fact that a variant of the method used to get uniform bounds for integer points could be applied successfully to rational points was inexplicably missed in [8]. Unlike Jarnik's result these results are presumeably very far from optimal in any sense. For strengthenings of Jarnik's result using minimal additional regularity see [13], [12].

When f is a transcendental analytic function on a compact interval, Theorem 1.3 may be applied for arbitrary positive ϵ after dividing I into finitely many (depending on ϵ) intervals in the interior of which Z_ϵ is nonvanishing. This yields an estimate of the shape

$$N(\Gamma, B) \leqslant c(f,\epsilon)B^{\epsilon}.$$

Now such an estimate for rational points on a transcendental analytic curve was established in [8] but with the constant dependent on the norms of derivatives of f (up to order $O_\epsilon(1)$). The present estimate depends only on the number of vanishing points of Z_ϵ. This uniformity is the key in the application to surfaces.

A final objective of this paper is to apply the present methods to rational points on algebraic curves. Although the height H is somewhat unnatural in the algebraic context, the result obtained is of the same shape as those previously obtained for the projective height, and hence is somewhat stronger.

Theorem 1.4. — *Let $b, c \geqslant 2$ be integers and $B \geqslant 3$. Let $F \in \mathbb{R}[x,y]$ be irreducible of bidegree (b,c). Let $d = \max(b,c)$ and let $X = \{P \in \mathbb{R}^2 : F(P) = 0\}$. Then*

$$N(X,B) \leqslant \left(8d^2\right)^{2d+7} B^{2/d} \left(\log B\right)^{2d+4}.$$

Heath-Brown [4] has shown that, for an irreducible plane curve X of degree d,

$$N_{\mathrm{proj}}(X,B) = \#\{P \in X(\mathbb{Q}), H_{\mathrm{proj}}(P) \leqslant B\} \leqslant c(d,\epsilon)B^{2/d+\epsilon}.$$

It appears very likely that, in Heath-Brown's approach, one can replace B^ϵ by $(\log B)^A$ for some constant A depending (at most) on d. As observed by Bombieri [2], Heath-Brown's result can be combined with Segre embeddings and a neat height argument to yield an estimate for $N(X,B)$ with exponent

$2/d + \epsilon$, the same exponent of B as in 1.4. It is unclear if this argument, which uses Segre embeddings of increasing degree as $\epsilon \to 0$, yields so sharp a result as above. The exponent $2/d$ is best possible here (and in Heath-Brown's result) in view of the curve $y = x^d$.

It seems interesting to consider diophantine questions in other classes of sets having suitable finiteness properties. Wilkie [14] studies integer points on curves in o-minimal structures; a result on the rational points of a *pfaff curve* is contained in [11].

Acknowledgements. This paper was written while I was a visitor at the Mathematical Institute, University of Oxford. I am grateful to the Institute for its hospitality, and would like to express thanks in particular to A. Lauder and D.R. Heath-Brown. I thank A. Venkatesh for a helpful conversation, and E. Descheemaeker for assistance. My thanks also to the referee for a careful reading. My visit to Oxford was supported by my home institution, McGill University, and in part by a grant from NSERC, Canada.

2. Smooth curves.

The starting point is the following alternant mean value theorem. In the form given it is contained in [3] Proposition 2 et seq.; variants go back to the nineteenth century.

Proposition 2.1. — *Let $D \in \mathbb{N}$. Suppose $f_1, \ldots, f_D$ possess $D-1$ continuous derivatives on an interval I and let $x_1, x_2, \ldots, x_D \in I$ with $x_1 < x_2 < \ldots < x_D$. Then there exist points $\xi_{ij} \in [x_1, x_D]$ such that*

$$\det\Big(f_j(x_i)\Big) = V(x_1, x_2, \ldots, x_D) \det\left(\frac{f_j^{(i-1)}(\xi_{ij})}{(i-1)!}\right),$$

where $V(x_1, x_2, \ldots, x_D)$ denotes the Vandermonde determinant. $\square$

The above will be applied with $f_j = x^h f(x)^k$ for suitable index sets of pairs (h, k). The following notation will be convenient.

Let $M = \{x^h y^k : (h,k) \in J\}$ be a finite set of monomials in the indeterminates x, y. Let

$$D = \#M, \quad R = \sum_{(h,k)\in J} (h+k), \quad s = \max_{(h,k)\in J}(h), \quad t = \max_{(h,k)\in J}(k), \quad S = D\big(s+t\big),$$

$$\alpha = \frac{2R}{D(D-1)}, \quad C = \big(D!D^R\big)^{2/(D(D-1))} + 1.$$

Define a relation $\preceq$ on the set of monomials in x, y by setting $x^h y^k \preceq x^u y^v$ if $h \leqslant u$ and $k \leqslant v$ and call a M *closed under* $\preceq$ if $m_1 \preceq m_2 \in M$ implies $m_1 \in M$.

If Y is a plane algebraic curve defined by $G(x,y) = 0$, say Y is *defined in* M if the monomials appearing in G all belong to M. If f is a function and $m = x^h y^k$ is a monomial let f_m denote the function $x^h f(x)^k$.

Definition 2.2. — *Let $L \geqslant 0, k \in \mathbb{N}, k \geqslant 1$. Let I be a closed bounded interval. For a function $f \in C^k(I)$ set*

$$A_{L,k}(f) = \max_{1 \leqslant \kappa \leqslant k} \sup_{t \in I} \left\{1, \frac{L^{\kappa-1}|f^{(\kappa)}(t)|}{\kappa!}\right\}^{k/\kappa}.$$

For a finite set M of monomials set

$$A_{L,M}(f) = A_{L,D-1}^{1/(D-1)}(f).$$

With the above notation, Proposition 2.1 can be reformulated as follows.

Lemma 2.3. — *Let $M = \{m_j, j = 1, \ldots, D\}$ be a finite set of monomials, closed under $\preceq$ with $D \geqslant 2$. Suppose that I is a closed interval with $|I| \leqslant L$ and that $f \in C^{D-1}(I)$ with $|f'| \leqslant 1$. Let $x_1, x_2, \ldots, x_D \in I$ with $x_1 < x_2 < \ldots < x_D$ and put $f_j = f_{m_j}$. Let*

$$\Delta = \det\big(f_j(x_i)\big)$$

Then

$$|\Delta| \leqslant V(x_1, \ldots, x_D) L^{R-D(D-1)/2} D!\, D^R\, A_{L,D-1}^{D/2}(f).$$

Proof. — This is essentially [9], Lemma 3. The assumption there that $|f| \leqslant L$ is obviated by the assumption here that M is closed under $\preceq$. With this assumption, elementary column operations can be used to replace each function f_m by $f_m(x) - f_m(x_0)$ for some $x_0 \in I$. □

Lemma 2.4. — *Let M be a finite set of monomials, and define D, C, R, S as above. Let $B \geqslant 1, L \geqslant 0$ with $L^R B^S \geqslant 1$.*

Let I be a closed interval with $|I| \leqslant L$ and $f \in C^{D-1}(I)$ with $|f'| \leqslant 1$ and graph Γ. Then $\Gamma(\mathbb{Q}, B)$ is contained in the union of not more than

$$C\big(L^R B^S\big)^{2/(D(D-1))} A_{L,M}(f)$$

real algebraic curves defined in M.

Proof. — The proof proceeds as the proof of the "Main Lemma" of [3], [8]. Suppose $M = \{m_j, j = 1, \ldots, D\}$ and write f_j for f_{m_j}. If $x_1 < x_2 < \ldots < x_D$ and $(x_1, y_1), \ldots, (x_D, y_D)$ are points of $\Gamma(\mathbb{Q}, B)$ that do not lie on any real algebraic defined in M, then

$$\Delta = \det\Big(f_j(x_i)\Big) \neq 0.$$

Now $H(x_i), H(y_i) \leqslant B$, so there are positive integers $b_i, c_i \leqslant B$ such that $b_i x_i, c_i y_i \in \mathbb{Z}$ whence

$$\Delta \prod_{i=1}^{D} b_i^s\, c_i^t \in \mathbb{Z}.$$

By 2.3 and the preceding definitions it follows that

$$1 \leqslant V(x_1, \ldots, x_D)\, L^{R-D(D-1)/2}\, B^S\, D!\, D^R\, A_{L,D-1}^{D/2}(f).$$

Now $V(x_1, \ldots, x_D) \leqslant (x_D - x_1)^{D(D-1)/2}$, and $(D! D^R)^{2/(D(D-1))} = C - 1$ and so

$$(C-1)(x_D - x_1) \geqslant L\big(L^R B^S\big)^{-2/(D(D-1))} A_{L,D-1}^{-1/(D-1)}(f).$$

Since $|I| \leqslant L$, it can be divided into at most

$$(C-1)\big(L^R B^S\big)^{2/(D(D-1))} A_{L,D-1}^{1/(D-1)}(f) + 1 \leqslant C\big(L^R B^S\big)^{2/(D(D-1))} A_{L,M}(f)$$

subintervals, on each of which the points in question lie on a single curve defined in M. □

For the set $M(d)$ of all monomials of total degree $\leqslant d$, elementary computations find

$$D = \frac{(d+1)(d+2)}{2}, \quad R = 2dD/3, \quad s = t = d, \quad S = 2dD = 3R,$$
$$\alpha = \frac{8}{3(d+3)}, \quad C \leqslant 6.$$

Corollary 2.5. — *Let $M = M(d), d \geqslant 2$. Then $\Gamma(\mathbb{Q}, B)$ is contained in the union of at most*

$$6\Big(LB^3\Big)^{8/3(d+3)} A_{L,M}(f)$$

real algebraic curves of degree d. □

To deduce 1.2 it remains to eliminate the dependence of 2.5 on the norms of derivatives of f. This will be accomplished by showing that, if f does not oscillate, intervals where derivatives are large are short and few.

LEMMA 2.6 ([3], Lemma 7). — *Suppose $A \geqslant 1, L > 0, k \in \mathbb{N}$. Let I be a closed interval with $|I| \leqslant L$ and $g \in C^k(I)$ with $|g'(x)| \leqslant 1$ throughout I. Suppose further that*

$$|g^{(\kappa)}(x)| \leqslant i! A^{\kappa/k} L^{1-\kappa}$$

for $1 \leqslant i < k$ and all $x \in I$ and that, for all $x \in I$,

$$|g^{(k)}(x)| \geqslant k! A L^{1-k}.$$

Then

$$|I| \leqslant 2A^{-1/k} L.$$

□

Proof of Theorem 1.2. — The proof follows the recurrence argument used in [3] and [8]. Choose $d = d(\epsilon)$ such that

$$\frac{8}{3(d+3)} \leqslant \epsilon.$$

Let $M = M(d)$, so that $D = D(\epsilon) = (d+1)(d+2)/2$.

For a function g verifying the conditions stated for f in Theorem 1.2 and with graph Γ, let $G(g)$ denote the minimum number of curves defined in M that contain $\Gamma(\mathbb{Q}, B)$. Let $G(L) = G(D, d, B, L)$ denote the maximum of $G(g)$ over all g.

Now suppose g is such a function. Let $A \geqslant 1$. Since $g^{(D)}$ is nonvanishing in the interior of I, an equation of the form $g^{(\kappa)}(x) = c, 1 \leqslant \kappa \leqslant D-1, c \in \mathbb{R}$, has at most $D - \kappa$ solutions interior to I. Thus I may be divided into most $2\sum_{\kappa=1}^{D-1}(D-\kappa) \leqslant D^2$ subintervals I_ν such that, for each I_ν and each $\kappa = 1, 2, \ldots, D-1$ either (i) or (ii) holds:

(i) $|g^{(\kappa)}(x)| \leqslant \kappa! A^{\kappa/(D-1)} L^{1-\kappa}$ for all $x \in I_\nu$;

(ii) $|g^{(\kappa)}(x)| \geqslant \kappa! A^{\kappa/(D-1)} L^{1-\kappa}$ for all $x \in I_\nu$.

On an interval I_ν satisfying (i) for all κ, $A_{L,D-1}(g) \leqslant A$. According to Corollary 2.5, the points in question on this interval then lie on not more than

$$6(LB^3)^{2R/(D(D-1))}\, A^{1/(D-1)}$$

real algebraic curves of degree d.

If an interval I_ν has (ii) for some κ, and hence for some least $\kappa \geqslant 2$, then, by Lemma 2.6,

$$|I_\nu| \leqslant 2\, A^{-1/(D-1)}\, L.$$

The function $G(L)$ therefore satisfies the following recurrence when $L \geqslant 1/H^2$:

$$G(L) \leqslant u\, B^{3\alpha}\, L^{\alpha} + v\, G(\lambda L),$$

where

$$\lambda = 2A^{-1/(D-1)}, \;\; u = 6\, D^2\, A^{1/(D-1)}, \;\; v = D^2.$$

Thus, provided $\lambda^{n-1} L \geqslant 1/B^2$,

$$G(L) \leqslant u\,(LB^3)^{\alpha}(1 + v\lambda^{\alpha} + \ldots + (v\lambda^{\alpha})^{n-1}) + v^n G(\lambda^n L).$$

Choose λ so that $v\lambda^{\alpha} = 1/2$; that is,

$$\lambda = \Big(\frac{1}{2v}\Big)^{1/\alpha} = \big(2D^2\big)^{-D(D-1)/2R}.$$

Then A is determined (and note $A \geqslant 1$), with

$$A^{1/(D-1)} = \frac{2}{\lambda} = 2\big(2D^2\big)^{D(D-1)/2R}.$$

Now take n such that

$$\frac{\lambda}{LB^2} \leqslant \lambda^n < \frac{1}{LB^2}.$$

Then $G(\lambda^n L) \leqslant 1$ and

$$\begin{aligned} G(L) \leqslant 2u(LB^3)^{\alpha} + 2^{-n}\lambda^{-\alpha}(LB^2)^{\alpha} &\leqslant 12D^2(LB^3)^{\alpha}A^{1/(D-1)} + 2D^2(LB^2)^{\alpha} \\ &\leqslant 28D^2(2D^2)^{D(D-1)/2R}\big(LB^3\big)^{8/3(d+3)}. \end{aligned}$$

□

The additional ingredient needed to prove 1.3 is to control the number of points of Γ that may lie on any curve of degree d. This can be effected by the nonvanishing of appropriate Wronskian determinants, as shown in [8]. If $f_1, \ldots, f_n$ are functions with $n-1$ derivatives, let $W(f_1, \ldots, f_n)$ denote the Wronskian determinant.

Lemma 2.7 ([8], Theorem 1). — *Let $M = \{m_1, \ldots, m_D\}$ be a set of monomials. Let f possess $D-1$ derivatives on an interval I, and put $f_j = f_{m_j}, j = 1, \ldots, D$. If the D Wronskians*

$$W(f_1, f_2, \ldots, f_k), \quad k = 1, \ldots, D$$

are nonvanishing throughout the interior of I then the intersection of Γ and any curve defined in M consists of at most $D-1$ points. □

Note that a different condition is obtained by reordering the set of monomials (or using polynomials). See [8] for further discussion and applications; it is shown there that there is natural necessary and sufficient nonvanishing condition under which Γ (where $f \in C^5(I)$) intersects any curve of degree 2 in at most 5 points (counting multiplicity).

Definition 2.8. — *Let $d \in \mathbb{N}$ and f a function possessing D derivatives on an interval I. Fix an ordering of the set $M(d) = \{m_1, \ldots, m_D\}$ of monomials of degree $\leqslant d$. Let $f_j = f_{m_j}$. Define*

$$Z_d(f, f', \ldots, f^{(D)}) = f^{(D)} \prod_{k=1}^{D} W(f_1, \ldots, f_k).$$

Proof of Theorem 1.3. — The first assertion is immediate from 1.2, 2.7. The second assertion follows from [8], Proposition 4. □

Remarks 2.9. — 1. As already mentioned, a simpler choice of Z for $d = 2$ is possible by [8].

2. A result for parametrized curves Γ can be proved by the same method. The number of possible intersections of Γ with curves of degree d is intrinsic to Γ, but the oscillation of the parametrizing functions depends on the parametrization. This raises the question of how "good" a parametrization can be expected. The method of proof in effect replaces the parametrizing interval I by a system of intervals on which not only f' but the subsequent derivatives up to order $D-1$ are absolutely bounded, using the nonvanishing of $f^{(D)}$ to control the number of intervals required. The question arises whether reparametrizing Γ using a single interval could yield a better result.

3. Theorems 1.2 and 1.3 remain valid with respect to a still weaker "denominator only" height $H^*(P) = \max\{b_i\}$, where $P = (a_1/b_1, \ldots, a_n/b_n)$, $a_i, b_i \in \mathbb{Z}, b_i > 0, (a_i, b_i) = 1$, with counting function $N^*(X, B) = \#\{P \in X(\mathbb{Q}), H^*(P) \leqslant B\}$. Note that H^* does not have the property $\#\{P \in \mathbb{R}^n(\mathbb{Q}), H^*(P) \leqslant B\} < \infty$ usually required of height functions; indeed $\{P \in \mathbb{R}^n(\mathbb{Q}), H^*(P) \leqslant 1\} = \mathbb{Z}^n$.

3. Subanalytic surfaces.

Proof of Theorem 1.1. — The deduction of 1.1 from 1.2 is identical to the deduction of [10], Theorem 1.3 from [10], Proposition 8.1. A sketch of the argument is as follows.

Let $X \subset \mathbb{R}^n$ be a compact subanalytic surface. By the Uniformization Theorem [1], 0.1, there is a compact real analytic manifold N of dimension 2, and a proper real analytic map $\psi : N \to \mathbb{R}^n$ with $\psi(N) = X$. Such N has a finite number of connected components, and it suffices to consider the case that N is connected.

Arguing as in the early paragraphs of [10], Proof of 1.3: if $n \leqslant 2$ or if the image of X in every projection of $\mathbb{R}^n$ onto three of its coordinates is contained in a hypersurface, then X^{t} has dimension $\leqslant 1$, and the conclusion follows from [10], Proof of Conjecture 1.1 and 1.2 for curves and Remark 7.4.

Now by [10], Lemma 4.4 and Remark 4.5, for suitably large $b \in \mathbb{N}$, the set $X(\mathbb{Q}, B)$ is contained in the intersection of X with at most

$$O_{X,\epsilon}(B^{\epsilon/2})$$

hypersurfaces Υ of degree b that do not contain X.

Fix $d \in \mathbb{N}$ with $8/3(d+3) \leqslant \epsilon/2$, $D = (d+1)(d+2)/2$ for the application of 1.2.

The sets $V = \psi^{-1}(\Upsilon)$ are semianalytic sets of dimension $\leqslant 1$. Moreover the number of connected components of such V (which may be points or curves) are bounded by Gabrielov's Theorem [1], 3.14, as Υ ranges over all hypersurfaces of degree d. This principle will be applied again after a further decomposition of the sets V.

Let $\Pi \subset \mathbb{R}^n$ be a plane with coordinates (u, v) and $\pi : \mathbb{R}^n \to \Pi$ the orthogonal projection. Let V_{s} be the singular points of V, a set of dimension $\leqslant 0$. With respect to Π, the set V_{ns} of nonsingular points of V may be decomposed as follows into subanalytic subsets. First, V_{u} is the subset of V_{ns} of points at which the projection $\pi(V_{\mathrm{ns}})$ has indeterminate slope (i.e., for components of dimension 1, they map to a point in Π); next V_{a} is the subset of $V_{\mathrm{ns}} - V_{\mathrm{u}}$ where the slope in Π belongs to $\{0, \pm 1, \infty\}$. At the remaining points $\pi(V)$ is a graph with respect to both axes, (and with slope $\leqslant 1$ in absolute value with respect to one of the axes). Let V_{b} be the subset of points where the derivative of order D with respect to one of the axes vanishes. Call the remaining set V_{c}.

The number of connected components in each of the sets $V_{\mathrm{s}}, V_{\mathrm{a}}, V_{\mathrm{b}}, V_{\mathrm{c}}$ is again uniformly bounded over all Υ by Gabrielov's theorem. So components of dimension 0, i.e. points, contribute at most $O_{X,\epsilon}(B^{\epsilon/2})$ in total.

If $P \in X(\mathbb{Q}, B)$ then P lies on one of the sets V. If it belongs to a connected component γ of dimension 1 of V_{c} then, after projection into Π, the point $\pi(P)$ lies on a graph with respect to one of the coordinate axes of an analytic function f having slope $|f'| \leqslant 1$ and $f^{(D)} \neq 0$. Moreover $H(\pi(P)) \leqslant B$.

If f is transcendental then the number of intersections of $\pi(\gamma)$ with a plane curve $Y \subset \Pi$ of degree d will be finite and moreover bounded over all Υ of degree b and $Y \subset \Pi$ by Gabrielov's theorem. For such components γ an estimate $N(\gamma, B) = O_{X,\epsilon}(B^{\epsilon/2})$ follows from Theorem 1.2 applied with curves of degree d.

It remains to take care of the cases in which P lies in a connected component of dimension 1 of one of the other sets $V_{\mathrm{u}}, V_{\mathrm{a}}$ or V_{b}, and the case that $P \in V_{\mathrm{c}}$ where V_{c} is not semialgebraic but its projection into Π is semialgebraic. Note that the projections of components $V_{\mathrm{u}}, V_{\mathrm{a}}, V_{\mathrm{b}}$ are semialgebraic.

Let then $\mathbf{\Pi}$ be the set of coordinate planes of $\mathbb{R}^n$ (i.e. planes on two of the coordinates of $\mathbb{R}^n$). If a connected subanalytic curve $\gamma \subset X$ has the property that its projection into Π is semialgebraic for all $\Pi \in \mathbf{\Pi}$ then $\gamma \subset X^{\mathrm{a}}$ (see [10], 7.2 and Proof of 1.3).

Decompose V with respect to all $\Pi \in \mathbf{\Pi}$, i.e. for each map $\theta : \mathbf{\Pi} \to \{\mathrm{u}, \mathrm{a}, \mathrm{b}, \mathrm{c}\}$ take

$$V_\theta = \bigcap_{\Pi \in \mathbf{\Pi}} V^{\Pi}_{\theta(\Pi)}$$

where $V^{\Pi}_{\mathrm{u}}, V^{\Pi}_{\mathrm{a}}, V^{\Pi}_{\mathrm{b}}, V^{\Pi}_{\mathrm{c}}$ is the decomposition with respect to Π.

If $P \in X(\mathbb{Q}, B) \cap V$ is not in X^{a}, and is not one of $O_{X,\epsilon}(1)$ isolated points of a component in the decomposition of V, then, for some $\Pi \in \mathbf{\Pi}$, it lies in a component of dimension 1 of V_{c} whose image in Π is transcendental.

Now, by Gabrielov's Theorem, the number of connected components of each constituent set V_θ is again uniformly bounded (over Υ of degree b), and the number of intersections of the projection of any component into any $\Pi \in \mathbf{\Pi}$ whose image is transcendental with a curve Y of degree d is uniformly bounded (over Y of degree d and $\Pi \in \mathbf{\Pi}$). There are thus $O_{X,\epsilon}(B^{\epsilon/2})$ components in all. So now application of 1.2. completes the proof. $\square$

Remark 3.1. — Theorem 1.1 remains valid with respect to H^*.

4. Algebraic curves.

For integers $\beta, \gamma \geqslant 2$ let

$$M(\beta,\gamma) = \{x^h y^k : 0 \leqslant h \leqslant \beta - 1, 0 \leqslant k \leqslant \gamma - 1\}.$$

Then, for $M = M(\beta, \gamma)$,

$$D = \beta\gamma, \quad R = \frac{D\,(\gamma + \beta - 2)}{2}, \quad S = D(\beta - 1 + \gamma - 1) = 2R, \quad C \leqslant 2D.$$

The last requires an elementary computation; A further elementary observation ([9]) is that

$$\max\left(\frac{1}{\beta}, \frac{1}{\gamma}\right) \leqslant \alpha \leqslant \frac{1}{\beta} + \frac{1}{\gamma}.$$

Note that M is closed under $\preceq$. The following results from 2.4.

LEMMA 4.1. — *Let $M = M(\beta,\gamma), B \geqslant 1, L \geqslant 1/B^2$.*

Suppose I is a closed interval with $|I| \leqslant L$ and $f \in C^{D-1}(I)$ with $|f'| \leqslant 1$. Let Γ be the graph of f. Then $\{P \in \Gamma, H(P) \leqslant B\}$ is contained in the union of at most

$$2D(LB^2)^{2R/(D(D-1))} A_{L,M}(f)$$

real algebraic curves defined in $M(\beta,\gamma)$. □

LEMMA 4.2. — *Let $B \geqslant 1, L \geqslant 1/B^2$ and $b, c \geqslant 2$ integers.*

Let f be a C^∞ function on a closed interval I with $|I| \leqslant L$ and $|f'| \leqslant 1$. Suppose f satisfies an algebraic relation $F(x, f(x)) = 0$ where F is irreducible of bidegree (b, c). Let $d = \max(b, c)$, and $\delta \in \mathbb{N}, \delta \geqslant d$. Let Γ be the graph of f. Then

$$N(\Gamma, B) \leqslant \left(4d^2\delta\right)^{2d+4} (LB^2)^{1/d+1/\delta}.$$

Proof. — This will follow the scheme of 2.9.

Let $G(L) = G(b, c, B, L)$ denote the maximum number of rational points of height $\leqslant B$ that can lie on the graph Γ of a function g with the hypothesized properties on an interval I. So g satisfies a relation $F(x, g(x)) = 0$. The curve $Y : F(x, y) = 0$ has degree $\leqslant b + c \leqslant 2d$.

By [3], Lemma 6, for $A \geqslant 1$, the interval I can be subdivided into at most $2(2d)^2(D-1)^2$ subintervals I_ν such that, on each subinterval and for each $\kappa = 1, \ldots, D-1$ either (i) or (ii) holds:

(i) $|g^{(\kappa)}(x)| \leqslant \kappa! A^{\kappa/(D-1)} L^{1-\kappa}$ for all $x \in I_\nu$; or

(ii) $|g^{(\kappa)}(x)| \geqslant \kappa! A^{\kappa/(D-1)} L^{1-\kappa}$ for all $x \in I_\nu$.

If case (i) holds for all κ then $A_{L,D-1}(g) \leqslant A$. Intervals I_ν that are in case (ii) for any index (and hence for some smallest index $k \geqslant 2$) have length at most $2A^{-1/(D-1)}L$, according to 2.6 applied with $A = A^{k/(D-1)}$.

Let $\delta \geqslant d$ and apply 4.1 with $M = M(d,\delta)$ if $d = b$, or with $M = M(\delta, d)$ if $d = c$. Then Γ intersects properly with any curve defined in M, hence such intersection consists of at most $(b+c)(d+\delta) \leqslant 2d\,2\delta \leqslant 4D$ points.

It follows that $G(L)$ satisfies the recurrence relation

$$G(L) \leqslant u\, B^{2\alpha} L^\alpha + v\, G(\lambda L)$$

while $LB^2 \geqslant 1$, where

$$u = 64\, d^2\, D^2\, (D-1)^2\, A^{1/(D-1)}, \quad v = 8\, d^2\, (D-1)^2, \quad \lambda = 2\, A^{-1/(D-1)}.$$

Choosing $A^{1/(D-1)} = 2(2v)^{1/\alpha} \leqslant 2\big(16d^2(D-1)^2\big)^d$, so that $v\lambda^\alpha = 1/2$, and n so that

$$\frac{\lambda}{LB^2} \leqslant \lambda^n < \frac{1}{LB^2},$$

(whence $G(\lambda^n L) \leqslant 1$) implies that

$$\begin{aligned} G(L) &\leqslant uB^{2\alpha}\big(1 + v\lambda^\alpha + \ldots + (v\lambda^\alpha)^{n-1}\big)L^\alpha + v^n\, G(\lambda^n L) \\ &\leqslant 2u(LB^2)^\alpha + \lambda^{-\alpha}(LB^2)^\alpha \leqslant 2(u+v)(LB^2)^\alpha \\ &\leqslant 16 d^2 D^2 \big(16 D^2 \big(16 d^2 (D-1)^2\big)^d + 1\big)\big)(LB^2)^\alpha \\ &\leqslant 256 d^6 \delta^4 \big(16 d^4 \delta^2\big)^d \big(LB^2\big)^{1/d + 1/\delta}. \end{aligned}$$

□

Proof of Theorem 1.4. — Let $P = (x,y) \in X(\mathbb{Q})$ with $H(P) \leqslant B$. Then one of the following holds:

(i) $|x|, |y| \leqslant 1$

(ii) $|x| \leqslant 1, |y| > 1$

(iii) $|x| > 1, |y| \leqslant 1$

(iv) $|x| > 1, |y| > 1$.

In case (i), P lies in the box $[-1,1]^2 \subset \mathbb{R}^2$.

In case (ii), the point $Q = (x, 1/y)$ is on the curve $Y : y^c F(x, 1/y) = 0$. This curve is also irreducible and of bidegree (b,c) (because F must have a term independent of y). The point Q is then in the box $[-1,1]^2$ and has $H(Q) \leqslant B$. Likewise in cases (iii) and (iv) the corresponding points $R = (1/x, y), S = (1/x, 1/y)$ lie on irreducible curves $x^b F(1/x, y) = 0, x^b y^c F(1/x, 1/y) = 0$ of bidegree (b,c) in the box $[-1,1]^2$ and have height $\leqslant B$.

Therefore, up to a factor 4 in the estimate, it suffices to consider the points of F inside the box $[-1,1]^2$.

Now the total degree of F is at most $b+c \leqslant 2d$. There are at most $d(2d-1)$ singular points of X, at most $4d(2d-1)$ points with slope ± 1, and $2d$ intersections of X with (each of) $y = \pm 1$. On intervals between the corresponding $\leqslant 10d^2$ x-coordinates (including $x = \pm 1$), X has at most d branches. So $X \cap [-1,1]^2$ consists of at most $10\,d^3$ graphs of C^∞ functions g with slope $|g'| \leqslant 1$ with respect to one of the coordinate axes and satisfying an algebraic equation of bidegree (b,c) or (c,b). Thus combining with 4.2 implies

$$N(X,B) \leqslant 40d^3 \big(4d^2\delta\big)^{2d+4} (2B^2)^{1/d+1/\delta}.$$

Now take δ to be the least integer exceeding $\log B$. Since $B \geqslant 3$, $\delta \leqslant 2\log B$. Then $2^{1/d+1/\delta} \leqslant 2$, $B^{2/\delta} \leqslant e^2$ and so

$$N(X,B) \leqslant 80e^2\, d^3 \big(8d^2\big)^{2d+4} B^{2/d} (\log B)^{2d+4}.$$

□

BIBLIOGRAPHY

[1] E. Bierstone and P.D. Milman, Semianalytic and subanalytic sets, Pub. Math. I.H.E.S., 67 (1988), 5–42.

[2] E. Bombieri, email, 9 March 2003.

[3] E. Bombieri and J. Pila, The number of integral points on arcs and ovals, Duke Math. J., 59 (1989), 337–357.

[4] D. R. Heath-Brown, The density of rational points on curves and surfaces, Ann. Math., 155 (2002), 553–595.

[5] M. Hindry and J. H. Silverman, Diophantine geometry: an introduction, Graduate Texts in Mathematics 201, Springer, New York (2000).

[6] V. Jarnik, Über die Gitterpunkte auf konvexen Curven, Math. Z., 24 (1926), 500–518.

[7] S. Lang, Number theory III: diophantine geometry, Encyclopedia of Mathematical Sciences, Volume 60, Springer, Berlin (1991).

[8] J. Pila, Geometric postulation of a smooth function and the number of rational points, Duke Math. J., 63 (1991), 449–463.

[9] J. Pila, Density of integer points on plane algebraic curves, International Mathematics Research Notices, (1996), 903–912.

[10] J. Pila, Integer points on the dilation of a subanalytic surface, Quart. J. Math., 55 (2004), 207–223.

[11] J. Pila, Note on the rational points of a pfaff curve, submitted.

[12] W. M. Schmidt, Integer points on curves and surfaces, Monatsh. Math., 99 (1985), 45–72.

[13] H. P. F. Swinnerton-Dyer, The number of lattice points on a convex curve, J. Number Theory, 6 (1974), 128–135.

[14] A. Wilkie, Diophantine properties of sets definable in *o*-minimal structures, J. Symb. Logic, 69 (2004), 851–861.

Manuscrit reçu le 5 novembre 2004,
Accepté le 28 février 2005.

Jonathan PILA,
McGill University
Department of Mathematics and Statistics
Burnside Hall
805 Sherbrooke Street West
Montreal, Quebec, H3A 2K6 (Canada)
pila@math.mcgill.ca

University of Oxford
Mathematical Institute
24-29 St Giles
Oxford OX1 3LB (United Kingdom)