2

Point-Counting

The Counting Function

We will count the rational points in a set in real Euclidean space according to their height. Height serves as a convenient complexity measure for rational points.

2.1 Definition The *height* of a rational number $r = a/b$, where a, b are integers and the fraction is in lowest terms, is

$$H(r) = \max\{|a|, |b|\}.$$

This is extended to tuples $r = (r_1, \ldots, r_n) \in \mathbb{Q}^n$ by setting

$$H(r) = \max \left\{H(r_i), i = 1, \ldots, n\right\}.$$

2.2 Definition For a set $Z \subset \mathbb{R}^n$ and $T \geq 1$, set

$$Z(\mathbb{Q}, T) = \left\{z \in Z \cap \mathbb{Q}^n : H(z) \leq T\right\},$$

and then define the *counting function* to be

$$N(Z, T) = \#Z(\mathbb{Q}, T),$$

considered as a function of the height parameter T.

Analytic Curves

The most basic counting result of the type we consider is the following theorem concerning the graph $Z \subset \mathbb{R}^2$ of a function $f\colon [0, 1] \to \mathbb{R}$ that is real analytic on an open neighbourhood of $[0, 1]$ and *transcendental*, meaning that there is no algebraic relation (over $\mathbb{R}$) satisfied identically by x and $y = f(x)$.

2.3 Theorem ([419, Theorem 9]) *Let Z be as above and $\epsilon > 0$. Then there is a constant $c(f, \epsilon)$ such that $N(Z, T) \leq c(f, \epsilon)T^\epsilon$ for all $T \geq 1$.*

https://doi.org/10.1017/9781009170314.003 Published online by Cambridge University Press

An estimate of this form for the counting function is our sense of “Z contains few rational points”. This result is proved in [419] using the methods introduced in Bombieri–Pila [93], which focussed on counting integer points on the *dilation* of a plane curve, variously assumed to be analytic, sufficiently smooth, or algebraic.

We employ the following mean-value theorem for *alternants* (determinants of the form of det $\big(\phi_i(x_j)\big)$ for functions $\phi_i, i = 1, \dots, n$ and points $x_j, j = 1, \dots, n$).

2.4 Lemma (H. A. Schwarz [478] or [93, p. 342]) *Let D be a positive integer and $J \subset \mathbb{R}$ a compact interval. Let $\phi_1, \dots, \phi_D \in C^{D-1}(J)$, $x_1, \dots, x_D \in J$ and set*

$$\Delta = \Big(\phi_i(x_j)\Big)_{i,j=1,\dots,D}.$$

Then there exist points $\xi_{ij} \in J$ (intermediate to the points x_i) such that

$$\Delta = V(x_1, \dots, x_D) \det \big(\phi_i^{(j-1)}(\xi_{ij})\big),$$

where $V(x_1, \dots, x_D)$ is the Vandermonde determinant.

2.5 Corollary *With the notation as above we have*

$$|\Delta| \leq c(\phi_1, \dots, \phi_D)\, |J|^{D(D-1)/2},$$

where $c(\phi_1, \dots, \phi_D)$ depends on the maximum sizes of the functions ϕ_i and their first $D - 1$ derivatives on the interval J.

The proof of Theorem 2.3 is a typical transcendence-style argument, involving the “fundamental theorem of transcendence theory” (namely, that there are no integers between 0 and 1) and a “zero estimate”.

Proof of Theorem 2.3 Fix a positive integer d and set $D = (d + 1)(d + 2)/2$. Suppose $\big(x_1, f(x_1)\big), \dots, \big(x_D, f(x_D)\big) \in Z(\mathbb{Q}, T)$ with $x_1, \dots, x_D \in J$ some subinterval of I. Apply Corollary 2.5 to these points with the D monomial functions

$$\phi_{ij} = x^i f(x)^j, \quad 0 \leq i, j \leq i + j \leq d$$

to conclude that

$$|\Delta| \leq c(f, D)\, |J|^{D(D-1)/2},$$

where $c(f, D) = c\big(\phi_{ij}, 0 \leq i, j \leq i + j \leq d\big)$ is the constant in Corollary 2.5.

The denominator of each row of Δ can be cleared by multiplying through by a suitable integer of absolute value at most T^{2d} (the product of the dth powers of the denominators of x_i and $f(x_i)$). Hence (clearing all the rows), if $\Delta \neq 0$, then $|\Delta| \geq T^{-2dD}$.

https://doi.org/10.1017/9781009170314.003 Published online by Cambridge University Press

The crucial point is the **ratio** *of the exponents:* $D(D-1)/2 \asymp d^4$ *in the estimate for* $|\Delta|$ *and* $2dD \asymp d^3$ *in the height estimate.* Thus, if

$$c(f,D)|J|^{D(D-1)/2}T^{2dD} < 1,$$

then we must have $\Delta = 0$ (the fundamental theorem of transcendence theory), and this holds provided

$$|J| \leq c'(f,d)\,T^{-4dD/D(D-1)},$$

which, after simplification, becomes

$$|J| \leq c'(f,d)T^{-8/(d+3)}.$$

On such an interval J, a determinant of the form of Δ must vanish. This means that if we form the rectangular array $\big(x_k^i f(x_k)^j\big)$, where k indexes rows and $i,j : i+j \leq d$ index columns, using all points $x_k \in J$ for which $\big(x_k, f(x_k)\big) \in Z(\mathbb{Q},T)$, then this array has rank less than D. Then there exists $a_{ij} \in \mathbb{R}, i+j \leq d$, not all zero, such that (summing over $i+j \leq d$)

$$\sum_{i,j} a_{ij} x_k^i f(x_k)^j = 0, \quad \text{for all } k;$$

that is, the points $\big(x_k, f(x_k)\big) \in Z(\mathbb{Q},T)$ with $x_k \in J$ all lie on a single real algebraic curve V of degree d determined by the a_{ij}.

Now we consider such intersections $V \cap Z$, where V is a real algebraic curve of degree d. Since f is transcendental, the number of intersection points is finite, and indeed there is a uniform bound $\gamma(f,d)$ on $\#\big(V \cap Z\big)$ over all curves V of degree d (this is the zero estimate). This follows, for example, from the fact that Z is definable in an o-minimal structure; see Remark 8.14.2. For Z of this specific (analytic or subanalytic) form, it follows from Gabrielov's Theorem [222] (see alternatively [61]). Since I may be covered by at most

$$c''(f,D)T^{8/(d+3)} + 1 \leq c'''(f,D)T^{8/(d+3)},$$

subintervals J of length at most $c'(f,D)T^{-8/(d+3)}$, we have

$$N(Z,\mathbb{Q}) \leq 2\,c'''(f,D)\,\gamma(f,d)\,T^{8/(d+3)}.$$

The proof is completed by choosing d so that $8/(d+3) \leq \epsilon$. □

2.6 Remarks

1. For the lemma one does not need analyticity but only $D-1$ continuous derivatives. So for the theorem one needs somewhat less as well. This may seem a minor point but is important. We require that (i) given $\epsilon > 0$, the graph Z can be divided into finitely many pieces on which it can be parameterized

https://doi.org/10.1017/9781009170314.003 Published online by Cambridge University Press

by functions with sufficiently (but finitely) many bounded derivatives; and (ii) given d, the cardinalities $\#(Z \cap Y)$, where Y is an algebraic curve of degree d, are uniformly bounded. O-minimality provides both of these for its definable sets.

2. A proof of Theorem 2.3 using Siegel's Lemma instead of determinants is given in [531], also used in [530]. A proof via complex analysis (and Siegel's Lemma) is given in [351] (see also [353, 354]).

Improved Bounds

Theorem 2.3 cannot be much improved in general, as shown by constructions in [421, 498] of complex analytic functions for which the ϵ goes to zero arbitrarily slowly along some (lacunary) sequence of values of T. In the other direction, it is shown in [498] that, for an entire function, a bound polynomial in $\log T$ always holds on a sequence of T going to infinity (even in arbitrarily long intervals [234]). A much stronger bound for integer points on curves definable in $\mathbb{R}_{\text{an}}$ is established in [530].

Various results give bounds polynomial in $\log T$ for all T, moreover effective or even explicit, under additional assumptions on f. See generally [293]. The main difficulty is to control the growth of the *Bézout bounds* $\gamma(f, d)$ with d. For complex analytic functions, various conditions ensuring polynomial growth of Bézout bounds are explored in [156], with corresponding polynomial-in-$\log T$ improvements of Theorem 2.3. Bézout bounds for solutions of algebraic differential equations are given in [68].

In the real variable setting, a variant method in [93] enables a bound using only estimates for the *number* of zeros of successive derivatives of the function f, rather than the norms of derivatives, and the $\gamma(f, d)$. If one works with Pfaffian functions (see §8.28), then one has strong bounds [223] on the required quantities. Bounds polynomial in $\log T$ are obtained in this way in [294, 423]. For real analytic functions, local conditions governing the $\gamma(f, d)$ are explored in [419], using a mean value theorem [447] for linear homogeneous differential equations.

Results under other conditions, utilizing transcendence measures of a known value of f, or suitable growth restrictions, are obtained in [98, 99, 125, 126, 127] (see also [100]). Transcendence measures are exploited in more general settings in [234]. Results for various classical functions are given in [59, 97, 299, 351], and for certain oscillatory functions in [155]; see also [250].

In the complex setting, the ideas are close to the classical Schneider–Lang method in transcendence theory, see, for example, [325]. Interpolation

https://doi.org/10.1017/9781009170314.003 Published online by Cambridge University Press

determinants (alternants) were introduced into transcendence theory by Laurent [330]. Independently, the ideas of [419] were used to give proofs of some classical transcendence statements in the real variable setting via determinants in [420]; see also [114; 298, Proposition 5.6; 426].

Complex-variable methods seem to be less flexible for higher-dimensional sets.

Higher-Dimensional Sets

Consider now a set $Z \subset \mathbb{R}^n$. We would like an estimate for the counting function registering that non-algebraic sets have few rational points in our height density sense. There are two points to consider regarding the kind of result one might anticipate.

First, as for plane curves, one cannot hope to do this meaningfully for an arbitrary set, and some tameness assumption is needed along the lines of analyticity. Our condition is that Z is *definable in an o-minimal structure*. We postpone defining this notion until Part II, but we note that it includes sets of a form naturally generalizing the graphs in the planar case.

2.7 Proposition *Let $Z \subset \mathbb{R}^n$ be the union of a finite number of images of maps $\phi : (0,1)^k \to (0,1)^n$, where ϕ is real analytic on an open neighbourhood of $[0,1]^k$. Then Z is definable in an o-minimal structure.*

Proof Such sets are definable in the o-minimal structure $\mathbb{R}_{\mathrm{an}}$; see §8.21. □

This gives quite a broad class of sets, though the sets definable in an o-minimal structure are significantly richer, and indeed this is crucial in the applications.

Second, and a new feature when $n \geq 3$, such a set Z of real dimension $k \geq 2$, even if it is non-algebraic, could nevertheless contain semi-algebraic sets of positive dimension, and these might contain many (i.e. not few) rational points. For example, the set

$$Z = \left\{(x, y, z) \in \mathbb{R}^3 : z = x^y, x, y \in [2, 3]\right\}$$

contains, for each rational value of y, a segment of the rational curve $z = x^y$, and every such arc contains $\gg T^\eta$ rational points up to height T for some $\eta = \eta(y) > 0$.

2.8 Definition ([189, p. 1]) A *semi-algebraic set* in $\mathbb{R}^n$ is a finite union of sets each of which is defined by finitely many equations and inequalities between polynomials with real coefficients.

https://doi.org/10.1017/9781009170314.003 Published online by Cambridge University Press

Thus, in the first instance, we count rational points of Z not lying in any connected positive-dimensional semi-algebraic subset of Z, and so make the following definition.

2.9 Definition Let $Z \subset \mathbb{R}^n$. We define the *algebraic part* of Z to be the union of all positive-dimensional connected semi-algebraic subsets $A \subset Z$, and denote it Z^{alg}. The complement $Z - Z^{\mathrm{alg}}$ is referred to as the *transcendental part* of Z, and denoted Z^{trans}.

The connectedness condition is essential. Otherwise, if Z contained a positive-dimensional semi-algebraic set A, then this set, together with any individual point $z \in Z$, would be a semi-algebraic set of positive dimension, and we would get $Z^{\mathrm{alg}} = Z$.

The basic point-counting result is the following. We refer to Theorem 2.10, and its various elaborations such as Theorems 2.13 and 9.14, as the Counting Theorem.

2.10 Theorem ([439, Theorem 1.8]) *Let $Z \subset \mathbb{R}^n$ be definable in an o-minimal structure, and $\epsilon > 0$. Then there is a constant $c(Z, \epsilon)$ such that*

$$N(Z^{\mathrm{trans}}, T) \leq c(Z, \epsilon) T^{\epsilon}$$

for all $T \geq 1$.

2.11 Remarks

1. One can view the theorem as a crude analogue of Lang's general conjecture, with Z^{alg} as a crude analogue of the special set in diophantine geometry. The result says that, away from Z^{alg}, there are few rational points.
2. Since definable sets are more general than the real analytic images we have been using as provisional representatives, even in dimension one, this theorem generalizes Theorem 2.3 to a larger class of real curves.
3. By examining the proof one can do better than simply exclude all of Z^{alg}: only some parts need to be excluded for any given ϵ. Furthermore, the points are contained in few connected semi-algebraic subsets. This is important in some applications.
4. The result is uniform in *definable families*; see Definition 8.6. This is an essential feature required in the proof, but leads to strong uniformities in applications; see Chapter 23.
5. The bound in Theorem 2.10 is qualitative and is what follows from o-minimality. It is natural to ask whether the bound $\ll T^{\epsilon}$ can be improved to $\ll (\log T)^{O(1)}$. This is not possible in general, as already remarked, but

https://doi.org/10.1017/9781009170314.003 Published online by Cambridge University Press

Wilkie conjectured that it should hold in certain special (but central) cases. Various results in this direction are discussed in Chapters 10 and 11.

An estimate of the same form holds for algebraic points up to some given bounded degree $k \geq 1$. This is stated in terms of the *absolute multiplicative Weil height* $H(\alpha)$ of an algebraic number that extends the height of a rational number as in Definition 2.1. A definition is given, for example, in [85, Definition 1.5.4]. (So $h(\alpha) = \log H(\alpha)$ is the *absolute logarithmic Weil height*.)

We can then define the counting function for algebraic points of degree $k \geq 1$.

2.12 Definition For a set $Z \subset \mathbb{R}^n$, integer $k \geq 1$, and a $T \geq 1$, we set

$$Z(k,T) = \left\{z = (z_1, \ldots, z_n) \in Z : [\mathbb{Q}(z_i) : \mathbb{Q}] \leq k, H(z_i) \leq T, i = 1, \ldots, n\right\},$$

$$N(k,Z,T) = \#Z(k,T).$$

2.13 Theorem ([424, Theorem 1.6]) *Let $Z \subset \mathbb{R}^n$ be definable in an o-minimal structure, $k \geq 1$, and $\epsilon > 0$. Then there is a constant $c(Z,k,\epsilon)$ such that*

$$N(k, Z^{\text{trans}}, T) \leq c(Z,k,\epsilon)T^{\epsilon}$$

for all $T \geq 1$.

Theorems 2.10 and 2.13 follow from the stronger version given in Theorem 9.14.

Counting Rational and Integral Points on Algebraic Varieties

The paper [93] also establishes a result on integer points of bounded height on a plane algebraic curve, getting a uniform bound for (irreducible) curves of given degree.

2.14 Theorem ([93, Theorem 5]) *Let $F \in \mathbb{R}[X,Y]$ be irreducible of degree d. Then the number of integer points (x,y) with $F(x,y) = 0$ and $|x|, |y| \leq T$ is at most*

$$c(d,\epsilon)T^{1/d+\epsilon}.$$

The exponent $1/d$ is best possible in view of the example $Y = X^d$. Heath-Brown [271] develops a p-adic version of the method applicable to rational points on projective varieties in all dimensions, in particular giving the analogue of Theorem 2.14 for rational points of height up to T with exponent $2/d + \epsilon$. The exponent $2/d$ is best possible here (same example; non-uniformly such a bound was established in [419]; see also [204]).

https://doi.org/10.1017/9781009170314.003 Published online by Cambridge University Press

The applicability of the p-adic methods of [271] to higher-dimensional algebraic varieties suggested investigating the applicability of the real variable determinant approach to higher-dimensional non-algebraic sets. This was instigated in [421], for integer points on the dilation of a subanalytic surface (and then [422] for rational points). The real variable approach is applied to rational points on higher-dimensional algebraic varieties in [347].

These determinant methods (real, p-adic, and the global version of Salberger) have been useful in a variety of applications to counting rational points on algebraic varieties (see e.g. [272]), in particular towards the *dimension-growth conjecture* [269, 486]; see [271, Conjectures 1, 2]. This posits an exponent $\dim X + \epsilon$ for the counting function for a projective variety $X \subset \mathbb{P}^n$. In the strongest form one asks for the constant dependent only on n, $\deg X$, and ϵ. This is proven (in the strong form) for $d \geq 4$ in work of Browning, Heath-Brown, and Salberger [108, 464]; see also [123].

The T^ϵ in Theorem 2.14 was improved to a power of $\log T$ in [425] and removed altogether from the corresponding result for rational points in [526]. In higher dimensions, real variable parameterization is used in [77] to replace the ϵ by a power of $\log T$, with polynomial dependence of the constants, for rational points on hypersurfaces. This is further refined in [123], using the global determinant method, eliminating the ϵ factor entirely in the dimension-growth conjecture while retaining polynomial dependence of the constants; see further [403].

W. M. Schmidt [477] conjectured that, for curves of positive genus, one has a bound of the form of Theorem 2.14 but with exponent ϵ instead of $1/d + \epsilon$. Here one has finiteness for an individual curve by a famous theorem of Siegel, and the issue is the uniformity. Some progress towards this for elliptic curves is obtained in [273]. A T^ϵ bound for integral points on moduli spaces of varieties is proved in [206]. One would also expect stronger estimates for rational points on curves of positive genus, and such an improvement is obtained in [207]. Under a suitable hypothesis on ranks of elliptic curves, a uniform bound $N(Z,T) \ll_\epsilon T^\epsilon$ for rational points on non-singular cubic plane curves is established in [270].

Counting Rational and Integral Points on Sufficiently Smooth Curves

The paper [93] also considered functions with a finite number of derivatives, generalizing results of Jarnik [291].

2.15 Theorem ([93, Theorem 7]) *Let $f \in C^\infty([0,1])$ be strictly convex with graph Γ and let $\epsilon > 0$. Then, for $t \geq 1$,*

$$\#\big(t\Gamma \cap \mathbb{Z}^2\big) \leq c(f,\epsilon)t^{1/2+\epsilon}.$$

https://doi.org/10.1017/9781009170314.003 Published online by Cambridge University Press

Further conjectures and results in this direction are given in [93] and [419, 477]. See also [288] on estimating integer points on or near a plane curve, and references there for such problems with rational points. On rational points near a definable set, see [260] and Theorem 9.17.

https://doi.org/10.1017/9781009170314.003 Published online by Cambridge University Press