

Research Statement

Martin Widmer

October 27, 2010

1 Introduction

My research area lies within the broad field of Diophantine analysis. I am particular interested in the distribution of discrete algebraic objects in algebraic structures and aspects of heights such as height bounds and the Northcott property.

Heights are functions that measure the arithmetic complexity of an algebraically defined object. They have become a major tool in many branches of number theory such as Diophantine analysis, transcendental number theory, Diophantine approximation, arithmetic of dynamical systems, etc. Moreover, they have also some very subtle functorial and functional properties, making it worthwhile to study them for their own sake, e.g. the famous but notoriously difficult Lehmer problem, originated in [22].

A classical height is the Weil height or simple the height, defined on algebraic points. Let k be a number field and write $d = [k : \mathbb{Q}]$ for its degree. Let M_k be the set of places of k and choose for each $v \in M_k$ the unique representative $|\cdot|_v$ that either extends the usual absolute value on \mathbb{Q} or a p -adic absolute value. Let k_v be the completion at v and \mathbb{Q}_v the completion with respect to the place which extends to v and write $d_v = [K_v : \mathbb{Q}_v]$ for the local degree. The height on k^n is defined by

$$H(\alpha_1, \dots, \alpha_n) = \prod_{M_k} \max\{1, |\alpha_1|_v, \dots, |\alpha_n|_v\}^{\frac{d_v}{d}}. \quad (1.1)$$

This is in fact a finite product. Furthermore this definition is independent of the field k containing the coordinates and therefore defines a height on $\overline{\mathbb{Q}}^n$. The product formula implies that the right hand-side in (1.1) does not change if we multiply $1, \alpha_1, \dots, \alpha_n$ with a fixed element of k^* . Therefore one can also define a height on points $P = (\alpha_0 : \dots : \alpha_n)$ in $\mathbb{P}^n(\overline{\mathbb{Q}})$ by

$$H(P) = \prod_{M_k} \max\{|\alpha_0|_v, \dots, |\alpha_n|_v\}^{\frac{d_v}{d}}. \quad (1.2)$$

Another popular height is the l^2 -height $H_2(\cdot)$ gotten by choosing l^2 -norms at the infinite places. Heights have several wonderful properties; firstly they have a very good behavior under algebraic operations. Secondly they induce a finiteness property, nowadays well-known as Northcott's Theorem [28]. We say a subset S of $\overline{\mathbb{Q}}^n$ or $\mathbb{P}^n(\overline{\mathbb{Q}})$ has bounded degree (over \mathbb{Q}) if there exists a D such that $[\mathbb{Q}(P) : \mathbb{Q}] \leq D$ for each $P \in S$ where $\mathbb{Q}(P) = \mathbb{Q}(x_1, \dots, x_n)$ if $P = (x_1, \dots, x_n) \in \overline{\mathbb{Q}}^n$ and $\mathbb{Q}(P) = \mathbb{Q}(\dots, x_i/x_j, \dots)$ ($0 \leq i, j \leq n$; $x_j \neq 0$) if $P = (x_0 : \dots : x_n) \in \mathbb{P}^n(\overline{\mathbb{Q}})$.

Theorem 1.1 (Northcott). *Subsets of $\overline{\mathbb{Q}}^n$ or $\mathbb{P}^n(\overline{\mathbb{Q}})$ of bounded degree (over \mathbb{Q}) and bounded height are finite.*

The proof of Northcott's Theorem is very simple. Nonetheless it is an important result that has been used extensively during the last few decades, especially to deduce finiteness statements in Diophantine geometry and Diophantine approximation such as the Mordell-Weil Theorem, Schmidt's

Subspace Theorem or Faltings' proof of the Mordell Conjecture. However, Northcott's original motivation came from dynamics of polynomial mappings.

2 (A) Northcott type Theorems

2.1 State of research in the area

Motivated by Northcott's Theorem Bombieri and Zannier [7] introduced the Northcott property, short property (N) . A subsets \mathcal{A} of $\overline{\mathbb{Q}}^n$ has the Northcott property if each of its subsets of bounded height is finite. Thus Northcott's Theorem is equivalent to the statement sets of bounded degree have the property (N) . Since $H(x_1, \dots, x_n) \geq H(x_i)$ the higher dimensional case can usually be reduced to the one-dimensional case, therefore we restrict ourselves to subsets of $\overline{\mathbb{Q}}$. In [7] Bombieri and Zannier raised the question whether property (N) holds for other interesting sets, in particular they addressed the following question.

Question 1 (Bombieri, Zannier). *Does $k^{(d)}$, the field generated by all algebraic numbers of degree at most d over k , have property (N) ?*

It is not difficult to see that Northcott's Theorem remains valid for any ground field with property (N) , and not only \mathbb{Q} . An affirmative answer to the above question would yield an impressive generalization of Northcott's Theorem. Unfortunately Question 1 is widely open, in fact only the case $d = 2$ is settled. Bombieri and Zannier (Corollary 1 [7]) showed that $k^{(2)}$, the compositum of all (at most) quadratic extensions of the number field k has property (N) . This is an immediate consequence of the following beautiful result.

Theorem 2.1 (Bombieri, Zannier). *The maximal abelian extension of k in $k^{(d)}$ has property (N) .*

Another impressive corollary of Theorem 2.1 is the following statement.

Corollary 2.1 (Bombieri, Zannier). *The field $\mathbb{Q}(1^{1/d}, 2^{1/d}, 3^{1/d}, \dots)$ has property (N) for any positive integer d .*

It is known already since Northcott's paper [11] that if L is a field with property (N) then for each polynomial map f in $L[t]$ of degree > 1 there exist only finitely many preperiodic points in L under f . This provides a strategy, at least for some fields L , to treat the following widely open general problem formulated by Dvornicich and Zannier ([9], Question).

Question 2 (Dvornicich, Zannier). *Let L be a subfield of $\overline{\mathbb{Q}}$ and let $f \in L[t]$ be a polynomial map of degree > 1 . Can one decide whether the set of preperiodic points in L under f is finite or infinite?*

Dvornicich and Zannier showed also that property (N) implies the so-called property (P) , introduced by Narkiewicz [27] to study polynomial mappings. In this way they solved several open problems formulated by Narkiewicz on property (P) e.g. the field $\mathbb{Q}^{(2)}$ has property (P) (see Open Question XVII p.69 in [27]). Inspired by this and all the well-known applications in Diophantine geometry Dvornicich and Zannier [9] raised the problem of finding other examples satisfying property (N) . *"It may be of interest, both for its own sake and also in view of the many applications of the Northcott property, to produce examples of fields of algebraic numbers other than number fields possessing it; a priori there might be no such field, i.e. with Northcott property and infinite degree over \mathbb{Q} ."* However, in 2009 (see [42]) I found the following simple but new criterion of property (N) for infinite extensions.

Theorem 2.2 (W. 2009). *Suppose $k = K_0 \subsetneq K_1 \subsetneq K_2 \subsetneq K_3 \subsetneq \dots$ is a sequence of finite extensions such that*

$$\inf_{K_{i-1} \subsetneq M \subseteq K_i} (N_{K_{i-1}/\mathbb{Q}}(D_{M/K_{i-1}}))^{\frac{1}{[M:K_0][M:K_{i-1}]}} \longrightarrow \infty. \quad (2.1)$$

Then $L = \bigcup_i K_i$ has property (N) .

Here M runs over the intermediate fields and $D_{M/K_{i-1}}$ is the relative discriminant of the ring of integers \mathcal{O}_M and $N_{K_{i-1}/\mathbb{Q}}$ denotes the norm from K_{i-1} to \mathbb{Q} . A simple application of this criterion yields a small step towards an affirmative answer on Question 1 for $d = 3$.

Corollary 2.2 (W. 2009). *For $i = 1, 2, 3, \dots$ let F_i be extensions of k with $[F_i : k] \leq 3$ and let p_i be primes such that*

$$p_i \mid \Delta_{F_i} \quad \text{and} \quad p_i \nmid \Delta_{F_j} \text{ for } j < i.$$

Then the compositum of k, F_1, F_2, F_3, \dots has property (N).

Here Δ_{F_i} is the absolute discriminant of F_i . The same result holds for fields F_i with $[F_i : k] \leq d$ for an arbitrary d , provided the primes p_i ramify totally in F_i . The latter is a consequence of the following theorem.

Theorem 2.3 (W. 2009). *For $i = 1, 2, 3, \dots$ let p_i be primes and let D_i be p_i -Eisenstein polynomials in $\mathbb{Z}[x]$ with $D_i(\alpha_i) = 0$. Write $d_i = \deg D_i$ and suppose that*

$$p_i \nmid \Delta_{\mathbb{Q}(\alpha_j)} \text{ for } 1 \leq j < i \quad \text{and} \quad |p_i^{1/d_i}| \longrightarrow \infty.$$

Then $k(\alpha_1, \alpha_2, \alpha_3, \dots)$ has property (N).

Another immediate application of Theorem 2.3 is the following precise refinement of Bombieri and Zannier's Corollary 2.1.

Corollary 2.3 (W. 2009). *Let d_1, d_2, d_3, \dots be a sequence of positive integers and let $0 < p_1 < p_2 < p_3 < \dots$ be a sequence of primes. Then*

$$k(p_1^{1/d_1}, p_2^{1/d_2}, p_3^{1/d_3}, \dots) \text{ has property (N)} \iff |p_i^{1/d_i}| \longrightarrow \infty.$$

Let us close this section with a result that connects part (A) and part (B) of this research plan. The latter is concerned with estimates for the smallest height of a generator of a number field. Together with Vaaler we have shown that each number field k of degree d contains a generator whose height does not exceed $|\Delta_k|^{1/d}$. Therefore a union of infinitely many number fields of bounded root discriminant cannot have the Northcott property. Now let $H(k)$ be the Hilbert class field of k , and let \mathcal{H}_k be the Hilbert class field tower, i.e. the union of $k, H(k), H(H(k)), \dots$. Note that each of the fields $k, H(k), H(H(k)), \dots$ has root discriminant $|\Delta_k|^{1/d}$. Hence we conclude the sequence $k, H(k), H(H(k)), \dots$ becomes stationary if and only if \mathcal{H}_k has the Northcott property.

2.2 Research goals and methods

We will continue our study of property (N) for certain infinite extensions of \mathbb{Q} , especially with regard to Question 1. A complete answer to this question is probably very difficult but we are confident to make some valuable steps towards a complete answer. Of course, possibly not even $\mathbb{Q}^{(3)}$ satisfies the property (N). On the other hand it is clear that Corollary 2.2 is only a first step and that the same strategy provides more general results. First we will carefully examine the contribution of not only one but several (and if possible all) primes to the norm of the relative discriminant. This will yield a stronger version of Corollary 2.2, here is a simple example: let F'_i be fields satisfying the same conditions (with the same primes p_i) as the fields F_i in Corollary 2.2 and additionally $\text{ord}_{p_i} \Delta_{F_i} \neq \text{ord}_{p_i} \Delta_{F'_i}$. Then the compositum of the fields $k, F_1, F'_1, F_2, F'_2, F_3, F'_3, \dots$ has the Northcott property. We are confident to strengthen our results in this way to obtain a significant progress on Question 1; we hope to prove that the composite field of any collection of cubic fields with pairwise distinct discriminants has the Northcott property.

Let us point out that the strategy of Bombieri and Zannier in [7] is quite different from ours in [42]. In a second step we will combine the ideas and this might extend the results of both papers. For instance, if we replace the term in (2.1) by $\inf_M |\Delta_M|^{1/[M:\mathbb{Q}]^2}$, where M runs over all number

fields such that the compositum MK_{i-1} is K_i , then the ground field k in Theorem 2.2 can be replaced by any field of algebraic numbers possessing property (N) , in particular we can incorporate Bombieri and Zannier's main result and replace k with the maximal abelian extension of k in $k^{(d)}$. However, the degree of M can now get arbitrarily large which seems to create additional problems.

Dvornicich and Zannier pointed out that property (N) is preserved under taking finite extensions. Using Corollary 2.3 we have constructed an example showing that property (N) is not preserved under the more general procedure of taking the compositum of two extensions. Moreover, Corollary 2.3 tells us in particular that for extensions of the form $k(p_1^{1/d_1}, p_2^{1/d_2}, p_3^{1/d_3}, \dots)$ it suffices to check property (N) on the ring of integers. So one might ask the following, rather brave, question: suppose $0 \neq R$ is a subring of $\overline{\mathbb{Q}}$ satisfying property (N) . Does this imply that its field of fractions $\text{frac}(R)$ has property (N) ?

Finally let us briefly mention possible applications of the Northcott property. Well-known are the implied finiteness results for the number of preperiodic points under rational maps (of degree at least 2). Less clear, but certainly very interesting, is the question to what extent the Mordell-Weil Theorem can hold for fields with property (N) . The latter is definitely not a sufficient criterion, so the question is rather: under what additional properties can one prove the Mordell-Weil Theorem or a variation thereof?

(A1): Refine Theorem 2.2 to derive new examples of fields with property (N) .

(A2): Answer Question 1, at least partially e.g. for $d = 3$.

(A3): Investigate applications of the newly established Northcott-type theorems e.g. in Diophantine geometry and the arithmetic of dynamical systems.

3 (B): Small generators of global fields

3.1 State of research in the area

Another problem, but one with ultimate connections to part (A) and (C), is to determine good bounds for the smallest height of a generator of a given number field K . So let k be a number field and let K be a finite extension of k and write $d = [k : \mathbb{Q}]$ and $e = [K : k]$ for the degrees. We define the invariant

$$\delta(K/k) = \inf\{H(\alpha); K = k(\alpha)\}.$$

Already Mahler [23] proved a lower bound for $\delta(K/\mathbb{Q})$ in terms of the discriminant $|\Delta_K|$ and the degree $[K : \mathbb{Q}]$. Mahler's result was generalized by Silverman [37] and yields the following lower bound

$$\delta(K/k) \geq \frac{1}{2} |\Delta_k|^{-\frac{1}{2d(e-1)}} |\Delta_K|^{\frac{1}{2de(e-1)}}. \quad (3.1)$$

For the rest of this section we assume $k = \mathbb{Q}$ so that $[K : \mathbb{Q}] = e$. Silverman's inequality turned out to be extremely useful; it has been applied by Silverman [37], Baker-Wüstholz [2], Schmidt [36], Gao [14], Widmer [41],[42], Bilu-Strambi [4], Ellenberg-Venkatesh [12] and Ellenberg [10], to name just a few. Let us briefly explain the applications in [12] and [10]. Brumer, Duke, Silverman, Zhang and others have conjectured that the ℓ -torsion part $Cl_K[\ell]$ of the class group of K is bounded from above by $C(e, \ell, \epsilon) |\Delta_K|^\epsilon$ for any $\epsilon > 0$. The Siegel-Brauer Theorem gives the trivial exponent $1/2 + \epsilon$ but until Ellenberg and Venkatesh's work [12] no nontrivial results, conditional or unconditional, were known, unless $\ell = 3$ and $e = 2$. However, assuming the Generalized Riemann Hypothesis (GRH) Ellenberg and Venkatesh's argument (see [10] p.3) gives the following relation between $\delta(K/\mathbb{Q})$ and $Cl_K[\ell]$

$$|Cl_K[\ell]| \leq C(e, \ell, \epsilon) |\Delta_K|^{\frac{1}{2} + \epsilon} \delta(K/\mathbb{Q})^{-\frac{\epsilon}{\ell} + \epsilon}. \quad (3.2)$$

Here ℓ is a positive prime number. Then applying (3.1) gives the bound

$$|Cl_K[\ell]| \leq C(e, \ell, \epsilon) |\Delta_K|^{\frac{1}{2} - \frac{1}{2(e-1)\ell} + \epsilon}, \quad (3.3)$$

subject to GRH. In some special cases, e.g. $e = 2$ and $\ell = 3$, they could use Scholz' reflection principle to get an unconditional result which improves upon the previously known unconditional results of Pierce [30] and Helfgott, Venkatesh [17]. This in turn implies (by well-known arguments) the best known upper bounds for the number of cubic fields with given discriminant and the number of elliptic curves over \mathbb{Q} with given conductor.

An improvement of (3.1) would yield immediately an improvement upon Ellenberg and Venkatesh's result (3.3). Driven by a function field result of Arbarello and Cornalba (Thm.2.6 [1]) Ellenberg asks ([10] p.4) whether $\delta(K/\mathbb{Q}) \geq C_e |\Delta_K|^{1/2(e-1)}$ holds for a "typical" number field K . However, Masser and Ruppert have shown (independently) that the exponent $1/2e(e-1)$ in (3.1) cannot be improved in this general setting. As a strong contrast to Ellenberg's question Ruppert ([32] Question 1) addressed the following problem.

Question 3 (Ruppert). *Does there exist a constant C_e depending only on e such that $\delta(K/\mathbb{Q}) \leq C_e |\Delta_K|^{1/2e(e-1)}$ for all number fields K of degree e ?*

Ruppert answered this question, in the affirmative, for $e = 2$. However, for $e = 2$ one has $1/2e(e-1) = 1/2e$ and thus for general e (3.1) might suggest that the correct exponent in the upper bound is $1/2e$. So Ruppert formulated also a second, analogous question ([32] Question 2), this time with exponent $1/2e$.

Question 4 (Ruppert). *Does there exist a constant C_e depending only on e such that $\delta(K/\mathbb{Q}) \leq C_e |\Delta_K|^{1/2e}$ for all number fields K of degree e ?*

In a recent article [43] I answered this question in the affirmative in the function field case. A general upper bound for the smallest integral generator, in particular for $\delta(K/\mathbb{Q})$, was given in [40]. However, the smallest integral generator is often much larger than $\delta(K/\mathbb{Q})$, for instance $H(\alpha) \geq (1/2)|\Delta_K|^{1/2}$ for any integral generator α of an imaginary quadratic field K whereas Ruppert's result shows $\delta(K/\mathbb{Q}) \leq C_2 |\Delta_K|^{1/4}$. Interesting enough Ruppert's constant C_2 is ineffective but he conjectured ([32] Conjecture 1) that one can take $C'_2 = 3.22$ (here C'_2 corresponds to the naive height as used by Ruppert).

3.2 Research goals and methods

In January 2009 Jeffrey Vaaler from The University of Texas at Austin and myself started a common project. Based on a simple counting argument and using results from [35] and [11] we showed in [39] that Silverman's bound (3.1) can be improved significantly for an infinite class of extensions, at least if $e > 2$ is not a prime. This implies that (3.3) can be improved for a certain class of fields but unfortunately, due to the non-constructive nature of the proof, we do not have any methods to find this class of fields. However, the result answers Ruppert's Question 3 in the negative, at least if e is not a prime. We aim to extend this result to cover all cases $e > 2$.

We have also shown the general upper bound $\delta(K/\mathbb{Q}) \leq |\Delta_K|^{1/e}$ which was already mentioned in part (A). If K has a real embedding we can replace the exponent $1/e$ by $1/2e$ and this answers Ruppert's Question 4, at least for this class of extensions; this time in the affirmative. However, the remaining case, i.e. K has no real embedding, is the most interesting one. We found a strategy to deal with all cases simultaneously; the problem boils down to the following question which is of interest for its own sake: does there exist a constant C_e depending solely on e such that for any number field K of degree $e = [K : \mathbb{Q}]$ there exists a $t \geq 1$ and prime ideals \wp_1, \dots, \wp_t of degree one in the ring of integers \mathcal{O}_K such that none two of them lie above the same rational prime and $\sqrt{|\Delta_K|} < N_{K/\mathbb{Q}}(\wp_1 \dots \wp_t) \leq C_e \sqrt{|\Delta_K|}$? Under the GRH the answer is yes and we can even find a single prime. Hence our strategy provides an affirmative answer to Ruppert's Question 4 under the

GRH. And using a precise estimate of Schmidt [36] for the number of integral ideals with bounded norm, which came out as a by product of the estimate (4.9) further down, we also recover a slightly weaker version of Ruppert's bound $\delta(K/\mathbb{Q}) \leq C_2 |\Delta_K|^{1/4}$ for quadratic fields. What is more, our strategy might yield a completely effective proof so that one could tackle Ruppert's Conjecture (Conjecture 1 in [32]). Special cases of Ruppert's Conjecture have been proven by Kihel in [21] but the general case is still open.

Now consider $\log \delta(K/\mathbb{Q}) / \log |\Delta_K|$ as K runs over all number fields of degree $e > 1$. Silverman's inequality shows that the smallest cluster point is at least $1/2e(e-1)$, and examples of Masser and Ruppert have shown that this is best possible. Hence the smallest cluster point is exactly $1/2e(e-1)$. Ruppert's Question 3 and Question 4 ask in particular whether the largest cluster point is at most $1/2e(e-1)$ and $1/2e$ respectively. We have shown that the largest cluster point is strictly larger than $1/2e(e-1)$ if e is not a prime, e.g. it is at least $1/3e$ if e is divisible by 2, and at most $1/2e$ if e is odd. Assuming a very weak form of Linnik's Conjecture (see [11] p.723), we can deduce the lower bound $1/e(e+1)$ for the largest cluster point. More ambitiously one could ask: what is the distribution of these cluster points? Are they dense in a certain interval, maybe even in $[1/2e(e-1), 1/2e]$? Can one explicitly construct families of fields that lead to a given cluster point? In view of (3.2) it would be particularly interesting to construct fields with large invariant $\delta(K/\mathbb{Q})$? John Voight's tables for totally real fields of small degrees (see <http://www.cems.uvm.edu/~voight/nf-tables/index.html>) indicate that (3.1) can be improved for totally real fields of degree at least 3.

- (B1): Answer Question 3 (in the negative?) for all $e > 2$.
- (B2): Answer Question 4 (in the affirmative?) for all $e > 1$.
- (B3): Try to find effective upper bounds in (B2), at least for $e = 2$, to tackle Ruppert's Conjecture 1.
- (B4): Construct explicit families of fields with large delta invariant to improve (3.3) for these fields.
- (B5): Study the distribution of the cluster points of $\log \delta(K/\mathbb{Q}) / \log |\Delta_K|$ as K runs over all number fields of degree $e > 1$.

4 (C): Counting points of fixed degree and bounded height

4.1 State of research in the area

In this project we are studying certain subsets of projective space, hence, unless stated otherwise, we are working with the projective height as defined in (1.2). Suppose S is a set in $\mathbb{P}^n(\mathbb{Q})$ with the property (N). Then one may consider the associated counting function

$$N(S, X) = \#\{P \in S; H(P) \leq X\} \quad (4.1)$$

where $X > 0$ is a real parameter. So far only counting functions of sets with bounded degree have been studied and in fact most people even restricted to the case where S lies in $\mathbb{P}^n(k)$ for a certain number field k . Usually there is no hope to describe $N(S, X)$ by a simple expression but for many interesting sets there is hope to find an asymptotic law. The oldest and probably most well-known result of this kind is due to Schanuel [33]. Let k be a number field of degree d and denote by n a natural number.

Theorem 4.1 (Schanuel). *As X tends to infinity one has*

$$N(\mathbb{P}^n(k), X) = S_k(n) X^{d(n+1)} + O(X^{d(n+1)-1} \log X). \quad (4.2)$$

The constant $S_k(n)$ involves all classical field invariants more precisely

$$S_k(n) = \frac{h_k R_k}{\omega_k \zeta_k(n+1)} \left(\frac{2^{r_k} (2\pi)^{s_k}}{\sqrt{|\Delta_k|}} \right)^{n+1} (n+1)^{r_k+s_k-1}. \quad (4.3)$$

Here h_k is the class number, R_k the regulator, ω_k the number of roots of unity in k , ζ_k the Dedekind zeta-function of k , Δ_k the discriminant, r_k is the number of real embeddings of k and s_k is the number of pairs of distinct complex conjugate embeddings of k .

A projective variety is the set of projective points vanishing at a given finite collection of homogeneous polynomials. Points whose homogeneous coordinates can be chosen to lie in the field k are called k -rational points. One of the big achievements in number theory of the last century (Mordell, Siegel, Weil, Faltings) was to understand that the geometry of the variety is crucial for the number of rational points, at least for projective non-singular curves. So the well-known question ‘‘Can one hear the shape of a drum?’’ could be recast as ‘‘Can one count the geometry of a variety?’’. Much effort has been made to derive asymptotic estimates for the counting functions of rational points on varieties. A nice example is Néron-Tate’s asymptotic formula (see e.g.[18] Thm. B.6.3.) for $N_{\hat{H}}(A(k), X)$, the number of k -rational points P on an abelian variety A/k of rank r with Néron-Tate height $\hat{H}(P) \leq X$,

$$N_{\hat{H}}(A(k), X) = c(\log X)^{r/2} + O((\log X)^{(r-1)/2}). \quad (4.4)$$

Here $c > 0$ is a constant depending on A/k . A general program was started by Franke, Manin and Tschinkel [20] and developed by Batyrev, Salberger, Peyre and others. In this theory the set S is a Fano variety. The asymptotics are predicted by conjectures of Batyrev, Manin [3] and Peyre [29]. But these conjectures are proved only in some special cases (see [29] p.70) and the original conjectures had to be modified due to some counterexamples. The simplest case of a Fano variety is given by a linear projective variety. This case was treated by Thunder. Here it is more convenient to use the l^2 -height instead of the Weil height.

Theorem 4.2 (Thunder). *Let n and $N \geq n+1$ be natural numbers and let V be a linear subvariety of \mathbb{P}^{N-1} of dimension n defined over k . Let $N_2(V(k), X)$ be the number of k -rational points on V with l^2 -height not exceeding X . Then*

$$N_2(V(k), X) = H_2(V)^{-d} \alpha(n, k) X^{d(n+1)} + O(X^{d(n+1)-1} \log X). \quad (4.5)$$

The height $H_2(V)$ is simply the l^2 -height of a set of grassmann coordinates of the subspace of k^N induced by V . The constant α is given by

$$\alpha(n, k) = (2^{-r_k} \pi^{-s_k})^{n+1} V(n+1)^{r_k} V(2n+2)^{s_k} S_k(n) \quad (4.6)$$

where $V(m)$ denotes the volume of the euclidean ball in \mathbb{R}^m with radius one. Since the important work of Bombieri, Pila [6] and Pila [31] various people (Browning, Mc-Kinnon and especially Heath-Brown [15],[16]) succeeded in studying higher dimensional varieties by interpreting them as a collection of curves. If the variety is generated by lines Theorem 4.2 can be used to get information about $N(S, X)$ (see [26] and [5] Theorem 11.10.11).

According to Northcott’s Theorem there is no need to restrict the coordinates of points in S to a fixed number field. Therefore it might be more natural to investigate the set $\mathbb{P}^n(k; e)$; the set of points in $\mathbb{P}^n(\bar{k})$ with relative degree $[k(P) : k] = e$. A first detailed treatment of the counting function of $\mathbb{P}^n(k; e)$ was presented by Schmidt in [35]. No asymptotic estimates were given in this paper but Schmidt already announced his asymptotic results for quadratic points over \mathbb{Q} that appeared in [36]. This initiated the problem (see also [34] p.27) of finding the asymptotics for the more general set $\mathbb{P}^n(k; e)$.

Problem 1 (Schmidt). *Find (when possible) an asymptotic estimate for $N(\mathbb{P}^n(k; e), X)$ as X tends to infinity.*

As already mentioned it was Schmidt himself who made a first contribution with his pioneering work [36].

Theorem 4.3 (Schmidt). *One has*

$$N(\mathbb{P}^n(\mathbb{Q}; 2), X) = \begin{cases} C(\mathbb{Q}, 2, 1)X^6 + O(X^4 \log X) & \text{if } n = 1 \\ C(\mathbb{Q}, 2, 2)X^6 \log X + O(X^6 \sqrt{\log X}) & \text{if } n = 2 \\ C(\mathbb{Q}, 2, n)X^{2(n+1)} + O(X^{2n+1}) & \text{if } n > 2 \end{cases} \quad (4.7)$$

Here $C(\mathbb{Q}, 2, 1) = \frac{8}{\zeta(3)}$, $C(\mathbb{Q}, 2, 2) = \frac{96+8\pi^2}{\zeta(3)^2}$ and $C(\mathbb{Q}, 2, n)$ is given by the infinite sum $C(\mathbb{Q}, 2, n) = \sum_K S_K(n)$ where the sum runs over all quadratic extensions K .

Schmidt proved also an analogue to the above result for a more general kind of height and showed that this leads to asymptotic formulae for the number of decomposable quadratic forms $f(x_0, \dots, x_n) = \sum_{0 \leq i < j \leq n} a_{ij} x_i x_j$ with coefficients a_{ij} in \mathbb{Z} having $|a_{ij}| \leq X$. The form f can also be written as $f = \sum_{i,j=0}^n b_{ij} x_i x_j$. By definition a form is decomposable if it is a product of linear forms with algebraic coefficients. This is exactly the case when the symmetric matrix $[b_{ij}]$ has rank ≤ 2 . Therefore the number of quadratic decomposable forms as above can be interpreted as the number of symmetric $(n+1) \times (n+1)$ matrices with rank ≤ 2 such that $b_{ii} \in \mathbb{Z}$, $|b_{ii}| \leq X$ and $2b_{ij} \in \mathbb{Z}$, $2|b_{ij}| \leq X$ for $i \neq j$. One year after Schmidt's article his Ph.D. student X. Gao [14] established results for arbitrary degrees in large dimensions, but still with $k = \mathbb{Q}$ only.

Theorem 4.4 (Gao). *For $n > e > 2$ one has*

$$N(\mathbb{P}^n(\mathbb{Q}; e), X) = C(\mathbb{Q}, e, n)X^{e(n+1)} + O(X^{e(n+1)-1}). \quad (4.8)$$

The constant $C(\mathbb{Q}, e, n)$ is given by the infinite sum $C(\mathbb{Q}, e, n) = \sum_K S_K(n)$ where the sum runs over all extensions K of degree e .

Note that even the case of cubic points in two dimensions remains unsolved. The strategy of Schmidt and Gao was to prove a result similar to (4.2) but with k^n replaced by the subset of "primitive" points P in K^n i.e. $\mathbb{Q}(P) = K$. The main term remains the same as in (4.2), with K instead of k of course, but Schmidt could replace the error term by

$$O\left(\frac{\sqrt{h_K R_K \log(3 + h_K R_K)}}{|\Delta_K|^{n/2}} X^{2n+1}\right) \quad (4.9)$$

where the constant in O depends only on n but is independent of the field K . This is the major step of the proof and involves many new ideas. Now one can sum over all number fields of degree e and the Theorem of Siegel-Brauer ensures that the sum over the main term $S_K(n)$ as well as over the error term converges, provided n is large enough compared to e . This condition on n is the reason for the restriction $n > e$ in Gao's result. For $1 \leq n \leq e$ Gao found also the correct order of magnitude of $N(\mathbb{P}^n(\mathbb{Q}; e), X)$. However, for $k \neq \mathbb{Q}, e > 1$ there was no asymptotic formula, not even in a single case, until in 2003 when Masser and Vaaler [25] realized that adapting Schanuel's proof to a new class of heights and using the volume computations of Chern and Vaaler [8] provides an asymptotic formula for $n = 1$.

Theorem 4.5 (Masser, Vaaler). *One has*

$$N(\mathbb{P}^1(k; e), X) = eV_{\mathbb{R}}(e)^{r_k} V_{\mathbb{C}}(e)^{s_k} S_k(e) X^{de(e+1)} + O(X^{de(e+1)-e} \log X). \quad (4.10)$$

The constants $V_{\mathbb{R}}(e), V_{\mathbb{C}}(e)$ have their origins in [8]. A simpler version of Theorem 4.5 for $k = \mathbb{Q}$ was given in [24]. Unfortunately the proof of Masser and Vaaler's Theorem shed no light on the case $n > 1$ and more seriously: for $k \neq \mathbb{Q}$ and $e, n > 1$ not even the correct order of magnitude was known. However, for n large enough I was able to deduce an asymptotic estimate (see [40] or [41]).

Theorem 4.6 (W. 2007). *Suppose k is a number field of degree d and $n > 5e/2 + 4 + 2/(de)$. Then*

$$N(\mathbb{P}^n(k; e), X) = C(k, e, n)X^{de(n+1)} + O(X^{de(n+1)-1} \log X),$$

where $C(k, e, n) = \sum_K S_K(n)$ and the sum is taken over all extensions K of k of degree e .

The proof of Theorem 4.6 depends heavily on the work [45] where we proved estimates for the error terms similar to (4.9) but we were using the simpler invariant $\delta(K/k)$ from Section 3 instead of the discriminant. With Jeff Thunder [38] we have recently obtained analogous results in the function field case in positive characteristic.

Regarding integral points not so much is known. However, very recently [46] I have been able to prove an asymptotic estimate for the number of integral points in \bar{k}^n of degree e over the fixed number field k , provided either $e = 1$ or $n > e + 7$ (for $e \geq 9$ we can take $n > e + 2$). The somewhat astonishing aspect of our result is that we actually have found the first $e(q_k + 1)$ main terms (here $q_k = r_k + s_k - 1$ denotes the rank of the unit group of k), whereas all the other mentioned asymptotic results provide only the first main term. In the simplest situation our result counts integral points of k^n . Let $L_q(t)$ be the q -th Laguerre polynomial then the result reads

$$N(\mathcal{O}_k^n, X) = \frac{2^{r_k n} (2\pi)^{s_k n} X^{dn}}{|\Delta_k|^{n/2}} L_{q_k}(-n \log(X^d)) + O(X^{dn-1} (\log X)^{q_k}).$$

The points on a variety over k are necessarily restricted via Diophantine constraints like Faltings' Theorem [13] or the various conjectural generalizations. Indeed, the points are often restricted to proper Zarisky-closed subsets. But any variety defined over \mathbb{Q} say, has a Zarisky dense set of points over $\bar{\mathbb{Q}}$ of sufficiently large fixed degree. Thus one can hope that the behavior of points of fixed degree should be easier to study. However, only little attempts have been made towards this modified Franke-Manin-Tschinkel program (see also Remarks (a) in [19]). The analogue to Gao's result for Thunder's Theorem 4.2, deduced in [40] and [44], can be considered as a first step in this program. For a variety V in \mathbb{P}^{N-1} defined over k we set

$$V(k; e) = V(\bar{k}) \cap \mathbb{P}^{N-1}(k; e).$$

As in Theorem 4.2 we are counting with respect to the l^2 -height.

Theorem 4.7 (W. 2007). *Let e, n and $N \geq n + 1$ be natural numbers and let V be a linear subvariety of \mathbb{P}^{N-1} of dimension n defined over k . Suppose that either $e = 1$ or*

$$n > 5e/2 + 4 + 2/(de).$$

Then

$$N_2(V(k; e), X) = H_2(V)^{-de} \beta(e, n, k) X^{de(n+1)} + O(X^{de(n+1)-1} \log X).$$

The constant β is defined by the sum

$$\beta(e, n, k) = \sum_K \alpha(n, K)$$

taken over all extensions K of k of relative degree e and $\alpha(n, K)$ is defined in Theorem 4.2.

However, more interesting than counting results for linear varieties are results for elliptic curves, defined over \mathbb{Q} , and more generally, for abelian varieties defined over a number field. Su-ion Ih from the University of Colorado and others have thought about this problem and formulated an interesting question. We shall get back at this question in the next subsection.

4.2 Research goals and methods

Let A be an abelian variety defined over a number field k . The famous formula of Néron-Tate gives an asymptotic estimate for the number of k -rational points of bounded height on A as the height tends to infinity. Just as in Problem 1 it would be interesting to prove asymptotic estimates for the set of points on A with given degree $e > 1$ over k . No results in this direction appeared

so far, although some people, mainly Su-ion Ih, have worked on the special case where A is an elliptic curve defined over \mathbb{Q} . In a personal communication Su-ion Ih suggested an interesting asymptotic formula that might be the starting point of a new program. This formula merges two fundamental asymptotic formulae: Schanuel’s formula and the Néron-Tate formula. To the best of our knowledge they have never appeared in the same context so far. If Su-ion Ih’s suggestion is correct then it might be a more general phenomenon that holds for arbitrary abelian varieties. Unfortunately it seems that the strategy of proving asymptotics for fixed number fields and then summing over all number fields of fixed degree, as done in [36], [14], [41] and [44] does not work here. However, the problem of quadratic points P over a rational elliptic curve E is promising. One can take the conjugate P' , and then $Q = P + P'$ is rational. One can consider Q fixed and try to count the points P , e.g. by taking lines through Q and seeing where they cut E . The case $Q = O$ gives the examples with random rational x which show that the dependence is at least polynomial (here $y^2 = x^3 + ax + b$ is an affine model of E). Or one could throw in $R = P - P'$. This is rational on a “twist” E_d of E . So the study of P reduces to the study of the pairs (Q, R) on $E \times E_d$. We might try fixing d and counting the points R . The height should behave quite well; for example the logarithmic Néron-Tate height $\hat{h}(\cdot)$ satisfies the exact formula $\hat{h}(Q) + \hat{h}(R) = 2\hat{h}(P) + 2\hat{h}(P') = 4\hat{h}(P)$. Even though a general asymptotic formula might be out of reach it would be interesting to provide numerical evidence for the suggested formula, at least for quadratic points and some simple elliptic curves of small rank.

- (C1): Provide numerical data to test Su-ion Ih’s “asymptotic formula”.
- (C2): Prove or disprove Su-ion Ih’s suggested formula for elliptic curves.
- (C3): Generalize the previous results to abelian varieties.

References

- [1] E. Arbarello and M. Cornalba, *Footnotes to a paper of Benjamino Segre*, Math. Ann. **256** (1981), 341–362.
- [2] A. Baker and G. Wüstholz, *Logarithmic forms and group varieties*, J. reine angew. Math. **442** (1993), 19–62.
- [3] V. V. Batyrev and Y. I. Manin, *Sur le nombre des points rationnelles de hauteurs bornée des variétés algébriques*, Math. Ann. **286** (1990), 27–43.
- [4] Y. F. Bilu and M. Strambi, *Quantitative Riemann existence theorem over a number field*, arXiv:0809.0345v3 [math.NT] (3 Oct 2008).
- [5] E. Bombieri and W. Gubler, *Heights in Diophantine Geometry*, Cambridge University Press, 2006.
- [6] E. Bombieri and J. Pila, *The number of integral points on arcs and ovals*, Duke Math. J. **59** (1989), 337–357.
- [7] E. Bombieri and U. Zannier, *A Note on heights in certain infinite extensions of \mathbb{Q}* , Rend. Mat. Acc. Lincei **12** (2001), 5–14.
- [8] S-J. Chern and J. D. Vaaler, *The distribution of values of Mahler’s measure*, J. reine angew. Math. **540** (2001), 1–47.
- [9] R. Dvornicich and U. Zannier, *On the properties of Northcott and Narkiewicz for fields of algebraic numbers*, Functiones et Approximatio **39** (2008), 163–173.
- [10] J. Ellenberg, *Points of low height on \mathbb{P}^1 over number fields and bounds for torsion in class groups*, to appear in Computational Arithmetic Geometry.

- [11] J. Ellenberg and A. Venkatesh, *The number of extensions of a number field with fixed degree and bounded discriminant*, Ann. of Math. **163** (2006), 723–741.
- [12] ———, *Reflection principles and bounds for class group torsion*, Int. Math. Res. Not. **no.1**, Art. ID rnm002 (2007).
- [13] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), 349–366.
- [14] X. Gao, *On Northcott’s Theorem*, Ph.D. Thesis, University of Colorado (1995).
- [15] R. Heath-Brown, *Counting rational points on cubic surfaces*, Astérisque **251** (1998), 13–30.
- [16] ———, *The density of rational points on curves and surfaces*, Astérisque **155** (2002), 553–598.
- [17] H. A. Helfgott and A. Venkatesh, *Integral points on elliptic curves and 3-torsion in class groups*, J. Amer. Math. Soc. **19** (2006), 527–550.
- [18] M. Hindry and J.H. Silverman, *Diophantine Geometry An Introduction*, Springer, 2000.
- [19] S. Ih, *Algebraic points on the projective line*, J. Korean Math. Soc. **45** (2008), 1635–1646.
- [20] Y. I. Manin J. Franke and Y. Tschinkel, *Rational points of bounded height on Fano varieties*, Invent. Math. **95** (1989), 421–435.
- [21] O. Kihel, *Sur une conjecture de M. Ruppert*, C. R. Math. rep. Acad. Sci. Canada **22 (2)** (2000), 66–69.
- [22] D. H. Lehmer, *Factorization of certain cyclotomic functions*, Ann. of Math. **34** (1933), 461–469.
- [23] K. Mahler, *An inequality for the discriminant of a polynomial*, Michigan Math. J. **11** (1964), 257–262.
- [24] D. W. Masser and J. D. Vaaler, *Counting algebraic numbers with large height I*, Diophantine Approximation - Festschrift für Wolfgang Schmidt (eds. H. P. Schlickewei, K. Schmidt, R. F. Tichy), Developments in Mathematics 16, Springer 2008, (pp.237–243).
- [25] ———, *Counting algebraic numbers with large height II*, Trans. Amer. Math. Soc. **359** (2007), 427–445.
- [26] D. McKinnon, *Counting rational points on ruled varieties*, Canad. Math. Bull. **47** (2004), 264–270.
- [27] W. Narkiewicz, *Polynomial Mappings*, Lecture Notes in Mathematics 1600, Springer, 1995.
- [28] D. G. Northcott, *An inequality in the theory of arithmetic on algebraic varieties*, Proc. Cambridge Phil. Soc. **45** (1949), 502–509 and 510–518.
- [29] E. Peyre, *Counting points on varieties using universal torsors*, Arithmetic of higher-dimensional algebraic varieties, (B. Poonen, Yu. Tschinkel, eds.), Progress in Mathematics, Birkhäuser Boston, Cambridge, MA **226** (2004), 61–81.
- [30] L. Pierce, *The 3-part of class numbers of quadratic fields*, J. London Math. Soc. **71** (2005), 579–598.
- [31] J. Pila, *Density of integral and rational points on varieties*, Astérisque **228** (1995), 183–187.
- [32] W. Ruppert, *Small generators of number fields*, Manuscripta math. **96** (1998), 17–22.

- [33] S. H. Schanuel, *Heights in number fields*, Bull. Soc. Math. France **107** (1979), 433–449.
- [34] W. M. Schmidt, *Diophantine Approximations and Diophantine Equations*, Lecture Notes in Mathematics 1467, Springer, 1991.
- [35] ———, *Northcott’s Theorem on heights I. A general estimate*, Monatsh. Math. **115** (1993), 169–183.
- [36] ———, *Northcott’s Theorem on heights II. The quadratic case*, Acta Arith. **70** (1995), 343–375.
- [37] J. Silverman, *Lower bounds for height functions*, Duke Math. J. **51** (1984), 395–403.
- [38] J. L. Thunder and M. Widmer, *Counting points of fixed degree and given height over function fields*, In preparation (2010).
- [39] J. D. Vaaler and M. Widmer, *On small generators of number fields*, in preparation (2009).
- [40] M. Widmer, *Asymptotically counting points of bounded height*, Ph.D. Thesis, Universität Basel (2007).
- [41] ———, *Counting points of fixed degree and bounded height*, Acta Arith. **140.2** (2009), 145–168.
- [42] ———, *On certain infinite extensions of the rationals with Northcott property*, to appear in Monatsh. Math. (2009).
- [43] ———, *Small generators of function fields*, to appear in J. Théor. Nombres Bordeaux (2009).
- [44] ———, *Counting points of fixed degree and bounded height on linear varieties*, J. Number Theory **130** (2010), 1763–1784.
- [45] ———, *Counting primitive points of bounded height*, Trans. Amer. Math. Soc. **362** (2010), 4793–4829.
- [46] ———, *The distribution of integral points in affine space*, in preparation (2010).