1 Introduction

My research starts with computation and ends with theory. I tend to choose problems which I can explore first by doing explicit computations, both by hand and by computer. The data collected in this way often gives direction to the theoretical side of my research (illustrated examples below). After all, figuring out what to prove is often a bigger obstacle than the proof itself.

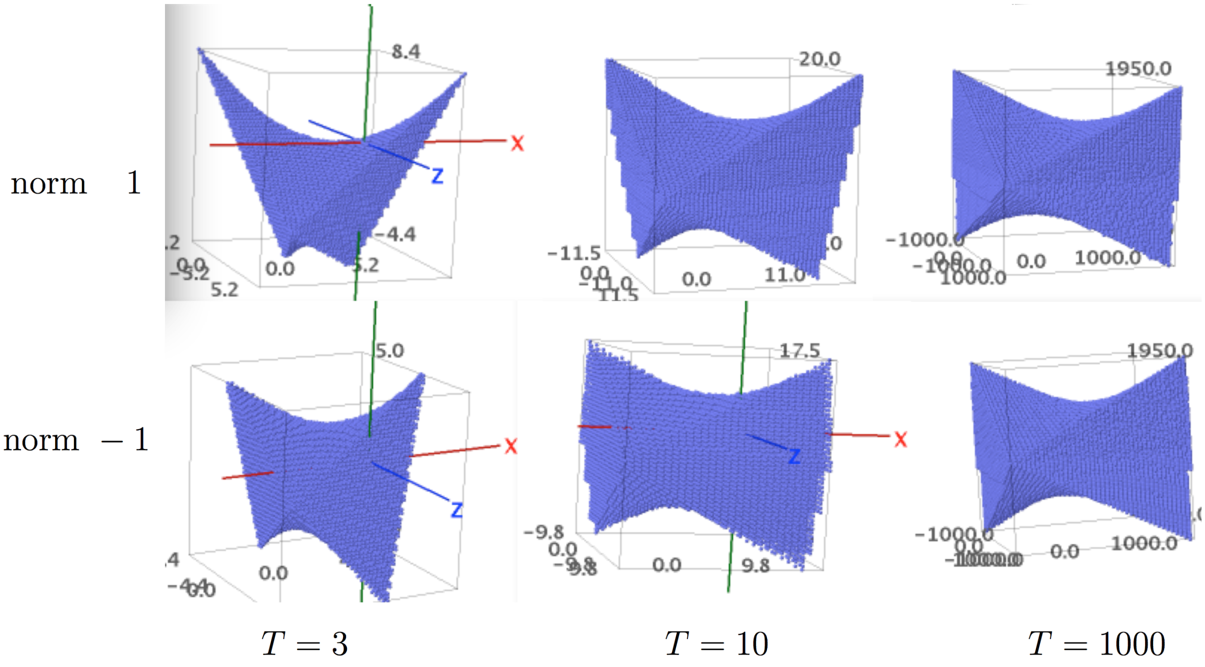


Figure 1: Some scatterplots illustrating the shape of the set of monic degree 4 polynomials $f(Z) = Z^4 + xZ^3 + yZ^2 + zZ \pm 1$ with Mahler measure $M(f) \leq T$. I produced these images to aid in understanding the problem of counting the number of algebraic units of given degree over $\mathbb{Q}$ and increasing height, discussed in Section 2.1.

I've always hated the idea of having to choose one specific focus, because I feel drawn to all branches of mathematics. That's why I'm a number theorist – we use tools from algebra, geometry, analysis, probability, logic, and beyond, all in the study of one of the most basic objects in all of mathematics: the integers. It's also a field that has a long history of being advanced through experimental computation. Gauss's famous quadratic reciprocity theorem was first conjectured by Euler and Legendre based on experimental data. Centuries later, Birch and Swinnerton-Dyer used one of the world's first computers to count the number of mod p solutions to cubic equations in two variables, producing data which led to a conjecture which is today one of the most important in the field, and one of the Millenium Prize problems.

Research in number theory traces back to the basic questions about the integers: what can we say about their algebraic structure (elementary/prime number theory, additive combinatorics, etc.)? What can we say about the solutions to integer polynomial equations in one variable (algebraic number theory) or several variables (diophantine equations/ geometry)? My own research focuses on algebraic number theory and diophantine geometry.

Order is important. For example, we study the prime numbers, of which there are infinitely many, using they fact that they are ordered. This lets us ask questions such as: what proportion of prime numbers are congruent to 1 mod 4? This question makes sense if we consider the proportion of all prime numbers up to an arbitrary given size. In algebraic number theory and diophantine geometry, the notion of a "height function" is an attempt to find the right way to order the points we want to study. Such functions play a fundamental role in diophantine geometry (for example they appear in the proof of the Mordell-Weil theorem and the statement of the Birch and Swinnerton-Dyer conjecture). There are two qualities a good height function (such as the Weil height introduced in the next section) should have:

1. The height of a point be a sensible measure of how complicated a point is, and there should be only finitely many points of bounded height and degree (so that the height can be used for "counting"). For example, in defining the height of an algebraic number, it would make sense if the height of a plain old rational number were an indication of how large the numerator and denominator are when the number is in lowest terms. For general algebraic numbers, the height should in some sense reflect how complicated a polynomial one needs to define it. For solutions to diophantine equations (points on a variety), the height should be related to the heights of the coordinates as algebraic numbers.

2. The height function should "respect" any algebraic structure present. This is similar to what we ask of a norm in a vector space, which is also a measure of the size of points, and which satisfies axioms defined in terms of the algebraic structure of the space.

Quality 1 is what makes height functions a useful approach to bring order to an infinite set of points, allowing people to "count" them: how many points have height less than X? In Section 2 I'll discuss my recent and future work on this theme, including a current project (Section 2.3) which features an application of these ideas to a diophantine problem on the linear relations which can exist between conjugate algebraic numbers.

Quality 2 leads to more subtle questions about "small points." The oldest and deepest such question is known as Lehmer's problem, which is essentially the following question: if the complex roots of an integer polynomial are not all on the unit circle, how close can they be? Is there a theory that explains that the roots are "pushed away" from the unit circle, in some sense? These questions are made precise by being phrased in terms of lower bounds on height functions. These lower bounds, together with upper bounds which come from different considerations, have important applications in diophantine equations. The majority of my published work has been related to questions of small points (how small can they be?). These are discussed in Section 3, along with ongoing and future projects in the area.

2 Arithmetic statistics and asymptotics

2.1 Counting algebraic numbers

For a polynomial

$$f(Z) = x_0 Z^d + \cdots + x_d = x_0(Z - \alpha_1) \cdots (Z - \alpha_d)$$

having real coefficients $x_0, \ldots, x_d$ (with $x_0 \neq 0$) and complex roots $\alpha_1, \ldots, \alpha_d$, we define the *Mahler measure* $M(f)$ of the polynomial f by

$$M(f) = |x_0| \prod_{|\alpha_i|>1} |\alpha_i|.$$

The *absolute Weil height* $H(\alpha)$ of an algebraic number $\alpha \in \overline{\mathbb{Q}}$ can be defined as

$$H(\alpha) = M(f)^{1/d}, \tag{1}$$

where f is the minimal polynomial of α over $\mathbb{Z}$, having degree d. This height function turns out to be the one which generalizes to important height functions used in diophantine geometry and arithmetic dynamics.

If $\mathcal{S}$ is a subset of $\overline{\mathbb{Q}}$ one considers the asymptotics of

$$N(\mathcal{S}, \mathcal{H}) = \#\{x \in \mathcal{S} \mid H(x) \leq \mathcal{H}\},$$

Schanuel [23, Corollary] proved a now classical result in this direction: for any number field K, as $\mathcal{H}$ grows,

$$N(K, \mathcal{H}) = c_K \cdot \mathcal{H}^{2[K:\mathbb{Q}]} + O\left(\mathcal{H}^{2[K:\mathbb{Q}]-1} \log \mathcal{H}\right),$$

where the constant c_K involves all the classical invariants of the number field K, and the $\log \mathcal{H}$ factor disappears for $K \neq \mathbb{Q}$. More recently, natural subsets that aren't contained within a single number field have been examined. Masser and Vaaler [22, Theorem] determined the asymptotic for the entire set $\overline{\mathbb{Q}}_d = \{x \in \overline{\mathbb{Q}} \mid [\mathbb{Q}(x) : \mathbb{Q}] = d\}$:

$$N(\overline{\mathbb{Q}}_d, \mathcal{H}) = \frac{d \cdot V_d}{2\zeta(d+1)} \cdot \mathcal{H}^{d(d+1)} + O\left(\mathcal{H}^{d^2} (\log \mathcal{H})\right),$$

where the $\log \mathcal{H}$ factor disappears for $d \geq 3$, and V_d is an explicit positive constant in terms of d.

This asymptotic was deduced from results of Chern and Vaaler [7], which also imply an asymptotic for the set $\mathcal{O}_d$ of all algebraic integers of degree d, as noted in Widmer [29, (1.2)]. It was sharpened by Barroero [2, Theorem 1.1, case $k = \mathbb{Q}$]:

$$N(\mathcal{O}_d, \mathcal{H}) = d \cdot V_{d-1} \cdot \mathcal{H}^{d^2} + O\left(\mathcal{H}^{d(d-1)} (\log \mathcal{H})\right),$$

where again the $\log \mathcal{H}$ factor disappears for $d \geq 3$.

In a recent paper with Joseph Gunther [18], we added to these results in two ways. First, we extended the results to counting units in the ring of algebraic integers. Secondly, we were able to make explicit the implied constants in the "big O" error terms of Masser-Vaaler and Barroero. The following theorem summarizes these results.

Theorem 2.1. *Let $\overline{\mathbb{Q}}_d$ denote the set of algebraic numbers of degree d over $\mathbb{Q}$, let $\mathcal{O}_d$ denote the set of algebraic integers of degree d over $\mathbb{Q}$, and let $\mathcal{O}_d^*$ denote the set of units of degree d over $\mathbb{Q}$ in the ring of all algebraic integers. For all $d \geq 3$ we have*

$$\begin{array}{lll}
\text{(I)} \ \left|N(\overline{\mathbb{Q}}_d, \mathcal{H}) - \frac{d \cdot V_d}{2\zeta(d+1)}\mathcal{H}^{d(d+1)}\right| & \leq 3.37 \cdot (15.01)^{d^2} \cdot \mathcal{H}^{d^2}, & \text{for } \mathcal{H} \geq 1; \\
\text{(ii)} \ \left|N(\mathcal{O}_d, \mathcal{H}) - dp_d(\mathcal{H}^d)^*\right| & \leq 1.13 \cdot 4^d d^d 2^{d^2} \cdot \mathcal{H}^{d(d-1)}, & \text{for } \mathcal{H} \geq 1; \textit{and} \\
\text{(iii)} \ \left|N(\mathcal{O}_d^*, \mathcal{H}) - 2dV_{d-2} \cdot \mathcal{H}^{d(d-1)}\right| & \leq 0.0000126 \cdot d^3 4^d (15.01)^{d^2} \cdot \mathcal{H}^{d(d-1)-1}, & \\
 & & \text{for } \mathcal{H} \geq d2^{d+1/d}.
\end{array}$$

I place a high value on explicit results, and in this context it is easy to explain this value. While the results cited above with "big O" error terms can be used to pose (asymptotic) questions about the probability that a "random algebraic number of degree d" has a certain property, results that have explicit error bounds, i.e. are uniform in both d and $\mathcal{H}$, allow one to pose more general questions about a "random algebraic number" of unspecified degree, counting numbers in arbitrary "height-degree boxes."

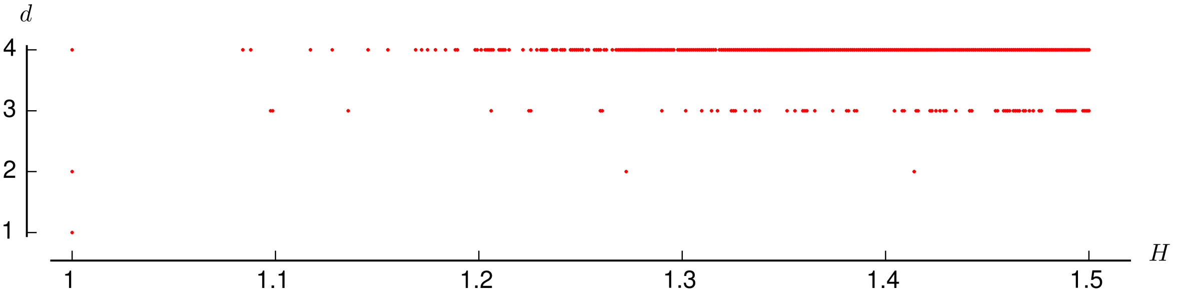


Figure 2: Algebraic numbers of degree $d \leq 4$ and height $H \leq 1.5$. Each dot represents d conjugate algebraic numbers.

These problems of counting algebraic numbers of bounded height amount to those of counting integer polynomials with bounded Mahler measure (i.e. counting the minimal polynomials of the algebraic numbers. The pioneers of this subject were Chern and Vaaler, who showed how to solve the problem by computing the number of lattice points in certain "star-bodies" in euclidean space (where the coordinates correspond to the coefficients of the polynomials) cut out by the condition that the Mahler measure of the polynomials is bounded. The constants V_d above represent the volume of the set of degree d polynomials of Mahler measure at most 1, and were computed explicitly by Chern and Vaaler. For our new problem of counting units, it was important to understand the asymptotic volume of "slices" of these star-bodies corresponding to specifying that the polynomials be monic and have constant coefficient ± 1. The images in Figure 1 above were generated to help understand the asymptotic shape of these slices. Degree 4 polynomials represent both the simplest case where the shapes of the slices cannot be

[*] The function $p_d(T)$ is an explicit polynomial described by Chern and Vaaler whose leading term is $V_{d-1}T^d$.

easily computed by hand, and also the largest degree case where the set can be easily visualized (as degree 4 polynomials have 5 coefficients, but specifying the first and last coefficients yields a 3-dimensional set).

In [18] one of the key steps is to estimate the asymptotic number of integer polynomials with bounded coefficients which are reducible, as the coefficient bound T increases. For general polynomials of degree d, there are $\sim T^{d+1}$ such polynomials, and general Hilbert irreducibility theorem (HIT) results imply that the number of reducible polynomials is $O(T^{d+\frac{1}{2}})\log(T)$, however it can be shown using a technique of W. Schmidt that a stronger estimate of order $O(T^d)$ holds. In other words, a “full power savings” is achieved. Gunther and I used this method to prove similar results for monic polynomials with given second and/or final coefficients. In a forthcoming paper, I am extending these results to as general as possible a setting, proving the following.

Theorem 2.2 (G., forthcoming). *Let $N^{red}_{s,d}$ denote the number of reducible polynomials of degree d with exactly s of their coefficients taking specified values, having all coefficients at most T. Then if $s < d-2$, we have*

$$N^{red}_{s,d} = O(T^{d-s}), \text{ as } T \to \infty.$$

Note that the total number of such polynomials (reducible and irreducible) is $\sim T^{d+1-s}$. In the cases where this applies, it gives a better bound than the previous result [10, Theorem 1].

2.2 Counting number fields

[21, Theorem 1] Let $F(d, X)$ denote the number of number fields (up to isomorphism) of degree d over $\mathbb{Q}$ and discriminant at most X in absolute value. It has been conjectured that $F(d, X) \sim c_d \cdot X$, as $X \to \infty$, where the constant c_d depends only on d[†]. The cases $d = 1, 2$ are trivial, and beyond this the only known cases of this result are in degree 3 (Davenport and Heilbronn), 4 and 5 (mostly Bhargava).

For arbitrary d, the best upper and lower bounds on $F(d, X)$ are due to Ellenberg and Venkatesh [14, Theorem 1.1]. We focus here on their lower bound, which is of the form

$$F(d, X) \gg X^{1/2+1/n^2}.$$

A slightly weaker bound than this could be obtained relatively easily by using my results with Gunther on counting units discussed in the previous section, along with the following classical result (we include a brief proof as it is important for this discussion):

Theorem 2.3 (Mahler). *Let f be any polynomial of degree d,* $\operatorname{disc}(f) = D$*, and $M(f) = M$. Then*

$$|D| \le d^d M^{2d-2}$$

[†] This statement is often described as a “folk” conjecture “possibly” due to the late Soviet mathematician Y. V. Linnik. Etiquette dictates we must continue the tradition of speculative attribution in perpetuity.

Proof. We let $\alpha_1, \ldots, \alpha_d$ denote the roots of f. By expanding the discriminant in terms of a Vandermonde determinant and applying Hadamard's inequality, we find that

$$\begin{aligned} |D| &\leq |\text{leading coefficient}|^{2d-2} \prod_{i=1}^{d} \left(\sum_{j=0}^{d-1} |\alpha_i^j|^2 \right) \\ &\leq |\text{leading coefficient}|^{2d-2} \prod_{i=1}^{d} d \max\{1, |\alpha_i|^{2d-2}\} = d^d M^{2d-2}. \end{aligned}$$

Since the ith factor in this product is at most $d \max\{1, |\alpha_i|^{2d-2}\}$, we achieve (2.3). □

Indeed, using this method to produce a lower bound on $F(d, X)$ is quite similar to the approach taken by Ellenberg and Venkatesh, who use the size of the largest root outside the unit circle in place of the Mahler measure (the size of the product of all roots outside the unit circle). It is worth considering the question: how much can Mahler's inequality be improved? The figure below is an illustration suggesting that improvement is possible.

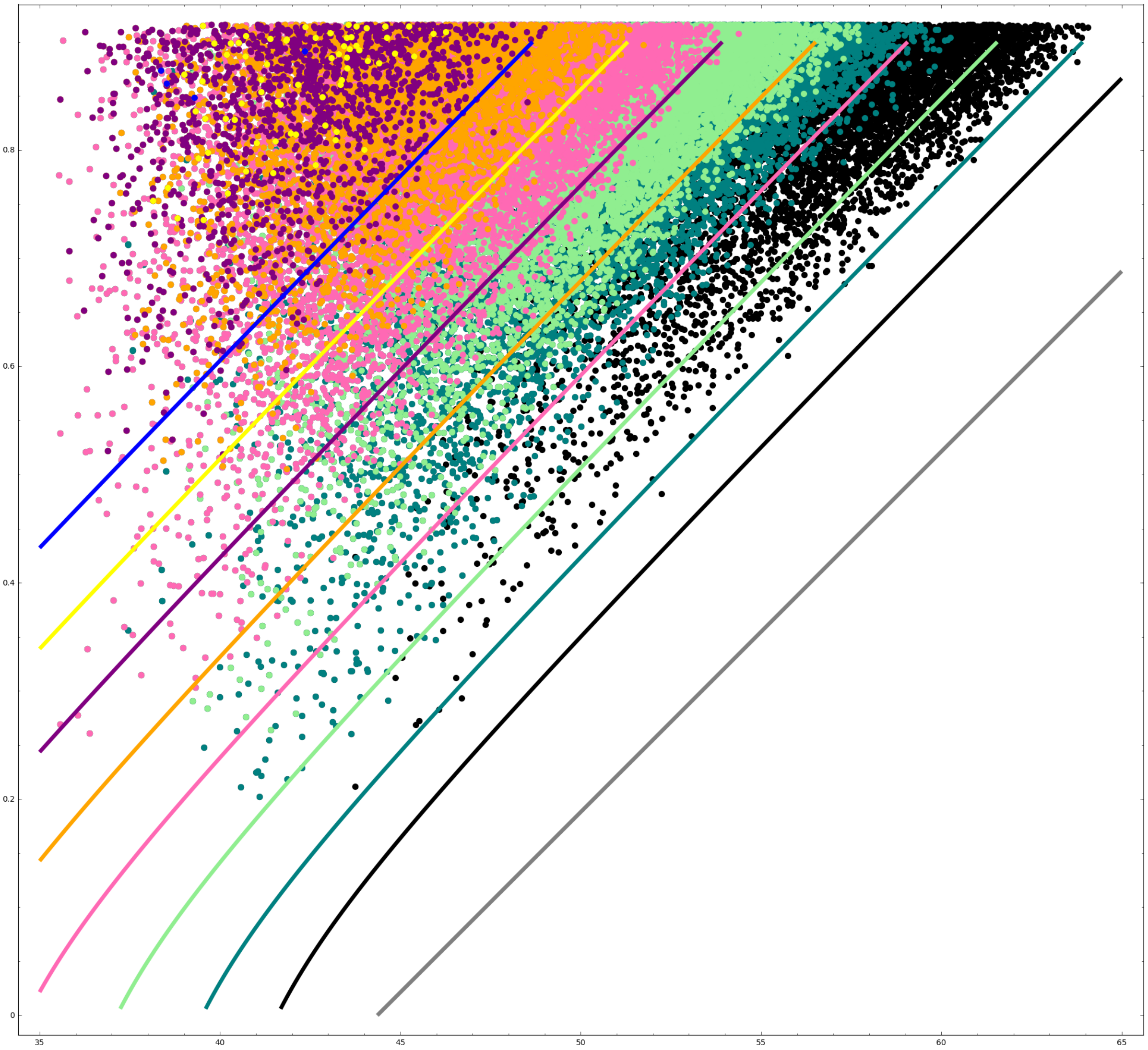


Figure 3: Scatterplot showing $\log M(f)$ (Mahler measure) vs $\log \operatorname{disc}(f)$ for reciprocal polynomials f (of degree 16). Each dot represents a polynomial, and the colors correspond to the number of roots outside the unit circle. The data used to generate this image were computed by my collaborator Michael Mossinghoff. That all dots lie above the gray line is the classical bound of Mahler. The other curves represent bounds in terms of the location of the roots that were easily discovered after analyzing the data.

Unfortunately, it is provably not possible to improve the bounds by replacing the gray line in the figure with one of steeper slope. However, if one could prove that, asymptotically, a positive proportion of the "dots" lie above any line with steeper slope than the gray one, this would be sufficient to improve Ellenberg and Venkatesh's lower bound on $F(d, X)$. While the colorful curves in the figure correspond to tightening the *second* inequality in the proof above of Mahler's theorem, what we need is an improvement in the *first* inequality, which is simply Hadamard's inequality: the determinant is majorized by the product of the euclidean lengths of the matrix's rows. This inequality cannot be sharpened in general, but as is apparent from looking at the data, for many polynomials the result is not sharp. I plan to explore in detail the extent to which heuristic models for the distribution of the lattices spanned by power bases for number fields can be shown to imply improvements on Ellenberg and Venkatesh's lower bound in this way, and, if possible, prove a result along these lines.

2.3 Relations among conjugates

In the 1986 paper [26], Smyth made a striking conjecture about conjugate solutions to linear equations, which is the subject of an current joint project with Jennifer Berg. We work here with the simplest case of the problem. Let a, b, and c be positive integers with no common factor. Smyth observed that there can only be a solution to the equation

$$ax + by + cz = 0 \tag{2}$$

with x, y, and z conjugate algebraic numbers (i.e. all roots of the same irreducible polynomial with integer coefficients) if

- $a \leq b + c$, $b \leq a + c$, and $c \leq a + b$ (i.e. a, b, and c could be the side lengths of a euclidean triangle), and
- a, b, and c are pair-wise relatively prime (i.e. a, b, and c could be the side lengths of a p-adic triangle).

Smyth's conjecture, which remains open, is that these necessary conditions are also sufficient. This is very much in the spirit of classical diophantine problems in which there are obvious "local obstructions" to the existence of solutions, and it is hoped that these are the *only* obstructions.

The rationale behind Smyth's conjecture lies in an equivalent formulation of the problem he discovered. Smyth showed that (2) has a solution in conjugate algebraic numbers if and only if it admits a finite set

$$\mathcal{S} = \{(n_{\ell 1}, n_{\ell 2}, n_{\ell 3})\}_{\ell=1}^{L}$$

of not necessarily distinct *integer* solutions[‡] (always excluding the trivial solution $(0, 0, 0)$) satisfying

$$\{|n_{\ell 1}|\}_\ell = \{|n_{\ell 2}|\}_\ell = \{|n_{\ell 2}|\}_\ell$$

as multisets. We'll call such a family of integer solutions a *happy family.* The proof of the equivalence makes it possible to take a happy family and produce conjugate solutions. For example the set $\{1, -2, 1), (2, 1, -2)$ is a happy family of solutions to

$$3x + 4y + 5z = 0. \tag{3}$$

Using these points, Smyth's proof, and a program written in SAGE, I produced the polynomial $t^8 - 70t^6 + 1435t^4 - 7350t^2 + 16641$, which one can verify has 3 roots x, y, and z satisfying (3). The formulation in terms of happy families makes it possible to search for conjugate solutions systematically.

[‡] So it's really a multiset of points, or a set of points together with weights telling how many of each point to take.

In our forthcoming paper, Berg and I discuss this problem from both perspectives. We describe a precise probabilistic heuristic argument in favor of the conjecture, extend the computational verification of the conjecture begun by Smyth (who verified it for $|a|, |b|, |c| \leq 30$; we are in the lengthy process of verifying it up to 100), and prove the following negative result.

Theorem 2.4 (Berg, G.)**.** *There is no positive integer d such that, for all (a, b, c) satisfying the bulleted conditions above, the equation (2) admits a solution in conjugate algebraic numbers of degree at most d. That is, conjugate solutions to (2) must be of arbitrarily large degree (if they exist), as a, b, and c vary.*

Our strategy of proof is the reason I have chosen to discuss this paper in the section on "arithmetic statistics and asymptotics." We refine yet another of Smyth's equivalent formulations of the conjecture to a statement about rational points on curves: if (a, b, c) admits a solution in conjugates of degree d, then (a, b, c) must lie on one of finitely many projective curves. However, the size of the set of (a, b, c) of bounded height and satisfying the necessary conditions can be estimated asymptotically, and this estimate is large enough to prove the set is Zariski-dense in $\mathbb{P}^2$, i.e. cannot lie in the union of finitely many curves.

Our paper will also discuss the reasons why traditional tools from arithmetic geometry, such as the circle method, do not seem as though they could be useful for proving Smyth's conjecture.

3 Small points

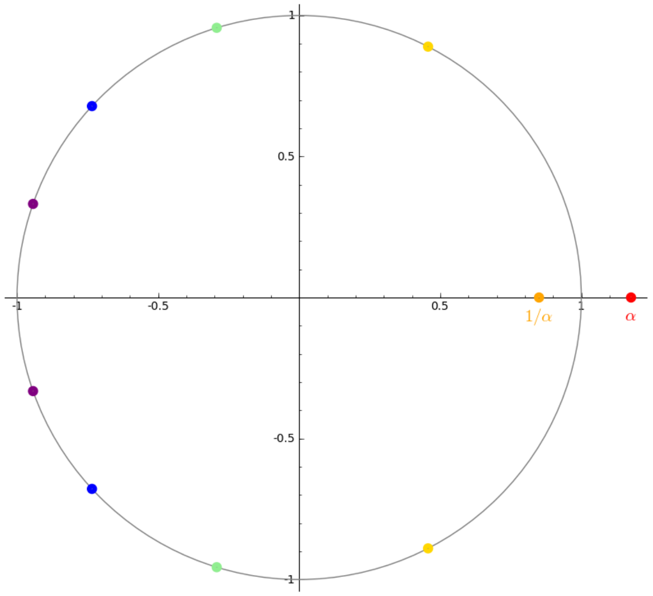
3.1 Background: the Lehmer problem

If $f(x)$ is a monic integer polynomial, then the Mahler measure of f is the size of the product of all its roots which lie outside the unit circle. Let's just focus on the case where $f(x)$ is irreducible over the integers. One possibility is that $f(x)$ is a cyclotomic polynomial, vanishing only at roots of unity. In this case, clearly $M(f) = 1$. It follows from a theorem of Kronecker that this is the only situation where $M(f) = 1$. The *Lehmer problem* is the question: is the Mahler measure of non-cyclotomic polynomials bounded away from 1 by a universal constant? In his search for polynomials with small Mahler measure (though it wasn't known by that name at the time), D.H. Lehmer in 1933 discovered that the polynomial

$$f(x) = x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1$$

has unusually small Mahler measure.

Figure 4: The ten complex roots of Lehmer's polynomial



This polynomial has only one root outside the unit circle, a real number $\alpha \approx 1.17628$ (known as "Lehmer's number"). Its reciprocal $1/\alpha$ is also a root, and the other 8 roots all lie on the unit circle. (Such a real number, having the property that its reciprocal is a conjugate and all its other conjugates lie on the unit circle, is called a "Salem number." These numbers have been thoroughly studied in connection to this problem, but also occur naturally in geometry[§]). Since there is only one root of f outside the unit circle, we have

$$M(f) = \alpha \approx 1.17628.$$

Since then, extensive computations have failed to find a (non-cyclotomic) polynomial with smaller Mahler measure than Lehmer's, and it is thought by many that none exists.

While the simplicity of this problem makes it one of natural independent interest, especially in algebraic number theory, Lehmer's problem today sits within a large area of research about height functions and "small points" – how small can the values of various height functions be? Using (1), Lehmer's problem can be rephrased as: does there exist a universal positive constant c such that

$$\log H(\alpha) \geq \frac{c}{[\mathbb{Q}(\alpha) : \mathbb{Q}]},$$

whenever α is a nonzero algebraic number which is not a root of unity? Phrased this way, the Lehmer problem has a natural analogue for elliptic curves, which has been

[§] for example, Salem numbers arise in studying lengths of geodesics on hyperbolic manifolds, where a gap as suggested in the Lehmer problem would have implications about the minimal length of geodesics. Lehmer's problem is also connected with knot theory, and with measuring the entropy of diffeomorphisms of a complex surface.

studied extensively by Silverman, Hindry, Masser, and Laurent, but remains as open as the original Lehmer problem.

Since $\alpha^{1/n}$ will have height $H(\alpha)^{1/n}$ for any algebraic number α and integer n, the conjectured lower bound in Lehmer's problem is clearly the strongest one can hope for in general. However, under additional assumptions on α we can ask for even stronger results, and this has been the focus of much of my work described below.

3.2 Property (B) and relative Bogomolov extensions

A classical theorem of Kronecker [4, 1.5.9] states that the only elements of $\overline{\mathbb{Q}}^{\times}$ of height 1 are roots of unity (torsion points of the multiplicative group). In [5] Bombieri and Zannier define the Bogomolov Property, or property (B), for a subset of $\overline{\mathbb{Q}}$. This property is satisfied if the height of non-torsion points (i.e. non-roots of unity) is bounded away from 1. (Briefly: the field contains "no small points.") There are many theorems and open questions concerning which subfields of $\overline{\mathbb{Q}}$ satisfy this property. In a recent paper [16] I defined a generalization of this property as follows.

Definition 3.1 (G.)**.** Let $\mathbb{Q} \subseteq K \subseteq L \subseteq \overline{\mathbb{Q}}$ be fields. We say that L/K is *Bogomolov*, or that L/K satisfies the *relative Bogomolov property*, (RB), if there exists $\varepsilon > 0$ such that

$$\{\alpha \in L \bigm| 1 < H(\alpha) < 1 + \varepsilon\} \subseteq K.$$

That is, an extension L/K satisfied (RB) if L has "no new small points." The following facts follow quickly from the definition.

Proposition 3.2. *Suppose $K \subseteq L \subseteq M$ are subfields of $\overline{\mathbb{Q}}$.*

(a) If K satisfies (B), then L/K is Bogomolov if and only if L satisfies (B);

(b) M/K is Bogomolov if and only if M/L and L/K are both Bogomolov; and

(c) if $L \setminus M$ contains a root of unity and M/K is not Bogomolov, then L/K is not Bogomolov.

I construct examples which give the following result, showing that the definition is nontrivial.

Theorem 3.3 (G.)**.** *Let $K/\mathbb{Q}$ be an infinite extension that does not satisfy property (B), and suppose L/K is an algebraic extension. All of the following possibilities can occur:*

(a) L/K is finite and Bogomolov,

(b) L/K is finite and not Bogomolov,

(c) L/K is infinite and Bogomolov, and

(d) L/K is infinite and not Bogomolov.

Note that the real content here is that examples exist of (b) and (c), since examples of (a) and (b) are numerous and easy to construct. My paper also describes a method for explicitly bounding below the height of points in $L \setminus K$ for the type of examples I produce.

My main result is the following, which is proved using a combination of archimedean and non-archimedean estimates.

Theorem 3.4 (G.)**.** *Let $K/\mathbb{Q}$ be a Galois extension. If there exists a (finite) rational prime ℓ with finite ramification index in K, then there exist relative Bogomolov extensions L/K. These extensions can be constructed explicitly of the form $K(\sqrt[\ell]{\alpha})$ for appropriately chosen elements $\alpha \in K$.*

This theorem should be compared with [5, Theorem 2], which states that a Galois extension with bounded *local degree* (ramification index times inertial degree) above some prime has the Bogomolov property.

3.3 Multiplicative diophantine approximation

In the recently submitted paper [20], I some natural questions that arise when the height is thought of as a norm on the multiplicative group. Concretely, properties (1) and (2) (from Section 2 above) actually mean that the *logarithmic Weil height* $h := \log(H)$ is actually a norm on the multiplicative group modulo roots of unity, $\mathcal{G} := \overline{\mathbb{Q}}^\times / \overline{\mathbb{Q}}^\times_{\text{tors}}$ (or equivalently on $\overline{\mathbb{Q}}^\times \otimes_{\mathbb{Z}} \mathbb{Q}$).

One should observe that $\overline{\mathbb{Q}}^\times$ is an abelian group, or $\mathbb{Z}$-module, which is *divisible* – that is, you can take arbitrary roots. The n^{th} root of an algebraic number is well-defined up to multiplication by roots of unity (which are exactly the elements of height zero), and this makes $\overline{\mathbb{Q}}^\times / \overline{\mathbb{Q}}^\times_{\text{tors}}$ into a $\mathbb{Q}$-module, i.e. a vector space over $\mathbb{Q}$. This vector space is written multiplicatively! The vector "addition" arises from traditional multiplication, while "scalar multiplication" by rational numbers arises from exponentiation. The "zero vector" is the equivalence class of 1, which is to say that all roots of unity represent the zero vector.

This norm induces a distance function $(\alpha, \beta) \mapsto h(\alpha/\beta)$, and we are addressing questions about "the distance to a subspace." Specifically, if inside the vector space $\mathcal{G}$ we consider the subspace generated by (the multiplicative group of) a subfield K of $\overline{\mathbb{Q}}$, we show (effectively) that *elements outside of this subspace cannot be arbitrarily close to the space.* Concretely, we have:

Theorem 3.5 (G., Vaaler)**.** *Let K be a subfield of $\overline{\mathbb{Q}}$, and α an algebraic number. Let*

$$h_K(\alpha) = \inf \left\{ h\left(\alpha/\beta^{1/n}\right) \;\middle|\; \beta \in K^\times,\ n \in \mathbb{N} \right\} ¶.$$

Then either some power of α lies in K, in which case $h_K(\alpha) = 0$, or

$$h_K(\alpha) \geq \frac{1}{2} \max\{h(\sigma\alpha/\alpha) \mid \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)\} > 0.$$

¶This is the right definition of "the distance from α to the subspace generated by $K^\times$."

Our result improves on [12, Theorem 2], which establishes this result only for number fields. This should be interpreted as a kind of diophantine approximation result in the multiplicative group scheme $\mathbb{G}_m$, whereas traditional diophantine approximation addresses the additive group $\mathbb{G}_a$. Our paper also includes a generalization of this theorem to the case of studying several fields at once.

Another recent paper of mine, [17], explores some consequences of the above theorem to the cojectures included in the "generalized Lehmer problems" of G. Rémond. I prove that the weakest of these conjectures, the so-called "degree one" form, already implies a seemingly much more general conjecture.

3.4 Small points in free abelian groups

If a subfield K of $\overline{\mathbb{Q}}$ satisfies property (B) – that is, if it has no "small points" – then $\mathbb{G}_m(K)/\text{tors}$ (that is, $K^\times/K^\times_{\text{tors}}$) is a free abelian group (something it's not hard to show holds for a finite extension of $\mathbb{Q}$). This follows immediately from the Lawrence-Zorzitto-Steprans Theorem, which says that "a discretely normed abelian group is free abelian" – property (B) gives the discreteness. My joint paper [19] with Philipp Habegger and Lukas Pottmeyer explores (failure of) the converse of this statement: we show, by constructing explicit examples, that there exist fields K which have points of arbitrarily small positive height, yet where $K^\times/K^\times_{\text{tors}}$ is free abelian. This main difficulties here are:

1. How to make points of small height: one way to do this to consider roots of a sequence of polynomials of increasing degree and bounded coefficients.
2. How to make a "large" (Galois) extension $K/\mathbb{Q}$ which maintains the property that $K^\times/K^\times_{\text{tors}}$ is free abelian. This can be done by controlling the Galois groups of the polynomials, in an effort to make $K^\times$ "far from divisible."

For these purposes, one can take for example the field $\mathbb{Q}^{sym}$ generated over $\mathbb{Q}$ by all polynomials with full symmetric Galois groups. Since the polynomials $x^n - x - 1$ each have symmetric Galois group, and the heights of their roots tend to zero, we can explicitly construct the points of small height, and what remains is a Galois-theoretic argument that $(\mathbb{Q}^{sym})^\times/\text{tors}$ is free abelian.

Real difficulties arise in showing the analogous result for elliptic curves, but we were able to prove the same result in that case as well. If E is an elliptic, defined curve over $\mathbb{Q}$ (for simplicity), then $E(\overline{\mathbb{Q}})/\text{tors}$ is a vector space much in the same way as $\mathbb{G}_m(\overline{\mathbb{Q}})/\text{tors}$, and we also have a height function (namely the square root of the Néron-Tate canonical height) with similar properties to the Weil height (it also induces a norm). Here we are also able to construct fields K such that, if E is any elliptic curve over $\mathbb{Q}$, then $E(K)$ contains points of arbitrarily small height, yet $E(K)/\text{tors}$ is free abelian. Both 1 and 2 above become much more involved in this setting, and proof is rather technical, however an example of a field which works is:

$$K = \left(\left(\mathbb{Q}^{ab}\right)^{sa}\right)^{(2)},$$

where $\mathbb{Q}^{ab}$ denotes the maximal abelian extension of $\mathbb{Q}$, $\left(\mathbb{Q}^{ab}\right)^{sa}$ denotes the field attained by adjoining to $\mathbb{Q}^{ab}$ all roots of polynomials over $\mathbb{Q}^{ab}$ having alternating or symmetric

Galois groups (of all degrees), and $\left(\left(\mathbb{Q}^{ab}\right)^{sa}\right)^{(2)}$ denotes the compositum of all degree 2 extensions of $\left(\mathbb{Q}^{ab}\right)^{sa}$. The construction of the small points is quite elaborate, since it must be done with control over the Galois group of the field of definition, and the proof that the result satisfies the free abelian property is also a lot more work, and is different in the CM and non-CM cases.

To summarize our results:

Theorem 3.6 (G., Habegger, Pottmeyer)**.** *If $\mathcal{G}$ is either $\mathbb{G}_m$ or an elliptic curve defined over $\mathbb{Q}$,*[‖] *then there exist subfields K of $\overline{\mathbb{Q}}$ such that $\mathcal{G}(K)/\mathrm{tors}$ is free abelian, but there are points of arbitrarily small height in $\mathcal{G}(K)$.*

3.5 The compositum of all degree d extensions of a number field

My paper [15], a collaboration with Itamar Gal, focused on basic and general properties of number fields and their Galois groups, but was inspired by questions about heights. We addressed the following two questions about $k^{[d]}$, the compositum of all degree d extensions of an arbitrary number field k :

1. Does $k^{[d]}$ contain all extensions of degree less than d?

   Answer:

   Theorem 3.7 (Gal, G.)**.** *The field $k^{[d]}$ contains all extensions of k of degree less than d if and only if $d < 5$ ("Yes" for $d < 5$ is simply a reinterpreting of old results, but "no" for $d \geq 5$ was new.)*

2. Are all subfields of $k^{[d]}$ generated over k by elements of bounded degree? (If so, we say $k^{[d]}$ is "bounded.") If not, is this at least true if we restrict our attention to subfields which are Galois over k? (If so, we say $k^{[d]}$ is "Galois bounded.")

   Answer: For the first question, we showed this only holds for $d \leq 2$. That is, a compositum of degree d extensions can contain subfields requiring arbitrarily large degree polynomials to generate, whenever $d \geq 3$. For the question about *Galois* subfields, we showed that such a bound exists when d is prime, and fails to exist when d is even, divisible by a square, or satisfies certain other divisibility conditions, but the problem remains open for infinitely many d. The smallest d for which we left the problem open is $d = 15$. To summarize our results:

   Theorem 3.8. *The field $k^{[d]}$ is "bounded" in the above sense if and only if $d \leq 2$, and is "Galois bounded" in the above sense when d is prime*[**]*. It is not Galois bounded whenever d is even, divisible by a square, or divisible by a pair of primes p and q such that $q \equiv 1 \pmod{p}$.*

[‖] Actually, our result as stated in the paper is more general than this.

[**] the result for $d = 3$ has been recently applied as an important ingredient in [11], where the authors classify all torsion structures for rational elliptic curves over $\mathbb{Q}^{(3)}$.

Why was I looking at this problem in the first place? A fundamental result on heights is Northcott's Theorem [4, Theorem 1.6.8], which in its most basic form states that for any bounds d and T there are only finitely many algebraic numbers of degree at most d and height at most T. This result (along with its more general version about points in projective space [4, Theorem 2.4.9]) is simple but powerful. Bombieri and Zannier explored generalizations of this result in [5], where they defined the Northcott property (property (N)). A subset of $\overline{\mathbb{Q}}$ satisfies the Northcott property if for any T it contains only finitely many points of height at most T. The authors were hopeful that Northcott's theorem could be generalized to prove that, for any number field k, property (N) is satisfied by the field $k^{(d)}$ obtained by adjoining to k all algebraic numbers of degree at most d over k. This problem remains open for $d \geq 3$, but they were able to prove that the property is enjoyed by the maximal abelian subextension of $k^{(d)}$.

In this proof, a crucual role is played by the fact that if L/k is an abelian extension generated by elements of degree at most d, then all subextensions K/k are also generated by elements of degree at most d. In [6], Checcoli observed that this property does not hold in general when the assumption that L/k is abelian is dropped. We explored this property further for the fields $k^{[d]}$, analyzing for which values of d the property holds. In all the cases we considered, this issue boiled down via Galois theory to intricate questions about permutation groups.

3.6 Property (N) and number field statistics

I am very interested in the following question, mentioned above in section 3.5.

Question 3.9 (Bombieri and Zannier [5]). *If K is a number field, and $d \geq 3$, does $K^{[d]}$ satisfy property (N)?*

Originally, I hoped that our work on the fields $k^{[d]}$ in [15] would be helpful in showing that those fields do satisfy the property, but I feel the most important next step in the "Northcott problem" is to gather statistical evidence in support of either its truth or falsehood. As pointed out by Widmer [28], crucial to this problem is our ability to determine the smallest height of an element generating a relative extension L/K of number fields. Lower bounds on heights (such as Silverman's inequality [24, Theorem 2], which Widmer uses to prove that property (N) holds in some cases) have been researched thoroughly, and could conceivably be used to answer Question 3.9 positively.

Upper bounds on the smallest height of a generator have been explored very little – see [27] for a discussion of generators of number fields over $\mathbb{Q}$. A more refined estimate along these lines for the generator of a *relative* extension could conceivably be useful in producing an infinite list of elements of bounded height contained in some field $k^{[d]}$, giving a negative answer to the question.

To establish new theorems on fields with the Northcott property it would be desirable to obtain stronger results along the lines of estimating the lowest height of a generator of an extension of number fields, both from above and below. Indeed, even numerical evidence that the best existing estimates could be improved would be desirable. I am very interested in developing computer algorithms for determining or estimating the lowest height of an element in a number field, or properly contained in an extension. To my knowledge, the most similar algorithm that has been implimented along these lines was that of Doyle and Krumm [13], which computes all elements of height below a prescribed bound in a number field, but involves quite a bit of computation, involving the unit and class groups. As the question of the Northcott property is still wide open even for $\mathbb{Q}^{(3)}$, the challenge will be to make an algorithm that helps us find new small points in a tower of cubic and quadratic extensions. Then it would be possible to gather sufficient statistical data to suggest whether or not $\mathbb{Q}^{(3)}$ satisfies the Northcott property. It is also possible that we may be able to apply the wealth of theorems and conjectures on the arithmetic statistics of number fields of low degree, ranging from the Davenport-Heilbronn Theorem and its recent improvements (e.g. [3]) to the Cohen-Lenstra conjectures [9]. I suspect that there is a connection between statistics for cubic fields and the Northcott problem for $\mathbb{Q}^{(3)}$.

3.7 Galois groups in Lehmer's problem

I have a strong feeling that Lehmer's conjecture should be much easier to prove in all cases of reciprocal polynomials where the Galois group is much smaller than it "has to be," and have begun to collect computational evidence that even stronger bounds exist in this case. This idea can be illustrated via Figure 3 above. The Lehmer conjecture asserts that there is a horizontal line above which lie not only all the points in *that* plot (degree 16 polynomials), but all the points in the corresponding plots for each degree. So the conjecture is about the position of the "lowest dot" on all such plots (our figure provably contains this point for degree 16). If we only plot polynomials with various "small" Galois groups, we see that in some cases the lowest dot is much higher.

Some authors have already explored the relationship between the Galois group of the polynomial f and the Lehmer problem. In this direction there is the following theorem, which is a corollary [1, Corollaire 1.8] of a deep result of Amoroso and David that gives a Dobrowolski-type bound[††] for a higher dimensional version of Lehmer's problem.

Theorem 3.10 (Amoroso & David)**.** *For each positive integer m, there exists a constant $c(m) > 0$ such that the following holds. If α is an algebraic number, not a root of unity, of degree d over $\mathbb{Q}$ and whose minimal polynomial has Galois group of order at most d^m, then*

$$h(\alpha) \geq \frac{c(m)}{d}.$$

In particular (taking $m = 1$), there is a universal constant c such that $h(\alpha) \geq c/d$ whenever α is not a root of unity and $\mathbb{Q}(\alpha)/\mathbb{Q}$ is a Galois extension.

This result should be interpreted as a lower bound on the Galois groups which must be considered in attacking Lehmer's problem – in fact, it has very recently been observed by David Masser (and given as an exercise in a soon-to-be-published book) that one can achieve even stronger bounds under the assumption that $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois, of the form $h(\alpha) \geq c_\varepsilon d^{-\frac{1}{2}-\varepsilon}$.

[††] Dobrowolski's Theorem is a lower bound of the form $h(\alpha) \geq \frac{c}{d}\left(\frac{\log\log(3d)}{\log(3d)}\right)^3$, where $d = [\mathbb{Q}(\alpha) : \mathbb{Q}]$.

If we seek an *upper* bound on the Galois group, we may turn to one of the most significant early breakthroughs in Lehmer's problem, which was achieved in 1971 by Smyth in [25]. Smyth showed, using analytic techniques, that Lehmer's problem has a positive answer for polynomials which are not reciprocal. Recall that a polynomial $f(x)$ of degree $d = 2n$ is reciprocal if $f(x) = x^d f(1/x)$, or equivalently if each root α of $f(x)$ has the property that $1/\alpha$ is also a root of $f(x)$. Since Lehmer's problem is trivial in the case where $f(x)$ is not monic, the only polynomials we must study in attacking Lehmer's problem are therefore monic, irreducible, reciprocal polynomials of even degree $d = 2n$ in $\mathbb{Z}[x]$ (these include the Salem polynomials mentioned above). This condition places an upper bound on the Galois group, because the group must respect the partition of the $2n$ roots into pairs of reciprocals.

Let f be a such a polynomial, with a root α. In general such a polynomial has a Galois group which is naturally a subgroup of the group of permutations which respect the fact that the $2n$ roots are partitioned into pairs $(\alpha_i, 1/\alpha_i)$. This group is isomorphic to $C_2 \wr S_n = C_2^n \rtimes S_n \leq S_d$ (here C_2 represents a cyclic group of order 2). The Galois group of f will be a (not necessarily split) extension $A.H$, where $A \leq C_2^n$ has order 2^r, $1 \leq r \leq n$, and H is a transitive subgroup of S_n, which is the Galois group of the "trace polynomial," i.e. the minimal polynomial of $\alpha + 1/\alpha$. McKee and Christopoulos have shown in [8] that if f is a Salem polynomial, then $r \in \{n-1, n\}$. I have begun a computational project with Michael Mossinghoff, in which we compute Galois groups for all reciprocal polynomials of a given degree and bounded Mahler measure, finding for various Galois groups the polynomial which provably has the smallest Mahler measure. Preliminary data suggest that polynomials in which $r < n - 1$ must have higher Mahler measure because of this restriction, but much more data needs to be collected to formulate a precise conjecture. We are also interested in whether or not we can expect a better lower bound on Mahler measure under the assumption that H is strictly smaller than the symmetric group S_n.

References

[1] Francesco Amoroso and Sinnou David. Le problème de Lehmer en dimension supérieure. *J. Reine Angew. Math.*, 513:145–179, 1999.

[2] Fabrizio Barroero. Counting algebraic integers of fixed degree and bounded height. *Monatsh. Math.*, 175(1):25–41, 2014.

[3] Manjul Bhargava, Arul Shankar, and Jacob Tsimerman. On the Davenport–Heilbronn theorems and second order terms. *Invent. Math.*, 193(2):439–499, 2013.

[4] Enrico Bombieri and Walter Gubler. *Heights in Diophantine geometry*, volume 4 of *New Mathematical Monographs*. Cambridge University Press, Cambridge, 2006.

[5] Enrico Bombieri and Umberto Zannier. A note on heights in certain infinite extensions of $\mathbb{Q}$. *Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei (9) Mat. Appl.*, 12:5–14 (2002), 2001.

[6] Sara Checcoli. Fields of algebraic numbers with bounded local degrees and their properties. *Trans. Amer. Math. Soc.*, 365(4):2223–2240, 2013.

[7] Shey-Jey Chern and Jeffrey D. Vaaler. The distribution of values of Mahler's measure. *J. Reine Angew. Math.*, 540:1–47, 2001.

[8] Christos Christopoulos and James McKee. Galois theory of Salem polynomials. *Math. Proc. Cambridge Philos. Soc.*, 148(1):47–54, 2010.

[9] Henri Cohen and H. W. Lenstra, Jr. Heuristics on class groups. In *Number theory (New York, 1982)*, volume 1052 of *Lecture Notes in Math.*, pages 26–36. Springer, Berlin, 1984.

[10] S. D. Cohen. The distribution of the Galois groups of integral polynomials. *Illinois J. Math.*, 23(1):135–152, 1979.

[11] Harris B. Daniels, Álvaro Lozano-Robledo, Filip Najman, and Andrew V. Sutherland. Torsion subgroups of rational elliptic curves over the compositum of all cubic fields. *Math. Comp.*, 87(309):425–458, 2018.

[12] Ana Cecilia de la Maza and Eduardo Friedman. Heights of algebraic numbers modulo multiplicative group actions. *J. Number Theory*, 128(8):2199–2213, 2008.

[13] John R. Doyle and David Krumm. Computing algebraic numbers of bounded height. *Math. Comp.*, 84(296):2867–2891, 2015.

[14] Jordan S. Ellenberg and Akshay Venkatesh. The number of extensions of a number field with fixed degree and bounded discriminant. *Ann. of Math. (2)*, 163(2):723–741, 2006.

[15] Itamar Gal and Robert Grizzard. On the compositum of all degree d extensions of a number field. *J. Théor. Nombres Bordeaux*, 26(3):655–673, 2014.

[16] Robert Grizzard. Relative Bogomolov extensions. *Acta Arith.*, 170(1):1–13, 2015.

[17] Robert Grizzard. Remarks on Rémond's generalizes Lehmer problems, preprint: arxiv.org/abs/1710.11614. 2017.

[18] Robert Grizzard and Joseph Gunther. Slicing the stars: counting algebraic numbers, integers, and units by degree and height. *Algebra Number Theory*, 11(6):1385–1436, 2017.

[19] Robert Grizzard, Philipp Habegger, and Lukas Pottmeyer. Small points and free abelian groups. *Int. Math. Res. Not. IMRN*, (20):10657–10679, 2015.

[20] Robert Grizzard and Jeffrey D. Vaaler. Multiplicative approximation by the Weil height, preprint: arxiv.org/abs/1710.08399. 2017.

[21] K. Mahler. An inequality for the discriminant of a polynomial. *Michigan Math. J.*, 11:257–262, 1964.

[22] David Masser and Jeffrey D. Vaaler. Counting algebraic numbers with large height. I. In *Diophantine approximation*, volume 16 of *Dev. Math.*, pages 237–243. Springer-WienNewYork, Vienna, 2008.

[23] Stephen Hoel Schanuel. Heights in number fields. *Bull. Soc. Math. France*, 107(4):433–449, 1979.

[24] Joseph H. Silverman. Lower bounds for height functions. *Duke Math. J.*, 51(2):395–403, 1984.

[25] Christopher. J. Smyth. On the product of the conjugates outside the unit circle of an algebraic integer. *Bull. London Math. Soc.*, 3:169–175, 1971.

[26] Christopher J. Smyth. Additive and multiplicative relations connecting conjugate algebraic numbers. *J. Number Theory*, 23(2):243–254, 1986.

[27] Jeffrey D. Vaaler and Martin Widmer. A note on generators of number fields. In *Diophantine methods, lattices, and arithmetic theory of quadratic forms*, volume 587 of *Contemp. Math.*, pages 201–211. Amer. Math. Soc., Providence, RI, 2013.

[28] Martin Widmer. On certain infinite extensions of the rationals with Northcott property. *Monatsh. Math.*, 162(3):341–353, 2011.

[29] Martin Widmer. Integral points of fixed degree and bounded height. *International Mathematics Research Notices*, 2016(13):3906–3943, 2016.