Improving Schmidt's Bound for Number Fields

David Lowry-Duda

May 2022

ICERM
May 2022 Meeting of Simons AGNTC

This began with a series of ideas coming from an AIM workshop on Arithmetic Statistics, Discrete Reduction, and Fourier Analysis from February of last year.

In many ways this is a continuation to the talk I gave in November of 2021, in which I described [AGO$^+$], *Quantitative Hilbert irreducibility and almost prime values of polynomial discriminants*. I will describe ideas that led to our recent preprint *Improved bounds on number fields of small degree*.

This work was done in collaboration with Theresa Anderson, Ayla Gafni, Kevin Hughes, Robert Lemke Oliver, Frank Thorne, Jiuya Wang, and Ruixiang Zhang.

But I note that I'm describing conceptually simpler, typically weaker arguments than in our work — any mistakes are probably my own.

Broad Strategy

Our goal is to count the number $N_n(X)$ of degree n number fields over $\mathbb{Q}$ with discriminant up to X. The typical bound is due to Schmidt:

$$N_n(X) \ll X^{\frac{n+2}{4}}.$$

We use the same initial setup: to count $N_n(X)$, we count monic polynomials

$$f(x) = x^n + c_1 x^{n-1} + \cdots + c_n.$$

It will be convenient to introduce an auxiliary notation

$$H = X^{\frac{1}{2n-2}}.$$

Schmidt showed that it suffices to count irreducible polynomials f with trace 0 (i.e. with $c_1 = 0$) and where $|c_i| \ll_n H^i$. We refer to polynomials satisfying this coefficient bound as *the set of polynomials of height H*.

It's not hard to show that including polynomials that don't have trace 0 causes no problems. This naively adds a factor of H (as we count over $|c_1| \leq H^1$) — but this family overcounts also by a factor of at least H.

We summarize this in the following lemma.

Lemma

The cardinality of the set of monic irreducible polynomials of height H bounds $H \cdot N_n(X)$. Thus to bound $N_n(X)$, it suffices to count these polynomials and divide by H.

Sources of Loss

This rough outline clearly detects all number fields, but typically vastly overestimates. There are two large sources of error.

1. The typical polynomial of height H has $\mathrm{Disc}(f) \approx H^{n^2-n} = X^{\frac{n}{2}}$, and typically cuts out a number field with similar discriminant. Thus we are including many, many extraneous polynomials by including all polynomials of height up to H.
2. Overcounting: the same number field might be counted repeatedly.

From one point of view, in this work we identify some of the extraneous polynomials and omit them from the count. But I note that without many substantially new ideas, any method using similar strategies will still produce a large overestimate.

To count these polynomials, we split them into two pieces:

1. We first count polynomials with ‘small’ discriminant, and then
2. We count polynomials with ‘large’ discriminant.

Most polynomials have large discriminant. If $f(x)$ cuts out the field K, then

$$\mathrm{Disc}(f) = \mathrm{Disc}(K)[\mathcal{O}_K \colon \mathbb{Z}[\alpha]]^2,$$

where α is a root of f over K. We call the last factor $\mathrm{Index}(f)^2$. In order to bound the number of polynomials with large discriminant, we split these into two subpieces, depending on whether the radical of the index is small or large.

1. We first count polynomials with ‘small’ discriminant, and then
2. 2.1 We then count polynomials with ‘large’ discriminant and ‘large’ index radical.
   2.2 We then count polynomials with ‘large’ discriminant and ‘small’ index radical.

Small discriminant

For polynomials of small discriminant, we appeal to “trivial” bounds coming from Davenport’s Lemma.

Lemma (Davenport’s Lemma)

Suppose $\Omega \subset \mathbb{R}^n$ is a region cut out by algebraic inequalities. Then the number of lattice points $\mathbb{Z} \cap \Omega$ is

$$\mathrm{Vol}(\Omega) + O\big(\max_{\pi} \mathrm{Vol}(\pi(\Omega))\big),$$

where the maximum runs over projections π of $\mathbb{R}^n$ onto its various coordinate hyperplanes.

Morally, the number of lattice points in a region is the volume of the region, up to an error comparable to the *surface area* of the region (appropriately defined).

We define our region to be

$$\Omega_{H,Y} := \{(c_1, \dots, c_n) \in \mathbb{R}^n : |c_i| \le H^i, \mathrm{Disc}(f_c) \le H^{n^2-n}/Y\}.$$

We will freely translate between $\mathbf{c} \in F^n$ and monic polynomials in $F[x]$, via

$$f_c(x) = x^n + c_1 x^{n-1} + \dots + c_n.$$

The maximum volume of coordinate projections is trivially $O_n(H^{\frac{n^2+n}{2}-1})$, coming from projecting $(c_1, \dots, c_n) \mapsto (c_2, \dots, c_n)$ (i.e. forgetting c_1) and ignoring the discriminant condition.

It remains to consider the volume of $\Omega_{H,Y}$. As

$$\mathrm{Vol}(\Omega_{H,Y}) = H^{\frac{n^2+n}{2}} \mathrm{Vol}(\Omega_{1,Y}),$$

it suffices to consider $\Omega_{1,Y}$.

The discriminant $\mathrm{Disc}(f_c)$ is a polynomial in $c_1, \ldots, c_n$ with integer coefficients. Explicit computation shows that, as a polynomial in c_n,

$$\mathrm{Disc}(c_n) = (-1)^{\frac{n(n-1)}{2}} n^n c_n^{n-1} + O(c_n^{n-2}).$$

Van der Corput's lemma then implies that

$$|\{c_n \in [-1,1] : |\mathrm{Disc}(c_n)| \leq 1/Y\}| \ll_n Y^{-\frac{1}{n-1}}.$$

Applying this bound pointwise for each $c_1, \ldots, c_{n-1}$ in $[-1,1]^{n-1}$, we estimate $\mathrm{Vol}(\Omega_{1,Y} \ll_n Y^{-\frac{1}{n-1}})$.

Lemma (Small discriminant bound)

Let $n \geq 3$, $Y \geq 1$, $H \gg_n 1$. Then the number of polynomials $f(x) \in \mathbb{Z}[x]$ of the form $f(x) = x^n + c_1 x^{n-1} + \cdots + c_n$ with $|c_i| \leq H^i$ and $\mathrm{Disc}(f) \leq H^{n^2-n}/Y$ is

$$O_n\Big(H^{\frac{n^2+n}{2}}/Y^{\frac{1}{n-1}} + H^{\frac{n^2+n}{2}-1}\Big).$$

Large discriminant and large index radical

Our work was first inspired from an old preprint of Bhargava, Shankar, and Wang [BSW22], in which they prove the following.

Lemma (BSW-Inventiones)

For $n \geq 3, H \geq 1, M \geq 1$, we have that

$$\#\left\{ f_c : {}_{m^2 | \mathrm{Disc}(f_c) \text{ for some squarefree } m \geq M}^{|c_i| \leq H^i} \right\} \ll_n \frac{H^{\frac{n^2+n}{2}}}{M} + H^{\frac{n^2+n}{2} - \frac{1}{5}}.$$

Note that $\mathrm{Index}(f)^2 \mid \mathrm{Disc}(f)$, and if $\mathrm{Index}(f)$ is large and has large radical, then it has a large squarefree part. On its own, this could prove nontrivial bounds for the large index radical subcase.

In our paper, we also describe how to sharpen this result, going saving $-\frac{1}{2} + \epsilon$ instead of $-\frac{1}{5}$.

Small index radical

It remains to count polynomials with large discriminant, but small index radical. We prove that

Theorem

The number of polynomials of degree n and height H for which $\mathrm{rad}(\mathrm{Index}(f)) < H^{1-\epsilon}$ *but* $\mathrm{Index}(f) > H^{\frac{n(n-3)}{2}}$ *is* $O(H^{\frac{n^2+n}{2}-\frac{4}{3}-\frac{4}{n}+\epsilon} + H^{\frac{n^2+n}{2}-\frac{2n}{3}+3+\epsilon})$.

We'll return to this later. A large part of our recent preprint works on proving this result. More broadly, suppose we had a hypothetical result for some $0 < \alpha < 1$ and $\beta > 0$:

Proposition (Proposition $P(\alpha, \beta)$)

The number of polynomials of degree n and height H for which $\mathrm{rad}(\mathrm{Index}(f)) < H^{\alpha}$ *but* $\mathrm{Index}(f) > H^{\frac{n(n-3)}{2}}$ *is* $O(H^{\frac{n^2+n}{2}-\beta+\epsilon})$.

Assembling a proof

As noted before, $\mathrm{Disc}(f) = \mathrm{Disc}(K)\,\mathrm{Index}(f)^2$. Taking $Y = H^{n-1}$ in the *small discriminant lemma* shows that the number of polynomials of height up to H and having $\mathrm{Disc}(f) \leq H^{(n-1)^2}$ is $O(H^{\frac{n^2+n}{2}-1})$. Thus with at most that many exceptions,

$$\mathrm{Index}(f)^2 \cdot \mathrm{Disc}(K) = \mathrm{Disc}(f) \geq H^{(n-1)^2}.$$

We are counting number fields K with $\mathrm{Disc}(K) \leq X \sim H^{2(n-1)}$, and thus each of the corresponding polynomials has index bounded below by

$$\mathrm{Index}(f) \gg H^{\frac{(n-1)(n-3)}{2}}.$$

Taking $M = H^\alpha$ in the BSW Lemma shows that the number of polynomials of height H, index bounded below by $H^{\frac{(n-1)(n-3)}{2}}$, and index radical bounded below by H^α is at most $H^{\frac{n^2+n}{2}-\alpha} + H^{\frac{n^2+n}{2}-\frac{1}{5}}$. And Proposition $P(\alpha, \beta)$ (if true) implies that the number of remaining polynomials (with $\mathrm{rad}(\mathrm{Index}(f)) < H^\alpha$) is at most $H^{\frac{n^2+n}{2}-\beta+\epsilon}$.

In total, these bounds imply that

$$H \cdot N_n(X) \ll H^{\frac{n^2+n}{2} - \alpha + \epsilon} + H^{\frac{n^2+n}{2} - \beta + \epsilon} + H^{\frac{n^2+n}{2} - \frac{1}{5}}.$$

Recalling that $H \approx X^{\frac{1}{2n-2}}$, let $\delta = \min\{\frac{1}{5}, \alpha, \beta\}$. Then this shows that

$$N_n(X) \ll X^{\frac{n+2}{4} - \frac{\delta}{2n-2} + \epsilon}.$$

In particular, *any* proved form of Proposition $P(\alpha, \beta)$ yields an improvement over Schmidt.

In our preprint, we show that we can take $\delta = \frac{1}{2}$. I note that a preprint of Bhargava, Shankar, and Wang (appearing on the arxiv on the same day as ours) shows that one can take $\delta \asymp_n 1$.

In the remainder of this talk, I'd like to describe how one might try to prove propositions $P(\alpha, \beta)$.

Intuitively, one first quantifies the intuition that if $\mathsf{Index}(f)$ is large but $\mathrm{rad}\mathsf{Index}(f)$ is small, then $\mathsf{Index}(f)$ should be highly divisible by 'large' powers of primes. In practice we show that there is a cubefull divisor d of $\mathsf{Index}(f)$ of size $H^2 < d \leq H^3$.

Then we bound the number of polynomials of height H with $d^2 \mid \mathsf{Disc}(f)$, and take the union bound across various possible cubefull d.

To bound the number of polynomials with $d^2 \mid \mathrm{Disc}(f)$, we use Fourier analysis. Let $\psi_{p^{2k}}$ be the characteristic function for polynomials having p^{2k} dividing their discriminants and define

$$\widehat{\psi_{p^{2k}}}(\mathbf{u}) := \frac{1}{p^{2kn}} \sum_{f} \psi_{p^{2k}}(f) \exp\left(\frac{2\pi i \langle f, \mathbf{u} \rangle}{p^{2k}}\right).$$

Then our goal is to produce good bounds for $\widehat{\psi_{p^{2k}}}$ and to study its support.

Bounds

The "trivial" Fourier estimate is the density of the relevant polynomials.

Lemma

Let $n \geq 2, k \geq 1$. The set of monic polynomials $f \in \mathbb{Z}_p[x]$ for which $p^{2k} \mid \mathrm{Disc}(f)$ has relative density $O_n(p^{-k})$.[1]

To prove this, we appeal to work of Shankar and Tsimerman [ST20]. Let $d\nu$ denote the Haar measure on polynomial coefficient space and $d\mu$ denote the Haar measure on the p-adic completion of the space of roots. Shankar and Tsimerman related these Haar measures, implying

$$\begin{aligned}\int \mathbf{1}_{p^{2k}}(f) d\nu(f) &= \sum_{[K_p:\mathbb{Q}_p]=n} \frac{|\mathrm{Disc}(K_p)|_p^{1/2}}{|\mathrm{Aut}(K_p)|} \int_{O_{K_p}} |\mathrm{Disc}(\alpha)|_p^{1/2} \mathbf{1}_{p^{2k}}(\alpha) d\mu(\alpha) \\ &\leq \frac{1}{p^k} + O(p^{-k-\frac{1}{2}}).\end{aligned}$$

[1] In our paper, we atually show it's $O_n(p^{-k-\frac{2k}{n}})$.

Nontrivial bounds

Lemma

Write $\mathbf{u} = (u_1, \ldots, u_n)$. Let $m \leq n$ be the greatest coefficient index for which $u_m \neq 0 \bmod p^{2k}$.

- *If $\mathbf{u} = 0$, then $\widehat{\psi_{p^{2k}}}(\mathbf{0}) \ll_n p^{-k}$.*
- *If $m = 1$, then $\widehat{\psi_{p^{2k}}}(\mathbf{u}) = 0$ unless u_1 is divisible by $p^{2k} / \gcd(n, p^{2k})$.*
- *If $m > 1$, then $\widehat{\psi_{p^{2k}}}(\mathbf{u}) \ll_n p^{-\frac{5k}{2} + v_p(u_m)}$.*

Heuristic proof: the group $\mathrm{AGL}(1)$ acts on these polynomials via

$$f(x) \mapsto \alpha^n f(\alpha^{-1} x + \beta),$$

and this preserves the condition that $p^{2k} \mid \mathrm{Disc}(f)$. An application of Plancherel's Theorem shows that (for $\mathbf{u}$ having orbit $\mathcal{O}$)

$$|\widehat{\psi_{p^{2k}}}(\mathbf{u})| \ll_n p^{-k/2} / \sqrt{|\mathcal{O}|}.$$

Support

Finally, we show that the support of $\widehat{\psi_{p^{2k}}}$ is constrained to "near arithmetic progressions." Roughly, if $\mathbf{u} = (u_1, \ldots, u_n) \in (\mathbb{Z}/p^{2k}\mathbb{Z})^n$, then $\mathbf{u}$ is in the support only if

$$\min\{v_p(u_i), k\} = \min\{v_p(u_n) + (n-i)a, k\}.$$

This is like an arithmetic progression, except that terms above k are considered k (and don't break arithmetic progressions).

Heuristic proof: The discriminant polynomial satisfies many algebraic relationships. We show that if $p^{2k} \mid \mathrm{Disc}(f)$, and defining D_i to be the partial derivative of f with respect to its ith coefficient, then we show that $\mathrm{Disc}(f)$ is in the ideal $(D_r D_s - D_{r+k} D_{s-k})$ over $\mathbb{Z}$.

Thank you very much.

Please note that these slides (and references for the cited works) are (or will soon be) available on my website (davidlowryduda.com).

References i

Theresa C Anderson, Ayla Gafni, Robert J Lemke Oliver, David Lowry-Duda, George Shakan, and Ruixiang Zhang.
Quantitative hilbert irreducibility and almost prime values of polynomial discriminants.
Int. Math. Res. Not.
To appear. `https://arxiv.org/abs/2107.02914`.

Manjul Bhargava, Arul Shankar, and Xiaoheng Wang.
Squarefree values of polynomial discriminants I.
Inventiones Mathematicae, 2022.
To appear.

Arul Shankar and Jacob Tsimerman.
Heuristics for the asymptotics of the number of S_n-number fields, 2020.
arxiv:2006.09620.