ARITHMETIC STATISTICS COURSE NOTES

ROBERT J. LEMKE OLIVER

3. Bounds on number fields and Schmidt's theorem

We now turn to proving one of the most fundamental results in arithmetic statistics.

Theorem 3.1 (Hermite–Minkowksi)**.** *There are finitely many number fields of bounded discriminant.*

This is a statement that's independent of degree. To clarify, a simple consequence of Theorem 3.1 is that there are only finitely many number fields, of any degree, whose discriminant is at most 1000 – or, indeed, at most X for any X. We refer to this as a fundamental result because it then enables the question:

Question ("The fundamental question of arithmetic statistics")**.** How many number fields are there of discriminant at most X? In other words, how does the function

$$N(X) := \#\{K/\mathbb{Q} : |\mathrm{Disc}(K)| \leq X\}$$

grow as $X \to \infty$?

Historically, Theorem 3.1 was proved in two steps. First, Minkowski proved that discriminants must grow as degrees grow. More specifically, he proved:

Theorem 3.2 (Minkowski; 1889)**.** *For any number field K of degree $n \geq 2$, the discriminant satisfies*

$$\sqrt{|\mathrm{Disc}(K)|} \geq \left(\frac{\pi}{4}\right)^{n/2} \frac{n^n}{n!}.$$

An exercise in the ratio test shows this quantity tends to infinity as n tends to infinity, and thus if we are interested only in the number fields for which $|\mathrm{Disc}(K)| \leq X$, this theorem shows there are only finitely many degrees to consider. The second component in the proof of Theorem 3.1 is to show that, for a given degree $n \geq 2$, there are only finitely many fields of that degree and discriminant at most X. This is the piece that Hermite resolved, but in fact, we will give a different and stronger proof of this result due to Schmidt.

Theorem 3.3 (Schmidt; 1995)**.** *For any integer $n \geq 2$, let $N_n(X) := \#\{K/\mathbb{Q} : [K : \mathbb{Q}] = n, |\mathrm{Disc}(K)| \leq X\}$. Then*

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

We will actually prove Schmidt's theorem first. The central ideas in the two proofs turn out to be similar, and most of the details in the proof of Theorem 3.3 turn out to be simpler. There are some "edge cases" involved in the proof that turn out to be more complicated, and we save those for the very end of these notes, but the main idea is relatively natural.

Date: February 2, 2022.

3.1. **Bounding fields by bounding minimal polynomials.** The key idea behind the proof of Theorem 3.3 is that every field of degree n is determined by some integer polynomial of degree n, and if we can understand how complicated that minimal polynomial can be in terms of the discriminant, we should be able to work our way to an understanding of how many number fields there could possibly be.

To carry this out, we first introduce two important definitions attached to elements of number fields that relate to their minimal polynomials.

Definition. Let K be a number field of degree n, and let $\sigma_1, \dots, \sigma_n$ denote the n embeddings of K. We define the *trace* $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)$ of an element $\alpha \in K$ by the sum of its embeddings, that is

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) := \sigma_1(\alpha) + \cdots + \sigma_n(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$

We define the *norm* $\mathrm{Nm}_{K/\mathbb{Q}}(\alpha)$ similarly by the product of its embeddings,

$$\mathrm{Nm}_{K/\mathbb{Q}}(\alpha) := \sigma_1(\alpha) \cdots \sigma_n(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha).$$

Since the n embeddings of $\alpha \in K$ are its n conjugates, the trace and norm can be related to the coefficients of its minimal polynomial, namely, the sub-leading and constant terms, respectively. These particular coefficients are special, however, in that each respect some of the arithmetic structure of K.

Lemma 3.4. *Let K be a number field of degree $n \geq 2$ and let $\alpha, \beta \in K$. Then:*

1. $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha + \beta) = \mathrm{Tr}_{K/\mathbb{Q}}(\alpha) + \mathrm{Tr}_{K/\mathbb{Q}}(\beta)$.
2. $\mathrm{Nm}_{K/\mathbb{Q}}(\alpha\beta) = \mathrm{Nm}_{K/\mathbb{Q}}(\alpha)\mathrm{Nm}_{K/\mathbb{Q}}(\beta)$.
3. $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha), \mathrm{Nm}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Q}$.
4. *If $\alpha \in \mathcal{O}_K$, then $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$ and $\mathrm{Nm}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$.*
5. *If $\alpha \in \mathbb{Q}$, then $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = n\alpha$ and $\mathrm{Nm}_{K/\mathbb{Q}}(\alpha) = \alpha^n$.*

Proof. 1) and 2) follow from the definitions and the fact that embeddings are field homomorphisms. To see 3), notice that the trace and norm a priori live in the splitting field $\widetilde{K}$, but are invariant under the action of Galois, and thus must live in $\mathbb{Q}$. 5) follows from noting that every embedding must preserve $\mathbb{Q}$.

For 4), if $\alpha \in \mathbb{O}_K$, then every embedding of α is an algebraic integer, and thus their sums and products must also be algebraic integers. By 3), the trace and norm are in $\mathbb{Q}$, so they must be integers. □

The trace will end up being more important in the proof of Theorem 3.3 and the norm more important in the proof of Theorem 3.2. In particular, we're going to approach Theorem 3.3 by finding the "smallest" element of $\mathcal{O}_K$ – but we have to exhibit some care here, since certainly $1 \in \mathcal{O}_K$ and 1 is not very large at all, nor is it useful for generating $\mathcal{O}_K$! Similarly, 2 is not very large or useful, nor is any integer. We therefore restrict our attention to a subset of $\mathcal{O}_K$ that excludes the integers.

Definition. The *trace 0 subspace* of $\mathcal{O}_K$, denoted $\mathcal{O}_K^0$ is the kernel of the trace map $\mathrm{Tr}_{K/\mathbb{Q}} \colon \mathcal{O}_K \to \mathbb{Z}$. That is,

$$\mathcal{O}_K^0 := \{\alpha \in \mathcal{O}_K : \mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = 0\}.$$

Since the trace of an integer $a \in \mathbb{Z}$ is na, it follows that $\mathcal{O}_K^0 \cap \mathbb{Z} = \{0\}$. In fact, more than this is true: in the Minkowski embedding, $\mathcal{O}_K^0$ and $\mathbb{Z}$ are nearly *orthogonal*.

INSERT PICTURE HERE

The important properties of $\mathcal{O}_K^0$ are summarized in the following lemma.

Lemma 3.5. *Let K be a number field of degree n with ring of integers $\mathcal{O}_K$ and trace 0 subspace $\mathcal{O}_K^0$.*

1. *The set $\mathcal{O}_K^0 \oplus \mathbb{Z}$ is an additive subgroup of $\mathcal{O}_K$ with index at most n.*
2. *$\mathcal{O}_K^0 \oplus \mathbb{Z}$ is a lattice in $\mathbb{R}^n$ with covolume at most $\frac{n}{2^{r_2}}\sqrt{|\mathrm{Disc}(K)|}$.*
3. *Under the Minkowski embedding, $\mathcal{O}_K^0$ is contained in a $n-1$ dimensional subspace $V_0^{r_1,r_2}$ of $\mathbb{R}^n$ that depends only on the signature (r_1, r_2) of K.*
4. *Inside the subspace $V_0^{r_1,r_2}$, $\mathcal{O}_K^0$ is a lattice with covolume at most $\sqrt{n|\mathrm{Disc}(K)|}$.*

Proof. 1) This follows from recognizing $\mathcal{O}_K^0 \oplus \mathbb{Z}$ as the kernel of the trace map $(\mathrm{mod}\, n)$, i.e. of the map $\mathcal{O}_K \xrightarrow{\mathrm{Tr}_{K/\mathbb{Q}}} \mathbb{Z} \xrightarrow{(\mathrm{mod}\, n)} \mathbb{Z}/n\mathbb{Z}$.

2) It follows from 1) that $\mathcal{O}_K^0 \oplus \mathbb{Z}$ is a sublattice of $\mathcal{O}_K$ inside $\mathbb{R}^n$. That means its fundamental parallelotope $\mathbb{R}^n/(\mathcal{O}_K^0 \oplus \mathbb{Z})$ is tiled by that of $\mathbb{R}^n/\mathcal{O}_K$, with $[\mathcal{O}_K : \mathcal{O}_K^0 \oplus \mathbb{Z}]$ tiles needed. Thus, the volume of this fundamental parallelope increases by a factor of the index, so the covolume of $\mathcal{O}_K^0 \oplus \mathbb{Z}$ is at most $n\sqrt{|\mathrm{Disc}(K)|}$.

3) Notice that the trace of $\alpha \in \mathcal{O}_K$ can be determined solely from its Minkowski embedding $\iota(\alpha)$. If K is totally real (i.e., it has signature $(n, 0)$), then, writing $\iota(\alpha) = (\alpha_1, \ldots, \alpha_n)$, the trace of α is simply $\alpha_1 + \cdots + \alpha_n$. Thus, we define in this case

$$V_0^{r_1,r_2} := \{(x_1, \ldots, x_n) \in \mathbb{R}^n : x_1 + \cdots + x_n = 0\}.$$

More generally, if K has signature (r_1, r_2), let $\sigma_1, \ldots, \sigma_{r_1}$ denote the real embeddings of K and let $\sigma_{r_1+1}, \ldots, \sigma_{r_1+r_2}$ denote a choice from each pair of complex embeddings. The Minkowksi embedding of $\alpha \in \mathcal{O}_K$ is then

$$\iota(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_{r_1}(\alpha), \Re(\sigma_{r_1+1}(\alpha)), \Im(\sigma_{r_1+1}(\alpha)), \ldots, \Re(\sigma_{r_1+r_2}(\alpha)), \Im(\sigma_{r_1+r_2}(\alpha)),$$

where $\Re$ and $\Im$ denote the real and imaginary parts of a complex number. Because the Minkowski embedding only uses one of each pair of complex embeddings, with the other differing only in the imaginary part, the trace of α is then

$$\sigma_1(\alpha) + \cdots + \sigma_{r_1}(\alpha) + 2\Re(\sigma_{r_1+1}(\alpha)) + \cdots + 2\Re(\sigma_{r_1+r_2}(\alpha)).$$

Thus, $\mathcal{O}_K^0$ lives in the subspace $V_0^{r_1,r_2}$ defined by

$$V_0^{r_1,r_2} := \{(x_1, \ldots, x_{r_1}, x_{r_1+1}, y_{r_1+1}, \ldots, x_{r_1+r_2}, y_{r_1+r_2}) \in \mathbb{R}^n : \\ x_1 + \ldots x_{r_1} + 2x_{r_1+1} + \cdots + 2x_{r_1+r_2} = 0\}.$$

4) If K is either totally real ($r_2 = 0$) or totally complex ($r_1 = 0$), the space $V_0^{r_1,r_2}$ is orthogonal to the image of $\mathbb{Z}$ under the Minkowski embedding. Thus, the covolume of $\mathcal{O}_K^0 \oplus \mathbb{Z}$ will be equal to the covolume of $\mathcal{O}_K^0$ inside $V_0^{r_1,r_2}$ times the length of $\iota(1)$. The length of $\iota(1)$ is $\sqrt{n}$ if K is totally real, and $\sqrt{r_2} = \sqrt{n/2}$ if K is totally complex. Combined with 2), this yields the claim in either of these two cases.

If K is neither totally real nor totally complex, we can still relate the covolumes of $\mathcal{O}_K^0$ and $\mathcal{O}_K^0 \oplus \mathbb{Z}$ by finding the length of the projection of $\iota(1) = (1, \ldots, 1, 1, 0, \ldots, 1, 0)$ onto

the direction of the normal vector $(1, \dots, 1, 2, 0, \dots, 2, 0)$. A little linear algebra reveals this length to be

$$\frac{n}{\sqrt{r_1 + 4r_2}} = \frac{n}{\sqrt{n + 2r_2}} \geq \sqrt{n/2}.$$

Thus, $\text{covol}(\mathcal{O}_K^0) \leq \sqrt{2/n} \cdot \text{covol}(\mathcal{O}_K^0 \oplus \mathbb{Z}) \leq \sqrt{n|\text{Disc}(K)|}$ by part 2). □

The reason we care about the covolume of $\mathcal{O}_K^0$ is that it will directly influence our ability to find "small" elements in $\mathcal{O}_K^0$. The next definition will make clear how we're measuring size.

Definition. The *height* of $\alpha \in \mathcal{O}_K$, written either $\text{ht}(\alpha)$ or $||\alpha||$, is defined to be

$$||\alpha|| := \max\{|\sigma_1(\alpha)|, \dots, |\sigma_n(\alpha)|\}.$$

The relevance of the height is provided by the following lemma.

Lemma 3.6. *Let K be a number field of degree n, and for $\alpha \in \mathcal{O}_K$, define*

$$f_\alpha(x) = \prod_{i=1}^{n} (x - \sigma_i(\alpha)).$$

Then $f \in \mathbb{Z}[x]$, and if we write $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$, then $|a_i| \leq \binom{n}{i} ||\alpha||^i$.

Proof. (Added later. Or, exercise!) □

Thus, our goal is to show that there is some $\alpha \in \mathcal{O}_K^0$ with small height. If we succeed, then its associated polynomial f_α will have reasonably small coefficients. Multiplying together the number of choices for each coefficient will ultimately yield Theorem 3.3.

Lemma 3.7. *There is an element $\alpha \in \mathcal{O}_K^0$ with $||\alpha|| \leq |\text{Disc}(K)|^{\frac{1}{2n-2}}$.*

Proof. Covolumes... □