Geometry of Numbers TCC 2024 Exercises

Updated June 11, 2024, corrections in red

Motivation

The motivation for these questions is explained in the summer project of Kate Thomas.

We are going to study, for a variable $t \in (0,1)$ and a parameter $N > 1$ which can be thought of as very large, the quantity

$$I(t,N) = \int_{\substack{\alpha \in \mathrm{Mat}_d^{\mathrm{Sym}}(\mathbb{R}) \\ \|\alpha\|<1}} \#\{A, B \in \mathrm{Mat}_{d\times d}(\mathbb{Z}) : \|A\| < N, \|tA\alpha - B\| < 1/N\}$$

$$= \sum_{A,B \in \mathrm{Mat}_{d\times d}(\mathbb{Z}):\|A\|<N} \mathrm{measure}\{\alpha \in \mathrm{Mat}_d^{\mathrm{Sym}}(\mathbb{R}) : \|\alpha\| < 1, \|tA\alpha - B\| < 1/N\},$$

but we'll work up to it by steps.

Notation

For an $m \times n$ real matrix M, we define the 2-norm $\|M\| = \sqrt{\sum M_{ij}^2}$.

Recall the Smith normal form of $A \in \mathrm{Mat}_{n\times n}(\mathbb{Z})$,

$$A = U^{-1} \,\mathrm{diag}(e_1, \ldots, e_d) V^{-1},$$

where $U, V \in \mathrm{SL}_n(\mathbb{Z})$ and $e_i \in \mathbb{N}$ with $e_1 \mid \cdots \mid e_n$.

We will use big-O/little-o and Vinogradov $\ll$ notation. You may want to use the "divisor bound"

$$\{d \in \mathbb{N} : d|m\} \ll_\varepsilon m^\varepsilon (m \in \mathbb{N}).$$

In general, in these questions, when you're asked for an upper bound it's always OK for it to be multiplied by $O_\varepsilon((\text{some variable})^\varepsilon)$.

Marking

Out of 100. You are strongly encouraged to collaborate with other students; if you take the course for credit you must write up your answers separately.

25% for sending me plausible strategies for two questions by the check-in deadline. (2 pages, clearly expressed, you can use more pages if you want.)

75% for submitting solutions to at least three questions (25 each, best three count). Many questions are open-ended or hard. **I will be looking only for a plausible strategy followed through to its logical conclusion, whether or not it successfully answers the question.** You are welcome to check with me if you're not sure. If between you all questions get answers, we should almost have a theorem!

Answer three questions. (Check-in: Show strategies for two.)

1. As a warm-up we'll count invertible matrices A with $\|A\| < N$, given values of $e_1, \dots, e_{n-1}$, and e_n in a given range. Note A invertible $\iff$ $e_n \neq 0$.

   (a) *5 marks.* Let $e \in \mathbb{N}$. Give an upper bound for the number of subgroups L of $(\mathbb{Z}/e\mathbb{Z})^n$ of the form

   $$L = L^{\bmod e}(v) = \{nv \mod e : 0 \leq n < e\} \qquad (v \in (\mathbb{Z}/e\mathbb{Z})^n).$$

   (Notice that two different v in $(\mathbb{Z}/e\mathbb{Z})^n$ may lead to the same subgroup $L^{\bmod e}(v)$.)

   (b) *5 marks.* Let $d < n$ and let $e_i \in \mathbb{N}$ with $e_1 \mid \cdots \mid e_d$. Give an upper bound for the number of subgroups of $(\mathbb{Z}/e_d\mathbb{Z})^n$ of the form

   $$L^{\bmod e_d}(e_1 v_1, \dots, e_d v_d) = \{n_1 e_1 v_1 + \dots + n_d e_d v_d \mod e_d : 0 \leq n_i < e_d/e_i\}$$
   $$(v_i \in (\mathbb{Z}/e_d e_i^{-1}\mathbb{Z})^n, \gcd(v_i, e_d/e_i) = 1).$$

   (c) *10 marks.* Let A be an $n \times n$ invertible real matrix with columns $a_1, \dots, a_n$. You are given that, possibly after permuting the columns of A,

   $$a_n = x_1 a_1 + \dots + x_{n-1} a_{n-1} + v$$
   $$(v_i, x_i \in \mathbb{R}, x_i \ll_n 1, \|v\| \ll \det(A)/\det(L(a_1, \dots, a_{n-1})), v \cdot a_i = 0).$$

   (This is proved using "singular value decomposition", which I will aim to discuss in lectures; it is a special case of the perhaps unenlightening Lemma 5.6 in this paper.)

   Recall that if $\lambda_n(\Lambda) < 1$, then $|\Lambda \cap B(0,1)| \ll_n 1/\det(\Lambda)$.

   Let $L \subseteq \mathbb{Z}^n$ be a rank n lattice and let $N, D > 1$. Show that the number of an $n \times n$ invertible matrices A, with $\|A\| < N$, $|\det A| \leq D$, and columns belonging to L, is

   $$\ll_n \frac{D}{\det L}(N^n/\det L)^{n-1}.$$

   (d) *5 marks.* Putting the last two parts together, give an upper bound for the number of invertible integer matrices A with $\|A\| < N$, given values of $e_1, \dots, e_{n-1}$, and e_n in a given range (i.e. $e_n \in [E, 2E]$ for some $E \geq 1$ which you can think of as large).

2. This is a continuation of question 1.

   (a) *5 marks.* Fix matrices A and B, and let $\det_k(A)$ be the largest $k \times k$ subdeterminant in the first k rows of A, that is

   $$\det_k(A) = \max\{|\det(A_{ij})_{1\le j\le k, i\in I}| : I \subset \{1,\dots,n\}, |I| = k\}.$$

   Show that

   $$\text{measure}\{\alpha \in \text{Mat}_d^{\text{Sym}}(\mathbb{R}) : \|tA\alpha - B\| < 1/N\} \ll_n (tN)^{-n(n+1)/2} |\det(A)|^{-1} \prod_{1\le k<n} \det_j(A)^{-1}.$$

   (b) *20 marks.* Now let A, a_i and L be as in part 1c again. Show that for $N, D, D_k > 1$, the number of an $n \times n$ invertible matrices A, with $\|A\| < N$, $|\det A| \le D$, columns belonging to L, and every $k \times k$ subdeterminant in the first k rows of A of size at most $O(D_k)$, is

   $$\ll_n \frac{D}{\det L} \prod_{k=1}^{n-1} \frac{N^{n-k} D_k}{\det(L)}.$$

3. The questions above give some way to count the number of A, and to estimate the volume of the α's. It remains to count the number of B. This will also reveal why we were concerned with the elementary divisors in question 1.

   To simplify the problem, we'll strengthen the condition $\|tA\alpha - B\| < 1/N$ to $tA\alpha = B$. Suppose A is an invertible $d \times d$ integer matrix. Define

   $$\Lambda_A = (A^{-1} \text{Mat}_{d\times d}(\mathbb{Z})) \cap \text{Mat}_d^{\text{Sym}}(\mathbb{R}).$$

   Observe that

   $$\#\{B \in \text{Mat}_{d\times d}(\mathbb{Z}) : \exists \alpha \in \text{Mat}_d^{\text{Sym}}(\mathbb{R}) : \|\alpha\| < 1, tA\alpha = B\} = |\Lambda_A \cap B(0,t)|.$$

   (There is a bijection by mapping B to $t\alpha = A^{-1}B \in \Lambda_A$, and mapping $\beta \in \Lambda_A$ to $A\beta = B$ with $\alpha = \beta/t$.)

   (a) *15 marks.* Suppose that $e_1 = \cdots = e_{d-1} = 1$, so that $e_d = \det(A)$. Show that

   $$A^{-1} \text{Mat}_{d\times d}(\mathbb{Z}) = L(E_{11}, \dots, E_{dd}, G)$$

   where $E_{11}, E_{12}, \dots, E_{dd}$ is a basis of $\text{Mat}_{d\times d}(\mathbb{Z})$, and $G_{ij} = V_{id}U_{dj}/\det(A)$. Here $U = (U_{ij}), V = (V_{ij})$ are the matrices from the Smith normal form of A. Hence give, in terms of A,

   i. an upper bound for the index $[\Lambda_A : \text{Mat}_d^{Sym}(\mathbb{Z})]$,
   ii. lower bounds for the Minkowski minima of Λ_A, and
   iii. upper bounds for $|\Lambda_A \cap B(0,t)|$, in terms of A.

(b) *10 marks.* Now we will drop the assumption that $e_1 = \cdots = e_{d-1} = 1$, so that e_i could be any natural numbers with $e_1 \mid \cdots \mid e_d$ and $e_1 \cdots e_d = \det(A)$. Give a set of generators for Λ_A. Hence give bounds (i)-(iii) as above.

4. This is a continuation of question 3.

   (a) *15 marks.* Let A be an invertible $d \times d$ integer matrix with $\|A\| < N$. Using the results of question 3, what upper bounds can you give for

   $$\{B \in \mathrm{Mat}_{d\times d}(\mathbb{Z}) : \exists \alpha \in \mathrm{Mat}_d^{\mathrm{Sym}}(\mathbb{R}) \text{ s.t. } \|tA\alpha - B\|_2 < 1/N\}?$$

   (b) *10 marks.* Let us think now about matrices in $A^{-1}\,\mathrm{Mat}_{d\times d}(\mathbb{Z})$ which are not symmetric, but which are close to a symmetric matrix.
   If there is $M \in A^{-1}\,\mathrm{Mat}_{d\times d}(\mathbb{Z})$ with $0 \neq \|M - M^T\| < \|A\|^{-1}N^{-1-\varepsilon}$, what does this say about A?
   Does it seem that for typical A there is likely to be such an M?
   Can you improve your bound in part (a)?

5. *25 marks.* Suppose that A has rank $r < n$, so A is an integer matrix with $\|A\| < N$, $\det(A) = 0$, and elementary divisors $e_1 \mid \ldots \mid e_r \neq 0$ and $e_{r+1} = \cdots = e_d = 0$. What upper bounds can you give for

   $$\{B \in \mathrm{Mat}_{d\times d}(\mathbb{Z}) : \exists \alpha \in \mathrm{Mat}_d^{\mathrm{Sym}}(\mathbb{R}) \text{ s.t. } \|tA\alpha - B\|_2 < 1/N\}?$$

Hints

1.

(a), (b) The motivation here is that later we will count $n \times n$ matrices A with given elementary divisors. To do this we will let L be the lattice generated by the columns of A, we see that L will be of the form $L \bmod e_n(e_1 v_1 + \ldots + e_n v_n)$, where the v_i are the columns of the matrix U^{-1} from the Smith normal form of A. We will count the number of possible L, then for each L we will count the number of possible A. The question is about $L \bmod e_d(e_1 v_1 + \ldots + e_d v_d)$ with $d \leq n$, suggesting maybe induction on d.

Part (a) is about the easiest case; do (a) first and then the same idea should work for part (b).

If you're stuck on (a): let e, L be fixed. How many v satisfy $L = L \bmod e(v)$? That is, how many v generate a given $L \bmod e$?

If you're still stuck on (a): Without loss of generality we can assume $\gcd(v, e) = 1$, since otherwise we can replace (e, v, L) by $(\frac{1}{\gcd(v,e)} e, \frac{1}{\gcd(v,e)} v, \frac{1}{\gcd(v,e)} L)$ and count the number of possibilities there instead.

(c) Actually it is true that, possibly after permuting the columns of A,

$$a_m = x_1 a_1 + \ldots + x_{m-1} a_{m-1} + v$$
$$(v_i, x_i \in \mathbb{R}, x_i \ll_n 1, \|v\| \ll \det(L(a_1, \ldots, a_m)) / \det(L(a_1, \ldots, a_{m-1})), v \cdot a_i = 0).$$

If you need to you can use this more general statement (my idea was that you don't need it, but maybe it's helpful). The point is that we can permute the a_i so that a_{i+1} is close to being in the span of $a_1, \ldots, a_i$.

Hint: the factor $(N^n / \det L)^{n-1}$ is the number of choice for the first $n-1$ columns and the factor $D / \det L$ is the number of choices we then have for the last column.

(d) Hint: $e_1 \cdots e_n = \det A$.

2. The key is to estimate the measure of some possible α_{ij}) first, then fix them and estimate the measure of some other α_{ij})s, and so on.

   Hint: part (b) looks like 1(c)...

3. Most $d \times d$ matrices have e_1, e_{d-1} quite small, so the condition $e_1 = \cdots = e_{d-1} = 1$ is just a simplification which shouldn't make a big difference most of the time.

   For example $e_1 = \gcd(A)$, and it would be unusual for all the elements of A to have a large common divisor. Similarly all the 2×2 subdeterminants of A are divisible by e_2, and so on.

   The big idea of this question:

$$\Lambda_A = \mathrm{Mat}_d^{\mathrm{Sym}}(\mathbb{R}) \cap A^{-1} \mathrm{Mat}_{d \times d}(\mathbb{Z}) \supseteq \mathrm{Mat}_d^{\mathrm{Sym}}(\mathbb{Z}),$$

so for example

$$\det(A)\Lambda_A \subseteq \mathrm{Mat}_{d\times d}(\mathbb{Z})$$

and

$$[\det(A)\Lambda_A : \det(A)\,\mathrm{Mat}_d^{\mathrm{Sym}}(\mathbb{Z})] = |\det(A)_A \mod \det(A)|.$$

In (b), 'give a set of generators' coudl mean doing an explicit computation of some kinds, or an induction on d, or working modulo e_1 then e_2 and so on, or working modulo e_d then e_{d-1} and so on...

4. (a) This might mean working with the minima $\lambda_i(L, F)$ with respect to a different norm, or doing a linear transformation on L so that we can use the Euclidean norm. You might use Q3 to get some relatively crude bounds for the Minkowski minima; this question isn't necessarily going to result in a bound that's very close to the truth.

   (b) In (a) just use the contruction in Q3 to bound some minima somehow. In (b), you might start to think about what size those minima should really have.