Geometry of Numbers TCC 2024 Exercises

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.

Marking

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!

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,

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

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

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 youre asked for an upper bound its always OK for it to be multiplied by $O_\varepsilon((\text{some variable})^\varepsilon)$.

1. As a warm-up well count invertible matrices A with $\|A\| < N$, given values of $e_1, \ldots, e_{n-1}$, and e_n in a given range.

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

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

   (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

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

(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,

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

(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.)

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

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

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 a $n \times n$ 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 $e_1, \ldots, e_{n-1}$, and e_n in a given range.

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

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

   Show that

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

(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 $\|A\| < N$, $|\det A| \leq D$, 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, well strengthen the condition $\|tA\alpha - B\| < 1/N$ to $tA\alpha = B$. Suppose A is an invertible $d \times d$ integer matrix. Define

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

Observe that

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

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

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

where $E_{11}, E_{12}, \ldots, E_{dd}$ is a basis of $\mathrm{Mat}_d^{\mathrm{Sym}}(\mathbb{Z})$, and $G_{ij} = V_{id}U_{dj}/\det(A)$. [...]

(a) [...]

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

where $G_{ij} = V_{id}U_{dj}/\det(A)$.Hence give, in terms of A,

i. an upper bound for the index $[\Lambda_A : \mathrm{Mat}_d^{Sym}(\mathbb{Z})]$,
ii. lower bounds for the Minkowski minima of Λ, 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 $A^{-1}\operatorname{Mat}_{d\times d}(\mathbb{Z})$ which are not symmetric, but which are close to a symmetric matrix.
If there is $M \in A^{-1}\operatorname{Mat}_{d\times d}(\mathbb{Z})$ with $\|M - M^T\| < \|A\|^{-1}N^{-1-\varepsilon}$, 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

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