A Minkowski-type result for linearly independent subsets of ideal lattices

Gergely Harcos

Alfréd Rényi Institute of Mathematics
http://www.renyi.hu/∼gharcos/

15 August 2019
First Analysis Mathematica International Conference

Setup and motivation

- k: totally real number field of degree d, embedded into $\mathbb{R}^d$
- Δ: discriminant of k
- $\mathfrak{o}$: ring of integers of k
- $\mathcal{B} := [-B_1, B_1] \times \cdots \times [-B_d, B_d]$

Setup and motivation

- k: totally real number field of degree d, embedded into $\mathbb{R}^d$
- Δ: discriminant of k
- $\mathfrak{o}$: ring of integers of k
- $\mathcal{B} := [-B_1, B_1] \times \cdots \times [-B_d, B_d]$

Question 1

Assume $\mathrm{vol}(\mathcal{B}) = \Delta^{3/2}$. *Is it true that* $|\mathfrak{o} \cap \mathcal{B}| \ll_d \Delta$*?*

Setup and motivation

- k: totally real number field of degree d, embedded into $\mathbb{R}^d$
- Δ: discriminant of k
- $\mathfrak{o}$: ring of integers of k
- $\mathcal{B} := [-B_1, B_1] \times \cdots \times [-B_d, B_d]$

Question 1

Assume $\mathrm{vol}(\mathcal{B}) = \Delta^{3/2}$. *Is it true that* $|\mathfrak{o} \cap \mathcal{B}| \ll_d \Delta$?

Theorem (Minkowski 1891, Blichfeldt 1921)

- $|\mathfrak{o} \cap \mathcal{B}| \gg_d \frac{\mathrm{vol}(\mathcal{B})}{\Delta^{1/2}}$
- $|\mathfrak{o} \cap \mathcal{B}| \ll_d \frac{\mathrm{vol}(\mathcal{B})}{\Delta^{1/2}}$ *if* $\mathfrak{o} \cap \mathcal{B}$ *contains* d *independent vectors.*

Setup and motivation

- k: totally real number field of degree d, embedded into $\mathbb{R}^d$
- Δ: discriminant of k
- $\mathfrak{o}$: ring of integers of k
- $\mathcal{B} := [-B_1, B_1] \times \cdots \times [-B_d, B_d]$

Question 1

Assume $\mathrm{vol}(\mathcal{B}) = \Delta^{3/2}$. *Is it true that* $|\mathfrak{o} \cap \mathcal{B}| \ll_d \Delta$*?*

Theorem (Minkowski 1891, Blichfeldt 1921)

- $|\mathfrak{o} \cap \mathcal{B}| \gg_d \frac{\mathrm{vol}(\mathcal{B})}{\Delta^{1/2}}$
- $|\mathfrak{o} \cap \mathcal{B}| \ll_d \frac{\mathrm{vol}(\mathcal{B})}{\Delta^{1/2}}$ *if* $\mathfrak{o} \cap \mathcal{B}$ *contains* d *independent vectors.*

Question 2

Assume $\mathrm{vol}(\mathcal{B}) = \Delta^{3/2}$. *Does* $\mathfrak{o} \cap \mathcal{B}$ *contain* d *independent vectors?*

Main result (crude version)

- k: totally real number field of degree d, embedded into $\mathbb{R}^d$
- Δ: discriminant of k
- $\mathfrak{o}$: ring of integers of k
- $\mathcal{B} := [-B_1, B_1] \times \cdots \times [-B_d, B_d]$

Theorem (Frączyk–Harcos–Maga 2019)

If $\mathfrak{o} \cap \mathcal{B}$ does not contain d independent vectors, then

$$\mathrm{vol}(\mathcal{B}) \ll_d \Delta, \qquad \textit{and in fact} \qquad |\mathfrak{o} \cap \mathcal{B}| \ll_d \Delta^{1/2}.$$

Main result (crude version)

- k: totally real number field of degree d, embedded into $\mathbb{R}^d$
- Δ: discriminant of k
- $\mathfrak{o}$: ring of integers of k
- $\mathcal{B} := [-B_1, B_1] \times \cdots \times [-B_d, B_d]$

Theorem (Frączyk–Harcos–Maga 2019)

If $\mathfrak{o} \cap \mathcal{B}$ does not contain d independent vectors, then

$$\mathrm{vol}(\mathcal{B}) \ll_d \Delta, \qquad \text{and in fact} \qquad |\mathfrak{o} \cap \mathcal{B}| \ll_d \Delta^{1/2}.$$

Remarks

1. The volume bound admits a quick proof by a deep topological result of McMullen (2005). We explain this in the next slide.
2. Our proof combines group theory, ramification theory, and the geometry of numbers. It works for all number fields and all nonzero ideals.

Deducing the volume bound from McMullen's result

1. McMullen (2005) proved that there is a box $\mathcal{C} = \prod_j [-C_j, C_j]$ such that $\mathrm{vol}(\mathcal{C}) \ll_d \Delta^{1/2}$ and $\mathfrak{o} \cap \mathcal{C}$ contains d independent vectors. Fix such a box $\mathcal{C}$.

Deducing the volume bound from McMullen's result

1. McMullen (2005) proved that there is a box $\mathcal{C} = \prod_j [-C_j, C_j]$ such that $\text{vol}(\mathcal{C}) \ll_d \Delta^{1/2}$ and $\mathfrak{o} \cap \mathcal{C}$ contains d independent vectors. Fix such a box $\mathcal{C}$.

2. Assume that $\mathcal{B} = \prod_j [-B_j, B_j]$ is an arbitrary box of sufficiently large volume: $\text{vol}(\mathcal{B}) / \text{vol}(\mathcal{C}) > 2^d \Delta^{1/2}$.

Deducing the volume bound from McMullen's result

1. McMullen (2005) proved that there is a box $\mathcal{C} = \prod_j [-C_j, C_j]$ such that $\mathrm{vol}(\mathcal{C}) \ll_d \Delta^{1/2}$ and $\mathfrak{o} \cap \mathcal{C}$ contains d independent vectors. Fix such a box $\mathcal{C}$.

2. Assume that $\mathcal{B} = \prod_j [-B_j, B_j]$ is an arbitrary box of sufficiently large volume: $\mathrm{vol}(\mathcal{B}) / \mathrm{vol}(\mathcal{C}) > 2^d \Delta^{1/2}$.

3. By Minkowski's theorem, the box $\prod_j [-B_j/C_j, B_j/C_j]$ contains a nonzero lattice point $x \in \mathfrak{o}$.

Deducing the volume bound from McMullen's result

1. McMullen (2005) proved that there is a box $\mathcal{C} = \prod_j [-C_j, C_j]$ such that $\mathrm{vol}(\mathcal{C}) \ll_d \Delta^{1/2}$ and $\mathfrak{o} \cap \mathcal{C}$ contains d independent vectors. Fix such a box $\mathcal{C}$.

2. Assume that $\mathcal{B} = \prod_j [-B_j, B_j]$ is an arbitrary box of sufficiently large volume: $\mathrm{vol}(\mathcal{B}) / \mathrm{vol}(\mathcal{C}) > 2^d \Delta^{1/2}$.

3. By Minkowski's theorem, the box $\prod_j [-B_j/C_j, B_j/C_j]$ contains a nonzero lattice point $x \in \mathfrak{o}$.

4. Clearly, $x(\mathfrak{o} \cap \mathcal{C}) \subset \mathfrak{o} \cap \mathcal{B}$ contains d independent vectors.

Deducing the volume bound from McMullen's result

1. McMullen (2005) proved that there is a box $\mathcal{C} = \prod_j [-C_j, C_j]$ such that $\operatorname{vol}(\mathcal{C}) \ll_d \Delta^{1/2}$ and $\mathfrak{o} \cap \mathcal{C}$ contains d independent vectors. Fix such a box $\mathcal{C}$.

2. Assume that $\mathcal{B} = \prod_j [-B_j, B_j]$ is an arbitrary box of sufficiently large volume: $\operatorname{vol}(\mathcal{B}) / \operatorname{vol}(\mathcal{C}) > 2^d \Delta^{1/2}$.

3. By Minkowski's theorem, the box $\prod_j [-B_j/C_j, B_j/C_j]$ contains a nonzero lattice point $x \in \mathfrak{o}$.

4. Clearly, $x(\mathfrak{o} \cap \mathcal{C}) \subset \mathfrak{o} \cap \mathcal{B}$ contains d independent vectors.

5. Hence if $\mathfrak{o} \cap \mathcal{B}$ does not contain d independent vectors, then

$$\operatorname{vol}(\mathcal{B}) \leqslant 2^d \Delta^{1/2} \operatorname{vol}(\mathcal{C}) \ll_d \Delta.$$

Sketching the proof of the main result (1 of 2)

1. Assume that $\mathfrak{o} \cap \mathcal{B}$ generates an m-dimensional sublattice Λ.

Sketching the proof of the main result (1 of 2)

1. Assume that $\mathfrak{o} \cap \mathcal{B}$ generates an m-dimensional sublattice Λ.

2. By the rank theorem in linear algebra, we can project Λ orthogonally onto a coordinate m-subspace such that the image is an m-dimensional lattice. By Blichfeldt's theorem,

$$|\mathfrak{o} \cap \mathcal{B}| \ll_d \frac{\mathrm{vol}(\mathrm{proj}\, \mathcal{B})}{\mathrm{covol}(\mathrm{proj}\, \Lambda)}.$$

Sketching the proof of the main result (1 of 2)

1. Assume that $\mathfrak{o} \cap \mathcal{B}$ generates an m-dimensional sublattice Λ.

2. By the rank theorem in linear algebra, we can project Λ orthogonally onto a coordinate m-subspace such that the image is an m-dimensional lattice. By Blichfeldt's theorem,

$$|\mathfrak{o} \cap \mathcal{B}| \ll_d \frac{\operatorname{vol}(\operatorname{proj} \mathcal{B})}{\operatorname{covol}(\operatorname{proj} \Lambda)}.$$

3. The Galois group G of the Galois closure of k acts on the admissible m-projections by permuting the coordinate axes. Taking the geometric mean over a G-orbit, we obtain

$$|\mathfrak{o} \cap \mathcal{B}| \ll_d \frac{\text{geometric mean of } \operatorname{vol}(\operatorname{proj} \mathcal{B})}{\text{geometric mean of } \operatorname{covol}(\operatorname{proj} \Lambda)}.$$

Sketching the proof of the main result (2 of 2)

4. Recall from the previous slide that

$$|\mathfrak{o} \cap \mathcal{B}| \ll_d \frac{\text{geometric mean of } \mathrm{vol}(\mathrm{proj}\,\mathcal{B})}{\text{geometric mean of } \mathrm{covol}(\mathrm{proj}\,\Lambda)}.$$

It is straightforward to show that

$$\text{numerator} \asymp_d \mathrm{vol}(\mathcal{B})^{\frac{m}{d}}.$$

Sketching the proof of the main result (2 of 2)

4. Recall from the previous slide that

$$|\mathfrak{o} \cap \mathcal{B}| \ll_d \frac{\text{geometric mean of } \mathrm{vol}(\mathrm{proj}\, \mathcal{B})}{\text{geometric mean of } \mathrm{covol}(\mathrm{proj}\, \Lambda)}.$$

It is straightforward to show that

$$\text{numerator} \asymp_d \mathrm{vol}(\mathcal{B})^{\frac{m}{d}}.$$

5. It is much harder to show that

$$\text{denominator} \gg_d \begin{cases} \Delta^{\max\left(0, \frac{m}{d} - \frac{1}{2}\right)} & \text{in general;} \\ \Delta^{\frac{m(m-1)}{2d(d-1)}} & \text{if } G \text{ is 2-homogeneous.} \end{cases}$$

Sketching the proof of the main result (2 of 2)

4. Recall from the previous slide that
$$|\mathfrak{o} \cap \mathcal{B}| \ll_d \frac{\text{geometric mean of } \mathrm{vol}(\mathrm{proj}\, \mathcal{B})}{\text{geometric mean of } \mathrm{covol}(\mathrm{proj}\, \Lambda)}.$$
It is straightforward to show that
$$\text{numerator} \asymp_d \mathrm{vol}(\mathcal{B})^{\frac{m}{d}}.$$

5. It is much harder to show that
$$\text{denominator} \gg_d \begin{cases} \Delta^{\max\left(0, \frac{m}{d} - \frac{1}{2}\right)} & \text{in general;} \\ \Delta^{\frac{m(m-1)}{2d(d-1)}} & \text{if } G \text{ is 2-homogeneous.} \end{cases}$$

6. Combining these bounds with Minkowski's theorem, we infer
$$\frac{\mathrm{vol}(\mathcal{B})}{\Delta^{\frac{1}{2}}} \ll_d |\mathfrak{o} \cap \mathcal{B}| \ll_d \mathrm{vol}(\mathcal{B})^{\frac{m}{d}} \begin{cases} \Delta^{\min\left(0, \frac{1}{2} - \frac{m}{d}\right)} & \text{in general;} \\ \Delta^{-\frac{m(m-1)}{2d(d-1)}} & \text{if } G \text{ is 2-homog.} \end{cases}$$

Main result (fine version)

- k: totally real number field of degree d, embedded into $\mathbb{R}^d$
- G: Galois group of Galois closure of k
- Δ: discriminant of k
- $\mathfrak{o}$: ring of integers of k
- $\mathcal{B} := [-B_1, B_1] \times \cdots \times [-B_d, B_d]$
- m: maximal number of independent vectors contained in $\mathfrak{o} \cap \mathcal{B}$

Theorem (Frączyk–Harcos–Maga 2019)

If $m < d$, then

$$\operatorname{vol}(\mathcal{B}) \ll_d \Delta^{\min\left(1, \frac{d}{2d-2m}\right)}, \quad \text{and in fact} \quad |\mathfrak{o} \cap \mathcal{B}| \ll_d \Delta^{\min\left(\frac{1}{2}, \frac{m}{2d-2m}\right)}.$$

Further, if $m < d$ and G is 2-homogeneous, then

$$\operatorname{vol}(\mathcal{B}) \ll_d \Delta^{\frac{d-1+m}{2d-2}}, \qquad \text{and in fact} \qquad |\mathfrak{o} \cap \mathcal{B}| \ll_d \Delta^{\frac{m}{2d-2}}.$$

Bounds for successive minima

- k: totally real number field of degree d, embedded into $\mathbb{R}^d$
- G: Galois group of Galois closure of k
- Δ: discriminant of k
- $\mathfrak{o}$: ring of integers of k
- $\lambda_1 \leqslant \cdots \leqslant \lambda_d$: successive minima of $\mathfrak{o}$

Corollary (Frączyk–Harcos–Maga 2019)

For all $m \in \{0, \ldots, d-1\}$ *we have*

$$\Delta^{\max\left(0,\frac{1}{d}-\frac{1}{2m+2}\right)} \ll_d \lambda_{m+1} \ll_d \Delta^{\min\left(\frac{1}{d},\frac{1}{2d-2m}\right)}.$$

If G *is* 2*-homogeneous, then for all* $m \in \{0, \ldots, d-1\}$ *we have*

$$\Delta^{\frac{m}{2d(d-1)}} \ll_d \lambda_{m+1} \ll_d \Delta^{\frac{d-1+m}{2d(d-1)}}.$$

Bounds for successive minima

- k: totally real number field of degree d, embedded into $\mathbb{R}^d$
- G: Galois group of Galois closure of k
- Δ: discriminant of k
- $\mathfrak{o}$: ring of integers of k
- $\lambda_1 \leqslant \cdots \leqslant \lambda_d$: successive minima of $\mathfrak{o}$

Corollary (Frączyk–Harcos–Maga 2019)

For all $m \in \{0, \ldots, d-1\}$ *we have*

$$\Delta^{\max\left(0, \frac{1}{d} - \frac{1}{2m+2}\right)} \ll_d \lambda_{m+1} \ll_d \Delta^{\min\left(\frac{1}{d}, \frac{1}{2d-2m}\right)}.$$

If G *is* 2*-homogeneous, then for all* $m \in \{0, \ldots, d-1\}$ *we have*

$$\Delta^{\frac{m}{2d(d-1)}} \ll_d \lambda_{m+1} \ll_d \Delta^{\frac{d-1+m}{2d(d-1)}}.$$

Interestingly, the upper bound for λ_d was established earlier by Bhargava–Shankar–Taniguchi–Thorne–Tsimerman–Zhao (2017).