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

Gergely Harcos

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

30 October 2019
Universität Leipzig
Felix Klein Colloquium

Setup and initial questions

- k: totally real number field of degree d, embedded into $\mathbb{R}^d$
- $\mathfrak{o}$: ring of integers of k
- Δ: discriminant 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?*

Motivation and work in progress (1 of 2)

Conjecture (following Sarnak–Xue 1991)

Let $\Gamma\backslash\mathcal{H}$ be a compact arithmetic hyperbolic surface of volume V. Let m be the multiplicity of some exceptional Laplace eigenvalue $1/4-\nu^2$ ($\nu>0$) occuring in $L^2(\Gamma\backslash\mathcal{H})$. Then $m \ll_\varepsilon V^{1-2\nu+\varepsilon}$.

Strategy (following Sarnak–Xue 1991)

Starting from ν, construct $f \in C_c(K\backslash G/K)$ such that

$$m \cdot V^{4\nu} \ll \operatorname{tr} R(f) \ll_\varepsilon V^{1+2\nu+\varepsilon}.$$

$$\begin{aligned}
\operatorname{tr} R(f) &= \sum_{\gamma\in\Gamma} \int_{\Gamma\backslash G} f(x^{-1}\gamma x)\,dx \\
&= \sum_{[\gamma]\subset\Gamma} \int_{\Gamma_\gamma\backslash G} f(x^{-1}\gamma x)\,dx \\
&= \sum_{[\gamma]\subset\Gamma} \operatorname{vol}(\Gamma_\gamma\backslash G_\gamma) \int_{G_\gamma\backslash G} f(x^{-1}\gamma x)\,dx.
\end{aligned}$$

Motivation and work in progress (2 of 2)

1. Let Γ be the unit group of a maximal order in an admissible quaternion algebra over k. The goal is to prove that
$$\sum_{[\gamma]\subset\Gamma} \mathrm{vol}(\Gamma_\gamma\backslash G_\gamma)\int_{G_\gamma\backslash G} f(x^{-1}\gamma x)\,dx \ll_{d,\varepsilon} V^{1+2\nu+\varepsilon}.$$

2. The units $\gamma = t + x\mathbf{i} + y\mathbf{j} + z\mathbf{k}$ have trace $2t \in \mathfrak{o}$ and norm $t^2 - ax^2 - by^2 + abz^2 = 1$, where $a \in k$ is positive in exactly one embedding $k \hookrightarrow \mathbb{R}$, while $b \in k$ is negative in every embedding $k \hookrightarrow \mathbb{R}$. Hence in fact $\mathrm{tr}(\gamma) \in \mathfrak{o} \cap \mathcal{B}$, where $\mathcal{B} = [-V, V] \times [-2,2]^{d-1}$ is a box of volume $\asymp_d V \asymp_d \Delta^{3/2}$.

3. We group the classes $[\gamma] \subset \Gamma$ according to $\mathrm{tr}(\gamma)$, and obtain:
$$\sum_{[\gamma]\subset\Gamma} \cdots \ll_{d,\varepsilon} \frac{V}{\Delta^{1/2}} \cdot \Delta^{1/2} V^{2\nu+\varepsilon}.$$

Main result (crude version)

- k: totally real number field of degree d, embedded into $\mathbb{R}^d$
- $\mathfrak{o}$: ring of integers of k
- Δ: discriminant 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

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

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

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

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

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

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
- $\mathfrak{o}$: ring of integers of k
- Δ: discriminant 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

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

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

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

Bounds for successive minima (1 of 2)

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

Theorem (Frączyk–Harcos–Maga 2019)

$$\lambda_1 \cdots \lambda_m \gg_d \begin{cases} \Delta^{\max\left(0, \frac{m}{d} - \frac{1}{2}\right)} & \textit{in general;} \\ \Delta^{\frac{m(m-1)}{2d(d-1)}} & \textit{if } G \textit{ is 2-homogeneous.} \end{cases}$$

$$\lambda_{m+1} \cdots \lambda_d \ll_d \begin{cases} \Delta^{\min\left(\frac{1}{2}, 1 - \frac{m}{d}\right)} & \textit{in general;} \\ \Delta^{\frac{(d-m)(d+m-1)}{2d(d-1)}} & \textit{if } G \textit{ is 2-homogeneous.} \end{cases}$$

Bounds for successive minima (2 of 2)

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

Corollary (Frączyk–Harcos–Maga 2019)

$$\Delta^{\max\left(0,\frac{1}{d}-\frac{1}{2m}\right)} \ll_d \lambda_m \ll_d \Delta^{\min\left(\frac{1}{2d-2m+2},\frac{1}{d}\right)} \quad \textit{in general;}$$

$$\Delta^{\frac{m-1}{2d(d-1)}} \ll_d \lambda_m \ll_d \Delta^{\frac{d+m-2}{2d(d-1)}} \quad \textit{if } G \textit{ is 2-homogeneous.}$$

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

The tame discriminant

- k: number field of degree d
- Σ: the set of embeddings $\sigma : k \hookrightarrow \overline{\mathbb{Q}}$
- G: Galois group of Galois closure of k
- $\mathfrak{o}$: ring of integers of k
- Δ, Δ_{tame}: discriminant of k, tame discriminant of k
- p, $\mathfrak{p}$: a prime number, and a prime ideal in $\mathfrak{o}$ dividing it
- $e_{\mathfrak{p}}$, $f_{\mathfrak{p}}$: ramification index of $k_{\mathfrak{p}}$, inertia degree of $k_{\mathfrak{p}}$

Definition

The *tame discriminant* of k is defined as

$$\Delta_{\mathrm{tame}} := \prod_{\mathfrak{p}} N_{k/\mathbb{Q}}(\mathfrak{p})^{e_{\mathfrak{p}}-1} = \prod_{p} p^{d-f_p} \quad \text{with} \quad f_p := \sum_{\mathfrak{p}|p} f_{\mathfrak{p}}.$$

Lemma

Δ_{tame} divides Δ, and the quotient is less than d^{d^3}.

The key divisibility result

- k: number field of degree d
- Σ: the set of embeddings $\sigma : k \hookrightarrow \overline{\mathbb{Q}}$
- G: Galois group of Galois closure of k
- $\mathfrak{o}$: ring of integers of k
- Δ_{tame}: tame discriminant of k

Theorem (Frączyk–Harcos–Maga 2019)

Let $m \in \{1, \dots, d\}$. For any m-subsets $X \subset \mathfrak{o}$ and $S \subset \Sigma$,

$$\prod_{g \in G} \det{}^2(\sigma(x))_{x \in X}^{\sigma \in gS} \quad \textit{is divisible by} \quad \Delta_{\mathrm{tame}}^{|G| \max\left(0, \frac{2m}{d} - 1\right)}.$$

The exponent of Δ_{tame} can be improved to $|G| \frac{m(m-1)}{d(d-1)}$ when G is 2-homogeneous.

Inertial equivalence

- k: number field of degree d
- Σ: the set of embeddings $\sigma : k \hookrightarrow \overline{\mathbb{Q}}$
- G: Galois group of Galois closure of k
- $\mathfrak{o}$: ring of integers of k
- p, $\mathfrak{p}$: a prime number, and a prime ideal in $\mathfrak{o}$ dividing it
- $e_\mathfrak{p}$, $f_\mathfrak{p}$: ramification index of $k_\mathfrak{p}$, inertia degree of $k_\mathfrak{p}$

Definition

Fix p, and think of Σ as the set of embeddings $\sigma : k \hookrightarrow \overline{\mathbb{Q}_p}$. For each $\sigma \in \Sigma$, there is a unique prime ideal $\mathfrak{p} \mid p$ and a unique $\mathbb{Q}_p$-linear embedding $\tilde{\sigma} : k_\mathfrak{p} \hookrightarrow \overline{\mathbb{Q}_p}$ that extends σ. Two elements $\sigma_1, \sigma_2 \in \Sigma$ are *inertially equivalent* if they belong to the same $\mathfrak{p}$, and $\tilde{\sigma}_1$ agrees with $\tilde{\sigma}_2$ on the maximal unramified subfield of $k_\mathfrak{p}$.

Lemma

The inertial equivalence classes can be labeled as $I_{\mathfrak{p},l}$, where $\mathfrak{p} \mid p$ and $l \in \{1, 2, \ldots, f_\mathfrak{p}\}$. Each class $I_{\mathfrak{p},l}$ has size $e_\mathfrak{p}$.

The central proposition

- k: number field of degree d
- Σ: the set of embeddings $\sigma : k \hookrightarrow \overline{\mathbb{Q}}$
- $\mathfrak{o}$: ring of integers of k
- p, $\mathfrak{p}$: a prime number, and a prime ideal in $\mathfrak{o}$ dividing it
- $e_{\mathfrak{p}}$, $f_{\mathfrak{p}}$: ramification index of $k_{\mathfrak{p}}$, inertia degree of $k_{\mathfrak{p}}$
- $I_{\mathfrak{p},l}$: inertial equivalence classes on Σ

Proposition (Frączyk–Harcos–Maga 2019)

Let $m \in \{1, \ldots, d\}$. For any m-subsets $X \subset \mathfrak{o}$ and $S \subset \Sigma$,

$$v_p\Big(\det{}^2(\sigma(x))_{x\in X}^{\sigma\in S}\Big) \geqslant \sum_{\mathfrak{p}|p} \frac{1}{e_{\mathfrak{p}}} \sum_{l=1}^{f_{\mathfrak{p}}} s_{\mathfrak{p},l}(s_{\mathfrak{p},l}-1),$$

where v_p is the unique additive valuation on $\overline{\mathbb{Q}_p}$ extending the usual additive valuation on $\mathbb{Q}_p$, and $s_{\mathfrak{p},l}$ abbreviates $|S \cap I_{\mathfrak{p},l}|$.

Central proposition implies key divisibility

$$v_p\Big(\det{}^2(\sigma(x))_{x\in X}^{\sigma\in gS}\Big) \geqslant \sum_{\mathfrak{p}|p} \frac{1}{e_{\mathfrak{p}}} \sum_{l=1}^{f_{\mathfrak{p}}} \sum_{\substack{\sigma,\sigma'\in I_{\mathfrak{p},l}\\ \sigma\neq\sigma'}} 1_{gS}(\sigma)1_{gS}(\sigma')$$

We average both sides over the Galois group G:

$$\frac{1}{|G|}\sum_{g\in G} 1_{gS}(\sigma)1_{gS}(\sigma') \geqslant \frac{1}{|G|}\sum_{g\in G}(1_{gS}(\sigma)+1_{gS}(\sigma')-1) = \frac{2m}{d}-1$$

$$\begin{aligned}\frac{1}{|G|}\sum_{g\in G} v_p\Big(\det{}^2(\sigma(x))_{x\in X}^{\sigma\in gS}\Big) &\geqslant \max\left(0,\frac{2m}{d}-1\right)\sum_{\mathfrak{p}|p} f_{\mathfrak{p}}(e_{\mathfrak{p}}-1)\\ &= \max\left(0,\frac{2m}{d}-1\right) v_p(\Delta_{\mathrm{tame}}).\end{aligned}$$

If G is 2-homogeneous, then we can improve the above by noting

$$\frac{1}{|G|}\sum_{g\in G} 1_{gS}(\sigma)1_{gS}(\sigma') = \frac{1}{|G|}\sum_{g\in G} 1_S(g^{-1}\sigma)1_S(g^{-1}\sigma') = \frac{m(m-1)}{d(d-1)}.$$

Proof of the central proposition (1 of 2)

- k: number field of degree d
- Σ: the set of embeddings $\sigma : k \hookrightarrow \overline{\mathbb{Q}}$
- $\tilde{K}$: extension of $\mathbb{Q}_p$ generated by the fields $\sigma(k)$ for $\sigma \in \Sigma$
- $\tilde{d}$: degree of $\tilde{K}$ over $\mathbb{Q}_p$
- $\tilde{\mathfrak{o}}$: ring of integers of $\tilde{K}$

1. $A := (\sigma(x))_{x \in X}^{\sigma \in S}$ decomposes into $s_{\mathfrak{p},l} \times m$ blocks $A_{\mathfrak{p},l}$
2. $\tilde{\mathfrak{o}}^m \xrightarrow{\sim} \prod_{\mathfrak{p}} \prod_l \tilde{\mathfrak{o}}^{s_{\mathfrak{p},l}}$ induces $A\tilde{\mathfrak{o}}^m \hookrightarrow \prod_{\mathfrak{p}} \prod_l A_{\mathfrak{p},l}\tilde{\mathfrak{o}}^m$
3. $v_p\big([\tilde{\mathfrak{o}}^m : A\tilde{\mathfrak{o}}^m]\big) \geqslant \sum_{\mathfrak{p}|p} \sum_{l=1}^{f_{\mathfrak{p}}} v_p\big([\tilde{\mathfrak{o}}^{s_{\mathfrak{p},l}} : A_{\mathfrak{p},l}\tilde{\mathfrak{o}}^m]\big)$.
4. LHS equals $\tilde{d} \cdot v_p(\det A)$, hence it suffices to show that

$$v_p\big([\tilde{\mathfrak{o}}^{s_{\mathfrak{p},l}} : A_{\mathfrak{p},l}\tilde{\mathfrak{o}}^m]\big) \geqslant \frac{\tilde{d}}{e_{\mathfrak{p}}} \binom{s_{\mathfrak{p},l}}{2}.$$

Proof of the central proposition (2 of 2)

Writing $t := s_{\mathfrak{p},l}$, we can list the entries of $A_{\mathfrak{p},l}$ as

$$A_{\mathfrak{p},l} = \begin{pmatrix} \sigma_1(x_1) & \cdots & \sigma_1(x_m) \\ \vdots & \ddots & \vdots \\ \sigma_t(x_1) & \cdots & \sigma_t(x_m) \end{pmatrix}.$$

Without loss of generality, we can assume that

$$v_{\mathfrak{p}}(x_1) \leqslant \cdots \leqslant v_{\mathfrak{p}}(x_m).$$

From here we use that

- the σ_i's are inertially equivalent, hence their $\mathbb{Q}_p$-linear extensions $\tilde{\sigma}_i$ are even linear over the maximal unramified subfield of $k_{\mathfrak{p}}$;
- $[\tilde{\mathfrak{o}}^t : A_{\mathfrak{p},l}\tilde{\mathfrak{o}}^m]$ remains unchanged if we multiply $A_{\mathfrak{p},l}$ by elements of $\mathrm{GL}_m(\tilde{\mathfrak{o}})$ on the right and by elements of $\mathrm{GL}_t(\tilde{\mathfrak{o}})$ on the left.