Positive semigroups in lattices and totally real number fields

Lenny Fukshansky
Claremont McKenna College
(joint work with Siki Wang)

JMM 2023, Boston, AMS Special Session on
Number Theory at Non-PhD Granting Institutions
January 4 - 7, 2023

Lattice monoid

Let $d \geq 2$ and $L \subset \mathbb{R}^d$ be a lattice of full rank, and let us write

$$\mathbb{R}^d_{\geq 0} = \left\{ \boldsymbol{x} \in \mathbb{R}^d : x_i \geq 0 \ \forall \ 1 \leq i \leq d \right\}$$

for the positive orthant of the Euclidean space $\mathbb{R}^d$ and $\mathbb{R}^d_{>0}$ for its interior. Define

$$L^+ = L \cap \mathbb{R}^d_{\geq 0},$$

then L^+ is an additive monoid in L.

Lattice monoid

Let $d \geq 2$ and $L \subset \mathbb{R}^d$ be a lattice of full rank, and let us write

$$\mathbb{R}^d_{\geq 0} = \left\{ \boldsymbol{x} \in \mathbb{R}^d : x_i \geq 0 \ \forall \ 1 \leq i \leq d \right\}$$

for the positive orthant of the Euclidean space $\mathbb{R}^d$ and $\mathbb{R}^d_{>0}$ for its interior. Define

$$L^+ = L \cap \mathbb{R}^d_{\geq 0},$$

then L^+ is an additive monoid in L.

Our goal is to study the geometry of this monoid L^+.

Lattice monoid

Let $d \geq 2$ and $L \subset \mathbb{R}^d$ be a lattice of full rank, and let us write

$$\mathbb{R}^d_{\geq 0} = \left\{ \boldsymbol{x} \in \mathbb{R}^d : x_i \geq 0 \ \forall \ 1 \leq i \leq d \right\}$$

for the positive orthant of the Euclidean space $\mathbb{R}^d$ and $\mathbb{R}^d_{>0}$ for its interior. Define

$$L^+ = L \cap \mathbb{R}^d_{\geq 0},$$

then L^+ is an additive monoid in L.

Our goal is to study the geometry of this monoid L^+.

Lemma 1

There exist infinitely many bases for L contained in L^+.

Positive basis

If $X = \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\}$ is a basis for L contained in L^+, which we refer to as a *positive basis* for L, we can write

$$\mathcal{X} = (\boldsymbol{x}_1 \ \ldots \boldsymbol{x}_d)$$

for the corresponding $d \times d$ positive basis matrix, so $L = \mathcal{X}\mathbb{Z}^d$.

Positive basis

If $X = \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\}$ is a basis for L contained in L^+, which we refer to as a *positive basis* for L, we can write

$$\mathcal{X} = (\boldsymbol{x}_1 \ \ldots \boldsymbol{x}_d)$$

for the corresponding $d \times d$ positive basis matrix, so $L = \mathcal{X}\mathbb{Z}^d$.

Define a submonoid of L^+

$$S(X) = \left\{ \sum_{i=1}^{n} a_i \boldsymbol{x}_i : a_1, \ldots, a_n \in \mathbb{Z}_{\geq 0} \right\} = \mathcal{X}\mathbb{Z}^d_{\geq 0},$$

as well as the positive cone spanned by X

$$\mathcal{C}(X) = \left\{ \sum_{i=1}^{n} a_i \boldsymbol{x}_i : a_1, \ldots, a_n \in \mathbb{R}_{\geq 0} \right\} = \mathcal{X}\mathbb{R}^d_{\geq 0}.$$

Gaps

Define the set of *gaps* of $S(X)$ in L^+ to be $G(X) := L^+ \setminus S(X)$.

Gaps

Define the set of *gaps* of $S(X)$ in L^+ to be $G(X) := L^+ \setminus S(X)$.

Lemma 2

Let $X = \{\mathbf{x}_1, \ldots, \mathbf{x}_d\}$ *be a positive basis for* L*, then*

$$L^+ \cap \mathcal{C}(X) = S(X), \text{ and so } G(X) = L^+ \setminus \mathcal{C}(X).$$

In particular, the set $G(X)$ *is infinite unless* X *is an orthogonal basis, in which case* $L^+ = S(X)$*.*

Gaps

Define the set of *gaps* of $S(X)$ in L^+ to be $G(X) := L^+ \setminus S(X)$.

Lemma 2

Let $X = \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_d\}$ be a positive basis for L, then

$$L^+ \cap \mathcal{C}(X) = S(X), \text{ and so } G(X) = L^+ \setminus \mathcal{C}(X).$$

In particular, the set $G(X)$ is infinite unless X is an orthogonal basis, in which case $L^+ = S(X)$.

From here on, assume that X is a positive non-orthogonal basis for L. Since $G(X)$ is infinite, we can define

$$G(X, t) = \{\boldsymbol{z} \in G(X) : \|\boldsymbol{z}\| \leq t\},$$

and ask for asymptotic behavior of $|G(X, t)|$ as $t \to \infty$.

Counting gaps

Proposition 3

Let $L \subset \mathbb{R}^d$ be a lattice of full rank and X a positive basis for L. Let $B_d(t)$ be a ball of radius $t > 0$ centered at the origin in $\mathbb{R}^d$ and write ω_d for the volume of a unit ball in $\mathbb{R}^d$. Let

$$\nu(X) = \frac{\mathrm{Vol}_d(\mathcal{C}(X) \cap B_d(1))}{\omega_d},$$

be the measure of the solid angle of the cone $\mathcal{C}(X)$. As $t \to \infty$,

$$|G(X,t)| = \left(\frac{\omega_d (1 - \nu(X) 2^d)}{2^d \det L} \right) t^d + O(t^{d-1}). \qquad (1)$$

Counting gaps

Proposition 3

Let $L \subset \mathbb{R}^d$ be a lattice of full rank and X a positive basis for L. Let $B_d(t)$ be a ball of radius $t > 0$ centered at the origin in $\mathbb{R}^d$ and write ω_d for the volume of a unit ball in $\mathbb{R}^d$. Let

$$\nu(X) = \frac{\mathrm{Vol}_d(\mathcal{C}(X) \cap B_d(1))}{\omega_d},$$

be the measure of the solid angle of the cone $\mathcal{C}(X)$. As $t \to \infty$,

$$|G(X,t)| = \left(\frac{\omega_d(1 - \nu(X)2^d)}{2^d \det L}\right) t^d + O(t^{d-1}). \tag{1}$$

Since $\mathcal{C}(X) \subsetneq \mathbb{R}^d_{\geq 0}$, the solid angle $\nu(X) < 1/2^d$, so the constant in the main term of (1) is positive.

Successive minima

Let

$$\mu(L) = \min\left\{t \in \mathbb{R}_{>0} : B_d(t) + L = \mathbb{R}^d\right\}$$

be the covering radius of L.

Successive minima

Let

$$\mu(L) = \min\left\{t \in \mathbb{R}_{>0} : B_d(t) + L = \mathbb{R}^d\right\}$$

be the covering radius of L.

For $t \in \mathbb{R}_{>0}$, let $C_d(t) = \left\{\boldsymbol{x} \in \mathbb{R}^d : |\boldsymbol{x}| \leq t\right\}$. We define three different sets of *successive minima* with respect to the cube $C_d(1)$.

Successive minima

Let

$$\mu(L) = \min\left\{t \in \mathbb{R}_{>0} : B_d(t) + L = \mathbb{R}^d\right\}$$

be the covering radius of L.

For $t \in \mathbb{R}_{>0}$, let $C_d(t) = \left\{\boldsymbol{x} \in \mathbb{R}^d : |\boldsymbol{x}| \leq t\right\}$. We define three different sets of *successive minima* with respect to the cube $C_d(1)$.

- $\lambda_i(L) = \min\left\{t \in \mathbb{R}_{>0} : \dim_{\mathbb{R}} \operatorname{span}_{\mathbb{R}}\left(L \cap C_d(t)\right) \geq i\right\}.$

Successive minima

Let

$$\mu(L) = \min \left\{ t \in \mathbb{R}_{>0} : B_d(t) + L = \mathbb{R}^d \right\}$$

be the covering radius of L.

For $t \in \mathbb{R}_{>0}$, let $C_d(t) = \left\{ \boldsymbol{x} \in \mathbb{R}^d : |\boldsymbol{x}| \leq t \right\}$. We define three different sets of *successive minima* with respect to the cube $C_d(1)$.

- $\lambda_i(L) = \min \{ t \in \mathbb{R}_{>0} : \dim_{\mathbb{R}} \operatorname{span}_{\mathbb{R}} (L \cap C_d(t)) \geq i \}$.
- $\lambda_i(L^+) := \min \{ t \in \mathbb{R}_{>0} : \dim_{\mathbb{R}} \operatorname{span}_{\mathbb{R}} (L^+ \cap C_d(t)) \geq i \}$.

Successive minima

Let

$$\mu(L) = \min\left\{t \in \mathbb{R}_{>0} : B_d(t) + L = \mathbb{R}^d\right\}$$

be the covering radius of L.

For $t \in \mathbb{R}_{>0}$, let $C_d(t) = \left\{\boldsymbol{x} \in \mathbb{R}^d : |\boldsymbol{x}| \leq t\right\}$. We define three different sets of *successive minima* with respect to the cube $C_d(1)$.

- $\lambda_i(L) = \min\left\{t \in \mathbb{R}_{>0} : \dim_{\mathbb{R}} \operatorname{span}_{\mathbb{R}}\left(L \cap C_d(t)\right) \geq i\right\}.$
- $\lambda_i(L^+) := \min\left\{t \in \mathbb{R}_{>0} : \dim_{\mathbb{R}} \operatorname{span}_{\mathbb{R}}\left(L^+ \cap C_d(t)\right) \geq i\right\}.$
- For a positive basis X of L,

$$\lambda_i(L^+, X) := \min\left\{t \in \mathbb{R}_{>0} : \dim_{\mathbb{R}} \operatorname{span}_{\mathbb{R}}\left(G(X) \cap C_d(t)\right) \geq i\right\}.$$

Successive minima

Let

$$\mu(L) = \min\left\{t \in \mathbb{R}_{>0} : B_d(t) + L = \mathbb{R}^d\right\}$$

be the covering radius of L.

For $t \in \mathbb{R}_{>0}$, let $C_d(t) = \left\{\boldsymbol{x} \in \mathbb{R}^d : |\boldsymbol{x}| \leq t\right\}$. We define three different sets of *successive minima* with respect to the cube $C_d(1)$.

- $\lambda_i(L) = \min\left\{t \in \mathbb{R}_{>0} : \dim_{\mathbb{R}} \operatorname{span}_{\mathbb{R}}\left(L \cap C_d(t)\right) \geq i\right\}.$
- $\lambda_i(L^+) := \min\left\{t \in \mathbb{R}_{>0} : \dim_{\mathbb{R}} \operatorname{span}_{\mathbb{R}}\left(L^+ \cap C_d(t)\right) \geq i\right\}.$
- For a positive basis X of L,

$$\lambda_i(L^+, X) := \min\left\{t \in \mathbb{R}_{>0} : \dim_{\mathbb{R}} \operatorname{span}_{\mathbb{R}}\left(G(X) \cap C_d(t)\right) \geq i\right\}.$$

We obtain bounds on these successive minima in the spirit of Minkowski.

Minkowski-type inequalities

First recall the classical inequalities of Minkowski and Jarnik:

$$\prod_{i=1}^{d} \lambda_i(L) \leq \det L, \;\; \mu(L) \leq \frac{\sqrt{d}}{2} \sum_{i=1}^{d} \lambda_i(L).$$

Minkowski-type inequalities

First recall the classical inequalities of Minkowski and Jarnik:

$$\prod_{i=1}^{d} \lambda_i(L) \leq \det L, \;\; \mu(L) \leq \frac{\sqrt{d}}{2} \sum_{i=1}^{d} \lambda_i(L).$$

Theorem 4

Let $L \subset \mathbb{R}^d$ be a lattice of full rank. Then

$$\lambda_1(L^+) \leq 2\mu(L) + 1, \;\; \lambda_i(L^+) \leq 2\lambda_i(L)(\mu(L)+1) \;\forall\; 2 \leq i \leq d.$$

Further, assume that no $d-1$ elements of X lie in a coordinate hyperplane, then $\lambda_d(L^+, X) \leq$

$$\max_{1\leq i\leq d} \max_{1\leq m\leq d} \left\{ \left(\max_{1\leq k\leq d} \left\lceil \frac{x_{ik}}{\sum_{j=1, j\neq i}^{d} x_{jk}} \right\rceil + 1 \right) \sum_{j=1, j\neq i}^{d} x_{jm} - x_{im} \right\}.$$

Application to totally real number fields

Let K be a totally real number field, $d = [K : \mathbb{Q}]$, and

$$\sigma_1, \dots, \sigma_d : K \to \mathbb{R}$$

be the embeddings of K. Let $\mathbb{N}_K$ be the field norm, Tr_K trace and Δ_K the discriminant of K. Let $\mathcal{O}_K$ be the ring of integers of K.

Application to totally real number fields

Let K be a totally real number field, $d = [K : \mathbb{Q}]$, and

$$\sigma_1, \dots, \sigma_d : K \to \mathbb{R}$$

be the embeddings of K. Let $\mathbb{N}_K$ be the field norm, Tr_K trace and Δ_K the discriminant of K. Let $\mathcal{O}_K$ be the ring of integers of K.

An ideal $I \subseteq \mathcal{O}_K$ can be viewed as a Euclidean lattice of rank d with respect to the symmetric bilinear form

$$\langle \alpha, \beta \rangle = \mathrm{Tr}_K(\alpha\beta) = \sum_{i=1}^{d} \sigma_i(\alpha)\sigma_i(\beta).$$

Let $I^+ = \{\alpha \in I : \sigma_i(\alpha) \geq 0 \ \forall\ 1 \leq i \leq d\}$, and let $\mathbb{Z}^+ = \mathbb{Z} \cap \mathcal{O}_K^+$. Then I has a $\mathbb{Z}$-basis contained in I^+. Let $\boldsymbol{\beta} = \{\beta_1, \dots, \beta_d\} \subset I^+$ be such a $\mathbb{Z}$-basis for I, which we call a positive basis.

Application to totally real number fields

Let

$$S(\beta) = \left\{ \sum_{i=1}^{d} c_i \beta_i : c_1, \ldots, c_d \in \mathbb{Z}^+ \right\} \subseteq I^+$$

be the corresponding sub-semigroup, and define the set of gaps of $S(\beta)$ in I^+ to be

$$G(\beta) = I^+ \setminus S(\beta).$$

The basis β cannot be orthogonal, hence $G(\beta)$ is infinite.

Application to totally real number fields

Let

$$S(\boldsymbol{\beta}) = \left\{ \sum_{i=1}^{d} c_i \beta_i : c_1, \dots, c_d \in \mathbb{Z}^+ \right\} \subseteq I^+$$

be the corresponding sub-semigroup, and define the set of gaps of $S(\boldsymbol{\beta})$ in I^+ to be

$$G(\boldsymbol{\beta}) = I^+ \setminus S(\boldsymbol{\beta}).$$

The basis $\boldsymbol{\beta}$ cannot be orthogonal, hence $G(\boldsymbol{\beta})$ is infinite.

We write h for the absolute Weil height: for every $\alpha \in K$,

$$h(\alpha) = \prod_{v \in M(K)} \max\{1, |\alpha|_v\}^{d_v/d},$$

where $M(K) =$ the set of all places of K, $d_v = [K_v : \mathbb{Q}_v]$ is the local degree of K at the place $v \in M(K)$. Notice that for each $v \mid \infty$, $d_v = 1$ since K is totally real.

Application to totally real number fields

Theorem 5

Let $I \subseteq \mathcal{O}_K$ be an ideal. Then there exist $\mathbb{Q}$-linearly independent elements $s_1, \dots, s_d \in I$ such that $\prod_{i=1}^{d} h(s_i) \leq \mathbb{N}_K(I)\sqrt{|\Delta_K|}$. Further, there exist $\mathbb{Q}$-linearly independent elements $\alpha_1, \dots, \alpha_d \in I^+$ such that

$$\prod_{i=1}^{d} h(\alpha_i) \leq \left(3d\sqrt{d}\right)^d \left(\mathbb{N}_K(I)\sqrt{|\Delta_K|}\right)^{d+1}.$$

Let $\boldsymbol{\beta} = \{\beta_1, \dots, \beta_d\} \subset I^+$ be a positive basis for I and $G(\boldsymbol{\beta})$ the corresponding set of gaps. For each $1 \leq i \leq d$, let $\beta_i' = \sum_{j=1, j\neq i}^{d} \beta_j$. Then there exist $\mathbb{Q}$-linearly independent gaps $\alpha_1, \dots, \alpha_d \in G(\boldsymbol{\beta})$ such that

$$h(\alpha_i) \leq \left(h(\beta_i/\beta_i')^d + 1\right) h(\beta_i')^d, \ \forall\ 1 \leq i \leq d.$$

Reference

L. Fukshansky, S. Wang, *Positive semigroups in lattices and totally real number fields*, Advances in Geometry, vol. 22 no. 4 (2022), pg. 503–512

Preprint is available at:

`http://math.cmc.edu/lenny/research.html`

Reference

L. Fukshansky, S. Wang, *Positive semigroups in lattices and totally real number fields*, Advances in Geometry, vol. 22 no. 4 (2022), pg. 503–512

Preprint is available at:

`http://math.cmc.edu/lenny/research.html`

Thank you!