SUCCESSIVE MINIMA AND LATTICE POINTS (AFTER HENK, GILLET AND SOULÉ)

S.BOUCKSOM

Abstract. The goal of this note is to present a remarkably simple proof, due to Henk, of a result previously obtained by Gillet-Soulé, relating the number of lattice points in a symmetric convex body to its successive minima.

Introduction

Let $\|\cdot\|$ be a norm on $\mathbb{R}^N$, and denote by B its closed unit ball (which can thus be any symmetric convex body). Let also

$$M(B) := \#\left(B \cap \mathbb{Z}^N\right)$$

be the number of lattice points in B. Recall that the *successive minima* of the lattice $\Lambda := \mathbb{Z}^N$ with respect to the norm $\|\cdot\|$ are defined as

$$r_i = r_i(\Lambda, B) = \inf\left\{r > 0 \mid \mathrm{rk}\,(rB \cap \Lambda) \geq i\right\}.$$

The main result we aim at is:

Theorem A. With the above notation we have

$$\frac{1}{N!} \leq M(B) \prod_{r_i<1} r_i \leq 6^N.$$

As we shall see, the lower bound is a straightforward consequence of a well-known variant, due to Van der Corput, of Minkowski's first theorem. The upper bound is basically [Hen02, Theorem 1.5].

A result of this kind is stated (in a less explicit way) in [GS91, Proposition 6]. Among other things, the proof provided there uses Minkowski's second theorem and the difficult Bourgain-Milman theorem.

We note that in the applications to the study of the arithmetic volume given in [BC11], only the coarser estimate

$$\log M(B) = \sum_{r_i<1} -\log r_i + O\left(N \log N\right)$$

is actually used.

Date: April 16, 2013.

1. Minkowski's first theorem

The following variant of Minkowski's first theorem is due to Van der Corput.

Proposition 1.1. *We have* $M(B) \geq 2^{-N}\operatorname{vol}(B)$.

Taking $\|\cdot\|$ to $(1+\varepsilon)$ times the ℓ^∞-norm shows that the constant 2^{-N} cannot be improved.

Lemma 1.2 (Blichtfeld's principle)**.** *Let $A \subset \mathbb{R}^N$ be a measurable set with finite volume. Then some translate of A contains at least $\lceil \operatorname{vol}(A) \rceil$ lattice points.*

Proof. Set $m := \lceil \operatorname{vol}(A) \rceil - 1$. Let P be a fundamental domain for Λ, so that $\operatorname{vol}(P) = 1$. For each $v \in \Lambda$ set

$$A_v := (A \cap (P+v)) - v,$$

and consider

$$f := \sum_{v\in\Lambda} \mathbf{1}_{A_v}.$$

Since each A_v is contained in P, we have

$$\sup_{x\in P} f(x) \geq \int_P f(x)dx = \sum_{v\in\Lambda} \operatorname{vol}(A_v)$$

$$= \sum_{v\in\mathbb{Z}^N} \operatorname{vol}\left(A \cap (P+v)\right) = \operatorname{vol}(A) > m.$$

It follows that there exists $x \in P$ belonging to at least $m+1$ A_v's, hence the result. □

Proof of Proposition 1.1. Set $m := \lceil 2^{-N}\operatorname{vol}(B) \rceil - 1$ and $A := 2^{-1}B$. Since $\operatorname{vol}(A) > m$, Lemma 1.2 shows that A contains $m+1$ distinct points $v_0, ..., v_m$ such that $v_i - v_j \in \Lambda$ for all i, j. It follows that $v_1 - v_0, ..., v_m - v_0$ are m distinct and non-zero lattice points in B, and we get as desired $M(B) \geq m+1$. □

2. Henk's theorem

The following result will immediately imply the upper bound in Theorem A.

Theorem 2.1. [Hen02, Theorem 1.5] *We have*

$$M(B) \leq 2^N \prod_{i=1}^N \left\lfloor 2r_i^{-1} + 1 \right\rfloor.$$

We start with two easy lemmas.

Lemma 2.2. *There exists a $\mathbb{Z}$-basis (e_i) of Λ such that*

$$\Lambda \cap r_i \mathring{B} \subset \mathbb{Z}e_1 + ... + \mathbb{Z}e_{i-1}$$

for each $i = 1, ..., N$.

We then say that (e_i) is an *adapted basis* of Λ (with respect to B).

Proof. By compactness, we may find linearly independent vectors $u_1, ..., u_N \in \Lambda$ such that $\|u_i\| = r_i$. It is then easy to check that

$$r_i = \min\left\{\|u\| \mid u \in \Lambda \setminus (\mathbb{R}u_1 + ... + \mathbb{R}u_{i-1})\right\}. \tag{2.1}$$

We then choose a $\mathbb{Z}$-basis $(e_1, ..., e_N)$ of Λ such that

$$u_i \in \mathbb{Z}e_1 + ... + \mathbb{Z}e_i,$$

and the result follows easily. □

Lemma 2.3. *Given a non-increasing sequence $a_1 \geq ... \geq a_N$ of positive integers, there exists positive integers $b_1, ..., b_N$ such that*

(i) $a_i \leq b_i < 2a_i$ *for all* i*;*
(iii) b_{i+1} *divides* b_i *for all* i*.*

Proof. Set $b_i := 2^{m_i} a_N$ with $m_i := \min\{m \in \mathbb{N} \mid 2^m a_N \geq a_i\}$. □

Proof of Theorem 2.1. For each i set

$$a_i = \left\lfloor 2r_i^{-1} \right\rfloor + 1,$$

so that a_i is the smallest positive integer with $2a_i^{-1} < r_i$. Pick $b_1, ..., b_N$ as in Lemma 2.3, let (e_i) be an adapted basis of Λ as in Lemma 2.2, and consider the sublattice of finite index

$$\Lambda' := \sum_i \mathbb{Z}b_i e_i.$$

We claim that $\Lambda' \cap 2B = \{0\}$. Indeed, let $u \in \Lambda'$ with $\|u\| \leq 2$, and write $u = \sum_i m_i b_i e_i$ with $m_i \in \mathbb{Z}$. If u is non zero, set

$$k := \max\{i \mid m_i \neq 0\}.$$

Since b_k divides $b_1, ..., b_{k-1}$, we then have $b_k^{-1} u \in \Lambda$, and

$$\left\|b_k^{-1} u\right\| \leq 2b_k^{-1} \leq 2a_k^{-1} < r_k.$$

By definition of an adapted basis, we should thus have $b_k^{-1} u \in \mathbb{Z}e_1 + ... + \mathbb{Z}e_{k-1}$, a contradiction.

As a consequence of the claim, the projection map $\pi : \mathbb{R}^N \to \mathbb{R}^N / \Lambda'$ is injective on B, so that $M(B) = \#\pi(B \cap \Lambda)$. But $\pi(B \cap \Lambda)$ is contained in Λ/Λ', and hence

$$M(B) = \#\pi(B \cap \Lambda) \leq [\Lambda : \Lambda'] = \prod_i b_i \leq 2^N \prod_i a_i.$$

□

3. Proof of Theorem A

Let $r_1 \leq ... \leq r_n < 1$, $1 \leq n \leq N$, be those successive minima that are less than 1. To prove the lower bound, pick linearly independent vectors $u_1, ..., u_n \in \Lambda$ such that $\|u_i\| = r_i$, and introduce the hypercube

$$P := \mathrm{Conv}\{\pm r_i^{-1} u_i \mid 1 \leq i \leq r\}$$

and the discrete abelian group $\Lambda' := \mathbb{Z}u_1 + ... + \mathbb{Z}u_n$. Since P is contained in B, we then have by Proposition 1.1

$$M(B) \ge \#(P \cap \Lambda') \ge 2^{-n} \operatorname{vol}_{\Lambda'}(P),$$

where $\operatorname{vol}_{\Lambda'}$ denotes the Haar measure on $\mathbb{R}u_1 + ... + \mathbb{R}u_n$ normalized by its lattice Λ'. Since

$$\operatorname{vol}_{\Lambda'}(P) = \frac{2^n}{n!} (r_1 \dots r_n)^{-1},$$

the lower bound in Theorem A follows.

We now turn to the upper bound. We have $\lfloor 2r_i^{-1} + 1 \rfloor \le 3r_i^{-1}$ for $i = 1, ..., n$, and $\lfloor 2r_i^{-1} + 1 \rfloor \le 3$ for $i > n$. We thus get

$$\prod_{i=1}^{N} \lfloor 2r_i^{-1} + 1 \rfloor \le 3^N \prod_{r_i < 1} r_i^{-1}$$

and the upper bound in Theorem A is now a consequence of Theorem 2.1.

4. Minkowski's second theorem

As a direct consequence of Theorem 2.1, we get the following version of Minkowski's second theorem:

$$\frac{2^N}{N!} \le \operatorname{vol}(B) \prod_{i=1}^{N} r_i \le 4^N. \tag{4.1}$$

Indeed, the upper bound follows directly from Theorem 2.1, replacing B with tB and letting $t \to +\infty$, using the obvious scaling property

$$r_i(\Lambda, tB) = t^{-1} r_i(\Lambda, B)$$

for $t > 0$. As to the lower bound, it is obtained as in the proof of Theorem A: the polytope P is contained in B, and hence

$$\operatorname{vol}(B) \ge \operatorname{vol}(P) = \frac{2^N}{N!} \left|\det\left(r_1^{-1} u_1, ..., r_N^{-1} u_N\right)\right|,$$

which yields the lower bound follows since $\det(u_1, ..., u_N)$ is a non-zero integer. For comparison, the classical statement of Minkowski's second theorem is as follows:

Theorem 4.1. *We have*

$$\frac{2^N}{N!} \le \operatorname{vol}(B) \prod_{i=1}^{N} r_i \le 2^N.$$

It thus improves on the upper bound in (4.1) by a factor 2^N. We now present Esterman's proof of Theorem 4.1, following [GL87, pp.58-61].

Proof of Theorem 4.1. We have already recalled the standard argument proving the lower bound. To get the upper bound, let $(e_1, ..., e_N)$ be an adapted basis of Λ as in Lemma 2.2, and set $\Lambda_0 := \{0\}$ and

$$\Lambda_i := \mathbb{Z}e_1 + ... + \mathbb{Z}e_i$$

for $i = 1, ..., N$. Let $\rho_i := V/\Lambda_{i-1} \to V/\Lambda_i$ and $\pi_i : V \to V/\Lambda_i$ be the natural projections, and for each measurable subset S of V let

$$v_i(S) := \mathrm{vol}_i\left(\pi_i(S)\right),$$

where vol_i denotes the normalized Haar measure on V/Λ_i.

By (2.1), if u is a lattice point such that $\|u\| < r_i$ then $u \in \Lambda_{i-1}$. It follows that ρ_i is injective on $\pi_{i-1}\left(\frac{r_i}{2}\mathring{B}\right)$, so that

$$v_i\left(\frac{r_i}{2}\mathring{B}\right) = v_{i-1}\left(\frac{r_i}{2}\mathring{B}\right)$$

for $i = 1, ..., N$, where we have set $v_0 := \mathrm{vol}$ and $r_0 := 1$. By Lemma 4.2 below this implies

$$v_i\left(\frac{r_i}{2}\mathring{B}\right) \geq \left(\frac{r_i}{r_{i-1}}\right)^{N-i+1} v_{i-1}\left(\frac{r_{i-1}}{2}\mathring{B}\right),$$

hence

$$1 \geq v_N\left(\frac{r_N}{2}\mathring{B}\right) \geq \prod_{i=1}^{N}\left(\frac{r_i}{r_{i-1}}\right)^{N-i+1} v_0\left(\frac{1}{2}\mathring{B}\right) = \frac{r_1 \dots r_N}{2^N}\,\mathrm{vol}(B)$$

which concludes the proof. □

Lemma 4.2. *Let $C \subset V$ be a convex subset. Then*

$$v_i(tC) \geq t^{N-i} v_i(C)$$

for all $t \geq 1$.

Proof. By translation invariance of the Haar measure on V/Λ_i, we may assume that $0 \in C$. If we let $V_i \subset V$ be the vector space generated by Λ_i, then each fiber F of $\tau_i : V/\Lambda_i \to V_i/\Lambda_i$ is canonically isomorphic to V/V_i, and $\mathrm{vol}(tC \cap F) = t^{N-i}\,\mathrm{vol}(C \cap F)$. Since tC contains C, we have on the other hand

$$\mathrm{vol}(\tau_i(tC)) \geq \mathrm{vol}(\tau_i(C)),$$

and the result follows by Fubini's theorem. □

References

[BHW93] U. Betke, M. Henk, J.M. Wills. *Successive-minima-type inequalities.* Discrete Comput. Geom. **9** (1993), 165 –175.

[BC11] S. Boucksom, H. Chen. *Okounkov bodies of filtered linear series.* Compos. Math. **147** (2011), no. 4, 1205–1229.

[GS91] H. Gillet, C. Soulé. *On the number of lattice points in convex symmetric bodies and their duals.* Israel J. Math. **74** (1991), no. 2-3, 347–357.

[GL87] P. M. Gruber, C. G. Lekkerkerker. *Geometry of numbers.* Second edition. North-Holland Mathematical Library, **37**. North-Holland Publishing Co., Amsterdam, 1987.

[Hen02] M. Henk. *Successive minima and lattice points.* IVth International Conference in "Stochastic Geometry, Convex Bodies, Empirical Measures and Applications to Engineering Science", Vol. I (Tropea, 2001). Rend. Circ. Mat. Palermo (2) Suppl. No. **70**, part I (2002), 377–384.

CNRS-Université Pierre et Marie Curie, Institut de Mathématiques de Jussieu, F-75251 Paris Cedex 05, France
E-mail address: boucksom@math.jussieu.fr