Lattice Points in Large Borel Sets and Successive Minima

Iskander Aliev and Peter M. Gruber

Abstract. Let B be a Borel set in $\mathbb{E}^d$ with volume $V(B) = \infty$. It is shown that almost all lattices L in $\mathbb{E}^d$ contain infinitely many pairwise disjoint d-tuples, that is sets of d linearly independent points in B. A consequence of this result is the following: let S be a star body in $\mathbb{E}^d$ with $V(S) = \infty$. Then for almost all lattices L in $\mathbb{E}^d$ the successive minima $\lambda_1(S, L), \dots, \lambda_d(S, L)$ of S with respect to L are 0. A corresponding result holds for most lattices in the Baire category sense. A tool for the latter result is the semi-continuity of the successive minima.

Key words. Borel sets, star bodies, lattices, successive minima, measure, Baire category, semicontinuity.

MSC 2000. 11H16, 11H50, 11J25.

1 Introduction and Statement of Results

A *lattice* L in Euclidean d-space $\mathbb{E}^d$ is the system of all integer linear combinations of d linearly independent vectors in $\mathbb{E}^d$. These vectors form a *basis* of L and the absolute value of their determinant is the *determinant* $d(L)$ of L. $d(L)$ is independent of the particular choice of a basis. To each lattice L we let correspond all $d \times d$ matrices the column vectors of which form a basis of L. Identify each such matrix with a point in $\mathbb{E}^{d^2}$. There is a Borel set $\mathfrak{F}$ in $\mathbb{E}^{d^2}$ consisting of such matrices, which has infinite Lebesgue measure and such that to each lattice L corresponds precisely one matrix in $\mathfrak{F}$. Thus there is a one-to-one correspondence between the space $\mathfrak{L}$ of all lattices in $\mathbb{E}^d$ and $\mathfrak{F}$. The Lebesgue measure on $\mathfrak{F}$ then yields a measure ν on $\mathfrak{L}$.

Results of Rogers [7] (for $d \geq 3$) and Schmidt [8] (for $d = 2$) show that for a Borel set B in $\mathbb{E}^d$ with Lebesgue measure $V(B) = \infty$, ν-almost all lattices L contain infinitely many primitive points in B, where a point $l \in L$ is *primitive* if it is different from the origin o and on the line-segment $[o, l]$ there are no points of L, except o and l. A refinement of this result is as follows.

Theorem 1. *Let B be a Borel set in $\mathbb{E}^d$ with $V(B) = \infty$. Then for ν-almost every lattice $L \in \mathfrak{L}$, the set B contains infinitely many, pairwise disjoint d-tuples of linearly independent primitive points of L.*

Tools for the proof are measure theoretic results of Rogers [7] and Schmidt [8] and a result of Yao and Yao [10] from applied computational geometry on dissection of sets in $\mathbb{E}^d$.

A *star body* S in $\mathbb{E}^d$ is a closed set with o in its interior such that each ray with endpoint o meets the boundary of S in at most one point. Equivalently,

$S = \{x : f(x) \leq 1\}$, where $f : \mathbb{E}^d \to \mathbb{R}$ is a *distance function*, i.e. it is non-negative, continuous and positively homogeneous of degree 1. The *successive minima* of S or f with respect to a lattice L are defined as follows:

$$\begin{aligned}\lambda_i(S, L) = \lambda_i(f, L)&\\ &= \inf\{\lambda > 0 : \lambda S \cap L \text{ contains } i \text{ linearly independent vectors}\}\\ &= \inf\{\max\{f(l_1), \dots, f(l_i)\} : l_1, \dots, l_i \in L \text{ linearly independent}\}\end{aligned}$$

for $i = 1, \dots, d$. Clearly,

$$0 \leq \lambda_1(S, L) \leq \cdots \leq \lambda_d(S, L) \leq \infty. \tag{1}$$

Successive minima play an important role in the geometry of numbers, algebraic number theory, Diophantine approximation and computational geometry, see e.g. [3, 2, 9, 5, 1]. For a surprising relation to Nevanlinna's value distribution theory see [4].

Let $\mathfrak{L}$ be endowed with its natural topology, see [3]. Then $\mathfrak{L}$ is locally compact by Mahler's compactness theorem. Thus a version of the Baire category theorem implies that $\mathfrak{L}$ is *Baire*. That is, any meager set has dense complement, where a set is *meager* or *of first Baire category*, it it is a countable union of nowhere dense sets, see [6].

Theorem 2. *Let S be a star body in $\mathbb{E}^d$ with $V(S) = \infty$. Then $\lambda_1(S, L) = \cdots = \lambda_d(S, L) = 0$ for*

(i) *ν-almost all lattices L in $\mathfrak{L}$ and for*

(ii) *all lattices L in $\mathfrak{L}$, with a meager set of exceptions.*

Tools for the proof are Theorem 1 and a semi-continuity result for successive minima which may be described as follows:

Let (S_n) be a sequence of star bodies and (f_n) the corresponding sequence of distance functions. Then (S_n) *converges* to a star body S with corresponding distance function f if the sequence (f_n) converges uniformly to f on the solid unit ball $\{x : \|x\| \leq 1\}$ of $\mathbb{E}^d$. A sequence (L_n) of lattices *converges* to a lattice L, if there are bases $\{b_{n1}, \dots, b_{nd}\}$ of L_n and $\{b_1, \dots, b_d\}$ of L such that $b_{n1} \to b_1, \dots, b_{nd} \to b_d$. This notion of convergence induces the topology on $\mathfrak{L}$.

Lemma. *Let (S_n) be a sequence of star bodies and (L_n) a sequence of lattices in $\mathbb{E}^d$, converging to a star body S and a lattice L, respectively. Then,*

(i) $\limsup_{n\to\infty} \lambda_i(S_n, L_n) \leq \lambda_i(S, L)$, *for $i = 1, \dots, d$, and*

(ii) *if S is bounded, then $\lim_{n\to\infty} \lambda_i(S_n, L_n)$ exists and is equal to $\lambda_i(S, L)$, for $i = 1, \dots, d$.*

To see that λ_i is *not* continuous, let S be a star body with $V(S) = \infty$ such that there is a lattice L which has only o in common with the interior of S, for example the star body $\{x : |x_1 \cdots x_d| \leq 1\}$, see [3], p. 28. Then $1 \leq \lambda_i(S, L) < \infty$, while by Theorem 2 there is a sequence (L_n) of lattices such that $L_n \to L$ with $\lambda_i(S, L_n) = 0$ for all n.

2 Proof of Theorem 1

A result of Yao and Yao [10] says that any mass distribution in $\mathbb{E}^d$ with positive, continuous density which tends rapidly to 0 as $\|x\| \to \infty$, and of total mass V, can be dissected into 2^d disjoint Borel parts, each of mass $2^{-d}V$ and such that no hyperplane meets all these 2^d masses. We need the following version of this result:

(2) Let $A \subset \mathbb{E}^d$ be a bounded Borel set with volume $V(A) > V > 0$. Then A contains 2^d pairwise disjoint Borel subsets, each of volume $2^{-d}V$ and such that no $(d-1)$-dimensional subspace of $\mathbb{E}^d$ meets each of these 2^d sets.

To see (2), choose a compact set $C \subset A$ with $V(C) > V$. This is possible by the inner regularity of Lebesgue measure. Next, choose a continuous function $g : \mathbb{E}^d \to \mathbb{R}^+$ such that

$$g \geq \chi_C, \int\limits_{\mathbb{E}^d} (g - \chi_C)\, dx < 2^{-d}(V(C) - V),\ g(x) \to 0 \text{ rapidly as } \|x\| \to \infty,$$

where χ_C is the characteristic function of C. This is possible by the outer regularity of Lebesgue measure and Urysohn's lemma. Let $F_i, i = 1, \ldots, 2^d$, be a dissection of $\mathbb{E}^d$ for the density g as described by Yao and Yao such that

$$\int\limits_{F_i} g\, dx = 2^{-d} \int\limits_{\mathbb{E}^d} g\, dx \geq 2^{-d}V(C).$$

Then there is no $(d-1)$-dimensional subspace of $\mathbb{E}^d$ which meets each of the sets $C \cap F_i$, and for the respective volumes of these sets we have the following estimate:

$$\begin{aligned} V(C \cap F_i) &= \int\limits_{F_i} \chi_C dx = \int\limits_{F_i} g\, dx - \int\limits_{F_i} (g - \chi_C)\, dx \geq \int\limits_{F_i} g\, dx - \int\limits_{\mathbb{E}^d} (g - \chi_C)\, dx \\ &> 2^{-d}V(C) - 2^{-d}(V(C) - V) = 2^{-d}V. \end{aligned}$$

This concludes the proof of (2).

For the proof of Theorem 2 assume first that $d \geq 3$. The following result is an immediate consequence of a result of Rogers [7], p. 286:

(3) Let $k = 1, 2, \ldots$, and A a Borel set in $\mathbb{E}^d$ with $0 < V(A) < \infty$. Then the function $\#^*(A \cap \cdot\,) : \mathfrak{L} \to \{0, 1, \ldots\}$, which counts the number of primitive points of L in A, is Borel measurable and

$$\int\limits_{\mathfrak{L}(k)} \Big(\#^*(A \cap L) - \frac{V(A)}{\zeta(d)}\Big)^2 d\nu(L) \leq \alpha V(A).$$

Here $\mathfrak{L}(k) = \{L \in \mathfrak{L} : d(L) \leq k\}$, $\zeta(\cdot)$ denotes the Riemann zeta-function, and $\alpha > 0$ is a constant depending on k and d.

The main step of the proof is to show the following proposition:

(4) Let $k = 1, 2, \ldots$ Then for ν-almost every lattice $L \in \mathfrak{L}(k)$ the set B contains infinitely many pairwise disjoint d-tuples of linearly independent points of L.

To prove this, let $0 = \varrho_0 < \varrho_1 < \ldots$ be such that

$$V(B_n) > 2^d \zeta(d) n, \text{ where } B_n = \{x \in B : \varrho_{n-1} < \|x\| \leq \varrho_n\}.$$

By (2),

(5) for $n = 1, 2, \ldots$, there are 2^d pairwise disjoint Borel sets $B_{ni}, i = 1, \ldots, 2^d$, of B_n such that $V(B_{ni}) = \zeta(d)n$ and no $(d-1)$-dimensional subspaces of $\mathbb{E}^d$ meets each set B_{ni}.

Consequently (3) implies that

(6) $$\int\limits_{\mathfrak{L}(k)} (\#^*(B_{ni} \cap L) - n)^2 d\nu(L) \leq \alpha\, \zeta(d) n.$$

By (5) and (3) the sets $\mathfrak{L}_{ni} = \{L \in \mathfrak{L}(k) : \#^*(B_{ni} \cap L) = 0\}$, $i = 1, \ldots, 2^d$, are Borel. It thus follows from (6) that $n^2 \nu(\mathfrak{L}_{ni}) \leq \alpha\, \zeta(d) n$, or

(7) $$\nu(\mathfrak{L}_{ni}) \leq \frac{\alpha\, \zeta(d)}{n}.$$

The set $\mathfrak{L}_n = \mathfrak{L}_{n1} \cup \cdots \cup \mathfrak{L}_{n2^d}$ is Borel and consists of all lattices $L \in \mathfrak{L}(k)$ such that at least one of the sets B_{ni} contains no primitive point of L. Hence $\mathfrak{L}(k) \backslash \mathfrak{L}_n$ is the set of all lattices $L \in \mathfrak{L}(k)$ such that each set B_{ni} contains a primitive point of L. Hence (5) shows that

(8) for any lattice $L \in \mathfrak{L}(k) \backslash \mathfrak{L}_n$, the set B_n contains a d-tuple of linearly independent points of L.

By (7),

(9) $$\nu(\mathfrak{L}_n) \leq \frac{\alpha\, 2^d \zeta(d)}{n}.$$

By definition the sets B_n are pairwise disjoint subsets of B. Hence (8) implies that

$$\begin{aligned}
&\{L \in \mathfrak{L}(k) : && B \text{ contains infinitely many pairwise disjoint } d\text{-tuples} \\
& && \text{of linearly independent primitive points of } L\} \\
&\supset \{L \in \mathfrak{L}(k) : && \text{for infinitely many } n, \text{ the set } B_n \text{ contains a } d\text{-tuple} \\
& && \text{of linearly independent primitive points of } L\} \\
&\supset \{L \in \mathfrak{L}(k) : && \text{for infinitely many } n \text{ the lattice } L \text{ is not contained in } \mathfrak{L}_n\} \\
&= \bigcap_{m=1}^{\infty} \bigcup_{n=m}^{\infty} (\mathfrak{L}(k) \backslash \mathfrak{L}_n) = \mathfrak{L}(k) \backslash \bigcup_{m=1}^{\infty} \bigcap_{n=m}^{\infty} \mathfrak{L}_n. &&
\end{aligned}$$

Since by (9),

$$\nu\Big(\bigcap_{n=m}^{\infty}\mathfrak{L}_n\Big)=0 \text{ for } m=1,2,\dots, \text{ and thus } \nu\Big(\bigcup_{m=1}^{\infty}\bigcap_{n=m}^{\infty}\mathfrak{L}_n\Big)=0,$$

the proof of (4) is complete.

Since $\mathfrak{L}=\bigcup\mathfrak{L}(k)$, Theorem 1 for $d\geq 3$ is an immediate consequence of (4).

Assume now that $d=2$ and let ξ be the measure on $\mathfrak{L}$ used by Schmidt [8], p. 525. A result of Schmidt [8], p. 526/7, shows that (3) continues to hold, but with the following weaker inequality:

$$\int\limits_{\mathfrak{L}(k)}\Big(\#^*(A\cap L)-\frac{V(A)}{\zeta(2)}\Big)^2 d\xi(L)\leq \beta\, V(A)\log_2 V(A).$$

Using this, we see that in the case $d=2$ the proof is, in essence, the same as the above proof for $d\geq 3$. Finally, note that the sets of measure 0 with respect to ξ and ν coincide.□

3 Proof of the Lemma

Let f_n and f be the distance functions of S_n and S, respectively. Since distance functions are positively homogeneous of degree 1, and $f_n\to f$ uniformly for $\|x\|\leq 1$, we have that $f_n\to f$ uniformly on each bounded set in $\mathbb{E}^d$. This yields the following statement:

(10) Let $l_n, l\in\mathbb{E}^d$ be such that $l_n\to l$. Then $f_n(l_n)\to f(l)$.

The following claims are simple consequences of the convergence $L_n\to L$, see [3], p. 178/9:

(11) Given $l\in L$, there are $l_n\in L$ such that $l_n\to l$.

(12) If $l_n\in L_n$ and $l\in\mathbb{E}^d$ such that $l_n\to l$, then $l\in L$.

(i): Let $\varepsilon>0$. By the definition of successive minima one can show that there are linearly independent lattice points $l_1,\dots,l_d\in L$ such that

(13) $\max\{f(l_1,\dots,f(l_i)\}\leq\lambda_i(S,L)+\varepsilon.$

By (11) we may choose points $l_{nj}\in L_n, j=1,\dots,d$, such that

(14) $l_{nj}\to l_j.$

Since $l_1,\dots,l_d$ are linearly independent, it follows that

(15) $l_{n1},\dots,l_{nd}\in L_n$ are also linearly independent for all sufficiently large n.

Hence, by the definition of λ_i together with (15), (14), (10), and (13) we obtain that

$$\begin{aligned}\lambda_i(f_n, L_n) &\leq \max\{f_n(l_{n1}), \dots, f_n(l_{ni})\} \leq \max\{f(l_1, \dots, f(l_{ni})\} + \varepsilon \\ &\leq \lambda_i(f, L) + 2\varepsilon \text{ for all sufficiently large } n,\end{aligned}$$

Since $\varepsilon > 0$ was arbitrary, this concludes the proof of claim (i).

(ii): Let $0 < \varepsilon < 1$. Since $f_n \to f$ uniformly on $\{x : \|x\| = 1\}$ and $f(x) > 0$ for $\|x\| = 1$ by the boundedness of S, and f_n, f all are continuous and positively homogeneous of degree 1, there is a constant $\alpha > 0$ such that

(16) $\quad \alpha\|x\| \leq (1-\varepsilon)f(x) \leq f_n(x)$ for all $x \in \mathbb{E}^d$ if n is sufficiently large.

For such n we have that $f(x) > 0$ for $x \neq o$, hence S_n is bounded. The definition of λ_i then yields that

(17) $\quad$ for all sufficiently large n, there are linearly independent points $l_{n1}, \dots, l_{nd}$ in L_n, such that $\lambda_i(f_n, L_n) = \max\{f_n(l_{n1}), \dots, f_n(l_{ni})\}$ for $i = 1, \dots, d$.

(16), (17), (1) and (i) together imply that

(18) $$\begin{aligned}\|l_{ni}\| &\leq \frac{1}{\alpha} f_n(l_{ni}) \leq \frac{1}{\alpha}\lambda_i(f_n, L_n) \leq \frac{1}{\alpha}\lambda_d(f_n, L_n) \\ &\leq \frac{1}{\alpha}\lambda_d(f, L) + \varepsilon \text{ for all sufficiently large } n.\end{aligned}$$

For all sufficiently large n, the vectors $l_{n1}, \dots, l_{nd}$ are linearly independent by (17). Consequently, $|\det(l_{n1}, \dots, l_{nd})|$ is an integer multiple of $d(L)$. By assumption, $L_n \to L$. Hence $d(L_n) \to d(L)$. Combining this, it follows that

(19) $\quad |\det(l_{n1}, \dots, l_{nd})| \geq d(L_n) \geq (1-\varepsilon)\, d(L)$ for all sufficiently large n.

By (18), all the sequences $(l_{n1}), \dots, (l_{nd})$ are bounded. Fix an index $i = 1, \dots, d$. By considering a suitable subsequence of $1, 2, \dots,$ and re-numbering, if necessary, we may suppose that

(20) $\quad \liminf_{n \to \infty} \lambda_i(f_n, L_n)$ is the same as for the original sequence,

and $l_{n1} \to l_1, \dots, l_{nd} \to l_d$, say. By (10), (12) and (19) the latter implies that

$$\begin{aligned}&f_n(l_{n1}) \to f(l_1), \dots, f_n(l_{nd}) \to f(l_d), l_1, \dots, l_d \in L, \\ &|\det(l_1, \dots, l_d)| \geq (1-\varepsilon)\, d(L) > 0.\end{aligned}$$

In particular, $l_1, \dots, l_d$ are linearly independent. Using (17) and the definition of λ_i, it follows that

$$\lambda_i(f_n, L_n) = \max\{(f_n(l_{n1}), \dots, f_n(l_{ni})\} \to \max\{f(l_1), \dots, f(l_i)\} \geq \lambda_i(f, L).$$

This together with (20) and (i) finally yields (ii).□

4 Proof of Theorem 2

(i): Apply Theorem 1 with $B = \frac{1}{k}S, k = 1, 2, \ldots$, to see that for ν-almost all lattices εS contains a d-tuple of linearly independent primitive points of L for any $\varepsilon > 0$. Hence $\lambda_d(S, L) = 0$ for ν-almost all lattices L. In conjunction with (1), this completes the proof of claim (i).

(ii): Let $\mathcal{M}_n = \{L \in \mathcal{L} : \lambda_d(S, L) \geq \frac{1}{n}\}, n = 1, 2, \ldots$ Since $\lambda_d(S, \cdot)$ is upper semi-continuous by the Lemma, $\mathcal{M}_n$ is closed. If the interior of $\mathcal{M}_n$ is non-empty, then $\nu(\mathcal{M}_n) > 0$ by the definitions of ν and the topology on $\mathcal{L}$, in contradiction to (i). Hence $\mathcal{M}_n$ has empty interior. Being closed, $\mathcal{M}_n$ is nowhere dense in $\mathcal{L}$. Hence

$$\bigcup_{n=1}^{\infty} \mathcal{M}_n = \{L \in \mathcal{L} : \lambda_d(S, L) > 0\} \text{ is meager.}$$

Now note (1) to conclude the proof of claim (ii).□

5 Acknowledgement

For their helpful hints we are obliged to Professors Groemer and Welzl and the referees. Emo Welzl, in particular, pointed out to us the existence of the article of Yao and Yao which is reviewed neither in the Mathematical Reviews nor in the Zentralblatt. The first author was supported by the Austrian Science Fund (FWF), project M821-N12.

References

[1] Blömer, J., Closest vectors, successive minima, and dual HKZ-bases of lattices, in: Automata, languages and programming (Geneva 2000) 248–259, Lect. Notes Comput. Sci. **1853**, Springer–Verlag, Berlin 2000

[2] Gruber, P.M., Geometry of numbers, in: Handbook of convex geometry **B** 739–763, North–Holland, Amsterdam 1993

[3] Gruber, P.M., Lekkerkerker, C.G., Geometry of numbers, 2nd ed., North–Holland, Amsterdam 1987

[4] Hyuga, T., An example of analogy of Nevanlinna theory and Diophantine approximation, in: Proc. Second ISAAC Congress **1** (Fukuoka 1999) 459–465, Kluwer, Dordrecht 2000

[5] Lagarias, J.C., Point lattices, in: Handbook of combinatorics **1** 919–966, Elsevier, Amsterdam 1995

[6] Oxtoby, J.C., Measure and category, 2nd ed., Springer–Verlag, New York 1980

[7] Rogers, C.A., Mean values over the space of lattices, Acta Math. **94** (1955) 249–287

[8] Schmidt, W.M., A metrical theorem in geometry of numbers, Trans. Amer. Math. Soc. **95** (1960) 516–529

[9] Schmidt, W.M., Diophantine approximation, Lect. Notes Math. **785**, Springer–Verlag, Berlin 1980

[10] Yao, A.C., Yao, F.F., A general approach to d-dimensional geometric queries, in: Proc. 17th ACM Symp. Theory of Computations (1985) 163–169

Iskander Aliev
School of Mathematics
University of Edinburgh
James Clerk Maxwell Building,
King's Buildings
Mayfield Road,
Edinburgh EH9 3JZ, UK
I.Aliev@ed.ac.uk
Peter M. Gruber
Forschungsgruppe
Konvexe und Diskrete Geometrie
Technische Universität Wien
Wiedner Hauptstraße 8–10/1046
A–1040 Vienna, Austria
peter.gruber@tuwien.ac.at