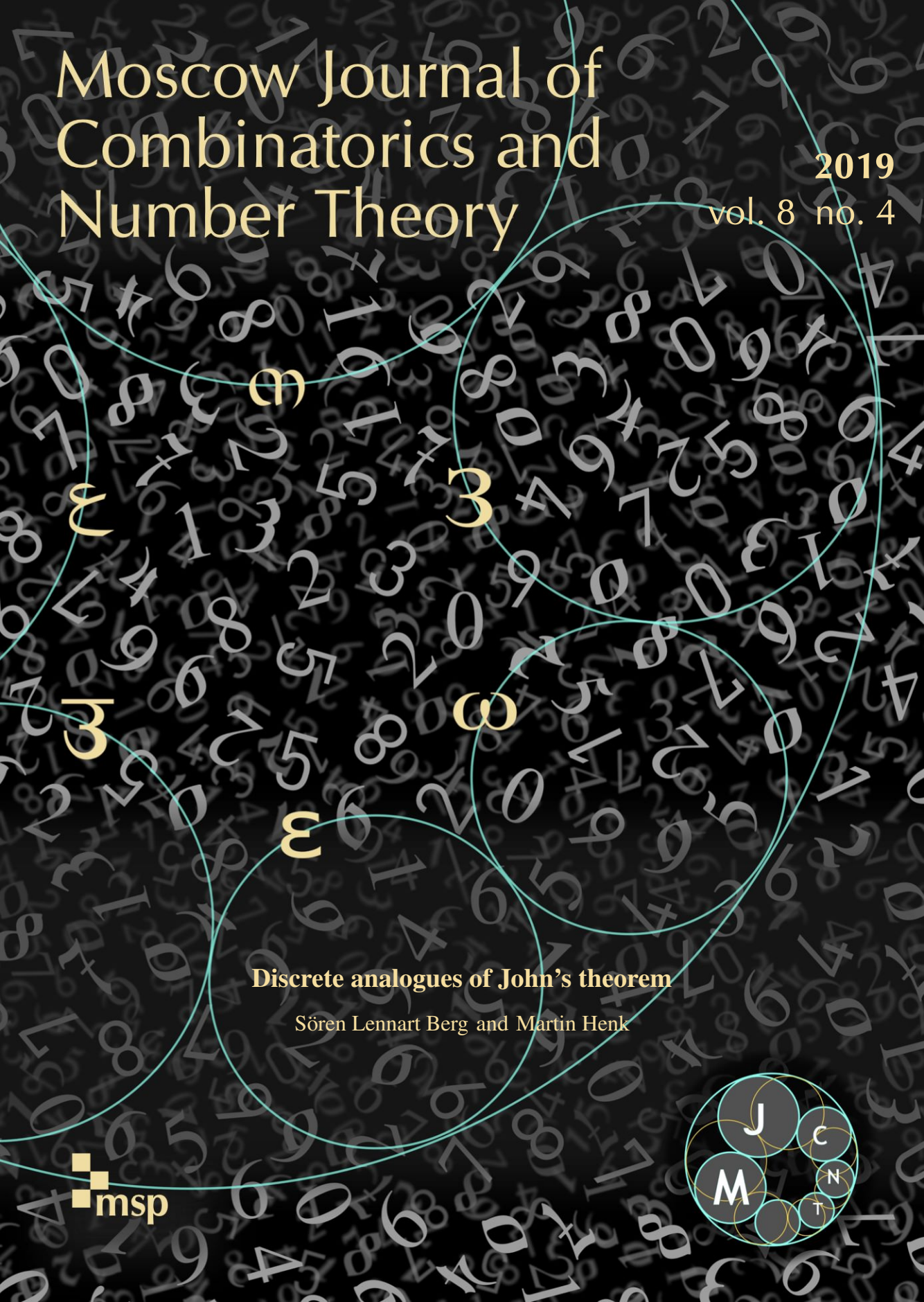
Moscow Journal of Combinatorics and Number Theory

2019
vol. 8 no. 4



Discrete analogues of John's theorem

Sören Lennart Berg and Martin Henk

msp

msp

Moscow Journal of Combinatorics and Number Theory
Vol. 8, No. 4, 2019
dx.doi.org/10.2140/moscow.2019.8.367

Discrete analogues of John's theorem

Sören Lennart Berg and Martin Henk

As a discrete counterpart to the classical theorem of Fritz John on the approximation of symmetric n-dimensional convex bodies K by ellipsoids, Tao and Vu introduced so called generalized arithmetic progressions $\mathrm{P}(A, \boldsymbol{b}) \subset \mathbb{Z}^n$ in order to cover (many of) the lattice points inside a convex body by a simple geometric structure. Among others, they proved that there exists a generalized arithmetic progressions $\mathrm{P}(A, \boldsymbol{b})$ such that $\mathrm{P}(A, \boldsymbol{b}) \subset K \cap \mathbb{Z}^n \subset \mathrm{P}(A, O(n)^{3n/2}\boldsymbol{b})$. Here we show that this bound can be lowered to $n^{O(\ln n)}$ and study some general properties of so called unimodular generalized arithmetic progressions.

1. Introduction

Let $\mathcal{K}^n_{(s)}$ be the set of all o-symmetric convex bodies in $\mathbb{R}^n$, i.e., $K \in \mathcal{K}^n_{(s)}$ is a compact convex set in $\mathbb{R}^n$ with nonempty interior and $K = -K$. By $B_n \in \mathcal{K}^n_{(s)}$ we denote the n-dimensional Euclidean unit ball, i.e., $B_n = \{\boldsymbol{x} \in \mathbb{R}^n : \langle \boldsymbol{x}, \boldsymbol{x} \rangle \leq 1\}$, where $\langle \cdot, \cdot \rangle$ is the standard inner product.

For $K \in \mathcal{K}^n_{(s)}$, John's (ellipsoid) theorem states that there exists an ellipsoid $\mathcal{E} \in \mathcal{K}^n_{(s)}$ such that

$$\mathcal{E} \subseteq K \subseteq \sqrt{n}\,\mathcal{E}. \tag{1-1}$$

(See, e.g., [Artstein-Avidan et al. 2015, Theorem 2.1.3] and [Schneider 2014, Theorem 10.12.2].) It turns out that the volume maximal ellipsoid contained in K gives the desired approximation, and in the nonsymmetric (or general) case the factor $\sqrt{n}$ has to be replaced by n (after a suitable translation of K).

This theorem has numerous applications in convex geometry or in the local theory of Banach spaces (see the two works just cited for examples). It allows one to get a first quick estimate on the value $f(K)$ of any homogenous and monotone functional f on $\mathcal{K}^n_{(s)}$ by the value of the functional at ellipsoids. For instance, if vol denotes the n-dimensional volume, i.e., n-dimensional Lebesgue measure, than (1-1) implies that for $K \in \mathcal{K}^n_{(s)}$ there exists an ellipsoid $\mathcal{E}$ such that

$$\operatorname{vol}\mathcal{E} \leq \operatorname{vol} K \leq n^{n/2} \operatorname{vol}\mathcal{E}. \tag{1-2}$$

In particular, the volume of an ellipsoid can easily be evaluated as $\mathcal{E} = A\,B_n$ for some $A \in \mathrm{GL}(n, \mathbb{R})$, and thus $\operatorname{vol}\mathcal{E} = |\det A| \operatorname{vol} B_n$.

Tao and Vu [2006] started to study a discrete version of John's theorem, where the aim of the approximation is the set of lattice points in K, i.e., the set $K \cap \mathbb{Z}^n$. The approximation itself is carried out

This paper contains some material from Berg's PhD thesis.

MSC2010: primary 11H06, 52C07; secondary 52A40.
Keywords: John's theorem, arithmetic progressions, convex bodies, lattices.

not by lattice points in ellipsoids, which are hard to control or to compute, but by a so called symmetric generalized arithmetic progression (GAP for short)

$$\mathrm{P}(A, \boldsymbol{b}) = \{A\, z : z \in \mathbb{Z}^n,\ |z_i| \le b_i, 1 \le i \le n\},$$

where $A \in \mathbb{Z}^{n\times n}$, $\det A \neq 0$, and $\boldsymbol{b} \in \mathbb{R}^n$. Hence, $\mathrm{P}(A, \boldsymbol{b})$ consists of the lattice points of the lattice $A\mathbb{Z}^n$ in the parallelepiped $\sum_{i=1}^n \operatorname{conv}\{-b_i \boldsymbol{a}_i, b_i \boldsymbol{a}_i\}$, where $\boldsymbol{a}_i$ is the i-th column of A and conv denotes the convex hull.

The same authors proved an improvement of an earlier result of theirs, [Tao and Vu 2006, Lemma 3.36]:

Theorem [Tao and Vu 2008, Theorem 1.6]. *Let $K \in \mathcal{K}^n_{(s)}$. There exists a GAP $\mathrm{P}(A, \boldsymbol{b}) \subset K$ such that*

$$K \cap \mathbb{Z}^n \subset \mathrm{P}(A, \mathrm{O}(n)^{3n/2}\boldsymbol{b}), \tag{1-3a}$$

$$|K \cap \mathbb{Z}^n| < \mathrm{O}(n)^{7n/2}|\mathrm{P}(A, \boldsymbol{b})|. \tag{1-3b}$$

(If C is a finite set, $|C|$ denotes its cardinality.) Observe that $|\mathrm{P}(A, \boldsymbol{b})| = \prod_{i=1}^n (2\lfloor b_i \rfloor + 1)$ can be easily computed. Obviously, (1-3a) and (1-3b) may be regarded as discrete counterparts to (1-1) and (1-2).

A first qualitative version of such a theorem, without mentioning explicit constants, was given in [Bárány and Vershik 1992, Theorem 3]. Here we prove:

Theorem 1.1. *Let $K \in \mathcal{K}^n_{(s)}$.*

(i) *There exists a GAP $\mathrm{P}(A, \boldsymbol{b}) \subset K$ such that*

$$K \cap \mathbb{Z}^n \subset \mathrm{P}(A, n^{\mathrm{O}(\ln n)}\, \boldsymbol{b}). \tag{1-4}$$

(ii) *There exists a GAP $\mathrm{P}(A, \boldsymbol{b}) \subset K$ such that*

$$|K \cap \mathbb{Z}^n| < \mathrm{O}(n)^n |\mathrm{P}(A, \boldsymbol{b})|. \tag{1-5}$$

In comparison to the volume case (John's ellipsoid) a GAP contained in $K \in \mathcal{K}^n_{(s)}$ that is optimal for the cardinality bound (1-5), i.e., covering most of the lattice points in K, does not need to be optimal for the inclusion bound (1-4) as well. We will give an example of this in Proposition 2.1. In fact, also the two GAPs leading to the bounds in (1-4) and (1-5) are different (in general).

Regarding a GAP $\mathrm{P}(A, \boldsymbol{b})$ which is simultaneously good with respect to inclusion and cardinality we have the following slight improvement on the above theorem of Tao and Vu.

Theorem 1.2. *Let $K \in \mathcal{K}^n_{(s)}$. There exists a GAP $\mathrm{P}(A, \boldsymbol{b}) \subset K$ such that*

$$K \cap \mathbb{Z}^n \subset \mathrm{P}(A, \mathrm{O}(n)^{2n/\ln n}\boldsymbol{b}), \tag{1-6a}$$

$$|K \cap \mathbb{Z}^n| < \mathrm{O}(n)^{2n} |\mathrm{P}(A, \boldsymbol{b})|. \tag{1-6b}$$

An *unconditional* convex body $K \in \mathcal{K}^n_{(s)}$ is one that is symmetric with respect to all coordinate hyperplanes. For such K, the inclusion bound can be made linear:

Proposition 1.3. *Let $K \in \mathcal{K}^n_{(s)}$ be an unconditional convex body. There exists a GAP $\mathrm{P}(A, \boldsymbol{b}) \subset K$ with*

$$K \cap \mathbb{Z}^n \subseteq \mathrm{P}(A, n\,\boldsymbol{b}), \tag{1-7a}$$

$$|K \cap \mathbb{Z}^n| < O(n)^n |\mathrm{P}(A, \boldsymbol{b})|. \tag{1-7b}$$

As we will show in Proposition 3.4, the linear inclusion bound in Proposition 1.3 is essentially best possible, and it might be even true that the bound of order $n^{\mathrm{O}(\ln n)}$ in (1-4) can be replaced by a linear or polynomial bound in n. In general, it seems to be a hard problem to construct explicitly a best possible GAP for one of the bounds; in fact, even the proofs yielding the results in the theorems above are rather nonconstructive. For unconditional bodies, however, the GAP behind the bounds in Proposition 1.3 can easily be described; see the proof of Proposition 1.3 on page 376 and the subsequent discussion.

For some other recent results regarding discretization of well-known inequalities from convex geometry we refer to, e.g., [Alexander et al. 2017; Hernández Cifre et al. 2018; Ryabogin et al. 2017].

The paper is organized as follows. In Section 2 we introduce and collect some basic properties of GAPs approximating the lattice points in symmetric convex bodies. In turns out that GAPs where the columns of A form a lattice basis of $\mathbb{Z}^n$ are of particular interest and we study them in Section 3. Finally, Section 4 contains the proofs of the theorems and of the proposition above.

2. Preliminaries and GAPs

For the proof of Theorem 1.1 it is more convenient to introduce GAPs for general lattices $\Lambda \subset \mathbb{R}^n$, i.e., $\Lambda = B\,\mathbb{Z}^n$, $B \in \mathbb{R}^{n\times n}$ with $\det B \neq 0$. Let $\mathcal{L}^n$ be the set of all these lattices. Following [Tao and Vu 2008], and adapting their definition to our special geometric situation, we define a generalized symmetric arithmetic progression with respect to Λ, or GAP, as the set of lattice points in Λ given by

$$\mathrm{P}(A, \boldsymbol{b}) = \{Az : -\boldsymbol{b} \le z \le \boldsymbol{b}, z \in \mathbb{Z}^n\},$$

where $A \in \mathbb{R}^{n\times n}$ is a matrix with columns $\boldsymbol{a}_i \in \Lambda$, $1 \le i \le n$, and $\boldsymbol{b} \in \mathbb{R}^n_{>0}$.

Actually, Tao and Vu defined GAPs more generally, namely, for general $n \times m$ matrices A. In our geometric setting, however, this would make the inclusion bound needless as A may consist of all (up to $\pm$) lattice points in $K \in \mathcal{K}^n_{(s)}$. Then, letting $\boldsymbol{b} = (1-\varepsilon)\mathbf{1}$, where $\mathbf{1}$ is the appropriate all 1-vector and ε an arbitrary positive number less than 1, gives the trivial inclusions

$$\{\mathbf{0}\} = P(A, \boldsymbol{b}) \subset K \cap \mathbb{Z}^n \subset P(A, (1-\varepsilon)^{-1}\boldsymbol{b})$$

Tao and Vu were mainly interested in so called infinitely proper GAPs which here means $m = \mathrm{rank}(A)$, and so we restrict the definition to the case $A \in \mathbb{R}^{n\times n}$, $\det A \neq 0$.

The size or cardinality of a GAP $\mathrm{P}(A, \boldsymbol{b})$ is given

$$|\mathrm{P}(A, \boldsymbol{b})| = \prod_{i=1}^{n} (2\lfloor b_i \rfloor + 1),$$

where $\lfloor \cdot \rfloor$ denotes the floor function. In general, for a vector $\boldsymbol{b} \in \mathbb{R}^n$ we denote by $\lfloor \boldsymbol{b} \rfloor = (\lfloor b_1 \rfloor, \ldots, \lfloor b_n \rfloor)^{\mathsf{T}}$ its integral part. The parallelepiped associated to $\mathrm{P}(A, \boldsymbol{b})$ is denoted by

$$\mathrm{P}_{\mathbb{R}}(A, \boldsymbol{b}) = \{A\boldsymbol{x} : -\boldsymbol{b} \le \boldsymbol{x} \le \boldsymbol{b},\ \boldsymbol{x} \in \mathbb{R}^n\} = \sum_{i=1}^{n} \mathrm{conv}\,\{-b_i\boldsymbol{a}_i, b_i\boldsymbol{a}_i\}.$$

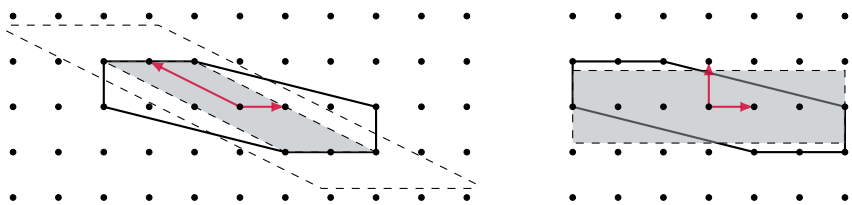
Observe that

$$\mathrm{P}_{\mathbb{R}}(A, \lfloor \boldsymbol{b} \rfloor) = \operatorname{conv} \mathrm{P}(A, \boldsymbol{b}). \tag{2-1}$$

Whenever we are interested in a GAP $\mathrm{P}(A, \boldsymbol{b})$ covering most of the lattice points in a convex body, i.e., a GAP which is optimal with respect to the cardinality bound, then it suffices to assume $\boldsymbol{b} \in \mathbb{N}^n$. However, for an optimal GAP with respect to the inclusion bound it might be essential to consider nonintegral vectors $\boldsymbol{b} \in \mathbb{R}^n_{>0}$. This is also reflected by the next example showing that those GAPs yielding an optimal cardinality bound can be different from those leading to an optimal inclusion bound.

Proposition 2.1. *Let $n \geq 2$. There exists a $K \in \mathcal{K}^n_{(s)}$ such that any GAP $\mathrm{P}(A, \boldsymbol{b}) \subset K$ covering most of the lattice points of K is not an optimal GAP with respect to inclusions, i.e., there exists another GAP $\mathrm{P}(\bar{A}, \bar{\boldsymbol{b}}) \subset K$ such that for any $t > 1$ with $K \cap \mathbb{Z}^n \subseteq \mathrm{P}(A, t\,\boldsymbol{b})$ there exits a $\bar{t} < t$ with $K \cap \mathbb{Z}^n \subseteq \mathrm{P}(\bar{A}, \bar{t}\,\bar{\boldsymbol{b}})$.*

Proof. We start with dimension 2, and let $K = \operatorname{conv}\{\pm(3, 0)^\intercal, \pm(-3, 1)^\intercal, \pm(-1, 1)^\intercal\}$, the hexagon in the figure.



We will argue that an optimal cardinality GAP $P(A, \boldsymbol{b}) \subseteq K$ contains 9 out of the 13 lattice points in K. To this end we may assume that the columns $\boldsymbol{a}_i$ of A belong to K, i.e., $\boldsymbol{a}_i \in K$ and $\boldsymbol{b} \geq \mathbf{1}$. Otherwise, we could only cover lattice points on a line which would be at most 7. Since for all $\boldsymbol{x} \in K$ we have $|x_2| \leq 1$, and since also the sum $\boldsymbol{a}_1 + \boldsymbol{a}_2$ has to belong to K, there is at most one column $\boldsymbol{a}_i$ of A having a nonzero last coordinate.

If there would be none, then again only the 7 points with last coordinate 0 could be covered.

Next assume that $\boldsymbol{a}_2$ is the vector having last coordinate nonzero and let $\boldsymbol{a}_1$ be the vector with last coordinate 0. The only possibility so that $\boldsymbol{a}_1 \pm \boldsymbol{a}_2$ belong to K is (up to sign) the one depicted in the left figure, i.e., $\boldsymbol{a}_1 = (1, 0)^\intercal$ and $\boldsymbol{a}_2 = (-2, 1)^\intercal$, and for any $\boldsymbol{b}$ with $1 \leq b_i < 2$, $i = 1, 2$, the GAP $\mathrm{P}(A, \boldsymbol{b})$ covers 9 out of the 13 lattice points of K. Hence, the GAPs covering the maximal amount of lattice points of K are given – up to $\pm$ and permutations of the columns of A – by $\mathrm{P}(A, \boldsymbol{b})$ for any $\boldsymbol{b}$ with $1 \leq b_i < 2$, $i = 1, 2$. Since $(3, 0)^\intercal \in K$, we observe that in order to cover all the points of $K \cap \mathbb{Z}^2$ by $\mathrm{P}(A, t\,\boldsymbol{b})$ we must have $t > \frac{3}{2}$.

On the other hand, if we take for the columns of $\bar{A}$ the vectors $(1, 0)^\intercal$ and $(0, 1)^\intercal$ and setting $\bar{\boldsymbol{b}} = (3, 1 - \varepsilon)^\intercal$ we get $|\mathrm{P}(\bar{A}, \bar{\boldsymbol{b}})| = 7$, but $K \cap \mathbb{Z}^2 \subset P(\bar{A}, (1 - \varepsilon)^{-1}\bar{\boldsymbol{b}})$ for any $\varepsilon \in (0, 1)$ (see the right half of the figure above).

This verifies the assertion in the plane. By building successively prisms over Q the example can be extended to all dimensions. □

3. Unimodular GAPs

Without loss of generality we consider here only the case $\Lambda = \mathbb{Z}^n$. The group of all unimodular matrices, i.e., integral $n \times n$-matrices of determinant ± 1, is denoted by $\mathrm{GL}(n, \mathbb{Z})$; it consists of all lattice bases of

$\mathbb{Z}^n$. Apparently, if $K \cap \mathbb{Z}^n$ contains a lattice basis of $\mathbb{Z}^n$ and $K \cap \mathbb{Z}^n \subseteq \mathrm{P}(A, \boldsymbol{b})$ then $A \in \mathrm{GL}(n, \mathbb{Z})$. This basically shows that for the inclusion bound it suffices to consider GAPs $\mathrm{P}(U, \boldsymbol{b})$ with $U \in \mathrm{GL}(n, \mathbb{Z})$. We will call such a GAP an unimodular GAP.

Proposition 3.1. *Let $c = c(n) \in \mathbb{R}_{>0}$ be a constant depending on n. The following statements are equivalent.*

(i) *For every $K \in \mathcal{K}^n_{(s)}$ there exists a GAP $\mathrm{P}(A, \boldsymbol{b}) \subset K$ such that $K \cap \mathbb{Z}^n \subset \mathrm{P}(A, c\,\boldsymbol{b})$.*

(ii) *For every $K \in \mathcal{K}^n_{(s)}$ there exists an unimodular GAP $\mathrm{P}(U, \boldsymbol{b}) \subset K$ such that $K \cap \mathbb{Z}^n \subset \mathrm{P}(U, c\,\boldsymbol{b})$.*

Proof. Obviously, we only have to show that (i) implies (ii). To this end let $l \in \mathbb{N}$ such that $l\,K$ contains a basis of $\mathbb{Z}^n$. By assumption there exists a GAP $P(U, \boldsymbol{b}) \subset lK$ such that $lK \cap \mathbb{Z}^n \subseteq P(U, c\,\boldsymbol{b})$ and since lK contains a basis of $\mathbb{Z}^n$ we have $U \in \mathrm{GL}(n, \mathbb{Z})$. Next we claim that

$$P(U, l^{-1}\boldsymbol{b}) \subseteq K \cap \mathbb{Z}^n \subseteq P(U, c\,l^{-1}\boldsymbol{b}). \tag{3-1}$$

Let $\boldsymbol{u} \in P(U, l^{-1}\boldsymbol{b})$. Then there exists a $\boldsymbol{z} \in \mathbb{Z}^n$ with $\boldsymbol{u} = U\boldsymbol{z}$ and $-l^{-1}\boldsymbol{b} \le \boldsymbol{z} \le l^{-1}\boldsymbol{b}$. Thus $l\boldsymbol{u} = U\,l\boldsymbol{z}$ and since $l\,\boldsymbol{z} \in \mathbb{Z}^n$ we get $l\boldsymbol{u} \in \mathrm{P}(U, \boldsymbol{b}) \subset l\,K$. Hence $\boldsymbol{u} \in K \cap \mathbb{Z}^n$ which shows the first inclusion in (3-1). For the second let $\boldsymbol{a} \in K \cap \mathbb{Z}^n$. Then $l\,\boldsymbol{a} \in l\,K \cap \mathbb{Z}^n \subseteq P(U, c\,\boldsymbol{b})$ and so there exists a $\boldsymbol{z} \in \mathbb{Z}^n$ with $-c\,\boldsymbol{b} \le \boldsymbol{z} \le c\,\boldsymbol{b}$ with $l\,\boldsymbol{a} = U\boldsymbol{z}$. Hence, $\boldsymbol{a} = U\,l^{-1}\boldsymbol{z}$ and since $U \in \mathrm{GL}(n, \mathbb{Z})$ we conclude $l^{-1}\boldsymbol{z} \in \mathbb{Z}^n$ which shows $\boldsymbol{a} \in P(U, c\,l^{-1}\boldsymbol{b})$. □

Next we want to point out a relation between GAPs and approximations of a convex body by an "unimodular" parallelepiped $\mathrm{P}_{\mathbb{R}}(U, \boldsymbol{u})$, $U \in \mathrm{GL}(n, \mathbb{Z})$. To this we first note that

Lemma 3.2. *Let $K \in \mathcal{K}^n_{(s)}$ containing n linearly independent points $\beta\boldsymbol{a}_i$ with $\beta \in \mathbb{R}_{>0}$ and $\boldsymbol{a}_i \in \mathbb{Z}^n$, $1 \le i \le n$. Then for any unimodular GAP $\mathrm{P}(U, \boldsymbol{u})$ with $K \subseteq \mathrm{P}_{\mathbb{R}}(U, \boldsymbol{u})$ we have $u_i \ge \beta$, $1 \le i \le n$.*

Proof. Let $\beta\boldsymbol{a}_i = U\boldsymbol{x}_i$ with $-\boldsymbol{u} \le \boldsymbol{x}_i \le \boldsymbol{u}$, $\boldsymbol{x}_i \in \mathbb{R}^n$. Since $U \in \mathrm{GL}(n, \mathbb{Z})$ we get $\boldsymbol{x}_i \in \beta\mathbb{Z}^n$, which shows that for each nonzero coordinate j, say, of $\boldsymbol{x}_i$ we have $u_j \ge \beta$. Since $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ are linearly independent for each coordinate k we can find a vector $\boldsymbol{x}_l$ whose k-th coordinate is nonzero. □

Observe, for an unimodular GAP $\mathrm{P}(U, \boldsymbol{u})$ we have $\mathrm{P}(U, \boldsymbol{u}) = \mathrm{P}_{\mathbb{R}}(U, \boldsymbol{u}) \cap \mathbb{Z}^n$.

Proposition 3.3. *Let $c = c(n) \in \mathbb{R}_{>0}$ be a constant depending on n. The following statements are equivalent.*

(i) *For every $K \in \mathcal{K}^n_{(s)}$ there exists a GAP $\mathrm{P}(A, \boldsymbol{b}) \subset K$ such that $K \cap \mathbb{Z}^n \subseteq \mathrm{P}(A, c\,\boldsymbol{b})$.*

(ii) *For every $K \in \mathcal{K}^n_{(s)}$ there exists an unimodular GAP $\mathrm{P}(U, \boldsymbol{u}) \subset K$ such that*

$$\mathrm{P}_{\mathbb{R}}(U, \boldsymbol{u}) \subseteq K \subset \mathrm{P}_{\mathbb{R}}(U, c\,\boldsymbol{u}).$$

Proof. We start by showing that (i) implies (ii). Let $\varepsilon > 0$, and let $Q \subseteq K$ be a o-symmetric rational polytope with $K \subset (1+\varepsilon)Q$ (see, e.g., [Schneider 2014, Theorem 1.8.19]). Moreover, let $m \in \mathbb{N}$ be such that $m\,Q$ is an integral polytope (all its vertices are in $\mathbb{Z}^n$) and contains the scaled unit vectors $c(1+c/\varepsilon)\boldsymbol{e}_i$, $1 \le i \le n$. In view of Proposition 3.1 there exists an unimodular GAP $\mathrm{P}(U, \boldsymbol{u})$ such that

$$\mathrm{P}(U, \boldsymbol{u}) \subset m\,Q \cap \mathbb{Z}^n \subseteq \mathrm{P}(U, c\,\boldsymbol{u}).$$

The polytopes $\mathrm{P}_{\mathbb{R}}(U, \lfloor \boldsymbol{u} \rfloor)$ and $m\,Q$ are integral and so we get

$$\begin{aligned}\mathrm{P}_{\mathbb{R}}(U, \lfloor \boldsymbol{u} \rfloor) &= \operatorname{conv}\left(\mathrm{P}_{\mathbb{R}}(U, \lfloor \boldsymbol{u} \rfloor) \cap \mathbb{Z}^n\right) = \operatorname{conv} \mathrm{P}(U, \lfloor \boldsymbol{u} \rfloor) \\ &\subseteq \operatorname{conv} \mathrm{P}(U, \boldsymbol{u}) \subseteq \operatorname{conv}\left(m\,Q \cap \mathbb{Z}^n\right) = m\,Q \subseteq m\,K. \end{aligned} \tag{3-2}$$

Since $m\,Q$ is integral we have $m\,Q \subseteq \mathrm{P}_{\mathbb{R}}(U, c\,\boldsymbol{u})$ and due to Lemma 3.2 we know for the entries of $\boldsymbol{u}$ that $u_i \geq 1 + c/\varepsilon$, $1 \leq i \leq n$, which implies that

$$\frac{u_i}{\lfloor u_i \rfloor} \leq \frac{u_i}{u_i - 1} \leq 1 + \frac{\varepsilon}{c},$$

and thus $c\,\boldsymbol{u} \leq (c + \varepsilon)\lfloor \boldsymbol{u} \rfloor$. Hence,

$$\begin{aligned} m\,Q &= \operatorname{conv}\left(m\,Q \cap \mathbb{Z}^n\right) \subseteq \operatorname{conv} \mathrm{P}(U, c\,\boldsymbol{u}) \\ &\subseteq \mathrm{P}_{\mathbb{R}}(U, c\,\boldsymbol{u}) \subseteq \mathrm{P}_{\mathbb{R}}(U, (c+\varepsilon)\,\lfloor \boldsymbol{u} \rfloor), \end{aligned}$$

and with (3-2)

$$\mathrm{P}_{\mathbb{R}}(U, m^{-1}\lfloor \boldsymbol{u} \rfloor) \subseteq K \subseteq \mathrm{P}_{\mathbb{R}}(U, (1+\varepsilon)\,(c+\varepsilon)\,m^{-1}\lfloor \boldsymbol{u} \rfloor). \tag{3-3}$$

Observe, that actually $m = m_\varepsilon$, $U = U_\varepsilon$ as well as $\boldsymbol{u} = \boldsymbol{u}_\varepsilon$ depend on the chosen ε. Now, since K is bounded and all entries of U are integral, the first inclusion above shows that the sequence $m_\varepsilon^{-1}\lfloor \boldsymbol{u}_\varepsilon \rfloor$, $\varepsilon > 0$, has to be bounded. Therefore, we may assume that it converges to $\bar{\boldsymbol{u}}$ as ε approaches 0. Next assume that a sequence of a (fixed) column vector of the unimodular matrices U_ε is unbounded. Since $\operatorname{vol} \mathrm{P}_{\mathbb{R}}(U_\varepsilon, \mathbf{1}) = 2^n$ and since $m_\varepsilon^{-1}\lfloor \boldsymbol{u}_\varepsilon \rfloor$ is bounded this shows that the inradius of $\mathrm{P}_{\mathbb{R}}(U_\varepsilon, (1+\varepsilon)\,(c+\varepsilon)\,m_\varepsilon^{-1}\lfloor \boldsymbol{u}_\varepsilon \rfloor)$ must converge to 0 as ε tends to 0. This contradicts the second inclusion above and hence, also U_ε converges to an unimodular matrix $\overline{U}$. So we have shown

$$\mathrm{P}_{\mathbb{R}}(\overline{U}, \bar{\boldsymbol{u}}) \subseteq K \subseteq \mathrm{P}_{\mathbb{R}}(\overline{U}, c\,\bar{\boldsymbol{u}}).$$

For the reverse implication we assume that there exists an unimodular GAP $\mathrm{P}(U, \boldsymbol{u})$ fulfiling (ii). Then

$$\mathrm{P}_{\mathbb{R}}(U, \boldsymbol{u}) \cap \mathbb{Z}^n \subseteq K \cap \mathbb{Z}^n \subseteq \mathrm{P}_{\mathbb{R}}(U, c\,\boldsymbol{u}) \cap \mathbb{Z}^n,$$

and by the unimodularity of U we have $\mathrm{P}_{\mathbb{R}}(U, \boldsymbol{u}) \cap \mathbb{Z}^n = \mathrm{P}(U, \boldsymbol{u})$ as well as $\mathrm{P}_{\mathbb{R}}(U, c\,\boldsymbol{u}) \cap \mathbb{Z}^n = \mathrm{P}(U, c\,\boldsymbol{u})$. □

We close this section with lower bounds on the factors in (1-4) and (1-5) of Theorem 1.1.

Proposition 3.4.

(i) *Let $\tau = \tau(n) \in \mathbb{R}_{>0}$ be a constant depending on n such that for every $K \in \mathcal{K}^n_{(s)}$ there exists a GAP $\mathrm{P}(A, \boldsymbol{b}) \subset K$ such that $K \cap \mathbb{Z}^n \subseteq \mathrm{P}(A, \tau\,\boldsymbol{b})$. Then $\tau \geq n!^{1/n} > \frac{1}{\mathrm{e}} n$.*

(ii) *Let $\nu = \nu(n) \in \mathbb{R}_{>0}$ be a constant depending on n such that for every $K \in \mathcal{K}^n_{(s)}$ there exists a GAP $\mathrm{P}(A, \boldsymbol{b}) \subset K$ such that $|K \cap \mathbb{Z}^n| \leq \nu\,|\mathrm{P}(A, \boldsymbol{b})|$. Then $\nu \geq (2^n + 1)/3$.*

Proof. For (i) we consider for an integer $m \in \mathbb{N}$ the cross-polytope $mC_n^\star = \{\boldsymbol{x} \in \mathbb{R}^n : |x_1| + \cdots + |x_n| \leq m\}$ and let $\mathrm{P}(U, \boldsymbol{u})$ be a GAP such that

$$\mathrm{P}(U, \boldsymbol{u}) \subseteq mC_n^\star \cap \mathbb{Z}^n \subseteq \mathrm{P}(U, \tau\,\boldsymbol{u}). \tag{3-4}$$

In view of Proposition 3.1, or since $mC_n^\star$ contains the unit vectors $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ we have $U \in \mathrm{GL}(n, \mathbb{Z})$. Moreover, since $m\boldsymbol{e}_i \in mC_n^\star$, $1 \le i \le n$, we get from the second inclusion in (3-4) and Lemma 3.2 that $m \le \tau\, u_i$, $1 \le i \le n$, and so

$$\mathrm{vol}\,(mC_n^\star) = m^n \frac{2^n}{n!} \le \tau^n \frac{2^n}{n!} \prod_{i=1}^n u_i. \tag{3-5}$$

On the other hand, the first inclusion in (3-4) implies

$$\mathrm{P}_{\mathbb{R}}(U, \lfloor \boldsymbol{u} \rfloor) = \mathrm{conv}\,\mathrm{P}(U, \boldsymbol{u}) \subseteq mC_n^\star,$$

and so

$$2^n \prod_{i=1}^n \lfloor u_i \rfloor = \mathrm{vol}\,\mathrm{P}_{\mathbb{R}}(U, \lfloor \boldsymbol{u} \rfloor) \le \mathrm{vol}\,(mC_n^\star).$$

Combined with (3-5) we obtain

$$\tau \ge n!^{1/n} \left(\prod_{i=1}^n \frac{\lfloor u_i \rfloor}{u_i} \right)^{1/n}.$$

This is true for any $m \in \mathbb{N}$, and since $u_i \to \infty$ for $m \to \infty$, we find $\tau \ge n!^{1/n} > n/\mathrm{e}$.

To prove (ii), let Q be the o-symmetric lattice polytope given by $Q = \mathrm{conv}\,(\pm([0,1]^{n-1} \times \{1\}))$. Then it is easy to see that $Q \cap \mathbb{Z}^n = \pm(\{0,1\}^{n-1} \times \{1\}) \cup \{\boldsymbol{0}\}$ and hence, Q does not contain $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{Z}^n \setminus \{\boldsymbol{0}\}$, $\boldsymbol{x} \ne -\boldsymbol{y}$, and $\boldsymbol{x} + \boldsymbol{y} \in Q$. Thus for any GAP $\mathrm{P}(A, \boldsymbol{b}) \subset Q$ we have $|\mathrm{P}(A, \boldsymbol{b})| \le 3$ and so

$$2^n + 1 = |Q \cap \mathbb{Z}^n| \le \nu\, |\mathrm{P}(A, \boldsymbol{b})| \le 3\, \nu,$$

yielding the desired lower bound. □

4. Proofs of the theorems

For the proof of the inclusion bound (1-4) of Theorem 1.1 we follow essentially the proof of [Tao and Vu 2008], but we apply a different lattice reduction taking into account also the polar lattice. More precisely, for a lattice $\Lambda \in \mathcal{L}^n$ with basis $B = (\boldsymbol{b}_1, \dots, \boldsymbol{b}_n)$, i.e., $\Lambda = B\mathbb{Z}^n$, we denote by

$$\Lambda^\star = \{\boldsymbol{y} \in \mathbb{R}^n : \langle \boldsymbol{x}, \boldsymbol{y} \rangle \in \mathbb{Z} \text{ for all } \boldsymbol{x} \in \Lambda\} = B^{-\mathsf{T}}\mathbb{Z}^n$$

its polar lattice. In particular, if $B^{-T} = (\boldsymbol{b}_1^\star, \dots, \boldsymbol{b}_n^\star)$, then

$$\langle \boldsymbol{b}_i^\star, \boldsymbol{b}_j \rangle = \delta_{i,j}, \tag{4-1}$$

where $\delta_{i,j}$ denotes the Kronecker-symbol. Now a basis B of a lattice Λ is called Seysen reduced if

$$S(B) = \sum_{i=1}^n \|\boldsymbol{b}_i\|^2 \|\boldsymbol{b}_i^\star\|^2$$

is minimal among all bases of Λ (cf. [Seysen 1993]). Here, $\|\cdot\|$ denotes the Euclidean norm.

Theorem 4.1 [Seysen 1993, Theorem 7]. *Let $\Lambda \in \mathcal{L}^n$. There exists a basis $B = (\boldsymbol{b}_1, \dots, \boldsymbol{b}_n)$ of Λ such that $S(B) \le n^{O(\ln n)}$. In particular, for $1 \le i \le n$,*

$$\|\boldsymbol{b}_i\| \, \|\boldsymbol{b}_i^\star\| \le n^{O(\ln n)}. \tag{4-2}$$

For an explicit bound we refer to [Maze 2010] and for more information on lattice reduction and geometry of numbers we refer to [Gruber and Lekkerkerker 1987; Cassels 1959]. For the sake of comprehensibility we split the proof of Theorem 1.1 into two parts, one covering the inclusion bound and one the cardinality bound.

Proof of Theorem 1.1(i). In view of John's theorem (1-1) we may apply a linear transformation T to K such that with $\tilde{K} = TK$

$$B_n \subseteq \tilde{K} \subseteq \sqrt{n} B_n. \tag{4-3}$$

With $\Lambda = T\mathbb{Z}^n$ the problem is now to find a GAP $\mathrm{P}(A, \boldsymbol{b})$ in Λ such that $\mathrm{P}(A, \boldsymbol{b}) \subset \tilde{K}$ and

$$\tilde{K} \cap \Lambda \subset \mathrm{P}(A, n^{O(\ln n)} \boldsymbol{b}).$$

Let $B = (\boldsymbol{b}_1, \dots, \boldsymbol{b}_n)$ be a Seysen reduced basis of Λ with associated basis $B^{-\mathsf{T}} = (\boldsymbol{b}_1^\star, \dots, \boldsymbol{b}_n^\star)$ of the polar lattice and let $\boldsymbol{u} \in \mathbb{R}^n$ be given by $u_i = (1/n)\|\boldsymbol{b}_i\|^{-1}$, $1 \le i \le n$.

First, for $\boldsymbol{x} \in \mathrm{P}_{\mathbb{R}}(B, \boldsymbol{u})$ we have $\boldsymbol{x} = \sum_{i=1}^n \lambda_i \boldsymbol{b}_i$ with $|\lambda_i| \le u_i$ and by the triangle inequality we conclude $\|\boldsymbol{x}\| \le 1$. Hence, with (4-3) we certainly have $\mathrm{P}(B, \boldsymbol{u}) \subset \tilde{K}$. On the other hand, given $\boldsymbol{x} = \sum_{i=1}^n \beta_i \boldsymbol{b}_i \in \tilde{K}$ we get by Cramer's rule and (4-3)

$$|\beta_i| = \frac{|\det(\boldsymbol{x}, \boldsymbol{b}_1, \dots, \boldsymbol{b}_{i-1}, \boldsymbol{b}_{i+1}, \boldsymbol{b}_n)|}{|\det B|} \le \sqrt{n} \frac{\mathrm{vol}_{n-1}(\boldsymbol{b}_1, \dots, \boldsymbol{b}_{i-1}, \boldsymbol{b}_{i+1}, \boldsymbol{b}_n)}{\mathrm{vol}\,(\boldsymbol{b}_1, \dots, \boldsymbol{b}_n)},$$

where $\mathrm{vol}_k(\boldsymbol{c}_1, \dots, \boldsymbol{c}_k)$ denotes the k-dimensional volume of the parallelepiped $\left\{\sum_{i=1}^k \mu_i \boldsymbol{c}_i : 0 \le \mu_i \le 1\right\}$. By (4-1) we find that

$$\mathrm{vol}\,(\boldsymbol{b}_1, \dots, \boldsymbol{b}_n) = \mathrm{vol}_{n-1}(\boldsymbol{b}_1, \dots, \boldsymbol{b}_{i-1}, \boldsymbol{b}_{i+1}, \boldsymbol{b}_n) \frac{\langle \boldsymbol{b}_i^\star, \boldsymbol{b}_i \rangle}{\|\boldsymbol{b}_i^\star\|} = \mathrm{vol}_{n-1}(\boldsymbol{b}_1, \dots, \boldsymbol{b}_{i-1}, \boldsymbol{b}_{i+1}, \boldsymbol{b}_n) \frac{1}{\|\boldsymbol{b}_i^\star\|},$$

and thus for $1 \le i \le n$

$$|\beta_i| \le \sqrt{n} \|\boldsymbol{b}_i^\star\|. \tag{4-4}$$

Together with the definition of u_i and Seysen's bound (4-2) we conclude that $|\beta_i| \le n^{3/2} n^{O(\ln n)} u_i$, for $1 \le i \le n$. Hence,

$$\tilde{K} \cap \Lambda \subseteq \mathrm{P}_{\mathbb{R}}(B, n^{O(\ln n)} \boldsymbol{u}) \cap \Lambda = \mathrm{P}(B, n^{O(\ln n)} \boldsymbol{u}),$$

since B is a basis of Λ. □

Remark 4.2. The optimal upper bound in Theorem 4.1 for a Seysen reduced basis is not known, but any improvement on this bound would immediately yield an improvement of (1-4).

For the cardinality bound (1-5) of Theorem 1.1 we need another tool from geometry of numbers: Minkowski's successive minima $\lambda_i(K, \Lambda)$, which for $K \in \mathcal{K}^n_{(s)}$, $\Lambda \in \mathcal{L}^n$ and $1 \le i \le n$ are defined by

$$\lambda_i(K, \Lambda) = \min\{\lambda > 0 : \dim(\lambda K \cap \Lambda) \ge i\}.$$

In words, $\lambda_i(K, \Lambda)$ is the smallest dilation factor λ such that λK contains i linearly independent lattice points of Λ. Minkowski's fundamental second theorem on successive minima (e.g., [Gruber and Lekkerkerker 1987, §9, Theorem 1]) states that

$$\operatorname{vol} K \le \det \Lambda \prod_{i=1}^{n} \frac{2}{\lambda_i(K, \Lambda)}, \tag{4-5}$$

and here we need a discrete version of it. In [Henk 2002] it was shown that

$$|K \cap \Lambda| \le 2^{n-1} \prod_{i=1}^{n} \left\lfloor \frac{2}{\lambda_i(K, \Lambda)} + 1 \right\rfloor, \tag{4-6}$$

and for an improvement on the constant 2^{n-1} and related results we refer to [Malikiosis 2010; Malikiosis 2012]. It is conjectured in [Betke et al. 1993] that (4-6) holds without any additional factor in front of the product which would, in particular, imply Minkowski's volume bound.

Proof of Theorem 1.1(ii). Let $\boldsymbol{a}_i \in \mathbb{Z}^n$, $1 \le i \le n$, be linearly independent lattice vectors corresponding to the successive minima $\lambda_i = \lambda_i(K, \mathbb{Z}^n)$, i.e., $\boldsymbol{a}_i \in \lambda_i K$, $1 \le i \le n$. Since $\lambda_i^{-1}\boldsymbol{a}_i \in K$ it follows

$$\left\{ \sum_{i=1}^{n} \mu_i \frac{1}{n\lambda_i} \boldsymbol{a}_i : -1 \le \mu_i \le 1 \right\} \subset \operatorname{conv}\{\pm\lambda_i^{-1}\boldsymbol{a}_i : 1 \le i \le n\} \subseteq K.$$

Thus, denoting by A the matrix with columns $\boldsymbol{a}_i$ and letting $\boldsymbol{b}$ be the vector with entries $b_i = (n\lambda_i)^{-1}$ we have $\mathrm{P}(A, \boldsymbol{b}) \subset K$ and

$$|P(A, \boldsymbol{b})| = \prod_{i=1}^{n} \left(2\left\lfloor \frac{1}{n\lambda_i} \right\rfloor + 1\right).$$

Now it is not hard to see that

$$2\left\lfloor \frac{1}{n\lambda_i} \right\rfloor + 1 \ge \frac{1}{3}\frac{1}{n}\left\lfloor \frac{2}{\lambda_i} + 1 \right\rfloor, \tag{4-7}$$

and with (4-6) we get

$$|P(A, \boldsymbol{b})| \ge \left(\frac{1}{3n}\right)^n \left(\frac{1}{2}\right)^{n-1} 2^{n-1} \prod_{i=1}^{n} \left\lfloor \frac{2}{\lambda_i} + 1 \right\rfloor > (6n)^{-n} |K \cap \mathbb{Z}^n|.$$

This shows (1-5). □

Remark 4.3. The columns of the matrix A of the GAP in the proof of the cardinality bound of Theorem 1.1 do not in general build a basis of $\mathbb{Z}^n$; hence this GAP cannot be used in order to obtain an inclusion bound.

Now the proof of Theorem 1.2 is a kind of combination of the two proofs leading to (1-4) and (1-5). Instead of a Seysen reduced basis we exploit properties of a so called Hermite–Korkin–Zolotarev (HKZ) reduced basis $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ of the lattice Λ. For such a basis it was shown by Mahler (see, e.g., [Lagarias et al. 1990, Theorem 2.1]) that for $1 \le i \le n$

$$\|\boldsymbol{b}_i\| \le \frac{\sqrt{i+3}}{2} \lambda_i(B_n, \Lambda). \tag{4-8}$$

Håstad and Lagarias [1990] pointed out that for a HKZ-basis one has

$$\|b_i\| \, \|b_i^\star\| \le \left(\tfrac{3}{2}\right)^n < n^{\frac{1}{2}n/\ln n}. \tag{4-9}$$

This bound is worse than the one given in (4-2), but the advantage of a HKZ reduced basis is its close relation to the successive minima (4-8).

Proof of Theorem 1.2. First we may assume that $\lambda_n(K, \mathbb{Z}^n) \le 1$, i.e., that K contains n linearly independent lattice points. Otherwise, all lattice points of K lying in a hyperplane H and it would be sufficient to prove the theorem with respect to the $n-1$-dimensional convex body $K \cap H$ and lattice $H \cap \mathbb{Z}^n$.

Now we proceed completely analogously to the proof of Theorem 1.1(i); we just replace the Seysen reduced basis by a HKZ-reduced basis $B = (\boldsymbol{b}_1, \dots, \boldsymbol{b}_n)$, and the GAP is given by $\mathrm{P}(B, \boldsymbol{u})$ with $u_i = (1/n)\|\boldsymbol{b}_i\|^{-1}$, $1 \le i \le n$. Replacing (4-2) by (4-9) in (4-4) leads then to

$$\mathrm{P}(B, \boldsymbol{u}) \subseteq \tilde{K} \cap \Lambda \subseteq \mathrm{P}(B, n^{O(n/\ln n)}\boldsymbol{u}),$$

where $\tilde{K}$ was a linear image of K such that

$$B_n \subseteq \tilde{K} \subseteq \sqrt{n} B_n. \tag{4-10}$$

It remains to prove the cardinality bound for the GAP $\mathrm{P}(B, \boldsymbol{u})$ and $\tilde{K}$. Regarding the size of $\mathrm{P}(B, \boldsymbol{u})$ we have

$$|\mathrm{P}(B, \boldsymbol{u})| = \prod_{i=1}^{n} \left(2 \left\lfloor \frac{1}{n\|\boldsymbol{b}_i\|} \right\rfloor + 1 \right) \ge n^{-n} \prod_{i=1}^{n} \frac{1}{\|\boldsymbol{b}_i\|}. \tag{4-11}$$

On the other hand, for an upper bound on $\tilde{K} \cap \Lambda$ we use (4-6) and since $\lambda_n(K, \Lambda) \le 1$ we get

$$|K \cap \Lambda| \le 2^{n-1} \prod_{i=1}^{n} \left(\frac{2}{\lambda_i(K, \Lambda)} + 1 \right) \le 6^n \prod_{i=1}^{n} \frac{1}{\lambda_i(K, \Lambda)}.$$

In view of (4-10) and (4-8) we obtain

$$|K \cap \Lambda| \le 6^n \prod_{i=1}^{n} \frac{1}{\lambda_i(\sqrt{n} B_n, \Lambda)} = (6\sqrt{n})^n \prod_{i=1}^{n} \frac{1}{\lambda_i(B_n, \Lambda)} \le (6n)^n \prod_{i=1}^{n} \frac{1}{\|\boldsymbol{b}_i\|}.$$

Combined with (4-11) we get $|K \cap \Lambda| \le O(n)^{2n} |\mathrm{P}(B, \boldsymbol{u})|$. □

Next we consider unconditional bodies $K \in \mathcal{K}^n_{(s)}$, i.e., bodies which are symmetric with respect to all coordinate hyperplanes. As stated in Proposition 1.3, in this special case the inclusion bound can be made linear in the dimension. In view of Proposition 3.4 this is also the optimal order within this class of bodies as the given example used for the lower bound in Proposition 3.4 is unconditional.

Proof of Proposition 1.3. For $i = 1, \dots, n$ let u_i be the maximal entry of the i-th coordinate of a point of K. Then $u_i > 0$ and

$$K \cap \mathbb{Z}^n \subseteq \mathrm{P}(I_n, \boldsymbol{u}) \tag{4-12}$$

with $\boldsymbol{u} = (u_1, \dots, u_n)^\intercal$ and I_n the $n \times n$-identity matrix. By the unconditionality of K we have $\pm u_i \, \boldsymbol{e}_i \in K$, $1 \le i \le n$, and thus

$$\mathrm{P}_{\mathbb{R}}(I_n, n^{-1}\boldsymbol{u}) \subset \mathrm{conv}\,\{\pm u_i \boldsymbol{e}_i : 1 \le i \le n\} \subseteq K.$$

Hence, $\mathrm{P}(I_n, n^{-1}\boldsymbol{u}) \subset K$. For the remaining cardinality bound observe that $(2\,u_i+1) < (2\lfloor u_i/n \rfloor)+1)\,3n$ and so (4-12) implies

$$|K \cap \mathbb{Z}^n| \le \prod_{i=1}^{n}(2\,\lfloor u_i \rfloor + 1) < (3n)^n \prod_{i=1}^{n}(2\lfloor u_i/n \rfloor) + 1) = (3n)^n |\mathrm{P}(I_n, n^{-1}\boldsymbol{u})|. \qquad \square$$

For instance, for $p \ge 1$ and a positive vector $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_n)^{\mathsf{T}} \in \mathbb{R}^n_{>0}$ let

$$B_n^p(\boldsymbol{\alpha}) = \Big\{ \boldsymbol{x} \in \mathbb{R}^n : \sum_{i=1}^{n} \alpha_i^{-p} |x_i|^p \le 1 \Big\}$$

be the scaled l_p-ball in $\mathbb{R}^n$. Then, by the preceding argument we get

$$\mathrm{P}(I_n, n^{-1/p}\boldsymbol{\alpha}) \subset B_n^p(\boldsymbol{\alpha}) \subset \mathrm{P}(I_n, \boldsymbol{\alpha}).$$

Assuming $\alpha_1 \ge \alpha_2 \ge \cdots \ge \alpha_n$ we also have $\lambda_i(B_n^p(\boldsymbol{\alpha}), \mathbb{Z}^n) = \alpha_i^{-1}$, and so the GAP corresponds to the vectors $\alpha_i \boldsymbol{e}_i \in K$ attaining the successive minima (compare Remark 4.3).

Finally, we remark that for a symmetric planar convex body K there always exists vectors $\boldsymbol{a}_1, \boldsymbol{a}_2 \in \mathbb{Z}^2$ such that $\boldsymbol{a}_i \in \lambda_i(K, \mathbb{Z}^2)\,K$, $i = 1, 2$, and $\boldsymbol{a}_1, \boldsymbol{a}_2$ build a basis of $\mathbb{Z}^2$. Setting $A = (\boldsymbol{a}_1, \boldsymbol{a}_2)$, it can be shown (see [Berg 2018, Theorem 4.21]) that there exists a GAP $\mathrm{P}(A, \boldsymbol{u}) \subset K$ satisfying

$$K \cap \mathbb{Z}^n \subseteq \mathrm{P}(A, 3\,\boldsymbol{u}).$$

It is not known, however, whether the dilation factor 3 is optimal.

References

[Alexander et al. 2017] M. Alexander, M. Henk, and A. Zvavitch, "A discrete version of Koldobsky's slicing inequality", *Israel J. Math.* **222**:1 (2017), 261–278. MR Zbl

[Artstein-Avidan et al. 2015] S. Artstein-Avidan, A. Giannopoulos, and V. D. Milman, *Asymptotic geometric analysis, I*, Math. Surv. Monogr. **202**, Amer. Math. Soc., Providence, RI, 2015. MR Zbl

[Bárány and Vershik 1992] I. Bárány and A. M. Vershik, "On the number of convex lattice polytopes", *Geom. Funct. Anal.* **2**:4 (1992), 381–393. MR Zbl

[Berg 2018] S. L. Berg, *Lattice points in convex bodies: counting and approximating*, Ph.D. thesis, Technische Universität Berlin, 2018, Available at https://tinyurl.com/bergconv.

[Betke et al. 1993] U. Betke, M. Henk, and J. M. Wills, "Successive-minima-type inequalities", *Discrete Comput. Geom.* **9**:2 (1993), 165–175. MR Zbl

[Cassels 1959] J. W. S. Cassels, *An introduction to the geometry of numbers*, Grundlehren der Math. Wissenschaften **99**, Springer, 1959. MR Zbl

[Gruber and Lekkerkerker 1987] P. M. Gruber and C. G. Lekkerkerker, *Geometry of numbers*, 2nd ed., North-Holland Math. Library **37**, North-Holland, Amsterdam, 1987. MR Zbl

[Håstad and Lagarias 1990] J. Håstad and J. C. Lagarias, "Simultaneously good bases of a lattice and its reciprocal lattice", *Math. Ann.* **287**:1 (1990), 163–174. MR Zbl

[Henk 2002] M. Henk, "Successive minima and lattice points", *Rend. Circ. Mat. Palermo* (2) *Suppl.* **70**:1 (2002), 377–384. MR Zbl

[Hernández Cifre et al. 2018] M. A. Hernández Cifre, D. Iglesias, and J. Yepes Nicolás, "On a discrete Brunn–Minkowski type inequality", *SIAM J. Discrete Math.* **32**:3 (2018), 1840–1856. MR Zbl

[Lagarias et al. 1990] J. C. Lagarias, H. W. Lenstra, Jr., and C.-P. Schnorr, "Korkin–Zolotarev bases and successive minima of a lattice and its reciprocal lattice", *Combinatorica* **10**:4 (1990), 333–348. MR Zbl

[Malikiosis 2010] R. Malikiosis, "An optimization problem related to Minkowski's successive minima", *Discrete Comput. Geom.* **43**:4 (2010), 784–797. MR Zbl

[Malikiosis 2012] R.-D. Malikiosis, "A discrete analogue for Minkowski's second theorem on successive minima", *Adv. Geom.* **12**:2 (2012), 365–380. MR Zbl

[Maze 2010] G. Maze, "Some inequalities related to the Seysen measure of a lattice", *Linear Algebra Appl.* **433**:8-10 (2010), 1659–1665. MR Zbl

[Ryabogin et al. 2017] D. Ryabogin, V. Yaskin, and N. Zhang, "Unique determination of convex lattice sets", *Discrete Comput. Geom.* **57**:3 (2017), 582–589. MR Zbl

[Schneider 2014] R. Schneider, *Convex bodies: the Brunn–Minkowski theory*, 2nd expanded ed., Encycl. Math. Appl. **151**, Cambridge Univ. Press, 2014. MR Zbl

[Seysen 1993] M. Seysen, "Simultaneous reduction of a lattice basis and its reciprocal basis", *Combinatorica* **13**:3 (1993), 363–376. MR Zbl

[Tao and Vu 2006] T. Tao and V. Vu, *Additive combinatorics*, Cambridge Studies in Adv. Math. **105**, Cambridge Univ. Press, 2006. MR Zbl

[Tao and Vu 2008] T. Tao and V. Vu, "John-type theorems for generalized arithmetic progressions and iterated sumsets", *Adv. Math.* **219**:2 (2008), 428–449. MR Zbl

Received 14 Apr 2019. Revised 27 May 2019.

SÖREN LENNART BERG:

berg@math.tu-berlin.de
Institut für Mathematik, Technische Universität Berlin, Berlin, Germany

MARTIN HENK:

henk@math.tu-berlin.de
Institut für Mathematik, Technische Universität Berlin, Berlin, Germany

Moscow Journal of Combinatorics and Number Theory

msp.org/moscow

See inside back cover or msp.org/moscow for submission instructions.

The subscription price for 2019 is US $310/year for the electronic version, and $365/year (+$20, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Moscow Journal of Combinatorics and Number Theory (ISSN 2640-7361 electronic, 2220-5438 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

MJCNT peer review and production are managed by EditFlow® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

Moscow Journal of Combinatorics and Number Theory
vol. 8 no. 4 2019