The Subspace Flatness Conjecture and Faster Integer Programming

Victor Reis
University of Washington
Seattle, United States
voreis@uw.edu

Thomas Rothvoss
University of Washington
Seattle, United States
rothvoss@uw.edu

Abstract—In a seminal paper, Kannan and Lovász (1988) considered a quantity $\mu_{KL}(\Lambda, K)$ which denotes the best volume-based lower bound on the covering radius $\mu(\Lambda, K)$ of a convex body K with respect to a lattice Λ. Kannan and Lovász proved that $\mu(\Lambda, K) \leq n \cdot \mu_{KL}(\Lambda, K)$ and the Subspace Flatness Conjecture by Dadush (2012) claims a $O(\log(2n))$ factor suffices, which would match the lower bound from the work of Kannan and Lovász. We settle this conjecture up to a constant in the exponent by proving that $\mu(\Lambda, K) \leq O(\log^3(2n)) \cdot \mu_{KL}(\Lambda, K)$. Our proof is based on the Reverse Minkowski Theorem due to Regev and Stephens-Davidowitz (2017). Following the work of Dadush (2012, 2019), we obtain a $(\log(2n))^{O(n)}$-time randomized algorithm to solve integer programs in n variables. Another implication of our main result is a near-optimal flatness constant of $O(n \log^3(2n))$.

Index Terms—integer programming

I. Introduction

Lattices are fundamental objects studied in various areas of mathematics and computer science. Here, a lattice Λ is a discrete subgroup of $\mathbb{R}^n$. If $B \in \mathbb{R}^{n \times k}$ is a matrix with linearly independent columns $b_1, \dots, b_k$, then we may write a lattice in the form $\Lambda(B) := \{\sum_{i=1}^k y_i b_i : y_i \in \mathbb{Z}\}$. In mathematics, lattices are the central object of study in the geometry of numbers with many applications for example to number theory, see e.g. [KL88]. On the computer science side, lattices found applications for example in lattice-based cryptography [Reg09b] and cryptanalysis [Odl90]. One of the most important algorithms at least in this area is the LLL-algorithm by Lenstra, Lenstra and Lovász [LLL82] which finds an approximately orthogonal basis for a given lattice in polynomial time. One of the consequences of the LLL-reduction is a polynomial time $2^{n/2}$-approximation algorithm for the problem of finding a (nonzero) shortest vector in a lattice. We should also mention that the problem of finding a shortest vector in any norm can be solved in time $2^{O(n)}$ using a variation of the sieving algorithm [AKS01] while in the Euclidean norm, even the closest vector to any given target vector can be found in time $2^{O(n)}$ [MV13]. A more general problem with tremendous applications in combinatorial optimization and operations research is the one of finding an integer point in an arbitrary convex body or polytope. Lenstra [Len83] used the then-recent lattice basis reduction algorithm to solve any n-variable integer program in time $2^{O(n^2)}$. This was later improved by Kannan [Kan87] to $n^{O(n)}$ and then by Dadush [Dad12] and by Dadush, Eisenbrand and Rothvoss [DER22] to $2^{O(n)}n^n$.

A parameter appearing in the geometry of numbers is the covering radius

$$\mu(\Lambda, K) := \min\left\{r \geq 0 \mid \Lambda + rK = \mathrm{span}(\Lambda)\right\}$$

of a lattice $\Lambda \subseteq \mathbb{R}^n$ with respect to a compact convex set $K \subseteq \mathbb{R}^n$ with $\mathrm{span}(\Lambda) = \mathrm{affine.hull}(K)$. This quantity seems to be substantially harder computationally, in the sense that the question whether $\mu(\Lambda, K)$ is at least/at most a given threshold seems to be neither in **NP** nor in **coNP**. In terms of approximating $\mu(\Lambda, K)$, one can quickly observe that one has the lower bound of $\mu(\Lambda, K) \geq (\frac{\det(\Lambda)}{\mathrm{Vol}_n(K)})^{1/n}$, simply because for $r < (\frac{\det(\Lambda)}{\mathrm{Vol}_n(K)})^{1/n}$, the average density of the translates $\Lambda + rK$ is less than 1. However, this lower bound may be arbitrarily far off the real covering radius, for example if $\Lambda = \mathbb{Z}^2$ and $K = [-\frac{1}{M}, \frac{1}{M}] \times [-M, M]$ with $M \to \infty$. On the other hand, for any subspace $W \subseteq \mathbb{R}^n$ one trivially has $\mu(\Lambda, K) \geq \mu(\Pi_W(\Lambda), \Pi_W(K))$, where Π_W is the orthogonal projection into W. Hence, following Kannan and Lovász [KL88], one might instead consider the best volume based lower bound for any projection, i.e.

$$\mu_{KL}(\Lambda, K) := \max_{\substack{W \subseteq \mathrm{span}(\Lambda) \text{ subspace} \\ d := \dim(W)}} \Big(\frac{\det(\Pi_W(\Lambda))}{\mathrm{Vol}_d(\Pi_W(K))}\Big)^{1/d}$$

Kannan and Lovász [KL88] indeed provide an upper bound of

$$\mu_{KL}(\Lambda, K) \leq \mu(\Lambda, K) \leq n \cdot \mu_{KL}(\Lambda, K)$$

On the other hand, they also construct a simplex $K \subseteq \mathbb{R}^n$ for which $\mu(\mathbb{Z}^n, K) \geq \Omega(\log(2n)) \cdot \mu_{KL}(\mathbb{Z}^n, K)$ holds. Dadush [Dad12] states the following conjecture, attributing it to Kannan and Lovász [KL88]:

Conjecture 1 (Subspace Flatness Conjecture). For any full rank lattice $\Lambda \subseteq \mathbb{R}^n$ and any convex body $K \subseteq \mathbb{R}^n$ one has

$$\mu_{KL}(\Lambda, K) \leq \mu(\Lambda, K) \leq O(\log(2n)) \cdot \mu_{KL}(\Lambda, K)$$

Supported by NSF CAREER grant 1651861 and a David & Lucile Packard Foundation Fellowship.

Dadush also realized the tremendous implications of this conjecture to optimization and showed that it would imply a $O(\log(2n))^n$-time algorithm to solve n-variable integer programs, assuming that the subspace W attaining $\mu_{KL}(\Lambda, K)$ could also be found in the same time. Later, Dadush and Regev [DR16] conjectured a Reverse Minkowski-type Inequality, which intuitively says that any lattice without dense sublattices should contain only few short vectors. Among other applications, they proved that this conjecture would imply Conjecture 1 (with some logarithmic loss) at least for the case that K is an ellipsoid. The conjecture of [DR16] was then resolved by Regev and Stephens-Davidowitz [RS17] with a rather ingenious proof. More precisely, they prove the following:

Theorem 1 (Reverse Minkowski Theorem [RS17]). Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice that satisfies $\det(\Lambda') \geq 1$ for all sublattices $\Lambda' \subseteq \Lambda$. Then for a large enough constant $C > 0$ and $s = C\log(2n)$ one has $\rho_{1/s}(\Lambda) \leq \frac{3}{2}$.

Here, one has $\rho_t(x) := \exp(-\pi\|x/t\|_2^2)$ where $t > 0$ and for a discrete set $S \subseteq \mathbb{R}^n$ we abbreviate $\rho_t(S) := \sum_{x\in S}\rho_t(x)$. To understand the power of this result compared to classical arguments, note that from $\det(\Lambda') \geq 1$ for all $\Lambda' \subseteq \Lambda$ one can derive that each vector $x \in \Lambda \setminus \{\mathbf{0}\}$ has length $\|x\|_2 \geq 1$ and so by a standard packing argument we know that for any $r \geq 1$ one has $|\Lambda \cap rB_2^n| \leq (3r)^n$, which is exponential in n. On the other hand, again under the assumption that $\det(\Lambda') \geq 1$ for all $\Lambda' \subseteq \Lambda$, the Reverse Minkowski Theorem implies that $|\Lambda \cap rB_2^n| \leq \exp(\Theta(\log^2(2n)) \cdot r^2)$ which is quasi-polynomial in n. Also, [RS17] tighten the reduction to the Subspace Flatness Conjecture and show that it holds for any ellipsoid with a factor of $O(\log^{3/2}(2n))$. While for any convex body K, there is an ellipsoid E and a center c so that $c + E \subseteq K \subseteq c + nE$ [Joh48], this factor of n is the best possible, and hence there does not seem to be a blackbox reduction from the general case of Conjecture 1 to the one of ellipsoids.

A. Our contribution

Our main result is as follows:

Theorem 2. For any full rank lattice $\Lambda \subseteq \mathbb{R}^n$ and any convex body $K \subseteq \mathbb{R}^n$ one has

$$\mu_{KL}(\Lambda, K) \leq \mu(\Lambda, K) \leq O(\log^3(2n)) \cdot \mu_{KL}(\Lambda, K).$$

We will break the proof into two parts that can be found in Section IV. Our result is constructive in the following sense:

Theorem 3. Given a full rank lattice $\Lambda := \Lambda(B)$ and a convex body $K \subseteq \mathbb{R}^n$ with $c + r_0B_2^n \subseteq K \subseteq r_1B_2^n$, there is a randomized algorithm to find a subspace $W \subseteq \mathbb{R}^n$ with $d := \dim(W)$ so that

$$\mu(\Lambda, K) \leq O(\log^4(2n)) \cdot \Big(\frac{\det(\Pi_W(\Lambda))}{\mathrm{Vol}_d(\Pi_W(K))}\Big)^{1/d}.$$

The running time of that algorithm is $2^{O(n)}$ times a polynomial in $\log(\frac{1}{r_0})$, $\log(r_1)$ and in the encoding length of B.

Here, a separation oracle suffices for K. See Section V for a proof. Following the framework layed out by Dadush [Dad12], this implies a faster algorithm to find a lattice point in a convex body:

Theorem 4. Given a convex body $K \subseteq rB_2^n$ represented by a separation oracle and a lattice $\Lambda = \Lambda(B)$, there is a randomized algorithm that with high probability finds a point in $K \cap \Lambda$ or correctly decides that there is none. The running time is $(\log(2n))^{O(n)}$ times a polynomial in $\log(r)$ and the encoding length of B.

The proof can be found in Section VI. Applying Theorem 4 to integer programming we obtain the following:

Theorem 5. Given $A \in \mathbb{Q}^{m\times n}$, $b \in \mathbb{Q}^m$ and $c \in \mathbb{Q}^n$, the integer linear program $\max\{c^Tx \mid Ax \leq b, x \in \mathbb{Z}^n\}$ can be solved in time $(\log(2n))^{O(n)}$ times a polynomial in the encoding length of A, b and c.

An immediate consequence of our main result (Theorem 2) is that K can be replaced by a larger symmetric body without decreasing the covering radius significantly:

Theorem 6. For any full rank lattice $\Lambda \subseteq \mathbb{R}^n$ and any convex body $K \subseteq \mathbb{R}^n$ one has

$$\mu(\Lambda, K - K) \leq \mu(\Lambda, K) \leq O(\log^3(2n)) \cdot \mu(\Lambda, K - K).$$

Another consequence is that the flatness constant in dimension n is bounded by $O(n\log^3(2n))$, which is an improvement from the previously known bound of $O(n^{4/3}\log^{O(1)}(2n))$ obtained by combining the result of Rudelson [Rud98] with [BLPS99].

Theorem 7. For any convex body $K \subseteq \mathbb{R}^n$ and any full rank lattice $\Lambda \subseteq \mathbb{R}^n$ one has

$$\mu(\Lambda, K) \cdot \lambda_1(\Lambda^*, (K - K)^\circ) \leq O(n\log^3(2n)).$$

It is well known that Theorem 7 can also be rephrased in the following convenient form:

Corollary 8. Let $K \subseteq \mathbb{R}^n$ be a convex body with $K \cap \mathbb{Z}^n = \emptyset$. Then there is a vector $c \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$ so that at most $O(n\log^3(2n))$ many hyperplanes of the form $\langle c, x\rangle = \delta$ with $\delta \in \mathbb{Z}$ intersect K.

We will prove Theorem 6, Theorem 7 and Corollary 8 in Section VII.

II. Preliminaries

In this section, we introduce the tools that we rely on later. We write $A \lesssim B$ if there is a universal constant

$C > 0$ so that $A \leq C \cdot B$ holds. We write $A \asymp B$ if both $A \lesssim B$ and $B \lesssim A$ hold.

A. Lattices

For a lattice $\Lambda = \Lambda(B)$ given by a matrix $B \in \mathbb{R}^{n \times k}$ with linearly independent columns, we define the rank as $\text{rank}(\Lambda) := k = \dim(\text{span}(\Lambda))$ and the determinant as $\det(\Lambda) = \sqrt{\det_k(B^T B)}$. A lattice $\Lambda \subseteq \mathbb{R}^n$ with $\text{rank}(\Lambda) = n$ has full rank. For a lattice $\Lambda \subseteq \mathbb{R}^n$, we define the dual lattice as $\Lambda^* := \{x \in \text{span}(\Lambda) \mid \langle x, y\rangle \in \mathbb{Z}\ \forall y \in \Lambda\}$. Recall that $\det(\Lambda) \cdot \det(\Lambda^*) = 1$. A consequence of the Poisson Summation Formula is as follows:

Lemma 9. For any full rank lattice $\Lambda \subseteq \mathbb{R}^n$, vector $u \in \mathbb{R}^n$ and any $s > 0$ one has

$$|\rho_s(\Lambda + u) - s^n \det(\Lambda^*)| \leq s^n \det(\Lambda^*) \cdot \rho_{1/s}(\Lambda^* \setminus \{\mathbf{0}\}).$$

A set $K \subseteq \mathbb{R}^n$ is called a convex body if it is convex, compact (i.e. bounded and closed) and has a non-empty interior $\text{int}(K)$. A set Q is called symmetric if $-Q = Q$. For a symmetric convex set Q, the norm $\|x\|_Q$ is defined as the least scaling $r \geq 0$ so that $x \in rQ$. For a lattice Λ and a symmetric convex body Q we denote the length of the shortest vector by

$$\lambda_1(\Lambda, Q) := \min_{x \in \Lambda \setminus \{\mathbf{0}\}} \|x\|_Q.$$

Later we will also need a classical bound on short vectors in a lattice:

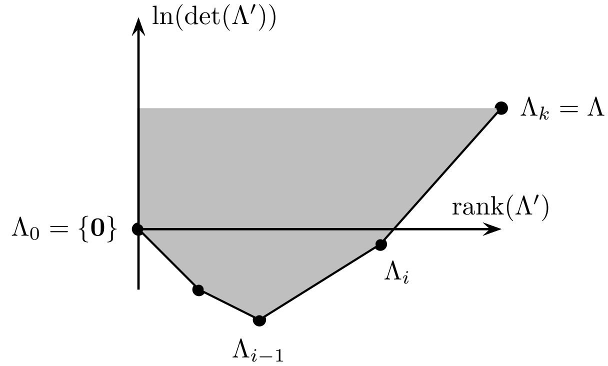
Theorem 10 (Minkowski's First Theorem). Let $\Lambda \subseteq \mathbb{R}^n$ be a full rank lattice and $Q \subseteq \mathbb{R}^n$ be a symmetric convex body. Then $\lambda_1(\Lambda, Q) \leq 2\left(\frac{\det(\Lambda)}{\text{Vol}_n(Q)}\right)^{1/n}$.

We recommend the excellent notes of Regev [Reg09a] for background.

B. Stable lattices and the canonical filtration

A subspace $W \subseteq \mathbb{R}^n$ is a lattice subspace of a lattice $\Lambda \subseteq \mathbb{R}^n$ if $\text{span}(W \cap \Lambda) = W$. Similarly, a sublattice $\Lambda' \subseteq \Lambda$ is called primitive if there is a subspace W with $\Lambda \cap W = \Lambda'$. For a lattice Λ and a primitive sublattice $\Lambda' \subseteq \Lambda$, we define the quotient lattice as $\Lambda/\Lambda' := \Pi_{\text{span}(\Lambda')^\perp}(\Lambda)$. In many ways one can imagine that the quotient operation factors Λ into two lattices Λ' and Λ/Λ'. In particular Λ' and Λ/Λ' are orthogonal and $\det(\Lambda) = \det(\Lambda') \cdot \det(\Lambda/\Lambda')$.

A lattice $\Lambda \subseteq \mathbb{R}^n$ is called stable if $\det(\Lambda) = 1$ and $\det(\Lambda') \geq 1$ for all sublattices $\Lambda' \subseteq \Lambda$. That means a stable lattice does not contain any sublattice that is denser than the lattice itself. One can easily verify that for example $\mathbb{Z}^n$ is stable. We denote $\text{nd}(\Lambda) := \det(\Lambda)^{1/\text{rank}(\Lambda)}$ as the normalized determinant. One can prove that the extreme points of the 2-dimensional convex hull of the points $\{(\text{rank}(\Lambda'), \ln(\det(\Lambda'))) \mid \text{sublattice } \Lambda' \subseteq \Lambda\}$ correspond to a unique chain of nested sublattices $\{\mathbf{0}\} = \Lambda_0 \subset \Lambda_1 \subset \ldots \subset \Lambda_k = \Lambda$. That chain is called the canonical filtration. It is useful to observe that each Λ_i in this sequence is the unique densest sublattice of Λ with given dimension $\text{rank}(\Lambda_i)$. Moreover, the quotient lattices Λ_i/Λ_{i-1} are all scalars of a stable lattice and one can prove that $\text{nd}(\Lambda_i/\Lambda_{i-1})$ are strictly increasing in i. We refer to the thesis of [Ste17] for details.



It will be useful to replace the canonical filtration by an approximate filtration where the normalized determinants grow exponentially. We make the following definition:

Definition 11. We call a lattice $\Lambda \subseteq \mathbb{R}^n$ t-stable with $t \geq 1$ if the following holds:

(I) For any sublattice $\tilde{\Lambda} \subseteq \Lambda$ one has $\text{nd}(\tilde{\Lambda}) \geq t^{-1}$.
(II) For any sublattice $\tilde{\Lambda} \subseteq \Lambda^*$ one has $\text{nd}(\tilde{\Lambda}) \geq t^{-1}$.

Note that a lattice is 1-stable if and only if it is stable. We can similarly define t-stable filtrations:

Definition 12. Given a lattice $\Lambda \subseteq \mathbb{R}^n$, we call a sequence $\{\mathbf{0}\} = \Lambda_0 \subset \ldots \subset \Lambda_k = \Lambda$ a t-stable filtration of Λ if the following holds:

(a) The normalized determinants $r_i := \text{nd}(\Lambda_i/\Lambda_{i-1})$ satisfy $r_1 < \ldots < r_k$.
(b) The lattices $\frac{1}{r_i}(\Lambda_i/\Lambda_{i-1})$ are t-stable for all $i = 1, \ldots, k$.

We call a t-stable filtration well-separated if additionally the following holds:

(c) One has $r_i \leq \frac{1}{2} r_{i+2}$ for all $i = 1, \ldots, k-2$.

For example, the canonical filtration is 1-stable. It turns out we can make any t-stable filtration well-separated:

Theorem 13. Given a lattice $\Lambda \subseteq \mathbb{R}^n$ and a t-stable filtration $\{\mathbf{0}\} = \Lambda_0 \subset \ldots \subset \Lambda_k = \Lambda$, in polynomial time we can compute a $2t$-stable well-separated filtration $\{\mathbf{0}\} = \tilde{\Lambda}_0 \subseteq \ldots \subseteq \tilde{\Lambda}_{\tilde{k}} = \Lambda$.

We defer the proof to Appendix A. Using the canonical filtration as input to Theorem 13 yields:

Corollary 14. For any lattice $\Lambda \subseteq \mathbb{R}^n$, there exists a 2-stable well-separated filtration $\{\mathbf{0}\} = \Lambda_0 \subset \ldots \subset \Lambda_k = \Lambda$.

We collect a few more properties of t-stable lattices:

Lemma 15. There is a universal constant $C > 0$ so that the following holds: Let Λ be a t-stable lattice for $t \geq 1$. Then for $s = C\log(2n)$ one has

(a) Λ^* is t-stable.
(b) $\rho_{1/(st)}(\Lambda) \leq \frac{3}{2}$.
(c) For any $u \in \mathbb{R}^n$ one has $\frac{\rho_{st}(\Lambda+u)}{\rho_{st}(\Lambda)} \geq \frac{1}{3}$.

Proof. (a) is immediate from the definition of t-stability. Next, let $s = C\log(2n)$ be the parameter from Theorem 1. For (b), we can see that for any $\Lambda' \subseteq t\Lambda$ one has $\det(\Lambda') \geq 1$ and so the Reverse Minkowski Theorem (Theorem 1) applies to the lattice $t\Lambda$. Then $\rho_{1/(st)}(\Lambda) = \rho_{1/s}(t\Lambda) \leq \frac{3}{2}$ which gives (b). For (c), applying Lemma 9 twice gives

$$\begin{aligned}\frac{\rho_{st}(\Lambda+u)}{\rho_{st}(\Lambda)} &\geq \frac{(st)^n \det(\Lambda^*)\cdot(1-\rho_{1/(st)}(\Lambda^*\setminus\{\mathbf{0}\}))}{(st)^n \det(\Lambda^*)\cdot(1+\rho_{1/(st)}(\Lambda^*\setminus\{\mathbf{0}\}))} \\ &\overset{(a)+(b)}{\geq} \frac{1-\frac{1}{2}}{1+\frac{1}{2}} = \frac{1}{3}. \quad \square\end{aligned}$$

C. The ℓ-value and volume estimates

We review a few results from convex geometry that can all be found in the textbook by Artstein-Avidan, Giannopoulos and Milman [AAGM15]. We denote $B_2^n := \{x \in \mathbb{R}^n \mid \|x\|_2 \leq 1\}$ and $S^{n-1} := \{x \in \mathbb{R}^n \mid \|x\|_2 = 1\}$ as the Euclidean ball and sphere, resp. Let $\nu_n := \mathrm{Vol}_n(B_2^n)$. The relative interior of K is $\mathrm{rel.int}(K) := \{x \in K \mid \exists \varepsilon > 0 : (x + \varepsilon \cdot B_2^n) \cap \mathrm{affine.hull}(K) \subseteq K\}$.

We define the mean width of a convex body K as $w(K) := \mathbb{E}_{\theta\sim S^{n-1}}[\max\{\langle \theta, x-y\rangle : x, y \in K\}]$. For a compact convex $K \subseteq \mathbb{R}^n$ with $\mathbf{0} \in \mathrm{rel.int}(K)$ we denote its polar by $K^\circ := \{y \in \mathrm{span}(K) : \langle x, y\rangle \leq 1 \ \forall x \in K\}$. Recall the following basic facts.

Lemma 16 (Properties of polarity). For two convex bodies $K, Q \subseteq \mathbb{R}^n$ with $\mathbf{0} \in \mathrm{int}(K)$ and $\mathbf{0} \in \mathrm{int}(Q)$ the following holds:

(a) One has $(K^\circ)^\circ = K$.
(b) For any subspace $F \subseteq \mathbb{R}^n$ one has $\Pi_F(K)^\circ = K^\circ \cap F$.
(c) One has $(K \cap Q)^\circ = \mathrm{conv}(K^\circ \cup Q^\circ)$.
(d) One has $(-K)^\circ = -K^\circ$.

We write $N(\mathbf{0}, I_n)$ as the standard Gaussian distribution on $\mathbb{R}^n$. The ℓ-value of a symmetric convex $Q \subseteq \mathbb{R}^n$ is defined as

$$\ell_Q = \mathop{\mathbb{E}}_{x\sim N(\mathbf{0},I_n)}[\|x\|_Q^2]^{1/2}$$

One may think of ℓ_Q as the "average thinness" of Q. It turns out that the ℓ-value is also related to the mean width. To see this, note that $\|\cdot\|_{Q^\circ}$ is the dual norm to $\|\cdot\|_Q$, i.e. for all $x \in \mathbb{R}^n$ one has $\|x\|_{Q^\circ} = \max\{\langle x, y\rangle : y \in Q\}$ Then

$$\begin{aligned}\ell_{Q^\circ} &= \mathop{\mathbb{E}}_{x\sim N(\mathbf{0},I_n)}[\|x\|_{Q^\circ}^2]^{1/2} \\ &= \mathop{\mathbb{E}}_{\boldsymbol{x}\sim N(\mathbf{0},I_n)}\left[\max\{\langle x, y\rangle^2 : y \in Q\}\right]^{1/2}\end{aligned}$$

We can see that the right hand side of (1) almost matches the definition of $w(Q)$. In fact, one can prove:

Lemma 17. For any symmetric convex body $Q \subseteq \mathbb{R}^n$ one has $\ell_{Q^\circ} \asymp \sqrt{n}\cdot w(Q)$.

For a positive semidefinite matrix Σ we write $N(\mathbf{0}, \Sigma)$ as the Gaussian with mean $\mathbf{0}$ and covariance matrix Σ and for a subspace $U \subseteq \mathbb{R}^n$ we write I_U as the identity matrix on that subspace. Occasionally we will need to refer to the ℓ-value of a compact symmetric convex set Q that is not necessarily full-dimensional. In that case we extend the definition to $\ell_Q = \mathbb{E}_{x\sim N(\mathbf{0},I_{\mathrm{span}(Q)})}[\|x\|_Q^2]^{1/2}$.

We say that a symmetric convex body Q is in ℓ-position if $\ell_Q \cdot \ell_{Q^\circ} \leq O(n\log(2n))$. One of the most powerful tools in convex geometry is that every symmetric convex body can indeed be brought into ℓ-position:

Theorem 18 (Figiel, Tomczak-Jaegerman, Pisier). For any symmetric convex body $Q \subseteq \mathbb{R}^n$, there is an invertible linear map $T : \mathbb{R}^n \to \mathbb{R}^n$ so that $\ell_{T(Q)} \cdot \ell_{(T(Q))^\circ} \leq O(n\log(2n))$.

By Lemma 17, the conclusion of Theorem 18 is equivalent to $w(T(Q)) \cdot w(T(Q)^\circ) \leq O(\log(2n))$. Moreover one can prove that for any symmetric convex body Q one has $w(Q)\cdot w(Q^\circ) \gtrsim w(B_2^n)^2 \gtrsim 1$. Then one can interpret Theorem 18 as every symmetric convex body can be linearly transformed so that in terms of mean width and average thinness it is within a $O(\log(2n))$-factor of the Euclidean ball. For the sake of comparison, we note that the bound that could be obtained via the more classical John's Theorem [Joh48] would be of the order of $\sqrt{n}$. We would like to point out that Theorem 18 is only known for symmetric convex bodies, and it is open to what extent it generalizes to the non-symmetric case.

We state two estimates concerning monotonicity of the ℓ-value that will be crucial for our later arguments:

Lemma 19. Let $Q \subseteq \mathbb{R}^n$ be a symmetric convex body. Then for any subspace $U \subseteq \mathbb{R}^n$, one has $\ell_{Q\cap U} \leq \ell_Q$.

Proof. Indeed, one has

$$\begin{aligned}\ell_Q^2 &= \mathbb{E}_{z\sim N(\mathbf{0},I_U)}\left[\mathbb{E}_{y\sim N(\mathbf{0},I_{U^\perp})}[\|z+y\|_Q^2]\right] \\ &\geq \mathbb{E}_{z\sim N(\mathbf{0},I_U)}\Big[\big\|z + \underbrace{\mathbb{E}_{y\sim N(\mathbf{0},I_{U^\perp})}[y]}_{=\mathbf{0}}\big\|_Q^2\Big] = \ell_{Q\cap U}^2,\end{aligned}$$

where the inequality follows from Jensen's inequality and the convexity of $y \mapsto \|z+y\|_Q^2$. $\square$

Lemma 20. Let $Q \subseteq \mathbb{R}^n$ be a symmetric convex body. For any subspaces $V \subset W \subseteq \mathbb{R}^n$, one has $\ell_{\Pi_{V^\perp}(Q\cap W)} \leq \ell_Q$.

Proof. We have $\ell_{\Pi_{V^\perp}(Q\cap W)} \leq \ell_{Q\cap W\cap V^\perp} \leq \ell_Q$ using that $\Pi_{V^\perp}(Q\cap W) \supseteq Q\cap W\cap V^\perp$ and using Lemma 19. $\square$

The following classical result says that among all bodies with identical volume, the Euclidean ball minimizes the mean width.

Theorem 21 (Urysohn Inequality I). For any convex body $K \subseteq \mathbb{R}^n$ one has

$$w(K) \geq 2 \cdot \Big(\frac{\mathrm{Vol}_n(K)}{\mathrm{Vol}_n(B_2^n)}\Big)^{1/n}.$$

A slight variant of this inequality will be handy for us:

Corollary 22 (Urysohn Inequality II). For any symmetric convex body $Q \subseteq \mathbb{R}^n$ one has $\mathrm{Vol}_n(Q)^{1/n} \lesssim \frac{\ell_{Q^\circ}}{n}$.

Proof. Applying Urysohn's Inequality I we obtain

$$\mathrm{Vol}_n(Q)^{1/n} \overset{\text{Thm 21}}{\lesssim} w(Q) \cdot \underbrace{\mathrm{Vol}_n(B_2^n)^{1/n}}_{\lesssim 1/\sqrt{n}} \overset{\text{Lem 17}}{\lesssim} \frac{\ell_{Q^\circ}}{n}$$

Here we use in particular that $\mathrm{Vol}_n(B_2^n) \leq (\frac{2e}{\sqrt{n}})^n$. □

The following can be found e.g. in [AAGM15], Chapter 8:

Theorem 23 (Blaschke-Santaló-Bourgain-Milman). For any symmetric convex body $K \subseteq \mathbb{R}^n$ one has

$$C_1^n \nu_n^2 \leq \mathrm{Vol}_n(K) \cdot \mathrm{Vol}_n(K^\circ) \leq C_2^n \nu_n^2$$

where $C_1, C_2 > 0$ are constants.

Let $b(K) := \frac{1}{\mathrm{Vol}_n(K)} \int_K x \, dx$ denote the barycenter or centroid of a convex body K. We will run into the issue that we need to control the volume of a non-symmetric convex body K, but Theorem 18 only holds for symmetric ones. A popular strategy in convex geometry is to translate K so that $b(K) = \mathbf{0}$ and then consider the inner symmetrizer $K \cap -K$ which by construction is a symmetric convex body contained in K which captures much of the geometry of K. For example a classical result by Milman and Pajor says that $\mathrm{Vol}_n(K \cap -K) \geq 2^{-n} \mathrm{Vol}_n(K)$. However, in our case we need a more powerful estimate that was proven by Vritsiou [Vri23] in the context of showing the existence of regular M-ellipsoids for non-symmetric convex bodies.

Proposition 24 ([Vri23], Corollary 11). Let $K \subseteq \mathbb{R}^n$ be a convex body so that $b(K) = \mathbf{0}$ and let $F \subseteq \mathbb{R}^n$ be a d-dimensional subspace. Then

$$\mathrm{Vol}_d(\Pi_F(K))^{1/d} \lesssim \Big(\frac{n}{d}\Big)^5 \cdot \log\Big(\frac{en}{d}\Big)^2 \cdot \mathrm{Vol}_d(\Pi_F(K \cap -K))^{1/d}.$$

On a previous preprint, we had shown an inequality with better exponent when the body is centered so that $b(K^\circ) = \mathbf{0}$, i.e. the origin is the Santaló point of K. However, algorithmically the barycenter is much easier to compute and the exponent only affects the implicit universal constant in our main result, hence we choose to work with Vritsiou's estimate. For the interested reader, the bound with the Santaló point as center can be found in v2 on arXiv and also independently in [Vri23].

We prove a custom-tailored inequality for later:

Lemma 25. Let $K \subseteq \mathbb{R}^n$ be a convex body with $b(K) = \mathbf{0}$ and let $F \subseteq \mathbb{R}^n$ be a d-dimensional subspace. Then

$$(\mathrm{Vol}_d(\Pi_F(K)))^{1/d} \lesssim \Big(\frac{n}{d}\Big)^6 \cdot \frac{\ell_{(K \cap -K)^\circ}}{d}.$$

Proof. We abbreviate $K_{\mathrm{sym}} := K \cap -K$. Using the volume estimate from Proposition 24 with the assumption that the barycenter of K lies at the origin, we obtain

$$\begin{aligned}
(\mathrm{Vol}_d(\Pi_F(K)))^{1/d} &\overset{\text{Prop 24}}{\lesssim} \Big(\frac{n}{d}\Big)^6 \cdot (\mathrm{Vol}_d(\Pi_F(K_{\mathrm{sym}})))^{1/d} \\
&\overset{\text{Cor 22}}{\lesssim} \Big(\frac{n}{d}\Big)^6 \cdot \frac{\ell_{(\Pi_F(K_{\mathrm{sym}}))^\circ}}{d} \\
&\overset{\text{Lem 16}}{=} \Big(\frac{n}{d}\Big)^6 \cdot \frac{\ell_{K_{\mathrm{sym}}^\circ \cap F}}{d} \\
&\overset{\text{Lem 19}}{\leq} \Big(\frac{n}{d}\Big)^6 \cdot \frac{\ell_{K_{\mathrm{sym}}^\circ}}{d}.
\end{aligned}$$

Here we also used the fact that $(\Pi_F(K_{\mathrm{sym}}))^\circ = K_{\mathrm{sym}}^\circ \cap F$. □

D. Properties of the covering radius

While the set K may not be symmetric, the sets Λ and $\mathbb{R}^n$ are symmetric, which implies the following:

Lemma 26 (Properties of the covering radius). Consider a lattice $\Lambda \subseteq \mathbb{R}^n$ and a compact convex set $K \subseteq \mathbb{R}^n$ with $\mathrm{span}(\Lambda) = \mathrm{affine.hull}(K)$. Then

(a) $\mu(\Lambda, K) = \mu(\Lambda, K + u)$ for all $u \in \mathrm{span}(\Lambda)$.
(b) $\mu(\Lambda, K) = \min\{r \geq 0 \mid (x + rK) \cap \Lambda \neq \emptyset \ \forall x \in \mathrm{span}(\Lambda)\}$.

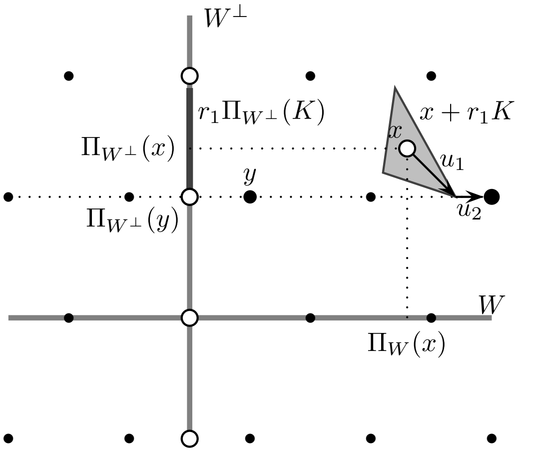
We need a triangle inequality for the covering radius:

Lemma 27. Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice and let $\Lambda' \subseteq \Lambda$ be a primitive sublattice. Then for any compact convex set $K \subseteq \mathbb{R}^n$ with $\mathbf{0} \in \mathrm{rel.int}(K)$ and $\mathrm{span}(\Lambda) = \mathrm{span}(K)$ one has

$$\mu(\Lambda, K) \leq \mu(\Lambda', K \cap W) + \mu(\Lambda/\Lambda', \Pi_{W^\perp}(K)),$$

where $W := \mathrm{span}(\Lambda')$.

Proof. W.l.o.g. we may assume that Λ has full rank, so $\mathbf{0} \in \mathrm{int}(K)$. Following the characterization in Lemma 26.(b), we fix an $x \in \mathbb{R}^n$. For $r_1 := \mu(\Pi_{W^\perp}(\Lambda), \Pi_{W^\perp}(K))$ we know that $\Pi_{W^\perp}(x + r_1 K) \cap \Pi_{W^\perp}(\Lambda) \neq \emptyset$. That means there is a $u_1 \in r_1 K$ and a lattice point $y \in \Lambda$ so that $\Pi_{W^\perp}(x + u_1) = \Pi_{W^\perp}(y)$. Next, for $r_2 := \mu(\Lambda \cap W, K \cap W)$ we know that $(x + u_1 - y + r_2 \cdot (K \cap W)) \cap (\Lambda \cap W) \neq \emptyset$ which is equivalent to $(x + u_1 + r_2 \cdot (K \cap W)) \cap (y + (\Lambda \cap W)) \neq \emptyset$. Let $u_2 \in r_2 \cdot (K \cap W)$ be the vector so that $x + u_1 + u_2 \in \Lambda$. Then $u_1 + u_2 \in (r_1 + r_2)K$ by convexity, so $(x + (r_1 + r_2) \cdot K) \cap \Lambda \neq \emptyset$.



□

The natural extension of Lemma 27 to a filtration is as follows:

Lemma 28. Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice with any sequence of sublattices $\{\mathbf{0}\} = \Lambda_0 \subset \Lambda_1 \subset \ldots \subset \Lambda_k = \Lambda$. Then for any compact convex set $K \subseteq \mathbb{R}^n$ with $\mathbf{0} \in \text{rel.int}(K)$ and $\text{span}(\Lambda) = \text{span}(K)$, one has

$$\mu(\Lambda, K) \leq \sum_{i=1}^{k} \mu\left(\Lambda_i/\Lambda_{i-1}, \Pi_{\text{span}(\Lambda_{i-1})^\perp}(K \cap \text{span}(\Lambda_i))\right).$$

Proof. We can use the previous lemma to show by induction over $i_0 = k, k-1, \ldots, 1$ that

$$\begin{aligned}\mu(\Lambda, K) \quad &\leq \quad \mu(\Lambda_{i_0-1}, K \cap \text{span}(\Lambda_{i_0-1})) + \\ &\quad\sum_{i=i_0}^{k} \mu\left(\Lambda_i/\Lambda_{i-1}, \Pi_{\text{span}(\Lambda_{i-1})^\perp}(K \cap \text{span}(\Lambda_i))\right).\end{aligned}$$

Indeed, for $i_0 = k$ this is exactly Lemma 27. If it holds for some $i_0 > 1$, then

$$\begin{aligned}&\mu(\Lambda_{i_0-1}, K \cap \text{span}(\Lambda_{i_0-1})) \\ \leq \quad &\mu(\Lambda_{i_0-2}, K \cap \text{span}(\Lambda_{i_0-2})) + \\ &\mu\left(\Lambda_{i_0-1}/\Lambda_{i_0-2}, \Pi_{\text{span}(\Lambda_{i_0-2})^\perp}(K \cap \text{span}(\Lambda_{i_0-1}))\right),\end{aligned}$$

since $\text{span}(\Lambda_{i_0-2}) \subset \text{span}(\Lambda_{i_0-1})$. So the claim follows by induction, and taking $i_0 := 1$ yields the statement. □

E. Properties of μ_{KL}

We also need the following fact:

Lemma 29. For any lattice $\Lambda \subseteq \mathbb{R}^n$, compact convex set K with $\text{span}(\Lambda) = \text{affine.hull}(K)$ and subspace $V \subseteq \text{span}(\Lambda)$ one has $\mu_{KL}(\Pi_V(\Lambda), \Pi_V(K)) \leq \mu_{KL}(\Lambda, K)$.

Proof. Let $W \subseteq V$ be the subspace attaining the left side with $\dim W = d$. Then

$$\begin{aligned}\mu_{KL}(\Pi_V(\Lambda), \Pi_V(K)) \quad &= \quad \Big(\frac{\det(\Pi_W(\Pi_V(\Lambda)))}{\text{Vol}_d(\Pi_W(\Pi_V(K)))}\Big)^{1/d} \\ &= \quad \Big(\frac{\det(\Pi_W(\Lambda))}{\text{Vol}_d(\Pi_W(K))}\Big)^{1/d} \\ &\leq \quad \mu_{KL}(\Lambda, K),\end{aligned}$$

since $\Pi_W(\Pi_V(x)) = \Pi_W(x)$ for all $x \in \mathbb{R}^n$ as $W \subseteq V$. □

F. Approximate stable lattices and the covering radius

Using the Reverse Minkowski Theorem it would not be hard to prove that for any stable lattice $\Lambda \subseteq \mathbb{R}^n$ one has $\mu(\Lambda, B_2^n) \leq O(\sqrt{n}\log(2n))$. In this section, we show how to generalize this to t-stable lattices and to general symmetric convex bodies. For a symmetric convex body Q, we consider the following quantity

$$\beta(Q) = \sup_{\Lambda \subseteq \mathbb{R}^n \text{ lattice}} \sup_{u \in \mathbb{R}^n} \frac{\rho_1((u + \Lambda) \setminus Q)}{\rho_1(\Lambda)}$$

Note that always $0 < \beta(Q) \leq 1$. Intuitively, a body Q with $\beta(Q) \ll 1$ is large enough that for any lattice a substantial fraction of the discrete Gaussian weight has to fall in Q. As part of the celebrated Transference Theorem, Banaszczyk showed how to relate the ℓ-value of a body to its β-value:

Lemma 30 (Banaszczyk [Ban96]). For any $\varepsilon > 0$, there is a $\delta > 0$ so that the following holds: for any symmetric convex body $Q \subseteq \mathbb{R}^n$ with $\ell_Q \leq \delta$ one has $\beta(Q) \leq \varepsilon$.

Next, we can get a fairly tight upper bound on the covering radius of a t-stable lattice:

Proposition 31. Let $\Lambda \subseteq \mathbb{R}^n$ be a full rank lattice that is the r-scaling of a t-stable lattice and let $Q \subseteq \mathbb{R}^n$ be a symmetric convex body. Then $\mu(\Lambda, Q) \leq O(\log(2n)) \cdot t \cdot r \cdot \ell_Q$.

Proof. Let $\varepsilon > 0$ be a small enough constant that we determine later. Let δ be the constant so that Lemma 30 applies (w.r.t. ε). The claim is invariant under scaling Q, hence we may scale Q so that $\ell_Q \leq \delta$ and consequently $\beta(Q) \leq \varepsilon$. We may also scale the lattice so that Λ is t-stable (i.e. $r = 1$). It suffices to prove that under these assumptions, $\mu(\Lambda, Q) \leq s \cdot t$ where $s := C\log(2n)$ is the parameter from Lemma 15. Now suppose for the sake of contradiction that there is a translate $u \in \mathbb{R}^n$ so that $(u + \Lambda) \cap stQ = \emptyset$. Since $\beta(Q) \leq \varepsilon$, we know that

$$\rho_1\Big(\Big(\frac{u}{st} + \frac{\Lambda}{st}\Big) \setminus Q\Big) \leq \varepsilon\rho_1\Big(\frac{\Lambda}{st}\Big).$$

Multiplying the sets and parameters by st gives

$$\rho_{st}((u + \Lambda) \setminus stQ) \leq \varepsilon\rho_{st}(\Lambda). \quad (*)$$

Using that Λ is t-stable, we get

$$\begin{aligned}\frac{1}{3}\rho_{st}(\Lambda) \quad &\overset{\text{Lem 15}}{\leq} \quad \rho_{st}(u + \Lambda) \\ &\overset{(u+\Lambda)\cap stQ=\emptyset}{=} \quad \rho_{st}((u + \Lambda) \setminus stQ) \\ &\overset{(*)}{\leq} \quad \varepsilon\rho_{st}(\Lambda).\end{aligned}$$

Then choosing $\varepsilon \in (0, \frac{1}{3})$ gives a contradiction. □

III. Overview

Goal of this section is to provide the reader with an overview and some intuition concerning the proof of our main result, Theorem 2. First, we want to prove the inequality from Theorem 2 (with an even better exponent) in the special case that both the lattice and the body K are well-scaled. We will not actually use Prop 32 later in this form, but it will provide us with the idea for a general proof strategy.

Proposition 32. Let $\Lambda \subseteq \mathbb{R}^n$ be a full rank 2-stable lattice and let K be a convex body with $b(K) = \mathbf{0}$ so that $K \cap -K$ is in ℓ-position. Then $\mu(\Lambda, K) \leq O(\log^2(2n)) \cdot \mu_{KL}(\Lambda, K)$.

Proof. We denote the inner symmetrizer by $K_{\text{sym}} := K \cap -K$. Then applying the estimate for stable lattices from Prop 31 we can upper bound the covering radius:

$$\mu(\Lambda, K) \overset{K \supseteq K_{\text{sym}}}{\leq} \mu(\Lambda, K_{\text{sym}}) \overset{\text{Prop 31}}{\lesssim} \log(2n) \cdot \ell_{K_{\text{sym}}}$$

Next, we lower bound $\mu_{KL}(\Lambda, K)$ by simply choosing the subspace $W := \mathbb{R}^n$ as witness. Then

$$\begin{aligned} \mu_{KL}(\Lambda, K) &\geq \Big(\frac{\det(\Lambda)}{\mathrm{Vol}_n(K)}\Big)^{1/n} \\ &\overset{(*)}{\gtrsim} \frac{1}{\mathrm{Vol}_n(K_{\text{sym}})^{1/n}} \\ &\overset{\text{Cor 22}}{\gtrsim} \frac{n}{\ell_{K^\circ_{\text{sym}}}} \\ &\overset{\ell\text{-position}}{\gtrsim} \frac{\ell_{K_{\text{sym}}}}{\log(2n)}, \end{aligned}$$

where we use in $(*)$ that $\det(\Lambda) \geq 2^{-n}$ and $\mathrm{Vol}_n(K_{\text{sym}}) \geq 2^{-n}\mathrm{Vol}_n(K)$. Combining both inequalities gives the claim. □

Next, we want to develop a proof strategy that works for general Λ and K. Translating K and applying a linear transformation to both Λ and K does not affect the claim, hence we may assume that K has the barycenter at $\mathbf{0}$ and the symmetrizer $K_{\text{sym}} := K \cap -K$ is in ℓ-position. But in general, Λ will not be a 2-stable lattice and we cannot expect that one can always choose the subspace $W = \mathbb{R}^n$ as witness like in Prop 32.

But we know by Cor 14 that the lattice Λ admits a 2-stable well-separated filtration $\{\mathbf{0}\} = \Lambda_0 \subset \ldots \subset \Lambda_k = \Lambda$. Let us abbreviate $d_i := \mathrm{rank}(\Lambda_i/\Lambda_{i-1})$ and $r_i := \det(\Lambda_i/\Lambda_{i-1})^{1/d_i}$. Then each quotient lattice $\frac{1}{r_i}\Lambda_i/\Lambda_{i-1}$ is a 2-stable lattice of dimension d_i and hence an argument similar to Prop 32 becomes feasible.

We can use the triangle inequality that we developed in Lemma 28 to obtain

$$\begin{aligned} \mu(\Lambda, K) &\overset{K \supseteq K_{\text{sym}}}{\leq} \mu(\Lambda, K_{\text{sym}}) \\ &\overset{\text{Lem 28}}{\leq} \sum_{i=1}^{k} \mu(\Lambda_i/\Lambda_{i-1}, K_i) \\ &\overset{\text{Prop 31}}{\lesssim} \log(2n) \sum_{i=1}^{k} r_i \ell_{K_i} \\ &\lesssim \log(2n) \cdot r_k \ell_K, \end{aligned}$$

where $K_i := \Pi_{\mathrm{span}(\Lambda_{i-1})^\perp}(K_{\text{sym}} \cap \mathrm{span}(\Lambda_i))$. Here we have used that the sequence $r_1 < \ldots < r_k$ is geometrically increasing. This provides a convenient upper bound on the covering radius in terms of the relative determinant of the last quotient lattice in the filtration (which is the sparsest one). However we cannot avoid wondering whether we gave up too much by bounding $\ell_{K_i} \leq \ell_K$.

Next, we want to lower bound $\mu_{KL}(\Lambda, K)$. The only natural choices for a witness subspace seem to come from the filtration. Hence for some index $i \in \{1, \ldots, k\}$ we want to understand what can be obtained by choosing $W := \mathrm{span}(\Lambda_{i-1})^\perp$, meaning we project out the densest $i-1$ of the quotient lattices. Then abbreviating $d := \dim(W) = d_i + \ldots + d_k$ we have

$$\begin{aligned} \mu_{KL}(\Lambda, K) &\geq \Big(\frac{\det(\Pi_W(\Lambda))}{\mathrm{Vol}_d(\Pi_W(K))}\Big)^{1/d} \\ &\overset{(*)}{\gtrsim} r_i \cdot \Big(\frac{d}{n}\Big)^6 \frac{d}{\ell^\circ_{K_{\text{sym}}}} \\ &\overset{\ell\text{-position}}{\gtrsim} r_i \cdot \log(2n) \cdot \Big(\frac{d}{n}\Big)^7 \cdot \ell_{K_{\text{sym}}}. \end{aligned}$$

In $(*)$ we use that $\Pi_W(\Lambda) = \Lambda/\Lambda_{i-1}$ and so $\det(\Pi_W(\Lambda))^{1/d}$ is a geometric mean of factors that are all at least r_i. Here we also use Lemma 25 to bound $\mathrm{Vol}_d(\Pi_W(K))$. It seems the only direct comparison can be obtained when letting $i := k$ in which case we have

$$\mu(\Lambda, K) \lesssim \log^2(2n) \cdot \Big(\frac{n}{d_k}\Big)^7 \cdot \mu_{KL}(\Lambda, K).$$

Hence, we can conclude Theorem 2 if d_k is close n, i.e. the last quotient subspace is large. But of course this is not necessarily true. In fact, the issue is more substantial. If K_{sym} is in ℓ-position with $\ell_{K_{\text{sym}}}$ and $\ell_{K^\circ_{\text{sym}}}$ known and W is a d-dimensional subspace, then this determines $\mathrm{Vol}_d(\Pi_W(K))^{1/d}$ only up to a polynomial factor in $\frac{n}{d}$. Hence the information that we considered so far is simply too weak to approximate $\mu(\Lambda, K)$ up to a polylogarithmic factor. But fortunately there is a fix: instead of upper bounding the whole covering radius $\mu(\Lambda, K)$, we only estimate the covering radius corresponding to the less important half of the filtration. This means we will need to iterate the argument, which comes at the expense of a another logarithmic factor, but it will work!

IV. Proof of the main theorem

We will spend the next two subsections proving our main Theorem 2 by induction over n. At each step, we split the lattice Λ and the convex body K into a subspace section of dimension at least $n/2$ and a projection where most of the work will go into analyzing the subspace section.

A. The inductive step

First, we give a self-contained description of the inductive step, then later in Section IV-B we describe the main part of the induction.

Proposition 33. There is a universal constant $C_0 > 0$ so that the following holds: For any full rank lattice $\Lambda \subseteq \mathbb{R}^n$ and any convex body $K \subseteq \mathbb{R}^n$ with $b(K) = \mathbf{0}$, there exists a primitive sublattice $\Lambda' \subseteq \Lambda$ with $\operatorname{rank}(\Lambda') \geq n/2$ so that

$$\mu\big(\Lambda', (K \cap -K) \cap \operatorname{span}(\Lambda')\big) \leq C_0 \log^2(2n) \cdot \mu_{KL}(\Lambda, K).$$

Proof. Set $K_{\text{sym}} := K \cap (-K)$. The claim is invariant under applying a linear transformation to K and Λ. Hence we may assume that K_{sym} is in ℓ-position, i.e. $\ell_{K_{\text{sym}}} \cdot \ell_{K^\circ_{\text{sym}}} \leq O(n \log(2n))$. Consider a well-separated 2-stable filtration $\{\mathbf{0}\} = \Lambda_0 \subset \ldots \subset \Lambda_k = \Lambda$ which exists by Cor 14. We will later choose the lattice Λ' from one of the lattices Λ_i in the filtration, but we postpone the choice for now. We define

$$\begin{aligned} d_i &:= \operatorname{rank}(\Lambda_i/\Lambda_{i-1}) \quad \text{and} \\ r_i &:= \operatorname{nd}(\Lambda_i/\Lambda_{i-1}) = \det(\Lambda_i/\Lambda_{i-1})^{1/d_i}, \end{aligned}$$

which are the rank and normalized determinants of the quotient lattices in the filtration. Recall that $r_1 < r_2 < \ldots < r_k$ with $r_i \leq \frac{1}{2} r_{i+2}$ for all i.

Claim I. For any $i \in \{1, \ldots, k\}$ one has $\mu(\Lambda_i, K_{\text{sym}} \cap \operatorname{span}(\Lambda_i)) \lesssim \log(2n) \cdot r_i \cdot \ell_{K_{\text{sym}}}$.

Proof of Claim I. We abbreviate $K_j := \Pi_{\operatorname{span}(\Lambda_{j-1})^\perp}(K_{\text{sym}} \cap \operatorname{span}(\Lambda_j))$. Then K_j is convex and symmetric and $\frac{1}{r_j}(\Lambda_j/\Lambda_{j-1})$ is a 2-stable lattice. Hence we can bound the covering radii of the individual quotient lattices by

$$\begin{aligned} \mu\big(\Lambda_j/\Lambda_{j-1}, K_j\big) &\overset{\text{Prop 31}}{\lesssim} \log(2n) \cdot r_j \cdot \ell_{K_j} \\ &\overset{\text{Lem 20}}{\leq} \log(2n) \cdot r_j \cdot \ell_{K_{\text{sym}}}. \end{aligned}$$

Then using the triangle inequality for the covering radius we bound

$$\begin{aligned} \mu(\Lambda_i, K_{\text{sym}} \cap \operatorname{span}(\Lambda_i)) &\overset{\text{Lem 28}}{\leq} \sum_{j=1}^{i} \mu\left(\Lambda_j/\Lambda_{j-1}, K_j\right) \\ &\overset{(1)}{\lesssim} \log(2n) \cdot \ell_{K_{\text{sym}}} \cdot \sum_{j=1}^{i} r_j \\ &\lesssim \log(2n) \cdot \ell_{K_{\text{sym}}} \cdot r_i, \end{aligned}$$

using in the last step that $r_1 < \ldots < r_i$ and $r_j \leq \frac{1}{2} r_{j+2}$ for all j. □

In the following we abbreviate $d_{\geq i} := \sum_{j=i}^{k} d_j$.

Claim II. For any $i \in \{1, \ldots, k\}$ one has $\mu_{KL}(\Lambda, K) \gtrsim \frac{r_i}{\log(2n)} \cdot (\frac{d_{\geq i}}{n})^7 \cdot \ell_{K_{\text{sym}}}$.

Proof of Claim II. We choose the subspace $W := \operatorname{span}(\Lambda_{i-1})^\perp$ as witness and note that $\Pi_W(\Lambda) = \Lambda/\Lambda_{i-1}$. Abbreviating $d := \dim(W) = \operatorname{rank}(\Lambda/\Lambda_{i-1}) = d_{\geq i}$ we have

$$\det(\Lambda/\Lambda_{i-1})^{1/d} = \Big(\prod_{j=i}^{k} r_j^{d_j}\Big)^{1/\sum_{j=i}^{k} d_j} \geq r_i, \tag{1}$$

where the middle expression denotes a geometric average of values $r_i < r_{i+1} < \ldots < r_k$. Then lower bounding the covering radius proxy with the witness W gives

$$\begin{aligned} \mu_{KL}(\Lambda, K) &\geq \Big(\frac{\det(\Pi_W(\Lambda))}{\operatorname{Vol}_d(\Pi_W(K))}\Big)^{1/d} \\ &\overset{(1)}{\geq} \frac{r_i}{\operatorname{Vol}_d(\Pi_W(K))^{1/d}} \\ &\overset{\text{Lem 25}}{\gtrsim} r_i \cdot \Big(\frac{d}{n}\Big)^6 \cdot \frac{d}{\ell_{K^\circ_{\text{sym}}}} \\ &\overset{\ell\text{-position}}{\gtrsim} \frac{r_i}{\log(2n)} \cdot \Big(\frac{d}{n}\Big)^7 \cdot \ell_{K_{\text{sym}}}, \end{aligned}$$

using $\ell_{K_{\text{sym}}} \cdot \ell_{K^\circ_{\text{sym}}} \lesssim n \log(2n)$ in the last step. □

Combining Claim I and Claim II with the same index i gives

$$\mu(\Lambda_i, K_{\text{sym}} \cap \operatorname{span}(\Lambda_i)) \lesssim \log^2(2n) \cdot \Big(\frac{n}{d_{\geq i}}\Big)^7 \cdot \mu_{KL}(\Lambda, K).$$

Now, let $i^* \in \{1, \ldots, k\}$ be the minimal index so that $\operatorname{rank}(\Lambda_{i^*}) \geq \frac{n}{2}$. Then $d_{\geq i^*} \geq \frac{n}{2}$ by minimality. Hence $\Lambda' := \Lambda_{i^*}$ satisfies the claim. □

B. Completing the main proof

Using Proposition 33 we can finish the proof of our main theorem.

Proof of Theorem 2. Consider a full rank lattice $\Lambda \subseteq \mathbb{R}^n$ and a convex body $K \subseteq \mathbb{R}^n$. We will prove by induction over n that

$$\mu(\Lambda, K) \leq C_0 \log^3(2n) \cdot \mu_{KL}(\Lambda, K),$$

where $C_0 \geq 1$ is the constant from Proposition 33. The claim is true for $n = 1$, hence assume $n \geq 2$ from now on. The claim is invariant under translations of K, hence we may assume that $b(K) = \mathbf{0}$. Let $\Lambda' \subseteq \Lambda$ be the primitive sublattice from Prop 33 and set $W := \mathrm{span}(\Lambda')$. Then

$$\begin{aligned}
\mu(\Lambda, K) &\overset{\text{Lem 27}}{\leq} \mu(\Lambda \cap W, K \cap W) + \\
&\quad\ \mu(\Pi_{W^\perp}(\Lambda), \Pi_{W^\perp}(K)) \\
&\overset{K \supseteq K_{\mathrm{sym}}}{\leq} \mu(\Lambda \cap W, K_{\mathrm{sym}} \cap W) + \\
&\quad\ \mu(\Pi_{W^\perp}(\Lambda), \Pi_{W^\perp}(K)) \\
&\overset{\substack{\text{Prop 33}\\ \text{+ind.}}}{\leq} C_0 \log^2(2n) \cdot \mu_{KL}(\Lambda, K) + \\
&\quad\ C_0 \log^3(2 \underbrace{\dim(W^\perp)}_{\leq n/2}) \cdot \\
&\quad\ \underbrace{\mu_{KL}(\Pi_{W^\perp}(\Lambda), \Pi_{W^\perp}(K))}_{\leq \mu_{KL}(\Lambda, K)} \\
&\overset{\text{Lem 29}}{\leq} \underbrace{C_0 \log^2(2n) \cdot \Big(1 + \log(n)\Big)}_{=\log^3(2n)} \cdot \\
&\quad\ \mu_{KL}(\Lambda, K). \quad \square
\end{aligned}$$

We should point out that Regev and Stevens-Davidowitz [RS17] prove that in the Euclidean case one has $\mu(\Lambda, B_2^n) \leq O(\log^{3/2}(2n)) \cdot \mu_{KL}(\Lambda, B_2^n)$. Our proof could be seen as a generalization of their argument in the sense that [RS17] also relate both notions of covering radii to the quantities r_i and d_i as defined in Prop 33 by proving that

$$\begin{aligned}
\mu(\Lambda, B_2^n) &\leq O(\log(2n)) \cdot \sqrt{\sum_{i=1}^k d_i r_i^2} \\
&\leq O(\log^{3/2}(2n)) \cdot \mu_{KL}(\Lambda, B_2^n).
\end{aligned}$$

On the other hand, for them the "standard" canonical filtration suffices and they do not require an inductive step. Implicitly, our induction causes $O(\log(2n))$ many re-centering and rescaling operations using the result of Figiel, Tomczak-Jaegerman and Pisier (Theorem 18). This circumvents the issue that the covering radius might be dominated by a subspace of dimension d with $d \ll n$, which may not affect the ℓ-position of the body sufficiently. Then implicitly the induction will contain an iteration where d is relatively large compared to the current ambient dimension. It may also be instructive to reconsider the proof of Prop 33 in the case that $K = B_2^n$. Then in (1), we would obtain the inequality $\mu(\Lambda_j / \Lambda_{j-1}, K_j) \lesssim \log(2n) \cdot r_j \cdot \sqrt{n}$ while actually the much stronger bound of $\mu(\Lambda_j / \Lambda_{j-1}, K_j) \lesssim \log(2n) \cdot r_j \cdot \sqrt{d_j}$ holds. The trick is that using a well-separated filtration the arising loss can be efficiently bounded.

V. Finding the subspace W in single-exponential time

In this section, we prove Theorem 3, which guarantees that a suitable subspace subspace W can be found in time $2^{O(n)}$ at the expense of an additional logarithmic factor in the approximation guarantee. It will be convenient to first apply a linear transformation to well-scale K. This can be done in polynomial time and is a standard argument, see Lemma 40 for details. Hence, for us it suffices to prove the following:

Theorem 34. Given a full rank lattice $\Lambda \subseteq \mathbb{R}^n$ and a convex body $K \subseteq \mathbb{R}^n$ such that $B_2^n \subseteq K \subseteq (n+1)^{3/2} B_2^n$, there exists a randomized $2^{O(n)}$-time algorithm to compute a subspace $W \subseteq \mathbb{R}^n$ with $d := \dim(W)$ so that

$$\mu(\Lambda, K) \lesssim \log^4(2n) \cdot \Big(\frac{\det(\Pi_W(\Lambda))}{\mathrm{Vol}_d(\Pi_W(K))}\Big)^{1/d}.$$

The main technical tool will be the following result of Dadush, which is the only step in the algorithm which takes exponential time:

Theorem 35 (Theorem 6.4. in [Dad19]). Given a lattice $\Lambda \subseteq \mathbb{R}^n$ one can compute an $O(\log(2n))$-stable filtration of Λ in $2^{O(n)}$ time with probability at least $1 - 2^{-\Omega(n)}$.

The following algorithm mimics the proof in Section 4:

Find-Subspace
Input: Convex body $K \subseteq \mathbb{R}^n$ so that $B_2^n \subseteq K \subseteq (n+1)^{3/2} B_2^n$, full rank lattice $\Lambda \subseteq \mathbb{R}^n$
Output: Subspace $W \subseteq \mathbb{R}^n$ satisfying Theorem 34

(1) Compute an approximate barycenter $\tilde{x}$ such that $\|b(K) - \tilde{x}\|_2 \leq 1$
(2) Shift $K' := K - \tilde{x}$
(3) Set $K_{\mathrm{sym}} := K' \cap (-K')$ and compute an invertible linear map T so that
$$\ell_{T(K_{\mathrm{sym}})} \cdot \ell_{(T(K_{\mathrm{sym}}))^\circ} \leq C \cdot n \log(2n)$$
(4) Set $K' \leftarrow T(K)$ and $\Lambda' \leftarrow T(\Lambda)$
(5) Compute an $O(\log(2n))$-stable filtration
$$\{\mathbf{0}\} = \Lambda_0 \subset \ldots \subset \Lambda_k = \Lambda'$$
(6) Compute a well-separated $O(\log(2n))$-stable filtration $\{\mathbf{0}\} = \Lambda'_0 \subset \ldots \subset \Lambda'_{k'} = \Lambda'$
(7) Set i^* as the minimal index with $\mathrm{rank}(\Lambda'_{i^*}) \geq \frac{n}{2}$
(8) Set $W_{i^*} := \mathrm{span}(\Lambda'_{i^*})^\perp$.
(9) Recursively call $W_\Pi :=$ Find-Subspace$(\Pi_{\mathrm{span}(\Lambda'_{i^*})^\perp}(K'), \Pi_{\mathrm{span}(\Lambda'_{i^*})^\perp}(\Lambda'))$.
(10) Return $W := T^{-1} W'$ where $W' := \underset{W \in \{W_{i^*}, W_\Pi\}}{\mathrm{argmin}} \Big\{ \Big(\frac{\det(\Pi_W(\Lambda'))}{\mathrm{Vol}_{\dim(W)}(\Pi_W(K'))}\Big)^{1/\dim(W)} \Big\}$.

We will need several volume computations in the algorithm, for which we use the following theorem:

Theorem 36 ([KLS97]). Given a convex body $K \subseteq \mathbb{R}^n$ with $r \cdot B_2^n \subseteq K \subseteq R \cdot B_2^n$, there exists a randomized algorithm which outputs a positive number ζ with $\mathrm{Vol}_n(K)/\zeta \in [1 - \varepsilon, 1 + \varepsilon]$. The runtime is polynomial in n, $1/\varepsilon$, $\log(1/r)$ and $\log(R)$.

In fact, [KLS97] also computes an approximation to the barycenter of K:

Theorem 37 ([KLS97]). Given a convex body $K \subseteq \mathbb{R}^n$ with $B_2^n \subseteq K \subseteq (n+1)^{3/2} \cdot B_2^n$ and $\delta > 0$, there exists a randomized algorithm with running time polynomial in n and $\frac{1}{\delta}$, which returns an approximate barycenter $\tilde{x}$ such that $\|b(K) - \tilde{x}\|_2 \leq \delta$.

Now, we can prove the main result for this section:

Proof of Theorem 34. First we justify the running time of $2^{O(n)}$, later we discuss the approximation guarantee. We first apply Theorem 37 to compute an approximate barycenter $\tilde{x}$ and shift $K' := K - x$. Theorem 35 yields a filtration for step (5), which can be refined into a well-separated filtration by Theorem 13. Step (10) requires computation of determinants, which can be done in polynomial time via Gaussian elimination, and the volume of a convex body, which can also be done in randomized polynomial time using Theorem 36. The runtime $T(n)$ of Find-Subspace satisfies the recursion $T(n) \leq 2^{O(n)} + T(n/2)$, which can be resolved to $T(n) \leq 2^{O(n)}$.

Next, we justify the approximation guarantee. From the same argument in Section 3 and 4 one can see that the returned subspace satisfies

$$\mu(\Lambda, K) \lesssim \log^4(2n) \cdot \left(\frac{\det(\Pi_W(\Lambda))}{\mathrm{Vol}_d(\Pi_W(K))}\right)^{1/d},$$

where we have taken into account that we pay an additional $\log(2n)$ factor from Proposition 31 as our filtration is only guaranteed to be $O(\log(2n))$-stable. Another subtle point is that we are using only an approximate barycenter. Hence it remains to generalize Proposition 24 and show that the approximation costs us at most another constant factor:

Claim. Let $K \subseteq \mathbb{R}^n$ be a convex body so that $B_2^n \subseteq K$ and $\|b(K)\|_2 \leq 1$. Let $F \subseteq \mathbb{R}^n$ be a d-dimensional subspace. Then denoting $K_{\mathrm{sym}} := K \cap (-K)$,

$$\mathrm{Vol}_d(\Pi_F(K))^{1/d} \lesssim \left(\frac{n}{d}\right)^5 \cdot \log\left(\frac{en}{d}\right)^2 \cdot \mathrm{Vol}_d(\Pi_F(K_{\mathrm{sym}}))^{1/d}.$$

Proof of Claim. By Proposition 24, we know that denoting $\tilde{K}_{\mathrm{sym}} := (K - b(K)) \cap (-K + b(K))$, we have

$$\mathrm{Vol}_d(\Pi_F(K))^{1/d} \lesssim \left(\frac{n}{d}\right)^5 \cdot \log\left(\frac{en}{d}\right)^2 \cdot \mathrm{Vol}_d(\Pi_F(\tilde{K}_{\mathrm{sym}}))^{1/d}.$$

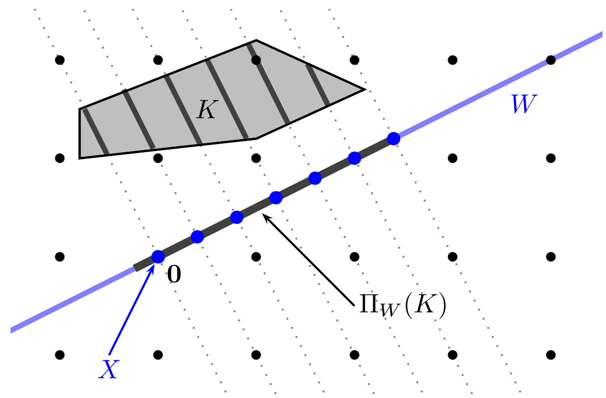
Since $-b(K) \subseteq B_2^n \subseteq K$, it follows that $K - b(K) \subseteq K + K = 2K$, so that $\tilde{K}_{\mathrm{sym}} \subseteq 2K_{\mathrm{sym}}$ and $\mathrm{Vol}_d(\Pi_F(\tilde{K}_{\mathrm{sym}}))^{1/d} \leq 2 \cdot \mathrm{Vol}_d(\Pi_F(K_{\mathrm{sym}}))^{1/d}$. □

VI. Integer programming in time $(\log(2n))^{O(n)}$

Next, we show that integer programming can be solved in time $(\log(2n))^{O(n)}$. In fact, this is a known consequence of Theorem 3. We do not claim any original contribution for this section, but we reproduce the arguments of Dadush [Dad12] to be self-contained. As it is common in the literature, we only state the dependence of running times on n; all running times that involve a convex set $K \subseteq rB_2^n$ and a lattice $\Lambda = \Lambda(B)$ also contain a not mentioned factor that is polynomial in $\log(r)$ and in the encoding length of B.

First, we describe the intuition behind Dadush's algorithm. Consider a convex body $K \subseteq \mathbb{R}^n$ and a lattice $\Lambda \subseteq \mathbb{R}^n$; the goal is to find a point in $K \cap \Lambda$. We compute a subspace $W \subseteq \mathbb{R}^n$ in time $2^{O(n)}$ that certifies the covering radius $\mu(\Lambda, K)$ up to a factor $\rho(n) := \Theta(\log^4(2n))$. Consider the points $X := \Pi_W(K) \cap \Pi_W(\Lambda)$ in the projection on W. For each $x \in K \cap \Lambda$, we also have $\Pi_W(x) \in X$. Note that the reverse may not be true in the sense that it is entirely possible that $K \cap \Lambda = \emptyset$ while $X \neq \emptyset$. However, we are guaranteed that all lattice points in K must be in one of the $(n-d)$-dimensional fibers of the projection, i.e.

$$K \cap \Lambda \subseteq \bigcup_{y \in X} \left((K \cap \Pi_W^{-1}(y)) \cap \Lambda\right).$$



The algorithm enumerates X and then recurses on all the fibers. In order for this algorithm to be efficient we need to (i) bound the cardinality $|X|$ and (ii) be able to enumerate X. For (ii), note that it is possible that $W = \mathbb{R}^n$ and hence we would not gain anything by treating $\Pi_W(K) \cap \Pi_W(\Lambda)$ as a general integer programming problem.

For convex bodies $A, B \subseteq \mathbb{R}^n$, the covering number $N(A, B) := \min\{N \mid \exists x_1, \ldots, x_N \in \mathbb{R}^n : A \subseteq \bigcup_{i=1}^N (x_i + B)\}$ is the minimum number of translates of B needed to cover A. For a convex body $K \subseteq \mathbb{R}^n$ and a full rank lattice $\Lambda \subseteq \mathbb{R}^n$ we define

$$G(\Lambda, K) := \max_{x \in \mathbb{R}^n} |(K + x) \cap \Lambda|.$$

In words, $G(\Lambda, K)$ denotes the maximum number of lattice points that any shift of K contains. Note that even if $K \cap \Lambda = \emptyset$, $G(\Lambda, K)$ might still be arbitrarily large. However, algorithmically the quantity $G(\Lambda, K)$ is useful:

Theorem 38 ([DPV11], [DV13]). Given a convex body $K \subseteq \mathbb{R}^n$ and a full rank lattice $\Lambda \subseteq \mathbb{R}^n$, one can enumerate all points in $K \cap \Lambda$ in deterministic time $2^{O(n)} \cdot G(\Lambda, K)$.

We briefly sketch the algorithm behind Theorem 38: We use the method of Dadush and Vempala [DV13] to compute an M-ellipsoid E of K which has the property that $N(K,E), N(E,K) \leq 2^{O(n)}$. Their deterministic algorithm takes time $2^{O(n)}$. In particular this means that $2^{-\Theta(n)} \leq \frac{G(\Lambda,K)}{G(\Lambda,E)} \leq 2^{\Theta(n)}$. Next, we compute[1] the translates $x_1, \ldots, x_N$ with $N \leq 2^{O(n)}$ so that $K \subseteq \bigcup_{i=1}^N (x_i+E)$. Then we can use the following argument by Dadush, Peikert and Vempala [DPV11] to enumerate all lattice points in $(x_i + E) \cap \Lambda$. After applying a linear transformation, it suffices to compute all points in $(t + B_2^n) \cap \Lambda$ for $t \in \mathbb{R}^n$. Let $R \subseteq \Lambda \setminus \{\mathbf{0}\}$ be the Voronoi-relevant vectors, which are all the vectors that define a facet of the Voronoi cell of Λ. It is known that $|R| \leq 2^{n+1}$ and moreover the set R can be computed in time $2^{O(n)}$ by the algorithm of [MV13]. Next, consider the graph $H = (\Lambda, E)$ with edges $E = \{\{x,y\} : x,y \in \Lambda \text{ and } x-y \in R\}$. Then it follows from the work of [MV13] that the subgraph induced by $\Lambda \cap (t + B_2^n)$ is connected. Hence, one can compute the closest lattice point to t (again using [MV13]) and then traverse the subgraph.

Next, we require an upper bound on $G(\Lambda, K)$ in terms of the volume of K and density of Λ. Surprisingly, such an upper bound exists if we additionally control the covering radius. We reproduce Dadush's proof as the argument is key to understanding the algorithm:

Lemma 39. For any full rank lattice $\Lambda \subseteq \mathbb{R}^n$ and any convex body $K \subseteq \mathbb{R}^n$ one has

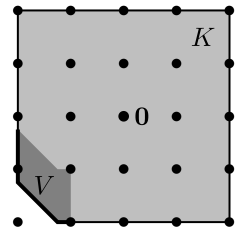
$$G(\Lambda, K) \leq 2^n \max\{\mu(\Lambda,K)^n, 1\} \cdot \frac{\mathrm{Vol}_n(K)}{\det(\Lambda)}.$$

Proof. After a linear transformation and scaling by $\max\{\mu(\Lambda,K),1\}$, the statement is equivalent to the following simpler claim:
Claim. For any convex body $K \subseteq \mathbb{R}^n$ with $\mu(\mathbb{Z}^n, K) \leq 1$ and any $x \in \mathbb{R}^n$ one has $|K \cap (x + \mathbb{Z}^n)| \leq 2^n \mathrm{Vol}_n(K)$.
Proof of Claim. The claim is invariant under translating K, hence we may assume that $\mathbf{0} \in K$. Let $\equiv$ be the equivalence relation on pairs $x, y \in K$ that is defined by $x \equiv y \Leftrightarrow x - y \in \mathbb{Z}^n$. We define a set $V \subseteq K$ by selecting one element from each equivalence class w.r.t. $\equiv$. It would not matter much which element was selected, but let us make the canonical choice of choosing the lexicographically minimal one. In other words, we choose

$$V = \big\{x \in K \mid x \leq_{\text{lex}} y \quad \forall y \in (x + \mathbb{Z}^n) \cap K\big\}$$

where $\leq_{\text{lex}}$ is the standard lexicographical ordering.

[1]At least in the case that E is an M-ellipsoid for K, one may find those translates with $N \leq 2^{O(n)} N(K,E)$ with ease. After applying a linear transformation, we may assume that $E = \sqrt{n} B_2^n$. Then take all translates $x + E$ with $x \in \mathbb{Z}^n$ that intersect K.



As we select at most one element from each equivalence class, we certainly have $\mathrm{Vol}_n(V) \leq 1$. On the other hand, $\mu(\mathbb{Z}^n, K) \leq 1$ implies that for all $x \in \mathbb{R}^n$ one has $(x+\mathbb{Z}^n) \cap K \neq \emptyset$. That in turn means that every equivalence class has a member in K and so $\mathrm{Vol}_n(V) \geq 1$. Together this gives $\mathrm{Vol}_n(V) = 1$. Next, we note that by construction all translates $x + V$ with $x \in \mathbb{Z}^n$ are disjoint. Moreover, for $x \in K \cap \mathbb{Z}^n$ one has that $x + V \subseteq K + K = 2K$. Then

$$\begin{aligned} |K \cap \mathbb{Z}^n| &= \sum_{x \in K \cap \mathbb{Z}^n} \underbrace{\mathrm{Vol}_n(x+V)}_{=1} \\ &\stackrel{\text{disj.}}{=} \mathrm{Vol}_n\Big(\bigcup_{x \in K \cap \mathbb{Z}^n} (x+V)\Big) \\ &\leq \mathrm{Vol}_n(2K), \end{aligned}$$

which gives the claim. □

One technicality we have to deal with is that Theorem 3 requires a lower bound on the inradius of K. Hence we run a preprocessing step: if there is no suitable lower bound for the inradius, then the lattice points of K are all contained in an easy-to-find hyperplane.

Lemma 40. Given a compact convex set $K \subseteq rB_2^n$ and a lattice $\Lambda = \Lambda(B)$. Then in time polynomial in n, times a polynomial in $\log(r)$ and the encoding length of B one can find at least one of the following:

(a) An ellipsoid E and center c so that $c + \frac{1}{(n+1)^{3/2}} E \subseteq K \subseteq c + E$.
(b) A vector $a \in \mathbb{R}^n \setminus \{\mathbf{0}\}$ and $\beta \in \mathbb{R}$ so that $K \cap \Lambda \subseteq \{x \in \mathbb{R}^n \mid \langle a, x\rangle = \beta\}$.

Proof. We may assume that $\mathrm{rank}(\Lambda) = n$, otherwise any a orthogonal to $\mathrm{span}(\Lambda)$ will satisfy (b). Next, we use a variant of the ellipsoid method from [GLS88] (see also Lemma 2.5.10 in [Dad12]) to find a pair (c, E) in time polynomial in n, $\log(r)$ and $\log(\frac{1}{\varepsilon})$ so that either (a) holds, or $K \subseteq c + E$ and $\mathrm{Vol}_n(E) \leq \varepsilon$. Suppose the latter happens. Then using Minkowski's Theorem (Theorem 10) in $(*)$ and the Blaschke-Santaló-Bourgain-Milman Theorem (Theorem 23) in $(**)$ we obtain

$$\begin{aligned} \lambda_1(\Lambda^*, E^\circ) &\stackrel{(*)}{\lesssim} \Big(\frac{\det(\Lambda^*)}{\mathrm{Vol}_n(E^\circ)}\Big)^{1/n} \\ &\stackrel{(**)}{\lesssim} \Big(\frac{\mathrm{Vol}_n(E)}{\det(\Lambda) \cdot \nu_n^2}\Big)^{1/n} \\ &\lesssim n \cdot \Big(\frac{\varepsilon}{\det(\Lambda)}\Big)^{1/n} \leq \frac{1}{2} \cdot 2^{-n/2}, \end{aligned}$$

for a suitable choice of $\varepsilon > 0$. Then the LLL-algorithm [LLL82] can find a dual lattice vector $a \in \Lambda^* \setminus \{\mathbf{0}\}$ with $\|a\|_{E^\circ} \leq 2^{n/2} \cdot \lambda_1(\Lambda^*, E^\circ) \leq \frac{1}{2}$. That vector a with $\beta := \lceil \langle a, c \rangle \rfloor$ will satisfy (b). □

We are now ready to state the complete algorithm. As mentioned earlier, we denote $\rho(n) := \Theta(\log^4(2n))$ as the approximation factor from Theorem 3.

Dadush's algorithm
Input: Compact convex set $K \subseteq \mathbb{R}^n$, lattice $\Lambda \subseteq \mathbb{R}^n$
Output: Point $x \in K \cap \Lambda$ or decision that there is none

(1) Use Lemma 40. If case (b) happens, obtain hyperplane H with $K \cap \Lambda \subseteq H$. Recurse on Dadush$(K \cap H, \Lambda \cap H)$ and return the answer.
(2) Compute a subspace $W \subseteq \mathbb{R}^n$ with $d := \dim(W)$ and $R := (\frac{\det(\Pi_W(\Lambda))}{\mathrm{Vol}_d(\Pi_W(K))})^{1/d}$ so that $R \leq \mu(\Lambda, K) \leq \rho(n) \cdot R$.
(3) Set $\tilde{K} := \min\{\rho(n) \cdot R, 1\} \cdot (K - c) + c$ for some $c \in K$.
(4) Compute an M-ellipsoid $E \subseteq W$ for $\Pi_W(\tilde{K})$.
(5) Compute $N \leq 2^{O(d)}$ points $x_1, \ldots, x_N \in W$ so that $\Pi_W(\tilde{K}) \subseteq \bigcup_{i=1}^N (x_i + E)$.
(6) Compute $X := \Pi_W(\tilde{K}) \cap \Pi_W(\Lambda) = \big(\bigcup_{i=1}^N ((x_i + E) \cap \Pi_W(\Lambda))\big) \cap \Pi_W(\tilde{K})$.
(7) Recursively call Dadush$(\tilde{K} \cap \Pi_W^{-1}(x), \Lambda \cap \Pi_W^{-1}(x))$ for all $x \in X$ and return any found lattice point (if there is any).

Here, to be more informative, we have expanded the blackbox from Theorem 38 into lines (4)-(6). The reader may also note a subtlety here that we have not discussed so far: if K is very large so that $\mu(\Lambda, K) \ll 1$, then we may shrink K to a smaller body $\tilde{K} \subseteq K$ as long as we ensure that still $\mu(\Lambda, \tilde{K}) \leq 1$. We can now finish the analysis:

Theorem 41. Dadush's algorithm finds a point in $K \cap \Lambda$ in time $(\log(2n))^{O(n)}$ if there is one.

Proof. If the algorithm recurses in (1), the claim is clear by induction. So assume otherwise. First we argue correctness of the algorithm. Let $s := \min\{\rho(n) \cdot R, 1\} \in [0, 1]$ and recall that $\tilde{K} \subseteq K$ is a scaling of K by a factor of s. After step (3), the algorithm searches for a lattice point in $\tilde{K}$ rather than in the original body K. If $s < 1$, then the covering radius of the shrunk body is $\mu(\Lambda, \tilde{K}) = \frac{1}{\rho(n) \cdot R} \mu(\Lambda, K) \leq 1$. In other words, even though we continue the search in the strictly smaller body $\tilde{K}$, we are still guaranteed that $\tilde{K} \cap \Lambda \neq \emptyset$. Next, we discuss the running time of the algorithm. We estimate that

$$\begin{aligned} G(\Pi_W(\Lambda), \Pi_W(\tilde{K})) &\overset{\text{Lem 39}}{\leq} 2^d \cdot \max \left\{ \mu(\Pi_W(\Lambda), \Pi_W(\tilde{K}))^d, 1 \right\} \cdot \frac{\mathrm{Vol}_d(\Pi_W(\tilde{K}))}{\det(\Pi_W(\Lambda))} \\ &\leq 2^d \cdot \max \Big\{ \Big(\underbrace{\frac{\rho(n) R}{s}}_{\geq 1} \Big)^d, 1 \Big\} \cdot s^d \cdot \underbrace{\frac{\mathrm{Vol}_d(\Pi_W(K))}{\det(\Pi_W(\Lambda))}}_{= R^{-d}} \\ &= 2^d \cdot (\rho(n) R)^d \cdot R^{-d} \\ &= (2\rho(n))^d. \end{aligned}$$

Here we use that $\mu(\Pi_W(\Lambda), \Pi_W(\tilde{K})) \leq \mu(\Lambda, \tilde{K}) = \frac{1}{s} \cdot \mu(\Lambda, K) \leq \frac{\rho(n) \cdot R}{s}$. Then $|X| \leq G(\Pi_W(\Lambda), \Pi_W(\tilde{K})) \leq 2^d \rho(n)^d$ and by Lemma 39, the computation of X in (4)-(6) takes time $2^{O(d)} \rho(n)^d$. Now, let $T(n)$ be the maximum running time of the algorithm on n-dimensional instances. Then we have the recursion

$$T(n) \leq \max_{d \in \{1, \ldots, n\}} \Big\{ 2^{O(n)} + (O(1) \cdot \rho(n))^d \cdot T(n - d) \Big\} \quad \text{and} \quad T(1) = \Theta(1),$$

which indeed resolves to $T(n) \leq O(\rho(n))^n$. □

We also explain how Dadush's algorithm can be used to solve integer linear programs in time $(\log(2n))^{O(n)}$. Again, the arguments used are standard. Details on the estimates can be found in the book of Schrijver [Sch99].

Proof of Theorem 5. Consider an arbitrary integer linear program $\max\{c^T x \mid Ax \leq b, x \in \mathbb{Z}^n\}$. One can compute a number M in time polynomial in n and the encoding length of A and b so that if the IP is bounded and feasible, then the optimum value is the same as $\max\{c^T x \mid Ax \leq b, \|x\|_\infty \leq M, x \in \mathbb{Z}^n\}$. Next, by applying binary search, it suffices to find an integer point in the compact convex set $K = \{x \in \mathbb{R}^n \mid c^T x \geq \delta, Ax \leq b, \|x\|_\infty \leq M\}$ for which Theorem 4 applies. □

VII. Implications of Theorem 2

Here we derive a few implications of our main result. The following classical inequality will be useful here:

Lemma 42 ([RS57]). For any convex set $K \subseteq \mathbb{R}^n$ we have $\mathrm{Vol}_n(K - K) \leq \binom{2n}{n} \cdot \mathrm{Vol}_n(K)$.

We restate Theorem 6, which yields a nearly tight relationship between the covering radii of K and $K - K$. We remark that it remains an open question whether the two quantities are equal up to a constant.

Theorem (Theorem 6). For any full rank lattice $\Lambda \subseteq \mathbb{R}^n$ and any convex body $K \subseteq \mathbb{R}^n$, one has

$$\mu(\Lambda, K-K) \leq \mu(\Lambda, K) \leq O(\log^3(2n)) \cdot \mu(\Lambda, K-K).$$

Proof. Let W denote the subspace attaining $\mu_{KL}(\Lambda, K)$ with $\dim W = d$. We can use Theorem 2 to upper bound

$$\begin{aligned}
\mu(\Lambda, K) &\lesssim \log^3(2n) \cdot \mu_{KL}(\Lambda, K) \\
&= \log^3(2n) \cdot \Big(\frac{\det(\Pi_W(\Lambda))}{\mathrm{Vol}_d(\Pi_W(K))}\Big)^{1/d} \\
&\overset{\text{Lem 42}}{\lesssim} \log^3(2n) \cdot 4 \cdot \Big(\frac{\det(\Pi_W(\Lambda))}{\mathrm{Vol}_d(\Pi_W(K-K))}\Big)^{1/d} \\
&\lesssim \log^3(2n) \cdot \mu_{KL}(\Lambda, K-K) \\
&\lesssim \log^3(2n) \cdot \mu(\Lambda, K-K). \quad \square
\end{aligned}$$

This in turn implies that the flatness constant in dimension n is bounded by $O(n \log^3(2n))$:

Theorem (Theorem 7). For any convex body $K \subseteq \mathbb{R}^n$ and any full rank lattice $\Lambda \subseteq \mathbb{R}^n$, one has

$$\mu(\Lambda, K) \cdot \lambda_1(\Lambda^*, (K-K)^\circ) \leq O(n \log^3(2n)).$$

Proof. First we show a slightly worse bound of $O(n \log^4(2n))$. Banaszczyk [Ban96] proved that for any symmetric convex body $Q \subseteq \mathbb{R}^n$ one has $\mu(\Lambda, Q) \cdot \lambda_1(\Lambda^*, Q^\circ) \leq O(n \log(2n))$. Setting $Q := K - K$ (which is a symmetric convex body) one then has by Theorem 6

$$\begin{aligned}
\mu(\Lambda, K) \cdot \lambda_1(\Lambda^*, Q^\circ) &\leq O(\log^3(2n)) \cdot \mu(\Lambda, Q) \cdot \lambda_1(\Lambda^*, Q^\circ) \\
&\leq O(n \log^4(2n)).
\end{aligned}$$

Now we give the argument of the stronger bound of $O(n \log^3(2n))$ which is due to Dadush. Let W denote the subspace attaining $\mu_{KL}(\Lambda, K)$ with $\dim W = d$. By Theorem 2,

$$\begin{aligned}
\mu(\Lambda, K) &\lesssim \log^3(2n) \cdot \mu_{KL}(\Lambda, K) \\
&= \log^3(2n) \cdot \Big(\frac{\det(\Pi_W(\Lambda))}{\mathrm{Vol}_d(\Pi_W(K))}\Big)^{1/d} \\
&\overset{\text{Lem 42}}{\lesssim} \log^3(2n) \cdot 4 \cdot \Big(\frac{\det(\Pi_W(\Lambda))}{\mathrm{Vol}_d(\Pi_W(Q))}\Big)^{1/d} \\
&\overset{\text{Lem 23}}{\asymp} \log^3(2n) \cdot d \cdot \Big(\frac{\mathrm{Vol}_d(Q^\circ \cap W)}{\det(\Lambda^* \cap W)}\Big)^{1/d} \\
&\overset{\text{Thm 10}}{\lesssim} n \log^3(2n) \cdot \frac{2}{\lambda_1(\Lambda^* \cap W, Q^\circ \cap W)}.
\end{aligned}$$

Here, we have used that $\Pi_W(\Lambda)^* = \Lambda^* \cap W$. Since $\lambda_1(\Lambda^*, Q^\circ) \leq \lambda_1(\Lambda^* \cap W, Q^\circ \cap W)$, the theorem follows. $\square$

We also explain the proof of Corollary 8 which again is standard:

Corollary (Cor 8). Let $K \subseteq \mathbb{R}^n$ by a convex body with $K \cap \mathbb{Z}^n = \emptyset$. Then there is a vector $c \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$ so that at most $O(n \log^3(2n))$ many hyperplanes of the form $\langle c, x \rangle = \delta$ with $\delta \in \mathbb{Z}$ intersect K.

Proof. We apply Theorem 7 for the lattice $\Lambda := \mathbb{Z}^n$ so that $\Lambda^* = \mathbb{Z}^n$. Then $K \cap \mathbb{Z}^n = \emptyset$ implies that $\mu(\mathbb{Z}^n, K) > 1$ and so $\lambda_1(\mathbb{Z}^n, (K-K)^\circ) \lesssim n \log^3(2n)$. Let $c \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$ be the vector attaining this bound. Then revisiting the definition of the dual norm (Sec II-C) we have $\max\{\langle c, x-y \rangle : x, y \in K\} = \|c\|_{(K-K)^\circ}$. That means at most $\|c\|_{(K-K)^\circ} + 1 \lesssim n \log^3(2n)$ hyperplanes of the form $\langle c, x \rangle = \delta$ with $\delta \in \mathbb{Z}$ intersect K. $\square$

Acknowledgments

The authors are grateful to Daniel Dadush for numerous discussions on related topics, a careful read of a preliminary draft, and for the proof of the improved bound in Theorem 7. The authors would also like to thank the anonymous reviewers who made several helpful suggestions.

References

[AAGM15] Shiri Artstein-Avidan, Apostolos Giannopoulos, and Vitali D. Milman. Asymptotic geometric analysis. Part I, volume 202 of Mathematical Surveys and Monographs. American Mathematical Society, Providence, RI, 2015.

[AKS01] Miklós Ajtai, Ravi Kumar, and D. Sivakumar. A sieve algorithm for the shortest lattice vector problem. In Proceedings on 33rd Annual ACM Symposium on Theory of Computing, July 6-8, 2001, Heraklion, Crete, Greece, pages 601–610, 2001.

[Ban96] Wojciech Banaszczyk. Inequalities for convex bodies and polar reciprocal lattices in $\mathbb{R}^n$ II: application of K-convexity. Discret. Comput. Geom., 16(3):305–311, 1996.

[BLPS99] Wojciech Banaszczyk, Alexander E. Litvak, Alain Pajor, and Stanislaw J. Szarek. The flatness theorem for nonsymmetric convex bodies via the local theory of Banach spaces. Math. Oper. Res., 24(3):728–750, 1999.

[Cas04] Bill Casselman. Stability of Lattices and the Partition of Arithmetic Quotients. Asian Journal of Mathematics, 8(4):607 – 638, 2004.

[Dad12] Daniel Nicolas Dadush. Integer Programming, Lattice Algorithms, and Deterministic Volume Estimation. PhD thesis, USA, 2012.

[Dad19] Daniel Dadush. On approximating the covering radius and finding dense lattice subspaces. In STOC, pages 1021–1026. ACM, 2019.

[DER22] Daniel Dadush, Friedrich Eisenbrand, and Thomas Rothvoss. From approximate to exact integer programming. CoRR, abs/2211.03859, 2022.

[DPV11] Daniel Dadush, Chris Peikert, and Santosh S. Vempala. Enumerative lattice algorithms in any norm via m-ellipsoid coverings. In FOCS, pages 580–589. IEEE Computer Society, 2011.

[DR16] Daniel Dadush and Oded Regev. Towards strong reverse Minkowski-type inequalities for lattices. In FOCS, pages 447–456. IEEE Computer Society, 2016.

[DV13] Daniel Dadush and Santosh S. Vempala. Near-optimal deterministic algorithms for volume computation via M-ellipsoids. Proc. Natl. Acad. Sci. USA, 110(48):19237–19245, 2013.

[GLS88] Martin Grötschel, László Lovász, and Alexander Schrijver. Geometric algorithms and combinatorial optimization. Springer, 1988.

[Joh48] Fritz John. Extremum problems with inequalities as subsidiary conditions. In Studies and Essays Presented to R. Courant on his 60th Birthday, January 8, 1948, pages 187–204. Interscience Publishers, Inc., New York, 1948.

[Kan87] Ravi Kannan. Minkowski's convex body theorem and integer programming. Math. Oper. Res., 12(3):415–440, August 1987.

[KL88] Ravi Kannan and László Lovász. Covering minima and lattice-point-free convex bodies. Annals of Mathematics, 128(3):577–602, 1988.

[KLS97] Ravi Kannan, László Miklós Lovász, and Miklós Simonovits. Random walks and an $O(n^5)$ volume algorithm for convex bodies. Random Structures and Algorithms, 11:1–50, 1997.

[Len83] Jr. Lenstra, H. W. Integer programming with a fixed number of variables. Mathematics of Operations Research, 8(4):pp. 538–548, 1983.

[LLL82] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász. Factoring polynomials with rational coefficients. Math. Ann., 261(4):515–534, 1982.

[MV13] Daniele Micciancio and Panagiotis Voulgaris. A deterministic single exponential time algorithm for most lattice problems based on Voronoi cell computations. SIAM J. Comput., 42(3):1364–1391, 2013.

[Odl90] A. M. Odlyzko. The rise and fall of knapsack cryptosystems. Cryptology and Computational Number Theory, pages 75–88, 1990.

[Reg09a] Oded Regev. Lecture notes on lattices, 2009.

[Reg09b] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. J. ACM, 56(6):34:1–34:40, 2009.

[RS57] Claude Ambrose Rogers and Geoffrey C. Shephard. The difference body of a convex body. Archiv der Mathematik, 8:220–233, 1957.

[RS17] Oded Regev and Noah Stephens-Davidowitz. A reverse Minkowski theorem. In STOC, pages 941–953. ACM, 2017.

[Rud98] Mark Rudelson. Distances between non-symmetric convex bodies and the MM*-estimate. Positivity, 4:161–178, 1998.

[Sch99] Alexander Schrijver. Theory of linear and integer programming. Wiley-Interscience series in discrete mathematics and optimization. Wiley, 1999.

[Ste17] Noah Stephens-Davidowitz. On the Gaussian Measure Over Lattices. PhD thesis, New York University, USA, 2017.

[Vri23] Beatrice-Helen Vritsiou. Regular ellipsoids and a Blaschke-Santaló-type inequality for projections of non-symmetric convex bodies, 2023.

Appendix

In this chapter, we prove Theorem 13. The proof idea is rather simple: given a t-stable filtration $\{\mathbf{0}\} = \Lambda_0 \subset \ldots \subset \Lambda_k = \Lambda$, we select one index from every density class in order to make the filtration well-separated. But before we come to the main argument, we require two lemmas.

Lemma 43 (Grayson's parallelogram rule [Cas04]). For any two lattices $\Lambda, \Lambda' \subseteq \mathbb{R}^n$,

$$\det(\Lambda) \cdot \det(\Lambda') \geq \det(\Lambda + \Lambda') \cdot \det(\Lambda \cap \Lambda').$$

A proof may also be found in Chapter 2 of [Ste17]. The t-stable filtration can be used to obtain lower bounds on the determinant of any sublattice:

Lemma 44. Let $\Lambda \subseteq \mathbb{R}^n$ be any lattice and let $\{\mathbf{0}\} = \Lambda_0 \subset \Lambda_1 \subset \ldots \subset \Lambda_k = \Lambda$ be a t-stable filtration. Then for any sublattice $\tilde{\Lambda} \subseteq \Lambda$ we have the inequality

$$\mathrm{nd}(\tilde{\Lambda}) \geq t^{-1} \cdot \mathrm{nd}(\Lambda_1).$$

Proof. Let $r_i := \mathrm{nd}(\Lambda_i/\Lambda_{i-1}) = \det(\Lambda_i/\Lambda_{i-1})^{1/\mathrm{rank}(\Lambda_i/\Lambda_{i-1})}$ be the normalized determinant. We prove by induction on $i \in \{1, \ldots, k\}$ that the result holds for all lattices $\tilde{\Lambda} \subseteq \Lambda_i$. The base case follows as $\Lambda_1 = \Lambda_1/\Lambda_0$ is a scalar of the t-stable lattice $\frac{1}{\mathrm{nd}(\Lambda_1)}\Lambda_1$. Now suppose that $\tilde{\Lambda} \subseteq \Lambda_i$ for some $i > 1$. Note that $\Lambda_+ := \tilde{\Lambda} + \Lambda_{i-1}$ satisfies $\Lambda_{i-1} \subseteq \Lambda_+ \subseteq \Lambda_i$, so that $\Lambda_+/\Lambda_{i-1} \subseteq \Lambda_i/\Lambda_{i-1}$ and $\mathrm{nd}(\Lambda_+/\Lambda_{i-1}) \geq t^{-1} \cdot r_i > t^{-1} \cdot r_1$. By Lemma 43,

$$\det(\tilde{\Lambda}) \cdot \det(\Lambda_{i-1}) \geq \det(\tilde{\Lambda} + \Lambda_{i-1}) \cdot \det(\tilde{\Lambda} \cap \Lambda_{i-1}).$$

Factoring out Λ_{i-1} gives

$$\det(\tilde{\Lambda}) \geq \det(\Lambda_+/\Lambda_{i-1}) \cdot \det(\tilde{\Lambda} \cap \Lambda_{i-1}).$$

Hence

$$\begin{aligned} \mathrm{nd}(\tilde{\Lambda}) \quad &\geq \quad \mathrm{nd}(\Lambda_+/\Lambda_{i-1})^{\mathrm{rank}(\Lambda_+/\Lambda_{i-1})/\mathrm{rank}(\tilde{\Lambda})} \cdot \\ &\quad\quad \mathrm{nd}(\tilde{\Lambda} \cap \Lambda_{i-1})^{\mathrm{rank}(\tilde{\Lambda}\cap\Lambda_{i-1})/\mathrm{rank}(\tilde{\Lambda})} \\ &\geq \quad t^{-1} \cdot r_1, \end{aligned}$$

where we used the inductive hypothesis on $\tilde{\Lambda} \cap \Lambda_{i-1} \subseteq \Lambda_{i-1}$ together with the fact that $\mathrm{rank}(\Lambda_+/\Lambda_{i-1}) + \mathrm{rank}(\tilde{\Lambda} \cap \Lambda_{i-1}) = \mathrm{rank}(\tilde{\Lambda})$. □

Now, we come to the main argument:

Proof of Theorem 13. Let $r_i := \mathrm{nd}(\Lambda_i/\Lambda_{i-1})$ and $d_i := \mathrm{rank}(\Lambda_i/\Lambda_{i-1})$. For $\ell \in \mathbb{Z}$ denote $I_\ell := \{i \in [k] : 2^\ell \leq r_i < 2 \cdot 2^\ell\}$. We define a sequence of indices $0 = \ell(0) < \ell(1) < \ldots < \ell(\tilde{k}) = k$ that contains precisely the largest index i in each I_ℓ with $I_\ell \neq \emptyset$ plus the index $\ell(0) = 0$. We set $\tilde{\Lambda}_j := \Lambda_{\ell(j)}$ and $\tilde{r}_j := \mathrm{nd}(\tilde{\Lambda}_j/\tilde{\Lambda}_{j-1})$. First, consider an index ℓ with $I_\ell \neq \emptyset$. Let $i_{\min}, i_{\max} \in I_\ell$ be the minimal and maximal indices in I_ℓ. Then

$$\begin{aligned} &\det(\Lambda_{i_{\max}}/\Lambda_{i_{\min}-1})^{1/\mathrm{rank}(\Lambda_{i_{\max}}/\Lambda_{i_{\min}-1})} \\ = \quad &\Big(\prod_{i=i_{\min}}^{i_{\max}} \det(\Lambda_i/\Lambda_{i-1})\Big)^{1/\sum_{i=i_{\min}}^{i_{\max}} \mathrm{rank}(\Lambda_i/\Lambda_{i-1})} \\ = \quad &\Big(\prod_{i=i_{\min}}^{i_{\max}} r_i^{d_i}\Big)^{1/\sum_{i=i_{\min}}^{i_{\max}} d_i}. \end{aligned}$$

Note that this value is a weighted geometric average of r_i-values for $i \in I_\ell$. From this it immediately follows that $\tilde{r}_1 < \ldots < \tilde{r}_k$ and $\tilde{r}_j \leq \frac{1}{2}\tilde{r}_{j+2}$ for all j, i.e. (a') holds. It remains to show that the quotient lattices are scalars of $2t$-stable lattices. Fix some index $j \in [\tilde{k}]$ and let $\Lambda' := \frac{1}{\tilde{r}_j}(\tilde{\Lambda}_j/\tilde{\Lambda}_{j-1})$. First note that by assumption, the filtration $\{\mathbf{0}\} = \Lambda'_0 \subset \cdots \subset \Lambda'_{k'} := \Lambda'$ given by $\Lambda'_i := \frac{1}{\tilde{r}_j}(\Lambda_{\ell(j-1)+i}/\Lambda_{\ell(j-1)})$ with $k' := \ell(j) - \ell(j-1)$ is also t-stable because $\Lambda'_{i+1}/\Lambda'_i = \frac{1}{\tilde{r}_j}(\Lambda_{\ell(j-1)+i+1}/\Lambda_{\ell(j-1)+i})$.

We will prove the following two statements.

(I) For any sublattice $\tilde{\Lambda} \subseteq \Lambda'$ one has $\mathrm{nd}(\tilde{\Lambda}) \geq (2t)^{-1}$.

(II) For any sublattice $\tilde{\Lambda} \subseteq (\Lambda')^*$ one has $\mathrm{nd}(\tilde{\Lambda}) \geq (2t)^{-1}$.

First we show (I). We apply Lemma 44 on Λ' to obtain

$$\mathrm{nd}(\tilde{\Lambda}) \geq t^{-1} \cdot \mathrm{nd}(\Lambda'_1) \geq t^{-1} \cdot \frac{r_{\ell(j-1)+1}}{\tilde{r}_j} \geq (2t)^{-1},$$

since both numerator and denominator belong to the same interval $[2^\ell, 2 \cdot 2^\ell)$ for some $\ell \in \mathbb{Z}$. Next, we prove (II).

Given the filtration $\{\mathbf{0}\} = \Lambda'_0 \subset \cdots \subset \Lambda'_{k'} = \Lambda'$ with $U_i := \mathrm{span}(\Lambda'_i)$, the dual filtration is given by $\{\mathbf{0}\} = (\Lambda')^*_0 \subset \cdots \subset (\Lambda')^*_{k'} = (\Lambda')^*$ with $(\Lambda')^*_i := \Lambda^* \cap U^\perp_{k'-i}$ and determinant $\det((\Lambda')^*_i) = \det((\Lambda')^*) \cdot \det(\Lambda'_{k'-i}) = \det(\Lambda'_{k'-i})$, see for example [Dad19]. Since quotients of the dual filtration are duals of the quotients of the original filtration, the dual filtration is also t-stable. We then apply Lemma 44 on $(\Lambda')^*$:

$$\begin{aligned}
\mathrm{nd}(\tilde{\Lambda}) &\geq t^{-1} \cdot \mathrm{nd}((\Lambda')^*_1) \\
&= t^{-1} \cdot (r'_{k'})^{-1} \\
&= t^{-1} \cdot \left(\frac{r_{\ell(j)}}{\tilde{r}_j}\right)^{-1} \\
&\overset{r_{\ell(j)} \leq 2 \cdot \tilde{r}_j}{\geq} (2t)^{-1}. \quad \square
\end{aligned}$$