The Subspace Flatness Conjecture

Thomas Rothvoss

Abstract. The *covering radius* $\mu(\Lambda, K)$ of a convex body $K \subseteq \mathbb{R}^n$ with respect to a full rank lattice $\Lambda \subseteq \mathbb{R}^n$ is the minimum scaling needed so that translates of K placed at every lattice point cover the whole $\mathbb{R}^n$. A question going back to work of Kannan and Lovász (1988) is how well the covering radius is described solely by the volume of K and the density of the lattice, after projecting both into a suitable subspace. We report on significant progress on this question due to Regev and Stephens-Davidowitz (2016) who resolve this problem for ellipsoids and Reis and Rothvoss (2023) who cover the general case. We also survey applications of these results that give near-optimal bounds on the flatness constant as well as a $(\log n)^{O(n)}$-time algorithm for solving n-variable integer programs, following work of Dadush (2012).

1 Introduction. A *lattice* Λ is a discrete subgroup of $\mathbb{R}^n$. Any lattice can be written as an integer linear combination of its *basis* B, i.e. $\Lambda := \Lambda(B) := \{Bx : x \in \mathbb{Z}^k\}$ where $B \in \mathbb{R}^{n \times k}$ is a matrix with linearly independent columns. The number k denotes the *rank* of the lattice and we say that a lattice has *full rank* if $k = n$.

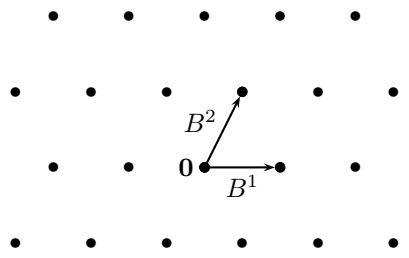

Figure 1.1: Lattice of rank 2 with basis B

Lattices are the central objects of study in the geometry of numbers with many applications for example to number theory. One classical application among others is *Dirichlet's Theorem* which says that for any real vector $a \in \mathbb{R}^n$ and any bound $Q \in \mathbb{N}$, one can find a rational approximation $\frac{p}{q}$ with $p \in \mathbb{Z}^n$ and $q \in \{1, \dots, Q\}$ so that $\|\frac{p}{q} - a\|_\infty \leq \frac{1}{Q^{1/n} q}$. We recommend the wonderful textbook of Matousek [22] for background.

Arguably the most important algorithm in the area of lattice is the *LLL-algorithm* by Lenstra, Lenstra and Lovász [19] which finds an approximately orthogonal basis for a given lattice in polynomial time. One of the applications of this algorithm is a polynomial time $2^{n/2}$-approximation algorithm for the problem of finding a (nonzero) *shortest vector* in a lattice.

One major application of lattices in computer science lies in *lattice-based cryptography*. Cryptosystems based on the hardness of factoring (such as the RSA cryptosystem) or the hardness of taking discrete logarithms (such as the ElGamal Cryptosystem or the Diffie-Hellman Key Exchange) have the disadvantage that they are vulnerable to quantum computers. In contrast, for lattice-based cryptosystems no such advantage for quantum computers is known. In fact, lattice-based cryptography admits certain provable security guarantees that other systems lack. One crucial aspect of a public key cryptosystem is that one of the involved parties generates a private and a public key at random and then shares the public key. This makes it neccessary to generate instances for a rather structured problem that should be computationally hard. But random instances for problems could be easy even if the problem is hard in the worst case. One illustrative case is the one of *Knapsack-based cryptosystems* which as the name suggests relies on the hardness of Knapsack which is an **NP**-hard problem. But the distributions over Knapsack instances used in the cryptosystem can be solved in polynomial time — in fact using the LLL-algorithm that we mentioned earlier. We recommend reading the fascinating work of Odlyzko [26] on this. This

is the situation where lattices can provide an advantage. Regev [30] introduced the lattice-based *Learning with Errors* public key cryptosystem. Crucially [30] could prove that if one could decode an LWE message (with respect to *random* keys) then one would also be able to solve certain lattice-problems efficiently in the *worst-case*.

The purpose of this article is to survey recent progress in lattice theory that has applications to optimization.

1.1 Basics of lattices. Before we continue, we want to review a few more basic objects related to lattices. The *fundamental parallelepiped* of a lattice Λ with basis $B \in \mathbb{R}^{n\times k}$ is the polytope

$$\mathcal{P}(B) := \{Bx : x \in [0,1)^k\}$$

see Figure 1.2.

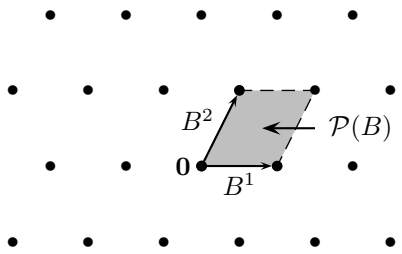

Figure 1.2: Fundamental parallelepiped

While the geometry of the fundamental parallelepiped depends on the choice of basis, the volume does not and it forms an important invariant of a lattice, called the *determinant* which we denote by $\det(\Lambda) := \mathrm{Vol}_k(\mathcal{P}(B))$. In the full rank case one also has $\det(\Lambda) = |\det(B)|$. A *convex body* $K \subseteq \mathbb{R}^n$ is a set that is (i) convex, (ii) bounded, (iii) closed and (iv) full dimensional. A set K is *symmetric* if $K = -K$. We abbreviate the unit ball of the $\|\cdot\|_p$-norm by $B_p^n := \{x \in \mathbb{R}^n \mid \|x\|_p \leq 1\}$. For any full rank lattice Λ and any symmetric convex body K one has[1]

$$|rK \cap \Lambda| \approx \frac{\mathrm{Vol}_n(rK)}{\det(\Lambda)}$$

as $r \to \infty$. In other words, $\det(\Lambda)$ is a measure for how dense (or sparse for that matter) a lattice is.

1.2 The covering radius. Now we come to the central quantity of this survey. For a full rank lattice $\Lambda \subseteq \mathbb{R}^n$ and a convex body $K \subseteq \mathbb{R}^n$ we define the *covering radius* as

$$\mu(\Lambda, K) := \min\left\{r \geq 0 \mid \Lambda + rK = \mathbb{R}^n\right\}$$

As it is the case with most lattice-related problems, computing $\mu(\Lambda, K)$ is a computationally difficult problem. We note that

$$\mu(\Lambda, K) \leq r \quad \Longleftrightarrow \quad \forall x \in \mathbb{R}^n : \exists y \in \Lambda : x \in y + rK$$

That means in complexity-theoretic terms, the question whether $\mu(\Lambda, K) \leq r$ sits on the second level of the *polynomial hierarchy* (see [2] for background). In fact, even for $K = B_\infty^n$, computing $\mu(\Lambda, K)$ is Π_2^P-hard [1]. Besides the computational aspect, for general convex bodies, one might be worried how much of the (potentially very complicated) geometry of K needs to be considered to determine $\mu(\Lambda, K)$. Hence it would be desirable to *approximate* the covering radius by a quantity that is simpler — both algorithmically and geometrically. In fact, it is not too difficult to come up with some naive lower bound:

FACT 1.1. *For a full rank lattice $\Lambda \subseteq \mathbb{R}^n$ and a convex body $K \subseteq \mathbb{R}^n$ one has $\mu(\Lambda, K) \geq \left(\frac{\det(\Lambda)}{\mathrm{Vol}_n(K)}\right)^{1/n}$.*

To see this, note that one needs at least a scaling of $r := \left(\frac{\det(\Lambda)}{\mathrm{Vol}_n(K)}\right)^{1/n}$ so that a point taken at random from a sufficiently large ball is on *average* contained in at least one translate of $\Lambda + rK$. However, this lower bound is too

[1] Here $\approx$ means that the ratio of the sides approaches 1 as $r \to \infty$.

simplistic and may be arbitrarily far off the real covering radius already in dimension 2, see for example $\Lambda = \mathbb{Z}^2$ and $K = [-\frac{1}{M}, \frac{1}{M}] \times [-M, M]$ with $M \to \infty$. But we can add in one more observation: for any subspace $W \subseteq \mathbb{R}^n$ one has $\mu(\Lambda, K) \geq \mu(\Pi_W(\Lambda), \Pi_W(K))$. Here, Π_W is the *orthogonal projection* into W, i.e. for all $x \in \mathbb{R}^n$ one has (i) $\Pi_W(x) \in W$ and (ii) $(x - \Pi_W(x)) \perp \Pi_W(x)$. Importantly, the volume/density lower bound from Fact 1.1 can be larger for the projection than for the original.

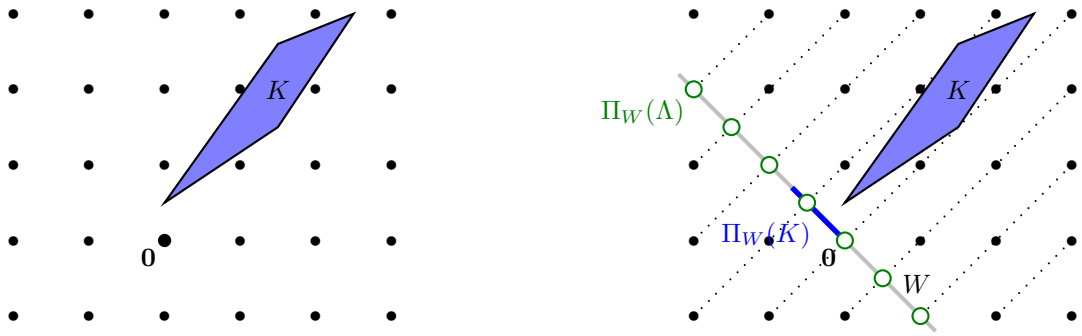

Figure 1.3: Left: Lattice Λ with convex body K. Right: projection attaining $\mu_{KL}(\Lambda, K)$.

This is an idea that goes back to Kannan and Lovász [16]. We define the best lower bound obtainable in this way by[2]

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

In fact, Kannan and Lovász [16] were able to prove that the gap between the covering radius and this lower bound is bounded:

THEOREM 1.2 (Kannan and Lovász [16]). *For any full rank lattice $\Lambda \subseteq \mathbb{R}^n$ and any convex body $K \subseteq \mathbb{R}^n$ one has*

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

On the other hand, no example is known where the gap between $\mu(\Lambda, K)$ and $\mu_{KL}(\Lambda, K)$ is even close to the upper bound of n. The largest known gap is only $\Theta(\log n)$ which can already be found in the work of [16].

LEMMA 1.3 (Kannan and Lovász [16]). *There is a convex body $K \subseteq \mathbb{R}^n$ so that $\mu(\mathbb{Z}^n, K) \geq \Theta(\log n) \cdot \mu_{KL}(\mathbb{Z}^n, K)$.*

Proof. Let $a \in \mathbb{R}^n_{\geq 0}$ be a vector with $a_1 \geq \ldots \geq a_n > 0$ and $\sum_{i=1}^n a_i = 1$. Now consider the simplex $K := \{x \in \mathbb{R}^n_{\geq 0} \mid \sum_{i=1}^n a_i x_i \leq 1\}$, see Fig 1.4. The covering radius with respect to the integer lattice is $\mu(\mathbb{Z}^n, K) = 1$. Now, consider the proxy $\mu_{KL}(\mathbb{Z}^n, K)$. Not unsurprisingly one can argue that regardless of the concrete values of the a_i's, the subspace attaining the maximum must be among $W_1, \ldots, W_n$ where $W_k = \text{span}\{e_1, \ldots, e_k\}$, i.e. for some k we project on the shortest k sides of the simplex. We note that $\det(\Pi_{W_k}(\mathbb{Z}^n)) = \det(\mathbb{Z}^k) = 1$. Setting $a_i := \frac{1}{i \cdot H_n} = \Theta(\frac{1}{i \log(n)})$ we can see that

$$\text{Vol}_k(\Pi_{W_k}(K)) = \text{Vol}_k\Big(\text{conv}\Big\{\mathbf{0}, \frac{e_1}{a_1}, \ldots, \frac{e_k}{a_k}\Big\}\Big) = \frac{1}{k! \cdot \prod_{i=1}^k a_i} = H_n^k$$

and hence $\mu_{KL}(\mathbb{Z}^n, K) = \frac{1}{H_n} = \Theta(\frac{1}{\log n})$. ∎

Dadush [11] conjectured that this construction already provides the worst case, at least asymptotically:

[2] Technically speaking if we allow W to be an arbitrary subspace, then $\Pi_W(\Lambda)$ may not even be a lattice. For example if $W := \text{span}\{(\frac{1}{\sqrt{2}})\}$, then the set $\Pi_W(\mathbb{Z}^2)$ is infinitely dense and not a lattice. But for such cases one could just define $\det(\Pi_W(\Lambda)) := 0$. Or one restricts W to subspaces spanned by vectors from the dual lattice Λ^* which in turn is equivalently to ask that $W^\perp$ is spanned by vectors in Λ. For details, see e.g. [16].

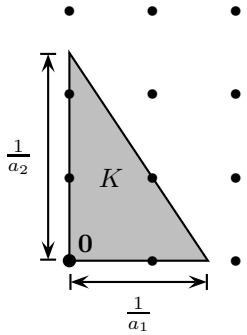

Figure 1.4: Simplex $K = \{x \in \mathbb{R}^n_{\geq 0} \mid \sum_{i=1}^n a_i \leq 1\}$ for $n = 2$

Conjecture 1.4 (Subspace Flatness Conjecture [11]). *For any full rank lattice $\Lambda \subseteq \mathbb{R}^n$ and any convex body $K \subseteq \mathbb{R}^n$ one has*

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

In fact, in his PhD thesis, Dadush [11] proved that assuming an affirmative answer to Conjecture 1.4, one could solve general integer programs in a dramatically faster time of $(\log n)^{O(n)}$. We will later describe Dadush's algorithm in Section 5.2.

On route towards Conjecture 1.4 it appears natural to start with simpler convex bodies, for example ellipsoids. Both quantities $\mu(\Lambda, K)$ and $\mu_{KL}(\Lambda, K)$ are invariant under application of some linear map $T : \mathbb{R}^n \to \mathbb{R}^n$ to both Λ and K. Hence the case for ellipsoids is equivalent to settling the case for the Euclidean ball. In particular the projection of a Euclidean ball is again a Euclidean ball which allows to simplify the function μ_{KL}. However, this case turned out to be still exceptionally difficult. Dadush and Regev [10] made some progress and showed that the question for Euclidean balls reduces to a rather deep open question concerning lattices which they termed the *Reverse Minkowski Theorem*. This conjecture was eventually proven by Regev and Stephens-Davidowitz [31, 32] which in turn settled the case for Euclidean balls and ellipsoids. In fact the current upper bound for ellipsoids is better than the lower bound for simplices from Lemma 1.3.

Theorem 1.5 ([31, 32]). *For any full rank lattice $\Lambda \subseteq \mathbb{R}^n$ one has*

$$\mu_{KL}(\Lambda, B_2^n) \leq \mu(\Lambda, B_2^n) \leq O(\sqrt{\log n}) \cdot \mu_{KL}(\Lambda, B_2^n)$$

We will explain this connection in Section 3. In regard of Conjecture 1.4, one could say that the work of Regev and Stephens-Davidowitz [31, 32] takes care of the difficulties arising from the lattice Λ. Then the difficulties arising from the convex body (also in respect to the lattice) were finally resolved by Reis, together with the author of this survey.

Theorem 1.6 (Reis, R. [33]). *For any full rank lattice $\Lambda \subseteq \mathbb{R}^n$ and any convex body $K \subseteq \mathbb{R}^n$ one has*

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

2 Preliminaries. For quantities A and B we write $A \lesssim B$ if there is a universal constant $C > 0$ so that $A \leq CB$. We write $A \asymp B$, if $A \lesssim B$ and $B \lesssim A$.

2.1 Convex geometry. We begin by reviewing facts on convex geometry that can all be found in great detail in the wonderful textbook by Artstein-Avidan, Giannopoulos and Milman [3]. The reader may note that some quoted results will only hold if the convex body K is symmetric. This will create some problems later in Section 4. But we cross that bridge once we get to it.

For a convex body $K \subseteq \mathbb{R}^n$ that contains the origin in its interior, we define the *polar* as $K^\circ = \{x \in \mathbb{R}^n \mid \langle x, y\rangle \leq 1 \ \forall y \in K\}$. Note that $(K^\circ)^\circ = K$. One could think of K° as the set of feasible inequalities for K and vice versa. Intuitively, whenever K is small, then K° is large which one can quantify as follows:

Theorem 2.1 (Blaschke-Santaló-Bourgain-Milman). *There are universal constants $C_0, C_1 > 0$ so that for every symmetric convex body $K \subseteq \mathbb{R}^n$,*

$$\frac{C_0}{n} \leq \left(\mathrm{Vol}_n(K) \cdot \mathrm{Vol}_n(K^\circ)\right)^{1/n} \leq \frac{C_1}{n}$$

We write $N(\mathbf{0}, I_n)$ as the *standard Gaussian distribution* on $\mathbb{R}^n$. For a measurable set $A \subseteq \mathbb{R}^n$ we define its *Gaussian measure* as $\gamma_n(A) = \Pr_{x\sim N(\mathbf{0},I_n)}[x \in A] = \frac{1}{(2\pi)^{n/2}} \int_A e^{-\|x\|_2^2/2} dx$. While the volume of a convex body is a very natural quantity, for many applications it is not the right value to consider. The *ℓ-value* of a symmetric convex $K \subseteq \mathbb{R}^n$ is defined as

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

One may think of ℓ_K as the "average thinness" of K. We note that for any $t > 0$, one has $\ell_{tK} = \frac{1}{t}\ell_K$. For example for the Euclidean ball the ℓ-value is $\ell_{B_2^n} = \mathbb{E}_{x\sim N(\mathbf{0},I_n)}[\|x\|_2^2]^{1/2} = \sqrt{n}$. One of the deepest and most powerful tools in convex geometry says that any symmetric convex body can be linearly transformed so that its ℓ-value and the ℓ-value of the polar are almost as small as for the Euclidean ball.

THEOREM 2.2 (Figiel and Tomczak-Jaegermann [12], Lewis [21], Pisier [28]). *For any symmetric convex body $K \subseteq \mathbb{R}^n$, there is an invertible linear map $T : \mathbb{R}^n \to \mathbb{R}^n$ so that $\ell_{T(K)} \cdot \ell_{(T(K))^\circ} \leq O(n \log(n))$.*

We will also say that K is in *ℓ-position* if $\ell_K \cdot \ell_{K^\circ} \leq O(n \log(n))$.

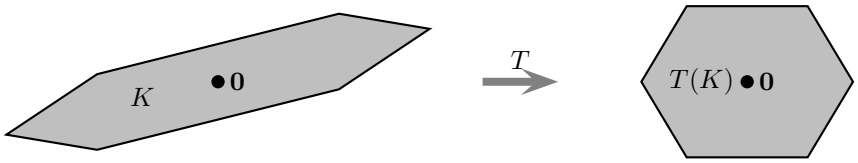

Figure 2.1: Visualization of bringing a symmetric convex body K into ℓ-position (see Theorem 2.2).

If the ℓ-value of K° is small, then K itself cannot be too large and we can bound its volume:

LEMMA 2.3. *For any symmetric convex body $K \subseteq \mathbb{R}^n$ one has* $\mathrm{Vol}_n(K)^{1/n} \lesssim \frac{\ell_{K^\circ}}{n}$.

This lemma is a consequence of *Urysohn's inequality* which denotes the fact that among convex bodies of the same volume, the Euclidean ball minimizes the *mean width*. Again, we refer to [3].

2.2 Lattices. For a full rank lattice $\Lambda \subseteq \mathbb{R}^n$ we define the *dual lattice* as $\Lambda^* = \{x \in \mathbb{R}^n \mid \langle x, y\rangle \in \mathbb{Z}\ \forall y \in \Lambda\}$. Note that $\det(\Lambda) \cdot \det(\Lambda^*) = 1$ and $(\Lambda^*)^* = \Lambda$. The *shortest vector* in a lattice is denoted by $\lambda_1(\Lambda) := \min\{\|x\|_2 : x \in \Lambda \setminus \{\mathbf{0}\}\}$ and more generally $\lambda_i(\Lambda) := \min\{r \geq 0 \mid \dim(\mathrm{span}(\Lambda \cap rB_2^n)) \geq i\}$ denotes the *ith successive minimum*, see Figure 2.2. For a symmetric convex body $K \subseteq \mathbb{R}^n$ we also write $\lambda_i(\Lambda, K)$ as the ith successive minimum w.r.t. norm $\|\cdot\|_K$.

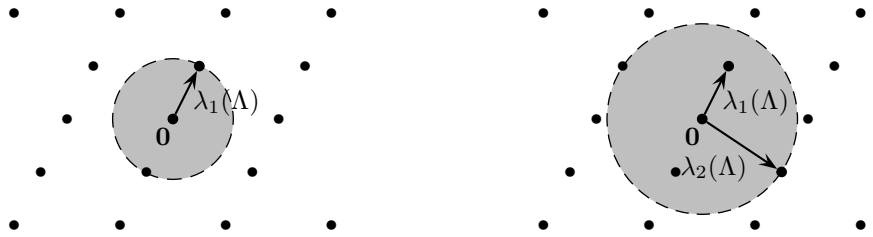

Figure 2.2: Visualization of shortest vector and successive minima.

For a parameter $t > 0$ and $x \in \mathbb{R}^n$ we let $\rho_t(x) := \exp(-\pi\|x/t\|_2^2)$ and we abbreviate $\rho_t(\Lambda) := \sum_{x\in\Lambda} \rho_t(x)$ which is also called the *discrete Gaussian weight of* Λ.

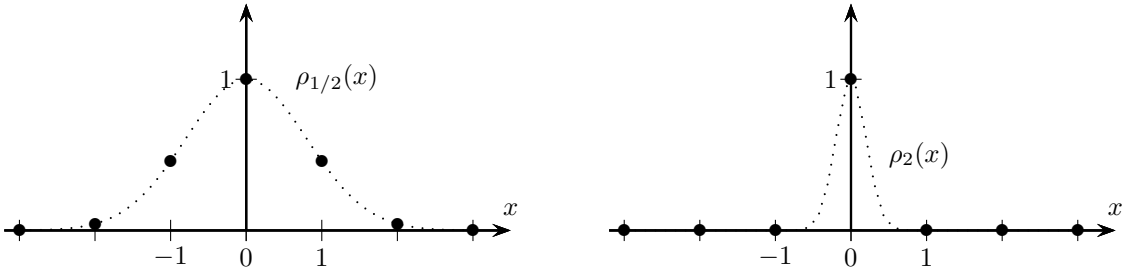

Figure 2.3: Discrete Gaussian of lattice $\mathbb{Z}$ for $t = 1/2$ and $t = 2$.

The discrete Gaussian weight allows for powerful reasoning about the lattice. For lack of space, we can only state a few needed facts, for proofs and more details we recommend the excellent notes of Regev [29]. We can observe that the origin will always contribute a value of 1 to $\rho_t(\Lambda)$. One can prove that if Λ^* is so sparse that the non-zero lattice points contribute little to $\rho_{1/t}(\Lambda^*)$, then Λ is so dense that $\rho_t(u + \Lambda)$ is approximately invariant for any shift u.

THEOREM 2.4. *Let $t > 0$ and let $\Lambda \subseteq \mathbb{R}^n$ be a full rank lattice with $\rho_{1/t}(\Lambda^* \setminus \{\mathbf{0}\}) \leq \frac{1}{2}$. Then for any $u \in \mathbb{R}^n$ one has $\frac{1}{3}\rho_t(\Lambda) \leq \rho_t(u + \Lambda) \leq \rho_t(\Lambda)$.*

This claim can be derived from the *Poisson Summation Formula* which relates the discrete Gaussian weight of the primal lattice Λ to the discrete Gaussian weight of the dual Λ^*. In fact, more generally it says that for any "nice enough" function $f : \mathbb{R}^n \to \mathbb{C}$ one has $f(\Lambda) = \det(\Lambda^*) \cdot \hat{f}(\Lambda^*)$ where $\hat{f}$ denotes the *Fourier transform* of f. Another result by Banaszczyk [4] is that a symmetric convex body K with say $\ell_K \leq 0.01$ is so huge that it contains most of the discrete Gaussian weight of any lattice. For example a Euclidean ball with radius $C\sqrt{n}$ for where $C \gg 1$ will have an ℓ-value of say 0.01.

THEOREM 2.5 (Banaszczyk [4]). *For any $\varepsilon > 0$, there is a $\delta > 0$ so that the following holds: for any symmetric convex body $K \subseteq \mathbb{R}^n$ with $\ell_K \leq \delta$, any full rank lattice $\Lambda \subseteq \mathbb{R}^n$ and any shift $u \in \mathbb{R}^n$ one has $\rho_1((u + \Lambda) \setminus K) \leq \varepsilon \cdot \rho_1(K)$.*

This result is an elegant combination of the fact that sampling a lattice point proportional to $\rho_1(x)$ gives a distribution that is $O(1)$-subgaussian in any direction with Talagrand's *Majorizing Measure Theorem*.

Consider a full rank lattice $\Lambda \subseteq \mathbb{R}^n$. A sublattice which is of the form $\Lambda \cap W$ for some subspace W is called *primitive*. Similarly, a *lattice subspace* W is a subspace with $\mathrm{span}(\Lambda \cap W) = W$. For a lattice Λ and a primitive sublattice $\Lambda' \subseteq \Lambda$, we define the *quotient lattice* as $\Lambda/\Lambda' := \Pi_{\mathrm{span}(\Lambda')^\perp}(\Lambda)$, see Figure 2.4. In many ways one can imagine that the quotient operation factors Λ into two lattices Λ' and Λ/Λ'. In particular $\det(\Lambda) = \det(\Lambda') \cdot \det(\Lambda/\Lambda')$.

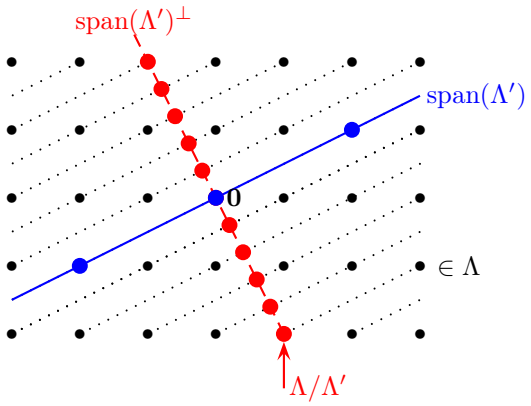

Figure 2.4: Lattice Λ with sublattice Λ' and quotient sublattice Λ/Λ'.

A lattice $\Lambda \subseteq \mathbb{R}^n$ is called *stable* if $\det(\Lambda) = 1$ and $\det(\Lambda') \geq 1$ for all sublattices $\Lambda' \subseteq \Lambda$. Intuitively, a stable lattice does not contain any sublattice that is denser than the lattice itself. For example $\mathbb{Z}^n$ is stable as well as the 2-dimensional lattice depicted in Figure 1.1. One might get the impression that stable lattices are very special and as we are aiming to prove a statement for arbitrary lattices, stability might not look useful to us. But it turns out that every lattice has a decomposition into stable lattices! To see this, let $\Lambda \subseteq \mathbb{R}^n$ be any lattice. Consider the 2-dimensional point set

$$Q := \big\{(\mathrm{rank}(\Lambda'), \ln(\det(\Lambda'))) \mid \text{sublattice } \Lambda' \subseteq \Lambda\big\}$$

Next, consider the extreme points of the *lower envelope* of the convex hull $\mathrm{conv}(Q)$. Each extreme point must arise from (at least) one lattice. Let us denote those lattices as $\Lambda_0, \ldots, \Lambda_k$, sorted by increasing rank, see Figure 2.5.

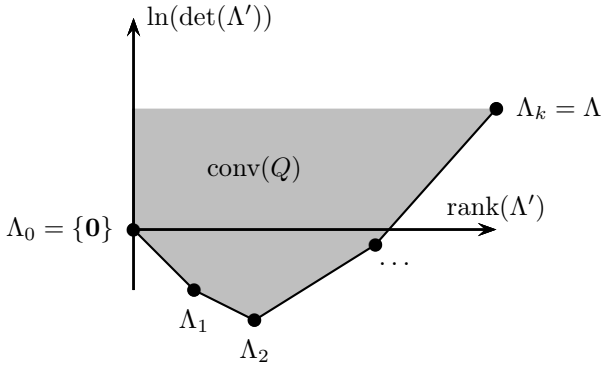

Figure 2.5: Canonical filtration

Clearly, by construction each Λ_i is the densest sublattice among all $\mathrm{rank}(\Lambda_i)$-dimensional sublattices of Λ. The sequence $\Lambda_0, \ldots, \Lambda_k$ is also called the *canonical filtration*. These lattices have a number of wonderful properties:

THEOREM 2.6 (Canonical filtration). *Let $\Lambda_0, \ldots, \Lambda_k$ be lattices corresponding to extreme points of the lower envelope of conv(Q) as defined above. Then:*

(i) Every extreme point on the lower envelope arises from a unique sublattice of Λ.

(ii) The lattices form a chain*, i.e. $\{\mathbf{0}\} = \Lambda_0 \subset \Lambda_1 \subset \ldots \subset \Lambda_k = \Lambda$.*

(iii) The normalized determinants $r_i := \det(\Lambda_i/\Lambda_{i-1})^{1/rank(\Lambda_i/\Lambda_{i-1})}$ satisfy $r_1 < \ldots < r_k$.

(iv) Each quotient lattice $\frac{1}{r_i}(\Lambda_i/\Lambda_{i-1})$ is stable.

Much of these statements follows from the fact that the log determinant function is *submodular*. To be precise, for any two primitive sublattices $\Lambda', \Lambda'' \subseteq \Lambda$ one has

$$\ln(\det(\Lambda' \cap \Lambda'')) + \ln(\det(\Lambda' + \Lambda'')) \leq \ln(\det(\Lambda')) + \ln(\det(\Lambda'')).$$

Item (*iii*) on the other hand is equivalent to the fact that the slopes of the segments defining the lower envelope of $\mathrm{conv}(Q)$ are increasing.

For the original work of these claims, see [14, 37, 13]. For a more recent exposition with detailed proofs we refer to [32] or the thesis of Stephens-Davidowitz [36]. Another useful fact will be the following:

LEMMA 2.7. *If Λ is stable then also Λ^* is stable.*

Finally, it will be convenient to have a triangle inequality for the covering radius. Note that K may not be symmetric and so $\|\cdot\|_K$ is not a norm. Still the following holds true where $\mathrm{int}(K)$ denotes the *interior* of K:

LEMMA 2.8 (Triangle inequality for covering radius). *Let Λ be a full rank lattice and let $K \subseteq \mathbb{R}^n$ be a convex body with $\mathbf{0} \in int(K)$. Then for any lattice subspace $W \subseteq \mathbb{R}^n$ one has*

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

See [33] for a proof.

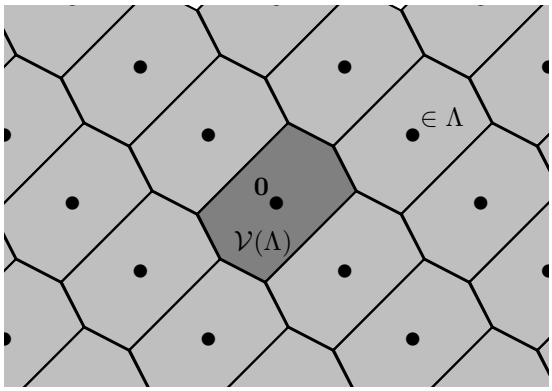

Figure 3.1: Voronoi cell of Λ and the induced tiling.

3 Subspace flatness for Euclidean balls and the Reverse Minkowski Theorem. Next, we want to explain why Theorem 1.5 is true and what goes into proving it. To be more precise we want to show that for any full rank lattice $\Lambda \subseteq \mathbb{R}^n$ one has

$$\mu(\Lambda, B_2^n) \leq \text{polylog}(n) \cdot \mu_{KL}(\Lambda, B_2^n), \tag{3.1}$$

where for the moment we are not further concerned what polylogarithmic factor we obtain. As we have just seen, the canonical filtration $\{\mathbf{0}\} = \Lambda_0 \subset \Lambda_1 \subset \ldots \subset \Lambda_k = \Lambda$ provides us with a decomposition of Λ into stable lattices. In the case of the Euclidean ball, this can be used to bound the covering radius as

$$\mu(\Lambda, B_2^n)^2 \leq \sum_{i=1}^{k} \mu(\Lambda_i/\Lambda_{i-1}, B_2^{d_i})^2$$

where $d_i := \text{rank}(\Lambda_i/\Lambda_{i-1})$ and all the quotient lattices are scalars of a stable lattice. We will not justify this inequality here further, but we take it as motivation to restrict our attention to the case where Λ was already a stable full rank lattice. Even under this assumption how would one then go on proving (3.1) in the first place? Suppose $W \subseteq \mathbb{R}^n$ is the subspace attaining $\mu_{KL}(\Lambda, B_2^n)$ where $d := \dim(W)$. Then $\text{Vol}_d(\Pi_W(B_2^n))^{1/d} = \text{Vol}_d(B_2^d)^{1/d} \asymp \frac{1}{\sqrt{d}}$. Moreover for the determinant one has $\det(\Pi_W(\Lambda)) = \frac{1}{\det(\Lambda^* \cap W)} \leq 1$ since projection and intersection are dual operations and since Λ^* is also stable (see Lemma 2.7). That means the optimal choice for the subspace must be $W := \mathbb{R}^n$, in which case $\mu_{KL}(\Lambda, B_2^n) \asymp \sqrt{n}$. Hence proving (3.1) for a stable lattice boils down to proving that $\mu(\Lambda, B_2^n) \leq \text{polylog}(n) \cdot \sqrt{n}$. This however turns out to be a rather challenging problem which requires the breakthrough result by Regev and Stephens-Davidowitz.

THEOREM 3.1 (Reverse Minkowski Theorem [31, 32]). *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 $s = C\log(n)$ one has $\rho_{1/s}(\Lambda) \leq \frac{3}{2}$.*

This beautiful result was presented by Oded Regev at ICM 2022 and here we will be satisfied with a very rough sketch of the rather miraculous proof. In the following we will interchangingly interpret a matrix $T \in \mathbb{R}^{n \times n}$ also as the corresponding linear map $T : \mathbb{R}^n \to \mathbb{R}^n$ with $T(x) = Tx$.

Proof sketch of Theorem 3.1. By using the canonical filtration one can reduce the claim to the case of stable lattices. Hence it suffices to prove that $\rho_{1/s}(\Lambda) \leq \frac{3}{2}$ for a full rank stable lattice $\Lambda \subseteq \mathbb{R}^n$. First, consider the *Voronoi cell*

$$\mathcal{V}(\Lambda) := \Big\{ x \in \mathbb{R}^n \mid \langle x, y \rangle \leq \frac{1}{2}\|y\|_2^2 \ \ \forall y \in \Lambda \Big\}$$

which is the set of points that are closer (or at equal distance) to the origin than any other lattice point, see Figure 3.1.

We note that $\mathcal{V}(\Lambda)$ is a centrally symmetric convex body. It is not difficult to prove that

$$\rho_{1/s}(\Lambda) \cdot \gamma_n\big(\sqrt{2\pi}s \cdot \mathcal{V}(\Lambda)\big) \leq 1. \tag{3.2}$$

That means in order to prove an *upper bound* on the discrete Gaussian weight it suffices to prove a *lower bound* on the Gaussian measure of the Voronoi cell of a stable lattice. It will be convenient to fix an upper bound N and prove by induction over $n \in \{1, \dots, N\}$ that

$$\gamma_n(t \cdot \mathcal{V}(\Lambda)) \geq \exp\Big(-\frac{n}{4N^2}\Big)$$

for any full rank stable lattice $\Lambda \subseteq \mathbb{R}^n$ where $t = \Theta(\log N)$ with a large enough implicit constant. Doing the induction in this non-standard way we can avoid having to change the parameter t as we recurse. So, for a given n, fix a stable lattice $\Lambda \subseteq \mathbb{R}^n$ (which exists for compactness reasons) that *minimizes* the Gaussian measure $\gamma_n(\frac{t}{2} \cdot \mathcal{V}(\Lambda))$.

If there happens to be a sublattice $\Lambda' \subseteq \Lambda$ with $\det(\Lambda') = 1$ then one can argue that both Λ' and the quotient lattice Λ/Λ' are stable as well. Hence one can apply induction and obtain

$$\begin{aligned}\gamma_n(t \cdot \mathcal{V}(\Lambda)) &\geq \gamma_n(t \cdot \mathcal{V}(\Lambda')) \cdot \gamma_n(t \cdot \mathcal{V}(\Lambda/\Lambda')) \\ &\overset{\text{induction}}{\geq} \exp\Big(-\frac{\operatorname{rank}(\Lambda')}{4N^2}\Big) \cdot \exp\Big(-\frac{\operatorname{rank}(\Lambda/\Lambda')}{4N^2}\Big) = \exp\Big(-\frac{n}{4N^2}\Big)\end{aligned}$$

and we are done.

So in the remaining case one may assume that $\det(\Lambda') > 1$ for any proper sublattice $\Lambda' \subset \Lambda$. Now we want to exploit a *variational argument*. For concreteness, let $B \in \mathbb{R}^{n \times n}$ be the basis of Λ. Recall that $\det(B) = 1$ because Λ is stable. Consider the sets of matrices

$$\begin{aligned}X &:= \{A \in \mathbb{R}^{n \times n} \mid \det(A) = 1\} \\ X_{\text{stable}} &:= \{A \in \mathbb{R}^{n \times n} \mid \det(A) = 1 \text{ and } \det(\Lambda') \geq 1 \text{ for all } \Lambda' \subseteq A(\Lambda)\}\end{aligned}$$

where $A(\Lambda)$ is the lattice linearly transformed by A. Note that $A \in X_{\text{stable}}$ if and only if $A(\Lambda)$ is stable. Then trivially $I_n \in X_{\text{stable}} \subseteq X$ as Λ is stable. We want to understand what happens as we vary the linear transformation A near I_n. Consider the function

$$G(A) := \frac{1}{|\det(A)|} \cdot \gamma_n\Big(\frac{t}{2} \cdot \mathcal{V}(A(\Lambda))\Big)$$

By the choice of Λ, I_n is a *global minimum* of $G_{|X_{\text{stable}}}$, which is the restriction of G to X_{stable}. But none of the $\det(..) \geq 1$ constraints were tight and so I_n must at least be a *local minimum* of $G_{|X}$. But X only has a single constraint of $\det(A) = 1$ and so the gradient of G at I_n must be some scalar multiple of the gradient of the determinant function. That means

$$(\nabla_A(G(A)))_{|A=I_n} = \alpha \cdot \nabla_A(\det(A))_{|A=I_n} = \alpha \cdot I_n$$

for some $\alpha \in \mathbb{R}$, see Figure 3.2 for a poor attempt of a visualization.

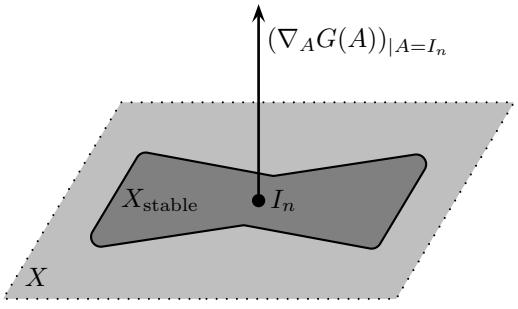

Figure 3.2: Schematic picture of manifold X and X_{stable}

Doing some more careful analysis (which we skip here) one can then derive that

$$\int_{\mathcal{V}(\Lambda)} \rho_{\Theta(1/t)}(x) \cdot xx^T dx = \beta \cdot I_n \tag{3.3}$$

for some $\beta \in \mathbb{R}$. Then (3.3) means that the Voronoi cell $\mathcal{V}(\Lambda)$ is in *Gaussian isotropic position* (w.r.t. to the Gaussian density $\rho_{\Theta(1/t)}$). Now we need a few deep tools from convex Geometry:

Fact I (Bobkov [6]). *If $K \subseteq \mathbb{R}^n$ is a symmetric convex body in Gaussian isotropic position ($\frac{1}{(2\pi)^{n/2}} \int_K e^{-\|x\|_2^2/2} xx^T dx = \beta I_n$ for some $\beta \in \mathbb{R}$), then $\gamma_n(K) \geq \gamma_n(T(K))$ for any linear map T with $\det(T) = 1$.*

Fact II (Figiel, Tomczak-Jaegermann, Lewis, Pisier). *For any symmetric convex body $K \subseteq \mathbb{R}^n$ with $\mathrm{Vol}_n(K) = 1$ there is a linear map T with $\det(T) = 1$ so that $\gamma_n(\Theta(\log n) \cdot T(K)) \geq \frac{2}{3}$.*

Fact III (Boosting). *For any symmetric convex body $K \subseteq \mathbb{R}^n$ with $\gamma_n(K) \geq \frac{1}{2}$ and $rB_2^n \subseteq K$ for $r > 0$ one has $\gamma_n(2K) \geq 1 - \exp(-\Theta(r^2))$.*

Note that the linear map T guaranteed in Fact II is the one from Theorem 2.2. Then we can derive that

$$\gamma_n\Big(\frac{t}{2} \cdot \mathcal{V}(\Lambda)\Big) \overset{\text{Fact I}}{\geq} \gamma_n\Big(\frac{t}{2} \cdot T(\mathcal{V}(\Lambda))\Big) \overset{\text{Fact II}}{\geq} \frac{2}{3}$$

using that the Voronoi cell of a stable lattice has indeed $\mathrm{Vol}_n(\mathcal{V}(\Lambda)) = \det(\Lambda) = 1$. But this probability is not quite enough for us, hence we now apply boosting. Since Λ is stable, the shortest vector must have length $\lambda_1(\Lambda) \geq 1$ and so $\frac{1}{2}B_2^n \subseteq \mathcal{V}(\Lambda)$ which in turn means that $\frac{t}{4}B_2^n \subseteq \frac{t}{2}\mathcal{V}(\Lambda)$. Then

$$\gamma_n(t \cdot \mathcal{V}(\Lambda)) \overset{\text{Fact III}}{\geq} 1 - \exp(-\Theta(t^2)) \geq \exp\Big(-\frac{1}{4N^2}\Big)$$

and we are done[3]. ∎

As mentioned earlier, already Dadush and Regev [10] found a reduction from (3.1) to the statement in Theorem 3.1 but at the time they did not go via the canonical filtration. On an intuitive level one can understand the Reverse Minkowski Theorem as the fact that a stable lattice does not have too many short vectors, as any short vector would contribute significantly to $\rho_{1/s}(\Lambda)$. More precisely, Theorem 3.1 implies the following:

COROLLARY 3.2. *For any stable lattice $\Lambda \subseteq \mathbb{R}^n$ and any $r \geq 1$ one has $|\Lambda \cap rB_2^n| \leq 2^{O(\log^2 n) \cdot r^2}$.*

In particular the number of lattice vectors of length at most some constant is at most *quasi-polynomial* in n — any previously known argument would have only provided an exponential bound. Though in regard of proving that $\mu(\Lambda, B_2^n) \leq \mathrm{polylog}(n) \cdot \sqrt{n}$, we would need to argue that a stable lattice is sufficiently dense everywhere while the Reverse Minkowski Theorem appears to prove the opposite. But then again, if Λ is stable then the dual lattice Λ^* is stable as well (see Lemma 2.7) and Theorem 2.4 provides the crucial connection.

THEOREM 3.3. *Let $\Lambda \subseteq \mathbb{R}^n$ be a full rank stable lattice. Then the following holds:*

(i) One has $\mu(\Lambda, B_2^n) \leq O(\log n \cdot \sqrt{n})$.

(ii) Let K be a symmetric convex body with $\ell_K \leq c$ where $c > 0$ is a small enough universal constant. Then $\mu(\Lambda, K) \leq O(\log n)$.

Proof. We note that $(ii) \Rightarrow (i)$. Hence we prove (ii), which is more general but only needed later in Section 4. Let $s := \Theta(\log n)$ be the parameter from the Reverse Minkowski Theorem (Theorem 3.1). We assume for the sake of contradiction that $\mu(\Lambda, K) > s$. We make three observations:

[3]Note that we were forced to use two different scaling factors of t and $\frac{t}{2}$. It might be possible to combine Fact II and Fact III into the following statement to avoid this. **Conjecture.** *For any symmetric convex body $K \subseteq \mathbb{R}^n$ with $\mathrm{Vol}_n(K) = 1$ there is a linear map T with $\det(T) = 1$ so that $\gamma_n(t \cdot T(K)) \geq 1 - e^{-c_1 t^2}$ for any $t \geq c_2 \log(n)$ where $c_1, c_2 > 0$ are suitable constants.* This seems plausible to the author of these lines but he is not aware of a proof.

It may also appear odd that we start out with a stable lattice Λ that *minimizes* the Gaussian measure of $\mathcal{V}(\Lambda)$ and then conclude via Fact I that the Gaussian measure is *maximized*! But the minimum is attained with respect to $\mathcal{V}(A(\Lambda))$ where A is a volume-preserving linear map and the maximum is for $T(\mathcal{V}(\Lambda))$.

(A) The assumption $\mu(\Lambda, K) > s$ means that there is a large hole in the lattice and for some shift $u \in \mathbb{R}^n$ one has $(u + \Lambda) \cap sK = \emptyset$.

(B) The dual of Λ is stable and hence by the Reverse Minkowski Theorem one has $\rho_{1/s}(\Lambda^* \setminus \{\mathbf{0}\}) \leq \frac{1}{2}$. Hence by Theorem 2.4, $\rho_s(u + \Lambda) \geq \frac{1}{3}\rho_s(\Lambda)$.

(C) The body K is so large that by Banaszczyk's Theorem (Theorem 2.5) it contains most of the discrete Gaussian weight, i.e. $\rho_s((u + \Lambda) \setminus sK) \leq \varepsilon\rho_s(K)$ where we can make $\varepsilon > 0$ as small as needed by adjusting c.

But $(A), (B), (C)$ contradict each other as

$$\frac{1}{3}\rho_s(\Lambda) \overset{(B)}{\leq} \rho_s(u + \Lambda) \overset{(A)}{=} \rho_s((u + \Lambda) \setminus sK) \overset{(C)}{\leq} \varepsilon\rho_s(\Lambda).$$

if we pick $0 < \varepsilon < \frac{1}{3}$. □

The bound stated in Theorem 3.3.(i) then suffices to derive the inequality $\mu(\Lambda, B_2^n) \leq O(\log^{3/2}(n)) \cdot \mu_{KL}(\Lambda, B_2^n)$ for stable lattices and then in turn for arbitrary lattices. This is the bound that was originally stated in Regev and Stephens-Davidowitz [31, 32]. But [31, 32] also provide a different line of arguments to upper bound the covering radius of a stable lattice. Assuming *Bourgain's Slicing Conjecture*, [31, 32] prove that even $\mu(\Lambda, B_2^n) \leq O(\sqrt{n})$ for any stable lattice Λ. In the meanwhile, Bourgain's Slicing Conjecture has indeed been proven by Klartag and Lehec [18] which then implies the following:

THEOREM 3.4 ([31, 32, 18]). *For any full rank stable lattice $\Lambda \subseteq \mathbb{R}^n$ one has $\mu(\Lambda, B_2^n) \leq O(\sqrt{n})$.*

Using Theorem 3.4 instead of Theorem 3.3.(i) one obtains the bound of $\mu(\Lambda, B_2^n) \leq O(\sqrt{\log(n)}) \cdot \mu_{KL}(\Lambda, B_2^n)$ for any lattice as claimed in Theorem 1.5.

4 The general case of Subspace flatness. In this section we want to prove main result of this survey, Theorem 1.6 and the inequality

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

for a full rank lattice $\Lambda \subseteq \mathbb{R}^n$ and an arbitrary convex body $K \subseteq \mathbb{R}^n$. The first issue is that much of the tools that we plan on using only hold in the presence of symmetry. Hence we temporarily need to replace K by a symmetric body. One (of the two) canonical choices is as follows: translate K so that its *barycenter* $\frac{1}{\text{Vol}_n(K)} \int_K x \, dx$ (or *centroid*) lies at the origin; then set $Q := K \cap (-K)$. A classical result by Milman and Pajor [25] says that $\text{Vol}_n(Q) \geq 2^{-n}\text{Vol}_n(K)$, meaning that Q is not actually that much smaller than K.

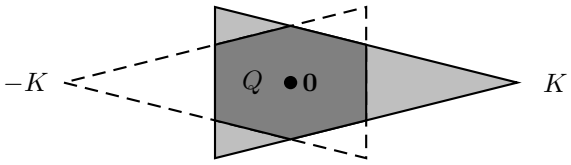

Figure 4.1: Inner symmetrizer $Q = K \cap -K$.

Another challenge is the following: even for a well-scaled symmetric convex body such as the cube, if we consider the volume $\text{Vol}_d(\Pi_W(B_\infty^n))^{1/d}$ of the projection into a d-dimensional subspace W, then this quantity can — dependent on the choice of W — vary by a factor of the order $\sqrt{n/d}$. We would like to fix this issue by restricting our attention to subspaces of dimension $d \geq \frac{n}{2}$. But then the actual covering radius $\mu(\Lambda, K)$ might be genuinely controlled by some low dimensional subspace which we could not capture. The solution is to upper bound only the covering radius for half the dimensions as well:

PROPOSITION 4.1. *For any full rank lattice $\Lambda \subseteq \mathbb{R}^n$ and any convex body $K \subseteq \mathbb{R}^n$ with the barycenter at the origin, there is a primitive sublattice $\Lambda' \subseteq \Lambda$ with rank$(\Lambda') \geq \frac{n}{2}$ so that*

$$\mu\big(\Lambda', Q \cap \textit{span}(\Lambda')\big) \leq O(\log^2(n)) \cdot \mu_{KL}(\Lambda, K).$$

where $Q := (-K) \cap K$.

This is the main technical contribution of [33] and we attempt to sketch the proof.

Proof Sketch. We know from Theorem 3.3 that in order to obtain a good upper bound on the covering radius we need an upper bound on the ℓ-value. On the other hand in order to obtain a good volume upper bound, by Lemma 2.3 we need an upper bound on the ℓ-value of the polar. Hence we bring Q into ℓ-position using Theorem 2.2 (and apply the same linear transformation to the lattice Λ). From now on we assume that $\ell_Q \cdot \ell_{Q^\circ} \leq O(n \log n)$. Let $\{\mathbf{0}\} = \Lambda_0 \subset \Lambda_1 \subset \ldots \subset \Lambda_k = \Lambda$ be the canonical filtration of our lattice. We abbreviate the dimensions and normalized determinants of the corresponding quotient lattices by

$$d_i := \operatorname{rank}(\Lambda_i/\Lambda_{i-1}) \quad \text{and} \quad r_i := \det(\Lambda_i/\Lambda_{i-1})^{1/d_i}$$

for $i = 1, \ldots, k$. From Theorem 2.6 we know that $r_1 < r_2 < \ldots < r_k$. But we do not know by how much those normalized determinants increase. However for indices $i \leq j$ with $r_{i-1} < \frac{r_j}{2} \leq r_i$ we can replace the quotient lattices $\Lambda_i/\Lambda_{i-1}, \ldots, \Lambda_j/\Lambda_{j-1}$ by Λ_j/Λ_{i-1}. The quotient lattice Λ_j/Λ_{i-1} is not exactly the scalar of a stable lattice but satisfies an approximate such notion. Then the covering radius bounds from Theorem 3.3 still hold with a constant factor loss. To simplify notion here, let us assume that the normalized determinants were geometrically increasing in the first place, i.e. $r_i \leq \frac{1}{2} r_{i+2}$ for all i; for a rigorous justification see the work of Reis and Rothvoss [33]. Next, let $i^* \in \{1, \ldots, k\}$ be minimal s.t. $\operatorname{rank}(\Lambda_{i^*}) \geq \frac{n}{2}$. Then we make a choice of $\Lambda' := \Lambda_{i^*}$. Intuitively, this means in the claim of Prop 4.1 we are upper bounding the covering radius for the *densest* $\frac{n}{2}$-dimensional sublattice of Λ. The analysis breaks into two parts.

Upper bounding the covering radius $\mu(\Lambda_{i^*}, Q \cap \operatorname{span}(\Lambda_{i^*}))$. The covering radius satisfies a triangle inequality in the form

$$\begin{aligned} \mu(\Lambda_{i^*}, Q \cap \operatorname{span}(\Lambda_{i^*})) &\leq \sum_{j=1}^{i^*} \mu(\Lambda_j/\Lambda_{j-1}, Q_j) \\ &\overset{\text{Thm 3.3}}{\leq} O(\log n) \cdot \underbrace{\sum_{j=1}^{i^*} r_j}_{\leq O(r_{i^*})} \underbrace{\ell_{Q_j}}_{\leq \ell_Q} \\ &\leq O(\log n) \cdot \ell_Q \cdot r_{i^*} \end{aligned} \tag{4.1}$$

One can prove via Lemma 2.8 that the right bodies Q_j to use in that triangle inequality are $Q_j := \Pi_{\operatorname{span}(\Lambda_{j-1})^\perp}(Q \cap \operatorname{span}(\Lambda_j))$. The ℓ-value cannot increase when projecting or intersecting with a lower dimensional subspace and so $\ell_{Q_j} \leq \ell_Q$. We also have used Theorem 3.3 with the fact that $\frac{1}{r_j}(\Lambda_j/\Lambda_{j-1})$ is stable.

Lower bounding $\mu_{KL}(\Lambda, K)$. The first crucial step is to make a choice for the subspace W that provides a good enough lower bound on $\mu_{KL}(\Lambda, K)$. We set $W := \operatorname{span}(\Lambda_{i-1})^\perp$. We note that $d := \dim(W) \geq \frac{n}{2}$ and $\Pi_W(\Lambda) = \Lambda/\Lambda_{i^*-1}$. Note that $d = d_{i^*} + \ldots + d_k$. Intuitively our choice for W groups the *sparsest* $n/2$ dimensions of quotient lattices from the canonical filtration together. The determinant of the projected lattice is

$$\det(\Lambda/\Lambda_{i^*-1})^{1/d} = \Big(\prod_{j=i^*}^{k} r_j^{d_j} \Big)^{1/d} \geq r_{i^*} \tag{4.2}$$

because the geometric average of the numbers $r_{i^*}, \ldots, r_k$ must be at least r_{i^*}. For the volume of the projection we can upper bound

$$\operatorname{Vol}_d(\Pi_W(K))^{1/d} \overset{(*)}{\lesssim} \underbrace{\Big(\frac{n}{d}\Big)^6}_{\leq O(1)} \cdot \operatorname{Vol}_d(\Pi_W(Q))^{1/d} \overset{\text{Lem 2.3}}{\lesssim} \frac{\ell_{Q^\circ}}{d} \leq O\Big(\frac{\log n}{\ell_Q}\Big) \tag{4.3}$$

We want to explain why $(*)$ holds. Here we want to compare the volume of $\Pi_W(K)$ with the volume of the smaller set $\Pi_W(Q)$. Without the projection we know that $\operatorname{Vol}_n(Q)^{1/n} \geq \frac{1}{2}\operatorname{Vol}_n(K)^{1/n}$ by the classical inequality of Pajor and Milman. It turns out that this inequality can be generalized to projections of convex bodies where

the loss is polynomial in $\frac{\dim(W)}{n}$, see the recent work of Vritsiou [38]. Hence the lower bound on the proxy that we obtain from our choice of W is

$$\mu_{KL}(\Lambda, K) \overset{(4.2)+(4.3)}{\geq} \Big(\frac{\det(\Lambda/\Lambda_{i^*-1})}{\mathrm{Vol}_d(\Pi_W(K))}\Big)^{1/d} \geq \Omega\Big(\frac{1}{\log(n)}\Big) \cdot r_i^* \cdot \ell_Q \tag{4.4}$$

Overall, adding the upper and lower bounds from (4.1) and (4.4) together gives that

$$\mu(\Lambda_{i^*}, Q \cap \mathrm{span}(\Lambda_{i^*})) \leq O(\log n) \cdot \ell_Q \cdot r_{i^*} \leq O(\log^2 n) \cdot \mu_{KL}(\Lambda, K)$$

as claimed. ∎

Now we can prove the main result which we restate for convenience:

THEOREM 4.2 (Theorem 1.6 restated). *For any full rank lattice $\Lambda \subseteq \mathbb{R}^n$ and any convex body $K \subseteq \mathbb{R}^n$ one has*

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

Proof. Denote the implicit constant in Prop 4.1 by $C > 0$. We prove by induction over n that

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

After translating we may assume that the barycenter of K lies at the origin. Again, set $Q := K \cap (-K)$ and let $\Lambda' \subseteq \Lambda$ be the sublattice guaranteed by Prop 4.1. We abbreviate $W := \mathrm{span}(\Lambda')$. Then using the triangle inequality for the covering radius we can bound

$$\begin{aligned}
\mu(\Lambda, K) &\leq \mu(\Lambda \cap W, Q \cap W) + \mu(\Pi_{W^\perp}(\Lambda), \Pi_{W^\perp}(K)) \\
&\overset{(**)}{\leq} C \log^2(n) \cdot \mu_{KL}(\Lambda, K) + C \log\Big(\frac{n}{2}\Big)^3 \cdot \underbrace{\mu_{KL}(\Pi_{W^\perp}(\Lambda), \Pi_{W^\perp}(K))}_{\leq \mu_{KL}(\Lambda, K)} \\
&\leq C \log^3(n) \cdot \mu_{KL}(\Lambda, K)
\end{aligned}$$

In $(**)$ we use Prop 4.1 on the left side and induction on the right. Finally note that projections can only decrease the covering radius proxy μ_{KL}. This concludes the argument. ∎

5 Applications

5.1 Bounds on the flatness constant. In this section, we explain another application of Theorem 1.6. One additional ingredient that we require is arguably the most classical result in the geometry of numbers:

THEOREM 5.1 (Minkowski's First Theorem). *Let $K \subseteq \mathbb{R}^n$ be a symmetric convex body and let $\Lambda \subseteq \mathbb{R}^n$ be a full rank lattice. Then there is a vector $c \in \Lambda \setminus \{\mathbf{0}\}$ of length*

$$\|c\|_K \leq 2 \cdot \Big(\frac{\det(\Lambda)}{\mathrm{Vol}_n(K)}\Big)^{1/n}$$

A convex body $K \subseteq \mathbb{R}^n$ is called *lattice-point free*, if $K \cap \mathbb{Z}^n = \emptyset$. It turns out that a lattice-point free convex body must be *flat* in some lattice direction. Let us define the *flatness constant* in dimension n as

$$\mathrm{flt}(n) := \sup_{\substack{K \subseteq \mathbb{R}^n \text{ lattice} \\ \text{point free}}} \min_{c \in \mathbb{Z}^n \setminus \{\mathbf{0}\}} \max\big\{c^T(x-y) : x, y \in K\big\}$$

Khintchine [17] was the first to prove that $\mathrm{flt}(n)$ is indeed finite, providing a bound of $\mathrm{flt}(n) \leq (n+1)!$. Until recently the best known upper bound was $O(n^{4/3+o(1)})$ due to combined work of Rudelson [35] and Banaszczyk, Litvak, Pajor and Szarek [5]. On the other hand, the best known lower bound is $\mathrm{flt}(n) \geq (2 - o(1))n$ due to Mayrhofer, Schade and Weltge [23].

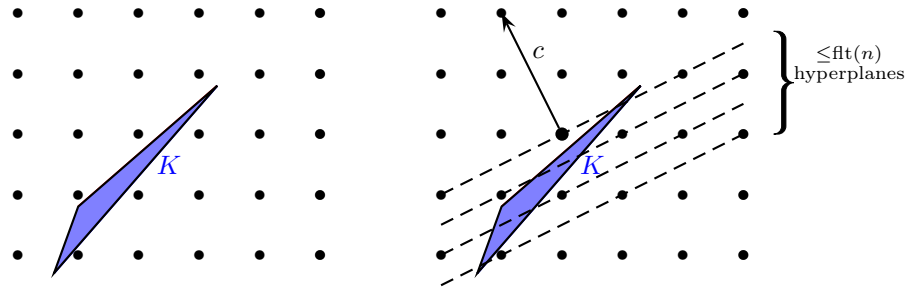

Figure 5.1: Lattice point free convex body K with (not neccessarily optimal) lattice direction c.

Now we can derive a near-optimal upper bound of $\mathrm{flt}(n) \leq O(n \log^3(n))$. We reproduce an argument of Dadush.

THEOREM 5.2. *Let $K \subseteq \mathbb{R}^n$ be a convex body that is lattice point free, i.e. $K \cap \mathbb{Z}^n = \emptyset$. Then there is a $c \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$ so that*

$$\max\{c^T(x-y) : x, y \in K\} \leq O(n \log^3(n))$$

Proof. As K is lattice point free, we know that $\mu(\mathbb{Z}^n, K) > 1$. Then by Theorem 1.6 one has $\mu_{KL}(\mathbb{Z}^n, K) \geq \Omega(\frac{1}{\log^3 n})$. Now consider the *difference body* $Q := K - K$ which is a symmetric convex body that contains some translate of K. A classical estimate by Rogers and Shephard [34] shows that Q is not much bigger than K volume-wise, i.e. $\mathrm{Vol}_n(Q)^{1/n} \leq 4 \cdot \mathrm{Vol}_n(K)^{1/n}$. The same applies to projections of K and the difference body and so $\mu_{KL}(\mathbb{Z}^n, Q) \asymp \mu_{KL}(\mathbb{Z}^n, K) \geq \Omega(\frac{1}{\log^3 n})$. Now we prove the conclusion for the larger body Q. Let $W \subseteq \mathbb{R}^d$ be the subspace attaining $\mu_{KL}(\mathbb{Z}^n, Q)$ and let $d := \dim(W)$ be its dimension. Our strategy is to find a suitable vector $c \in \mathbb{Z}^n \cap W$ in that subspace satisfying the claim. Note that intersection and projection are polar operations and so $(\mathbb{Z}^n)^* \cap W = \Pi_W(\mathbb{Z}^n)^*$ as well as $Q^\circ \cap W = \Pi_W(Q)^\circ$. Combining this with the volume inequality from Theorem 2.1 we have

$$\Big(\frac{\det((\mathbb{Z}^n)^* \cap W)}{\mathrm{Vol}_d(Q^\circ \cap W)}\Big)^{1/d} \asymp d \cdot \Big(\frac{\mathrm{Vol}_d(\Pi_W(Q))}{\det(\Pi_W(\mathbb{Z}^n))}\Big)^{1/d} = \frac{d}{\mu_{KL}(\mathbb{Z}^n, Q)} \leq O(d \log^3 n)$$

Then by Minkowski's Theorem (Theorem 5.1) there must be a non-zero $c \in (\mathbb{Z}^n)^* \cap W$ so that $\|c\|_{Q^\circ \cap W} \leq O(d \log^3 n)$.

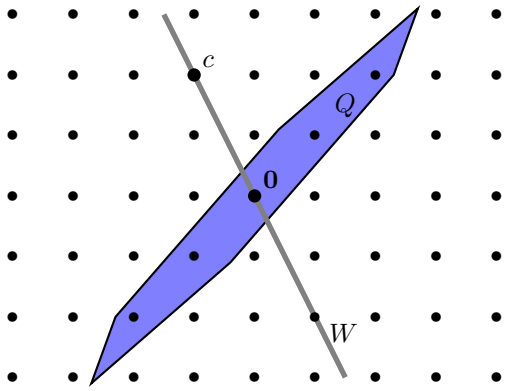

Figure 5.2: Difference body $Q = K - K$ for body K from Fig 5.1

Again by polarity

$$\|c\|_{Q^\circ \cap W} = \max\{|\langle c, x\rangle| : x \in \Pi_W(Q)\} \overset{c \in W}{=} \max\{|\langle c, x\rangle| : x \in Q\}$$

This completes the claim as $d \leq n$ and $(\mathbb{Z}^n)^* = \mathbb{Z}^n$. ∎

In a more general notation, the same result can also be stated as follows:

THEOREM 5.3. *For any convex body $K \subseteq \mathbb{R}^n$ and any full rank lattice $\Lambda \subseteq \mathbb{R}^n$, one has*

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

5.2 A $\log(n)^{O(n)}$-time algorithm for integer programming. One of the most versatile problems in discrete optimization is *integer programming* which is

$$\max\left\{c^T x \mid Ax \leq b, \;\; x \in \mathbb{Z}^n\right\} \qquad \text{(IP)}$$

The seminal algorithm by Lenstra [20] showed how to solve (IP) in time $2^{O(n^2)}$ by using an approximate version of the flatness bound based on the LLL-algorithm [19]. This running time was later improved by Kannan [15] to $n^{O(n)}$ and then by Dadush [11] and by Dadush, Eisenbrand and Rothvoss [9] to $2^{O(n)}n^n$. Now using Theorem 1.6 we can show a significant improvement:

THEOREM 5.4. *Given $A \in \mathbb{Q}^{m\times n}$, $b \in \mathbb{Q}^m$ and $c \in \mathbb{Q}^n$, the integer linear program $\max\{c^T x \mid Ax \leq b, x \in \mathbb{Z}^n\}$ can be solved in time $(\log(n))^{O(n)}$ times a polynomial in the encoding length of A, b and c.*

In fact, the algorithm we are going to present does not need that the feasible region is polyhedral and moreover the objective function can be eliminated using a standard binary search argument. Hence it will be more convenient to rephrase the problem we are about to solve as follows:

> *Given a full rank lattice $\Lambda \subseteq \mathbb{R}^n$ and a convex body $K \subseteq \mathbb{R}^n$, find a point in $K \cap \Lambda$ or decide that there is none.*

We reproduce the algorithm that already appeared in the PhD thesis of Dadush [11]; the only previously missing ingredient was a proof of Theorem 1.6. First, we need an upper bound on the number of lattice points in a convex body:

PROPOSITION 5.5 (Dadush [11]). *For any full rank lattice $\Lambda \subseteq \mathbb{R}^n$ and any convex body $K \subseteq \mathbb{R}^n$ one has*

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

We refer to [11] for the proof. Now suppose we are given K and Λ and we want to find a point in $K \cap \Lambda$. Let us assume for the sake of simplicity that $\mu(\Lambda, K) \geq 1$, that means K is not so huge that always $K \cap \Lambda \neq \emptyset$ (we could shrink K otherwise without loosing feasibility). Let W be the subspace attaining $\mu_{KL}(\Lambda, K)$ and let $d := \dim(W)$. Moreover, we abbreviate $X := \Pi_W(K) \cap \Pi_W(\Lambda)$ as the points in the projection, see Fig 5.3. Then by combining Theorem 1.6 and Prop 5.5 we can bound the number of points in the projection by

$$|X| \leq 2^d \underbrace{\max\{\mu(\Pi_W(\Lambda), \Pi_W(K))^d, 1\}}_{\leq \mu(\Lambda,K)^d} \cdot \frac{\mathrm{Vol}_d(\Pi_W(K))}{\det(\Pi_W(\Lambda))} \leq (\log n)^{O(d)}$$

This suggests a recursive strategy to find points in $K \cap \Lambda$: we enumerate all the points in X. Then for each $y \in X$ we are searching for a point in

$$(K \cap \Pi_W^{-1}(y)) \cap \Lambda$$

which is an $(n-d)$-dimensional integer program. If we denote $T(n)$ as the number of recursive calls that this strategy requires, then we obtain the recursion

$$T(n) \leq (\log n)^{O(d)} \cdot T(n-d) + 1 \qquad (5.1)$$

Regardless of the value of $d \in \{1, \ldots, n\}$, (5.1) is satisfied by $T(n) := (\log n)^{O(n)}$.

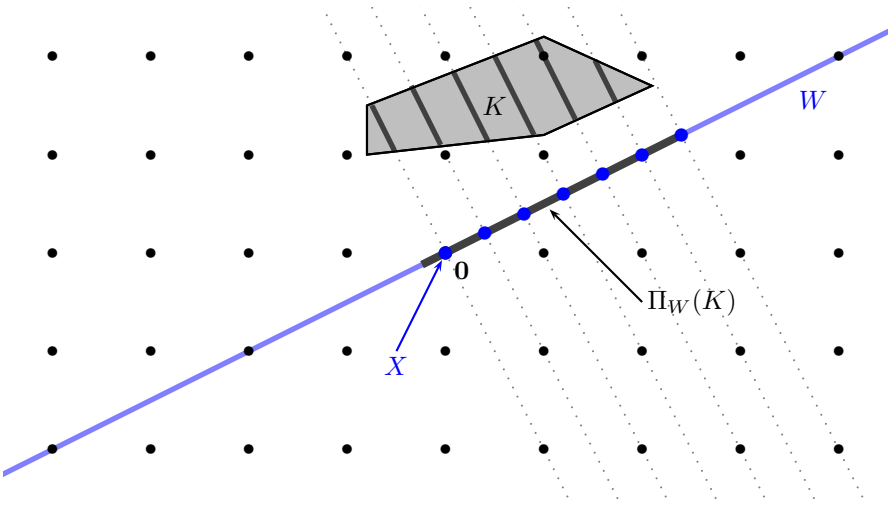

Figure 5.3: Dadush's algorithm

The only remaining gap in our argument is the question how to enumerate X in the first place. We note that finding a point in X is a d-dimensional integer program and as we are designing a recursive algorithm, it would be natural to just use that same algorithm on X. But there is a problem with this approach! It could be that d is as large as n and then we would not actually recurse. Fortunately, Dadush [11] has a solution for this dilemma: Compute an ellipsoid $\mathcal{E}$ so that $N(P,\mathcal{E}), N(\mathcal{E},P) \leq 2^{O(d)}$ where $P := \Pi_W(K)$ is the projection. Such an ellipsoid is also called an *M-ellipsoid* [3]. Here, for two convex bodies $A, B \subseteq \mathbb{R}^n$, $N(A,B)$ denotes the minimum number of translates of B to cover A. Consider the covering of P with $N(P,\mathcal{E})$ many translates of $\mathcal{E}$.

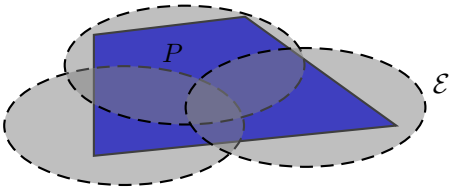

Figure 5.4: Covering of P with $N(P,\mathcal{E})$ translates of $\mathcal{E}$.

For each translate of $\mathcal{E}$ enumerate all the $\Pi_W(\Lambda)$-lattice points in it using the *Voronoi cell algorithm* by Micciancio and Voulgaris [24], paying a running time of $2^{O(d)}$ per point. Then keep the points that lie in P. Because Prop 5.5 also proves that every *translate* of P contains few lattice points and $2^{O(d)}$ translates of P cover $\mathcal{E}$, we know that for any shift v one has $|(v+\mathcal{E}) \cap \Pi_W(\Lambda)| \leq (\log n)^{O(d)}$. Another technicality that we skipped over so far is that for an algorithmic application we need to be able to construct the subspace W guaranteed by Theorem 1.6. In particular this requires computing the canonical filtration. While no single-exponential time algorithm is known to compute the canonical filtration exactly, a $O(\log n)$-approximation can be found in time $2^{O(n)}$ due to Dadush [8]. This provides a constructive Theorem 1.6 when replacing the factor $O(\log^3 n)$ by $O(\log^4 n)$.

5.3 Covering radius of the difference body. Our final application deals with the difference body $K-K$ that we have already used in Section 5.1. While $K-K$ is larger than K we can now prove that its covering radius cannot be much smaller.

THEOREM 5.6 ([33]). *For any full rank lattice $\Lambda \subseteq \mathbb{R}^n$ and any convex body $K \subseteq \mathbb{R}^n$ one has*

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

Proof. We set $Q := K - K$. It suffices to prove the second inequality. Let W be the subspace attaining $\mu_{KL}(\Lambda, K)$. Then

$$\frac{\mu(\Lambda,K)}{\mu(\Lambda,Q)} \leq O(\log^3(n)) \cdot \frac{\mu_{KL}(\Lambda,K)}{\mu_{KL}(\Lambda,Q)} \leq O(\log^3 n) \cdot \Big(\frac{\mathrm{Vol}_d(\Pi_W(Q))}{\mathrm{Vol}_d(\Pi_W(K))}\Big)^{1/d} \leq O(\log^3 n)$$

where we use the same subspace W to lowerbound $\mu_{KL}(\Lambda, Q)$ and use again the inequality of Milman and Pajor [25] in the last step since $\Pi_W(Q)$ is the difference body of $\Pi_W(K)$. ∎

6 Open problems. We discuss a few problems that are open at the time of this writing. Let us denote $C_{KL}(n)$ as the smallest parameter so that

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

for all full rank lattices $\Lambda \subseteq \mathbb{R}^n$ and all convex bodies $K \subseteq \mathbb{R}^n$. Then from Theorem 1.6 and Lemma 1.3 we know the $\Theta(\log n) \leq C_{KL}(n) \leq \Theta(\log^3 n)$ and the obvious open problem is to narrow that range.

Next, for the Reverse Minkowski Theorem the parameter of $s = \Theta(\log n)$ might not be tight.

Conjecture 6.1 (Tight Reverse Minkowski Theorem). *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 $s = C\sqrt{\log(n)}$ one has $\rho_{1/s}(\Lambda) \leq \frac{3}{2}$.*

In the affirmative case, Conjecture 6.1 would imply that for any stable lattice $\Lambda \subseteq \mathbb{R}^n$ and any $r \geq 1$ one has $|\Lambda \cap rB_2^n| \leq n^{O(r^2)}$ which is tight already for the integer lattice $\mathbb{Z}^n$. A related question is whether the $\Theta(n \log n)$ factor from Theorem 2.2 is tight.

Conjecture 6.2 (Optimal ℓ-position). *For any symmetric convex body $K \subseteq \mathbb{R}^n$, there is an invertible linear map $T : \mathbb{R}^n \to \mathbb{R}^n$ so that $\ell_{T(K)} \cdot \ell_{(T(K))^\circ} \leq O(n\sqrt{\log(n)})$.*

The quantity of $O(n\sqrt{\log(n)})$ would be best possible. To see this, consider the cube $K := B_\infty^n$ and its polar $K^\circ = B_1^n$. Then $\ell_K \asymp \mathbb{E}_{x \sim N(\mathbf{0}, I_n)}[\|x\|_\infty] \asymp \sqrt{\log(n)}$ while $\mathbb{E}_{x \sim N(\mathbf{0}, I_n)}[\|x\|_1] \asymp n$ and the product does not decrease under rescaling. Also note that one of the tools used in Theorem 2.2 is Pisier's proof that the *K-convexity constant* for any symmetric convex body is at most $O(\log n)$ [27]. However, that inequality is tight as proven by Bourgain [7].

Inspecting the proof of the Reverse Minkowski Theorem (Theorem 3.1) one can learn that the $\log(n)$ factor is indeed solely due to an application of Theorem 2.2. In fact, Conjecture 6.2 implies Conjecture 6.1. As we are separately using Theorem 2.2 in our bound of $C_{KL}(n) \leq O(\log^3 n)$, an affirmative answer to Conj 6.2 would imply that $C_{KL}(n) \leq O(\log^2 n)$.

As we discussed in Section 3, the resolution of Bourgain's Slicing Conjecture improves the covering radius of a stable lattice w.r.t. B_2^n from $O(\sqrt{n}\log n)$ to $O(\sqrt{n})$. However, this does not immediately appear to have implications for arbitrary convex bodies. We leave it as an open question whether and to what extend Theorem 3.3.(ii) can be improved.

Question 6.3. *Is it true that for any symmetric convex body $K \subseteq \mathbb{R}^n$ and any full rank stable lattice $\Lambda \subseteq \mathbb{R}^n$ one has $\mu(\Lambda, K) \leq O(\ell_K)$?*

Finally there is also an important algorithm question concerning the complexity of integer linear programming. A conjecture popularized by Fritz Eisenbrand is the following:

Conjecture 6.4. *Given $A \in \mathbb{Q}^{m \times n}$, $b \in \mathbb{Q}^m$ and $c \in \mathbb{Q}^n$, the integer linear program $\max\{c^T x \mid Ax \leq b, x \in \mathbb{Z}^n\}$ can be solved in time $2^{O(n)}$ times a polynomial in the encoding length of A, b and c.*

Currently no plausible approach to achieve this bound is known to the author.

Acknowledgement. The author is grateful to Victor Reis for a careful reading and helpful comments on a preliminary draft. The author would also like to thank the NSF for their support of the original work [33] under NSF grant 2318620 *AF: SMALL: The Geometry of Integer Programming and Lattices*.

References

[1] I. H. and Oded Regev, *Hardness of the covering radius problem on lattices*, Chicago Journal of Theoretical Computer Science, 2012 (2012).

[2] S. Arora and B. Barak, *Computational Complexity - A Modern Approach*, Cambridge University Press, 2009.

[3] S. Artstein-Avidan, A. Giannopoulos, and V. D. Milman, *Asymptotic geometric analysis. Part I*, vol. 202 of Mathematical Surveys and Monographs, American Mathematical Society, Providence, RI, 2015, https://doi.org/10.1090/surv/202, https://doi.org/10.1090/surv/202.

[4] W. Banaszczyk, *Inequalities for convex bodies and polar reciprocal lattices in $\mathbb{R}^n$ II: application of K-convexity*, Discret. Comput. Geom., 16 (1996), pp. 305–311, https://doi.org/10.1007/BF02711514, https://doi.org/10.1007/BF02711514.

[5] W. Banaszczyk, A. E. Litvak, A. Pajor, and S. J. Szarek, *The flatness theorem for nonsymmetric convex bodies via the local theory of Banach spaces*, Math. Oper. Res., 24 (1999), pp. 728–750, https://doi.org/10.1287/moor.24.3.728, https://doi.org/10.1287/moor.24.3.728.

[6] S. G. Bobkov, *On Milman's ellipsoids and M-position of convex bodies*, in Concentration, functional inequalities and isoperimetry, vol. 545 of Contemp. Math., Amer. Math. Soc., Providence, RI, 2011, pp. 23–33, https://doi.org/10.1090/conm/545/10762, https://doi.org/10.1090/conm/545/10762.

[7] J. Bourgain, *On martingales transforms in finite dimensional lattices with an appendix on the k-convexity constant*, Mathematische Nachrichten, 119 (1984), pp. 41–53, https://doi.org/https://doi.org/10.1002/mana.19841190104, https://onlinelibrary.wiley.com/doi/abs/10.1002/mana.19841190104, https://arxiv.org/abs/https://onlinelibrary.wiley.com/doi/pdf/10.1002/mana.19841190104.

[8] D. Dadush, *On approximating the covering radius and finding dense lattice subspaces*, in STOC, ACM, 2019, pp. 1021–1026.

[9] D. Dadush, F. Eisenbrand, and T. Rothvoss, *From approximate to exact integer programming*, CoRR, abs/2211.03859 (2022).

[10] D. Dadush and O. Regev, *Towards strong reverse Minkowski-type inequalities for lattices*, in FOCS, IEEE Computer Society, 2016, pp. 447–456.

[11] D. N. Dadush, *Integer Programming, Lattice Algorithms, and Deterministic Volume Estimation*, PhD thesis, USA, 2012.

[12] T. Figiel and N. Tomczak-Jaegermann, *Projections onto Hilbertian subspaces of Banach spaces*, Israel J. Math., 33 (1979), pp. 155–171, https://doi.org/10.1007/BF02760556, https://doi.org/10.1007/BF02760556.

[13] D. R. Grayson, *Reduction theory using semistability*, Comment. Math. Helv., 59 (1984), pp. 600–634, https://doi.org/10.1007/BF02566369, https://doi.org/10.1007/BF02566369.

[14] G. Harder and M. S. Narasimhan, *On the cohomology groups of moduli spaces of vector bundles on curves*, Mathematische Annalen, 212 (1975), pp. 215–248, https://doi.org/10.1007/BF01357141, https://doi.org/10.1007/BF01357141.

[15] R. Kannan, *Minkowski's convex body theorem and integer programming*, Math. Oper. Res., 12 (1987), pp. 415–440, https://doi.org/10.1287/moor.12.3.415, http://dx.doi.org/10.1287/moor.12.3.415.

[16] R. Kannan and L. Lovász, *Covering minima and lattice-point-free convex bodies*, Annals of Mathematics, 128 (1988), pp. 577–602, http://www.jstor.org/stable/1971436 (accessed 2022-07-08).

[17] A. Y. Khinchin, *A quantitative formulation of the approximation theory of kronecker*, Izvestiya Rossiiskoi Akademii Nauk. Seriya Matematicheskaya, 12 (1948), pp. 113–122.

[18] B. Klartag and J. Lehec, *Affirmative resolution of bourgain's slicing problem using guan's bound*, 2024, https://arxiv.org/abs/2412.15044, https://arxiv.org/abs/2412.15044.

[19] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann., 261 (1982), pp. 515–534, https://doi.org/10.1007/BF01457454, https://doi.org/10.1007/BF01457454.

[20] J. Lenstra, H. W., *Integer programming with a fixed number of variables*, Mathematics of Operations Research, 8 (1983), pp. pp. 538–548, http://www.jstor.org/stable/3689168.

[21] D. R. Lewis, *Ellipsoids defined by Banach ideal norms*, Mathematika, 26 (1979), pp. 18–29, https://doi.org/10.1112/S0025579300009566, https://doi.org/10.1112/S0025579300009566.

[22] J. Matousek, *Lectures on Discrete Geometry*, Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2002.

[23] L. Mayrhofer, J. Schade, and S. Weltge, *Lattice-free simplices with lattice width 2d - o(d)*, in IPCO, vol. 13265 of Lecture Notes in Computer Science, Springer, 2022, pp. 375–386.

[24] D. Micciancio and P. Voulgaris, *A deterministic single exponential time algorithm for most lattice problems based on Voronoi cell computations*, SIAM J. Comput., 42 (2013), pp. 1364–1391, https://doi.org/10.1137/100811970, http://dx.doi.org/10.1137/100811970.

[25] V. Milman and A. Pajor, *Entropy and asymptotic geometry of non-symmetric convex bodies*, Advances in Mathematics, 152 (2000), pp. 314–335, https://doi.org/https://doi.org/10.1006/aima.1999.1903, https://www.sciencedirect.com/science/article/pii/S0001870899919035.

[26] A. M. Odlyzko, *The rise and fall of knapsack cryptosystems*, Cryptology and Computational Number Theory, (1990), pp. 75–88, http://www.dtc.umn.edu/~odlyzko/doc/arch/knapsack.survey.pdf.

[27] G. Pisier, *Sur les espaces de Banach K-convexes*, in Seminar on Functional Analysis, 1979–1980 (French), École Polytech., Palaiseau, 1980, pp. Exp. No. 11, 15.

[28] G. Pisier, *Holomorphic semigroups and the geometry of Banach spaces*, Ann. of Math. (2), 115 (1982), pp. 375–392, https://doi.org/10.2307/1971396, https://doi.org/10.2307/1971396.

[29] O. Regev, *Lecture notes on lattices*, 2009, http://www.cims.nyu.edu/~regev/teaching/lattices_fall_2009.

[30] O. Regev, *On lattices, learning with errors, random linear codes, and cryptography*, J. ACM, 56 (2009), pp. 34:1–34:40.

[31] O. Regev and N. Stephens-Davidowitz, *A reverse Minkowski theorem*, in STOC, ACM, 2017, pp. 941–953.

[32] O. Regev and N. Stephens-Davidowitz, *A reverse Minkowski theorem*, Ann. of Math. (2), 199 (2024), pp. 1–49, https://doi.org/10.4007/annals.2024.199.1.1, https://doi.org/10.4007/annals.2024.199.1.1.

[33] V. Reis and T. Rothvoss, *The subspace flatness conjecture and faster integer programming*, in FOCS, IEEE, 2023, pp. 974–988.

[34] C. A. Rogers and G. C. Shephard, *The difference body of a convex body*, Archiv der Mathematik, 8 (1957), pp. 220–233.

[35] M. Rudelson, *Distances between non-symmetric convex bodies and the MM*-estimate*, Positivity, 4 (1998), pp. 161–178.

[36] N. Stephens-Davidowitz, *On the Gaussian Measure Over Lattices*, PhD thesis, 2017, https://cs.nyu.edu/media/publications/stephens-davidowitz_noah.pdf.

[37] U. Stuhler, *Eine Bemerkung zur Reduktionstheorie quadratischer Formen*, Arch. Math. (Basel), 27 (1976), pp. 604–610, https://doi.org/10.1007/BF01224726, https://doi.org/10.1007/BF01224726.

[38] B.-H. Vritsiou, *Regular ellipsoids and a Blaschke-Santaló-type inequality for projections of non-symmetric convex bodies*, 2023, https://arxiv.org/abs/2303.17753.