

A Reverse Minkowski Theorem

Oded Regev^{*†}

Noah Stephens-Davidowitz^{‡§}
noahsd@gmail.com

Abstract

We prove a conjecture due to Dadush, showing that if $\mathcal{L} \subset \mathbb{R}^n$ is a lattice such that $\det(\mathcal{L}') \geq 1$ for all sublattices $\mathcal{L}' \subseteq \mathcal{L}$, then

$$\sum_{\mathbf{y} \in \mathcal{L}} e^{-\pi t^2 \|\mathbf{y}\|^2} \leq 3/2,$$

where $t := 10(\log n + 2)$. From this we derive bounds on the number of short lattice vectors, which can be viewed as a partial converse to Minkowski's celebrated first theorem. We also derive a bound on the covering radius.

1 Introduction

A lattice $\mathcal{L} \subset \mathbb{R}^n$ is the set of integer linear combinations of linearly independent basis vectors $\mathbf{B} = (\mathbf{b}_1, \dots, \mathbf{b}_n)$. The determinant of the lattice, $\det(\mathcal{L}) = |\det(\mathbf{B})|$, is a measure of its global density in the sense that

$$\det(\mathcal{L}) = \lim_{r \rightarrow \infty} \frac{\text{vol}(rB_2^n)}{|\mathcal{L} \cap rB_2^n|},$$

where rB_2^n denotes the closed Euclidean ball of radius $r > 0$, whose volume is $(\pi n)^{-1/2} (2\pi e r^2/n)^{n/2} (1 + o(1))$. (Here and elsewhere, we write $o(1)$ for an arbitrary function that approaches zero as the dimension n approaches infinity.)

Minkowski's celebrated first theorem shows that a lattice with small determinant must have short non-zero vectors [Min10]. This is one of the foundational results in the study of lattices and the geometry of numbers, and it has innumerable applications. We consider the following point-counting form of this theorem due to Blichfeldt and van der Corput,¹ which says that a lattice with small determinant must have *many* short points, or informally, that “global density implies local density.”

^{*}Courant Institute of Mathematical Sciences, New York University.

[†]Supported by the Simons Collaboration on Algorithms and Geometry and by the National Science Foundation (NSF) under Grant No. CCF-1320188. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the NSF.

[‡]Cornell University.

[§]Much of this work was done while at New York University, supported by the National Science Foundation (NSF) under Grant No. CCF-1320188. Part of this work was done while visiting Chris Peikert at the University of Michigan.

¹They actually showed the slightly stronger bound $|\mathcal{L} \cap rB_2^n| \geq 2 \lfloor 2^{-n} \cdot \text{vol}(rB_2^n) \rfloor + 1$ and considered arbitrary norms, not just ℓ_2 . (See, e.g., [GL87, Thm. 1 of Ch. 2, Sec. 7].)

Theorem 1.1 ([vdC36]). *For any lattice $\mathcal{L} \subset \mathbb{R}^n$ with $\det(\mathcal{L}) \leq 1$ and $r > 0$,*

$$|\mathcal{L} \cap rB_2^n| \geq 2^{-n} \cdot \text{vol}(rB_2^n) = \frac{1}{\sqrt{\pi n}} \left(\frac{\pi e r^2}{2n} \right)^{n/2} (1 + o(1)) .$$

It is quite natural to ask whether a converse of Theorem 1.1 holds. In particular, if a lattice has sufficiently many short points, does it necessarily have small determinant? Does local density imply global density?

It is easy to see that the answer is actually no. Consider, for example, the lattice generated by the vectors $(1/t, 0)$ and $(0, t^2)$ for some arbitrarily large t . This lattice has at least $2\lfloor tr \rfloor + 1$ points of norm at most r , but it has arbitrarily large determinant t . Notice, however, that this lattice contains a *sublattice* generated by $(1/t, 0)$ that does have small determinant. This leads us to a more refined question:

If a lattice has sufficiently many short points, does it necessarily have a small-determinant *sublattice*? Does local density imply global density restricted to a subspace?

Equivalently, in the contrapositive, the question asks for an upper bound on the number of lattice points in a ball given that there is no sublattice of small determinant.

Dadush conjectured a suitably precise answer to these questions [Dad12a]. He later studied this conjecture in depth in joint work with the first named author [DR16]. Among other things, they showed a number of applications of the conjecture (from computational complexity of lattice problems to Brownian motion on flat tori) and gave some evidence for it. We refer the reader to [DR16] for a full list of their results.

Our main result is a proof of the conjecture of Dadush, which in particular implies the applications mentioned above.

Theorem 1.2 (Reverse Minkowski Theorem). *For any lattice $\mathcal{L} \subset \mathbb{R}^n$ with $\det(\mathcal{L}') \geq 1$ for all sublattices $\mathcal{L}' \subseteq \mathcal{L}$,*

$$\rho_{1/t}(\mathcal{L}) \leq \frac{3}{2} ,$$

where $t := 10(\log n + 2)$.

Here, for a lattice $\mathcal{L} \subset \mathbb{R}^n$ and $s > 0$,

$$\rho_s(\mathcal{L}) := \sum_{\mathbf{y} \in \mathcal{L}} e^{-\pi \|\mathbf{y}\|^2 / s^2}$$

is the *Gaussian mass* of the lattice with *parameter* s . This can be seen as a smooth version of the point-counting function $r \mapsto |\mathcal{L} \cap rB_2^n|$, with the parameter s playing the role of the radius r , and it arises naturally in a number of contexts (often in the form of the theta function, $\Theta_{\mathcal{L}}(iy) := \rho_{1/\sqrt{y}}(\mathcal{L})$). In particular, Theorem 1.2 immediately implies that $|\mathcal{L} \cap rB_2^n| \leq 3e^{\pi t^2 r^2} / 2$ for any radius $r > 0$. (We note that the constant $3/2$ in this bound and the theorem statement is chosen for convenience, and a similar statement holds with any constant strictly bigger than 1.)

One can view Theorem 1.2 as relating the parameters

$$\eta^*(\mathcal{L}) := \inf\{t : \rho_{1/t}(\mathcal{L}) \leq 3/2\}$$

(known as the smoothing parameter of the dual lattice [MR07]) and

$$\eta_{\det}(\mathcal{L}) := \max_{\mathcal{L}' \subseteq \mathcal{L}} \det(\mathcal{L}')^{-1/\text{rank}(\mathcal{L}')} .$$

Specifically, we claim that

$$\frac{2}{3} \cdot \eta_{\det}(\mathcal{L}) \leq \eta^*(\mathcal{L}) \leq 10(\log n + 2) \cdot \eta_{\det}(\mathcal{L}) . \quad (1)$$

Indeed, the first inequality is an immediate consequence of the Poisson Summation Formula, Eq. (5) (see Eq. (6)). When $\eta_{\det}(\mathcal{L}) = 1$, the second inequality is precisely Theorem 1.2; the general case follows by noting that both $\eta_{\det}(\mathcal{L})$ and $\eta^*(\mathcal{L})$ behave identically under scaling of \mathcal{L} (homogeneous of degree -1). Eq. (1) is not far from tight, as can be seen by noting that $\eta^*(\mathbb{Z}^n) = \sqrt{\log n/\pi} + o(1)$ and $\eta_{\det}(\mathbb{Z}^n) = 1$.

In Section 5, we extend Theorem 1.2 to obtain a bound on the Gaussian mass for all parameters, as follows.

Theorem 1.3. *Let $t := 10(\log n + 2)$. Then, for any lattice $\mathcal{L} \subset \mathbb{R}^n$ with $\det(\mathcal{L}') \geq 1$ for all sublattices $\mathcal{L}' \subseteq \mathcal{L}$,*

1. $\rho_s(\mathcal{L}) \leq 1 + e^{-\pi(1/s^2 - t^2)}/2$ for any $s \leq 1/t$;
2. $\rho_s(\mathcal{L}) \leq (Cst)^{n/2}$ for any $1/t < s < t$ and some universal constant $C > 1$; and
3. $\rho_s(\mathcal{L}) \leq 2s^n$ for any $s \geq t$.

Theorem 1.3 implies the following point-counting bounds. (See Section 5 for the proof.)

Corollary 1.4. *Let $t := 10(\log n + 2)$. Then, for any lattice $\mathcal{L} \subset \mathbb{R}^n$ with $\det(\mathcal{L}') \geq 1$ for all sublattices $\mathcal{L}' \subseteq \mathcal{L}$, and every shift vector $\mathbf{u} \in \mathbb{R}^n$,*

1. for any $r \geq 1$, $|\mathcal{L} \cap (rB_2^n + \mathbf{u})| \leq 3e^{\pi t^2 r^2}/2$;
2. for any $\sqrt{n/(2\pi)} \cdot t^{-1} \leq r \leq \sqrt{n/(2\pi)} \cdot t$, $|\mathcal{L} \cap (rB_2^n + \mathbf{u})| \leq (Ctr/\sqrt{n})^{n/2}$ for some universal constant $C > 0$; and
3. for any $r \geq \sqrt{n/(2\pi)} \cdot t$, $|\mathcal{L} \cap (rB_2^n + \mathbf{u})| \leq 2(2\pi e r^2/n)^{n/2}$.

In Section 8, we discuss the tightness of Theorem 1.3 and Corollary 1.4.

1.1 Approximation to the covering radius

The *covering radius* $\mu(\mathcal{L})$ of a lattice $\mathcal{L} \subset \mathbb{R}^n$ is the maximal distance from any point in \mathbb{R}^n to the lattice, or equivalently, the minimum radius r such that $\mathcal{L} + rB_2^n = \mathbb{R}^n$. It follows from the definition that $\mu(\mathcal{L})$ must be at least the radius of a ball of volume $\det(\mathcal{L})$, which is at least $\sqrt{n/(2\pi e)} \det(\mathcal{L})^{1/n}$. By considering projections, Kannan and Lovász [KL88] improved this lower bound, as follows. Let $\pi_{W^\perp}(\mathcal{L})$ be the projection of the lattice onto the space W^\perp orthogonal to some *lattice subspace* $W \subset \mathbb{R}^n$ —a subspace spanned by $k < n$ linearly independent lattice vectors.² Then clearly $\mu(\mathcal{L}) \geq \mu(\pi_{W^\perp}(\mathcal{L}))$, and the latter is at least $(\dim(W^\perp)/(2\pi e))^{1/2} \cdot \det(\pi_{W^\perp}(\mathcal{L}))^{1/\dim(W^\perp)}$. So, we obtain the lower bound

$$\mu(\mathcal{L}) \geq \frac{1}{\sqrt{2\pi e}} \cdot \mu_{\det}(\mathcal{L}) ,$$

²The projection $\pi_{W^\perp}(\mathcal{L})$ is a lattice if and only if W is a lattice subspace.

where

$$\mu_{\det}(\mathcal{L}) := \max_{W \subset \mathbb{R}^n} \sqrt{\dim(W^\perp)} \cdot \det(\pi_{W^\perp}(\mathcal{L}))^{\frac{1}{\dim(W^\perp)}},$$

with the maximum taken over lattice subspaces $W \subset \mathbb{R}^n$. To make the analogy to η_{\det} more apparent, we apply duality and write

$$\mu_{\det}(\mathcal{L}) = \max_{W \subset \mathbb{R}^n} \sqrt{\dim(W^\perp)} \cdot \det(\pi_{W^\perp}(\mathcal{L})^*)^{-\frac{1}{\dim(W^\perp)}} = \max_{\mathcal{M} \subseteq \mathcal{L}^*} \sqrt{\text{rank}(\mathcal{M})} \cdot \det(\mathcal{M})^{-\frac{1}{\text{rank}(\mathcal{M})}},$$

where \mathcal{L}^* denotes the dual of a lattice \mathcal{L} , the first equality uses the fact that the determinant of the dual lattice is the reciprocal of the determinant of the lattice, and the second equality uses the fact that $\pi_{W^\perp}(\mathcal{L})^* = W^\perp \cap \mathcal{L}^*$. Kannan and Lovász also observed the upper bound

$$\mu(\mathcal{L}) \leq C\sqrt{n} \cdot \mu_{\det}(\mathcal{L})$$

(see [DR16, Theorem 11.1] for a proof), and asked whether a better upper bound could be found.³ In Section 6, we use Theorem 1.2 to derive the following improved bound.

Theorem 1.5 (Covering-radius approximation). *For any lattice $\mathcal{L} \subset \mathbb{R}^n$,*

$$\frac{1}{\sqrt{2\pi e}} \cdot \mu_{\det}(\mathcal{L}) \leq \mu(\mathcal{L}) \leq 10(\log n + 10)^{3/2} \cdot \mu_{\det}(\mathcal{L}). \quad (2)$$

We emphasize that Dadush and Regev [DR16] already proved that Theorem 1.5 (with slightly weaker parameters) would follow from a proof of Theorem 1.2. Although our proof is shorter and achieves slightly better parameters, it is conceptually similar to the one in [DR16].

We note that the specific polylogarithmic factor that we obtain is likely not optimal. In fact, in Theorem 6.8 we prove a bound similar to that in Eq. (2) that replaces the factor $10(\log n + 10)^{3/2}$ by $C\sqrt{\log n}$, assuming the celebrated Slicing Conjecture [Bou91, Kla06, Che21, KL22]. However, it is not difficult to show that this factor cannot be smaller than $\sqrt{\log n}/(4e) + o(1)$.⁴

Covering radius of stable lattices and Minkowski's Conjecture. We say that a lattice $\mathcal{L} \subset \mathbb{R}^n$ is *stable* if $\det(\mathcal{L}) = 1$ and $\det(\mathcal{L}') \geq 1$ for all sublattices $\mathcal{L}' \subseteq \mathcal{L}$. Stable lattices arise in a number of contexts [HN75, Stu76, Gra84] and they play an important role in the sequel. Shapira and Weiss showed that a tight bound of $\mu(\mathcal{L}) \leq \mu(\mathbb{Z}^n) = \sqrt{n}/2$ on the covering radius of stable lattices would imply a well-known conjecture attributed to Minkowski [SW16]. Specifically, the conjecture asserts that for every lattice $\mathcal{L} \subset \mathbb{R}^n$ with $\det(\mathcal{L}) = 1$ and vector $\mathbf{t} = (t_1, \dots, t_n) \in \mathbb{R}^n$,

$$\inf_{\mathbf{y} \in \mathcal{L}} \prod_i |y_i - t_i| \leq 2^{-n}. \quad (3)$$

³They also proved similar bounds for arbitrary norms [KL88, Corollary 3.11].

⁴Consider the lattice \mathcal{L} generated by $(\mathbf{e}_1, \mathbf{e}_2/2, 2\mathbf{e}_3/3^{3/2}, \dots, (n-1)^{(n-1)/2}\mathbf{e}_n/n^{n/2})$. It is not difficult to verify that $\mu_{\det}(\mathcal{L}) = 1$, but

$$\mu(\mathcal{L})^2 = 1/4 + \sum_{k=2}^n \frac{(k-1)^{k-1}}{4k^k} = 1/4 + \sum_{k=2}^n \frac{(1-1/k)^k}{4(k-1)} = \sum_{k=2}^n \frac{1}{4e(k-1)} + O(1) = \frac{\log n}{4e} + O(1).$$

Therefore, $\mu(\mathcal{L}) = \sqrt{\log n/(4e)} + o(1)$.

(See [SW16] and [Sol19].)

We do not manage to prove a bound tight enough to imply Eq. (3), but en route to proving Theorem 1.5 we do show that $\mu(\mathcal{L}) \leq 4\sqrt{n}(\log n + 10)$ for all stable lattices. (See Theorem 6.2.) We also observe that a very strong resolution to the Slicing Conjecture would yield the desired tight bound, when combined with a recent result due to Magazinov [Mag18]. (See Theorem 6.7 and the discussion afterwards.)

1.2 An optimal bound on the Gaussian mass for “extreme” parameters

It is tempting to ask whether $\rho_s(\mathcal{L}) \leq \rho_s(\mathbb{Z}^n)$ for any lattice $\mathcal{L} \subset \mathbb{R}^n$ such that $\det(\mathcal{L}') \geq 1$ for all sublattices $\mathcal{L}' \subseteq \mathcal{L}$ and any parameter $s > 0$. (See Section 1.5.) The next theorem shows that indeed $\rho_s(\mathcal{L}) \leq \rho_s(\mathbb{Z}^n)$ for such lattices, but only for “extremely low” or “extremely high” parameters s . (See Section 7 for the proof.)

Theorem 1.6. *For any lattice $\mathcal{L} \subset \mathbb{R}^n$ such that $\det(\mathcal{L}') \geq 1$ for all sublattices $\mathcal{L}' \subseteq \mathcal{L}$ and parameter $s > 0$ such that either $s \leq \sqrt{2\pi/(n+2)}$ or $s \geq \sqrt{(n+2)/(2\pi)}$, we have $\rho_s(\mathcal{L}) \leq \rho_s(\mathbb{Z}^n)$.*

We hope that the proof of Theorem 1.6 might provide some hints as to how to extend it to all parameters s .

1.3 Proof overview

In this section, we give a high-level overview of the proof of Theorem 1.2.

Bounding the mass of stable lattices. Recall that a lattice \mathcal{L} is *stable* if $\det(\mathcal{L}) = 1$ and $\det(\mathcal{L}') \geq 1$ for all sublattices $\mathcal{L}' \subseteq \mathcal{L}$. I.e., stable lattices are determinant-one lattices that satisfy the assumption in Theorem 1.2. In this proof overview, we focus on bounding the Gaussian mass $\rho_s(\mathcal{L})$ of stable lattices \mathcal{L} . As it turns out, the general case then follows easily.

Crucially, the stable lattices form a compact subset of the set of determinant-one lattices, so that the continuous function $\rho_s(\mathcal{L})$ must attain a global maximum over the set of stable lattices. We may therefore restrict our attention to a lattice that corresponds to this global maximum. If this lattice is on the *boundary* of the set of stable lattices, then it has a strict sublattice \mathcal{L}' with determinant one. We can then “split the lattice” at \mathcal{L}' . Namely, we can replace the original lattice \mathcal{L} by the direct sum $\mathcal{L}' \oplus \mathcal{L}/\mathcal{L}'$, where both \mathcal{L}' and \mathcal{L}/\mathcal{L}' are stable. By using the fact that the Gaussian has a positive Fourier transform, it is not difficult to prove that

$$\rho_s(\mathcal{L}) \leq \rho_s(\mathcal{L}' \oplus \mathcal{L}/\mathcal{L}') = \rho_s(\mathcal{L}')\rho_s(\mathcal{L}/\mathcal{L}') .$$

(See Lemma 2.3.) So, we have reduced the question to a lower-dimensional one. Therefore, if we could show that for any dimension, the global maximizer is on the boundary, then we could use induction to show that the global maximizer of the Gaussian mass is simply the integer lattice $\mathbb{Z}^n = \mathbb{Z} \oplus \dots \oplus \mathbb{Z}$.

Indeed, this is how we prove Theorem 1.6 (in Section 7), which shows that \mathbb{Z}^n has maximal Gaussian mass for certain “extreme” parameters s . For such parameters, by taking the second derivative, we show that a stable lattice cannot be a local maximum over the set of determinant-one lattices. Therefore, the global maximizer of $\rho_s(\mathcal{L})$ over the compact subset of stable lattices must be on the boundary, and we can perform the “splitting” procedure described above to show by induction that $\rho_s(\mathcal{L}) \leq \rho_s(\mathbb{Z}^n)$.

However, it was recently shown by Heimendahl et al. that stable local maxima do exist for some parameters s [HMT⁺22].⁵ As a potential way around this issue, we could use a natural and very elegant idea due to Shapira and Weiss [SW16]—we could try to directly bound the value of $\rho_s(\mathcal{L})$ at any local maximum. Then, either the global maximum of $\rho_s(\mathcal{L})$ over the set of stable lattices is one of these local maxima, in which case we can apply this bound; or it is on the boundary, in which case we can “split the lattice” as above. (Shapira and Weiss suggested using this approach to bound the *covering radius* of stable lattices, which is also known to have local maxima [DSV12]; they showed that a tight bound would resolve Minkowski’s Conjecture [SW16].)

Enter the Voronoi cell. Unfortunately, directly bounding the value of $\rho_s(\mathcal{L})$ at local maxima seems to be beyond our grasp. So, instead of working with $\rho_s(\mathcal{L})$ directly, we work with a proxy for it: the Gaussian mass of the Voronoi cell of the lattice

$$\gamma_s(\mathcal{V}(\mathcal{L})) := \int_{\mathcal{V}(\mathcal{L})/s} e^{-\pi\|\mathbf{x}\|^2} d\mathbf{x} ,$$

where the Voronoi cell is the set of all points that are at least as close to the origin as to any other lattice point,

$$\mathcal{V}(\mathcal{L}) := \{\mathbf{x} \in \mathbb{R}^n : \forall \mathbf{y} \in \mathcal{L}, \|\mathbf{x}\| \leq \|\mathbf{y} - \mathbf{x}\|\} .$$

An elegant proof due to Chung, Dadush, Liu, and Peikert [CDLP13] shows that $\rho_s(\mathcal{L})$ is at most $1/\gamma_s(\mathcal{V}(\mathcal{L}))$. (See Lemma 4.1.) So, in order to prove an upper bound on $\rho_s(\mathcal{L})$, it suffices to prove a lower bound on $\gamma_s(\mathcal{V}(\mathcal{L}))$.

We accomplish this via the approach described above. Namely, we reduce the problem to bounding the value of $\gamma_s(\mathcal{V}(\mathcal{L}))$ at local minima \mathcal{L} . (We do not know whether these local minima exist.) For such an \mathcal{L} , we consider two functions, both defined over the set of all determinant-one matrices $A \in \text{SL}_n(\mathbb{R})$: $g(A) = \gamma_s(\mathcal{V}(A\mathcal{L}))$ and $h(A) = \gamma_s(A\mathcal{V}(\mathcal{L}))$. Notice that the value we wish to bound is $g(I_n) = h(I_n)$. Moreover, as we show (in Section 3), the two functions have the same gradient at $A = I_n$ and therefore the fact that g has a local minimum at $A = I_n$ implies that h has a critical point there. Using a result due to Bobkov [Bob11], which itself follows from a deep theorem due to Cordero-Erausquin, Fradelizi, and Maurey [CFM04],⁶ we can show that any such critical point of h must actually be a global *maximum*. I.e., in the language of convex geometry, the Voronoi cell is in a position that maximizes the Gaussian mass. (Note the rather surprising jump from a presumed local minimum over the set of determinant-one lattices to a global *maximum* over the set of positions of the Voronoi cell.) Finally, we complete the proof by applying the celebrated $\ell\ell^*$ theorem [FT79, Lew79, Pis82], which implies that for $s = 1/t$, the global maximum of h is at least $2/3$, where $t := 10(\log n + 2)$ as in Theorem 1.2.

1.4 Related work

Our main theorem was originally conjectured by Dadush [Dad12a]. Dadush together with the first named author described several applications of the conjecture [DR16]. In particular, they showed the connection between this conjecture and the Kannan-Lovász-style covering-radius approximation

⁵This was originally posed as an open question in an earlier version of this paper.

⁶We note in passing that one can prove Theorem 1.2 (at least up to constants) without using this rather heavy hammer by considering local maxima of the ℓ -norm of the Voronoi cell instead of local minima of the Gaussian mass of the Voronoi cell.

given in Theorem 1.5. They also used a result from convex geometry (specifically the Milman-Pisier Theorem [MP87]) as evidence for the conjecture. That theorem is related to the $\ell\ell^*$ theorem that we use in our proof.

The high-level outline of our proof (in which we obtain a bound on a lattice parameter by reducing the question to stable local extrema) is due to Shapira and Weiss [SW16]. They showed that an important conjecture attributed to Minkowski would follow if we could prove that \mathbb{Z}^n has maximal covering radius amongst all stable lattices (i.e., that the covering radius of an n -dimensional stable lattice is at most $\sqrt{n}/2$). They then observed that it would suffice to bound the covering radius of the lattices corresponding to local maxima of the covering radius function over the set of determinant-one lattices.

Stable lattices were introduced (in a more general context) by Harder and Narasimhan [HN75] and by Stuhler [Stu76]. Our presentation more-or-less follows that of Grayson [Gra84].

Counting the number of lattice points in a ball is a classical question, and a summary of all that is known is far beyond the scope of this paper. (See, e.g., [CS98].) In particular, much research has gone into studying the relationship between the number of points in a ball of radius r and the determinant of the densest *one-dimensional* sublattice, written $\lambda_1(\mathcal{L})$. (I.e., $\lambda_1(\mathcal{L})$ is the length of the shortest non-zero vector in the lattice.) It is easy to see that the number of lattice points in a ball of radius $r \geq \lambda_1(\mathcal{L})$ is at most $(Cr/\lambda_1(\mathcal{L}))^n$, which is essentially the best possible bound based on $\lambda_1(\mathcal{L})$.⁷ We consider the densest sublattice of any dimension (not just the densest one-dimensional sublattice) to obtain bounds that are much stronger in many cases. (Other authors have considered other generalizations of $\lambda_1(\mathcal{L})$ to derive incomparable bounds. E.g., [Hen02].)

Many authors have considered the extrema of various lattice parameters over the set of determinant-one lattices. Voronoi famously characterized the local maxima of the length of the shortest non-zero vector [Vor08], and a long line of work has gone into finding the specific global maxima in various dimensions. (See, e.g., [CS98, CK09].) Similarly, Montgomery [Mon88] and Sarnak and Strömbergsson [SS06] considered the minima of the Gaussian mass $\rho_s(\mathcal{L})$ and closely related functions.

Informally, the results mentioned above (and almost all literature on this topic since Minkowski) were concerned with the “best” lattices. E.g., they primarily considered lattices with the largest minimum distance, the smallest covering radius, the minimal Gaussian mass, etc. We are in some sense interested in the “worst” lattices. Thus, we consider *maxima* of the Gaussian mass, maxima of the covering radius (as in [DSV12]), etc. (These questions only make sense over a bounded subset of the determinant-one lattices, such as the stable lattices.) Note that, while the “best” lattices tend to have fascinating properties (see, e.g., [CS98]), in our setting the “worst” lattice that we know of is \mathbb{Z}^n .

We also note two follow-up works. First, Lovett and the first named author used Theorem 1.2 to give a counterexample to a very strong variant of the polynomial Freiman-Ruzsa conjecture over the integers [LR17]. This variant was introduced by Green (who suggested that it was likely to be false) [Gre07]. Second, Dadush showed a number of applications of Theorems 1.2 and 1.5, including an algorithm for finding dense lattice subspaces and a remarkably tight approximation to the covering radius in terms of the so-called canonical filtration [Dad19] (as defined in Section 2.4).

The reader might also be interested in the lecture notes of Bost providing a broader perspective

⁷Finding the exact best possible bounds on $|\mathcal{L} \cap s\lambda_1(\mathcal{L})B_2^n|$ in various regimes is a fascinating classical problem that is still an active area of research. For example, when $s = 1$, this is known as the lattice “kissing number” problem, and the limit as $s \rightarrow \infty$ is the lattice sphere-packing problem. See, e.g., [KL78, CS98, CK09].

on the results of this paper [Bos20].

1.5 Directions for future work

The most obvious direction for future work is to try to obtain a better value for t in Theorem 1.2. As far as we know, the correct value could be as small as $t = \eta^*(\mathbb{Z}^n) = \sqrt{\log(n)/\pi} + o(1)$. Our proof seems to be loose in two places: (1) Theorem 4.6, which bounds the maximal Gaussian mass of convex bodies; and (2) the induction argument in the proof of Proposition 4.14. It seems that one would need to improve both parts of the proof to obtain a significantly better bound.

A more ambitious goal would be to prove that

$$\rho_s(\mathcal{L}) \leq \rho_s(\mathbb{Z}^n) \quad (4)$$

for all $s > 0$ and all lattices $\mathcal{L} \subset \mathbb{R}^n$ such that $\det(\mathcal{L}') \geq 1$ for all sublattices $\mathcal{L}' \subseteq \mathcal{L}$. To that end, Eisenberg and the authors recently proved that this is true in an average sense over s , which can be stated as an inequality relating Epstein zeta functions as follows:

$$\sum_{\mathbf{y} \in \mathcal{L} \setminus \{\mathbf{0}\}} \|\mathbf{y}\|^{-2\sigma} \leq \sum_{\mathbf{z} \in \mathbb{Z}^n \setminus \{\mathbf{0}\}} \|\mathbf{z}\|^{-2\sigma}$$

for all such lattices $\mathcal{L} \subset \mathbb{R}^n$ and all $\sigma > n/2$ [ERS22]. They prove this by showing that the Epstein zeta function has no local maxima over the set of determinant-one lattices (and over certain subsets of this set). One might think to try to prove something similar for $\rho_s(\mathcal{L})$. However, local maxima are known to exist for some parameters s [HMT⁺22]. As an alternative, one can try using the technique of “characterizing the local extrema” that we use to prove Theorem 1.2. For this, we note that any local maximum of $\rho_s(\mathcal{L})$ must correspond to an “isotropic” lattice \mathcal{L} in the sense that

$$\sum_{\mathbf{y} \in \mathcal{L}} \mathbf{y} \mathbf{y}^T e^{-\pi \|\mathbf{y}\|^2 / s^2} = \alpha \cdot I_n$$

for some scalar $\alpha > 0$. So, it would suffice to show Eq. (4) for (stable) “isotropic” lattices. Unfortunately, we do not know how to make use of this.

Recall from Eq. (1) that Theorem 1.2 gives quite a tight approximation to the smoothing parameter $\eta^*(\mathcal{L})$. However, an analogous tightness result does not hold for Theorem 1.3 and Corollary 1.4. Dadush and Regev therefore suggested a potential refinement that depends on “the full spectrum of dense sublattices,” $\min_{\mathcal{L}' \subseteq \mathcal{L}, \text{rank}(\mathcal{L}')=k} \det(\mathcal{L}')^{1/k}$ for $k = 1, \dots, n$, rather than just $\min_{\mathcal{L}' \subseteq \mathcal{L}} \det(\mathcal{L}')^{1/\text{rank}(\mathcal{L}')} [DR16, \text{Section 9}]$. This could potentially give a tight characterization of $|\mathcal{L} \cap rB_2^n|$ for all radii r and all lattices $\mathcal{L} \subset \mathbb{R}^n$.

One can also consider generalizations of Theorems 1.5 and 1.2 to arbitrary norms, as discussed in [KL88] and [DR16, Section 9] respectively. Extending Theorem 1.5 to arbitrary norms could potentially yield faster algorithms for Integer Programming [Dad12b]. Unfortunately, a natural generalization of Theorem 1.2 actually fails. (See [DR16, Section 9].)

Acknowledgments

We are extremely grateful to Daniel Dadush for sharing his conjecture with us and for many helpful discussions. We are also indebted to Barak Weiss for introducing us to stable lattices and their salient properties and for telling us about the technique of “handling the stable local maxima

separately” from his paper with Uri Shapira [SW16]. We also thank him for his help with the proof of Proposition 6.4. We thank Bo’az Klartag for referring us to [Bob11] and for other useful comments. We thank Ronen Eldan for showing us how to greatly simplify the proof of Theorem 3.1. The first named author thanks Prof. Volker Kempe for his help with the two rascals.

2 Preliminaries

We use c, C, C' to denote arbitrary positive universal constants, whose value might change from one occurrence to the next. Logarithms are base e unless otherwise specified. Vectors $\mathbf{x} \in \mathbb{R}^n$ are column vectors. We write $\|\mathbf{x}\|$ to represent the Euclidean norm of \mathbf{x} , and we write I_n for the identity matrix in n dimensions. For a matrix $A \in \mathbb{R}^{n \times n}$, we write A^T for the transpose of A . We write $B_2^n := \{\mathbf{x} \in \mathbb{R}^n : \|\mathbf{x}\| \leq 1\}$ for the Euclidean ball in \mathbb{R}^n . We write $\pi_S(\mathbf{x})$ for the orthogonal projection of \mathbf{x} onto $\text{span}(S)$ for some $S \subseteq \mathbb{R}^n$. (E.g., $\pi_{\{\mathbf{y}\}}(\mathbf{x}) = \langle \mathbf{y}, \mathbf{x} \rangle \mathbf{y} / \|\mathbf{y}\|^2$.) For two additive subgroups $S_1 \subseteq \mathbb{R}^n$ and $S_2 \subseteq \mathbb{R}^m$, their direct sum $S_1 \oplus S_2 \subseteq \mathbb{R}^{n+m}$ is $\{(\mathbf{x}, \mathbf{y}) : \mathbf{x} \in S_1, \mathbf{y} \in S_2\}$.

A *convex body* $K \subset \mathbb{R}^n$ is a convex compact subset of \mathbb{R}^n with non-empty interior. It is *symmetric* if $-K = K$. A *position* of a convex body is simply AK for a determinant-one matrix A .

2.1 Lattices

A *lattice* $\mathcal{L} \subset \mathbb{R}^n$ of rank d is the set of integer linear combinations of linearly independent basis vectors $\mathbf{B} := (\mathbf{b}_1, \dots, \mathbf{b}_d)$,

$$\mathcal{L} = \mathcal{L}(\mathbf{B}) := \left\{ \sum_{i=1}^d a_i \mathbf{b}_i : a_i \in \mathbb{Z} \right\}.$$

We typically treat lattices as though they are full rank (i.e., $d = n$) by implicitly identifying $\text{span}(\mathcal{L})$ with \mathbb{R}^d . The *dual lattice*

$$\mathcal{L}^* := \{\mathbf{w} \in \text{span}(\mathcal{L}) : \forall \mathbf{y} \in \mathcal{L}, \langle \mathbf{w}, \mathbf{y} \rangle \in \mathbb{Z}\}$$

is the set of all vectors in the span of \mathcal{L} that have integer inner products with all lattice vectors. One can check that $\mathcal{L}^{**} = \mathcal{L}$ and that \mathcal{L}^* is generated by $\mathbf{B}^* := \mathbf{B}(\mathbf{B}^T \mathbf{B})^{-1}$.

We write

$$\lambda_1(\mathcal{L}) := \min_{\mathbf{y} \in \mathcal{L} \setminus \{\mathbf{0}\}} \|\mathbf{y}\|$$

for the length of the shortest non-zero lattice vector. The *covering radius* is

$$\mu(\mathcal{L}) := \max_{\mathbf{t} \in \text{span}(\mathcal{L})} \min_{\mathbf{y} \in \mathcal{L}} \|\mathbf{t} - \mathbf{y}\|.$$

It is not hard to show that $\lambda_1(\mathcal{L}) \leq 2\mu(\mathcal{L})$ (e.g., by taking $\mathbf{t} = \mathbf{v}/2$, where $\mathbf{v} \in \mathcal{L}$ has $\|\mathbf{v}\| = \lambda_1(\mathcal{L})$).

The *determinant* of the lattice is given by $\det(\mathcal{L}) := \sqrt{\det(\mathbf{B}^T \mathbf{B})}$, or simply $|\det(\mathbf{B})|$ in the full-rank case. One can show that the determinant is well defined (i.e., it does not depend on the choice of basis \mathbf{B}). It follows that if $\mathcal{L} \subset \mathbb{R}^n$ has full rank and $A \in \mathbb{R}^{n \times n}$ is non-singular, then $\det(A\mathcal{L}) = |\det(A)| \det(\mathcal{L})$, and that $\det(\mathcal{L}^*) = 1/\det(\mathcal{L})$.

A *sublattice* $\mathcal{L}' \subseteq \mathcal{L}$ is an additive subgroup of \mathcal{L} . We say that \mathcal{L}' is *primitive* if $\mathcal{L}' = \mathcal{L} \cap \text{span}(\mathcal{L}')$. For a primitive sublattice $\mathcal{L}' \subseteq \mathcal{L}$, we define the quotient lattice $\mathcal{L}/\mathcal{L}' := \pi_{\text{span}(\mathcal{L}')^\perp}(\mathcal{L})$ to be the

projection of \mathcal{L} onto the space orthogonal to \mathcal{L}' . In particular, \mathcal{L}/\mathcal{L}' is a lattice, and we have the identities $(\mathcal{L}/\mathcal{L}')^* = \mathcal{L}^* \cap \text{span}(\mathcal{L}')^\perp$ and $\det(\mathcal{L}/\mathcal{L}') = \det(\mathcal{L})/\det(\mathcal{L}')$.

For a parameter $s > 0$ and $\mathbf{x} \in \mathbb{R}^n$, we define $\rho_s(\mathbf{x}) = e^{-\pi\|\mathbf{x}\|^2/s^2}$. Then, for any discrete set A , we define its Gaussian mass as $\rho_s(A) = \sum_{\mathbf{x} \in A} \rho_s(\mathbf{x})$. When $s = 1$, we omit the subscript.

We recall the Poisson Summation Formula for the Gaussian mass of a lattice, which says that

$$\rho_s(\mathcal{L}) = \frac{s^n}{\det(\mathcal{L})} \cdot \rho_{1/s}(\mathcal{L}^*) \quad (5)$$

for any $s > 0$ and (full-rank) lattice $\mathcal{L} \subset \mathbb{R}^n$. As an example, it follows that for any full-rank lattice $\mathcal{L} \subset \mathbb{R}^n$,

$$\rho_s(\mathcal{L}) > \frac{s^n}{\det(\mathcal{L})} . \quad (6)$$

Lemma 2.1 ([Ban93, Lemma 1.5]). *For any lattice $\mathcal{L} \subset \mathbb{R}^n$, shift vector $\mathbf{u} \in \mathbb{R}^n$, and any $r \geq 1/\sqrt{2\pi}$,*

$$\rho((\mathcal{L} - \mathbf{u}) \setminus r\sqrt{n}B_2^n) \leq (\sqrt{2\pi}er^2e^{-\pi r^2})^n \cdot \rho(\mathcal{L}) .$$

The following claim was observed by Banaszczyk [Ban93] and is an immediate consequence of the Poisson Summation Formula and positivity.

Claim 2.2. *For any lattice $\mathcal{L} \subset \mathbb{R}^n$, shift vector $\mathbf{u} \in \mathbb{R}^n$, and parameter $s > 0$, $\rho_s(\mathcal{L} - \mathbf{u}) \leq \rho_s(\mathcal{L})$ with equality if and only if $\mathbf{u} \in \mathcal{L}$.*

Proof. By applying the Poisson summation formula to the shifted Gaussian $\rho_s(\mathcal{L} - \mathbf{u})$, we see that

$$\rho_s(\mathcal{L} - \mathbf{u}) = \frac{s^n}{\det(\mathcal{L})} \sum_{\mathbf{w} \in \mathcal{L}^*} \rho_{1/s}(\mathbf{w}) \cos(2\pi\langle \mathbf{w}, \mathbf{u} \rangle) \leq \frac{s^n}{\det(\mathcal{L})} \sum_{\mathbf{w} \in \mathcal{L}^*} \rho_{1/s}(\mathbf{w}) = \rho_s(\mathcal{L}) ,$$

as needed, where we have equality if and only if $\langle \mathbf{w}, \mathbf{u} \rangle \in \mathbb{Z}$ for all $\mathbf{w} \in \mathcal{L}^*$, i.e., if and only if $\mathbf{u} \in \mathcal{L}$. \square

Lemma 2.3. *For any lattice $\mathcal{L} \subset \mathbb{R}^n$, primitive sublattice $\mathcal{L}' \subset \mathcal{L}$, and $s > 0$,*

$$\rho_s(\mathcal{L}) \leq \rho_s(\mathcal{L}' \oplus \mathcal{L}/\mathcal{L}') = \rho_s(\mathcal{L}')\rho_s(\mathcal{L}/\mathcal{L}') ,$$

with equality if and only if $\mathcal{L} = \mathcal{L}' \oplus \mathcal{L}/\mathcal{L}'$.

Proof. Let $T \subset \mathcal{L}$ be any complete set of coset representatives of \mathcal{L} modulo \mathcal{L}' . (In other words, for every $\mathbf{y} \in \mathcal{L}$ there exists a unique $\mathbf{t} \in T$ such that $\mathbf{y} \equiv \mathbf{t} \pmod{\mathcal{L}'}$.) Let $\pi := \pi_{\text{span}(\mathcal{L}')}$, and $\pi^\perp := \pi_{\text{span}(\mathcal{L}')^\perp}$. Then,

$$\begin{aligned} \sum_{\mathbf{y} \in \mathcal{L}} \rho_s(\mathbf{y}) &= \sum_{\mathbf{t} \in T, \mathbf{y}' \in \mathcal{L}'} \rho_s(\mathbf{t} + \mathbf{y}') \\ &= \sum_{\mathbf{t} \in T, \mathbf{y}' \in \mathcal{L}'} \rho_s(\mathbf{y}' + \pi(\mathbf{t}))\rho_s(\pi^\perp(\mathbf{t})) \\ &= \sum_{\mathbf{t} \in T} \rho_s(\mathcal{L}' + \pi(\mathbf{t}))\rho_s(\pi^\perp(\mathbf{t})) \\ &\leq \rho_s(\mathcal{L}') \sum_{\mathbf{t} \in T} \rho_s(\pi^\perp(\mathbf{t})) \\ &= \rho_s(\mathcal{L}')\rho_s(\mathcal{L}/\mathcal{L}') , \end{aligned}$$

where the inequality is Claim 2.2 and the last equality uses the primitivity of \mathcal{L}' . \square

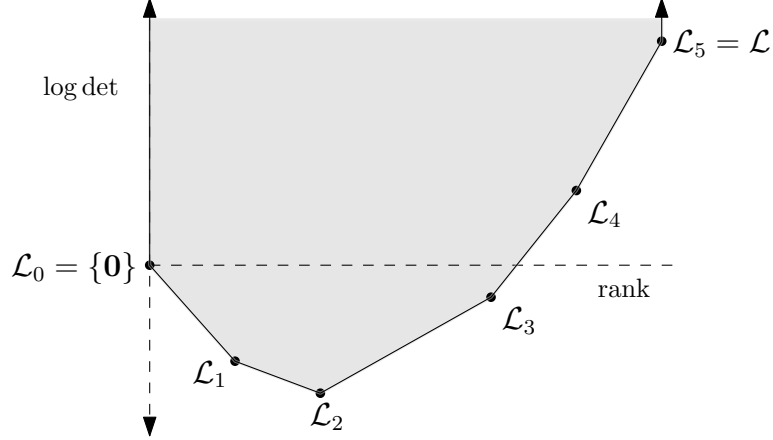


Figure 1: The canonical polygon of a (hypothetical) lattice \mathcal{L} .

2.2 Linear algebra

We write $\mathrm{SL}_n(\mathbb{R})$ for the group of all $n \times n$ determinant-one real matrices. A matrix $U \in \mathrm{SL}_n(\mathbb{R})$ is *orthogonal* if $U^T U = I_n$. Equivalently, a matrix is orthogonal if its associated linear transformation is an isometry. (I.e., $\|U\mathbf{x}\| = \|\mathbf{x}\|$ for all $\mathbf{x} \in \mathbb{R}^n$.) We write $\|A\| := \sup_{\mathbf{x} \in \mathbb{R}^n \setminus \{0\}} \|A\mathbf{x}\|/\|\mathbf{x}\|$ for the *operator norm* of A .

We recall the definition of the *matrix exponential*,

$$e^A := I_n + A + A^2/2 + A^3/6 + \cdots,$$

for any matrix $A \in \mathbb{R}^{n \times n}$, and the identity $\det(e^A) = e^{\mathrm{Tr}(A)}$. Every positive-definite matrix A has a matrix logarithm M such that $e^M = A$.

2.3 A note on the topology of the space of determinant-one lattices

Throughout this paper, we consider various topological notions over the space of determinant-one (full-rank) lattices in \mathbb{R}^n (e.g., local maxima of functions over this space, compact sets, etc.). Formally, the space of determinant-one lattices is $\mathrm{SO}_n(\mathbb{R}) \backslash \mathrm{SL}_n(\mathbb{R}) / \mathrm{SL}_n(\mathbb{Z})$, i.e., the set of determinant-one real matrices modulo the orthogonal matrices $\mathrm{SO}_n(\mathbb{R})$ (i.e., isometries) and the unimodular matrices $\mathrm{SL}_n(\mathbb{Z})$, which are transformations between bases of the same lattice. The topology is the quotient topology. (See [Ter16, Section 1.4].) However, the reader may prefer to think of the space of determinant-one lattice *bases*, which is simply $\mathrm{SL}_n(\mathbb{R})$ with its standard topology.

2.4 Stability

We say that a lattice $\mathcal{L} \subset \mathbb{R}^n$ is *stable* if $\det(\mathcal{L}) = 1$ and $\det(\mathcal{L}') \geq 1$ for all sublattices $\mathcal{L}' \subseteq \mathcal{L}$. (Some authors call such lattices “semistable.”) Note the obvious relationship between this notion and Theorem 1.2. Here, we describe the properties of stable lattices that we will need in the sequel, and include proofs for completeness. This theory was developed by [HN75, Stu76, Gra84]. See, e.g., [Gra84, Cas04] for a more thorough treatment.

We can in some sense “decompose” any lattice into stable lattices. To see this, we consider the two-dimensional scatter plot with points

$$\{(\text{rank}(\mathcal{L}'), \log \det(\mathcal{L}')) : \mathcal{L}' \subseteq \mathcal{L}\},$$

for some lattice $\mathcal{L} \subset \mathbb{R}^n$, where we explicitly include the trivial sublattice $\{\mathbf{0}\}$ and define $\log \det(\{\mathbf{0}\}) := 0$. We call this the *canonical plot* of \mathcal{L} . Note that these points are bounded from below and that for each rank $0 \leq k \leq n$, there is a (not necessarily unique) sublattice of rank k that has minimal determinant among all sublattices with rank k . The convex hull of these points is therefore a degenerate polygon (bounded from below, but unbounded from above), called the *canonical polygon* of \mathcal{L} . See Figure 1.

We are interested in the extremal points of this polygon. (E.g., $\mathcal{L}_0, \dots, \mathcal{L}_5$ in Figure 1.) Notice that any sublattice corresponding to an extremal point must necessarily be densest among all sublattices of that rank, but this necessary condition is not sufficient. In fact, it is known that each extremal point corresponds to a *unique* sublattice. Moreover, if two sublattices \mathcal{L}_1 and \mathcal{L}_2 both correspond to extremal points, then one is contained in the other. Therefore, the extremal points define a *canonical filtration* of \mathcal{L} ,

$$\{\mathbf{0}\} = \mathcal{L}_0 \subset \mathcal{L}_1 \subset \dots \subset \mathcal{L}_k = \mathcal{L}.$$

(Note that we only include in the canonical filtration lattices that correspond to *extremal points*, not any lattice on the boundary. E.g., the canonical filtration of \mathbb{Z}^n is trivial: $\{\mathbf{0}\} = \mathcal{L}_0 \subset \mathcal{L}_1 = \mathbb{Z}^n$.) It is also known that all of the quotients $\mathcal{L}_i/\mathcal{L}_{i-1}$ of adjacent sublattices in the canonical filtration are scalings of stable lattices. This is what we mean when we say that we can “decompose” a lattice into a sequence of stable lattices.

Following [Gra84, Cas04], we make the above (and other) facts precise in Proposition 2.5, which lists basic properties of the canonical filtration and stable lattices. We first need the following lemma, due to Stuhler [Stu76].

Lemma 2.4. *For any $\mathcal{L} \subset \mathbb{R}^n$ and any two primitive sublattices $\mathcal{L}_1, \mathcal{L}_2 \subseteq \mathcal{L}$,*

$$\text{rank}(\mathcal{L}_1) + \text{rank}(\mathcal{L}_2) = \text{rank}(\mathcal{L}_1 \cap \mathcal{L}_2) + \text{rank}(\mathcal{L}_1 + \mathcal{L}_2),$$

and

$$\det(\mathcal{L}_1 \cap \mathcal{L}_2) \det(\mathcal{L}_1 + \mathcal{L}_2) \leq \det(\mathcal{L}_1) \det(\mathcal{L}_2),$$

where we define $\det(\{\mathbf{0}\}) = 1$.

Proof. The equality of ranks follows by considering the dimensions of the subspaces spanned by $\mathcal{L}_1, \mathcal{L}_2, \mathcal{L}_1 \cap \mathcal{L}_2$, and $\mathcal{L}_1 + \mathcal{L}_2$. For the inequality, suppose that $\mathcal{M}_1, \mathcal{M}_2 \subseteq \mathcal{M}$ are sublattices such that $\mathcal{M}_1 \cap \mathcal{M}_2 = \{\mathbf{0}\}$ and $\mathcal{M}_1 + \mathcal{M}_2 = \mathcal{M}$. Then, we have

$$\det(\mathcal{M}) = \det(\mathcal{M}_1) \cdot \det(\pi_{\text{span}(\mathcal{M}_1)^\perp}(\mathcal{M}_2)) \leq \det(\mathcal{M}_1) \det(\mathcal{M}_2),$$

where we have used the fact that $\pi_{\text{span}(\mathcal{M}_1)^\perp}$ is a contraction that preserves the rank of \mathcal{M}_2 . Plugging in $\mathcal{M} := (\mathcal{L}_1 + \mathcal{L}_2)/(\mathcal{L}_1 \cap \mathcal{L}_2)$, $\mathcal{M}_1 := \mathcal{L}_1/(\mathcal{L}_1 \cap \mathcal{L}_2)$ and $\mathcal{M}_2 := \mathcal{L}_2/(\mathcal{L}_1 \cap \mathcal{L}_2)$ gives

$$\begin{aligned} \det(\mathcal{L}_1 + \mathcal{L}_2) / \det(\mathcal{L}_1 \cap \mathcal{L}_2) &= \det((\mathcal{L}_1 + \mathcal{L}_2)/(\mathcal{L}_1 \cap \mathcal{L}_2)) \\ &\leq \det(\mathcal{L}_1/(\mathcal{L}_1 \cap \mathcal{L}_2)) \det(\mathcal{L}_2/(\mathcal{L}_1 \cap \mathcal{L}_2)) \\ &= \det(\mathcal{L}_1) \det(\mathcal{L}_2) / \det(\mathcal{L}_1 \cap \mathcal{L}_2)^2. \end{aligned}$$

The result follows by rearranging. □

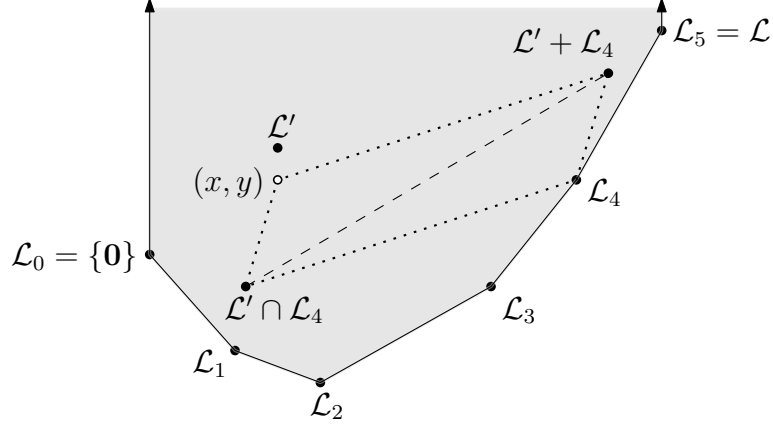


Figure 2: An illustration of the proof of Item 1 of Proposition 2.5 (similar to [Gra84, Figure 1.17]). In particular, if $\mathcal{L}' \not\subseteq \mathcal{L}_4$, then (x, y) must lie strictly above the dashed line, and therefore cannot be an extremal point (or even a boundary point) of the canonical polytope.

Proposition 2.5. *For any lattice $\mathcal{L} \subset \mathbb{R}^n$, let $\{0\} = \mathcal{L}_0, \mathcal{L}_1, \dots, \mathcal{L}_k = \mathcal{L}$ be all sublattices corresponding to extremal points of the canonical polytope, ordered by their rank. (See Figure 1.) Then,*

1. *the \mathcal{L}_i define a filtration $\mathcal{L}_0 \subset \mathcal{L}_1 \subset \dots \subset \mathcal{L}_k$ (in particular, the \mathcal{L}_i have distinct ranks);*
2. *the quotient lattice $\mathcal{L}_i/\mathcal{L}_{i-1}$ is a scaling of a stable lattice for $1 \leq i \leq k$ (i.e., $\alpha_i \cdot \mathcal{L}_i/\mathcal{L}_{i-1}$ is stable, where $\alpha_i := \det(\mathcal{L}_i/\mathcal{L}_{i-1})^{-1/\text{rank}(\mathcal{L}_i/\mathcal{L}_{i-1})}$); and*
3. *for all $1 \leq i \leq k-1$, $\det(\mathcal{L}_i/\mathcal{L}_{i-1})^{1/\text{rank}(\mathcal{L}_i/\mathcal{L}_{i-1})} < \det(\mathcal{L}_{i+1}/\mathcal{L}_i)^{1/\text{rank}(\mathcal{L}_{i+1}/\mathcal{L}_i)}$.*

Furthermore,

- (i) *the dual of a stable lattice is stable;*
- (ii) *the set of all stable lattices is compact;*
- (iii) *the direct sum of stable lattices is stable; and*
- (iv) *a lattice $\mathcal{L} \subset \mathbb{R}^n$ is on the boundary of the set of stable lattices if and only if \mathcal{L} is stable and there is a primitive sublattice $\mathcal{L}' \subset \mathcal{L}$ with $0 < \text{rank}(\mathcal{L}') < n$ such that \mathcal{L}' and \mathcal{L}/\mathcal{L}' are both stable.*

Proof. To prove Item 1, fix an index i and let $\mathcal{L}' \subset \mathcal{L}$ be a sublattice with $\text{rank}(\mathcal{L}') \leq \text{rank}(\mathcal{L}_i)$ but $\mathcal{L}' \not\subseteq \mathcal{L}_i$. Below we will show that \mathcal{L}' must lie in the interior of the canonical polytope. In particular, this would imply that each \mathcal{L}_j with $j \leq i$ must have $\mathcal{L}_j \subseteq \mathcal{L}_i$, as desired.

First, notice that we must have $\text{rank}(\mathcal{L}' + \mathcal{L}_i) > \text{rank}(\mathcal{L}_i)$, since otherwise $\mathcal{L}' + \mathcal{L}_i$ would be a strict superlattice of \mathcal{L}_i with the same rank, contradicting the assumption that \mathcal{L}_i is an extremal point of the canonical polytope. Notice that, by Lemma 2.4, this also implies that $\text{rank}(\mathcal{L}' \cap \mathcal{L}_i) < \text{rank}(\mathcal{L}') \leq \text{rank}(\mathcal{L}_i)$. Now, consider the point (x, y) in the plane with

$$x := \text{rank}(\mathcal{L}' \cap \mathcal{L}_i) + \text{rank}(\mathcal{L}' + \mathcal{L}_i) - \text{rank}(\mathcal{L}_i)$$

and

$$y := \log \det(\mathcal{L}' \cap \mathcal{L}_i) + \log \det(\mathcal{L}' + \mathcal{L}_i) - \log \det(\mathcal{L}_i) .$$

See Figure 2. By Lemma 2.4, we have $\text{rank}(\mathcal{L}') = x$ and $\log \det(\mathcal{L}') \geq y$, i.e., that the point $(\text{rank}(\mathcal{L}'), \log \det(\mathcal{L}'))$ lies on or above the point (x, y) in the plane. It therefore suffices to show that (x, y) is in the interior of the canonical polygon, which we do by showing that (x, y) lies strictly above the line segment between the points $(\text{rank}(\mathcal{L}' \cap \mathcal{L}_i), \log \det(\mathcal{L}' \cap \mathcal{L}_i))$ and $(\text{rank}(\mathcal{L}' + \mathcal{L}_i), \log \det(\mathcal{L}' + \mathcal{L}_i))$. (See the dashed line in Figure 2.) Equivalently, it is enough to show that $(\text{rank}(\mathcal{L}_i), \log \det(\mathcal{L}_i))$ lies strictly below this line segment (since it is the reflection of (x, y) through the midpoint of the line segment). This holds because \mathcal{L}_i corresponds to an extremal point, and, because $\text{rank}(\mathcal{L}' \cap \mathcal{L}_i) < \text{rank}(\mathcal{L}_i) < \text{rank}(\mathcal{L}' + \mathcal{L}_i)$, it is distinct from the two endpoints of the line segment.

To prove Item 2, let $\mathcal{L}' \subseteq \mathcal{L}_i / \mathcal{L}_{i-1}$ be a sublattice. Let $\widehat{\mathcal{L}} \subseteq \mathcal{L}_i$ be the sublattice satisfying $\mathcal{L}_{i-1} \subseteq \widehat{\mathcal{L}}$ and $\mathcal{L}' = \widehat{\mathcal{L}} / \mathcal{L}_{i-1}$. Since \mathcal{L}_{i-1} and \mathcal{L}_i are consecutive extremal points of the canonical polygon, the point $(\text{rank}(\widehat{\mathcal{L}}), \log \det(\widehat{\mathcal{L}}))$ must lie on or above the line between $(\text{rank}(\mathcal{L}_{i-1}), \log \det(\mathcal{L}_{i-1}))$ and $(\text{rank}(\mathcal{L}_i), \log \det(\mathcal{L}_i))$. This statement is equivalent to the inequality in the following:

$$\begin{aligned} \det(\mathcal{L}') &= \det(\widehat{\mathcal{L}}) / \det(\mathcal{L}_{i-1}) \\ &\geq \left(\frac{\det(\mathcal{L}_i)}{\det(\mathcal{L}_{i-1})} \right)^{\frac{\text{rank}(\widehat{\mathcal{L}}) - \text{rank}(\mathcal{L}_{i-1})}{\text{rank}(\mathcal{L}_i) - \text{rank}(\mathcal{L}_{i-1})}} \\ &= \det(\mathcal{L}_i / \mathcal{L}_{i-1})^{\frac{\text{rank}(\mathcal{L}')}{\text{rank}(\mathcal{L}_i / \mathcal{L}_{i-1})}} . \end{aligned}$$

I.e., if we set $\alpha_i := \det(\mathcal{L}_i / \mathcal{L}_{i-1})^{-1 / \text{rank}(\mathcal{L}_i / \mathcal{L}_{i-1})}$, then $\det(\alpha_i \mathcal{L}') \geq 1$. It follows that $\alpha_i \mathcal{L}_i / \mathcal{L}_{i-1}$ is stable, as claimed.

Item 3 simply says that the slopes of the lines between extremal points on the canonical polytope are strictly increasing. This follows immediately from the definition of the canonical polytope. (See Figure 1.)

To prove Item (i), let $\mathcal{M} \subset \mathbb{R}^n$ be a stable lattice and let $\mathcal{M}' \subseteq \mathcal{M}^*$ be a primitive sublattice of the dual. We have

$$\det(\mathcal{M}') = \frac{1}{\det(\mathcal{M}^* / \mathcal{M}')} = \det((\mathcal{M}^* / \mathcal{M}')^*) = \det(\mathcal{M} \cap \text{span}(\mathcal{M}')^\perp) \geq 1 .$$

Therefore, \mathcal{M}^* is stable.

Item (ii) follows immediately from Mahler's compactness theorem [Mah46] together with the observation that $\lambda_1(\mathcal{M}) \geq 1$ for any stable lattice \mathcal{M} .

To prove Item (iii), let $\mathcal{M}_1, \mathcal{M}_2$ be two stable lattices, and let $\mathcal{M}' \subset \mathcal{M}_1 \oplus \mathcal{M}_2$ be a primitive sublattice. Then, applying Lemma 2.4, we have

$$\det(\mathcal{M}') \geq \frac{\det(\mathcal{M}' \cap \mathcal{M}_1) \det(\mathcal{M}' + \mathcal{M}_1)}{\det(\mathcal{M}_1)} = \det(\mathcal{M}' \cap \mathcal{M}_1) \det(\mathcal{M}' + \mathcal{M}_1) .$$

Note that $\mathcal{M}' \cap \mathcal{M}_1$ is a sublattice of \mathcal{M}_1 , so that $\det(\mathcal{M}' \cap \mathcal{M}_1) \geq 1$. And $\mathcal{M}' + \mathcal{M}_1 = \mathcal{M}_1 \oplus \pi_{\text{span}(\mathcal{M}_2)}(\mathcal{M}')$ is the direct sum of \mathcal{M}_1 with a sublattice of \mathcal{M}_2 , so that $\det(\mathcal{M}' + \mathcal{M}_1) = \det(\pi_{\text{span}(\mathcal{M}_2)}(\mathcal{M}')) \geq 1$ as well. The result follows.

Finally, Item (iv) follows by first noting that a stable lattice \mathcal{M} is on the boundary if and only if there is some strict primitive non-zero sublattice $\mathcal{M}' \subset \mathcal{M}$ with $\det(\mathcal{M}') = 1$. Clearly, \mathcal{M}' is stable,

since it has determinant one and all of its sublattices are also sublattices of \mathcal{M} , so that they must have determinant at least one. To see that \mathcal{M}/\mathcal{M}' is stable, first notice that it has determinant one. Next, let $\mathcal{L}' \subseteq \mathcal{M}/\mathcal{M}'$ be an arbitrary sublattice. Let $\widehat{\mathcal{L}} \subseteq \mathcal{M}$ be the sublattice satisfying $\mathcal{M}' \subseteq \widehat{\mathcal{L}}$ and $\mathcal{L}' = \widehat{\mathcal{L}}/\mathcal{M}'$. Then $\det \mathcal{L}' = \det \widehat{\mathcal{L}} / \det \mathcal{M}' = \det \widehat{\mathcal{L}} \geq 1$, where the inequality uses that \mathcal{M} is stable. \square

2.5 The Voronoi cell and fundamental bodies

The *Voronoi cell* of a lattice $\mathcal{L} \subset \mathbb{R}^n$,

$$\mathcal{V}(\mathcal{L}) := \{ \mathbf{x} \in \mathbb{R}^n : \langle \mathbf{x}, \mathbf{y} \rangle \leq \|\mathbf{y}\|^2/2, \forall \mathbf{y} \in \mathcal{L} \},$$

is the set of vectors in \mathbb{R}^n that are at least as close to $\mathbf{0}$ than to any other lattice vector. In fact, it is a symmetric polytope.

A *fundamental body* of a lattice $\mathcal{L} \subset \mathbb{R}^n$ is any convex body $K \subset \mathbb{R}^n$ such that $K + \mathcal{L} = \mathbb{R}^n$ and $\text{Int}(K) \cap (K + \mathbf{y}) = \emptyset$ for any non-zero lattice point $\mathbf{y} \in \mathcal{L} \setminus \{\mathbf{0}\}$. Equivalently, $\text{vol}(K) = \det(\mathcal{L})$ and $\text{Int}(K) \cap (K + \mathbf{y}) = \emptyset$ for any non-zero lattice point $\mathbf{y} \in \mathcal{L} \setminus \{\mathbf{0}\}$. In particular, the Voronoi cell is a fundamental body.

Claim 2.6. *For any lattice $\mathcal{L} \subset \mathbb{R}^n$, primitive sublattice $\mathcal{L}' \subset \mathbb{R}^n$, fundamental body $K_1 \subset \text{span}(\mathcal{L}')$ of \mathcal{L}' , and fundamental body $K_2 \subset \text{span}(\mathcal{L}')^\perp$ of \mathcal{L}/\mathcal{L}' , the Minkowski sum $K := K_1 + K_2$ is a fundamental body of \mathcal{L} . In particular, if $\{\mathbf{0}\} = \mathcal{L}_0 \subset \mathcal{L}_1 \subset \dots \subset \mathcal{L}_k$ is a filtration of primitive sublattices, then*

$$\mathcal{V}\left(\bigoplus_i \mathcal{L}_i/\mathcal{L}_{i-1}\right) = \mathcal{V}(\mathcal{L}_1/\mathcal{L}_0) + \dots + \mathcal{V}(\mathcal{L}_k/\mathcal{L}_{k-1})$$

is a fundamental body of \mathcal{L} .

Proof. Notice that

$$\text{vol}(K) = \text{vol}(K_1) \cdot \text{vol}(K_2) = \det(\mathcal{L}') \cdot \det(\mathcal{L}/\mathcal{L}') = \det(\mathcal{L}).$$

It therefore suffices to show that $\text{Int}(K) \cap (K + \mathbf{y}) = \emptyset$ for any $\mathbf{y} \in \mathcal{L} \setminus \{\mathbf{0}\}$. So suppose there exists $\mathbf{y} \in \mathcal{L}$ such that $\text{Int}(K) \cap (K + \mathbf{y}) \neq \emptyset$. Then, by projecting orthogonally to \mathcal{L}' , we see that $\text{Int}(K_2) \cap (K_2 + \pi_{\text{span}(\mathcal{L}')^\perp}(\mathbf{y})) \neq \emptyset$. Since K_2 is a fundamental body of \mathcal{L}/\mathcal{L}' and $\pi_{\text{span}(\mathcal{L}')^\perp}(\mathbf{y}) \in \mathcal{L}/\mathcal{L}'$, it follows that $\pi_{\text{span}(\mathcal{L}')^\perp}(\mathbf{y}) = \mathbf{0}$, i.e., $\mathbf{y} \in \mathcal{L}'$. Intersecting with $\text{span}(\mathcal{L}')$, this implies that $\text{Int}(K_1) \cap (K_1 + \mathbf{y}) \neq \emptyset$. Since $\mathbf{y} \in \mathcal{L}'$ and K_1 is a fundamental body of \mathcal{L}' , we obtain that $\mathbf{y} = \mathbf{0}$. The result follows. \square

We will also need the following claim, which follows immediately from the definition of a fundamental body.

Claim 2.7. *For any lattice $\mathcal{L} \subset \mathbb{R}^n$, fundamental body K of \mathcal{L} , and non-singular matrix $A \in \mathbb{R}^{n \times n}$, the body AK is a fundamental body of $A\mathcal{L}$. In particular, $A\mathcal{V}(\mathcal{L})$ is a fundamental body of $A\mathcal{L}$.*

Proof. It suffices to notice that $AK + A\mathcal{L} = A(K + \mathcal{L}) = \mathbb{R}^n$ and $\text{Int}(AK) \cap (AK + A\mathbf{y}) = A(\text{Int}(K) \cap (K + \mathbf{y})) = \emptyset$ for $\mathbf{y} \in \mathcal{L} \setminus \{\mathbf{0}\}$. \square

The next lemma and its corollary show that the Voronoi cell is in some sense the “optimal fundamental body.” They are very similar to some results due to Dadush [Dad12b, Lemma 6.3.6, Corollary 6.3.7].

Lemma 2.8. *For any lattice $\mathcal{L} \subset \mathbb{R}^n$, there is a map $\psi_{\mathcal{L}} : \mathbb{R}^n \rightarrow \mathcal{V}(\mathcal{L})$ such that $\|\psi_{\mathcal{L}}(\mathbf{x})\| \leq \|\mathbf{x}\|$, and for every fundamental body K of \mathcal{L} , $\psi_{\mathcal{L}}$ restricted to $\text{Int}(K)$ is injective and volume-preserving.*

Proof. The function $\psi_{\mathcal{L}}$ just maps \mathbf{x} to a representative of $\mathbf{x} \bmod \mathcal{L}$ that is in the Voronoi cell. Specifically, let $\text{CVP}_{\mathcal{L}}(\mathbf{x}) := \arg\min_{\mathbf{y} \in \mathcal{L}} \|\mathbf{y} - \mathbf{x}\|$ be a closest lattice vector to \mathbf{x} (breaking ties arbitrarily), and let $\psi_{\mathcal{L}}(\mathbf{x}) := \mathbf{x} - \text{CVP}_{\mathcal{L}}(\mathbf{x})$. By the definition of CVP, it is immediate that $\|\psi_{\mathcal{L}}(\mathbf{x})\| = \min_{\mathbf{y} \in \mathcal{L}} \|\mathbf{y} - \mathbf{x}\| \leq \|\mathbf{x}\|$.

Suppose $\psi_{\mathcal{L}}(\mathbf{x}) = \psi_{\mathcal{L}}(\mathbf{x}')$ for some $\mathbf{x}, \mathbf{x}' \in \text{Int}(K)$. I.e., $\mathbf{x} - \text{CVP}_{\mathcal{L}}(\mathbf{x}) = \mathbf{x}' - \text{CVP}_{\mathcal{L}}(\mathbf{x}')$. Rearranging, we see that $\mathbf{y} := \mathbf{x} - \mathbf{x}' = \text{CVP}_{\mathcal{L}}(\mathbf{x}) - \text{CVP}_{\mathcal{L}}(\mathbf{x}')$ is a lattice point. But, $\mathbf{x} \in \text{Int}(K) \cap (K + \mathbf{y})$. Since K is a fundamental body, it follows that $\mathbf{y} = \mathbf{0}$. I.e., $\mathbf{x} = \mathbf{x}'$, and $\psi_{\mathcal{L}}$ is injective over $\text{Int}(K)$.

The fact that $\psi_{\mathcal{L}}$ is volume-preserving over $\text{Int}(K)$ follows from the fact that it is injective and preserves volume locally. \square

Corollary 2.9. *For any non-decreasing measurable function $f : \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}$, lattice $\mathcal{L} \subset \mathbb{R}^n$, and fundamental body K of \mathcal{L} ,*

$$\int_{\mathcal{V}(\mathcal{L})} f(\|\mathbf{x}\|) d\mathbf{x} \leq \int_K f(\|\mathbf{x}\|) d\mathbf{x}.$$

Proof.

$$\int_K f(\|\mathbf{x}\|) d\mathbf{x} = \int_{\text{Int}(K)} f(\|\mathbf{x}\|) d\mathbf{x} \geq \int_{\text{Int}(K)} f(\|\psi_{\mathcal{L}}(\mathbf{x})\|) d\mathbf{x} = \int_{\psi_{\mathcal{L}}(\text{Int}(K))} f(\|\mathbf{x}\|) d\mathbf{x} = \int_{\mathcal{V}(\mathcal{L})} f(\|\mathbf{x}\|) d\mathbf{x},$$

where the last equality follows from the fact that $\psi_{\mathcal{L}}$ preserves volume and $\text{vol}(\text{Int}(K)) = \text{vol}(\mathcal{V}(\mathcal{L}))$, so it must be the case that $\psi_{\mathcal{L}}(\text{Int}(K)) \subset \mathcal{V}(\mathcal{L})$ differs from $\mathcal{V}(\mathcal{L})$ on a set of measure zero. \square

2.6 Matrix calculus

We say that a function $g : \mathbb{R}^{n \times n} \rightarrow \mathbb{R}$ is *differentiable* at $Q \in \mathbb{R}^{n \times n}$ if there exists a $B \in \mathbb{R}^{n \times n}$ such that

$$\lim_{M \rightarrow 0} \frac{g(Q + M) - g(Q) - \text{Tr}(B^T M)}{\|M\|} = 0,$$

and we call B the *gradient* of g at Q ,

$$\nabla_A g(A)|_{A=Q} := B. \quad (7)$$

(Some authors prefer to define $\nabla_A g(A)|_{A=Q}$ as B^T .)

3 Gradients over lattices and over positions of the Voronoi cell

The purpose of this section is to prove the following theorem.

Theorem 3.1. *For any continuously differentiable function $f : \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}$ and lattice $\mathcal{L} \subset \mathbb{R}^n$, let*

$$g(A) := \frac{1}{|\det(A)|} \cdot \int_{\mathcal{V}(A\mathcal{L})} f(\|\mathbf{x}\|^2) d\mathbf{x}, \text{ and } h(A) := \frac{1}{|\det(A)|} \cdot \int_{A\mathcal{V}(\mathcal{L})} f(\|\mathbf{x}\|^2) d\mathbf{x},$$

where $A \in \mathbb{R}^{n \times n}$ is a non-singular matrix. Then, g and h are differentiable at $A = I_n$, with

$$\nabla_A g(A)|_{A=I_n} = \nabla_A h(A)|_{A=I_n} = 2 \int_{\mathcal{V}(\mathcal{L})} f'(\|\mathbf{x}\|^2) \mathbf{x} \mathbf{x}^T d\mathbf{x} ,$$

where $f'(x) := \frac{d}{dx} f(x)$.

We first compute the gradient of h , which is straightforward.

Claim 3.2. *For any continuously differentiable function $f : \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}$ and bounded measurable set $U \subset \mathbb{R}^n$, let*

$$h(A) := \frac{1}{|\det(A)|} \cdot \int_{AU} f(\|\mathbf{x}\|^2) d\mathbf{x} ,$$

where $A \in \mathbb{R}^{n \times n}$ is a non-singular matrix. Then, h is differentiable with

$$\nabla_A h(A)|_{A=I_n} = 2 \int_U f'(\|\mathbf{x}\|^2) \mathbf{x} \mathbf{x}^T d\mathbf{x} ,$$

where $f'(x) := \frac{d}{dx} f(x)$.

Proof. By a change of variables, we have

$$h(A) = \int_U f(\|A\mathbf{x}\|^2) d\mathbf{x} .$$

Next, by the chain rule, $\nabla_A f(\|A\mathbf{x}\|^2) = 2f'(\|A\mathbf{x}\|^2) A\mathbf{x} \mathbf{x}^T$, which is bounded as x ranges over U and A ranges over any bounded set. Therefore, we may use the bounded convergence theorem to swap the gradient and the integral and write

$$\begin{aligned} \nabla_A h(A) &= \int_U (\nabla_A f(\|A\mathbf{x}\|^2)) d\mathbf{x} \\ &= 2 \int_U f'(\|A\mathbf{x}\|^2) A\mathbf{x} \mathbf{x}^T d\mathbf{x} . \end{aligned} \quad \square$$

Now, we prove Theorem 3.1. (We thank Ronen Eldan for showing us this proof. An earlier version of this work had a much longer proof.)

Proof of Theorem 3.1. Fix a continuously differentiable function $f : \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}$ and a lattice $\mathcal{L} \subset \mathbb{R}^n$. By Claim 3.2, it suffices to show that the gradient of g at I_n exists and is equal to the gradient of h at I_n . Recalling the definition of the gradient in Eq. (7), we see that this is equivalent to proving that

$$\lim_{M \rightarrow 0} \frac{h(I_n + M) - g(I_n + M)}{\|M\|} = 0 . \quad (8)$$

In fact, setting $\nu = \nu(\mathcal{L}) > 1$ as in Claim 3.3 below, we will show that for any $M \in \mathbb{R}^{n \times n}$ with operator norm $\|M\| < 1/(n\nu)$,

$$|\det(I_n + M)| \cdot |h(I_n + M) - g(I_n + M)| \leq C^* \|M\|^2 , \quad (9)$$

where $C^* := C^*(\mathcal{L}, f) > 0$ is independent of M . This implies Eq. (8) because the determinant is bounded away from zero in a neighborhood around I_n , so that $\lim_{M \rightarrow 0} \|M\|^2 / (\|M\| \cdot |\det(I_n + M)|) = 0$.

Let $A := I_n + M$. By the definition of the Voronoi cell, $\|\mathbf{x}\| = \text{dist}(\mathbf{x}, A\mathcal{L})$ if $\mathbf{x} \in \mathcal{V}(A\mathcal{L})$. Therefore,

$$\begin{aligned} |\det(A)| \cdot g(A) &= \int_{\mathcal{V}(A\mathcal{L})} f(\|\mathbf{x}\|^2) d\mathbf{x} \\ &= \int_{\mathcal{V}(A\mathcal{L})} f(\text{dist}(\mathbf{x}, A\mathcal{L})^2) d\mathbf{x} \\ &= \int_{A\mathcal{V}(\mathcal{L})} f(\text{dist}(\mathbf{x}, A\mathcal{L})^2) d\mathbf{x} , \end{aligned} \quad (10)$$

where the last equality uses the facts that (1) $A\mathcal{V}(\mathcal{L})$ is a fundamental domain of $A\mathcal{L}$ (i.e., Claim 2.7), and (2) the distance function $\mathbf{x} \mapsto \text{dist}(\mathbf{x}, A\mathcal{L})$ is periodic over $A\mathcal{L}$ so that the integral is the same over any fundamental domain.

Now, let $\widehat{\mathcal{V}} := (A\mathcal{V}(\mathcal{L})) \setminus \mathcal{V}(A\mathcal{L})$ be the set of points in $A\mathcal{V}(\mathcal{L})$ such that $\|\mathbf{x}\| \neq \text{dist}(\mathbf{x}, A\mathcal{L})$. Using Eq. (10), we see that the left-hand side of Eq. (9) is

$$\begin{aligned} \left| \int_{A\mathcal{V}(\mathcal{L})} (f(\|\mathbf{x}\|^2) - f(\text{dist}(\mathbf{x}, A\mathcal{L})^2)) d\mathbf{x} \right| &= \left| \int_{\widehat{\mathcal{V}}} (f(\|\mathbf{x}\|^2) - f(\text{dist}(\mathbf{x}, A\mathcal{L})^2)) d\mathbf{x} \right| \\ &\leq \text{vol}(\widehat{\mathcal{V}}) \cdot \max_{\mathbf{x} \in \widehat{\mathcal{V}}} |f(\|\mathbf{x}\|^2) - f(\text{dist}(\mathbf{x}, A\mathcal{L})^2)| . \end{aligned}$$

We complete the proof by arguing that $\text{vol}(\widehat{\mathcal{V}}) \leq C_0^* \|M\|$ and $\max_{\mathbf{x} \in \widehat{\mathcal{V}}} |f(\|\mathbf{x}\|^2) - f(\text{dist}(\mathbf{x}, A\mathcal{L})^2)| \leq C_1^* \|M\|$, where $C_0^* := C_0^*(\mathcal{L}) > 0$ and $C_1^* := C_1^*(\mathcal{L}, f) > 0$ are independent of M .

By Claim 3.3,

$$\widehat{\mathcal{V}} = (A\mathcal{V}(\mathcal{L})) \setminus \mathcal{V}(A\mathcal{L}) \subset ((1 + \nu\|M\|) \cdot \mathcal{V}(\mathcal{L})) \setminus ((1 - \nu\|M\|) \cdot \mathcal{V}(\mathcal{L})) ,$$

and therefore,

$$\begin{aligned} \text{vol}(\widehat{\mathcal{V}}) &\leq ((1 + \nu\|M\|)^n - (1 - \nu\|M\|)^n) \cdot \text{vol}(\mathcal{V}(\mathcal{L})) \\ &\leq 100n\nu \text{vol}(\mathcal{V}(\mathcal{L})) \cdot \|M\| , \end{aligned}$$

as desired, where we have used that $\|M\| < 1/(n\nu)$.

Next, notice that for $\mathbf{x} \in \widehat{\mathcal{V}} \subset A\mathcal{V}(\mathcal{L})$, we have, say, $\|\mathbf{x}\| \leq \|A\|\mu(\mathcal{L}) \leq 2\mu(\mathcal{L})$ and $\text{dist}(\mathbf{x}, A\mathcal{L}) \leq \|\mathbf{x}\| \leq 2\mu(\mathcal{L})$. Therefore,

$$\begin{aligned} |f(\|\mathbf{x}\|^2) - f(\text{dist}(\mathbf{x}, A\mathcal{L})^2)| &\leq \|\mathbf{x}\| - \text{dist}(\mathbf{x}, A\mathcal{L}) \cdot \max_{0 \leq r \leq 2\mu(\mathcal{L})} \left| \frac{d}{dr} f(r^2) \right| \\ &= 2\|\mathbf{x}\| - \text{dist}(\mathbf{x}, A\mathcal{L}) \cdot \max_{0 \leq r \leq 2\mu(\mathcal{L})} r|f'(r^2)| , \end{aligned} \quad (11)$$

where the inequality follows, e.g., from the fundamental theorem of calculus. Since f' is continuous by assumption, the maximum in Eq. (11) is well defined and finite. To complete the proof, let $\mathbf{x}' := (1 - \nu\|M\|)^2 \mathbf{x}$, which satisfies $\mathbf{x}' \in \mathcal{V}(A\mathcal{L})$ because

$$(1 - \nu\|M\|)^2 A\mathcal{V}(\mathcal{L}) \subset (1 + \nu\|M\|)(1 - \nu\|M\|)\mathcal{V}(A\mathcal{L}) \subset \mathcal{V}(A\mathcal{L})$$

where we used the right containment in Eq. (12) and the left containment in Eq. (13) of Claim 3.3 below. Then, by the triangle inequality,

$$\begin{aligned}
|\|\mathbf{x}\| - \text{dist}(\mathbf{x}, A\mathcal{L})| &\leq 2\|\mathbf{x} - \mathbf{x}'\| + |\|\mathbf{x}'\| - \text{dist}(\mathbf{x}', A\mathcal{L})| \\
&= 2\|\mathbf{x} - \mathbf{x}'\| \\
&\leq 4\nu\|\mathbf{x}\|\|M\| \\
&\leq 8\nu\mu(\mathcal{L})\|M\|.
\end{aligned}$$

Combining this with Eq. (11) shows that there exists a C_1^* of the desired form. \square

Claim 3.3. *For any lattice $\mathcal{L} \subset \mathbb{R}^n$ there exists $\nu = \nu(\mathcal{L}) > 1$ such that for all $M \in \mathbb{R}^{n \times n}$ with $\|M\| < 1/\nu$, we have*

$$(1 - \nu\|M\|) \cdot \mathcal{V}(\mathcal{L}) \subset A\mathcal{V}(\mathcal{L}) \subset (1 + \nu\|M\|) \cdot \mathcal{V}(\mathcal{L}), \quad (12)$$

and similarly,

$$(1 - \nu\|M\|) \cdot \mathcal{V}(\mathcal{L}) \subset \mathcal{V}(A\mathcal{L}) \subset (1 + \nu\|M\|) \cdot \mathcal{V}(\mathcal{L}), \quad (13)$$

where $A := I_n + M$.

Proof. We take $\nu := 20\mu(\mathcal{L})/\lambda_1(\mathcal{L})$ and notice that $\nu \geq 10$. Then, for any $\mathbf{x} \in \mathcal{V}(\mathcal{L}) \subset \mu(\mathcal{L})B_2^n$, we have $\|A\mathbf{x} - \mathbf{x}\| = \|M\mathbf{x}\| \leq \mu(\mathcal{L})\|M\|$. Since $(\lambda_1(\mathcal{L})/2) \cdot B_2^n \subset \mathcal{V}(\mathcal{L})$, we have

$$A\mathcal{V}(\mathcal{L}) \subset \mathcal{V}(\mathcal{L}) + \mu(\mathcal{L})\|M\|B_2^n \subset (1 + \nu\|M\|) \cdot \mathcal{V}(\mathcal{L}).$$

Similarly,

$$\mathcal{V}(\mathcal{L}) \subset A\mathcal{V}(\mathcal{L}) + \mu(\mathcal{L})\|M\|B_2^n \subset (1 - \nu\|M\|)^{-1} \cdot A\mathcal{V}(\mathcal{L}),$$

where the second inclusion uses the fact that, say, $(\lambda_1(\mathcal{L})/4) \cdot B_2^n \subset A\mathcal{V}(\mathcal{L})$ since $\|A^{-1}\| \leq 2$. This establishes Eq. (12).

Next, let $\mathbf{x} \in \mathcal{V}(\mathcal{L})$. Let $\alpha := 2 \max_{\mathbf{y} \in \mathcal{L} \setminus \{\mathbf{0}\}} \langle A\mathbf{y}, \mathbf{x} \rangle / \|A\mathbf{y}\|^2$. Equivalently, $\alpha > 0$ is minimal such that $\mathbf{x}/\alpha \in \mathcal{V}(A\mathcal{L})$. We claim that $\alpha \leq 1 + \nu\|M\|$, which implies that $(1 - \nu\|M\|) \cdot \mathcal{V}(\mathcal{L}) \subset \mathcal{V}(A\mathcal{L})$. Indeed, for non-zero $\mathbf{y} \in \mathcal{L}$, we have

$$\begin{aligned}
\frac{\langle A\mathbf{y}, \mathbf{x} \rangle}{\|A\mathbf{y}\|^2} &\leq \frac{\langle \mathbf{y}, \mathbf{x} \rangle + \langle M\mathbf{y}, \mathbf{x} \rangle}{(1 - \|M\|)^2 \|\mathbf{y}\|^2} \\
&\leq \frac{|\langle \mathbf{y}, \mathbf{x} \rangle|}{(1 - \|M\|)^2 \|\mathbf{y}\|^2} + \frac{\|M\|}{(1 - \|M\|)^2} \cdot \frac{\|\mathbf{x}\|}{\|\mathbf{y}\|} \\
&\leq \frac{|\langle \mathbf{y}, \mathbf{x} \rangle|}{(1 - \|M\|)^2 \|\mathbf{y}\|^2} + \frac{\|M\|}{(1 - \|M\|)^2} \cdot \frac{\|\mathbf{x}\|}{\lambda_1(\mathcal{L})}.
\end{aligned}$$

Since $\mathbf{x} \in \mathcal{V}(\mathcal{L})$, $|\langle \mathbf{y}, \mathbf{x} \rangle|/\|\mathbf{y}\|^2 \leq 1/2$ and $\|\mathbf{x}\| \leq \mu(\mathcal{L})$. Therefore,

$$\alpha \leq \frac{1}{(1 - \|M\|)^2} + \frac{2\|M\|}{(1 - \|M\|)^2} \cdot \frac{\mu(\mathcal{L})}{\lambda_1(\mathcal{L})} \leq 1 + \nu\|M\|,$$

as claimed.

Finally, we use a similar argument to prove that $\mathcal{V}(A\mathcal{L}) \subset (1 + \nu\|M\|) \cdot \mathcal{V}(\mathcal{L})$. In particular, for any $\mathbf{x} \in \mathcal{V}(A\mathcal{L})$ and non-zero $\mathbf{y} \in \mathcal{L}$, we have

$$\begin{aligned} \frac{\langle \mathbf{y}, \mathbf{x} \rangle}{\|\mathbf{y}\|^2} &\leq \frac{\langle A\mathbf{y}, \mathbf{x} \rangle}{\|\mathbf{y}\|^2} + \|M\| \cdot \frac{\|\mathbf{x}\|}{\|\mathbf{y}\|} \\ &\leq (1 + \|M\|)^2 \cdot \frac{\langle A\mathbf{y}, \mathbf{x} \rangle}{\|A\mathbf{y}\|^2} + \|M\| \cdot \frac{\mu(A\mathcal{L})}{\lambda_1(\mathcal{L})} \\ &\leq \frac{(1 + \|M\|)^2}{2} + \|M\| \cdot \frac{\mu(A\mathcal{L})}{\lambda_1(\mathcal{L})} \\ &\leq \frac{1 + \nu\|M\|}{2}, \end{aligned}$$

which implies the result. For this last inequality, we use the fact that, e.g., $\mu(A\mathcal{L}) \leq 2\mu(\mathcal{L})$ since

$$\mu(A\mathcal{L}) = \max_{\mathbf{x} \in \mathbb{R}^n} \min_{\mathbf{y} \in \mathcal{L}} \|A\mathbf{x} - A\mathbf{y}\| \leq \|A\| \cdot \max_{\mathbf{x} \in \mathbb{R}^n} \min_{\mathbf{y} \in \mathcal{L}} \|\mathbf{x} - \mathbf{y}\| \leq 2\mu(\mathcal{L}). \quad \square$$

4 Proof of the Reverse Minkowski Theorem

In this section, we prove our main theorem, Theorem 1.2. Recall that the Voronoi cell $\mathcal{V}(\mathcal{L})$ of a lattice $\mathcal{L} \subset \mathbb{R}^n$ is the symmetric polytope of all vectors in \mathbb{R}^n that are closer to $\mathbf{0}$ than to any other lattice vector,

$$\mathcal{V}(\mathcal{L}) := \{\mathbf{x} \in \mathbb{R}^n : \forall \mathbf{y} \in \mathcal{L}, \langle \mathbf{y}, \mathbf{x} \rangle \leq \|\mathbf{y}\|^2/2\}.$$

Also recall that for parameter $s > 0$, $\gamma_s(\cdot)$ is the Gaussian measure on \mathbb{R}^n given by

$$\gamma_s(S) := \int_{S/s} e^{-\pi\|\mathbf{x}\|^2} d\mathbf{x}$$

for any measurable set $S \subseteq \mathbb{R}^n$. (Some authors prefer to parametrize γ in terms of the standard deviation $\sigma := s/\sqrt{2\pi}$.) We omit the subscript when $s = 1$. We are interested in the Gaussian mass $\gamma_s(\mathcal{V}(\mathcal{L}))$ of the Voronoi cell because, as the following lemma due to Chung, Dadush, Liu, and Peikert shows, this can be used to obtain an upper bound on the mass $\rho_s(\mathcal{L})$ of the lattice itself [CDLP13]. We include a proof for completeness.

Lemma 4.1 ([CDLP13, Lemma 3.4]). *For any lattice $\mathcal{L} \subset \mathbb{R}^n$ and $s > 0$,*

$$\rho_s(\mathcal{L}) \cdot \gamma_s(\mathcal{V}(\mathcal{L})) \leq 1.$$

Proof. By scaling appropriately, we may assume without loss of generality that $s = 1$. Note that the Voronoi cell tiles space with respect to \mathcal{L} . I.e., $\bigcup_{\mathbf{y} \in \mathcal{L}} (\mathcal{V}(\mathcal{L}) + \mathbf{y}) = \mathbb{R}^n$, where the union is

disjoint except on a measure-zero set. So,

$$\begin{aligned}
1 &= \int_{\mathbb{R}^n} e^{-\pi\|\mathbf{x}\|^2} d\mathbf{x} \\
&= \sum_{\mathbf{y} \in \mathcal{L}} \int_{\mathcal{V}(\mathcal{L})} e^{-\pi\|\mathbf{y}+\mathbf{t}\|^2} d\mathbf{t} \\
&= \sum_{\mathbf{y} \in \mathcal{L}} e^{-\pi\|\mathbf{y}\|^2} \int_{\mathcal{V}(\mathcal{L})} e^{-\pi\|\mathbf{t}\|^2} e^{2\pi\langle \mathbf{y}, \mathbf{t} \rangle} d\mathbf{t} \\
&= \sum_{\mathbf{y} \in \mathcal{L}} \rho(\mathbf{y}) \int_{\mathcal{V}(\mathcal{L})} e^{-\pi\|\mathbf{t}\|^2} \cosh(2\pi\langle \mathbf{y}, \mathbf{t} \rangle) d\mathbf{t} \\
&\geq \sum_{\mathbf{y} \in \mathcal{L}} \rho(\mathbf{y}) \int_{\mathcal{V}(\mathcal{L})} e^{-\pi\|\mathbf{t}\|^2} d\mathbf{t} \\
&= \rho(\mathcal{L}) \gamma(\mathcal{V}(\mathcal{L})) ,
\end{aligned}$$

where the fourth line follows from the fact that the Voronoi cell is symmetric. \square

Therefore, in order to prove Theorem 1.2, it suffices to show that $\gamma_{1/t}(\mathcal{V}(\mathcal{L})) \geq 2/3$ for every lattice $\mathcal{L} \subset \mathbb{R}^n$ with $\det(\mathcal{L}') \geq 1$ for all sublattices $\mathcal{L}' \subseteq \mathcal{L}$, where $t := 10(\log n + 2)$. As we explained in the introduction, we will reduce this to studying local minima of the function $\mathcal{L} \mapsto \gamma_{1/t}(\mathcal{V}(\mathcal{L}))$ over the set of determinant-one lattices. (We do not know whether such local minima actually exist.)

In Section 4.1, we collect some (mostly known) facts about the Gaussian mass of convex bodies. The statements of Theorem 4.2 and Lemma 4.11 are the only parts of Section 4.1 that will be used later on. In particular, in Section 4.2, we apply these two facts to prove Theorem 1.2.

4.1 Gaussian mass of convex bodies

We say that a measurable set $U \subset \mathbb{R}^n$ is in *isotropic Gaussian position* for parameter s if

$$\int_{U/s} e^{-\pi\|\mathbf{x}\|^2} \mathbf{x}\mathbf{x}^T d\mathbf{x} = \alpha \cdot I_n$$

for some scalar $\alpha > 0$. If $s = 1$, we simply say that U is in *isotropic Gaussian position*. Such a position has been considered elsewhere (e.g., [Bob11]), but as far as we know, it did not previously have a name.

The main goal of this section is to prove the following theorem. We will also include a standard fact in Lemma 4.11 towards the end of this section.

Theorem 4.2. *For any symmetric convex body $K \subset \mathbb{R}^n$ with $\text{vol}(K) \geq 1$, if K is in isotropic Gaussian position for some parameter $0 < s \leq 1/t$, then $\gamma_s(K) \geq 2/3$ where $t := 10(\log n + 2)$.*

Our proof of Theorem 4.2 proceeds in two parts. The first part is a result due to Bobkov [Bob11] (Proposition 4.3 below), showing that an isotropic Gaussian position of a convex body has maximal Gaussian mass. We include a proof for completeness. In the second part (Theorem 4.6 below), we show that any volume-one convex body $K \subset \mathbb{R}^n$ has a position such that $\gamma_s(K) \geq 2/3$.

Proposition 4.3 ([Bob11, Proposition 3.1]). *For any symmetric convex body $K \subset \mathbb{R}^n$, if K is in isotropic Gaussian position for some parameter $s > 0$, then $\gamma_s(K) \geq \gamma_s(AK)$ for any determinant-one matrix $A \in \text{SL}_n(\mathbb{R})$.*

We start by observing that isotropic Gaussian positions correspond to critical points of the Gaussian mass function over positions.

Fact 4.4. *For any measurable set $U \subset \mathbb{R}^n$, let*

$$h(A) := \frac{\gamma(AU)}{|\det(A)|},$$

where $A \in \mathbb{R}^{n \times n}$ is a non-singular matrix. Then,

$$\nabla_A h(A)|_{A=I_n} = -2\pi \int_U e^{-\pi\|\mathbf{x}\|^2} \mathbf{x}\mathbf{x}^T d\mathbf{x}.$$

In particular, $A \mapsto \gamma(AU)$ has a critical point at I_n when restricted to determinant-one matrices if and only if U is in isotropic Gaussian position.

Proof. Simply apply Claim 3.2 with $f(x) = e^{-\pi x}$ and notice that a differentiable function $h : \mathbb{R}^{n \times n} \rightarrow \mathbb{R}$ has a critical point at I_n when restricted to the set of determinant-one matrices if and only if its gradient is proportional to the identity. This follows from the fact that the tangent space to the set of determinant-one matrices at I_n is the space orthogonal to the identity. \square

We will also need the following result due to Cordero-Erausquin, Fradelizi, and Maurey [CFM04], which is related to the so-called (B) conjecture due to Banaszczyk (see [Lat02]).

Theorem 4.5 ([CFM04]). *For any symmetric convex body $K \subset \mathbb{R}^n$, the function $\gamma(e^M K)$, where $M \in \mathbb{R}^{n \times n}$ ranges over all diagonal matrices, is log-concave.*

Proof of Proposition 4.3. By scaling K , we may assume that $s = 1$. Let $A = UDV$ be the singular-value decomposition of A . (I.e., D is a diagonal matrix with non-negative entries along the diagonal and U and V are orthogonal matrices.) Since D has determinant one, we may write $D = e^{D'}$ for a diagonal matrix D' with trace zero.

Note that the Gaussian measure is invariant under orthogonal transformations, so that $\gamma(AK) = \gamma(UDVK) = \gamma(DVK)$. Let $K' := VK$, and note that $\gamma(K') = \gamma(K)$ and that K' is in isotropic Gaussian position, since V is an orthogonal transformation.

Let $\hat{h}(M) := \gamma(e^M K')/|\det(e^M)|$. By Fact 4.4 and the chain rule, we have

$$\nabla_M \hat{h}(M)|_{M=0} = -2\pi \int_{K'} e^{-\pi\|\mathbf{x}\|^2} \mathbf{x}\mathbf{x}^T d\mathbf{x} = -\alpha \cdot I_n$$

for some scalar $\alpha \in \mathbb{R}$, where the second equality is simply the fact that K' is in isotropic Gaussian position. Let $X \subset \mathbb{R}^{n \times n}$ be the set of trace-zero diagonal matrices. Then, the function \hat{h}_X obtained by restricting \hat{h} to X has a critical point at zero, since $\text{Tr}(I_n M) = 0$ for any $M \in X$. By Theorem 4.5, \hat{h}_X is log-concave, so that this critical point must be a global maximum. Therefore,

$$\gamma(AK) = \gamma(DK') = \gamma(e^{D'} K') \leq \gamma(K') = \gamma(K),$$

as needed. \square

We now proceed to the second part of the proof of Theorem 4.2. Namely, we prove the following.

Theorem 4.6. *For any symmetric convex body $K \subset \mathbb{R}^n$ with volume one, there is a determinant-one matrix $A \in \text{SL}_n(\mathbb{R})$ such that $\gamma_{1/t}(AK) \geq 2/3$, where $t := 2\sqrt{3e}(\log_2 n + 2) < 10(\log n + 2)$.*

The proof is based on an important theorem that follows from the work of Figiel and Tomczak-Jaegermann [FT79], Lewis [Lew79], and Pisier [Pis82]. We first need some definitions. Recall that any symmetric convex body $K \subset \mathbb{R}^n$ defines a norm $\|\cdot\|_K$ given by

$$\|\mathbf{x}\|_K := \inf\{s \geq 0 : \mathbf{x} \in sK\}.$$

We then define the ℓ -norm on $\mathbb{R}^{n \times n}$ by

$$\ell_K(A) := \left(\int_{\mathbb{R}^n} \|A\mathbf{x}\|_K^2 d\gamma(\mathbf{x}) \right)^{1/2},$$

where $d\gamma(\mathbf{x}) := e^{-\pi\|\mathbf{x}\|^2} d\mathbf{x}$. Finally, we recall that the *polar body* of a symmetric convex body K is given by

$$K^\circ := \{\mathbf{x} \in \mathbb{R}^n : \forall \mathbf{y} \in K, \langle \mathbf{y}, \mathbf{x} \rangle \leq 1\},$$

which is itself a convex body.

Theorem 4.7 ([FT79, Lew79, Pis82]; see [Dad12b, Theorem 4.4.3]). *For any symmetric convex body $K \subset \mathbb{R}^n$, there exists a determinant-one matrix $A \in \text{SL}_n(\mathbb{R})$ such that*

$$\ell_K(A) \ell_{K^\circ}((A^T)^{-1}) \leq n(\log_2 n + 2)/\pi.$$

Lemma 4.8. *For any symmetric convex body $K \subset \mathbb{R}^n$ with volume one and any determinant-one matrix $A \in \text{SL}_n(\mathbb{R})$, we have*

$$\ell_{K^\circ}((A^T)^{-1}) \geq \sqrt{n/(2\pi)} \cdot r_n > n/(2\pi\sqrt{e}).$$

where $r_n := \text{vol}(B_2^n)^{-1/n} > \sqrt{n/(2\pi e)}$ is the radius such that $\text{vol}(r_n B_2^n) = 1$.

Proof. Since $\ell_{K^\circ}((A^T)^{-1}) = \ell_{A^T K^\circ}(I_n) = \ell_{(A^{-1}K)^\circ}(I_n)$, and using that $A^{-1}K$ is also a symmetric convex body of volume one, it suffices to prove the case $A = I_n$ in the statement. Unpacking the definitions, we see that

$$\begin{aligned} \ell_{K^\circ}(I_n)^2 &= \int_{\mathbb{R}^n} \|\mathbf{x}\|_{K^\circ}^2 d\gamma(\mathbf{x}) \\ &= \int_{\mathbb{R}^n} \sup_{\mathbf{y} \in K} \langle \mathbf{y}, \mathbf{x} \rangle^2 d\gamma(\mathbf{x}) \\ &= \left(\int_{\mathbb{R}^n} \|\mathbf{x}\|^2 d\gamma(\mathbf{x}) \right) \cdot \left(\int_{\mathbb{R}^n} \sup_{\mathbf{y} \in K} \frac{\langle \mathbf{y}, \mathbf{x} \rangle^2}{\|\mathbf{x}\|^2} d\gamma(\mathbf{x}) \right) \\ &= \frac{n}{2\pi} \cdot \int_{\mathbb{R}^n} \sup_{\mathbf{y} \in K} \frac{\langle \mathbf{y}, \mathbf{x} \rangle^2}{\|\mathbf{x}\|^2} d\gamma(\mathbf{x}), \end{aligned} \tag{14}$$

where in the third equality we use integration in polar coordinates. By Jensen's inequality, we have

$$\int_{\mathbb{R}^n} \sup_{\mathbf{y} \in K} \frac{\langle \mathbf{y}, \mathbf{x} \rangle^2}{\|\mathbf{x}\|^2} d\gamma(\mathbf{x}) \geq \left(\int_{\mathbb{R}^n} \sup_{\mathbf{y} \in K} \frac{\langle \mathbf{y}, \mathbf{x} \rangle}{\|\mathbf{x}\|} d\gamma(\mathbf{x}) \right)^2, \tag{15}$$

and by Urysohn's inequality (see [AGM15, Theorem 1.5.11]), we have

$$\int_{\mathbb{R}^n} \sup_{\mathbf{y} \in K} \frac{\langle \mathbf{y}, \mathbf{x} \rangle}{\|\mathbf{x}\|} d\gamma(\mathbf{x}) \geq r_n. \quad (16)$$

The result follows by combining Eqs. (14), (15), and (16). \square

The following corollary is an immediate consequence of the previous two results.

Corollary 4.9. *For any symmetric convex body $K \subset \mathbb{R}^n$ with volume one, there exists a determinant-one matrix $A \in \text{SL}_n(\mathbb{R})$ such that $\ell_K(A) \leq 2\sqrt{e}(\log_2 n + 2)$.*

Proof of Theorem 4.6. By Corollary 4.9, there exists an $A \in \text{SL}_n(\mathbb{R})$ such that

$$\ell_K(A)^2 = \int_{\mathbb{R}^n} \|A\mathbf{x}\|_K^2 d\gamma(\mathbf{x}) \leq (2\sqrt{e}(\log_2 n + 2))^2.$$

We will use A^{-1} as our matrix. Note that

$$\gamma_{1/t}(A^{-1}K) = \int_{\mathbb{R}^n} 1_{\|\mathbf{x}\|_{A^{-1}K} \leq t} d\gamma(\mathbf{x}) = \int_{\mathbb{R}^n} 1_{\|A\mathbf{x}\|_K \leq t} d\gamma(\mathbf{x}) = 1 - \int_{\mathbb{R}^n} 1_{\|A\mathbf{x}\|_K > t} d\gamma(\mathbf{x}).$$

The result then follows by Markov's inequality, which tells us that

$$\int_{\mathbb{R}^n} 1_{\|A\mathbf{x}\|_K > t} d\gamma(\mathbf{x}) \leq \frac{1}{t^2} \cdot \int_{\mathbb{R}^n} \|A\mathbf{x}\|_K^2 d\gamma(\mathbf{x}) \leq \frac{1}{t^2} \cdot (2\sqrt{e}(\log_2 n + 2))^2 = \frac{1}{3}. \quad \square$$

We now obtain Theorem 4.2 as an immediate corollary of Proposition 4.3 and Theorem 4.6.

Proof of Theorem 4.2. By Theorem 4.6 and the monotonicity of $\gamma_s(AK)$ in s , there is some $A \in \text{SL}_n(\mathbb{R})$ such that $\gamma_s(AK) \geq 2/3$. By Proposition 4.3, $\gamma_s(K) \geq \gamma_s(AK) \geq 2/3$, as needed. \square

Concentration of measure. We will also need a standard lemma about the concentration of Gaussian measure. We first recall the Gaussian isoperimetric inequality [ST74, Bor75] (see also [AGM15, Theorem 3.1.9]).

Theorem 4.10 (Gaussian isoperimetric inequality). *For any measurable set $U \subset \mathbb{R}^n$ and any $\tau > 0$,*

$$\gamma(U + \tau B_2^n) \geq \int_{-\infty}^{\sigma + \tau} e^{-\pi x^2} dx,$$

where $\sigma \in [-\infty, \infty]$ is such that $\int_{-\infty}^{\sigma} e^{-\pi x^2} dx = \gamma(U)$.

Recall that the *inradius* of a convex body K is defined as $\max\{r \geq 0 : rB_2^n \subseteq K\}$, i.e., the radius of the largest ball contained in the body.

Lemma 4.11. *If $K \subset \mathbb{R}^n$ is a convex body with $\gamma_{1/t}(K) \geq 2/3$ for some $t > 0$, then*

$$\gamma_{1/(t+\tau)}(K) \geq 1 - e^{-\pi r^2 \tau^2} / 3,$$

for any $\tau \geq 0$, where $r \geq 0$ is the inradius of K .

Proof. Note that

$$\gamma_{1/(t+\tau)}(K) = \gamma((t+\tau)K) \geq \gamma(tK + r\tau B_2^n),$$

since by definition $rB_2^n \subseteq K$. Applying Theorem 4.10, we have

$$\gamma_{1/(t+\tau)}(K) \geq \int_{-\infty}^{\sigma+r\tau} e^{-\pi x^2} dx,$$

where $\sigma > 0$ is such that $\int_{-\infty}^{\sigma} e^{-\pi x^2} dx = 2/3$. Finally, we note that

$$\int_{-\infty}^{\sigma+r\tau} e^{-\pi x^2} dx = 1 - \int_{\sigma+r\tau}^{\infty} e^{-\pi x^2} dx \geq 1 - e^{-\pi r^2 \tau^2} \int_{\sigma}^{\infty} e^{-\pi x^2} dx = 1 - e^{-\pi r^2 \tau^2} / 3,$$

where the inequality follows from the fact that σ , τ , and r are non-negative, so that $(x + r\tau)^2 \geq x^2 + r^2 \tau^2$ for all $x \geq \sigma$. The result follows. \square

4.2 Proof of Theorem 1.2

We now use Theorem 3.1 and Theorem 4.2 to characterize local minima of $\gamma_s(\mathcal{V}(\mathcal{L}))$.

Theorem 4.12. *If $\mathcal{L} \subset \mathbb{R}^n$ corresponds to a local minimum (or maximum) of $\gamma_{1/t}(\mathcal{V}(\mathcal{L}))$ over the set of determinant-one lattices, then $\mathcal{V}(\mathcal{L})$ is in isotropic Gaussian position with parameter $1/t$, and*

$$\gamma_{1/t}(\mathcal{V}(\mathcal{L})) \geq 2/3,$$

where $t := 10(\log n + 2)$.

Proof. By Theorem 3.1 with $f(x) = t^n \cdot e^{-\pi t^2 x}$, we have

$$\begin{aligned} \nabla_A(\gamma_{1/t}(\mathcal{V}(A\mathcal{L}))/|\det(A)|)|_{A=I_n} &= 2 \int_{\mathcal{V}(\mathcal{L})} f'(\|\mathbf{x}\|^2) \mathbf{x} \mathbf{x}^T d\mathbf{x} \\ &= -2\pi t^{n+2} \cdot \int_{\mathcal{V}(\mathcal{L})} e^{-\pi t^2 \|\mathbf{x}\|^2} \mathbf{x} \mathbf{x}^T d\mathbf{x}. \end{aligned}$$

Recall that I_n corresponds to a local extremum of a differentiable function $g(A)$ restricted to the manifold of determinant-one matrices only if $\nabla_A g(A)|_{A=I_n}$ is a scalar multiple of the identity. So, the above expression must be a multiple of the identity. I.e., $\mathcal{V}(\mathcal{L})$ is in isotropic Gaussian position. The result then follows from Theorem 4.2. \square

Before moving to the proof of our main theorem, we need the following claim.

Claim 4.13. *For any $x > 1$,*

$$e^{-2\log^2 x} + e^{-2\log^2(x/(x-1))} < 1.$$

Proof. By symmetry, we may assume that $x \geq 2$. (Otherwise, we can replace x with $x/(x-1)$.) If $2 \leq x \leq 2.5$, then

$$e^{-2\log^2 x} + e^{-2\log^2(x/(x-1))} < e^{-2\log^2 2} + e^{-2\log^2(5/3)} < 1.$$

A similar computation works if $2.5 \leq x \leq e$. Finally, using the fact that $\log(x/(x-1)) = -\log(1 - 1/x) > 1/x$ for $x > 1$, we have for any $x \geq e$ that

$$e^{-2\log^2 x} + e^{-2\log^2(x/(x-1))} < \frac{1}{x^2} + e^{-2/x^2} < \frac{1}{x^2} + 1 - \frac{1}{x^2} = 1. \quad \square$$

We now prove our main theorem in the special case when \mathcal{L} is a stable lattice. The full result will follow as a relatively straightforward corollary.

Proposition 4.14. *For any stable lattice $\mathcal{L} \subset \mathbb{R}^n$, $\rho_{1/t}(\mathcal{L}) \leq \frac{3}{2}$, where $t := 10(\log n + 2)$.*

Proof. By Lemma 4.1, it suffices to show that $\gamma_{1/t}(\mathcal{V}(\mathcal{L})) \geq 2/3$. We assume for induction that $\gamma_{1/(10(\log d + 2))}(\mathcal{V}(\mathcal{L}')) \geq 2/3$ for any stable lattice \mathcal{L}' of rank $d < n$. (A quick check shows that this is true for $d = 1$.) Since the set of stable lattices is compact by Item (ii) of Proposition 2.5 and the function $\gamma_{1/t}(\mathcal{V}(\mathcal{L}))$ is continuous, we may assume without loss of generality that \mathcal{L} corresponds to a global minimum of $\gamma_{1/t}(\mathcal{V}(\mathcal{L}))$ over the set of stable lattices. If this global minimum is also a *local* minimum over the set of determinant-one lattices, then by Theorem 4.12, $\gamma_{1/t}(\mathcal{V}(\mathcal{L})) \geq 2/3$, and we are done.

Otherwise, \mathcal{L} lies on the boundary of the set of stable lattices. I.e., there is some primitive sublattice $\mathcal{L}' \subset \mathcal{L}$ of rank $d < n$ such that \mathcal{L}' and \mathcal{L}/\mathcal{L}' are stable. (See Item (iv) of Proposition 2.5.) By Corollary 2.9 (applied to the non-decreasing function $x \mapsto -e^{-\pi(tx)^2}$) together with Claim 2.6, we have

$$\gamma_{1/t}(\mathcal{V}(\mathcal{L})) \geq \gamma_{1/t}(\mathcal{V}(\mathcal{L}/\mathcal{L}' \oplus \mathcal{L}')) = \gamma_{1/t}(\mathcal{V}(\mathcal{L}/\mathcal{L}')) \cdot \gamma_{1/t}(\mathcal{V}(\mathcal{L}')). \quad (17)$$

Let $t_1 := 10(\log d + 2)$ and $t_2 := 10(\log(n - d) + 2)$. By the induction hypothesis, we see that $\gamma_{1/t_1}(\mathcal{V}(\mathcal{L}')) \geq 2/3$ and $\gamma_{1/t_2}(\mathcal{V}(\mathcal{L}/\mathcal{L}')) \geq 2/3$. By Lemma 4.11, we therefore have

$$\gamma_{1/t}(\mathcal{V}(\mathcal{L}')) \geq 1 - \frac{1}{3} \cdot e^{-2 \log^2(n/d)}, \text{ and } \gamma_{1/t}(\mathcal{V}(\mathcal{L}/\mathcal{L}')) \geq 1 - \frac{1}{3} \cdot e^{-2 \log^2(n/(n-d))},$$

where we have used the fact that the inradius of the Voronoi cell, which is equal to half the length of the shortest nonzero vector, is at least $1/2$ for stable lattices (and the constant in the exponent is very loose). Therefore, using (17),

$$\begin{aligned} \gamma_{1/t}(\mathcal{V}(\mathcal{L})) &\geq \left(1 - \frac{1}{3} \cdot e^{-2 \log^2(n/d)}\right) \cdot \left(1 - \frac{1}{3} \cdot e^{-2 \log^2(n/(n-d))}\right) \\ &> 1 - \frac{1}{3} \cdot (e^{-2 \log^2(n/d)} + e^{-2 \log^2(n/(n-d))}) \\ &> \frac{2}{3}, \end{aligned}$$

where the last inequality follows from Claim 4.13 with $x := n/d$.

So, for every stable lattice \mathcal{L} , we have $\gamma_{1/t}(\mathcal{V}(\mathcal{L})) \geq 2/3$, and the result then follows from Lemma 4.1. \square

We now derive our main theorem as a corollary.

Proof of Theorem 1.2. Let $\{\mathbf{0}\} = \mathcal{L}_0 \subset \dots \subset \mathcal{L}_k = \mathcal{L}$ be the canonical filtration of \mathcal{L} . Recall from Item 2 of Proposition 2.5 that for $1 \leq i \leq k$, $\alpha_i \cdot (\mathcal{L}_i/\mathcal{L}_{i-1})$ is a stable lattice, where $\alpha_i := \det(\mathcal{L}_i/\mathcal{L}_{i-1})^{-1/\text{rank}(\mathcal{L}_i/\mathcal{L}_{i-1})}$. Moreover, $\alpha_1 = \det(\mathcal{L}_1)^{-1/\text{rank}(\mathcal{L}_1)} \leq 1$ by our assumption on \mathcal{L} . By Item 3 of Proposition 2.5, α_i is non-increasing with i , implying that $\alpha_i \leq 1$ for $1 \leq i \leq k$. Therefore, by Lemma 2.3,

$$\rho_{1/t}(\mathcal{L}) \leq \rho_{1/t}\left(\bigoplus_{i=1}^k \mathcal{L}_i/\mathcal{L}_{i-1}\right) \leq \rho_{1/t}\left(\bigoplus_{i=1}^k \alpha_i \cdot (\mathcal{L}_i/\mathcal{L}_{i-1})\right).$$

By Item (iii) of Proposition 2.5, this direct sum of stable lattices is itself a stable lattice. The result then follows from Proposition 4.14. \square

5 Bounds on $\rho_s(\mathcal{L})$ for all parameters and point-counting bounds

We first give the proof of Corollary 1.4, which follows immediately from Theorem 1.3.

Proof of Corollary 1.4. For any $r > 0$

$$|\mathcal{L} \cap (rB_2^n + \mathbf{u})| \leq e^{\pi r^2/s^2} \rho_s(\mathcal{L} - \mathbf{u}) \leq e^{\pi r^2/s^2} \rho_s(\mathcal{L}) ,$$

where the last inequality is Claim 2.2. Item 1 then follows by plugging in $s = 1/t$ and applying Item 1 of Theorem 1.3. Item 2 follows by taking $s = r\sqrt{2\pi/n}$ and applying Item 2 of Theorem 1.3. Finally, Item 3 follows by taking $s = r\sqrt{2\pi/n}$ and applying Item 3 of Theorem 1.3. \square

We now prove Theorem 1.3, which gives bounds on the Gaussian mass for all parameters. We start with Item 1, addressing parameters $s \leq 1/t$.

Theorem 5.1 (Slight strengthening of Item 1 of Theorem 1.3). *For any lattice $\mathcal{L} \subset \mathbb{R}^n$ with $\det(\mathcal{L}') \geq 1$ for all sublattices $\mathcal{L}' \subseteq \mathcal{L}$,*

$$\rho_s(\mathcal{L}) \leq 1 + e^{-\pi \lambda_1(\mathcal{L})^2(1/s^2 - t^2)}/2 \leq 1 + e^{-\pi(1/s^2 - t^2)}/2$$

for any $s \leq 1/t$, where $t := 10(\log n + 2)$.

Proof. Note that for any $\mathbf{y} \in \mathcal{L} \setminus \{\mathbf{0}\}$,

$$\rho_s(\mathbf{y}) = \rho_{1/t}(\mathbf{y}) \cdot e^{-\pi \|\mathbf{y}\|^2(1/s^2 - t^2)} \leq \rho_{1/t}(\mathbf{y}) e^{-\pi \lambda_1(\mathcal{L})^2(1/s^2 - t^2)} .$$

The result follows by summing over all $\mathbf{y} \in \mathcal{L} \setminus \{\mathbf{0}\}$ and applying Theorem 1.2. The second inequality uses the fact that $\lambda_1(\mathcal{L}) \geq 1$. \square

We now prove the “high-parameter analogue” of Theorem 1.2. The proof uses Theorem 1.2 and duality.

Theorem 5.2 (Item 3 of Theorem 1.3). *For any lattice $\mathcal{L} \subset \mathbb{R}^n$ with $\det(\mathcal{L}') \geq 1$ for all sublattices $\mathcal{L}' \subseteq \mathcal{L}$ and any parameter $s \geq t$, $\rho_s(\mathcal{L}) \leq 2s^n$ where $t := 10(\log n + 2)$.*

Proof. Recall the Poisson Summation Formula applied to the Gaussian mass (Eq. (5)):

$$\rho_s(\mathcal{L}) = \frac{s^n}{\det(\mathcal{L})} \cdot \rho_{1/s}(\mathcal{L}^*) .$$

Assume first that \mathcal{L} is stable. Then, by Theorem 1.2 and the fact that the dual of a stable lattice is stable (Item (i) of Proposition 2.5),

$$\rho_s(\mathcal{L}) = s^n \cdot \rho_{1/s}(\mathcal{L}^*) \leq s^n \cdot \rho_{1/t}(\mathcal{L}^*) \leq 2s^n .$$

For a general lattice $\mathcal{L} \subset \mathbb{R}^n$, let $\{\mathbf{0}\} = \mathcal{L}_0 \subset \mathcal{L}_1 \subset \dots \subset \mathcal{L}_k = \mathcal{L}$ be the canonical filtration of \mathcal{L} . Recall from Item 2 that $\alpha_i \cdot (\mathcal{L}_i/\mathcal{L}_{i-1})$ is stable for some α_i . Furthermore, by Item 3 of Proposition 2.5, $\alpha_i \leq 1$. Then, by Lemma 2.3,

$$\rho_s(\mathcal{L}) \leq \rho_s\left(\bigoplus \mathcal{L}_i/\mathcal{L}_{i-1}\right) \leq \rho_s\left(\bigoplus \alpha_i \cdot \mathcal{L}_i/\mathcal{L}_{i-1}\right) \leq 2s^n ,$$

where the last inequality follows from the fact that the direct sum of stable lattices is stable together with the bound proven above for stable lattices. (See Item (iii) of Proposition 2.5.) \square

The rest of this section is dedicated to the proof of Item 2 of Theorem 1.3. Note that we already have a bound on $\rho_s(\mathcal{L})$ for $s \leq 1/t$ and for $s \geq t$, but we currently have no non-trivial bound for intermediate parameters $1/t < s < t$. To remedy this, we show in Theorem 5.5 below that $\rho_{e^\sigma}(\mathcal{L})$ is “approximately log-convex,” which allows us to interpolate between these two bounds. In the proof of Theorem 5.5, we are unable to work with $\rho_{e^\sigma}(\mathcal{L})$ directly, so we instead show that it can be approximated by $\gamma_{e^\sigma}(\mathcal{V}(\mathcal{L}))$ (Lemma 5.4). We then notice that the latter function is log-concave by Theorem 4.5.

Claim 5.3. *For any lattice $\mathcal{L} \subset \mathbb{R}^n$, $\mathbf{y} \in \mathcal{L}$, and $s > 0$,*

$$\rho_s(\mathbf{y})\gamma_s(\mathcal{V}(\mathcal{L})) \leq \gamma_s(\mathcal{V}(\mathcal{L}) + \mathbf{y}) \leq \gamma_s(\mathcal{V}(\mathcal{L}))$$

Proof. By scaling appropriately, we may assume that $s = 1$. We have

$$\begin{aligned} \gamma(\mathcal{V}(\mathcal{L}) + \mathbf{y}) &= \int_{\mathcal{V}(\mathcal{L})} e^{-\pi\|\mathbf{x}+\mathbf{y}\|^2} d\mathbf{x} \\ &= \rho(\mathbf{y}) \int_{\mathcal{V}(\mathcal{L})} \rho(\mathbf{x}) e^{-2\pi\langle \mathbf{y}, \mathbf{x} \rangle} d\mathbf{x} \\ &= \rho(\mathbf{y}) \int_{\mathcal{V}(\mathcal{L})} \rho(\mathbf{x}) \cosh(2\pi\langle \mathbf{y}, \mathbf{x} \rangle) d\mathbf{x} , \end{aligned}$$

where we have used the symmetry of the Voronoi cell in the last line. The lower bound now follows from noting that $\cosh(2\pi\langle \mathbf{x}, \mathbf{y} \rangle) \geq 1$. For the upper bound, we recall that, by definition, any vector in the Voronoi cell $\mathbf{x} \in \mathcal{V}(\mathcal{L})$ satisfies $\langle \mathbf{y}, \mathbf{x} \rangle \leq \|\mathbf{y}\|^2/2$ for any lattice vector $\mathbf{y} \in \mathcal{L}$. Therefore, $\cosh(2\pi\langle \mathbf{y}, \mathbf{x} \rangle) \leq \cosh(\pi\|\mathbf{y}\|^2) \leq 1/\rho(\mathbf{y})$, as needed. \square

Lemma 5.4. *For any lattice $\mathcal{L} \subset \mathbb{R}^n$ and any $s > 0$,*

$$e^{-4n}/2 \leq \gamma_s(\mathcal{V}(\mathcal{L}))\rho_s(\mathcal{L}) \leq 1 .$$

Proof. The upper bound is Lemma 4.1, repeated for comparison. By scaling appropriately, we may assume that $s = 1$. Recall that $\int_{\mathbb{R}^n} \|\mathbf{x}\|^2 e^{-\pi\|\mathbf{x}\|^2} d\mathbf{x} = n/(2\pi)$. It follows from Markov’s inequality that $\int_{\sqrt{n/\pi}B_2^n} e^{-\pi\|\mathbf{x}\|^2} d\mathbf{x} \geq 1/2$. Let

$$Y := \{\mathbf{y} \in \mathcal{L} : (\mathcal{V}(\mathcal{L}) + \mathbf{y}) \cap \sqrt{n/\pi}B_2^n \neq \emptyset\} .$$

I.e., Y is the set of vectors $\mathbf{y} \in \mathcal{L}$ such that there exists some $\mathbf{x} \in \sqrt{n/\pi}B_2^n$ with $\|\mathbf{y} - \mathbf{x}\| \leq \|\mathbf{y}' - \mathbf{x}\|$ for every $\mathbf{y}' \in \mathcal{L}$. By taking $\mathbf{y}' = \mathbf{0}$, we immediately see that $Y \subseteq \mathcal{L} \cap 2\sqrt{n/\pi}B_2^n$. Recalling that the Voronoi cell tiles space, we have

$$\begin{aligned} 1/2 &\leq \int_{\sqrt{n/\pi}B_2^n} e^{-\pi\|\mathbf{x}\|^2} d\mathbf{x} \\ &\leq \sum_{\mathbf{y} \in Y} \gamma(\mathcal{V}(\mathcal{L}) + \mathbf{y}) \\ &\leq |Y| \cdot \gamma(\mathcal{V}(\mathcal{L})) && \text{(Claim 5.3)} \\ &\leq |\mathcal{L} \cap 2\sqrt{n/\pi}B_2^n| \cdot \gamma(\mathcal{V}(\mathcal{L})) \\ &\leq e^{4n} \rho(\mathcal{L}) \gamma(\mathcal{V}(\mathcal{L})) , \end{aligned}$$

as needed. \square

We now prove the “approximate log-convexity” of $\rho_{e^\sigma}(\mathcal{L})$.

Theorem 5.5. *For any lattice $\mathcal{L} \subset \mathbb{R}^n$ and any $t_1 > s > t_2 > 0$,*

$$\rho_s(\mathcal{L}) \leq 2e^{4n} \rho_{t_1}(\mathcal{L})^\tau \rho_{t_2}(\mathcal{L})^{1-\tau} ,$$

where $\tau := \log(s/t_2)/\log(t_1/t_2)$.

Proof. We have

$$\rho_s(\mathcal{L}) \leq \frac{1}{\gamma_s(\mathcal{V}(\mathcal{L}))} \quad (\text{Lemma 4.1})$$

$$\leq \frac{1}{\gamma_{t_1}(\mathcal{V}(\mathcal{L}))^\tau \gamma_{t_2}(\mathcal{V}(\mathcal{L}))^{1-\tau}} \quad (\text{Theorem 4.5})$$

$$\leq 2e^{4n} \rho_{t_1}(\mathcal{L})^\tau \rho_{t_2}(\mathcal{L})^{1-\tau} \quad (\text{Lemma 5.4}) ,$$

as needed. \square

Corollary 5.6 (Item 2 of Theorem 1.3). *For any lattice $\mathcal{L} \subset \mathbb{R}^n$ with $\det(\mathcal{L}') \geq 1$ for all $\mathcal{L}' \subseteq \mathcal{L}$ and any parameter $1/t < s < t$, we have*

$$\rho_s(\mathcal{L}) \leq 4(e^8 st)^{n/2} ,$$

where $t := 10(\log n + 2)$.

Proof. Let $\tau := (1 - \log s / \log t)/2$. Then,

$$\rho_s(\mathcal{L}) \leq 2e^{4n} \rho_{1/t}(\mathcal{L})^\tau \cdot \rho_t(\mathcal{L})^{1-\tau} \quad (\text{Theorem 5.5})$$

$$\leq 2^{1+\tau} e^{4n} \rho_t(\mathcal{L})^{1-\tau} \quad (\text{Theorem 1.2})$$

$$\leq 4e^{4n} t^{(1-\tau)n} \quad (\text{Corollary 5.2})$$

$$= 4(e^8 st)^{n/2} ,$$

as needed. \square

6 Proof of the covering radius approximation

We will need the following lemma, which is implicit in [Ban93].

Lemma 6.1. *For any lattice $\mathcal{L} \subset \mathbb{R}^n$ and $t > 0$ such that $\rho_{1/t}(\mathcal{L}^*) \leq 3/2$,*

$$\mu(\mathcal{L}) < \left(\sqrt{\frac{n}{2\pi}} + 1 \right) \cdot t .$$

Proof. By scaling the lattice, we may assume without loss of generality that $t = 1$. Let $r := ((1 + 4/\sqrt{n})/(2\pi))^{1/2}$. By Lemma 2.1, for any $\mathbf{t} \in \mathbb{R}^n$, we have

$$\rho((\mathcal{L} - \mathbf{t}) \setminus r\sqrt{n}B_2^n) \leq (\sqrt{2\pi}er^2e^{-\pi r^2})^n \cdot \rho(\mathcal{L}) = e^{-2\sqrt{n}}(1 + 4/\sqrt{n})^{n/2} \cdot \rho(\mathcal{L}) < \rho(\mathcal{L})/3 ,$$

where the last inequality follows by noting that it holds for $n = 1$ and that $e^{-2x} \cdot (1 + 4/x)^{x^2/2}$ is a decreasing function in x for $x > 0$ (a fact that can be proven using a tedious but straightforward computation). On the other hand, it is an easy consequence of the Poisson Summation Formula (see, e.g., [MR07]) that for any $\mathbf{t} \in \mathbb{R}^n$,

$$\rho(\mathcal{L} - \mathbf{t}) \geq \frac{2 - \rho(\mathcal{L}^*)}{\rho(\mathcal{L}^*)} \cdot \rho(\mathcal{L}) \geq \rho(\mathcal{L})/3.$$

Therefore, $(\mathcal{L} - \mathbf{t}) \cap r\sqrt{n}B_2^n$ is nonempty, and in particular, $\text{dist}(\mathbf{t}, \mathcal{L}) \leq r\sqrt{n} < \sqrt{n/(2\pi)} + 1$. Since this holds for arbitrary \mathbf{t} , we have $\mu(\mathcal{L}) < \sqrt{n/(2\pi)} + 1$, as needed. \square

We now note that Theorem 1.2 (together with Lemma 6.1) immediately implies a bound on the covering radius of stable lattices.

Theorem 6.2. *For any stable lattice $\mathcal{L} \subset \mathbb{R}^n$,*

$$\mu(\mathcal{L}) \leq 4\sqrt{n}(\log n + 10).$$

Proof. Let $t := 10(\log n + 2)$. Since \mathcal{L}^* is also stable (by Item (i) of Proposition 2.5), Theorem 1.2 implies that $\rho_{1/t}(\mathcal{L}^*) \leq 3/2$. Applying Lemma 6.1, we have

$$\mu(\mathcal{L}) \leq (\sqrt{n/(2\pi)} + 1) \cdot t < 4\sqrt{n}(\log n + 10),$$

as needed. \square

Next, we show (Proposition 6.4) how to reduce the case of general lattices to the stable case. We will need the following technical lemma, which is a slight modification of [DR16, Lemma 4.9] (with an essentially identical proof).

Lemma 6.3 (Reverse AM-GM). *Let $0 < a_1 < \dots < a_k$ and $d_1, \dots, d_k \in \mathbb{N}$, and for $j = 1, \dots, k$, define $m_j := \sum_{i \geq j} d_i$. Then,*

$$\sum_{i=1}^k d_i a_i \leq 2e \cdot \lceil \log(2m_1) \rceil \cdot \max_j m_j \left(\prod_{i \geq j} a_i^{d_i} \right)^{1/m_j}.$$

Proof. For $\ell = 1, 2, \dots$, let $S_\ell := \{j : e^{-\ell} a_k < a_j \leq e^{1-\ell} a_k\}$, and let $j_\ell := \min\{j \in S_\ell\}$. For non-empty S_ℓ , we have

$$\sum_{i \in S_\ell} d_i a_i \leq m_{j_\ell} e^{1-\ell} a_k \leq e m_{j_\ell} a_{j_\ell} \leq e m_{j_\ell} \cdot \left(\prod_{i \geq j_\ell} a_i^{d_i} \right)^{1/m_{j_\ell}}.$$

Let $\ell^* := \lceil \log(2m_1) \rceil$. By the above inequality, it suffices to argue that there exists an ℓ such that $2\ell^* \cdot \sum_{i \in S_\ell} d_i a_i \geq \sum_{i=1}^k d_i a_i$. Indeed,

$$\sum_{\ell=1}^{\ell^*} \sum_{i \in S_\ell} d_i a_i = \sum_{i=1}^k d_i a_i - \sum_{\ell > \ell^*} \sum_{i \in S_\ell} d_i a_i > \sum_{i=1}^k d_i a_i - m_1 \cdot \frac{a_k}{2m_1} \geq \frac{1}{2} \cdot \sum_{i=1}^k d_i a_i,$$

where in the last inequality we have used that $d_k \geq 1$. Therefore, there exists an ℓ such that

$$\sum_{i \in S_\ell} d_i a_i \geq \frac{1}{2\ell^*} \cdot \sum_{i=1}^k d_i a_i,$$

as needed. \square

Recall that

$$\mu_{\det}(\mathcal{L}) := \max_{W \subset \mathbb{R}^n} \sqrt{\dim(W^\perp)} \cdot \det(\pi_{W^\perp}(\mathcal{L}))^{\frac{1}{\dim(W^\perp)}},$$

where the maximum is over lattice subspaces $W \subset \mathbb{R}^n$ of \mathcal{L} (i.e., subspaces W spanned by up to $n - 1$ lattice vectors).

Proposition 6.4. *Let*

$$C_\mu(n) := \max_{d \leq n} \sup \mu(\mathcal{L}) / \sqrt{d},$$

where the supremum is over stable lattices $\mathcal{L} \subset \mathbb{R}^d$. Then, for any lattice $\mathcal{L} \subset \mathbb{R}^n$,

$$\mu(\mathcal{L}) \leq \sqrt{2e \lceil \log(2n) \rceil} \cdot C_\mu(n) \cdot \mu_{\det}(\mathcal{L}).$$

Proof. Let $\{\mathbf{0}\} = \mathcal{L}_0 \subset \mathcal{L}_1 \subset \dots \subset \mathcal{L}_k = \mathcal{L}$ be the canonical filtration of some lattice $\mathcal{L} \subset \mathbb{R}^n$. Let $d_i := \text{rank}(\mathcal{L}_i / \mathcal{L}_{i-1})$. Note that $\mathcal{L}_i / \mathcal{L}_{i-1}$ is a scaling of a stable lattice, i.e., $\det(\mathcal{L}_i / \mathcal{L}_{i-1})^{-1/d_i} \cdot (\mathcal{L}_i / \mathcal{L}_{i-1})$ is stable. (See Item 2 of Proposition 2.5.) We therefore have by Claim 2.6 and Lemma 2.8 that

$$\begin{aligned} \mu(\mathcal{L})^2 &\leq \mu\left(\bigoplus_i \mathcal{L}_i / \mathcal{L}_{i-1}\right)^2 \\ &= \sum_i \mu(\mathcal{L}_i / \mathcal{L}_{i-1})^2 \\ &\leq C_\mu(n)^2 \cdot \sum_i d_i \det(\mathcal{L}_i / \mathcal{L}_{i-1})^{2/d_i}. \end{aligned} \tag{18}$$

Next, we recall from Item 3 of Proposition 2.5 that $a_i := \det(\mathcal{L}_i / \mathcal{L}_{i-1})^{2/d_i}$ is an increasing sequence, and we note that $\sum_{i \geq j} d_i = \text{rank}(\mathcal{L} / \mathcal{L}_{j-1})$. We may therefore use Lemma 6.3 to bound Eq. (18) from above by

$$\begin{aligned} &2e \lceil \log(2n) \rceil \cdot C_\mu(n)^2 \cdot \max_i \text{rank}(\mathcal{L} / \mathcal{L}_i) \cdot \det(\mathcal{L} / \mathcal{L}_i)^{\frac{2}{\text{rank}(\mathcal{L} / \mathcal{L}_i)}} \\ &\leq 2e \lceil \log(2n) \rceil \cdot C_\mu(n)^2 \max_{W \subset \mathbb{R}^n} \dim(W^\perp) \cdot \det(\pi_{W^\perp}(\mathcal{L}))^{\frac{2}{\dim(W^\perp)}}, \end{aligned}$$

as needed. \square

Theorem 1.5 now follows as an immediate corollary of the above results. In particular, we have $C_\mu(n) \leq 4(\log n + 10)$ and therefore $\sqrt{2e \lceil \log(2n) \rceil} \cdot C_\mu(n) \leq 10(\log n + 10)^{3/2}$. The result then follows from Proposition 6.4.

6.1 Connection with the Slicing Conjecture

In this section, we prove Theorem 6.8. The structure of the proof is based on the one suggested in [SW16], as was the case for the proof of our main theorem in Section 4.

As in Section 4, we are unable to work with the lattice parameter $\mu(\mathcal{L})$ that interests us directly.⁸ Instead, we work with the lattice parameter

$$\bar{\mu}(\mathcal{L}) := \sqrt{\frac{1}{\det(\mathcal{L})} \int_{\mathcal{V}(\mathcal{L})} \|\mathbf{x}\|^2 d\mathbf{x}},$$

⁸While [DSV12] give a characterization of lattices corresponding to local maxima of μ , we are unable to obtain a sufficiently strong bound on the covering radius of these lattices. See [SW16] for more about this question.

which gives a good approximation to μ . The following tight result due to Magazinov [Mag18] (and conjectured in [HLR09]) makes this precise. (See [HLR09, Claim 3.1] for a slightly weaker result with a simple proof. See, e.g., [ZF96, CS98, GMR05, HLR09, Mag18] for more about $\bar{\mu}$.)

Theorem 6.5 ([Mag18]). *For any lattice $\mathcal{L} \subset \mathbb{R}^n$,*

$$\bar{\mu}(\mathcal{L}) \leq \mu(\mathcal{L}) \leq \sqrt{3}\bar{\mu}(\mathcal{L}) .$$

We now observe that Theorem 3.1 is applicable to the function $\bar{\mu}(\mathcal{L})^2$. Recall that a symmetric convex body $K \subset \mathbb{R}^n$ is said to be *isotropic* if $\int_K \mathbf{x}\mathbf{x}^T d\mathbf{x} = \alpha \cdot I_n$ for some scalar $\alpha > 0$.

Proposition 6.6. *For any lattice $\mathcal{L} \subset \mathbb{R}^n$,*

$$\nabla_A \bar{\mu}(A\mathcal{L})^2|_{A=I_n} = \frac{2}{\det(\mathcal{L})} \int_{\mathcal{V}(\mathcal{L})} \mathbf{x}\mathbf{x}^T d\mathbf{x} ,$$

where $A \in \mathbb{R}^{n \times n}$ is a non-singular matrix. In particular, if \mathcal{L} corresponds to a local maximum (or local minimum) of $\bar{\mu}(\mathcal{L})$ over the set of determinant-one lattices, then $\mathcal{V}(\mathcal{L})$ is isotropic.

Proof. To compute the gradient, we simply apply Theorem 3.1 with $f(x) := x$, and recall that

$$\bar{\mu}(A\mathcal{L})^2 = \frac{1}{\det(\mathcal{L})} \cdot \frac{1}{|\det(A)|} \int_{\mathcal{V}(A\mathcal{L})} f(\|\mathbf{x}\|^2) d\mathbf{x} .$$

The “in particular” follows from the fact that a differentiable function $g(A)$ restricted to the set of determinant-one matrices has a critical point at $A = I_n$ if and only if $\nabla_A g(A)|_{A=I_n}$ is a scalar multiple of the identity. \square

We define the (symmetric) isotropic constant

$$L_n^2 := \max_{d \leq n} \frac{1}{d} \cdot \sup_K \int_K \|\mathbf{x}\|^2 d\mathbf{x} ,$$

where the supremum is taken over all isotropic symmetric convex bodies $K \subset \mathbb{R}^d$ of volume one. It is known to satisfy $1/(2\sqrt{3}) \leq L_n \leq n^{o(1)}$, and the Slicing Conjecture implies that L_n is bounded by a universal constant [Bou91, Kla06, Che21, KL22]. (The lower bound is due to the hypercube, $[-1/2, 1/2]^n$.) We note in passing that we are only concerned with the isotropic constant for Voronoi cells, which could conceivably be easier to bound than the isotropic constant for arbitrary convex bodies.

Theorem 6.7. *For any stable lattice $\mathcal{L} \subset \mathbb{R}^n$,*

$$\mu(\mathcal{L}) \leq \sqrt{3}\bar{\mu}(\mathcal{L}) \leq \sqrt{3n}L_n .$$

Proof. By Theorem 6.5, it suffices to prove that $\bar{\mu}(\mathcal{L}) \leq \sqrt{n}L_n$. Note that this is trivially true for $n = 1$. We assume for induction that $\bar{\mu}(\mathcal{L}') \leq \sqrt{d}L_d \leq \sqrt{d}L_n$ for all stable lattices \mathcal{L}' of rank $d < n$. Recall that the set of stable lattices is compact (Item (ii) of Proposition 2.5), so that we may assume without loss of generality that \mathcal{L} corresponds to a global maximum of the function $\bar{\mu}$ over this set. If this is also a *local* maximum over the set of determinant-one lattices, then by Proposition 6.6, the Voronoi cell is isotropic, and we have $\bar{\mu}(\mathcal{L}) \leq \sqrt{n}L_n$ by the definition of $\bar{\mu}$ and

L_n . Otherwise, \mathcal{L} must lie on the boundary of the set of stable lattices. I.e., there is some primitive sublattice $\mathcal{L}' \subset \mathcal{L}$ of rank $0 < d < n$ such that \mathcal{L}' and \mathcal{L}/\mathcal{L}' are both stable. (See Item (iv) of Proposition 2.5.) Applying the induction hypothesis and Corollary 2.9 (together with Claim 2.6), we have

$$\bar{\mu}(\mathcal{L})^2 \leq \bar{\mu}(\mathcal{L}' \oplus \mathcal{L}/\mathcal{L}')^2 = \bar{\mu}(\mathcal{L}')^2 + \bar{\mu}(\mathcal{L}/\mathcal{L}')^2 \leq dL_n^2 + (n-d)L_n^2 = nL_n^2,$$

as needed. \square

As far as we know, it is entirely possible that $L_n = 1/(2\sqrt{3})$, i.e., that the hypercube $[-1/2, 1/2]^n$ is the worst symmetric body for the Slicing Conjecture. If this is true, then we get that for any stable lattice $\mathcal{L} \subset \mathbb{R}^n$, $\mu(\mathcal{L}) \leq \sqrt{n}/2$, which is tight for \mathbb{Z}^n . Apart from being an interesting statement in its own right, it was shown by Shapira and Weiss [SW16] that such a result would imply the so-called Minkowski conjecture (see there for more information).

We can now use Proposition 6.4 to extend Theorem 6.7 to all lattices $\mathcal{L} \subset \mathbb{R}^n$.

Theorem 6.8. *For any lattice $\mathcal{L} \subset \mathbb{R}^n$,*

$$\frac{1}{\sqrt{2\pi e}} \cdot \mu_{\det}(\mathcal{L}) \leq \mu(\mathcal{L}) \leq 5\sqrt{\log n + 1} \cdot L_n \cdot \mu_{\det}(\mathcal{L}).$$

As we observed in Footnote 4, there are lattices with $\mu(\mathcal{L}) \geq C\sqrt{\log n} \cdot \mu_{\det}(\mathcal{L})$. So, up to a constant factor, Theorem 6.8 gives the strongest possible upper bound on $\mu(\mathcal{L})$ in terms of $\mu_{\det}(\mathcal{L})$, assuming the Slicing Conjecture. We note that Dadush recently proved a variant of Theorem 6.8 [Dad19, Theorem 2.5]. He avoids the $\sqrt{\log n}$ factor loss by replacing μ_{\det} with a parameter that depends on determinants of multiple projections of \mathcal{L} simultaneously, rather than just one as in the definition of μ_{\det} . In particular, assuming the Slicing Conjecture, his result gives a characterization of the covering radius up to a constant factor in terms of determinants of projections.

7 An optimal bound for extreme parameters

We now prove Theorem 1.6, which says that \mathbb{Z}^n has maximal Gaussian mass amongst all lattices \mathcal{L} with $\det(\mathcal{L}') \geq 1$ for all sublattices $\mathcal{L}' \subseteq \mathcal{L}$, for very small parameters $s \leq \sqrt{2\pi/(n+2)}$ and for very large parameters $s \geq \sqrt{(n+2)/(2\pi)}$. The proof is similar to that of Theorem 1.2, except here we work directly with $\rho_s(\mathcal{L})$ (instead of the proxy $\gamma_s(\mathcal{V}(\mathcal{L}))$). Moreover, we show that $\rho_s(\mathcal{L})$ has *no local maxima* for those values of s , which leads to a simpler proof and the clearly tight result. In order to show that local maxima do not exist, we will show that the Laplacian of $\rho_s(\mathcal{L})$ is always positive when \mathcal{L} is stable.

In more detail, for a lattice \mathcal{L} and $s > 0$ let $f_{\mathcal{L},s} : X \rightarrow \mathbb{R}$ be given by

$$f_{\mathcal{L},s}(A) := \rho_s(e^{A/2}\mathcal{L}) = \sum_{\mathbf{y} \in \mathcal{L}} e^{-\pi \mathbf{y}^T e^A \mathbf{y} / s^2},$$

where $X \subset \mathbb{R}^{n \times n}$ is the linear space of all symmetric matrices with zero trace. Notice that as A ranges over X , $e^{A/2} := I_n + \sum_{i=1}^{\infty} (A/2)^i / i!$ ranges over all determinant-one positive-definite matrices. In particular, $e^{A/2}\mathcal{L}$ ranges over all lattices of fixed determinant, up to orthogonal transformations. (To see this, notice that any \mathcal{L}' of the same determinant as \mathcal{L} can be written as $\mathcal{L}' = T\mathcal{L}$ for some matrix T of determinant one. Then, up to an orthogonal transformation, \mathcal{L}'

equals $V^T DV\mathcal{L}$ where $T = UDV$ is the singular value decomposition of T . Finally, notice that $V^T DV$ is a determinant-one positive-definite matrix.) See [Ter16, Section 1.1.3] for a more in-depth treatment of the space of determinant-one matrices.

Recall that the *Laplacian* of a twice differentiable function $g : X \rightarrow \mathbb{R}$ is given by

$$\Delta_X g(A) := \sum_i \frac{\partial^2}{\partial E_i^2} g(A) ,$$

where the E_i form an orthonormal basis of X (under the inner product $\langle A, B \rangle = \text{Tr}(A^T B)$), and

$$\frac{\partial^2}{\partial M^2} g(A) := \frac{\partial^2}{\partial r^2} g(A + rM)|_{r=0}$$

is the directional second derivative of g in the M direction. One can show that the Laplacian does not depend on the choice of basis. Clearly, if the Laplacian is positive at A , then A cannot correspond to a local maximum of g , since there must be at least one direction in which the second derivative is positive.

The Laplacian of $f_{\mathcal{L},s}$ is straightforward to calculate. It can be found, e.g., in the work by Sarnak and Strömbergsson [SS06] who used it to study local minima of $\rho_s(\mathcal{L})$.

Claim 7.1 ([SS06, Eq. (46)]). *Let $X \subset \mathbb{R}^{n \times n}$ be the space of trace-zero symmetric matrices. Then, for any lattice $\mathcal{L} \subset \mathbb{R}^n$ and any parameter $s > 0$,*

$$\Delta_X f_{\mathcal{L},s}(0) = \frac{\pi}{s^2} \cdot \frac{n-1}{n} \cdot \sum_{\mathbf{y} \in \mathcal{L}} \rho_s(\mathbf{y}) \|\mathbf{y}\|^2 \left(\frac{\pi}{s^2} \cdot \|\mathbf{y}\|^2 - \frac{n+2}{2} \right) .$$

Proposition 7.2. *For any lattice $\mathcal{L} \subset \mathbb{R}^n$ and*

$$0 < s \leq \sqrt{\frac{2\pi}{n+2}} \cdot \lambda_1(\mathcal{L}) ,$$

\mathcal{L} cannot correspond to a local maximum of $\rho_s(\mathcal{L})$ over the set of determinant-one lattices. In particular, since stable lattices have $\lambda_1(\mathcal{L}) \geq 1$, a stable lattice cannot correspond to a local maximum for $s \leq \sqrt{2\pi/(n+2)}$.

Proof. It suffices to show that the Laplacian given in Claim 7.1 is positive for such \mathcal{L} . Indeed, the summand is zero for $\mathbf{y} = \mathbf{0}$, and since

$$\frac{\pi}{s^2} \cdot \lambda_1(\mathcal{L})^2 \geq \frac{n+2}{2} ,$$

the summand is non-negative for all non-zero $\mathbf{y} \in \mathcal{L}$. Finally, since any lattice contains vectors of arbitrarily large length, there must be some strictly positive terms in the sum. Therefore, the full sum is strictly positive, as needed. \square

From this, we derive our main result for the special case of stable lattices.

Proposition 7.3. *For any $0 < s \leq \sqrt{2\pi/(n+2)}$ and stable lattice $\mathcal{L} \subset \mathbb{R}^n$, $\rho_s(\mathcal{L}) \leq \rho_s(\mathbb{Z}^n)$.*

Proof. Note that the result is trivial for $n = 1$. We assume for induction that the result holds for all dimensions less than n . Since the set of stable lattices is compact and $\rho_s(\mathcal{L})$ is a continuous function, we may assume that \mathcal{L} corresponds to a global maximum of $\rho_s(\mathcal{L})$ over the set of stable lattices. By Proposition 7.2, this cannot be a local maximum over the set of determinant-one lattices. So, \mathcal{L} must be on the boundary of the set of stable lattices. I.e., there is a non-trivial primitive sublattice $\mathcal{L}' \subset \mathcal{L}$ with $d := \text{rank}(\mathcal{L}')$ such that \mathcal{L}' and \mathcal{L}/\mathcal{L}' are themselves stable lattices of rank strictly less than n . (See Item (iv) of Proposition 2.5.) Applying the induction hypothesis, we have by Lemma 2.3 that

$$\rho_s(\mathcal{L}) \leq \rho_s(\mathcal{L}') \cdot \rho_s(\mathcal{L}/\mathcal{L}') \leq \rho_s(\mathbb{Z}^d) \cdot \rho_s(\mathbb{Z}^{n-d}) = \rho_s(\mathbb{Z}^n),$$

where we have used the fact that $s \leq \sqrt{2\pi/(n+2)} \leq \min\{\sqrt{2\pi/(d+2)}, \sqrt{2\pi/(n-d+2)}\}$ in order to apply the induction hypothesis. \square

We now “invert the parameter” using duality.

Corollary 7.4. *For any $s \geq \sqrt{(n+2)/(2\pi)}$ and stable lattice $\mathcal{L} \subset \mathbb{R}^n$, $\rho_s(\mathcal{L}) \leq \rho_s(\mathbb{Z}^n)$.*

Proof. Recall that the dual \mathcal{L}^* of a stable lattice is itself stable. (See Item (i) of Proposition 2.5.) Furthermore, by the Poisson Summation Formula for the discrete Gaussian (Eq. (5)),

$$\rho_s(\mathcal{L}) = \frac{s^n}{\det(\mathcal{L})} \cdot \rho_{1/s}(\mathcal{L}^*) \leq \frac{s^n}{\det(\mathcal{L})} \cdot \rho_{1/s}(\mathbb{Z}^n) = \rho_s(\mathbb{Z}^n),$$

as needed, where the inequality follows from Proposition 7.3, and the last equality follows from the Poisson Summation Formula applied to \mathbb{Z}^n . \square

We can now prove Theorem 1.6.

Proof of Theorem 1.6. Let $\{\mathbf{0}\} = \mathcal{L}_0 \subset \mathcal{L}_1 \subset \dots \subset \mathcal{L}_k = \mathcal{L}$ be the canonical filtration of \mathcal{L} , and let $d_i := \text{rank}(\mathcal{L}_i/\mathcal{L}_{i-1}) \leq n$. Then, by Lemma 2.3, we have

$$\rho_s(\mathcal{L}) \leq \prod_i \rho_s(\mathcal{L}_i/\mathcal{L}_{i-1}).$$

Note that, if $s \leq \sqrt{2\pi/(n+2)}$, then we also have $s \leq \sqrt{2\pi/(d_i+2)}$ for all i . And, $\alpha_i \cdot (\mathcal{L}_i/\mathcal{L}_{i-1})$ is a stable lattice for some $\alpha_i \leq 1$. (See Items 2 and 3 of Proposition 2.5.) So, in this case we may apply Proposition 7.3 to obtain

$$\rho_s(\mathcal{L}) \leq \prod_i \rho_s(\alpha_i \cdot (\mathcal{L}_i/\mathcal{L}_{i-1})) \leq \prod_i \rho_s(\mathbb{Z}^{d_i}) = \rho_s(\mathbb{Z}^n).$$

If, on the other hand, $s \geq \sqrt{(n+2)/(2\pi)}$, then $s \geq \sqrt{(d_i+2)/(2\pi)}$ for all i , so we may similarly apply Corollary 7.4 to obtain the same result. \square

Remark. *It is possible to show that, in the setting of Theorem 1.6, $\rho_s(\mathcal{L}) = \rho_s(\mathbb{Z}^n)$ if and only if \mathcal{L} is an orthogonal transformation of \mathbb{Z}^n . To see this, first notice that in order to get equality, all the α_i in the proof above must be one, i.e., \mathcal{L} must be stable. Next, we follow the induction argument in the proof of Proposition 7.3, and recall the case of equality in Lemma 2.3.*

8 Tightness of our bounds

In this section, we discuss the tightness of our bounds by considering some classes of lattices $\mathcal{L} \subset \mathbb{R}^n$.

8.1 Tightness of Item 3 of Theorem 1.3 for stable lattices

It is an immediate consequence of the Poisson Summation Formula (Eq. (5)) that $\rho_s(\mathcal{L}) \geq s^n / \det(\mathcal{L})$ for any $s > 0$ and $\mathcal{L} \subset \mathbb{R}^n$. Combining this with Item 3 of Theorem 1.3, we see that

$$s^n \leq \rho_s(\mathcal{L}) \leq 2s^n$$

for any *stable* lattice $\mathcal{L} \subset \mathbb{R}^n$ and any $s \geq 10(\log n + 2)$. I.e., Item 3 of Theorem 1.3 is tight for all stable lattices up to a factor of two in the mass.

8.2 The integer lattice \mathbb{Z}^n

We first prove bounds on the Gaussian mass of \mathbb{Z}^n . In particular, the lower bound in Eq. (19) below shows that $\rho_{\sqrt{\pi/\log n}}(\mathbb{Z}^n) \geq 3/2$, so that Theorem 1.2 is tight for \mathbb{Z}^n up to a factor of $C\sqrt{\log n}$ in t . Similar bounds hold for Items 1 and 2 of Theorem 1.3.

Claim 8.1. *For any $n \geq 1$ and parameter $s > 0$,*

$$(1 + 2e^{-\pi/s^2})^n \leq \rho_s(\mathbb{Z}^n) \leq (1 + (2 + s)e^{-\pi/s^2})^n, \quad (19)$$

and

$$s^n \cdot (1 + 2e^{-\pi s^2})^n \leq \rho_s(\mathbb{Z}^n) \leq s^n \cdot (1 + (2 + 1/s)e^{-\pi s^2})^n. \quad (20)$$

Proof. Note that $\rho_s(\mathbb{Z}^n) = \rho_s(\mathbb{Z})^n$. So, it suffices to bound $\rho_s(\mathbb{Z})$. Furthermore, Eq. (20) follows from Eq. (19) and the Poisson Summation Formula (Eq. (5)). So, it suffices to prove Eq. (19) for the case $n = 1$. For the lower bound, we have

$$\rho_s(\mathbb{Z}) = 1 + 2 \sum_{z=1}^{\infty} e^{-\pi z^2/s^2} \geq 1 + 2e^{-\pi/s^2}.$$

For the upper bound, we write

$$\rho_s(\mathbb{Z}) = 1 + 2e^{-\pi/s^2} + 2 \sum_{z=2}^{\infty} e^{-\pi z^2/s^2} \leq 1 + 2e^{-\pi/s^2} + 2 \int_1^{\infty} e^{-\pi x^2/s^2} dx \leq 1 + (2 + s)e^{-\pi/s^2},$$

where we have used [AS64, Eq. 7.1.13] to bound the error function. \square

We now bound $|\mathbb{Z}^n \cap rB_2^n|$. Note that the lower bound in the next claim, which shows that $|\mathbb{Z}^n \cap rB_2^n| \geq e^{C r^2 \log(n/r^2)}$, is relatively close to the upper bound $|\mathbb{Z}^n \cap rB_2^n| \leq e^{C' r^2 \log^2 n}$ given by Item 1 of Corollary 1.4. (We include a better upper bound on $|\mathbb{Z}^n \cap rB_2^n|$ below for completeness. See [Ste17] for a slightly tighter bound via a more careful application of the same proof and [MO90] for tighter bounds for $r = C\sqrt{n}$.)

Claim 8.2. *For any $n \geq 1$ and any radius $1 \leq r \leq \sqrt{n}$,*

$$(2n/\lfloor r^2 \rfloor)^{\lfloor r^2 \rfloor} \leq |\mathbb{Z}^n \cap rB_2^n| \leq (2e^3 n/\lfloor r^2 \rfloor)^{\lfloor r^2 \rfloor}.$$

Proof. Since all points in \mathbb{Z}^n have integer squared norm, we may assume without loss of generality that r^2 is an integer. For the lower bound, we note that the number of vectors of length r whose coordinates lie in the set $\{-1, 0, +1\}$ is

$$2^{r^2} \binom{n}{r^2} \geq (2n/r^2)^{r^2},$$

as needed.

For the upper bound, using Eq. (19) with $s := \sqrt{\pi/\log(2n/r^2)} < 4$,

$$\begin{aligned} |\mathbb{Z}^n \cap rB_2^n| &\leq e^{\pi r^2/s^2} \rho_s(\mathbb{Z}^n) \\ &\leq (2n/r^2)^{r^2} \cdot \left(1 + \frac{r^2(2+s)}{2n}\right)^n \\ &\leq (2n/r^2)^{r^2} \cdot (1 + 3r^2/n)^n \\ &\leq (2e^3 n/r^2)^{r^2}, \end{aligned}$$

as needed. □

8.3 Random lattices

There exists a unique probability measure \mathcal{L}_n over the set of determinant-one lattices in \mathbb{R}^n that is invariant under $\text{SL}_n(\mathbb{R})$ [Sie45]. (See, e.g., [Ter16] or [GL87, Chapter 3].) We call a random variable \mathcal{L} sampled from \mathcal{L}_n a *random lattice*, and we write this as $\mathcal{L} \sim \mathcal{L}_n$. The purpose of this section is to prove the following result.

Proposition 8.3. *For any sufficiently large n and any $r \geq \sqrt{n} \log n$,*

$$\Pr_{\mathcal{L} \sim \mathcal{L}_n} \left[\mathcal{L} \text{ is stable and } |\mathcal{L} \cap rB_2^n| \geq \text{vol}(rB_2^n)/2 \right] \geq 1 - (Cn/r^2)^{n/2} - (C/n)^{n/2},$$

where $C > 0$ is some universal constant. In particular, there exists a stable lattice \mathcal{L} satisfying

$$|\mathcal{L} \cap rB_2^n| \geq \text{vol}(rB_2^n)/2 = (4\pi n)^{-1/2} (2\pi e r^2/n)^{n/2} (1 + o(1)), \quad (21)$$

where the $o(1)$ term approaches zero as n approaches ∞ .

Note that the lower bound in Eq. (21) is within a factor of $C\sqrt{n}$ of the upper bound in Item 3 of Corollary 1.4, which applies to stable lattices.

We will need the following three results.

Theorem 8.4 ([Sie45]). *For any $n \geq 2$ and any measurable set $S \subset \mathbb{R}^n$,*

$$\mathbb{E}_{\mathcal{L} \sim \mathcal{L}_n} [|(\mathcal{L} \setminus \{\mathbf{0}\}) \cap S|] = \text{vol}(S).$$

Theorem 8.5 ([Rog55, Sch60]; see [Gru07, Theorem 24.3]). *For $n \geq 3$ and any Borel set $S \subset \mathbb{R}^n$,*

$$\mathbb{E}_{\mathcal{L} \sim \mathcal{L}_n} [(|(\mathcal{L} \setminus \{\mathbf{0}\}) \cap S| - \text{vol}(S))^2] \leq C \text{vol}(S),$$

where $C > 0$ is some universal constant.

Theorem 8.6 ([SW14]). *For any sufficiently large n , an n -dimensional random lattice is stable with probability at least $1 - (C/n)^{n/2}$, where $C > 0$ is some universal constant.*

Proof of Proposition 8.3. By Chebyshev’s inequality, Theorem 8.4, and Theorem 8.5, there is some universal constant $C > 0$ such that

$$\Pr_{\mathcal{L} \sim \mathcal{L}_n} [|\mathcal{L} \cap rB_2^n| < \text{vol}(rB_2^n)/2] \leq \frac{C}{\text{vol}(rB_2^n)} \leq (C'n/r^2)^{n/2}.$$

The result then follows by Theorem 8.6 and union bound. □

References

- [AGM15] Shiri Artstein-Avidan, Apostolos A. Giannopoulos, and Vitali D. Milman. *Asymptotic geometric analysis. Part I*, volume 202 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2015. 24
- [AS64] Milton Abramowitz and Irene A. Stegun. *Handbook of mathematical functions with formulas, graphs, and mathematical tables*, volume 55 of *National Bureau of Standards Applied Mathematics Series*. For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C., 1964. 36
- [Ban93] Wojciech Banaszczyk. New bounds in some transference theorems in the geometry of numbers. *Mathematische Annalen*, 296(4):625–635, 1993. 10, 29
- [Bob11] Sergey G. Bobkov. On Milman’s ellipsoids and M -position of convex bodies. In *Concentration, functional inequalities and isoperimetry*, volume 545 of *Contemp. Math.*, pages 23–33. Amer. Math. Soc., Providence, RI, 2011. 6, 9, 21, 22
- [Bor75] Christer Borell. The Brunn-Minkowski inequality in Gauss space. *Invent. Math.*, 30(2):207–216, 1975. 24
- [Bos20] Jean-Benoît Bost. Réseaux euclidiens, séries thêta et pentes. Number 422, pages Exp. No. 1151, 1–59. 2020. Séminaire Bourbaki. Vol. 2018/2019. Exposés 1151-1165. 8
- [Bou91] Jean Bourgain. On the distribution of polynomials on high-dimensional convex sets. In *Geometric aspects of functional analysis (1989–90)*, volume 1469 of *Lecture Notes in Math.*, pages 127–137. Springer, Berlin, 1991. 4, 32
- [Cas04] Bill Casselman. Stability of lattices and the partition of arithmetic quotients. *Asian J. Math.*, 8(4):607–637, 2004. 11, 12
- [CDLP13] Kai-Min Chung, Daniel Dadush, Feng-Hao Liu, and Chris Peikert. On the lattice smoothing parameter problem. In *CCC*, 2013. 6, 20
- [CFM04] Dario Cordero-Erausquin, Matthieu Fradelizi, and Bernard Maurey. The (B) conjecture for the Gaussian measure of dilates of symmetric convex sets and related problems. *J. Funct. Anal.*, 214(2):410–427, 2004. 6, 22
- [Che21] Yuansi Chen. An almost constant lower bound of the isoperimetric coefficient in the KLS conjecture. *GAFA*, 2021. 4, 32

- [CK09] Henry Cohn and Abhinav Kumar. Optimality and uniqueness of the Leech lattice among lattices. *Ann. of Math. (2)*, 170(3):1003–1050, 2009. 7
- [CS98] John Conway and Neil J. A. Sloane. *Sphere Packings, Lattices and Groups*. Springer New York, 1998. 7, 32
- [Dad12a] Daniel Dadush. Private communication, 2012. 2, 6
- [Dad12b] Daniel Dadush. *Integer Programming, Lattice Algorithms, and Deterministic Volume Estimation*. PhD thesis, Georgia Institute of Technology, 2012. 8, 15, 23
- [Dad19] Daniel Dadush. On approximating the covering radius and finding dense lattice subspaces. In *STOC*, 2019. 7, 33
- [DR16] Daniel Dadush and Oded Regev. Towards strong reverse Minkowski-type inequalities for lattices. In *FOCS*, 2016. [arXiv:1606.06913](https://arxiv.org/abs/1606.06913). 2, 4, 6, 8, 30
- [DSV12] Mathieu Dutour Sikirić, Achill Schürmann, and Frank Vallentin. Inhomogeneous extreme forms. *Ann. Inst. Fourier (Grenoble)*, 62(6):2227–2255 (2013), 2012. 6, 7, 31
- [ERS22] Yael Eisenberg, Oded Regev, and Noah Stephens-Davidowitz. A tight reverse Minkowski inequality for the Epstein zeta function, 2022. [arXiv:2201.05201](https://arxiv.org/abs/2201.05201). 8
- [FT79] Tadeusz Figiel and Nicole Tomczak-Jaegermann. Projections onto Hilbertian subspaces of Banach spaces. *Israel J. Math.*, 33(2):155–171, 1979. 6, 23
- [GL87] Peter M. Gruber and Cornelis Gerit Lekkerkerker. *Geometry of numbers*. Number 37. North-Holland Publishing Co., Amsterdam, 2nd ed edition, 1987. 1, 37
- [GMR05] Venkatesan Guruswami, Daniele Micciancio, and Oded Regev. The complexity of the Covering Radius Problem. *Comput. Complex.*, 14(2):90–121, 2005. 32
- [Gra84] Daniel R. Grayson. Reduction theory using semistability. *Comment. Math. Helv.*, 59(4):600–634, 1984. 4, 7, 11, 12, 13
- [Gre07] Ben Green. A guest post on Terrence Tao’s blog, 2007. <http://terrytao.wordpress.com/2007/03/11/ben-green-the-polynomial-freiman-ruzsa-conjecture/>. 7
- [Gru07] Peter M. Gruber. *Convex and discrete geometry*, volume 336 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer, Berlin, 2007. 37
- [Hen02] Martin Henk. Successive minima and lattice points. *Rend. Circ. Mat. Palermo (2) Suppl.*, (70, part I):377–384, 2002. IV International Conference in “Stochastic Geometry, Convex Bodies, Empirical Measures & Applications to Engineering Science”, Vol. I (Troepea, 2001). 7
- [HLR09] Ishay Haviv, Vadim Lyubashevsky, and Oded Regev. A note on the distribution of the distance from a lattice. *Discrete & Computational Geometry*, 41(1):162–176, 2009. 32

- [HMT⁺22] Arne Heimendahl, Aurelio Marafioti, Antonia Thiemeyer, Frank Vallentin, and Marc Christian Zimmermann. Critical Even Unimodular Lattices in the Gaussian Core Model. *International Mathematics Research Notices*, 2022. [rnac164](#). [6](#), [8](#)
- [HN75] Günter Harder and Mudumbai S. Narasimhan. On the cohomology groups of moduli spaces of vector bundles on curves. *Mathematische Annalen*, 212(3):215–248, 1975. [4](#), [7](#), [11](#)
- [KL78] Grigorii A. Kabatjanskiĭ and Vladimir I. Levenšteĭn. Bounds for packings on the sphere and in space. *Problemy Peredači Informacii*, 14(1):3–25, 1978. [7](#)
- [KL88] Ravi Kannan and László Lovász. Covering minima and lattice-point-free convex bodies. *Ann. of Math. (2)*, 128(3):577–602, 1988. [3](#), [4](#), [8](#)
- [KL22] Bo’az Klartag and Joseph Lehec. Bourgain’s slicing problem and KLS isoperimetry up to polylog, 2022. [arxiv:2203.15551](#). [4](#), [32](#)
- [Kla06] Bo’az Klartag. On convex perturbations with a bounded isotropic constant. *Geom. Funct. Anal.*, 16(6):1274–1290, 2006. [4](#), [32](#)
- [Lat02] Rafał Łatała. On some inequalities for Gaussian measures. In *Proceedings of the International Congress of Mathematicians, Vol. II (Beijing, 2002)*, pages 813–822. Higher Ed. Press, Beijing, 2002. [22](#)
- [Lew79] Daniel R. Lewis. Ellipsoids defined by Banach ideal norms. *Mathematika*, 26(1):18–29, 1979. [6](#), [23](#)
- [LR17] Shachar Lovett and Oded Regev. A counterexample to a strong variant of the polynomial Freiman-Ruzsa conjecture in Euclidean space. *Discrete Anal.*, pages Paper No. 8, 6, 2017. [7](#)
- [Mag18] Alexander Magazinov. A proof of a conjecture by Haviv, Lyubashevsky and Regev on the second moment of a lattice Voronoi cell. *Advances in Geometry*, 2018. [arXiv:1707.03809](#). [5](#), [32](#)
- [Mah46] K. Mahler. On lattice points in n -dimensional star bodies. I. Existence theorems. *Proc. Roy. Soc. London Ser. A*, 187:151–187, 1946. [14](#)
- [Min10] Hermann Minkowski. *Geometrie der Zahlen*. B.G. Teubner, 1910. [1](#)
- [MO90] James E. Mazo and Andrew M. Odlyzko. Lattice points in high-dimensional spheres. *Monatsh. Math.*, 110(1):47–61, 1990. [36](#)
- [Mon88] Hugh L. Montgomery. Minimal theta functions. *Glasgow Math. J.*, 30(1):75–85, 1988. [7](#)
- [MP87] V. D. Milman and G. Pisier. Gaussian processes and mixed volumes. *Ann. Probab.*, 15(1):292–304, 1987. [7](#)
- [MR07] Daniele Micciancio and Oded Regev. Worst-case to average-case reductions based on Gaussian measures. *SIAM Journal on Computing*, 37(1):267–302 (electronic), 2007. [2](#), [30](#)

- [Pis82] Gilles Pisier. Holomorphic semigroups and the geometry of Banach spaces. *Ann. of Math. (2)*, 115(2):375–392, 1982. [6](#), [23](#)
- [Rog55] Claude A. Rogers. Mean values over the space of lattices. *Acta Math.*, 94:249–287, 1955. [37](#)
- [Sch60] Wolfgang M. Schmidt. A metrical theorem in geometry of numbers. *Trans. Amer. Math. Soc.*, 95:516–529, 1960. [37](#)
- [Sie45] Carl Ludwig Siegel. A mean value theorem in geometry of numbers. *Ann. of Math. (2)*, 46:340–347, 1945. [37](#)
- [Sol19] Omri N. Solan. Stable and well-rounded lattices in diagonal orbits. *Israel J. Math.*, 234(2):501–519, 2019. [5](#)
- [SS06] Peter Sarnak and Andreas Strömbergsson. Minima of Epstein’s zeta function and heights of flat tori. *Invent. Math.*, 165(1):115–151, 2006. [7](#), [34](#)
- [ST74] Vladimir N. Sudakov and Boris S. Tsirelson. Extremal properties of half-spaces for spherically invariant measures. *Zap. Naučn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI)*, 41:14–24, 165, 1974. Problems in the theory of probability distributions, II. [24](#)
- [Ste17] Noah Stephens-Davidowitz. *On the Gaussian Measure Over Lattices*. PhD thesis, New York University, 2017. [36](#)
- [Stu76] Ulrich Stuhler. Eine Bemerkung zur Reduktionstheorie quadratischer Formen. *Arch. Math. (Basel)*, 27(6):604–610, 1976. [4](#), [7](#), [11](#), [12](#)
- [SW14] Uri Shapira and Barak Weiss. A volume estimate for the set of stable lattices. *C. R. Math. Acad. Sci. Paris*, 352(11):875–879, 2014. [38](#)
- [SW16] Uri Shapira and Barak Weiss. Stable lattices and the diagonal group. *J. Eur. Math. Soc. (JEMS)*, 18(8):1753–1767, 2016. [arXiv:1609.08481](#). [4](#), [5](#), [6](#), [7](#), [9](#), [31](#), [33](#)
- [Ter16] Audrey Terras. *Harmonic analysis on symmetric spaces—higher rank spaces, positive definite matrix space and generalizations*. Springer, New York, second edition, 2016. [11](#), [34](#), [37](#)
- [vdC36] Johannes van der Corput. Verallgemeinerung einer Mordellschen Beweismethode in der Geometrie der Zahlen, Zweite Mitteilung. *Acta Arithmetica*, 2(1):145–146, 1936. [2](#)
- [Vor08] Georges Voronoi. Nouvelles applications des paramètres continus à la théorie des formes quadratiques. Premier mémoire. Sur quelques propriétés des formes quadratiques positives parfaites. *J. Reine Angew. Math.*, 133:97–102, 1908. [7](#)
- [ZF96] Ram Zamir and Meir Feder. On lattice quantization noise. *IEEE Transactions on Information Theory*, 42(4):1152–1159, 1996. [32](#)