SOME QUESTIONS RELATED TO THE REVERSE MINKOWSKI THEOREM

ODED REGEV

ABSTRACT

In this review we give an overview of some recent "reverse Minkowski" results on the geometry of lattices. Such results provide upper bounds on the number of short vectors a lattice can have, assuming that it does not have any sublattice of low determinant. We also briefly describe the proof ideas, and mention some open questions.

MATHEMATICS SUBJECT CLASSIFICATION 2020

Primary 11H06; Secondary 52C07

KEYWORDS

Reverse Minkowski, geometry of lattices, stable lattices, Epstein zeta function

ICM INTERNATIONAL CONGRESS OF MATHEMATICIANS 2022 JULY 6—14

Proc. Int. Cong. Math. 2022, Vol. 6, pp. 4898–4912
DOI 10.4171/ICM2022/134

1. INTRODUCTION

Sphere packing is a classical question in mathematics, asking for the densest way to pack equal disjoint spheres in the n-dimensional Euclidean space, where density is defined as the fraction of space covered by the spheres. In two dimensions the optimal packing is given by the familiar hexagonal packing. The Kepler conjecture, stating that the face-centered cubic arrangement is densest in three dimensions was proven by Hales [18]. Recently the question was also resolved in dimension 8 by Viazovska [40] and in dimension 24 by Cohn et al. [6].

In all the above cases, the optimal packing is achieved by a lattice packing, i.e., spheres whose centers form a lattice (e.g., in dimension 24 it is the Leech lattice). For this and other reasons, much focus has been on understanding the geometry of lattices, especially in high dimensions. A *lattice* is a discrete subgroup of $\mathbb{R}^n$. Equivalently, it is the set of all *integer* linear combinations of some linearly independent vectors in $\mathbb{R}^n$. We typically consider full-rank lattices, which are generated by a basis of $\mathbb{R}^n$. The *determinant* or *covolume* of a full-rank lattice is the reciprocal of the number of lattice points per unit volume, in the asymptotic large volume limit,

$$\det(\mathcal{L}) = \lim_{r\to\infty} \frac{\mathrm{vol}(B_2(r))}{\mathcal{L} \cap B_2(r)},$$

where $B_2(r)$ denotes the Euclidean ball of radius r. If A is an $n \times n$ matrix whose columns form a basis of $\mathcal{L}$, then $\det(\mathcal{L}) = |\det(A)|$, hence the name. More generally, if A is an $n \times m$ matrix whose columns form a basis of the (possibly nonfull rank) lattice $\mathcal{L}$, $\det(\mathcal{L}) = \det(A^T A)^{1/2}$.

The lattice sphere packing question asks for the densest *lattice* packing in a given dimension. Notice that the largest sphere that can be packed with a given lattice has radius precisely half the length of the shortest nonzero vector in the lattice (typically denoted by λ_1). We can therefore phrase the lattice sphere packing question as follows: among all lattices $\mathcal{L} \subseteq \mathbb{R}^n$ containing asymptotically one lattice point per unit volume (i.e., with $\det(\mathcal{L}) = 1$), how large can the length of their shortest nonzero vector $\lambda_1(\mathcal{L})$ be? Minkowski's celebrated first theorem [30] bounds this length from above by the radius of a Euclidean ball of volume 2^n, which is roughly $\sqrt{2n/(\pi e)}$. (This follows immediately from the fact that a ball of volume greater than 1 cannot pack space with a lattice of determinant 1). More generally, a theorem of Blichfeldt and van der Corput [39] says that for any integer $k \geq 1$, an n-dimensional lattice with determinant 1 must contain at least $2k$ nonzero points inside the closed Euclidean ball around the origin of volume $k2^n$. For example, the ball of radius $\sqrt{n}$, whose volume is roughly $(2\pi e)^{n/2} > 4^n$, must contain at least 2^n lattice points.

The lattice packing question is part of a broader set of questions, all asking for lattices that in some sense have few short vectors assuming some fixed determinant, say 1. For instance, one can ask for the minimum of Epstein's zeta function or of the theta function [35] (see below for the definitions). Another classical related question asks for the minimum covering radius (defined as the maximum distance of a point in $\mathbb{R}^n$ from the lattice) [7].

Reverse Minkowski questions. Here we are interested in "reverse Minkowski" questions that are in some sense dual to the above questions. Specifically, instead of *minimizing* the

number of short lattice vectors, we would like to *maximize* it. At first glance, this seems nonsensical: the number of short vectors in a lattice can be arbitrarily large, even if we restrict to determinant 1 lattices. For instance, consider the two-dimensional lattice generated by the vectors $(\varepsilon, 0)$ and $(0, 1/\varepsilon)$ where $\varepsilon > 0$ is arbitrarily small. Its determinant is 1, yet it has at least $1/\varepsilon$ vectors of norm at most 1.

Clearly, assuming that $\det \mathcal{L} = 1$ is not enough. We therefore impose the additional constraint that *all sublattices* of $\mathcal{L}$ have determinant at least 1. Here, by a sublattice of $\mathcal{L}$, we mean the intersection of $\mathcal{L}$ with a *lattice subspace*, i.e., a subspace spanned by lattice vectors. (Alternatively, one could define a sublattice as any discrete subgroup of $\mathcal{L}$; in all the results below, restricting to intersections with subspaces is without loss of generality.) For instance, in the example above, the 1-dimensional sublattice generated by the vector $(\varepsilon, 0)$ has determinant ε. The set of all determinant-1 lattices whose sublattices all have determinant at least 1 is known as the set of *stable* lattices and arises in a number of contexts [16, 19, 38]. It will play an important role below.

With this terminology in place, we can phrase the reverse Minkowski question as asking to bound from above the number of short vectors that a stable lattice can have. A precise form of this question was originally conjectured by Dadush, who was motivated by algorithmic problems related to integer programming [22]. Together with the present author, he went on to analyze variants of the conjecture and identified applications of the conjecture in computational complexity, cryptography, and mixing of Brownian motion [10]. Another application to additive combinatorics was shown in [25]. Dadush's conjecture was proven in [33]. In this review we give an overview of some of the known reverse Minkowski-style results, including a high level overview of the proof. We also present several open questions. For more details, the reader is referred to the original papers, especially [10, 33]. See also Bost's lecture notes [2] for a broader perspective.

2. REVERSE MINKOWSKI THEOREM FOR THE GAUSSIAN MASS

The main result shown in [33] is a reverse Minkowski theorem for the Gaussian mass, answering Dadush's original question. Here and in the rest of this review, constants are mostly arbitrary and no attempt was made to optimize them.

Theorem 2.1 (Reverse Minkowski theorem for the Gaussian mass). *For any stable lattice* $\mathcal{L} \subset \mathbb{R}^n$,

$$\rho_{1/t}(\mathcal{L}) \leq \frac{3}{2}, \tag{2.1}$$

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

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

$$\rho_s(\mathcal{L}) := \sum_{\mathbf{y} \in \mathcal{L}} e^{-\pi \|\mathbf{y}\|^2/s^2} \tag{2.2}$$

is the *Gaussian mass* of the lattice with *parameter* s. It is related to the theta function by $\Theta_{\mathcal{L}}(iy) := \rho_{1/\sqrt{y}}(\mathcal{L})$. An upper bound on ρ implies an upper bound on the number of

short vectors in a lattice. Specifically, Theorem 2.1 immediately implies that $|\mathcal{L} \cap B_2(r)| \leq 3e^{\pi t^2 r^2}/2$ for any radius $r > 0$. In contrast to Minkowski-style theorems which provide a *lower bound* on the number of short lattice vectors, this theorem provides an *upper bound*, justifying the name "reverse Minkowski."

It is natural to ask how tight Theorem 2.1 is. Consider the lattice $\mathbb{Z}^n$, and notice that it is stable (because $\det(A^T A)$ is integer for any $A \in \mathbb{Z}^{n \times m}$ and the square root of a positive integer number is at least 1). A short calculation shows that equation (2.1) holds for t as small as $\sqrt{\log(n)/\pi} + o(1)$, but not any smaller. It is therefore possible that Theorem 2.1 holds for $t = \sqrt{\log(n)/\pi} + o(1)$. In fact, one might even conjecture the following much stronger statement, roughly saying that "$\mathbb{Z}^n$ has the most short vectors."

Question 2.2. Is it true that for all $s > 0$ and stable $\mathcal{L} \subseteq \mathbb{R}^n$, $\rho_s(\mathcal{L}) \leq \rho_s(\mathbb{Z}^n)$?

We remark that replacing $\rho_s(\mathcal{L})$ with the point counting function $|\mathcal{L} \cap B_2(s)|$ (i.e., the number of points of norm at most s) leads to a false statement, e.g., the hexagonal lattice (scaled to have determinant 1) has 7 points of norm at most $\sqrt{2}/\sqrt[4]{3}$, whereas $\mathbb{Z}^2$ has only 5. However, the question is still open for the Gaussian mass ρ_s, which is a smooth version of the point counting function.

Encouragingly, a positive answer is known for very low or high values of s, specifically, for $s \leq \sqrt{2\pi/(n+2)}$ or $s \geq \sqrt{(n+2)/(2\pi)}$ [33]. More evidence in favor of a positive answer comes from the case of the zeta function; see Theorem 3.1 below. Another piece of evidence is that better bounds are known for an important subset of stable lattices known as *unimodular* lattices. A lattice $\mathcal{L}$ is said to be unimodular if (1) $\langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z}$ for all $\mathbf{x}, \mathbf{y} \in \mathcal{L}$ (a property known as *integrality*); and (2) it has determinant 1. Equivalently, a lattice is unimodular if it is self-dual. Then it was shown in [34] that for all unimodular lattices (in fact, for all integral lattices), the inequality in equation (2.1) holds with $t = \sqrt{2(1 + o(1)) \log(n)/\pi}$ for some universal constant $c > 0$. Up to a constant of $\sqrt{2}$, this matches the behavior of $\mathbb{Z}^n$.

While Theorem 2.1 is stated only for stable lattices, it is possible to extend it to the set of all lattices $\mathcal{L} \subset \mathbb{R}^n$ such that $\det(\mathcal{L}') \geq 1$ for all sublattices $\mathcal{L}' \subseteq \mathcal{L}$ (i.e., we can drop the assumption that $\det(\mathcal{L}) = 1$). This is done using the so-called canonical decomposition (see [33] for details). In other words, it holds that for any $\mathcal{L}$ whose sublattices all have determinant at least 1,

$$\eta^*(\mathcal{L}) \leq 10(\log n + 2),$$

where

$$\eta^*(\mathcal{L}) := \inf\{t > 0 : \rho_{1/t}(\mathcal{L}) \leq 3/2\}$$

(known as the smoothing parameter of the dual lattice [27]). Since $\rho_{1/t}(\mathcal{L})$ is monotonically decreasing with t, goes to infinity as t goes to 0, and to 1 as t goes to infinity, the infimum is positive and achieved.

Interestingly, having a small $\eta^*(\mathcal{L})$ as above approximately characterizes the set of lattices having no sublattice with determinant less than 1. Indeed, if $\mathcal{L}'$ is a sublattice of determinant smaller than 1 of some dimension d, then by the Blichfeldt–van der Corput

theorem (see Introduction), there are at least 2^d vectors of norm at most $\sqrt{d}$ in $\mathcal{L}'$. A straightforward calculation then shows that $\rho_3(\mathcal{L}) \geq \rho_3(\mathcal{L}') > 3/2$ or, equivalently, $\eta^*(\mathcal{L}) > 1/3$. (Alternatively, this fact can be shown using the Poisson summation formula.)

There is nothing special about the bound 1 on the determinants, and we can easily extend the above discussion to other values, leading to a two-sided inequality relating η^* to sublattice determinants. Namely, we claim that *for all* lattices $\mathcal{L}$,

$$\frac{1}{3} \cdot \eta_{\det}(\mathcal{L}) \leq \eta^*(\mathcal{L}) \leq 10(\log n + 2) \cdot \eta_{\det}(\mathcal{L}), \tag{2.3}$$

where

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

To prove equation (2.3), note that both $\eta_{\det}(\mathcal{L})$ and $\eta^*(\mathcal{L})$ behave identically under scaling of $\mathcal{L}$ (homogeneous of degree -1), so we can assume without loss of generality that $\eta_{\det}(\mathcal{L}) = 1$, in which case equation (2.3) is precisely the statement we proved above.

3. REVERSE MINKOWSKI THEOREM FOR THE ZETA FUNCTION

Theorem 2.1 establishes a bound on the Gaussian mass of any stable lattice. It would be interesting to explore other functions in addition to the Gaussian mass. One particularly appealing choice is the Epstein zeta function.

Definition 1. For a lattice $\mathcal{L} \subset \mathbb{R}^n$ and $s > n/2$, we define the *Epstein zeta function* as the function

$$\zeta(\mathcal{L}, s) := \sum_{\mathbf{y} \in \mathcal{L} \setminus \{\mathbf{0}\}} \|\mathbf{y}\|^{-2s}.$$

Similarly to the Gaussian mass, the Epstein zeta function is a sum over lattice points of some function depending on the norm of the vector. The function decays quite rapidly, and therefore is heavily influenced by short vectors. The requirement $s > n/2$ is needed for the sum to converge. The Epstein zeta function has an analytic continuation to the complex plane except for a simple pole at $s = n/2$ [13], but in this review we only focus on $s > n/2$.

Using a proof similar to that of Theorem 2.1 (and in fact simpler, as we explain below), Eisenberg et al. recently showed the following.

Theorem 3.1 ([12]). *For any stable lattice $\mathcal{L} \subset \mathbb{R}^n$ and $s > n/2$,*

$$\zeta(\mathcal{L}, s) \leq \zeta\left(\mathbb{Z}^n, s\right),$$

with equality if and only if $\mathcal{L}$ is an orthogonal rotation of $\mathbb{Z}^n$.

Notice that unlike the case of Gaussian mass (Theorem 2.1), here we have a tight statement, showing that "$\mathbb{Z}^n$ has the most short vectors" (as quantified by the zeta function), hence answering Question 2.2 for the Epstein zeta function. We remark that a positive answer to Question 2.2 immediately implies Theorem 3.1 (so in a sense, the former is a harder

question). This follows by writing the zeta function as a positive combination of Gaussian functions,

$$\zeta(\mathcal{L}, s) = \frac{2\pi^s}{\Gamma(s)} \int_0^\infty t^{-(2s+1)} \big(\rho_t(\mathcal{L}) - 1\big) \mathrm{d}t.$$

4. PROOF OVERVIEW

In this section we give a high-level overview of the proofs of Theorems 2.1 and 3.1, starting with Theorem 3.1. Both proofs follow an approach suggested by Shapira and Weiss [36].

Recall that a lattice $\mathcal{L}$ is *stable* if $\det(\mathcal{L}) = 1$ and $\det(\mathcal{L}') \geq 1$ for all sublattices $\mathcal{L}' \subseteq \mathcal{L}$. The set of stable lattices is a compact subset of the set of determinant-one lattices (under the quotient topology of $\mathrm{SL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{Z})$). Therefore, the Epstein zeta function, being a continuous function, must attain a global maximum over the set of stable lattices. It can be shown that the Laplacian of the Epstein zeta function is positive everywhere (in fact, Epstein zeta is an eigenfunction of the Laplacian operator). It immediately follows that a global maximum $\mathcal{L}$ cannot be in the interior of the set of stable lattices. Therefore, $\mathcal{L}$ must be on the boundary of the set, which by definition, implies that there is a sublattice $\mathcal{L}_1$ of $\mathcal{L}$ such that $\det \mathcal{L}_1 = 1$ (see Figure 1). It follows immediately from the definition that $\mathcal{L}_1$ is stable. Let $\mathcal{L}_2 := \mathcal{L}/\mathcal{L}_1$ be the projection orthogonally to $\mathcal{L}_1$. It can also be shown that $\mathcal{L}_2$ is stable. Crucially, using the Poisson summation formula together with the fact that for any $q > 0$, the Fourier transform of the function $\mathbf{y} \mapsto (\|\mathbf{y}\|^2 + q)^{-s}$ is positive everywhere, it can be shown that $\zeta(\mathcal{L}, s) \leq \zeta(\mathcal{L}_1 \oplus \mathcal{L}_2, s)$. Informally speaking, "aligning the cosets" of $\mathcal{L}_1$ (see Figure 1) cannot decrease the zeta function. At this point we reduced the dimensionality of the problem, and we can continue iteratively in a similar way to split $\mathcal{L}_1$ and $\mathcal{L}_2$ into lower-dimensional stable lattices. Eventually, we arrive at the conclusion that the lattice maximizing $\zeta(\mathcal{L}, s)$ must be a direct sum of n 1-dimensional stable lattices, which is equivalent to saying that $\mathcal{L}$ is an orthogonal rotation of $\mathbb{Z}^n$. Notice that in order to continue iteratively, we need to show that the function $\mathcal{L}_1 \mapsto \zeta(\mathcal{L}_1 \oplus \mathcal{L}_2, s)$ also has a positive Laplacian (i.e., when we think of $\mathcal{L}_2$ as fixed and only vary $\mathcal{L}_1$); this turns out to indeed be the case [12]. This completes the description of the proof of Theorem 3.1.

We would like to use the same proof strategy to prove Theorem 2.1. Much of the above proof works if we replace the zeta function with the Gaussian mass. In particular, "aligning the cosets" cannot decrease the Gaussian mass, i.e., $\rho_s(\mathcal{L}) \leq \rho_s(\mathcal{L}_1 \oplus \mathcal{L}_2)$, which is proven in essentially the same way (Poisson summation formula combined with the positivity of the Fourier transform of ρ_s). Moreover, continuing iteratively is even a bit cleaner in this case since $\rho_s(\mathcal{L}_1 \oplus \mathcal{L}_2) = \rho_s(\mathcal{L}_1) \cdot \rho_s(\mathcal{L}_2)$ so once we are at the boundary, the problem truly reduces to a lower-dimensional problem. However, one serious issue is that the Gaussian mass function ρ is known to have local maxima for some parameters $s > 0$ [21]. We can therefore no longer argue as before that any global maximum must necessarily be on the boundary. (We note that for very small values of s, the Laplacian of ρ_s can be shown to

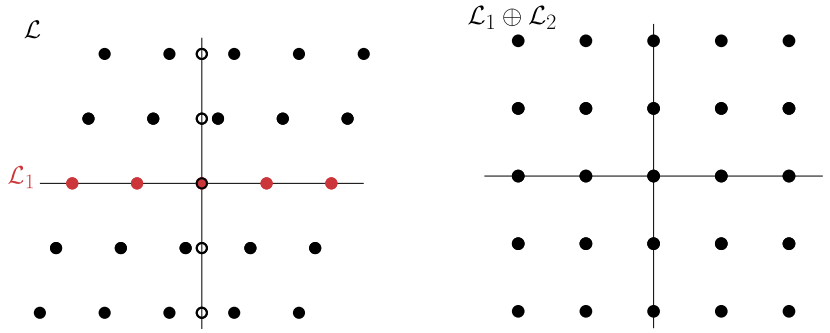

FIGURE 1

(Left) A two-dimensional stable lattice $\mathcal{L}$ (solid disks) is on the boundary of the set of stable lattices and therefore has a sublattice $\mathcal{L}_1$ of determinant 1 (red disks). Projecting $\mathcal{L}$ orthogonally to $\mathcal{L}_1$ (i.e., on the y axis) gives the lattice $\mathcal{L}_2 = \mathcal{L}/\mathcal{L}_1$, which is also stable (hollow circles). (Right) The lattice $\mathcal{L}_1 \oplus \mathcal{L}_2$.

be positive, and therefore no local maxima can exist, leading to the proof of the statement below Question 2.2; see [33]).

As a possible way around this issue, we can try to *bound ρ at local maxima*. In other words, we would like to use some property of local maxima (e.g., zero gradient) to argue that ρ cannot be too large there. We can then argue that the maximum must either be a local maximum in the interior (and then bound it as suggested here) or it must be on the boundary (in which case we can continue iteratively as before). While this approach is promising, we unfortunately do not know how to bound ρ at local maxima.

The actual proof of Theorem 2.1 follows the exact strategy described above, however, instead of working with ρ directly, it uses as a proxy another function which can be used to bound ρ from above. Namely, define the Gaussian measure of the Voronoi cell of the lattice as

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

where the Voronoi cell is the set of all points that are closer to the origin than to any other lattice vector,

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

It is known that $\rho_s(\mathcal{L}) \le 1/\gamma_s(\mathcal{V}(\mathcal{L}))$ [5]. Therefore, in order to prove an upper bound on $\rho_s(\mathcal{L})$, it suffices to prove a lower bound on $\gamma_s(\mathcal{V}(\mathcal{L}))$. This is achieved in [33] following the strategy suggested above. In particular, "aligning the cosets" cannot increase the Gaussian measure of the Voronoi cell, i.e., $\gamma_s(\mathcal{V}(\mathcal{L})) \ge \gamma_s(\mathcal{V}(\mathcal{L}_1 \oplus \mathcal{L}_2))$. This follows from the fact that $\mathcal{V}(\mathcal{L})$ and $\mathcal{V}(\mathcal{L}_1 \oplus \mathcal{L}_2) = \mathcal{V}(\mathcal{L}_1) \times \mathcal{V}(\mathcal{L}_2)$ are both fundamental bodies for the lattice $\mathcal{L}$, i.e., they both contain exactly one point in each coset of $\mathcal{L}$, but by definition, $\mathcal{V}(\mathcal{L})$ contains the *shortest* point in each coset, leading to the desired inequality (Figure 2). Moreover, continuing iteratively is again straightforward, since $\gamma_s(\mathcal{V}(\mathcal{L}_1 \oplus \mathcal{L}_2)) = \gamma_s(\mathcal{V}(\mathcal{L}_1) \times \mathcal{V}(\mathcal{L}_2)) = \gamma_s(\mathcal{V}(\mathcal{L}_1)) \cdot \gamma_s(\mathcal{V}(\mathcal{L}_2))$ so once we are at the boundary, the problem truly reduces

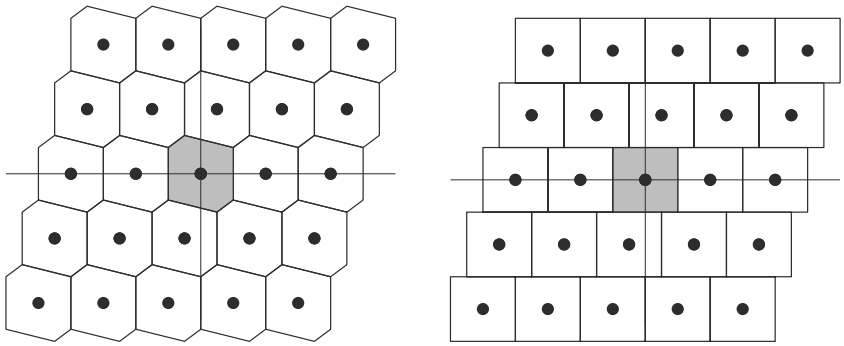

FIGURE 2
Both $\mathcal{V}(\mathcal{L})$ (left, gray) and $\mathcal{V}(\mathcal{L}_1 \oplus \mathcal{L}_2) = \mathcal{V}(\mathcal{L}_1) \times \mathcal{V}(\mathcal{L}_2)$ (right, gray) are fundamental bodies for the lattice $\mathcal{L}$.

to a lower-dimensional problem. The main technical effort is bounding the value of $\gamma_s(\mathcal{V}(\mathcal{L}))$ at local minima $\mathcal{L}$. (We do not know whether these local minima actually exist.) By considering the gradient of $\gamma_s(\mathcal{V}(\mathcal{L}))$ and using results from convex geometry [1, 8], we show that for such an $\mathcal{L}$, the convex body $\mathcal{V}(\mathcal{L})$ must be such that for all volume-preserving (determinant 1) linear transformations A, $\gamma_s(A\mathcal{V}(\mathcal{L})) \leq \gamma_s(\mathcal{V}(\mathcal{L}))$. In other words, it is in a position that maximizes its Gaussian measure. We complete the proof by using the $\ell\ell^*$ theorem [14, 24, 31], which implies that any convex body K satisfying the above must have $\gamma_s(K) \geq 2/3$ where $s = 1/(10(\log n + 2))$, as in Theorem 2.1.

5. IMPLICATIONS TO THE GEOMETRY OF VORONOI CELLS AND CONVEX BODIES

In [10], Dadush observed that Theorem 2.1 implies a certain statement about the geometry of Voronoi cells of lattices. Roughly speaking, reverse Minkowski shows that if a Voronoi cell is small (as measured by a certain Gaussian norm expectation) then there is an "explanation" of that in terms of a projection of low volume. Following [10], here we ask whether that statement might also hold for all symmetric convex bodies. (A convex body K is symmetric if $K = -K$.) We also observe that a somewhat weaker statement (where the explanation is in the form of a *slice* of low volume) is known to hold by a theorem of Milman and Pisier [29].

Definition 2 (K-norm). Let $K \subseteq \mathbb{R}^n$ be a centrally symmetric convex body. We define $\|\mathbf{x}\|_K = \min\{s \geq 0 : \mathbf{x} \in sK\}$ to be the norm on $\mathbb{R}^n$ induced by K.

Consider the quantity $\mathbb{E}[\|X\|_K]$ where $X \sim N(0, I_n)$ is a standard Gaussian vector. We can think of this quantity as measuring the size of a convex body by considering a ray starting from the origin and going in a random direction until it hits the boundary of K; we then take the expectation of the reciprocal of the (Euclidean) length of the ray. Notice that

the higher this expectation, the smaller the body. What are the bodies for which this quantity is at least 1? Following [32], we now observe that any body of volume at most 1 satisfies this. By $x \gtrsim y$ we mean that $x \geq cy$ for some universal constant $c > 0$.

Lemma 5.1. *Let $K \subseteq \mathbb{R}^n$ be a symmetric convex body of volume at most 1 and let $\|\cdot\|_K$ be the induced norm. Then for $X \sim N(0, I_n)$,*

$$\mathbb{E}\big[\|X\|_K\big] \gtrsim 1.$$

Proof. By integrating in polar coordinates and using Jensen's inequality,

$$\begin{aligned}\mathbb{E}\big[\|X\|_K\big] &= \mathbb{E}[\|X\|_2] \int_{S^{n-1}} \|\theta\|_K \mathrm{d}\theta \\ &\geq \mathbb{E}\big[\|X\|_2\big]\left(\int_{S^{n-1}} \|\theta\|_K^{-n} \mathrm{d}\theta\right)^{-1/n} \qquad \text{(by Jensen)} \\ &= \mathbb{E}[\|X\|_2]\left(\frac{\mathrm{vol}_n(K)}{\mathrm{vol}_n(B_2)}\right)^{-1/n} \gtrsim \frac{1}{\mathrm{vol}_n(K)^{1/n}}.\end{aligned}$$

■

In fact, more is true: instead of asking for volume at most 1, it is enough to ask for a slice of volume at most 1.

Corollary 5.2. *Let $K \subseteq \mathbb{R}^n$ be a symmetric convex body and let $\|\cdot\|_K$ be the induced norm. Then for $X \sim N(0, I_n)$, the following holds:*

$$\mathbb{E}\big[\|X\|_K\big] \gtrsim \max_{\substack{W \subseteq \mathbb{R}^n \\ d = \dim(W) \in [n]}} \frac{1}{\mathrm{vol}_d(K \cap W)^{1/d}} \tag{5.1}$$

$$\geq \max_{\substack{W \subseteq \mathbb{R}^n \\ d = \dim(W) \in [n]}} \frac{1}{\mathrm{vol}_d(\pi_W(K))^{1/d}}. \tag{5.2}$$

Proof. For the first inequality, note that

$$\mathbb{E}\big[\|X\|_K\big] = \mathbb{E}\big[\|\pi_W(X) + \pi_{W^\perp}(X)\|_K\big] \geq \mathbb{E}\big[\|\pi_W(X)\|_{K \cap W}\big],$$

by Jensen's inequality, since $\pi_W(X)$ and $\pi_{W^\perp}(X)$ are independent and $\mathbb{E}[\pi_{W^\perp}(X)] = 0$. We recover the desired lower bound by applying Lemma 5.1 to $\mathbb{E}[\|\pi_W(X)\|_{K \cap W}]$ (where we identify W with $\mathbb{R}^d$ for $d = \dim(W)$, and so $K \cap W$ is a convex body in $\mathbb{R}^d$ and $\pi_W(X)$ is distributed as $N(0, I_d)$). The second inequality is immediate from the fact that a slice of a convex body is contained in the corresponding projection. ■

It is a remarkable and nontrivial fact that follows from a theorem of Milman and Pisier [29] that, up to logarithmic terms, the right-hand side of equation (5.1) is also an *upper bound* on the expectation,

$$1 \lesssim \mathbb{E}\big[\|X\|_K\big] \min_{\substack{W \subseteq \mathbb{R}^n \\ d = \dim(W) \in [n]}} \mathrm{vol}_d(K \cap W)^{1/d} \lesssim \mathrm{poly}\log n.$$

In fact, up to a constant, the upper bound can be taken to be $\log^2(n+1)$. Here we ask whether equation (5.2) is also an upper bound on the expectation, i.e., whether for all symmetric

convex bodies K it holds that

$$1 \lesssim \mathbb{E}[\|X\|_K] \min_{\substack{W \subseteq \mathbb{R}^n \\ d=\dim(W)\in[n]}} \mathrm{vol}_d\big(\pi_W(K)\big)^{1/d} \lesssim \mathrm{poly}\log n. \tag{5.3}$$

See [15, 28] for some related work.

While we do not know if equation (5.3) holds for any symmetric convex body, we now observe that it does hold for Voronoi cells of lattices. We start with an approximation of $\eta^*(\mathcal{L})$ in terms of the Voronoi cell.

Theorem 5.3 ([9]). *Let $\mathcal{L} \subseteq \mathbb{R}^n$ be an n-dimensional lattice, and let $\mathcal{V} = \mathcal{V}(\mathcal{L})$. Then for $X \sim N(0, I_n)$, we have that*

$$\mathbb{E}\big[\|X\|_{\mathcal{V}}\big] \approx \eta^*(\mathcal{L}).$$

The notation $x \approx y$ means $cy \le x \le Cy$ for some universal constants $c, C > 0$. Therefore, equation (2.3) says that for any lattice $\mathcal{L} \subset \mathbb{R}^n$ with Voronoi cell $\mathcal{V}$,

$$1 \lesssim \mathbb{E}[\|X\|_{\mathcal{V}}] \min_{\substack{W \text{ lattice subspace of } \mathcal{L} \\ d=\dim(W)\in[n]}} \big(\det(\mathcal{L} \cap W)\big)^{1/d} \lesssim 1 + \log n. \tag{5.4}$$

To complete the proof, observe that for any lattice $\mathcal{L}$ with Voronoi cell $\mathcal{V}$, and any lattice subspace W of $\mathcal{L}$,

$$\det(\mathcal{L} \cap W) = \mathrm{vol}_d\big(\mathcal{V}(\mathcal{L} \cap W)\big) \ge \mathrm{vol}_d\big(\pi_W(\mathcal{V})\big),$$

where the inequality follows from the fact

$$\begin{aligned}\mathcal{V} &= \left\{\mathbf{x} \in \mathbb{R}^n : \langle \mathbf{x}, \mathbf{y}\rangle \le \frac{1}{2}\|\mathbf{y}\|_2^2,\ \forall \mathbf{y} \in \mathcal{L} \setminus \{\mathbf{0}\}\right\} \\ &\subseteq \left\{\mathbf{x} \in \mathbb{R}^n : \langle \mathbf{x}, \mathbf{y}\rangle \le \frac{1}{2}\|\mathbf{y}\|_2^2,\ \forall \mathbf{y} \in \mathcal{L} \cap W \setminus \{\mathbf{0}\}\right\},\end{aligned}$$

and the orthogonal projection of the latter set on W is precisely $\mathcal{V}(\mathcal{L} \cap W)$.

6. COVERING RADIUS

In Section 4 we described a general strategy to bound functions on the set of stable lattices, by (1) bounding their values at local extrema and (2) analyzing lattices on the boundary by induction on dimension. We applied this strategy to two functions: the zeta function (where local maxima do not exist, making (1) trivial) and the Gaussian measure of the Voronoi cell (used as a proxy for the Gaussian mass ρ of the lattice, which we do not know how to analyze directly). It is natural to ask if there are other functions to which we can apply this strategy. Here we show one more example related 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 $\mathcal{L} + B_2(r) = \mathbb{R}^n$. Yet another equivalent definition is $\max_{\mathbf{x}\in\mathcal{V}(\mathcal{L})} \|\mathbf{x}\|_2$. Notice that $\mu(\mathbb{Z}^n) = \sqrt{n}/2$ and analogously to Question 2.2, one can ask whether this is the maximum possible μ for a stable lattice.

Question 6.1. Is it true that for all stable $\mathcal{L} \subseteq \mathbb{R}^n$, $\mu(\mathcal{L}) \leq \mu(\mathbb{Z}^n)$?

Part of the interest in this question comes from a possible connection to integer programming, as observed by Kannan and Lovász [22] (see also [10]), as well as the connection to Minkowski's conjecture (see below) [36].

We do not know the answer to this question. It is possible, however, to derive a slightly weaker inequality directly from the statement of Theorem 2.1 using known inequalities between lattice parameters. Namely, for all stable $\mathcal{L} \subseteq \mathbb{R}^n$ it holds that [33]

$$\mu(\mathcal{L}) \leq 4\sqrt{n}(\log n + 10). \tag{6.1}$$

Below we will follow a different route, applying the strategy of Section 4 directly. Assuming a certain geometric conjecture holds, we would be able to improve on equation (6.1) and even answer Question 6.1 in the affirmative.

As was the case for the Gaussian mass ρ, we do not know how to work directly with μ, the main difficulty being bounding its value at local maxima (which were characterized in [11]). Instead, we work with the lattice parameter

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

While μ considers the point farthest away from $\mathcal{L}$, $\overline{\mu}$ looks at the (L_2) average distance of a random point in space from $\mathcal{L}$. (See also [7, 17, 28, 26, 41] for more about $\overline{\mu}$.) Magazinov showed that these two parameters are quite close to each other [26].

Theorem 6.2 ([26]). *For any lattice $\mathcal{L} \subset \mathbb{R}^n$,*

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

The lower bound is immediate from the definition, and the upper bound is tight for the lattice $\mathbb{Z}^n$. Because of the latter, it is plausible that one could resolve Question 6.1 entirely by considering $\overline{\mu}$ (see more below). We also remark that the natural extension of the upper bound in Theorem 6.2 to all convex bodies (and not just Voronoi cells) is totally false, as can be seen by taking the ℓ_1 ball (where the maximum ℓ_2 norm of a vector is 1, yet the typical norm is only $C/\sqrt{n}$).

Our goal is therefore to bound $\overline{\mu}(\mathcal{L})$ from above for stable lattices $\mathcal{L}$. As before, "aligning the cosets" cannot decrease $\overline{\mu}$, i.e., $\overline{\mu}(\mathcal{L}) \leq \overline{\mu}(\mathcal{L}_1 \oplus \mathcal{L}_2)$. The proof is also essentially the same, namely that $\mathcal{V}(\mathcal{L})$ and $\mathcal{V}(\mathcal{L}_1 \oplus \mathcal{L}_2) = \mathcal{V}(\mathcal{L}_1) \times \mathcal{V}(\mathcal{L}_2)$ are both fundamental bodies for the lattice $\mathcal{L}$, i.e., they both contain exactly one point in each coset of $\mathcal{L}$, but by definition, $\mathcal{V}(\mathcal{L})$ contains the *shortest* point in each coset, leading to the desired inequality. Moreover, continuing iteratively is again straightforward, since $\overline{\mu}(\mathcal{L}_1 \oplus \mathcal{L}_2)^2 = \overline{\mu}(\mathcal{L}_1)^2 + \overline{\mu}(\mathcal{L}_2)^2$ so once we are at the boundary, the problem truly reduces to a lower-dimensional problem. As before, the key step in the proof is bounding local maxima $\mathcal{L}$ of $\overline{\mu}$. Using a similar proof to the one in the case of the Gaussian measure of the Voronoi cell, it can be shown that such $\mathcal{L}$ must be such that their Voronoi cell $\mathcal{V}(\mathcal{L})$ is *isotropic*. Recall that a symmetric convex body $K \subset \mathbb{R}^n$ is said to be *isotropic* if its covariance matrix is a multiple of identity, i.e., $\int_K \mathbf{x}\mathbf{x}^T d\mathbf{x} = \alpha \cdot I_n$ for some scalar $\alpha > 0$. Intuitively, this says that the

Voronoi cell is not elongated in any one direction (e.g., a square is isotropic but a rectangle is not), which one might expect should imply that $\overline{\mu}$ is small. To make this precise, define the (symmetric) isotropic constant L_n as

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

where the supremum is taken over all isotropic symmetric convex bodies $K \subset \mathbb{R}^d$ of volume one. Therefore, by following the proof strategy from Section 4 we obtain the following.

Theorem 6.3 ([33]). *For any stable lattice $\mathcal{L} \subset \mathbb{R}^n$,*

$$\mu(\mathcal{L}) \le \sqrt{3}\overline{\mu}(\mathcal{L}) \le \sqrt{3n} L_n.$$

It is known that $1/(2\sqrt{3}) \le L_n \le n^{o(1)}$ [3, 4, 23], the lower bound being due to the hypercube $[-1/2, 1/2]^n$. This already gives a reasonably tight upper bound on $\mu(\mathcal{L})$ for stable lattices. But perhaps L_n is even smaller? The so-called slicing conjecture implies that L_n is bounded by a universal constant. In fact, 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 $\mathcal{L} \subset \mathbb{R}^n$, $\mu(\mathcal{L}) \le \sqrt{n}/2$, which is tight for $\mathbb{Z}^n$. That is, a positive answer to Question 6.1.

Apart from being an interesting statement in its own right, it was shown by Shapira and Weiss [36] that a positive answer to Question 6.1 implies the so-called Minkowski conjecture. The conjecture asserts that for every lattice $\mathcal{L} \subset \mathbb{R}^n$ (not necessarily stable) with $\det(\mathcal{L}) = 1$ and vector $\mathbf{t} = (t_1, \ldots, t_n) \in \mathbb{R}^n$,

$$\inf_{\mathbf{y} \in \mathcal{L}} \prod_i |y_i - t_i| \le 2^{-n}. \tag{6.2}$$

In order to derive the Minkowski conjecture, use the nontrivial fact that any lattice with determinant 1 can be made stable by multiplying it by a diagonal operator of determinant 1 [36, 37]. Since the left-hand side of equation (6.2) is invariant under multiplication by such operators, it follows that it suffices to prove the inequality for stable lattices. But a positive answer to Question 6.1 implies that for any $\mathbf{t}$, there exists a $\mathbf{y} \in \mathcal{L}$ such that $\|\mathbf{t} - \mathbf{y}\|_2 \le \sqrt{n}/2$. The AM–GM inequality now implies that $\prod_i |y_i - t_i| \le 2^{-n}$, as desired.

ACKNOWLEDGMENTS

I am grateful to Daniel Dadush, who conjectured the existence of a reverse Minkowski theorem, and with whom much of the initial work was done [10]. I also thank Yael Eisenberg, Dan Simon, and Noah Stephens-Davidowitz for their comments on an earlier draft of this review.

FUNDING

Supported by the Simons Collaboration on Algorithms and Geometry, by a Simons Investigator Award from the Simons Foundation, 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.

REFERENCES

[1] S. G. Bobkov, On Milman's ellipsoids and M-position of convex bodies. In *Concentration, functional inequalities and isoperimetry*, pp. 23–33, Contemp. Math. 545, Amer. Math. Soc., Providence, RI, 2011.

[2] J.-B. Bost, Réseaux euclidiens, séries thêta et pentes, Exp. Bourbaki **1151** (2020), 1–59, 422.

[3] J. Bourgain, On the distribution of polynomials on high-dimensional convex sets. In *Geometric aspects of functional analysis (1989–90)*, pp. 127–137, Lecture Notes in Math. 1469, Springer, Berlin, 1991.

[4] Y. Chen, An almost constant lower bound of the isoperimetric coefficient in the KLS conjecture. *Geom. Funct. Anal.* **31** (2021), no. 1, 34–61.

[5] K.-M. Chung, D. Dadush, F.-H. Liu, and C. Peikert, On the lattice smoothing parameter problem. In *2013 IEEE Conference on Computational Complexity—CCC 2013*, pp. 230–241, IEEE Computer Soc., Los Alamitos, CA, 2013.

[6] H. Cohn, A. Kumar, S. D. Miller, D. Radchenko, and M. Viazovska, The sphere packing problem in dimension 24. *Ann. of Math. (2)* **185** (2017), no. 3, 1017–1033.

[7] J. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups*. Springer, New York, 1998.

[8] D. Cordero-Erausquin, M. Fradelizi, and B. Maurey, The (B) conjecture for the Gaussian measure of dilates of symmetric convex sets and related problems. *J. Funct. Anal.* **214** (2004), no. 2, 410–427.

[9] D. Dadush, *Integer programming, lattice algorithms, and deterministic volume estimation*. Ph.D. thesis, Georgia Institute of Technology, 2012.

[10] D. Dadush and O. Regev, Towards strong reverse Minkowski-type inequalities for lattices. In *57th Annual IEEE Symposium on Foundations of Computer Science—FOCS 2016*, pp. 447–456, IEEE Computer Soc., Los Alamitos, CA, 2016.

[11] M. Dutour Sikirić, A. Schürmann, and F. Vallentin, Inhomogeneous extreme forms. *Ann. Inst. Fourier (Grenoble)* **62** (2012), no. 6, 2227–2255.

[12] Y. Eisenberg, O. Regev, and N. Stephens-Davidowitz, Reverse Minkowski for the Epstein zeta function (in preparation).

[13] P. Epstein, Zur Theorie allgemeiner Zetafunctionen. *Math. Ann.* **56** (1903), no. 4, 615–644.

[14] T. Figiel and N. Tomczak-Jaegermann, Projections onto Hilbertian subspaces of Banach spaces. *Israel J. Math.* **33** (1979), no. 2, 155–171.

[15] A. Giannopoulos and E. Milman, M-estimates for isotropic convex bodies and their L_q-centroid bodies. In *Geometric aspects of functional analysis*, pp. 159–182, Lecture Notes in Math. 2116, Springer, Cham, 2014.

[16] D. R. Grayson, Reduction theory using semistability. *Comment. Math. Helv.* **59** (1984), no. 4, 600–634.

[17] V. Guruswami, D. Micciancio, and O. Regev, The complexity of the Covering Radius Problem. *Comput. Complexity* **14** (2005), no. 2, 90–121.

[18] T. C. Hales, A proof of the Kepler conjecture. *Ann. of Math. (2)* **162** (2005), no. 3, 1065–1185.

[19] G. Harder and M. S. Narasimhan, On the cohomology groups of moduli spaces of vector bundles on curves. *Math. Ann.* **212** (1975), no. 3, 215–248.

[20] I. Haviv, V. Lyubashevsky, and O. Regev, A note on the distribution of the distance from a lattice. *Discrete Comput. Geom.* **41** (2009), no. 1, 162–176.

[21] A. Heimendahl, A. Marafioti, A. Thiemeyer, F. Vallentin, and M. C. Zimmermann, Critical even unimodular lattices in the Gaussian core model. 2021, arXiv:2105.07868.

[22] R. Kannan and L. Lovász, Covering minima and lattice-point-free convex bodies. *Ann. of Math. (2)* **128** (1988), no. 3, 577–602.

[23] B. Klartag, On convex perturbations with a bounded isotropic constant. *Geom. Funct. Anal.* **16** (2006), no. 6, 1274–1290.

[24] D. R. Lewis, Ellipsoids defined by Banach ideal norms. *Mathematika* **26** (1979), no. 1, 18–29.

[25] S. Lovett and O. Regev, A counterexample to a strong variant of the polynomial Freiman–Ruzsa conjecture in Euclidean space. *Discrete Anal.* **8** (2017), 6.

[26] A. Magazinov, A proof of a conjecture by Haviv, Lyubashevsky and Regev on the second moment of a lattice Voronoi cell. *Adv. Geom.* **20** (2020), no. 1, 117–120.

[27] D. Micciancio and O. Regev, Worst-case to average-case reductions based on Gaussian measures. *SIAM J. Comput.* **37** (2007), no. 1, 267–302 (electronic).

[28] E. Milman, On the mean-width of isotropic convex bodies and their associated L_p-centroid bodies. *Int. Math. Res. Not. IMRN* **11** (2015), 3408–3423.

[29] V. D. Milman and G. Pisier, Gaussian processes and mixed volumes. *Ann. Probab.* **15** (1987), no. 1, 292–304.

[30] H. Minkowski, *Geometrie der Zahlen*. B.G. Teubner, 1910.

[31] G. Pisier, Holomorphic semigroups and the geometry of Banach spaces. *Ann. of Math. (2)* **115** (1982), no. 2, 375–392.

[32] G. Pisier, *The volume of convex bodies and Banach space geometry*. Cambridge Tracts in Math. 94, Cambridge University Press, Cambridge, 1989.

[33] O. Regev and N. Stephens-Davidowitz, A reverse Minkowski theorem. In *STOC'17—Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, pp. 941–953, ACM, New York, 2017.

[34] O. Regev and N. Stephens-Davidowitz, A reverse Minkowski theorem for integral lattices (in preparation).

[35] P. Sarnak and A. Strömbergsson, Minima of Epstein's zeta function and heights of flat tori. *Invent. Math.* **165** (2006), no. 1, 115–151.

[36] U. Shapira and B. Weiss, Stable lattices and the diagonal group. *J. Eur. Math. Soc. (JEMS)* **18** (2016), no. 8, 1753–1767.

[37] O. N. Solan, Intersections of diagonal orbits. 2016, arXiv:1612.08765.

[38] U. Stuhler, Eine Bemerkung zur Reduktionstheorie quadratischer Formen. *Arch. Math. (Basel)* **27** (1976), no. 6, 604–610.

[39] J. van der Corput, Verallgemeinerung einer Mordellschen Beweismethode in der Geometrie der Zahlen, Zweite Mitteilung. *Acta Arith.* **2** (1936), no. 1, 145–146.

[40] M. S. Viazovska, The sphere packing problem in dimension 8. *Ann. of Math. (2)* **185** (2017), no. 3, 991–1015.

[41] R. Zamir and M. Feder, On lattice quantization noise. *IEEE Trans. Inf. Theory* **42** (1996), no. 4, 1152–1159.

ODED REGEV

Courant Institute of Mathematical Sciences, 251 Mercer St., New York, NY 10012, USA, regev@cims.nyu.edu