A NOTE ON SPHERE PACKINGS IN HIGH DIMENSION

AKSHAY VENKATESH

Abstract. We improve on the lower bounds for the optimal density of sphere packings. In all sufficiently large dimensions the improvement is by a factor of at least $10,000$; along a sparse sequence of dimensions n_i we improve the density by roughly $\log\log n_i$.

1. Introduction

Minkowski proved (cf. [6]) that there is an origin-centered ellipsoid $E \subset \mathbf{R}^n$ of volume 1, containing no nonzero integer vector (that is to say: $E \cap \mathbf{Z}^n = \{0\}$). Here, by *origin-centered ellipsoid*, we mean the image under a linear transformation of the standard unit ball. Write c_n for the largest volume of such an ellipsoid, that is to say:

$$c_n = \sup\{\text{volume}(E) : \ E \text{ is an origin-centered ellipsoid and } E \cap \mathbf{Z}^n = \{0\}\}.$$

The first substantial improvement on Minkowski's work was given by Rogers in 1947 (see [11]): he showed that $c_n > 0.73n$ for large enough n. Subsequent work – for example [4, 1, 17]; see also [5, 9] – have improved the constant modestly: it is known by work of K. Ball [1] that always

$$c_n \geq 2(n-1)$$

and $c_n > 2.2n$ when n is divisible by 4 (Vance [17]). It is striking that the quoted papers use quite different methods and yet all arrive at the same linear improvement on Minkowski's bound.

These results yield the best known lower bounds on the sphere packing problem. Namely, let S be the ball of volume 1 centered at the origin. We may reformulate Minkowski's result as claiming the existence of a lattice $\Lambda \subset \mathbf{R}^n$ of covolume 1 so that $\Lambda \cap S = \{0\}$. The translates $\lambda + \frac{S}{2} : \lambda \in \Lambda$ are then disjoint, so Minkowski's result furnishes a periodic sphere packing of density 2^{-n}. Similarly, Ball's result yields a sphere packing of density at least $2(n-1)2^{-n}$ in every dimension. This far surpasses the density of any "explicitly known" sphere packing.

Our goal here is to improve the linear bound by a large constant, and also to show that in many dimensions the asymptotic growth can be improved:

Theorem 1. *There exist infinitely many dimensions n for which $c_n > \frac{1}{2}n \cdot \log\log n$. Also, in every sufficiently large dimension, $c_n > 65963n$.*

The constant 65963 here could be replaced by any number less than $2\frac{\sinh^2(\pi e)}{\pi^2 e^3}$.

The two statements of the theorem are proved in different ways but with the same (naive) idea: One considers random lattices but constrained in some algebraic way. In the first case, one considers random lattices with automorphism group containing $\mathbf{Z}/k\mathbf{Z}$. The improvement comes from the fact that the degree of the field extension $[\mathbf{Q}(\mu_k) : \mathbf{Q}]$ can be as small as $\frac{k}{\log\log k}$; here $\mathbf{Q}(\mu_k)$ denotes the field obtained by

adjoining all kth roots of unity to $\mathbf{Q}$. In the second case, one considers "random orthogonal lattices": roughly speaking, a random lattice with fixed discriminant but subject to the constraint that all lengths are integers. The improvement comes from the fact that integrality sometimes forces vectors to be longer than they otherwise would be; we refer to §3.1 for further discussion of this effect. One needs to tweak the free parameter (the discriminant) to get the most out of it.

One can ask the more general question of packing translates of a general convex body. The theorem uses two special properties of the sphere: it is preserved by a large subgroup of linear automorphisms and its boundary is defined by a polynomial equation.

Our improvement is very modest, in particular if one takes into account that the best known upper bounds are *exponentially* greater [7]. However, it seems to me quite likely that, in the context of lattice packings, Minkowski's bound differs from the truth only by a polynomial in n. Thus even modest improvements are hopefully not without interest.

I found this result while trying to understand the geometry of the space of lattices in $\mathbf{R}^n$ in the limit when $n \to \infty$. This problem, and its relationship to the sphere-packing question, seems very interesting, and I hope to return to it elsewhere.

Acknowledgements. I am most grateful to Abhinav Kumar for helpful remarks and catching errors. I am also very grateful to the referee for a very careful reading and many helpful suggestions and corrections.

2. Random lattices with an action of a cyclic group

We give the proof of the first assertion of the theorem.

Let K be the cyclotomic field $\mathbf{Q}(\mu_n)$, let $\mathfrak{o}$ be the ring of integers in K, and let $V = K^2$, considered as a 2-dimensional vector space over K. We put $V_{\mathbf{R}} := V \otimes_{\mathbf{Q}} \mathbf{R}$; it is a vector space over $\mathbf{R}$ of dimension $2\varphi(n)$, where $\varphi(n)$ is the number of integers $1 \leq i \leq n$ that are relatively prime to n.

Let $\Lambda_0 = \mathfrak{o}^2 \subset V_{\mathbf{R}}$; it is a lattice in $V_{\mathbf{R}}$. Then the group μ_n of nth roots of unity in K acts on $V_{\mathbf{R}}$ and this action preserves the lattice Λ_0. Let q_0 be a positive definite quadratic form on $V_{\mathbf{R}}$ stable by $\mu_n \subset K^\times$. It exists by "averaging."

Let $G = \mathrm{SL}_2(K \otimes \mathbf{R})$. It acts naturally on $V_{\mathbf{R}}$. Let $\Gamma = \mathrm{SL}_2(\mathfrak{o}) \subset G$. Endow G/Γ with the G-invariant probability measure, which we denote by μ; endow $V_{\mathbf{R}}$ with the Lebesgue measure for which Λ_0 has covolume 1.

For $f \in C_c(V_{\mathbf{R}})$ and $\Lambda \subset V_{\mathbf{R}}$ any lattice, we put

$$E_f(\Lambda) = \sum_{v \in \Lambda - \{0\}} f(v).$$

Lemma 1. *With these notations, we have*

$$\int_{g \in G/\Gamma} E_f(g\Lambda_0) d\mu(g) = \int_{V_{\mathbf{R}}} f(x) dx.$$

Such results are well-known; we give a proof for completeness below. In outline, one sees by "unfolding" that the left-hand side is proportional to $\int f$: the key point here is that for *every* $v \in \Lambda_0 - \{0\}$, the orbit $G.v$ is all of $V_{\mathbf{R}}$, up to a set of measure 0. We compute the constant of proportionality by taking f to be (a continuous approximation to) the characteristic function of a large ball of radius R and taking R to ∞.

Thus, if the ellipsoid $E = \{x \in V_{\mathbf{R}} : q_0(x) \leq T\}$ has volume less than n, it follows from (*) that there exists a lattice $\Lambda = g\Lambda_0$ so that the size of $\Lambda \cap E - \{0\}$ is less than n; since E is μ_n invariant and μ_n acts without fixed points, $\Lambda \cap E = \{0\}$.

Thus we have proved that there is a lattice Λ of covolume 1 in dimension $2\varphi(n)$ and an ellipsoid of volume $n - \varepsilon$ so that $\Lambda \cap E = \{0\}$. This means, in the notation of the introduction, that $c_{2\varphi(n)} \geq n$.

If we take $n = \prod_{p<X} p$ to be the product of all primes less than X, then $\frac{\log n}{X} \to 1$ as $X \to \infty$ (for short we write $\log n \sim X$) and also $\varphi(n) = n \cdot \prod_{p<X}(1 - p^{-1}) \sim e^{-\gamma} \frac{n}{\log\log n}$. Here $\gamma = 0.577\ldots$ is Euler's constant, and we have used Merten's theorem [10]. This proves the first assertion of the theorem.

Proof. (of Lemma 1) As we have mentioned, such results are "well-known"; we make no claim to originality, and this proof is essentially the same as that of Siegel [12] for the analogous question with $\mathrm{SL}_n(\mathbf{Z})$ (see especially final remarks of that paper).

Take R a real number with $R \geq 1$. Let f_R be the characteristic function of a ball $q_0 \leq R^2$ and let $E_R = E_{f_R}$ and $\overline{E_R} = \frac{E_R}{\int f_R}$. We will in a moment show that

$$\int_{G/\Gamma} E_R < \infty \tag{1}$$

and indeed, we shall show that $\overline{E_R}$ is dominated, uniformly in R, by an integrable function on G/Γ. In particular, E_f is integrable for any $f \in C_c(V_{\mathbf{R}})$.

Let $v_1, \ldots, v_k, \ldots$ be a complete set of representatives (possibly infinite) for Γ-orbits on $\mathfrak{o}^2$; for each i, let Γ_i be the stabilizer of v_i in Γ. Then

$$\int_{G/\Gamma} E_f(g\Lambda_0) d\mu(g) = \int_{G/\Gamma} d\mu(g) \sum_{i, \gamma \in \Gamma/\Gamma_i} f(g\gamma v_i) = \sum_i \int_{G/\Gamma_i} d\mu(g) f(gv_i),$$

where the measure on G/Γ_i is that induced by μ.

Now, the map $G/\Gamma_i \to V_{\mathbf{R}}$ is easily seen to be proper; it pushes forward the measure on G to some positive multiple of the measure on $V_{\mathbf{R}}$: that is to say, $\int_{G/\Gamma_i} f(gv_i) d\mu(g) = c_i \int_{V_{\mathbf{R}}} f(x)dx$ for some $c_i > 0$. Indeed, the left-hand side – restricted to continuous functions of compact support on the orbit Gv_i of v_i in $V_{\mathbf{R}}$ – defines a G-invariant measure on this orbit; up to scaling, Lebesgue measure is the only possibility.

Now, for an arbitrary nonzero $f \in C_c(\mathbf{R})$ with $f \geq 0$, it follows from (1) that $\int_{G/\Gamma} E_f < \infty$, so also $\sum c_i < \infty$. Write $c = \sum c_i$, so that

$$\int E_f(g\Lambda_0) d\mu(g) = c \int f(x)dx. \tag{2}$$

A simple approximation argument shows that (2) continues to hold for $f = f_R$. So $\int \overline{E_R} = c$ for any R; since $\overline{E_R} \to 1$ pointwise, we take limits in (2) to conclude that $c = 1$. This limiting process is justified by the remark after (1).

It remains to show (1), as well as the subsequent statement concerning $\overline{E_R}$. Write $d = \varphi(n)$, so that $K \otimes \mathbf{R}$ is isomorphic to $\mathbf{C}^{\oplus d/2}$. Fix a compact subset $\Omega \subset K \otimes \mathbf{R}$ and let U be a maximal compact subgroup of $\mathrm{SL}_2(K \otimes \mathbf{R})$.

For $t \in (K \otimes \mathbf{R})^\times$ and $x \in K \otimes \mathbf{R}$ we define elements of $\mathrm{SL}_2(K \otimes \mathbf{R})$ via

$$a(t) = \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix}, \; n(x) = \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}.$$

There is a natural inclusion $\mathbf{R} \overset{x \mapsto 1 \otimes x}{\hookrightarrow} K \otimes \mathbf{R}$ and also a "norm" map Norm : $K \otimes \mathbf{R} \to \mathbf{R}$ i.e., the product of squared absolute values in each coordinate. Let $(K \otimes \mathbf{R})^{(1)}$ be the kernel of this norm map.

According to reduction theory (see [2, §12, §13] for a general formulation, which covers the present context) there is a finite subset $F \subset \mathrm{SL}_2(K)$, some positive real $T > 0$ and compact sets $\Omega \subset K \otimes \mathbf{R},\ \Omega' \subset (K \otimes \mathbf{R})^{(1)}$ such that the "Siegel set"

$$\mathfrak{S}_T := U \cdot \{a(tt') : t \in (T, \infty), t' \in \Omega'\} \cdot \{n(x) : x \in \Omega\} \cdot F$$

surjects onto G/Γ.

Take $\kappa \in U,\ t \in (T, \infty),\ t' \in \Omega',\ \omega \in \Omega, f \in F$. Then the lattice

$$\Lambda := \kappa a(tt') n(\omega) f \cdot \mathfrak{o}^2$$

– considered as a lattice in $V_{\mathbf{R}}$ – has the property that

$$|E_R(\Lambda)| \ll_d (1 + \frac{R}{t})^d (1 + Rt)^d \text{ and } |\overline{E_R}(\Lambda)| \ll_d (1 + t)^d. \tag{3}$$

In fact, we may find an integer M so that $f \cdot \mathfrak{o}^2 \subset M^{-1}\mathfrak{o}^2$ for every $f \in F$. Our claim (3) will follow from the following fact: $\kappa a(tt')n(\omega) \cdot \mathfrak{o}^2$ – again, considered as a lattice in $V_{\mathbf{R}}$ – has a reduced basis consisting of d vectors of length $\asymp t$ and d vectors of length $\asymp t^{-1}$. Indeed, $\kappa a(tt')n(\omega) = \kappa a(t')n(t^{-2}\omega)a(t)$ and $\kappa a(t')n(t^{-2}\omega)$ lies in a compact subset of G depending only on T, ω. Our assertion is reduced to the corresponding assertion about the successive minima for the lattice $a(t).\mathfrak{o}^2 \subset V_{\mathbf{R}}$, where it is easy to check.

The restriction of Haar measure to the set $\mathfrak{S}$ is of the form

$$du \cdot d^\times t' \cdot t^{-2d} d^\times t \cdot dx,$$

where $du, d^\times t', d^\times t, dx$ are respectively Haar measures on $U, (K \otimes \mathbf{R})^{(1)}, \mathbf{R}^\times$, and the additive group of $K \otimes \mathbf{R}$. Now (1), and the statement on $\overline{E_R}$ after (1), follow at once from (3), since $\int_{t>1} (1+t)^d t^{-2d} d^\times t < \infty$. □

3. Random orthogonal lattices

We now give the proof of the second assertion of the main theorem. It is significantly more involved and accordingly we give in §3.1 a fairly complete discussion of the main ideas.

We work with quadratic forms in n variables, or lattices in $\mathbf{R}^n$. It is convenient to set $k = n/2 \in \frac{1}{2}\mathbf{Z}$. We write simply $k!$ for $\Gamma(k+1)$, even if k is not integral. We write $A \sim B$ when the ratio A/B approaches 1 as the dimension approaches ∞. The symbol $\approx$ is occasionally used but without a mathematically precise meaning: it should be understood simply as the colloquial "is approximately equal to."

In high dimension $n = 2k$, the volume of a sphere of radius 1 is $\pi^k/k!$, which is very small. We will be more interested of spheres of volume around 1, which happens at radius $\approx \sqrt{k/(\pi e)}$. All the "action" will occur on spheres of radius very close to this, indeed, when the square of the radius is $\frac{k}{\pi e} + O(\log k)$.

3.1. **Notation and discussion.** Recall that the jth successive minima γ_j of a quadratic form q on a free abelian group Λ is, by definition, the smallest number for which $\{\mathbf{x} \in \Lambda : \sqrt{q(\mathbf{x})} \leq \gamma_j\}$ spans a real subspace of dimension $\geq j$.

If Λ is a lattice equipped with a quadratic form q on $\Lambda \otimes \mathbf{R}$, with successive minima $\gamma_1 \leq \cdots \leq \gamma_n$, then Minkowski proved [1] that there is a lattice $\Lambda' \subset \Lambda \otimes \mathbf{R}$, of the same covolume as Λ, with no nonzero vectors in the sphere $\sqrt{q(\mathbf{x})} < \Gamma$. Here $\Gamma := (\gamma_1 \dots \gamma_n)^{1/n}$ is the geometric mean of the γ_i.

It's convenient to define the jth volume-minima V_j to be the volume of the set $\sqrt{q} \leq \gamma_j$, and to think about the volume-minima instead of the γ_j. One reason is that the volume-minima are invariant under the rescaling $q \leftarrow Aq$, for any positive real A; so thinking about volume-minima helps us compare more easily quadratic forms of different discriminant. Phrased in terms of volume-minima, Minkowski's result says:

> There is a lattice Λ' of the same covolume as Λ, such that $\Lambda' - \{0\}$ is disjoint from an ellipsoid of volume $\sqrt[n]{V_1 \dots V_n}$.

What do the volume-minima behave like for a "random" lattice of covolume 1? The answer is independent of the quadratic form q and is given by a paper of Södergren [15, §6] : in large dimensions, the first few volume-minima of a random lattice behaves like a Poisson point process on the line with mean $1/2$. In particular, the expected value of the first, second, third ... volume-minima is $2, 4, 6, \dots$. Thus one might expect – applying Minkowski's result, and assuming that the validity of Södergren's result extends to all minima – one would obtain a lattice of covolume 1 disjoint from an ellipsoid of volume

$$\sqrt[n]{2 \cdot 4 \cdot 6 \cdot 8 \cdot \dots \cdot (2n)} \approx (2n)/e.$$

This is precisely what Rogers proved [11]. A direct way of proving it would be to push through the above analysis to show that the jth volume-minima typically does not differ too far from $2j$.

A very similar phenomenon happens if, instead of choosing a random lattice with respect to the $\mathrm{SL}_n(\mathbf{R})$-invariant probability measure, we take $\mathbf{Z}^n$ and a random *integral* quadratic form Q of a fixed discriminant D. (To make this precise, one samples the quadratic form Q from a genus $\mathcal{Q}$ of quadratic forms to be defined shortly.) For random Q one has a pretty good idea of the size of the successive minima of Q. The main difference with the prior discussion is that the requirement $\gamma_j^2 \in 2\mathbf{Z}$ puts restrictions on the volume-minima; roughly speaking, some get rounded up and some get rounded down. In order to make this work, we need to choose D so that the effect of forcing integrality is to "round up" most of the γ_j^2 rather than "round down."

We now implement this; although the analysis looks ugly, all the phenomena are already captured in the discussion above.

Remark. Here is a plausible strategy for doing better. It is overwhelmingly likely, it seems, that for any $\delta < 1$ and with $r = [\delta n]$, the rth minima γ_r has the property that the size of the set $\{\sqrt{q} \leq \gamma_r\}$ is as small as it can be – namely, $2r$ – and moreover the vectors $\mathbf{x}_1, \dots, \mathbf{x}_r$ (choose one from each pair $\pm\mathbf{x}$) inside this sphere may be extended to a $\mathbf{Z}$-basis $\mathbf{x}_1, \dots, \mathbf{x}_n$ of the ambient lattice. In that case the lattice $\{\sum a_i \mathbf{x}_i : \sum a_i \equiv 0 \bmod 2\}$ has covolume twice that of Λ and possesses

[1] This is the same argument by which Minkowski reduces the theorem on successive minima to existence of vectors in a large enough balanced convex set. It would be interesting to understand the geometric effect of the (not well defined) operation $\Lambda \mapsto \Lambda'$ on the space of lattices. It seems like it would be very strongly "contracting."

no vectors in the sphere of volume V_r. If this were to be carried through in the setup considered below, this should lead to a significant improvement in the constant.

3.2. **A genus of quadratic forms.** For any positive definite quadratic form Q on $\mathbf{Z}^n$, the discriminant of Q is defined to be the determinant of the Gram matrix $\langle e_i, e_j\rangle$ of the associated bilinear form $\langle x, y\rangle := \frac{Q(x+y)-Q(x)-Q(y)}{2}$. Then the volume $V(T)$ of the set $\{Q(\mathbf{x}) \leq T\}$ satisfies

$$V(T) = \frac{1}{\sqrt{\mathrm{disc}(Q)}} \frac{\pi^k T^k}{k!}.$$

Write $n = 8a+b$ with $1 \leq b \leq 8$, and suppose D is an integer for which $2^b | D$. We call such D admissible. Let $\mathcal{Q}$ be a set of representatives for isomorphism classes in the genus of the quadratic form

$$E_8^{\oplus a} \oplus \langle 2x^2\rangle^{\oplus(b-1)} \oplus \langle \frac{D}{2^{b-1}} x^2\rangle.$$

(Here E_8 is the quadratic form corresponding to the E_8 lattice; see [3, §8, Chapter 4] for background.)

The pertinent features of $\mathcal{Q}$ are that:

- every $q \in \mathcal{Q}$ is even (i.e. $q(\mathbf{Z}^n) \subset 2\mathbf{Z}$);
- every $q \in \mathcal{Q}$ has discriminant D.

Let $N_Q(m)$ be the number of representations of an even integer m by Q. We introduce the (weighted) average representation number:

$$N_{\mathcal{Q}}(m) = \frac{\sum_{\mathcal{Q}} N_Q(m) |\mathrm{Aut}(Q)|^{-1}}{\sum_{\mathcal{Q}} |\mathrm{Aut}(Q)|^{-1}}$$

We will require the following estimate:

Lemma 2.

$$N_{\mathcal{Q}}(m) = \frac{2k m^{k-1} \pi^k}{k! \sqrt{D}} \cdot (1 + O(2^{-k/2})) \tag{4}$$

Proof. The *mass formula of Minkowski–Siegel–Smith* (see [8, Chapter 6]) gives $N_{\mathcal{Q}}(m) = \prod_p \nu_p(m)$. Here $\nu_p(m)$ is the density, at m, of the pushforward of (additive) Haar probability measure on $\mathbf{Z}_p^n$ via $Q : \mathbf{Z}_p^n \to \mathbf{Z}_p$ for p finite; for p infinite, we replace $\mathbf{Z}_p$ by $\mathbf{R}$ and Haar probability measure by Lebesgue measure.

In particular,

$$\nu_\infty = \frac{d}{dt}\Big|_{t=m} V(t),$$

and so $\nu_\infty = \frac{k\pi^k m^{k-1}}{\sqrt{D} k!}$. As for $p \neq \infty$, we have, whenever $m \in 2\mathbf{Z}$

$$\nu_p(m) = \begin{cases} 1, & (p, 2mD) = 1 \\ 1 + O(p^{5-k}), & p \neq 2 \\ 2 + O(2^{-k}), & p = 2. \end{cases} . \tag{5}$$

The implicit constants in (5) do not depend on D. The fact that $\nu_2(m)$ is very close to 2 arises from the fact that the quadratic form only represents *even* values, and each such value is represented twice as often as one might expect.

To prove (5) for odd p, we note that if q, q' are quadratic forms with local densities ν_p, ν'_p, and V_p is the local density for $q \oplus q'$, then

$$\sup_{m \in \mathbf{Z}_p} |V_p(m) - 1| \leq \sup_{m \in \mathbf{Z}_p} |\nu_p(m) - 1|$$

because the measure $V_p(m)dm$ is obtained by additive convolution of $\nu_p(m)dm$ and $\nu'_p(m)dm$.

But, for the quadratic form $E_8^{\oplus a}$, the local density at p for representations of the integer $2m$ equals

$$\nu_p(E_8^{\oplus a}, 2m) = \left(\sum_{i=0}^{r} p^{-i(4a-1)} \right) \cdot (1 - p^{-4a}). \tag{6}$$

where r is the highest power of p dividing m. This is well-known; for p not equal to 2 it is [13, Hilfsatz 16]; for $p = 2$ more general results are derived by T. Yang [18].[2]

Thus $|\nu_p(m) - 1|$ is bounded by $O(p^{1-4a})$, and $4a - 1 \geq k - 5$.

The proof for even p is similar, with the convolutions taking place on the additive group $2\mathbf{Z}_2$ rather than on $\mathbf{Z}_2$. □

Now we study the behavior of $N_{\mathcal{Q}}(m)$ for m near the "transitional point": the point where $N_{\mathcal{Q}}(m)$ exceeds $2n$.

Let μ be the smallest real value for which $\frac{2km^{k-1}\pi^k}{k!\sqrt{D}}$ (that is, the approximation to $N_{\mathcal{Q}}(m)$ furnished above) exceeds $2n = 4k$, i.e. μ is the solution to

$$\frac{2k\mu^{k-1}\pi^k}{k!\sqrt{D}} = 4k.$$

Roughly μ is near $\frac{k}{\pi e}$. We will need a more precise version. Using Stirling's formula in the version $x! = \sqrt{2\pi x} \cdot x^x e^{-x}(1 + O(x^{-1}))$, with $x = k - 1$, we see:

$$\begin{aligned} \mu &= (2k!\sqrt{D}\pi^{-k})^{1/k-1} \\ &= (2k\sqrt{\frac{2D(k-1)}{\pi}})^{1/k-1} \cdot \frac{k-1}{\pi e}(1 + O(k^{-2})) \\ &= (k-1)/\pi e + \frac{1}{\pi e}\log\sqrt{\frac{16k^2D(k-1)}{2\pi}} + O(\frac{\log^2(k)}{k}) \quad \text{for } D < k. \end{aligned} \tag{7}$$

the assumption $D < k$ in the last equation is simply to give a nice form to the error term.

Therefore, under this assumption that $D < k$, we have in particular $\mu \sim k/\pi e$ and the volume $V(\mu)$ satisfies

$$\frac{V(\mu)}{2n} = \frac{1}{2n\sqrt{D}} \frac{\pi^k \mu^k}{k!} = \frac{1}{2n\sqrt{D}} 2\sqrt{D}\mu \sim (2\pi e)^{-1}. \tag{8}$$

Let m_0 be the largest even integer less than μ, and $m_1 = m_0 + 2$ the smallest even integer $\geq \mu$. This is a "transitional point": we expect that, for "most" $Q \in \mathcal{Q}$, $\{\mathbf{x} \in \mathbf{Z}^n : Q(\mathbf{x}) \leq m_0\}$ doesn't contain a basis for $\mathbf{R}^n$, but $\{\mathbf{x} \in \mathbf{Z}^n : Q(\mathbf{x}) \leq m_1\}$ usually does.

[2]The quoted reference [18] discusses a much more general case. One may alternately use the "Siegel-Weil" formula, which identifies the product of local densities with a Fourier coefficient of an Eisenstein series of weight $4k$ for $\mathrm{SL}_2(\mathbf{Z})$, together with the knowledge of $p \neq 2$, to deduce the values for $p = 2$.

3.3. **The proof.** We follow a method used by Rogers [11]: it avoids explicitly verifying that $N_Q(m)$ are usually near their mean values $N_{\mathcal{Q}}(m)$, which makes the proof shorter but also less revealing. We will suppose in all our estimates that $D < k$, so that we can apply (7); this will indeed be the case for our final application. Throughout the proof we use the abbreviation $C = e^{\pi e}$.

When m is near the transitional point m_0, an increase $m \leftarrow m+1$ increases $V(m)$ by a multiplicative factor $\left(1+\frac{1}{m}\right)^k \approx e^{\pi e} = C$. A similar result holds true for $N_{\mathcal{Q}}(m)$. Thus, putting $s = \mu - m_0 \in (0,2]$, we expect

$$N_{\mathcal{Q}}(m_1) \approx (2n)\cdot C^{2-s}, \quad N_{\mathcal{Q}}(m_1-2) \approx (2n)\cdot C^{-s}, \quad N_{\mathcal{Q}}(m_1-4) \approx (2n)\cdot C^{-2-s}$$

and so on; also, $V(m_1)/V(m_1-2) \approx C^2$ and $V(m_1)/V(m_1-4) \approx C^4$ and so on.

One checks easily that these approximations are good in the sense that, for $0 \le j \le (\log k)^2$, say, we have

$$\frac{1}{2n} N_{\mathcal{Q}}(m_1-2j)\log\frac{V(m_1)}{V(m_1-2j)} = C^{2-2j-s}\log(C^{2j})\left(1+O(k^{-1/2})\right). \tag{9}$$

We verify this at the end of the proof. The constant in $O(k^{-1/2})$ may depend on D.

Let s_0 be the solution to $C^{-s} = \frac{(1-C^{-2})^2}{2\log C}$. Numerically, $s_0 \approx 0.3323\ldots$. This is chosen so that $\sum_{j=1}^{\infty} \log(C^{2j})\cdot C^{2-2j-s_0} = 1$; indeed, this sum is

$$(0+\log(C^2)C^{-s_0} + \log(C^4)C^{-s_0-2} + \ldots) = (2\log C)\cdot\frac{C^{-s_0}}{(1-C^{-2})^2}.$$

Now *it is possible to choose D so that s is very close to s_0*, as one sees from (7). More exactly:

Lemma 3. *For any $\delta < 1$ there exists a constant $D_0(\delta)$ with the following property:*

In any sufficiently large dimension, there exists an admissible $D \le D_0(\delta)$ such that $\delta \le C^{s-s_0} \le \delta^{-1}$ and

$$\sum_{\text{even } m<m_1} N_{\mathcal{Q}}(m)\log\frac{\delta V(m_1)}{V(m)} < 2n. \tag{10}$$

We give the proof below in §3.4, to avoid interrupting the flow of the exposition.

Fix $1/2 < \delta < 1$; we will let it approach 1 at the end of the argument. Choosing D as in Lemma 3, there exists a quadratic form $Q_0 \in \mathcal{Q}(D)$ for which

$$\sum_{\text{even } m<m_1} N_{Q_0}(m)\log\frac{\delta V(m_1)}{V(m)} < 2n.$$

All the summands are non-negative, as long as the dimension is large enough; we assume that this is so in what follows. So we may discard any subset of terms on the left-hand side and still the sum is less than $2n$.

Let V_j be the jth volume-minima for $(\mathbf{Z}^n, Q_0)$, that is to say, the volume of the ellipsoid $Q_0(\mathbf{x}) \le \gamma_j^2$ where γ_j are the usual minima. Let j be the largest index for which $V_j < V(m_1)$, and set $V' = \delta V(m_1)/e$. Then:

$$\sum_{i=1}^{j} 2(1+\log\frac{V'}{V_i}) < 2n,$$

and so

$$\sum_{i=1}^{j} \log \frac{V'}{V_i} < (n-j).$$

The remaining $V_{j+1}, \dots, V_n$ all are $\geq V(m_1)$; in particular, $\log \frac{V'}{V_i} \leq -1$ for $i > j$. So

$$\sum_{i \leq n} \log \frac{V'}{V_i} < 0,$$

i.e. $\sqrt[n]{V_1 \dots V_n} \geq V'$. Minkowski's theorem [6], as quoted earlier, implies that there is a lattice of covolume 1 disjoint from the sphere of volume V'.

But

$$V' = \frac{\delta V(m_1)}{e} \sim \delta C^{2-s} \frac{V(\mu)}{e} \sim \left(\delta C^{s_0 - s}\right) \frac{C^{2-s_0}}{2\pi e^2} 2n \geq \delta^2 \frac{\sinh^2(\pi e)}{\pi^2 e^3} 2n$$

where we used:

- the previously noted fact – see (8) – that $\frac{V(\mu)}{2n} \sim (2\pi e)^{-1}$;
- the assumption that C^{s-s_0} lies between δ and δ^{-1};
- the fact that C^{2-s_0} equals, by definition, $\frac{(C-C^{-1})^2}{2\log C} = \frac{2\sinh^2(\pi e)}{\pi e}$.

Since δ can be made arbitrarily close to 1, the proof is complete.

3.4. **Proof of** (9) **and Lemma 3.**

Proof. (of (9)): Recall that we are supposing that $D < k$, so that (7) applies.

Now, if $j \leq (\log k)^2$, we have

$$\begin{aligned} \frac{N_{\mathcal{Q}}(m_1 - 2j)}{2n} &= (1 + O(2^{-k/2})) \left(\frac{\mu - s + 2 - 2j}{\mu}\right)^{k-1} \\ &= (1 + O(2^{-k/2})) \exp\left(\log(1 + \frac{2 - 2j - s}{\mu})(\pi e \mu + O(\log k))\right) \end{aligned}$$

which is $(1 + O(k^{-1/2})) \cdot C^{2-2j-s}$ under our assumptions. As for the second factor $\log \frac{V(m_1)}{V(m_1 - 2j)} = \left(-k \log(1 - \frac{2j}{m_1})\right)$, it is given by:

$$\frac{2jk}{m_1} + O(k^{-1/2}) = 2\pi e j + O(k^{-1/2}) = \log(C^{2j}) + O(k^{-1/2}).$$

This concludes the proof of (9), but for later use let us note a simple bound, valid when $j > (\log k)^2$:

$$\log \frac{V(m_1)}{V(m_1 - 2j)} \frac{N_{\mathcal{Q}}(m_1 - 2j)}{2n} = O(k^{-2}). \tag{11}$$

Indeed, $\log \frac{V(m_1)}{V(m_1 - 2j)} < \log \frac{V(m_1)}{V(2)} < k \log m_1 < O(k^2)$; also $\frac{N_{\mathcal{Q}}(m_1 - 2j)}{2n} = O(k^{-10})$. □

Proof. (of Lemma 3):

Let us agree to write $\{x\}'$ for the fractional part of x if x is not an integer, and 1 if x is an integer.

Then $s = 2\{\mu/2\}'$; by (7) we may write

$$s = 2\{\alpha + \frac{\log D}{4\pi e} + O(\frac{\log^2(k)}{k})\}', \tag{12}$$

where α depends only on the dimension. Recall that we must assume that $D < k$ for the validity of the error term in this estimate.

Choose ε so small that $C^{s-s_0} \in (1, \delta^{-1})$ whenever $s \in (s_0, s_0 + 10\varepsilon)$. This choice depends only on δ.

Next, choose D_0 so that the set $2\{\log(D)/4\pi e\} : D \leq D_0, 256|D\}$ is ε-dense in the interval $[0,1]$. (We say a set $S \subset [0,1]$ is ε-dense if any $x \in [0,1]$ satisfies $|x - s| < \varepsilon$ for some $s \in S$.) The condition that 256 divides D is to ensure that D is admissible. Again, D_0 depends only on δ.

Then, in every sufficiently large dimension – that is, taking k so large that the factor $O(\log^2(k)/k)$ in (12) is less than ε – we may choose admissible $D \leq D_0$ in such a way that $C^{s-s_0} \in (1, \delta^{-1})$.

With this choice of D, we have

$$\sum \log(C^{2j}) C^{2-2j-s} = C^{s_0 - s} \in (\delta, 1). \tag{13}$$

It remains to analyze (10), i.e. $\sum_{\text{even } m < m_1} N_{\mathcal{Q}}(m) \log \frac{\delta V(m_1)}{V(m)}$, and show that it is less than $2n$ in large enough dimension. That follows from the following three facts, all valid in any large enough dimension:

$$\begin{aligned}
\frac{1}{2n} \sum_{j \geq (\log k)^2} N_{\mathcal{Q}}(m_1 - 2j) \log \frac{V(m_1)}{V(m_1 - 2j)} &= O(k^{-1/2}) \\
\frac{1}{2n} \sum_{j < (\log k)^2} N_{\mathcal{Q}}(m_1 - 2j) \log \frac{V(m_1)}{V(m_1 - 2j)} &< 1 + O(k^{-1/2}), \\
\frac{1}{2n} \sum_{\text{even } m < m_1} N_{\mathcal{Q}}(m) \log \delta &< C^{-3} \log \delta.
\end{aligned}$$

Indeed, the first follows from (11); the second claim from (9) and (13); in the third claim, all terms on the left are negative and the term with $m = m_1 - 2$ is less than $C^{-3} \log \delta$. □

References

[1] K. Ball, *A lower bound for the optimal density of lattice packings.* Internat. Math. Res. Notices 10 (1992), 217–221.

[2] *Introduction aux groupes arithmtiques.* Publications de l'Institut de Mathmatique de l'Universit de Strasbourg, XV. Actualits Scientifiques et Industrielles, No. 1341 Hermann, Paris 1969.

[3] J. Conway and N. Sloane. *Sphere packings, lattices and groups.* Grundlehren der Mathematischen Wissenschaft, 290. Springer-Verlag, New York, 1999.

[4] H. Davenport and C. Rogers, *Hlawka's theorem in the geometry of numbers.* Duke Math. J. (1947), 367–375.

[5] Gaborit and Zémor. *On the construction of dense lattices with a given automorphisms group.* Ann. Inst. Fourier (Grenoble) 57 (2007), no. 4, 10511062.

[6] Hlawka, Edmund. *Zur Geometrie der Zahlen.* Math. Z. 49, (1943). 285312.

[7] Kabatjanskii and Levenshtein. *Bounds for packings on the sphere and in space.* Problemy Peredaci Informacii 14 (1978), no. 1, 325.

[8] Y. Kitaoka. *Arithmetic of quadratic forms.* Cambridge Tracts in Mathematics, 106. Cambridge University Press, Cambridge, 1993.

[9] Krivelevich, Litsyn and Vardy. *A lower bound on the density of sphere packings via graph theory.* Internat. Math. Res. Notices 43 (2004) 2271–2279.

[10] G. Hardy. *Note on a theorem of Mertens.* J. London Math. Soc. (1927), 70–72.

[11] C. Rogers. *Existence theorems in the geometry of numbers.* Annals of Mathematics (1947), 994–1002.

[12] C. L. Siegel. *A mean value theorem in geometry of numbers.* Ann. of Math. (2) 46, (1945). 340 – 347.

[13] C. L. Siegel. *Uber Die Analytische Theorie Der Quadratischen Formen.* Annals of Mathematics, 36, (1935), 527-606

[14] A. Södergren. *On the Posson distribution of lengths of lattice vectors in a random lattice.* Math Z., in press.

[15] A. Södergren. *On the distribution of angles between the N shortest vectors in a random lattice.* Journal LMS, in press.

[16] T. A. Springer. *Reduction theory over global fields.* Proc. Indian Acad. Sci. Math. Sci. 104 (1994), no. 1, 207216.

[17] S. Vance. *Improved sphere packing lower bounds from Hurwitz lattices.* Advances in Math, in press.

[18] T. Yang. *An Explicit Formula for Local Densities of Quadratic Forms.* Journal of Number Theory 72, (1998), 309–356.

Stanford University