Lattice packing of spheres in high dimensions using a stochastically evolving ellipsoid

Boaz Klartag

Abstract

We prove that in any dimension n there exists an origin-symmetric ellipsoid $\mathcal{E} \subset \mathbb{R}^n$ of volume cn^2 that contains no points of $\mathbb{Z}^n$ other than the origin, where $c > 0$ is a universal constant. Equivalently, there exists a lattice sphere packing in $\mathbb{R}^n$ whose density is at least $cn^2 \cdot 2^{-n}$. Previously known constructions of sphere packings in $\mathbb{R}^n$ had densities of the order of magnitude of $n \cdot 2^{-n}$, up to logarithmic factors. Our proof utilizes a stochastically evolving ellipsoid that accumulates at least cn^2 lattice points on its boundary, while containing no lattice points in its interior except for the origin.

1 Introduction

Let $n \geq 2$. A sphere packing in $\mathbb{R}^n$ is a collection of disjoint Euclidean balls of the same radius. A lattice in $\mathbb{R}^n$ is the image of $\mathbb{Z}^n$ under an invertible, linear transformation $T : \mathbb{R}^n \to \mathbb{R}^n$. Thus, by a lattice in $\mathbb{R}^n$ we always mean a lattice of full rank. The covolume of the lattice $L = T(\mathbb{Z}^n) \subset \mathbb{R}^n$ is

$$Vol_n(\mathbb{R}^n/L) := |\det(T)|.$$

A *lattice sphere packing* is a collection of disjoint Euclidean balls, all of the same radius, whose centers form a lattice in $\mathbb{R}^n$. The *density* of a lattice sphere packing is the proportion of space covered by the disjoint Euclidean balls of which it consists. Equivalently, if the lattice sphere packing consists of balls of radius r whose centers form the lattice L, then its density equals

$$\frac{Vol_n(rB^n)}{Vol_n(\mathbb{R}^n/L)},$$

where Vol_n stands for n-dimensional volume in $\mathbb{R}^n$, where $B^n \subset \mathbb{R}^n$ is the open Euclidean ball of radius 1 centered at the origin, and where $rA = \{rx\,;\, x \in A\}$ for $A \subset \mathbb{R}^n$. We write δ_n for the supremum of all densities of lattice sphere packings in $\mathbb{R}^n$. The Minkowski-Hlawka theorem (see, e.g., Gruber and Lekkerkerker [9, Chapter 3]) implies that

$$\delta_n \geq 2\zeta(n) \cdot 2^{-n},$$

where $\zeta(n) = \sum_{k=1}^{\infty} k^{-n}$. This bound was asymptotically improved in 1947 by Rogers [18], who showed that

$$\delta_n \geq cn \cdot 2^{-n} \tag{1}$$

for a universal constant $c > 0$. In his proof, Rogers used the Minkowski second theorem, as well as the concept of a random lattice and the Siegel summation formula, which we recall in Section 5 below.

The universal constant c that Rogers' proof of (1) yields satisfies $c \geq 2/e$. This was subsequently improved by Davenport and Rogers [7], who obtained (1) with $c \approx 1.67$. Ball [2] used Bang's solution of Tarski's plank problem, and proved (1) with $c = 2 - o(1)$. A plank is the region in space between two parallel hyperplanes, and the problem was to show that the sum of widths of planks covering a convex body, is at least its minimal width. Vance [24] obtained $c \geq 6/e$ in dimensions divisible by 4, by using random lattices with quaternionic symmetries. Her approach was further developed by Venkatesh [25], who used random lattices with sophisticated algebraic symmetries in order to show that

$$\limsup_{n \to \infty} \frac{\delta_n}{n \cdot \log \log n \cdot 2^{-n}} \geq \frac{1}{2}.$$

Campos, Jenssen, Michelen and Sahasrabudhe [4] used graph-theoretic methods to prove the existence of a non-lattice sphere packing in $\mathbb{R}^n$ of density

$$\left(\frac{1}{2} - o(1) \right) n \log n \cdot 2^{-n}.$$

Graph theory was used earlier by Krivelevich, Litsyn and Vardy [12] for the construction of a non-lattice sphere packing of density $cn \cdot 2^{-n}$ in $\mathbb{R}^n$. Schmidt [21] proved (1) by considering random lattices and by analyzing large hole events; these are rare events that occur with a probability of only $\exp(-\tilde{c}n)$. His analysis fits well with the theme that random lattices may sometimes be approximated by a Poisson process. The Poisson heuristic, which we recall below, was hinted at already in Rogers [19].

To summarize, up to logarithmic factors, several papers which are based on quite different ideas have essentially arrived at the same bound (1) over the years. This bound has represented the state of the art on sphere packing in high dimensions – again, up to logarithmic factors – until now. We improve it as follows:

Theorem 1.1. *For any $n \geq 2$,*

$$\delta_n \geq cn^2 \cdot 2^{-n},$$

where $c > 0$ is a universal constant.

The universal constant c arising from our proof of Theorem 1.1 can probably be computed numerically to a reasonable degree of accuracy; see Remark 5.3 below. Venkatesh [25] conjectures that $2^n \delta_n$ grows at most polynomially in n. It is not entirely unlikely that Theorem 1.1 is tight, up to the value of the universal constant c or perhaps up to a logarithmic correction. As for known upper bounds for δ_n, in a short 1929 paper, Blichfeldt [3] proved that

$$\delta_n \leq \frac{n+2}{2} \cdot 2^{-n/2}.$$

See also Rankin [17]. Kabatjanskiĭ and Levenšteĭn [10] improved the bound to roughly $\delta_n \lesssim (0.66)^n$, a result subsequently sharpened by constant factors by Cohn and Zhao [6] and by Sardari and Zargar [20]. These upper bounds also apply for non-lattice sphere packings. There is still a large gap between the known lower bound and the known upper bound for the optimal density of a sphere packing in high dimension. The precise optimal density is currently known in dimensions $2, 3, 8$ and 24, see Cohn [5] and references therein.

By considering the lattice sphere packing $x + K/2 \ \ (x \in L)$, Theorem 1.1 is easily seen to be equivalent to the following:

Theorem 1.2. *Let $n \geq 2$ and let $K \subset \mathbb{R}^n$ be a Euclidean ball centered at the origin of volume*

$$Vol_n(K) = cn^2. \tag{2}$$

Then there exists a lattice $L \subset \mathbb{R}^n$ of covolume one with $L \cap K = \{0\}$. Here, $c > 0$ is a universal constant.

An origin-symmetric ellipsoid in $\mathbb{R}^n$ is the image of the unit ball B^n under an invertible, linear map $T : \mathbb{R}^n \to \mathbb{R}^n$. Consider the lattice L and the Euclidean ball K from Theorem 1.2 . Since L may be represented as $L = T(\mathbb{Z}^n)$ for a linear map $T : \mathbb{R}^n \to \mathbb{R}^n$ with $|\det(T)| = 1$, we conclude from Theorem 1.2 that the origin-symmetric ellipsoid

$$\mathcal{E} = T^{-1}(K) \subset \mathbb{R}^n$$

has volume cn^2, yet it contains no points from $\mathbb{Z}^n$ other than the origin. This implies the statement in the abstract of this paper. We conjecture that the conclusion of Theorem 1.2 holds true for any origin-symmetric convex body $K \subset \mathbb{R}^n$ satisfying (2), and not just for Euclidean balls and ellipsoids. See Schmidt [22, 23] for a proof under the weaker assumption that $Vol_n(K) \leq cn$.

Before presenting the main ideas of the proof of Theorem 1.2, let us briefly discuss the proof of (1) from Rogers [18]. Consider a random lattice $L \subset \mathbb{R}^n$ satisfying $Vol_n(\mathbb{R}^n/L) = Vol_n(B^n)$. By using the Siegel summation formula, it is shown that with positive probability,

$$\prod_{i=1}^{n} \lambda_i \geq cn$$

where $0 < \lambda_1 \leq \lambda_2 \leq \ldots \leq \lambda_n$ are the successive minima of the lattice L. Minkowski's second theorem is then used in order to find a linear map $T : \mathbb{R}^n \to \mathbb{R}^n$ with $|\det(T)| \geq \prod_i \lambda_i$ such that $T(B^n) \cap L = \{0\}$. Intuitively, the ellipsoid $T(B^n)$ constructed this way "interacts" only with n vectors from the lattice – the ones corresponding to the successive minima.

In contrast, an ellipsoid in $\mathbb{R}^n$ is determined by $n(n+1)/2$ parameters, and it is reasonable to expect it to "interact" with roughly n^2 lattice points. In fact, it is not too difficult to show that there exists an open, origin-symmetric ellipsoid $\mathcal{E} \subset \mathbb{R}^n$ with $\mathcal{E} \cap \mathbb{Z}^n = \{0\}$ such that

$$|\partial \mathcal{E} \cap \mathbb{Z}^n| \geq n(n+1). \tag{3}$$

Here, $|A|$ is the cardinality of the set $A \subset \mathbb{R}^n$, and $\partial \mathcal{E}$ is the boundary of the ellipsoid $\mathcal{E}$. See Remark 3.5 below for a proof of (3).

Our construction of the ellipsoid $\mathcal{E} \subset \mathbb{R}^n$ begins with a random lattice $L \subset \mathbb{R}^n$ satisfying $Vol_n(\mathbb{R}^n/L) = Vol_n(B^n)$. Consider a relatively large Euclidean ball disjoint from $L \setminus \{0\}$, and run a Brownian-type stochastic motion in the space of ellipsoids, starting from this Euclidean ball. The crucial property of our stochastic process is that whenever the evolving ellipsoid

$$\mathcal{E}_t = \{x \in \mathbb{R}^n \, ; \, A_t x \cdot x < 1\}$$

hits a non-zero lattice point, it keeps it on its boundary at all later times. In other words, if the ellipsoid hits the point $0 \neq x_0 \in L$ at time t_0, then we ensure that for $t > t_0$,

$$A_t x_0 \cdot x_0 = 1. \tag{4}$$

Note that (4) imposes a one-dimensional linear constraint on the matrix A_t, and that the stochastic evolution of A_t may be continued in the linear subspace of matrices obeying this constraint. The vector space of all real symmetric $n \times n$ matrices, denoted by

$$\mathbb{R}^{n \times n}_{symm},$$

has dimension $n(n+1)/2$. Hence our evolving ellipsoid freezes only when it has absorbed $n(n+1)$ lattice points; note that the absorbed points come in pairs: $x_0 \in L$ and $-x_0 \in L$. Related ideas were used in [11]. Intuitively, the random lattice L behaves somewhat like a Poisson process of intensity

$$1/Vol_n(B^n)$$

in $\mathbb{R}^n$. Thus, one might expect the ellipsoid to cover a volume of about $cn^2 \cdot Vol_n(B^n)$ during its evolution, since it manages to find $n(n+1)$ lattice points. Our evolving ellipsoid expands and contracts in a random fashion, and its volume is not monotone. Still, we expect it not to withdraw too much from regions near absorbed lattice points. Thus the evolving ellipsoid is expected to reach a volume of $cn^2 \cdot Vol_n(B^n)$ while remaining L-free.

In the remainder of this paper we transform these vague heuristics into a mathematical proof. In Section 2 we construct the stochastically evolving ellipsoid for a given lattice (or a lattice-like set). In Section 3 we study the volume growth of the evolving ellipsoid, and in Section 4 we analyze the rate at which it absorbs lattice points. In Section 5 we discuss random lattices, and complete the proof of Theorem 1.2.

The linear space $\mathbb{R}^{n \times n}_{symm}$ is a Euclidean space equipped with the scalar product

$$\langle A, B \rangle = \mathrm{Tr}[AB] \qquad\qquad (A, B \in \mathbb{R}^{n \times n}_{symm}),$$

where $\mathrm{Tr}[A]$ is the trace of the matrix $A \in \mathbb{R}^{n \times n}$. We denote the collection of positive-definite, symmetric $n \times n$ matrices by

$$\mathbb{R}^{n \times n}_{+} \subset \mathbb{R}^{n \times n}_{symm}.$$

We write that $A \geq B$ (respectively, $A > B$) for two matrices $A, B \in \mathbb{R}^{n \times n}_{symm}$ if $A - B$ is positive semi-definite (respectively, positive-definite). We write Id for the identity matrix. The Euclidean norm of $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$ is denoted by $|x| = \sqrt{\sum_i x_i^2}$. For $x, y \in \mathbb{R}^n$ we write $x \cdot y = \sum_{i=1}^n x_i y_i$ for their standard scalar product, and $x \otimes y = (x_i y_j)_{i,j=1,\ldots,n} \in \mathbb{R}^{n \times n}$ for their tensor product. The natural logarithm is denoted by $\log$. A subset $A \subset \mathbb{R}^n$ is origin-symmetric if $A = -A$. All ellipsoids are assumed to be open and origin-symmetric. A random variable X is centered when $\mathbb{E}X = 0$.

Throughout this paper, we write $c, C, \tilde{C}, c', \hat{C}, \bar{C}$ etc. for various positive universal constants whose value may change from one line to the next. We write C_0, C_1, c_0 etc. – that is, the letters C or c with numerical subscripts – for positive universal constants that remain fixed throughout the paper. In proving Theorem 1.2, we may assume that the dimension n is sufficiently large; this is our standing assumption throughout the text.

Acknowledgement. I am grateful to Barak Weiss for interesting discussions and for his encouragement. Supported by a grant from the Israel Science Foundation (ISF).

2 Constructing a stochastically evolving ellipsoid

Let $L \subset \mathbb{R}^n$ be a discrete subset of $\mathbb{R}^n$ such that for any origin-symmetric ellipsoid $\mathcal{E} \subset \mathbb{R}^n$ with $\mathcal{E} \cap L \subseteq \{0\}$,

$$Vol_n(\mathcal{E}) \leq C_L \qquad \text{and} \qquad |\partial \mathcal{E} \cap L| \leq \tilde{C}_L, \tag{5}$$

for some constants $C_L, \tilde{C}_L > 0$ depending only on L. We refer to such a discrete set L as a *lattice-like set*. The most important case is when $L \subset \mathbb{R}^n$ is a lattice; in this case the inequalities in (5) hold true with $C_L = 2^n \cdot Vol_n(\mathbb{R}^n / L)$, by Minkowski's first theorem, and with

$$\tilde{C}_L = 2 \cdot (2^n - 1) \tag{6}$$

by an elementary argument which we reproduce in the Appendix below. For a symmetric matrix $A \in \mathbb{R}^{n \times n}_{symm}$ we consider the open set

$$\mathcal{E}_A = \{x \in \mathbb{R}^n \, ; \, Ax \cdot x < 1\} \, . \tag{7}$$

Its boundary $\partial \mathcal{E}_A$ is the collection of all $x \in \mathbb{R}^n$ with $Ax \cdot x = 1$. The matrix $A \in \mathbb{R}^{n \times n}_{symm}$ is positive-definite if and only if the set $\mathcal{E}_A$ is an ellipsoid, in which case

$$Vol_n(\mathcal{E}_A) = \det(A)^{-1/2} \cdot Vol_n(B^n). \tag{8}$$

When A is not positive-definite, necessarily $Vol_n(\mathcal{E}_A) = \infty$. We say that an open subset $\mathcal{E} \subseteq \mathbb{R}^n$ is *L-free* if $\mathcal{E} \cap L \subseteq \{0\}$. When we write that the matrix $A \in \mathbb{R}^{n \times n}_{symm}$ is L-free, we mean that the open set $\mathcal{E}_A$ is L-free. It follows from (5) that the volume of an L-free ellipsoid is at most C_L, and that it contains at most $\tilde{C}_L$ points on its boundary.

A point belonging both to the boundary $\partial \mathcal{E}_A$ and to the discrete set L is referred to as a contact point. The following lemma describes a continuous deformation of an L-free ellipsoid that keeps all of its contact points.

Lemma 2.1. *Let $M_t \in \mathbb{R}^{n\times n}_{symm}$ $(t \geq 0)$ be a family of matrices depending continuously on $t \geq 0$, such that not all of the matrices are positive-definite. Assume that the matrix $M_0 \in \mathbb{R}^{n\times n}_{symm}$ is positive-definite and L-free, and that for all $t \geq 0$,*

$$\partial\mathcal{E}_{M_0} \cap L \subseteq \partial\mathcal{E}_{M_t} \cap L. \tag{9}$$

Then the following hold:

(A) Denote

$$\tau := \sup\left\{ t \geq 0\, ;\ M_s \textit{ is L-free with } \partial\mathcal{E}_{M_s} \cap L = \partial\mathcal{E}_{M_0} \cap L \textit{ for all } s \in [0,t] \right\}.$$

Then $0 < \tau < \infty$.

(B) The symmetric matrix M_t is positive-definite and L-free for all $0 \leq t \leq \tau$.

(C) We gained at least one additional contact point at time τ. That is,

$$\partial\mathcal{E}_{M_0} \cap L \subsetneq \partial\mathcal{E}_{M_\tau} \cap L. \tag{10}$$

Proof. We claim that there exist $t_0, \varepsilon > 0$ such that for all $0 \leq t \leq t_0$ and $0 \neq x \in L \setminus \partial\mathcal{E}_{M_0}$,

$$M_t x \cdot x > 1 + \varepsilon. \tag{11}$$

In order to prove this claim, we use the fact that M_0 is positive-definite, and hence there exists $\varepsilon_1 > 0$ such that $M_0 \geq \varepsilon_1 \cdot \mathrm{Id}$. The symmetric matrix M_t depends continuously on t, and hence for some $t_1 > 0$ we have $M_t \geq (\varepsilon_1/2)\mathrm{Id}$ for all $0 \leq t \leq t_1$. Therefore (11) holds true for all $|x| > 2/\sqrt{\varepsilon_1}$, provided that $\varepsilon < 1$ and $t_0 \leq t_1$. All that remains is to prove (11) for $x \in F$ where

$$F = \left\{ 0 \neq x \in L \setminus \partial\mathcal{E}_{M_0}\, ;\ |x| \leq 2/\sqrt{\varepsilon_1} \right\}. \tag{12}$$

The set F is finite since L is discrete. The set F is disjoint from the ellipsoid $\mathcal{E}_{M_0}$ since M_0 is L-free. It thus follows from (12) that F is disjoint from the closure of the ellipsoid $\mathcal{E}_{M_0}$, and hence $M_0 x \cdot x > 1$ for all $x \in F$. Since M_t depends continuously on t while F is finite, there exists $t_0 \in (0, t_1)$ and $\varepsilon \in (0,1)$ such that $M_t x \cdot x > 1 + \varepsilon$ for all $x \in F$ and $0 \leq t \leq t_0$. This completes the proof of (11).

Let us prove (A). Fix $0 \leq t \leq t_0$. It follows from (11) that any point $0 \neq x \in L \setminus \partial\mathcal{E}_{M_0}$ does not belong to $\partial\mathcal{E}_{M_t}$, since $M_t y \cdot y = 1$ for all $y \in \partial\mathcal{E}_{M_t}$. Hence

$$\partial\mathcal{E}_{M_t} \cap (L \setminus \mathcal{E}_{M_0}) = \emptyset,$$

where we also used the fact that $0 \notin \partial\mathcal{E}_{M_t}$. Consequently,

$$\partial\mathcal{E}_{M_t} \cap L \subseteq \partial\mathcal{E}_{M_0} \cap L. \tag{13}$$

It follows from (9) that the open set $\mathcal{E}_{M_t}$ contains no points from $L \cap \partial\mathcal{E}_{M_0}$. It follows from (11) that the set $\mathcal{E}_{M_t}$ does not contain non-zero points from $L \setminus \partial\mathcal{E}_{M_0}$. Therefore $\mathcal{E}_{M_t}$ does not contain non-zero points from

$$(L \cap \partial\mathcal{E}_{M_0}) \cup (L \setminus \partial\mathcal{E}_{M_0}) = L.$$

In other words, the matrix M_t is L-free. It now follows from (9), (13) and the definition of τ that

$$\tau \geq t_0 > 0.$$

Since $\mathcal{E}_{M_t}$ is L-free for $0 \leq t < \tau$, by (5),

$$\sup_{0 \leq t < \tau} Vol_n(\mathcal{E}_{M_t}) \leq C_L < \infty. \tag{14}$$

It follows from (8) and (14) that the matrix M_t is positive-definite for all $0 \leq t < \tau$, and

$$\inf_{0 \leq t < \tau} \det(M_t) > 0. \tag{15}$$

This implies in particular that $\tau < \infty$, since we assumed that $(M_t)_{0 \leq t < \infty}$ is *not* a family of positive-definite matrices. Thus (A) is proven.

We move on to the proof of (B). We have seen that the matrix M_t is L-free for $0 \leq t < \tau$, and hence the matrix M_τ is L-free as well, by continuity. Since M_t is positive-definite for $0 \leq t < \tau$, the matrix M_τ is positive semi-definite, by continuity. It follows from (15) that $\det M_\tau > 0$ and hence M_τ is in fact positive-definite. This completes the proof of (B).

We still need to prove (C). If (10) does not hold true, then necessarily

$$\partial\mathcal{E}_{M_0} \cap L = \partial\mathcal{E}_{M_\tau} \cap L, \tag{16}$$

according to (9). Hence, by (9),

$$\partial\mathcal{E}_{M_\tau} \cap L \subseteq \partial\mathcal{E}_{M_t} \cap L \qquad \text{for all } t \geq \tau. \tag{17}$$

The matrix M_τ is positive-definite and L-free according to (B). Since M_t is positive-definite for $0 \leq t \leq \tau$, we know that $(M_{t+\tau})_{t \geq 0}$ is a family of matrices depending continuously on t, not all of them positive-definite. Therefore, thanks to (17), we may apply the lemma for the family of matrices $(M_{t+\tau})_{t \geq 0}$, and conclude from (A) that

$$\tau_1 := \sup \{ t \geq \tau \, ; \, M_s \text{ is } L\text{-free with } \partial\mathcal{E}_{M_s} \cap L = \partial\mathcal{E}_{M_\tau} \cap L \text{ for all } s \in [\tau, t] \}$$

satisfies $\tau_1 \in (\tau, \infty)$. However, equality (16) and the maximality property of τ implies that $\tau_1 = \tau$, in contradiction. □

We recall that the *standard Brownian motion* in a finite-dimensional, real, inner product space V is a centered, continuous, Gaussian process $(W_t)_{t\geq 0}$ attaining values in V, with $W_0 = 0$, and with independent increments[1], such that for all $t > s \geq 0$ and a linear functional $f : V \to \mathbb{R}$,

$$\mathbb{E}|f(W_t - W_s)|^2 = (t - s)\|f\|^2.$$

Here, $\|f\| = \sup_{0 \neq v \in V} |f(v)|/\|v\|$ and $\|v\| = \sqrt{\langle v, v\rangle}$. We refer the reader e.g. to Øksendal [14] or Revuz and Yor [15] for background on Brownian motion and stochastic analysis.

The *Dyson Brownian motion* is a standard Brownian motion $(W_t)_{t\geq 0}$ in the Euclidean space $\mathbb{R}^{n\times n}_{symm}$. For $A \in \mathbb{R}^{n\times n}_{symm}$ consider the subspace

$$F_A = \left\{ B \in \mathbb{R}^{n\times n}_{symm} \, ; \, \forall x \in \partial\mathcal{E}_A \cap L, \ Bx \cdot x = 0 \right\}, \tag{18}$$

where $\mathcal{E}_A$ is defined in (7). We write $\pi_A : \mathbb{R}^{n\times n}_{symm} \to \mathbb{R}^{n\times n}_{symm}$ for the orthogonal projection operator onto the subspace F_A. The following lemma explains how to randomly evolve an L-free ellipsoid until we gain an additional contact point.

Lemma 2.2. *Let $M_0 \in \mathbb{R}^{n\times n}_{+}$ be an L-free matrix with $F_{M_0} \neq \{0\}$. Let $(W_t)_{t\geq 0}$ be a Dyson Brownian motion in $\mathbb{R}^{n\times n}_{symm}$. For $t \geq 0$ denote*

$$M_t = M_0 + \pi_{M_0}(W_t). \tag{19}$$

Then, with probability one, the random variable

$$\tau := \sup\{ \, t \geq 0 \, ; \, M_s \text{ is } L\text{-free with } \partial\mathcal{E}_{M_s} \cap L = \partial\mathcal{E}_{M_0} \cap L \text{ for all } s \in [0,t] \, \},$$

is non-zero and finite. Moreover, almost surely, for $0 \leq t \leq \tau$ the set $\mathcal{E}_{M_t}$ is an L-free ellipsoid, and

$$\partial\mathcal{E}_{M_0} \cap L \subsetneq \partial\mathcal{E}_{M_\tau} \cap L. \tag{20}$$

Proof. Since $F_{M_0} \neq \{0\}$, the linear projection $\pi_{M_0} : \mathbb{R}^{n\times n}_{symm} \to \mathbb{R}^{n\times n}_{symm}$ is not identically zero. Hence there exists $x_0 \in \mathbb{R}^n$ such that $\pi_{M_0}(x_0 \otimes x_0) \neq 0$. Almost surely, a Brownian motion in $\mathbb{R}$ does not remain bounded from below indefinitely. Therefore, almost surely

$$\liminf_{t\to\infty} \pi_{M_0}(W_t)x_0 \cdot x_0 = \liminf_{t\to\infty} \langle W_t, \pi_{M_0}(x_0 \otimes x_0)\rangle = -\infty. \tag{21}$$

It follows from (19) and (21) that almost surely, $(M_t)_{t\geq 0}$ is *not* a family of positive-definite matrices. In order to verify all of the other assumptions of Lemma 2.1, we note that if $x \in \partial\mathcal{E}_{M_0} \cap L$ then by (18),

$$Bx \cdot x = 0 \qquad \text{for all } B \in F_{M_0}. \tag{22}$$

[1]i.e., $W_t - W_s$ is independent of $W_s - W_r$ for all $0 \leq r < s < t$.

Recall that $\pi_{M_0}(W_t) \in F_{M_0}$. Thus, by (22), for all $t \geq 0$ and $x \in \partial\mathcal{E}_{M_0} \cap L$,

$$M_t x \cdot x = M_0 x \cdot x + \pi_{M_0}(W_t) x \cdot x = M_0 x \cdot x = 1.$$

Hence $x \in \partial\mathcal{E}_{M_t} \cap L$ for all $t \geq 0$. We have thus shown that almost surely, for all $t \geq 0$,

$$\partial\mathcal{E}_{M_0} \cap L \subseteq \partial\mathcal{E}_{M_t} \cap L.$$

We have verified all of the assumptions of Lemma 2.1. We may therefore apply the lemma, and conclude that almost surely the random variable τ is finite and non-zero. From conclusion (B) of Lemma 2.1 we learn that almost surely, for all $0 \leq t \leq \tau$ the set $\mathcal{E}_{M_t}$ is an L-free ellipsoid. Conclusion (C) of Lemma 2.1 implies (20). □

Recall that the filtration associated with the Brownian motion $(W_t)_{t\geq 0}$ is $(\mathcal{F}_t)_{t\geq 0}$, where $\mathcal{F}_t$ is the σ-algebra generated by the random variables $(W_s)_{0\leq s\leq t}$. A stochastic process $(A_t)_{t\geq 0}$ is *adapted* to this filtration if for any fixed $t \geq 0$, the random variable A_t is measurable with respect to $\mathcal{F}_t$. A stopping time τ is a random variable attaining values in $[0, \infty)$ such that for any fixed $t \geq 0$, the event $\{\tau \leq t\}$ is measurable with respect to $\mathcal{F}_t$. For example, the random variable τ from Lemma 2.2 is a stopping time. The following proposition describes the construction of the stochastically evolving ellipsoid associated with the lattice-like set $L \subset \mathbb{R}^n$.

Proposition 2.3. *Let $a_0 > 0$ be such that the matrix $a_0 \cdot \mathrm{Id} \in \mathbb{R}^{n\times n}$ is L-free. Let $(W_t)_{t\geq 0}$ be a Dyson Brownian motion in $\mathbb{R}^{n\times n}_{symm}$. Then there exists a continuous stochastic process $(A_t)_{t\geq 0}$, attaining values in $\mathbb{R}^{n\times n}_{symm}$ and adapted to the filtration induced by $(W_t)_{t\geq 0}$, with the following properties:*

(A) Abbreviate $\pi_t = \pi_{A_t}$. Then there exist a bounded, integer-valued random variable $M \geq 0$ and stopping times $0 = \tau_0 < \tau_1 < \tau_2 < \ldots$ for which the following hold: for any fixed $i \geq 1$ and $t > 0$, if $i \leq M$ and $t \in [\tau_{i-1}, \tau_i)$ then $\pi_t = \pi_{\tau_{i-1}}$ and

$$A_t = A_{\tau_{i-1}} + \pi_t \left(W_t - W_{\tau_{i-1}} \right). \tag{23}$$

(B) For $t \geq \tau_M$ we have $A_t = A_{\tau_M}$ and $\pi_t = 0$. Moreover, $A_0 = a_0 \cdot \mathrm{Id}$.

(C) Almost surely, for all $t \geq 0$ the matrix A_t is positive-definite and L-free.

(D) Set $\mathcal{E}_t := \mathcal{E}_{A_T}$. Then almost surely, $\partial\mathcal{E}_s \cap L \subseteq \partial\mathcal{E}_t \cap L$ for all $0 \leq s \leq t$.

(E) Denote $F_t := F_{A_t}$. Then almost surely,

$$\tau_* := \inf\{t \geq 0\,;\, F_t = \{0\}\} \tag{24}$$

is finite, and $\tau_* = \tau_M$.

Proof. We will recursively iterate the construction of Lemma 2.2. Set

$$A_0 = a_0 \cdot \mathrm{Id}, \tag{25}$$

and $\tau_0 = 0$. We will inductively construct stopping times

$$0 = \tau_0 < \tau_1 < \tau_2 < \dots \tag{26}$$

and symmetric matrices $(A_{\tau_i})_{i\geq 1}$ such that almost surely, the random variable τ_i is finite and the matrix A_{τ_i} is a positive-definite, L-free matrix for all i. For the base of the induction, we note that the matrix A_{τ_0} is positive-definite and L-free, by assumption.

Let $i \geq 1$ and suppose that τ_{i-1} and $A_{\tau_{i-1}}$ have been constructed such that almost surely τ_{i-1} is finite, and $A_{\tau_{i-1}}$ is positive-definite and L-free. Let us contruct τ_i and A_{τ_i}. If

$$F_{\tau_{i-1}} = \{0\} \tag{27}$$

then we simply set $A_t := A_{\tau_{i-1}}$ for $t > \tau_{i-1}$. We also define $M := i-1$ and $\tau_{M+j} := \tau_M + j$ for $j \geq 1$, and end the recursive construction. By the induction hypothesis, A_{τ_j} is a positive-definite, L-free matrix for all $j \geq i$. This completes the description of the recursion step in the case where (27) holds true. Suppose now that

$$F_{\tau_{i-1}} \neq \{0\}. \tag{28}$$

Define

$$W_t^{(i)} := W_{t+\tau_{i-1}} - W_{\tau_{i-1}} \qquad\qquad (t \geq 0), \tag{29}$$

which is a standard Brownian motion in $\mathbb{R}^{n\times n}_{symm}$, or in other words, a Dyson Brownian motion. Set

$$M_0 = A_{\tau_{i-1}}, \tag{30}$$

which is positive-definite and L-free by the induction hypothesis. We know that $F_{M_0} \neq \{0\}$, thanks to (28). Denote

$$M_t = M_0 + \pi_{M_0}(W_t^{(i)}), \tag{31}$$

and apply Lemma 2.2. From the conclusion of the lemma, almost surely the stopping time

$$\tau_i := \tau_{i-1} + \sup\{t \geq 0\,;\, M_s \text{ is } L\text{-free with } \partial\mathcal{E}_{M_s} \cap L = \partial\mathcal{E}_{M_0} \cap L \text{ for all } s \in [0,t]\}, \tag{32}$$

is finite with $\tau_i > \tau_{i-1}$. Moreover, almost surely $\mathcal{E}_{M_t}$ is an L-free ellipsoid for $0 \leq t \leq \tau_i - \tau_{i-1}$. Therefore, setting

$$A_t := M_{t-\tau_{i-1}} \qquad\qquad \text{for } t \in (\tau_{i-1}, \tau_i] \tag{33}$$

we see that A_t is positive-definite and L-free for $t \in [\tau_{i-1}, \tau_i]$. Almost surely, the matrix A_t depends continuously on $t \in [\tau_{i-1}, \tau_i]$. Furthermore, from conclusion (20) of Lemma 2.2 we learn that almost surely,

$$\partial\mathcal{E}_{A_{\tau_{i-1}}} \cap L \subsetneq \partial\mathcal{E}_{A_{\tau_i}} \cap L. \tag{34}$$

This completes the description of the recursive construction of τ_i and A_{τ_i} for all $i \geq 0$. It follows from (26) that along the way we defined the random matrix A_t for all $0 < t \leq \tau_M$, via formula (33). For completeness, set

$$A_t = A_{\tau_M} \qquad \text{for } t > \tau_M. \tag{35}$$

Thus, almost surely the stochastic process $(A_t)_{t\geq 0}$ is well-defined and continuous. Let us discuss the basic properties of this construction.

We first claim that the random variable M – the number of steps in the construction – is a bounded random variable. Indeed, relation (34) holds true for all $i = 1, \ldots, M$. Therefore,

$$|\partial \mathcal{E}_{A_{\tau_i}} \cap L| \geq i \qquad\qquad (i = 1, \ldots, M), \tag{36}$$

while the ellipsoid $\mathcal{E}_{A_{\tau_i}}$ is L-free. It follows from (5) and (36) that almost surely $M \leq \tilde{C}_L$, and hence M is a bounded random variable. We conclude that the random variable τ_M is almost surely finite, being almost surely the sum of finitely many numbers.

Next, by the construction of A_t in (33), the matrix A_t is almost surely positive-definite and L-free for $t \in [\tau_{i-1}, \tau_i]$ for all $i = 1, \ldots, M$. It thus follows from (25) and (26) that A_t is positive-definite and L-free for $t \in [0, \tau_M]$. Observe that by (32) and (33), for any $i = 1, \ldots, M$ and $t \in [\tau_{i-1}, \tau_i)$,

$$\partial \mathcal{E}_{A_t} \cap L = \partial \mathcal{E}_{A_{\tau_{i-1}}} \cap L. \tag{37}$$

From (29), (30), (31), (33) and (37), for $i = 1, \ldots, M$ and $t \in [\tau_{i-1}, \tau_i)$ we have $F_t = F_{\tau_{i-1}}$ and

$$A_t = A_{\tau_{i-1}} + \pi_{A_{\tau_{i-1}}}(W^{(i)}_{t-\tau_{i-1}}) = A_{\tau_{i-1}} + \pi_{A_t}(W_t - W_{\tau_{i-1}}).$$

Since A_t depends continuously on t, and since A_t is constant for $t \in [\tau_M, \infty)$ by (35), conclusion (A) and conclusion (B) are proven. Note that the matrix A_t is a function of a_0, L and $(W_s)_{0\leq s\leq t}$. In particular, the stochastic process $(A_t)_{t\geq 0}$ is adapted to the filtration induced by the Dyson Brownian motion.

Conclusion (C) holds true as A_t is positive-definite and L-free for $t \in [0, \tau_M]$, and $A_t = A_{\tau_M}$ for $t \in [\tau_M, \infty)$. Conclusion (D) holds true in view of (34) and (37).

From our construction, if $M \geq 1$ then the subspace $F_t = F_{A_t}$ is constant and different from $\{0\}$ for $t \in [\tau_{i-1}, \tau_i)$ and $i = 1, \ldots, M$. We always have $F_{\tau_M} = \{0\}$. It thus follows that $\tau_* = \tau_M$, where τ_* is defined in (24). Thus the stopping time τ_* is almost surely finite, completing the proof of (E). □

We refer to the stochastic process $(\mathcal{E}_t)_{t\geq 0}$ from Proposition 2.3 as the *stochastically evolving ellipsoid*. The volume of the L-free ellipsoid $\mathcal{E}_t$ may increase or decrease with t, but it remains bounded at all times. In fact, it follows from (5), (8) and Proposition 2.3(C) that almost surely,

$$\det A_t \geq c_L \qquad\qquad \text{for all } t \geq 0, \tag{38}$$

with $c_L = (C_L / Vol_n(B^n))^2$. The Itô integral interpretation of conclusions (A) and (B) of Proposition 2.3 is given in the following:

Corollary 2.4. *Under the notation and assumptions of Proposition 2.3, for all $t \geq 0$,*

$$A_t = a_0 \cdot \mathrm{Id} + \int_0^t \pi_s(dW_s). \tag{39}$$

Thus $A_0 = a_0 \cdot \mathrm{Id}$ and we have the stochastic differential equation

$$dA_t = \pi_t(dW_t). \tag{40}$$

Proof. The Itô integral on the right-hand side of (39) may be defined as

$$\int_0^t \pi_s(dW_s) = \lim_{\varepsilon(P) \to 0} \sum_{i=1}^{N_p} \pi_{t_{i-1}} \left(W_{t_i} - W_{t_{i-1}} \right), \tag{41}$$

where $P = \{0 = t_0 < t_1 < \ldots < t_{N_p} = t\}$ is a non-random partition of $[0, t]$ into N_P intervals and $\varepsilon(P) = \max_{1 \leq i \leq N_P} |t_i - t_{i-1}|$. The convergence of the $\mathbb{R}^{n \times n}_{symm}$-valued random variables in (41) is in the sense of L^2.

Thus (39) follows from (41) and conclusions (A) and (B) of Proposition 2.3 via a standard argument, while (40) is the stochastic differential equation rewriting of (39). ☐

3 The shape and volume of the evolving ellipsoid

Let $L \subset \mathbb{R}^n$ be a lattice. Assume that $a_0 > 0$ is such that the matrix

$$a_0 \cdot \mathrm{Id} \in \mathbb{R}^{n \times n}$$

is L-free. Fix a Dyson Brownian motion $(W_t)_{t \geq 0}$ in $\mathbb{R}^{n \times n}_{symm}$, and consider the stochastic process $(A_t)_{t \geq 0}$ constructed in Proposition 2.3.

Lemma 3.1. *There exist two Dyson Brownian motions $(W^{(1)}_t)_{t \geq 0}$ and $(W^{(2)}_t)_{t \geq 0}$ in $\mathbb{R}^{n \times n}_{symm}$ such that for all $t \geq 0$,*

$$A_t = a_0 \cdot \mathrm{Id} + \frac{W^{(1)}_t + W^{(2)}_t}{2}. \tag{42}$$

Proof. We use an idea that is attributed to Bernard Maurey, see Eldan and Lehec [8, Proposition 4]. Recall from Proposition 2.3 the linear map

$$\pi_t : \mathbb{R}^{n \times n}_{symm} \to \mathbb{R}^{n \times n}_{symm}.$$

Almost surely, for all $t \geq 0$ the map π_t is an orthogonal projection. In particular, π_t is a symmetric operator and

$$0 \leq \pi_t \leq \mathrm{Id},$$

in the sense of symmetric operators on the Euclidean space $\mathbb{R}^{n\times n}_{symm}$. It follows from Corollary 2.4 that $(A_t)_{t\geq 0}$ is a martingale in $\mathbb{R}^{n\times n}_{symm}$. Its quadratic variation process is

$$[A]_t = \int_0^t \pi_s^2 ds = \int_0^t \pi_s ds. \qquad\qquad (t>0). \tag{43}$$

Denote $\tilde{\pi}_t = \mathrm{Id} - \pi_t : \mathbb{R}^{n\times n}_{symm} \to \mathbb{R}^{n\times n}_{symm}$ and set

$$W_t^{(1)} = \int_0^t \pi_s(dW_s) + \int_0^t \tilde{\pi}_s(dW_s)$$

and

$$W_t^{(2)} = \int_0^t \pi_s(dW_s) - \int_0^t \tilde{\pi}_s(dW_s).$$

Thus $(W_t^{(1)})_{t\geq 0}$ and $(W_t^{(2)})_{t\geq 0}$ are well-defined, continuous martingales in $\mathbb{R}^{n\times n}_{symm}$, with

$$W_t^{(1)} + W_t^{(2)} = 2\int_0^t \pi_s(dW_s) = 2(A_t - a_0\cdot \mathrm{Id}),$$

where the last passage follows from Corollary 2.4. This proves the desired conclusion (42). The quadratic variation processes of these two martingales satisfy, for $t>0$,

$$[W^{(1)}]_t = \int_0^t (\pi_s + \tilde{\pi}_s)^2 ds = t\cdot \mathrm{Id}$$

and

$$[W^{(2)}]_t = \int_0^t (\pi_s - \tilde{\pi}_s)^2 ds = t\cdot \mathrm{Id}.$$

Note that $W_0^{(1)} = W_0^{(2)} = 0$. Thus, by Paul Lévy's characterization of the standard Brownian motion, both $(W_t)^{(1)}_{t\geq 0}$ and $(W_t^{(2)})_{t\geq 0}$ are standard Brownian motions in $\mathbb{R}^{n\times n}_{symm}$. In other words, both stochastic processes are Dyson Brownian motions. □

Write $\|A\|_{op} = \sup_{0\neq x\in\mathbb{R}^n} |Ax|/|x|$ for the operator norm of the matrix $A\in\mathbb{R}^{n\times n}$.

Corollary 3.2. *For any $t>0$ and $r\geq\sqrt{tn}$,*

$$\mathbb{P}\left(\|A_t - a_0\cdot \mathrm{Id}\|_{op} \geq C_0 r\right) \leq C\exp(-r^2/t),$$

where $C, C_0 > 0$ are universal constants.

Proof. From Lemma 3.1, for any $r>0$,

$$\mathbb{P}\left(\|A_t - a_0\cdot \mathrm{Id}\|_{op} \geq r\right) = \mathbb{P}\left(\left\|\frac{W_t^{(1)} + W_t^{(2)}}{2}\right\|_{op} \geq r\right)$$
$$\leq 2\mathbb{P}\left(\|W_t\|_{op} \geq r\right) = 2\mathbb{P}\left(\sqrt{tn}\|\Gamma\|_{op} \geq r\right),$$

where Γ is a Gaussian Orthogonal Ensemble (GOE) random matrix. This means that $\Gamma = (\Gamma_{ij})_{i,j=1,\dots,n} \in \mathbb{R}^{n\times n}_{symm}$ is a random symmetric matrix such that $(\Gamma_{ij})_{i\leq j}$ are independent, centered Gaussian random variables, with $\mathbb{E}\Gamma_{ij}^2 = (1+\delta_{ij})/n$. It is well-known and proven by an epsilon-net argument (e.g., Vershynin [26, Corollary 4.4.8]) that for $s \geq 1$,

$$\mathbb{P}\left(\|\Gamma\|_{op} \geq Cs\right) \leq 4\exp(-s^2 n)$$

for a universal constant $C > 0$. The corollary is proven by setting $s = r/\sqrt{tn}$. □

Corollary 3.2 implies that if $t < c/n$ and $a_0 \geq 1/2$, then the ellipsoid $\mathcal{E}_t$ is typically sandwiched between two concentric Euclidean balls whose radii $r_1 < r_2$ satisfy $r_2/r_1 \leq C$. Our next goal is to study the volume growth of the ellipsoid $\mathcal{E}_t$, or equivalently, the decay of the determinant of the positive-definite matrix A_t. To this end we consider the non-negative, integer-valued random variable

$$N_t = \dim(F_t) \qquad\qquad (t \geq 0) \tag{44}$$

where $F_t = F_{A_t}$ is defined in (18) and in Proposition 2.3.

Lemma 3.3. *For any fixed $T > 0$,*

$$\mathbb{E}\log\det A_T \leq n\log a_0 - \frac{1}{2}\int_0^T \mathbb{E}\left[\|A_t\|_{op}^{-2}\cdot N_t\right]dt.$$

Proof. For two fixed matrices $P, B \in \mathbb{R}^{n\times n}_{symm}$ with P being positive-definite, we have the Taylor expansion as $\varepsilon \to 0$,

$$\log\det(P+\varepsilon B) = \log\det P + \varepsilon \mathrm{Tr}[P^{-1}B] - \frac{\varepsilon^2}{2}\mathrm{Tr}[(P^{-1}B)^2] + O(\varepsilon^3).$$

Denote the eigenvalues of P, repeated according to their multiplicity, by $\lambda_1,\dots,\lambda_n \in (0,\infty)$. Then for any orthonormal basis of eigenvectors $u_1,\dots,u_n \in \mathbb{R}^n$ corresponding to these eigenvalues,

$$\frac{d^2}{d\varepsilon^2}\log\det(P+\varepsilon B)\bigg|_{\varepsilon=0} = -\sum_{i,j=1}^n \frac{(Bu_i\cdot u_j)^2}{\lambda_i\lambda_j} = -\sum_{i,j=1}^n \frac{\langle B, u_i\otimes_s u_j\rangle^2}{\lambda_i\lambda_j},$$

where $x\otimes_s y = (x\otimes y + y\otimes x)/2$ for $x,y\in\mathbb{R}^n$. Observe that for any linear map $S : \mathbb{R}^{n\times n}_{symm} \to \mathbb{R}^{n\otimes n}_{symm}$,

$$\mathrm{Tr}[S] = \sum_{i,j=1}^n \left\langle S(u_i\otimes_s u_j), u_i\otimes_s u_j\right\rangle.$$

Recall that $dA_t = \pi_t(dW_t)$ by Corollary 2.4, and that $\pi_t : \mathbb{R}^{n\times n}_{symm} \to \mathbb{R}^{n\times n}_{symm}$ is an orthogonal projection. From the Itô formula,

$$d(\log\det A_t) = \langle A_t^{-1}, \pi_t(dW_t)\rangle - \frac{1}{2}\delta_t dt \tag{45}$$

where

$$\delta_t = \sum_{i,j=1}^n \frac{|\pi_t(u_i \otimes_s u_j)|^2}{\lambda_i \lambda_j},$$

and $\lambda_1, \ldots, \lambda_n \in (0, \infty)$ are the eigenvalues of A_t while $u_1, \ldots, u_n \in \mathbb{R}^n$ constitute a corresponding orthonormal basis of eigenvectors. Since $\lambda_i \leq \|A_t\|_{op}$ for all i, we have

$$\delta_t \geq \frac{1}{\|A_t\|_{op}^2} \sum_{i,j=1}^n |\pi_t(u_i \otimes_s u_j)|^2 = \frac{1}{\|A_t\|_{op}^2} \sum_{i,j=1}^n \langle \pi_t(u_i \otimes_s u_j), u_i \otimes_s u_j \rangle = \frac{1}{\|A_t\|_{op}^2} \cdot \mathrm{Tr}[\pi_t]. \quad (46)$$

Consider the martingale $(M_t)_{t \geq 0}$ with $M_0 = 0$ that satisfies

$$dM_t = \langle \pi_t(A_t^{-1}), dW_t \rangle \qquad (t > 0).$$

In order to show that it is indeed a well-defined martingale, we bound its quadratic variation:

$$\mathbb{E}|\pi_t(A_t^{-1})|^2 \leq \mathbb{E}|A_t^{-1}|^2 \leq n \cdot \mathbb{E}\|A_t^{-1}\|_{op}^2 \leq n \cdot \mathbb{E}\frac{\|A_t\|_{op}^{2(n-1)}}{\det^2 A_t} \leq \frac{n}{c_L^2} \cdot \mathbb{E}\|A_t\|_{op}^{2(n-1)},$$

where we used (38) in the last passage. By Corollary 3.2, for any fixed $t > 0$, the random variable $\|A_t\|_{op}$ has a uniformly sub-gaussian tail. Hence, $\mathbb{E}\|A_t\|_{op}^{n-2} \leq C_n(a_0 + \sqrt{t})^{n-2}$ for some constant C_n depending only on n, and $(M_t)_{t \geq 0}$ is indeed a martingale. It follows from (45) that

$$\log \det A_t = \log \det A_0 + M_t - \frac{1}{2} \int_0^t \delta_s ds \qquad (t \geq 0). \quad (47)$$

Since $\mathbb{E}M_T = M_0 = 0$, by (46) and (47),

$$\mathbb{E} \log \det A_T = \log \det A_0 - \frac{1}{2} \int_0^T \mathbb{E}\delta_t dt \leq n \log a_0 - \frac{1}{2} \int_0^T \mathbb{E}\|A_t\|_{op}^{-2} \cdot \mathrm{Tr}[\pi_t] dt.$$

Since π_t is the orthogonal projection operator onto the subspace $F_t \subseteq \mathbb{R}^{n \times n}_{symm}$ we have $\mathrm{Tr}[\pi_t] = \dim(F_t) = N_t$, and the lemma is proven. □

Recall the L-free evolving ellipsoid $\mathcal{E}_t = \mathcal{E}_{A_t}$ from Proposition 2.3.

Proposition 3.4. *Fix $0 < T \leq 20 \cdot n^{-5/3}$ and assume that $1 \leq a_0 \leq 1 + 10/n$. Then,*

$$\mathbb{E} \log \det A_T \leq C - \frac{n^2 T}{4} + \frac{1}{4} \int_0^T \mathbb{E}|\partial \mathcal{E}_t \cap L| dt,$$

where $C > 0$ is a universal constant.

Proof. Fix $0 < t \leq T$ and let $\mathcal{S}_t$ be the event that

$$\|A_t - a_0 \cdot \mathrm{Id}\|_{op} \leq C_0\sqrt{tn},$$

where $C_0 > 0$ is the constant from Corollary 3.2. Let $1_{\mathcal{S}_t}$ be the indicator of $\mathcal{S}_t$, that equals 1 if the event $\mathcal{S}_t$ occurs, and that vanishes otherwise. Then,

$$\begin{aligned}\mathbb{E}\left[\|A_t\|_{op}^{-2} \cdot N_t\right] &\geq \mathbb{E}\left[1_{\mathcal{S}_t}\|A_t\|_{op}^{-2} \cdot N_t\right] \geq (a_0 + C\sqrt{tn})^{-2}\mathbb{E}[1_{\mathcal{S}_t}N_t] \\ &= (a_0 + C\sqrt{tn})^{-2}\left(\mathbb{E}[N_t] - \mathbb{E}[(1 - 1_{\mathcal{S}_t})N_t]\right). \qquad (48)\end{aligned}$$

Since $N_t = \dim(F_t) \leq n^2$, by Corollary 3.2,

$$\mathbb{E}[(1 - 1_{\mathcal{S}_t})N_t] \leq n^2\mathbb{E}[1 - 1_{\mathcal{S}_t}] = n^2 \cdot \mathbb{P}(\|A_t - a_0 \cdot \mathrm{Id}\|_{op} > C_0\sqrt{tn}) \leq Cn^2e^{-n}.$$

Therefore, by using (48) and the inequalities $|a_0 - 1| \leq C/n$ and $N_t \leq n^2$,

$$\mathbb{E}\left[\|A_t\|_{op}^{-2} \cdot N_t\right] \geq (1 - C'\sqrt{tn} - C/n)\mathbb{E}[N_t] - \tilde{C}e^{-n/2} \geq \mathbb{E}[N_t] - C'\sqrt{t} \cdot n^{5/2} - \bar{C}n.$$

By integrating over t and recalling that $T \leq Cn^{-5/3}$ we thus obtain

$$\int_0^T \mathbb{E}\left[\|A_t\|_{op}^{-2} \cdot N_t\right] dt \geq \int_0^T \mathbb{E}\left[N_t\right] dt - C'T^{3/2}n^{5/2} - T \cdot \bar{C}n \geq \int_0^T \mathbb{E}\left[N_t\right] dt - \hat{C}.$$

Therefore, from Lemma 3.3,

$$\mathbb{E}\log\det A_T \leq n\log(1 + 10/n) - \frac{1}{2}\int_0^T \mathbb{E}\left[\|A_t\|_{op}^{-2} \cdot N_t\right] dt \leq C' - \frac{1}{2}\int_0^T \mathbb{E}\left[N_t\right] dt.$$

The subspace $F_t = F_{A_t}$ is defined in (18) as the orthogonal complement in $\mathbb{R}^{n\times n}_{symm}$ to the subspace E spanned by $x \otimes x$ $(x \in \partial\mathcal{E}_t \cap L)$. The dimension of the subspace E is at most $|\partial\mathcal{E}_t \cap L|/2$, since $\partial\mathcal{E}_t \cap L = -(\partial\mathcal{E}_t \cap L)$ while $0 \notin \partial\mathcal{E}_t \cap L$. Therefore,

$$N_t = \dim(F_t) = \dim(\mathbb{R}^{n\times n}_{symm}) - \dim(E) \geq \frac{n(n+1)}{2} - \frac{|\partial\mathcal{E}_t \cap L|}{2}.$$

Consequently,

$$\mathbb{E}\log\det A_T \leq C' - \frac{1}{2}\int_0^T \mathbb{E}\left[N_t\right] dt \leq C' - T\frac{n(n+1)}{4} + \frac{1}{4}\int_0^T \mathbb{E}|\partial\mathcal{E}_t \cap L| dt,$$

completing the proof. □

Remark 3.5. In the notation of Proposition 2.3, for $t = \tau_* = \tau_M$ the L-free ellipsoid $\mathcal{E}_t \subset \mathbb{R}^n$ almost surely satisfies

$$|\partial\mathcal{E}_t \cap L| \geq n(n+1). \qquad (49)$$

Indeed, since $F_t = \{0\}$ by Proposition 2.3(B), we know that the matrices $x\otimes x$ $(x \in \partial\mathcal{E}_t \cap L)$ span $\mathbb{R}^{n\times n}_{symm}$. The number of such distinct matrices is at most $|\partial\mathcal{E}_t \cap L|/2$, since $\partial\mathcal{E}_t \cap L = -(\partial\mathcal{E}_t \cap L)$. Thus (49) follows from the fact that $\dim(\mathbb{R}^{n\times n}_{symm}) = n(n+1)/2$. By applying a linear map $S : \mathbb{R}^n \to \mathbb{R}^n$ that transforms L to $\mathbb{Z}^n$, we see that the ellipsoid $\mathcal{E} = S(\mathcal{E}_t) \subset \mathbb{R}^n$ is disjoint from $\mathbb{Z}^n \setminus \{0\}$ and that inequality (3) above holds true.

4 Points absorbed by the evolving ellipsoid

We keep the notation and assumptions of the previous section. Thus $L \subset \mathbb{R}^n$ is a fixed lattice, $a_0 > 0$ is such that the matrix $a_0 \cdot \mathrm{Id}$ is L-free, and we study the stochastic process $(A_t)_{t \geq 0}$ introduced in Proposition 2.3. The following proposition is a step toward showing that, for a typical lattice $L \subset \mathbb{R}^n$, the number of points absorbed by the L-free ellipsoid $\mathcal{E}_t = \mathcal{E}_{A_t}$ up to time T is usually at most

$$C \exp(n^2 T/8).$$

Proposition 4.1. *For any fixed $T > 0$ and $0 \neq x \in L$,*

$$\mathbb{P}(x \in \partial \mathcal{E}_T) \ \leq \ 2\mathbb{P}\left(Z \geq \frac{1}{\sqrt{T}} \left(a_0 - \frac{1}{|x|^2} \right) \right),$$

where $Z \sim N(0,1)$ is a standard Gaussian random variable.

Proof. Since the matrix $a_0 \cdot \mathrm{Id}$ is L-free, necessarily $a_0|x|^2 \geq 1$. If $a_0|x|^2 = 1$ then the conclusion of the lemma holds trivially, so let us assume that $a_0|x|^2 > 1$. For $t \geq 0$ denote

$$M_t = A_t x \cdot x - 1 = \langle A_t, x \otimes x \rangle - 1.$$

If $M_t > 0$ then $x \notin \partial \mathcal{E}_t$, and hence

$$\mathbb{P}(x \in \partial \mathcal{E}_T) \ \leq \ \mathbb{P}(M_T \leq 0) \ \leq \ \mathbb{P}\left(\inf_{0 \leq t \leq T} M_t \leq 0 \right). \tag{50}$$

By Corollary 2.4,

$$dM_t = \langle \pi_t(dW_t), x \otimes x \rangle = \langle dW_t, \pi_t(x \otimes x) \rangle.$$

Thus $(M_t)_{t \geq 0}$ is a martingale with $M_0 = a_0|x|^2 - 1 > 0$. Its quadratic variation is given by

$$[M]_t = \int_0^t |\pi_s(x \otimes x)|^2 ds \leq \int_0^t |x \otimes x|^2 ds = t|x|^4, \tag{51}$$

where we used the fact that π_s is an orthogonal projection. For $t \geq 0$ denote

$$R_t = \inf\{ s \geq 0 \, ; \, [M]_s > t \}, \tag{52}$$

where the infimum of an empty set is defined as $+\infty$. Almost surely, the function R_t is non-decreasing in t with $M_{R_{t-0}} = M_{R_{t+0}}$ for all t for which $R_{t+0} < \infty$. Here we write $R_{t-0} = \lim_{s \to t^-} R_s$ and $R_{t+0} = \lim_{s \to t^+} R_s$. The Dambis-Dubins-Schwartz Theorem (e.g. Revuz and Yor [15, Chapter V]) states that there exists a standard Brownian motion $(B_t)_{t \geq 0}$ in $\mathbb{R}$ such that for all $t \geq 0$,

$$M_{R_t} - M_0 = B_t$$

whenever $R_t < \infty$. It follows from (51) and (52) that $R_t \geq t/|x|^4$. Consequently,

$$\inf_{0 \leq t \leq T|x|^4} [M_0 + B_t] \leq \inf_{\substack{0 \leq t \leq T|x|^4 \\ R_t < \infty}} M_{R_t} \leq \inf_{0 \leq t \leq T} M_t.$$

Thus, from (50),

$$\mathbb{P}(x \in \partial \mathcal{E}_T) \leq \mathbb{P}\left(\inf_{0 \leq t \leq T|x|^4} [M_0 + B_t] \leq 0 \right).$$

By the reflection principle for the standard Brownian motion (e.g. [15, Section III.3]),

$$\mathbb{P}\left(\inf_{0 \leq t \leq T|x|^4} [M_0 + B_t] \leq 0 \right) = \mathbb{P}\left(\sup_{0 \leq t \leq T|x|^4} B_t \geq M_0 \right) = 2\mathbb{P}\left(B_{T|x|^4} \geq M_0 \right).$$

The law of $B_{T|x|^4}$ is the same as the law of $\sqrt{T}|x|^2 \cdot Z$. Therefore,

$$\mathbb{P}(x \in \partial \mathcal{E}_T) \leq 2\mathbb{P}\left(\sqrt{T}|x|^2 \cdot Z \geq M_0 \right) = 2\mathbb{P}\left(Z \geq \frac{1}{\sqrt{T}} \left(a_0 - \frac{1}{|x|^2} \right) \right).$$

□

For $r \geq 0$ denote

$$\Phi(r) = \min\left\{ \frac{1}{2}, \frac{e^{-r^2/2}}{\sqrt{2\pi} \cdot r} \right\}, \tag{53}$$

with $\Phi(0) = \min\{1/2, +\infty\} = 1/2$. It is well-known that if Z is a standard Gaussian random variable, then for $r \geq 0$,

$$\mathbb{P}(Z \geq r) = \frac{1}{\sqrt{2\pi}} \int_r^\infty e^{-x^2/2} dx \leq \min\left\{ \frac{1}{2}, \frac{1}{\sqrt{2\pi}} \int_r^\infty \frac{x}{r} \cdot e^{-x^2/2} dx \right\} = \Phi(r). \tag{54}$$

In the remainder of this paper we will no longer refer to Brownian motion, let alone any denoted by $(B_t)_{t \geq 0}$ as in the previous proposition. In fact, from now on, for $t \geq 0$ we define

$$B_t = \{ x \in \mathbb{R}^n \, ; \, (a_0 - C_0 \sqrt{tn})|x|^2 < 1 \}, \tag{55}$$

where $C_0 > 0$ is the universal constant from Corollary 3.2. For $t > 0$ we consider the non-negative number

$$K_t(L) = \sum_{0 \neq x \in L \cap B_t} \Phi\left(\frac{1}{\sqrt{t}} \left(a_0 - \frac{1}{|x|^2} \right) \right) \in [0, +\infty]. \tag{56}$$

Proposition 4.2. *For any $t > 0$,*

$$\mathbb{E}|\partial \mathcal{E}_t \cap L| \leq 2K_t(L) + Ce^{-cn},$$

where $C, c > 0$ are universal constants.

Proof. By the linearity of expectation and Proposition 4.1,

$$\mathbb{E}|\partial\mathcal{E}_t \cap L \cap B_t| = \sum_{0 \neq x \in L \cap B_t} \mathbb{P}(x \in \partial\mathcal{E}_t) \leq 2 \sum_{0 \neq x \in L \cap B_t} \mathbb{P}\left(Z \geq \frac{1}{\sqrt{t}}\left(a_0 - \frac{1}{|x|^2}\right)\right),$$

where Z is a standard Gaussian random variable. The matrix $a_0 \cdot \mathrm{Id}$ is L-free. Thus $a_0 - 1/|x|^2 \geq 0$ for $x \in L$, and we may use the standard bound (54) and the definition (56) of $K_t(L)$ to conclude that

$$\mathbb{E}|\partial\mathcal{E}_t \cap L \cap B_t| \leq 2K_t(L). \tag{57}$$

We claim that

$$\mathbb{P}\left(\partial\mathcal{E}_t \cap L \cap B_t \neq \partial\mathcal{E}_t \cap L\right) \leq Ce^{-n}. \tag{58}$$

Indeed, it suffices to prove that

$$\mathbb{P}\left(\overline{\mathcal{E}_t} \subseteq B_t\right) \geq 1 - Ce^{-n},$$

where $\overline{\mathcal{E}_t} \subset \mathbb{R}^n$ is the closure of the ellipsoid $\mathcal{E}_t = \mathcal{E}_{A_t} \subset \mathbb{R}^n$. Equivalently, we need to show that

$$\mathbb{P}\left(A_t > \left(a_0 - C_0\sqrt{tn}\right)\mathrm{Id}\right) \geq 1 - Ce^{-n}.$$

This follows from Corollary 3.2, proving (58). Recall from (6) that $|\partial\mathcal{E}_t \cap L| \leq 2 \cdot (2^n - 1)$ as $\mathcal{E}_t$ is an L-free ellipsoid and $L \subset \mathbb{R}^n$ is a lattice. Thus, from (57) and (58),

$$\begin{aligned}\mathbb{E}|\partial\mathcal{E}_t \cap L| &\leq \mathbb{P}\left(\partial\mathcal{E}_t \cap L \cap B_t \neq \partial\mathcal{E}_t \cap L\right) \cdot 2 \cdot (2^n - 1) + \mathbb{E}|\partial\mathcal{E}_t \cap L \cap B_t| \\ &\leq C(2/e)^n + 2K_t(L),\end{aligned}$$

completing the proof. □

In view of Proposition 3.4 and Proposition 4.2, it is desirable to understand how large $K_t(L)$ is for a typical lattice L. Recall that for small $t > 0$, the parameter $K_t(L)$ is the sum of the function

$$x \mapsto \Phi\left(\frac{1}{\sqrt{t}}\left(a_0 - \frac{1}{|x|^2}\right)\right) \tag{59}$$

over all non-zero lattice points in a certain Euclidean ball. In the following lemma we analyze the integral of the function from (59) over a spherical shell approximating this ball.

Lemma 4.3. *Let $t > 0$. Assume that $0 < t \leq 20n^{-2} \cdot \log n$ and $1 \leq a_0 \leq 1 + 10/n$. Consider the spherical shell*

$$R = R_t = \left\{x \in \mathbb{R}^n\,;\, \frac{1}{a_0} \leq |x|^2 < \frac{1}{a_0 - C_0\sqrt{tn}}\right\}, \tag{60}$$

where $C_0 > 0$ is the universal constant from Corollary 3.2. Then,

$$\int_R \Phi\left(\frac{1}{\sqrt{t}}\left(a_0 - \frac{1}{|x|^2}\right)\right) dx \leq Ce^{n^2 t/8} \cdot Vol_n(B^n),$$

where $C > 0$ is a universal constant.

Proof. Denote $\kappa_n = Vol_n(B^n)$ and $a_1 = a_0 - C_0\sqrt{tn}$. Integrating in polar coordinates,

$$I := \int_R \Phi\left(\frac{1}{\sqrt{t}}\left(a_0 - \frac{1}{|x|^2}\right)\right) dx = n\kappa_n \int_{1/\sqrt{a_0}}^{1/\sqrt{a_1}} \Phi\left(\frac{a_0 - 1/r^2}{\sqrt{t}}\right) r^{n-1} dr.$$

Changing variables $y = t^{-1/2}(a_0 - 1/r^2)$ we see that

$$I = \frac{n\kappa_n\sqrt{t}}{2}\int_0^{C_0\sqrt{n}} \frac{\Phi(y)}{(a_0 - \sqrt{t}y)^{\frac{n+2}{2}}} dy = \frac{n\kappa_n\sqrt{t}}{2} a_0^{-\frac{n+2}{2}} \int_0^{C_0\sqrt{n}} \frac{\Phi(y)}{(1 - y\sqrt{t}/a_0)^{\frac{n+2}{2}}} dy.$$

Recall that $a_0 \geq 1$ while $t \leq 20n^{-2} \cdot \log n$. Thus $y\sqrt{t}/a_0 \leq y\sqrt{t} < 1$ for all $y \in (0, C_0\sqrt{n})$, assuming that n exceeds a certain given universal constant. Consequently,

$$\frac{I}{\kappa_n} \leq \frac{n\sqrt{t}}{2}\int_0^{C_0\sqrt{n}} \frac{\Phi(y)}{(1 - y\sqrt{t})^{\frac{n+2}{2}}} dy = \frac{n\sqrt{t}}{2} \cdot (I_1 + I_2 + I_3), \tag{61}$$

where I_1 is the integral from 0 to 1, where I_2 is the integral from 1 to $\log n$ and where I_3 is the integral from $\log n$ till $C_0\sqrt{n}$. Begin by bounding I_1. To this end we will use the elementary inequality $1 - x \geq \exp(-2x)$ for $0 < x \leq 1/2$. Since $\Phi(y) \leq 1/2$ and $t \leq 20n^{-2} \cdot \log n$,

$$I_1 = \int_0^1 \frac{\Phi(y)}{(1 - y\sqrt{t})^{\frac{n+2}{2}}} dy \leq \frac{1}{2}(1 - \sqrt{t})^{-\frac{n+2}{2}} \leq e^{(n+2)\sqrt{t}} \leq Ce^{n\sqrt{t}} \leq C'\frac{e^{n^2 t/8}}{n\sqrt{t}}, \tag{62}$$

where we used the bound $e^x \leq Cx^{-1} \cdot e^{x^2/8}$ for $x > 0$, as well as our standing assumption that n is sufficiently large. Next, we bound I_3 using the same elementary inequality. Since $\sqrt{t} \leq 5n^{-1} \cdot \sqrt{\log n}$,

$$I_3 \leq \int_{\log n}^{C_0\sqrt{n}} \Phi(y)e^{(n+2)y\sqrt{t}} dy \leq \int_{\log n}^{\infty} e^{-y^2/2 + 2Cy\sqrt{\log n}} dy = e^{2C^2\log n}\int_{\log n - 2C\sqrt{\log n}}^{\infty} e^{-x^2/2} dx.$$

The last integral is at most $C'e^{-c'\log^2 n}$ by a standard bound for the Gaussian tail such as (54) above. Consequently,

$$I_3 \leq C'e^{2C^2\log n - c'\log^2 n} \leq \bar{C} \leq \hat{C}\frac{e^{n^2 t/8}}{n\sqrt{t}}, \tag{63}$$

as $c \leq x^{-1} \cdot e^{x^2/8}$ for $x > 0$. For the estimation of the integral I_2 we use the elementary inequality $1 - x \geq \exp(-x - x^2)$ for $0 < x < 1/2$, as well as the bound $\sqrt{t} \leq 5n^{-1} \cdot \sqrt{\log n}$. This yields

$$\begin{aligned} I_2 &= \int_1^{\log n} \frac{\Phi(y)}{(1 - y\sqrt{t})^{\frac{n+2}{2}}} dy \leq \int_1^{\log n} \Phi(y)e^{\frac{(n+2)\sqrt{t}}{2}y + \frac{(n+2)y^2 t}{2}} dy \\ &\leq C'\int_1^{\log n} \frac{e^{-y^2/2}}{y} e^{\frac{n\sqrt{t}}{2}y} dy = C'e^{n^2 t/8}\int_1^{\log n} \frac{e^{-(y - n\sqrt{t}/2)^2/2}}{y} dy. \end{aligned}$$

Therefore,

$$
\begin{aligned}
I_2 &\leq C' e^{n^2 t/8} \left[\left| \int_1^{n\sqrt{t}/4} e^{-(y - n\sqrt{t}/2)^2/2} dy \right| + \int_{n\sqrt{t}/4}^{\infty} \frac{e^{-(y-n\sqrt{t}/2)^2/2}}{y} dy \right] \\
&\leq \bar{C} e^{n^2 t/8} \left[\mathbb{P}(Z \geq n\sqrt{t}/4) + \frac{4}{n\sqrt{t}} \cdot \sqrt{2\pi} \right] \leq \tilde{C} \frac{e^{n^2 t/8}}{n\sqrt{t}}, \qquad (64)
\end{aligned}
$$

where Z is a standard Gaussian random variable, and we used a standard tail estimate such as (54) which gives $\mathbb{P}(Z \geq n\sqrt{t}/4) \leq C/(n\sqrt{t})$. To summarize, by (61), (62), (63) and (64),

$$
\frac{I}{\kappa_n} \leq \frac{n\sqrt{t}}{2} \left[I_1 + I_2 + I_3 \right] \leq C e^{n^2 t/8},
$$

completing the proof. □

Remark 4.4. When $T = 16n^{-2} \cdot \log n$, most of the contribution to the integral in Lemma 4.3 arrives from points $x \in \mathbb{R}^n$ with

$$
\left| |x| - \left(1 + 4\frac{\log n}{n} \right) \right| \leq C \frac{\sqrt{\log n}}{n}, \qquad (65)
$$

as can be seen from the proof. When $L \subset \mathbb{R}^n$ is a random, uniformly distributed lattice as in the next section, there will typically be about $n^4 e^{C\sqrt{\log n}}$ lattice points satisfying (65).

5 Random lattices

Write $\mathscr{X}_n$ for the space of all lattices $L \subset \mathbb{R}^n$ with

$$
Vol_n(\mathbb{R}^n/L) = Vol_n(B^n).
$$

We emphasize that our normalization is *not* that of covolume one lattices, but rather we consider lattices whose covolume is the volume of the Euclidean unit ball. The space $\mathscr{X}_n$ is a homogenous space under the action of the group $SL_n(\mathbb{R}) = \{g \in \mathbb{R}^{n \times n} \, ; \, \det(g) = 1\}$, where the action of $g \in SL_n(\mathbb{R})$ on the lattice $L \subset \mathbb{R}^n$ is the lattice

$$
g.L = \{g(x) \, ; \, x \in L\}.
$$

Minkowski and Siegel [16] discovered that there is a unique Haar *probability* measure on $\mathscr{X}_n$ which is invariant under the action of $SL_n(\mathbb{R})$. When we say that $L \subset \mathbb{R}^n$ is a random lattice distributed uniformly in $\mathscr{X}_n$, we refer to the Haar probability measure on $\mathscr{X}_n$. For more information on random lattices we refer the reader e.g. to Gruber and Lekkerkerker [9, Section 19.3] or to Marklof [13]. Throughout this section we set

$$
a_0 := (1 - 1/n)^{-2}. \qquad (66)
$$

Clearly $1 \leq a_0 \leq 1 + 10/n$, as required in order to apply Proposition 3.4 and Lemma 4.3. Recall the parameter $K_t(L) \geq 0$ that is defined in (56) for any lattice $L \subset \mathbb{R}^n$ and any time $t > 0$.

Proposition 5.1. *Let $0 < T \leq 20n^{-2} \cdot \log n$. Then there exists a lattice $L \in \mathscr{X}_n$ such that $a_0|x|^2 > 1$ for any $0 \neq x \in L$ and*

$$\int_0^T K_t(L)dt \leq \frac{C}{n^2} \cdot e^{n^2 T/8}, \tag{67}$$

where $C > 0$ is a universal constant.

Proof. Let $L \in \mathscr{X}_n$ be a random, uniformly distributed lattice. The Siegel summation formula [16] states that for any measurable function $\varphi : \mathbb{R}^n \to (0, +\infty)$,

$$\mathbb{E} \sum_{0 \neq x \in L} \varphi(x) = \frac{1}{Vol_n(B^n)} \cdot \int_{\mathbb{R}^n} \varphi. \tag{68}$$

Write $f(x) = 1$ if $|x| \leq 1 - 1/n$ and $f(x) = 0$ otherwise. By (68),

$$\mathbb{E} \sum_{0 \neq x \in L} f(x) = \frac{1}{Vol_n(B^n)} \cdot \int_{\mathbb{R}^n} f = (1 - 1/n)^n \leq \frac{1}{e}.$$

Hence, by the Markov inequality,

$$\mathbb{P}\left(\exists 0 \neq x \in L\, ;\, |x| \leq 1 - 1/n\right) \leq \frac{1}{e}. \tag{69}$$

Let $0 < t \leq T$, and let $R = R_t \subseteq \mathbb{R}^n$ be the spherical shell defined in (60). Denote

$$\tilde{K}_t(L) = \sum_{0 \neq x \in L \cap R_t} \Phi\left(\frac{1}{\sqrt{t}}\left(a_0 - \frac{1}{|x|^2}\right)\right), \tag{70}$$

i.e., the difference between $\tilde{K}_t(L)$ and $K_t(L)$ is that we sum over the spherical shell R_t rather than over the ball B_t. According to (68) and Lemma 4.3,

$$\begin{aligned} \mathbb{E}\tilde{K}_t(L) &= \mathbb{E} \sum_{0 \neq x \in L \cap R_t} \Phi\left(\frac{1}{\sqrt{t}}\left(a_0 - \frac{1}{|x|^2}\right)\right) \\ &= \frac{1}{Vol_n(B^n)} \cdot \int_{R_t} \Phi\left(\frac{1}{\sqrt{t}}\left(a_0 - \frac{1}{|x|^2}\right)\right) dx \leq C_1 e^{n^2 t/8}. \end{aligned}$$

Since $\tilde{K}_t(L)$ is non-negative, we may apply Fubini's theorem and conclude that

$$\mathbb{E} \int_0^T \tilde{K}_t(L)dt \leq C_1 \int_0^T e^{n^2 t/8} dt \leq \frac{8C_1}{n^2} \cdot e^{n^2 T/8}.$$

By the Markov inequality,

$$\mathbb{P}\left(\int_0^T \tilde{K}_t(L)dt \geq \frac{16C_1}{n^2} \cdot e^{n^2 T/8}\right) \leq \frac{1}{2}. \tag{71}$$

Since $1/2 + 1/e < 1$, we conclude from (69) and (71) that there exists a lattice $L \in \mathscr{X}_n$ such that $|x| > 1 - 1/n$ for all $0 \neq x \in L$ and such that

$$\int_0^T \tilde{K}_t(L)dt < \frac{16C_1}{n^2} \cdot e^{n^2 T/8}. \tag{72}$$

From (66) we thus see that $a_0|x|^2 > 1$ for any $0 \neq x \in L$. Therefore the matrix $a_0 \cdot \mathrm{Id}$ is L-free, and from (55) and (60) we see that

$$(L \setminus \{0\}) \cap R_t = (L \setminus \{0\}) \cap B_t \qquad \text{for any } 0 < t \leq T.$$

Consequently, from (56) and (70),

$$\tilde{K}_t(L) = K_t(L) \qquad (0 < t \leq T).$$

The desired conclusion (67) thus follows from (72). □

Let $L \subset \mathbb{R}^n$ be the lattice whose existence is guaranteed by Proposition 5.1. Thus the matrix $a_0 \cdot \mathrm{Id}$ is L-free. We may therefore apply Proposition 2.3, and consider the stochastic process

$$(A_t)_{t \geq 0}$$

of positive-definite, symmetric $n \times n$ matrices. Recall that almost surely, for any $t > 0$ the ellipsoid $\mathcal{E}_t = \mathcal{E}_{A_t}$ is L-free.

Lemma 5.2. *Set $T = 16n^{-2} \cdot \log n$. Then with positive probability,*

$$\det A_T \leq \frac{C}{n^4},$$

for a universal constant $C > 0$.

Proof. From Proposition 4.2 and Proposition 5.1, for any $t > 0$,

$$\int_0^T \mathbb{E}|\partial\mathcal{E}_t \cap L|dt \leq \int_0^T \left(2K_t(L) + C'e^{-c'n}\right) dt \leq \frac{2C}{n^2} \cdot e^{n^2 T/8} + C'Te^{-c'n} \leq \tilde{C},$$

since $n^2 T/8 = 2 \log n$. By our standing assumption that n is sufficiently large, we have $T \leq 20 \cdot n^{-5/3}$. We may therefore apply Proposition 3.4, and conclude that

$$\mathbb{E} \log \det A_T \leq C - \frac{n^2 T}{4} + \frac{1}{4} \int_0^T \mathbb{E}|\partial\mathcal{E}_t \cap L|dt \leq C' - \frac{n^2 T}{4} = C' - 4 \log n.$$

In particular, with positive probability, $\log \det A_T \leq C' - 4 \log n$. The lemma follows by exponentiation. □

Proof of Theorem 1.2. Since the matrix A_T is almost surely L-free, Lemma 5.2 guarantees the existence of an L-free matrix $A \in \mathbb{R}_+^{n\times n}$ with

$$\det(A) \leq C/n^4.$$

According to (8),

$$Vol_n(\mathcal{E}_A) = \det(A)^{-1/2} \cdot Vol_n(B^n) \geq c_0 n^2 \cdot Vol_n(B^n). \tag{73}$$

The ellipsoid $\mathcal{E}_A$ is L-free, thus $L \cap \mathcal{E}_A = \{0\}$. All that remains is to normalize. Write $\kappa_n = Vol_n(B^n)$ and consider the matrix

$$S = \kappa_n^{-1/n} \cdot \det(A)^{-1/(2n)} \cdot \sqrt{A},$$

where $\sqrt{A} \in \mathbb{R}_+^{n\times n}$ is the positive-definite square root of the matrix $A \in \mathbb{R}_+^{n\times n}$. Note that $\mathcal{E}_A = (\sqrt{A})^{-1}(B^n)$, where we view an $n \times n$ matrix as a linear map on $\mathbb{R}^n$. Denote

$$\tilde{L} = S(L) \subset \mathbb{R}^n.$$

The lattice $\tilde{L} \subset \mathbb{R}^n$ has covolume one, since $L \in \mathscr{X}_n$. If $K \subseteq \mathbb{R}^n$ is an open Euclidean ball centered at the origin with $Vol_n(K) = c_0 n^2$, then $S^{-1}(K) \subseteq \mathcal{E}_A$ by (73) and hence

$$\tilde{L} \cap K \subseteq S(L \cap \mathcal{E}_A) = \{0\}.$$

□

Remark 5.3. Our proof of Theorem 1.2 suggests a randomized algorithm for constructing the sphere-packing lattice $L \subset \mathbb{R}^n$. Indeed, begin by sampling $L \in \mathscr{X}_n$ uniformly, for example by using Ajtai's algorithm [1], and then run the stochastic process described above. It would be interesting to carry out numerical simulations of our construction, or variants thereof (e.g., replacing π_t in (40) by another linear transformation with the same image – perhaps the linear map $X \mapsto \pi_t(A_t^\alpha X)$ for a certain exponent α). Such numerical simulations could help compute the universal constant c from Theorem 1.2 yielded by this construction.

A Appendix

Lemma A.1. *Let $L \subset \mathbb{R}^n$ be a lattice and let $\mathcal{E} \subseteq \mathbb{R}^n$ be a non-empty, open, origin-symmetric, bounded, strictly-convex set (e.g., an origin-symmetric ellipsoid) with $\mathcal{E} \cap L = \{0\}$. Then,*

$$|\partial\mathcal{E} \cap L| \leq 2 \cdot (2^n - 1).$$

Proof. We follow Minkowski's classical proof that the Voronoi cell of a lattice contains at most $2 \cdot (2^n - 1)$ facets. Since $\mathcal{E} \cap L = \{0\}$, no point of $\partial\mathcal{E}$ can belong to $2L$. Moreover, we claim that for any $x, y \in \partial\mathcal{E} \cap L$ with $x \neq y$ and $x \neq -y$, necessarily $x - y \notin 2L$. Indeed, otherwise $0 \neq x - y \in 2L$ while

$$\frac{x-y}{2} \in \left\{ \frac{x_1 + x_2}{2} \,;\, x_1, x_2 \in \partial\mathcal{E}, x_1 \neq x_2 \right\} \subseteq \mathcal{E}.$$

Thus $(x-y)/2$ is a non-zero point belonging both to L and to $\mathcal{E}$, in contradiction to $\mathcal{E} \cap L = \{0\}$. Consequently each coset of the subgroup of $2L$ of the lattice L, either contains no points from $\partial\mathcal{E}$, or else contains a pair of antipodal points from $\partial\mathcal{E}$. There are $2^n - 1$ such cosets, excluding the subgroup $2L$ itself which contains no points from $\partial\mathcal{E}$, and the union of these cosets covers $L \setminus (2L)$. Hence the cardinality of $\partial\mathcal{E} \cap L$ is at most $2 \cdot (2^n - 1)$. □

References

[1] Ajtai, M., *Random lattices and a conjectured 0 - 1 law about their polynomial time computable properties*. Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science, (2002), 733–742.

[2] Ball, K., *A lower bound for the optimal density of lattice packings.* Internat. Math. Res. Notices (IMRN), no. 10, (1992), 217–221.

[3] Blichfeldt, H. F., *The minimum value of quadratic forms, and the closest packing of spheres.* Math. Ann., Vol. 101, no. 1, (1929), 605–608.

[4] Campos, M., Jenssen, M., Michelen, M., Sahasrabudhe, J., *A new lower bound for sphere packing*. Preprint, arXiv:2312.10026

[5] Cohn, H., *A conceptual breakthrough in sphere packing*. Notices Amer. Math. Soc., Vol. 64, no. 2, (2017), 102–115.

[6] Cohn, H., Zhao, Y., *Sphere packing bounds via spherical codes.* Duke Math. J., Vol. 163, no. 10, (2014), 1965–2002.

[7] Davenport, H., Rogers, C. A., *Hlawka's theorem in the geometry of numbers.* Duke Math. J., Vol. 14, (1947), 367–375.

[8] Eldan, R., Lehec, J., *Bounding the norm of a log-concave vector via thin-shell estimates.* Geometric Aspects of Functional Analysis, Israel Seminar (2011–2013), Lecture Notes in Math., Vol. 2116, Springer, (2014), 107–122.

[9] Gruber, P. M., Lekkerkerker, C. G., *Geometry of numbers.* Second edition. North-Holland Publishing Co., 1987.

[10] Kabatjanskiĭ, G. A., Levenšteĭn, V. I., *Bounds for packings on the sphere and in space.* Problemy Peredači Informacii 14, no. 1, (1978), 3–25. In Russian. English translation in: Problems of Information Transmission, Vol. 14, no. 1, (1978), 1–17.

[11] Klartag, B., *Eldan's stochastic localization and tubular neighborhoods of complex-analytic sets.* J. Geom. Anal., Vol. 28, no. 3, (2018), 2008–2027.

[12] Krivelevich, M., Litsyn, S., Vardy, A., *A lower bound on the density of sphere packings via graph theory.* Internat. Math. Res. Notices (IMRN), no. 43, (2004), 2271–2279.

[13] Marklof, J., *Random lattices in the wild: from Pólya's orchard to quantum oscillators.* Lond. Math. Soc. Newsl., No. 493, (2021), 42–49.

[14] Øksendal, B., *Stochastic differential equations. An introduction with applications.* Sixth edition. Springer, 2003.

[15] Revuz, D., Yor, M., *Continuous martingales and Brownian motion.* Third edition. Springer, 1999.

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

[17] Rankin, R. A., *On the closest packing of spheres in n dimensions.* Ann. of Math., Vol. 48, (1947), 1062–1081.

[18] Rogers, C. A., *Existence Theorems in the Geometry of Numbers.* Ann. of Math., Vol. 48, (1947), 994–1002.

[19] Rogers, C. A., *The number of lattice points in a set.* Proc. London Math. Soc., Vol. s3-6, (1956), 305–320.

[20] Sardari, N. T., Zargar, M., *New upper bounds for spherical codes and packings.* Math. Ann., Vol. 389, no. 4, (2024), 3653–3703.

[21] Schmidt, W. M., *The measure of the set of admissible lattices.* Proc. Amer. Math. Soc., Vol. 9, No. 3, (1958), 390–403.

[22] Schmidt, W. M., *On the Minkowski-Hlawka theorem.* Illinois J. Math., Vol. 7, (1963), 18–23.

[23] Schmidt, W. M., *Correction to my paper, "On the Minkowski-Hlawka theorem".* Illinois J. Math., Vol. 7, (1963), 714.

[24] Vance, S., *Improved sphere packing lower bounds from Hurwitz lattices.* Adv. Math., Vol. 227, no. 5, (2011), 2144–2156.

[25] Venkatesh, A., *A note on sphere packings in high dimension.* Internat. Math. Res. Notices (IMRN), no. 7, (2013), 1628–1642.

[26] Vershynin, R., *High-dimensional probability.* Cambridge University Press, 2018.

Department of Mathematics, Weizmann Institute of Science, Rehovot 7610001, Israel.
e-mail: `boaz.klartag@weizmann.ac.il`