Near-optimal deterministic algorithms for volume computation via M-ellipsoids

Daniel Dadush and Santosh S. Vempala

We give a deterministic $2^{O(n)}$ algorithm for computing an M-ellipsoid of a convex body, matching a known lower bound. This leads to a nearly optimal deterministic algorithm for estimating the volume of a convex body and improved deterministic algorithms for fundamental lattice problems under general norms.

Ellipsoids have traditionally played an important role in the study of convex bodies. The classical Lowner–John ellipsoid, for instance, is the starting point for many interesting studies. To recall John’s theorem, for any convex body $K$ in $\mathbb{R}^n$, there is an ellipsoid $E$ with centroid $x_0$ such that

$$x_0 + E \subseteq K \subseteq x_0 + nE.$$ 

This bound is achieved by the maximum volume ellipsoid contained in $K$.

Ellipsoids have also been critical to the design and analysis of efficient algorithms. The most notable example is the ellipsoid algorithm (1–2) for linear (3) and convex optimization of $2^{O(n)}$, which represents a frontier of polynomial-time solvability. For the basic problems of sampling and integration in high dimension, the inertial ellipsoid defined by the covariance matrix of a distribution is an important ingredient of efficient algorithms (5–7). This ellipsoid also achieves the bounds of John’s theorem for general convex bodies (for centrally symmetric convex bodies, the maximum volume ellipsoid achieves the best possible sandwiching ratio of $\sqrt{n}$ whereas the inertial ellipsoid could still have a ratio of $n$).

Another ellipsoid that has played a critical role in the development of modern convex geometry is the M-ellipsoid (Milman’s ellipsoid). This object was introduced by Milman as a tool to prove fundamental inequalities in convex geometry (e.g., ref. 8, chap. 7). An M-ellipsoid $E$ of a convex body $K$ has small covering numbers with respect to $K$. We let $N(A, B)$ denote the number of translations of a set $B$ required to cover the set $A$. Then, as shown by Milman, every convex body $K$ in $\mathbb{R}^n$ has an ellipsoid $E$ for which $N(K, E)N(E, K)$ is bounded by $2^{O(n)}$. This is the best possible bound up to a constant in the exponent. In contrast, the John ellipsoid can have this covering bound as high as $n^{O(n)}$. Intuitively, an M-ellipsoid for $K$ is the largest ellipsoid with the property that roughly $1/2^n$ fraction of its volume is inside $K$ (as opposed to the entire ellipsoid being in $K$). The existence of M-ellipsoids now has several proofs in the literature: by Milman (9), multiple proofs by Pisier (8), and, more recently, by Klartag (10).

The complexity of computing these ellipsoids is interesting for its own sake, but also due to several important consequences that we discuss presently. John ellipsoids are hard to compute, but their sandwiching bounds can be approximated deterministically to within $O(\sqrt{n})$ in polynomial time (4). Inertial ellipsoids can be approximated to arbitrary accuracy by random sampling in polynomial time. Algorithms for M-ellipsoids have been considered more recently. The proof of Klartag (10) gives a randomized polynomial-time algorithm (11). This approach is based on estimating a covariance matrix from random samples and seems inherently difficult to derandomize. It has been open to give a deterministic algorithm for constructing an M-ellipsoid that achieves optimal covering bounds. The extent to which randomness is essential for efficiency is a very interesting question in general and specifically for problems on convex bodies where separations between randomized and deterministic complexity are known in the general oracle model (12, 13). Here we address the question of deterministic M-ellipsoid construction and consider its algorithmic consequences for volume estimation and also for fundamental lattice problems, namely the shortest vector problem (SVP) and the bounded distance decoding (BDD) problem.

The first discovery of this paper is a deterministic $2^{O(n)}$ algorithm for computing an M-ellipsoid of a convex body in the oracle model (4). This is the best possible up to a constant in the exponent as there is a $2^{\Omega(n)}$ lower bound for deterministic algorithms. We state this result formally and then proceed to its extensions and consequences. For all our algorithmic problems with convex bodies, we need to the body to be specified only by a standard well-guaranteed membership oracle; i.e., the algorithm has access to a membership oracle for the convex body of interest $K$, a point $x_0$ in $K$, and numbers $r$, and $R$ s.t. balls of these radii sandwich $K$; i.e., $x_0 + rB^2_2 \subseteq K \subseteq rB^2_2$ (4). By time complexity of an algorithm, we refer to the total number of oracle calls and additional arithmetic operations (we focus on the dependence of the complexity on the dimension and suppress factors that depend polynomially on the size of the input [in particular, $\log(R/r)$]).

Theorem 1.1. There is a deterministic algorithm that, given any convex body $K \subseteq \mathbb{R}^n$ specified by a well-guaranteed membership oracle, finds an ellipsoid $E$ such that $N(K, E)N(E, K) \leq 2^{O(n)}$. The time complexity of the algorithm is $2^{O(n)}$ and its space complexity is bounded by a polynomial in $n$.

In ref. 14, we gave a deterministic algorithm based on computing an approximate minimum mean-width ellipsoid (or $r$-ellipsoid, section 2.1). The resulting covering bound was $N(K, E)N(E, K) = O(\log n)^2$ rather than the optimal $2^{O(n)}$, and the complexity of the algorithm was also $O(\log n)^2$. Our approach here is to completely algorithmize Milman’s original existence proof and thereby obtain the best possible deterministic complexity of $2^{O(n)}$. By adjusting the parameters in the resulting algorithm to “slow down” Milman’s iteration, we get the optimal trade-off between approximation and complexity for volume computation.

1.1. Deterministic Volume Computation. The first consequence is for estimating the volume of a convex body. This is an ancient problem that has led to many developments in algorithmic techniques, high-dimensional geometry, and probability theory. On one hand, the problem can be solved for any convex body presented in the general membership oracle model in randomized polynomial time to arbitrary accuracy (15). On the other hand, the following lower bound (improving on ref. 16) shows that deterministic algorithms cannot achieve such approximations.

Author contributions: D.D. and S.S.V. designed research; D.D. and S.S.V. performed research; and S.S.V. wrote the paper.

The authors declare no conflict of interest.

This article is a PNAS Direct Submission.

To whom correspondence should be addressed. E-mail: vempala@cc.gatech.edu.

PNAS | November 26, 2013 | vol. 110 | no. 48 | 19237–19245

www.pnas.org/cgi/doi/10.1073/pnas.1203863110
Theorem 1.2 (12). Suppose there is a deterministic algorithm that takes as input a symmetric convex body $K$ satisfying $B_n^2 \subseteq K \subseteq B_n^2$ and outputs $A(K), B(K)$ such that $A(K) \leq \text{vol}(K) \leq B(K)$ and makes at most $n^c$ calls to the membership oracle for $K$. Then there is some convex body $K$ for which

$$\frac{B(K)}{A(K)} \geq \left( \frac{cn}{a \log n} \right)^{n/2},$$

where $c$ is an absolute constant.

In particular, Theorem 1.2 implies that achieving even a $2^{O(n)}$ approximation requires $2^{O(n)}$ oracle calls.

The volume of an M-ellipsoid $E$ of $K$ is clearly within a factor of $2^{O(n)}$ of the volume of $K$. Thus, Theorem 1.1 gives a $2^{O(n)}$ algorithm that achieves this volume approximation by computing the volume of the M-ellipsoid found. We state this consequence formally.

Theorem 1.3. There is a deterministic algorithm of time complexity $2^{O(n)}$ and polynomial space complexity that estimates the volume of a convex body given by a well-guaranteed membership oracle to within a factor of $2^{O(n)}$.

What is the complexity of achieving a smaller approximation factor for the volume? The following result of Furedi and Barany (17) gives a lower bound.

Theorem 1.4 (17). For any $0 \leq \epsilon \leq 1$, any deterministic algorithm that estimates the volume of any input convex body to within a $(1+\epsilon)^n$, given only a membership oracle to the body, must make at least $\Omega(1/\epsilon^n)^2$ queries to the membership oracle.

We show that our M-ellipsoid algorithm can be modified to obtain an algorithm that essentially matches this best possible complexity vs. approximation trade-off for centrally symmetric convex bodies.

Theorem 1.5. For any $0 \leq \epsilon \leq 1$, there is a deterministic algorithm that computes a $(1+\epsilon)^n$ approximation of the volume of a centrally symmetric convex body given by a well-guaranteed membership oracle in $O(1/\epsilon)^{O(n)}$ time and polynomial space.

1.2. Deterministic Lattice Algorithms. Efficient M-ellipsoid construction also has consequences for central lattice problems. We define these problems next. For a convex body $K \subseteq \mathbb{R}^n$ containing the origin, the gauge function of $K$ is

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

for $x \in \mathbb{R}^n$. For symmetric $K$ (i.e., $K = -K$), $||\cdot||_K$ is a usual norm on $\mathbb{R}^n$ (we refer to $||\cdot||_K$ as the norm induced by $K$ and specify asymmetric whenever relevant). We say that $K$ is well centered if $\text{vol}(K \cap -K) \geq 2^{-O(n)}\text{vol}(K)$ (every convex body is well centered with respect to its centroid or a point sufficiently close to its centroid).

The SVM is stated as follows: Given an n-dimensional lattice $L$, represented by a basis, and a convex body $K$, find a nonzero $v \in L$ such that $||v||_K$ is minimized. In the closest vector problem (CVP), in addition to a lattice and a convex body, we are also given a query point $x$ in $\mathbb{R}^n$, and the goal is to find a vector $v \in L$ that minimizes $||x-v||_K$. These problems are central to the geometry of numbers and have applications to integer programming, factoring polynomials, cryptography, etc.

The Ajtai-Kumar-Sivakumar (AKS) sieve (18, 19) can be used to solve the SVP in randomized $2^{O(n)}$ time, also using exponential space and randomness. Finding a deterministic algorithm of this complexity has been an important open problem. In a breakthrough paper, Micciancio and Voulgaris (20) gave deterministic $2^{O(n)}$ algorithms for the SVP and the exact CVP in the Euclidean norm. The focus then shifted to extending these results to general norms as in the AKS-sieve-based randomized algorithms.

Subsequently, ref. 11 gave a reduction from the general norm SVP to the CVP in the Euclidean norm (or, more specifically, to enumerating lattice points in ellipsoids) and thereby availed the algorithm of ref. 20. The reduction uses a $2^{O(n)}$ space and poly($n$) randomness, improving on the AKS sieve, and gives an expected running time of $2^{O(n)}$ for the general norm SVP. We now state the main part of the reduction precisely as it is useful for deterministic algorithms as well. For a lattice $L$ and convex body $K$ in $\mathbb{R}^n$, let $G(L,K)$ be the largest number of lattice points contained in any translate of $K$; i.e.,

$$G(L,K) = \max_{x \in \mathbb{R}^n} |(K+x) \cap L|.$$  \[1.1\]

The main result of ref. 11, using the algorithm of ref. 20, can be stated as follows.

Theorem 1.6 (11). Given any convex body $K \subseteq \mathbb{R}^n$ along with an ellipsoid $E$ of $K$ and any n-dimensional lattice $L \subseteq \mathbb{R}^n$, the set $K \cap L$ can be computed deterministically in time $G(L,K) \cdot \text{N}(K,E)(n,K)^{2^{O(n)}}$.

For an M-ellipsoid $E$ of $K$, the numbers $\text{N}(K,E)$ and $\text{N}(E,K)$ are both bounded by $2^{O(n)}$. From Theorem 1.1, we obtain the following corollary.

Corollary 1.7. Given any convex body $K \subseteq \mathbb{R}^n$ and any n-dimensional lattice $L \subseteq \mathbb{R}^n$, the set $K \cap L$ can be computed deterministically in time $G(L,K) \cdot 2^{O(n)}$.

For the SVP in any norm, a simple packing argument (11) shows that $G(\lambda_1 K,L) = 2^{O(n)}$, where $\lambda_1 = \inf_{x} ||x||_K$, the length of the shortest nonzero vector in $L$, giving us the following result.

Theorem 1.8. Given a basis for a lattice $L$ and a well-centered convex body $K$, both in $\mathbb{R}^n$, the shortest vector in $L$ under the norm $||\cdot||_K$ can be computed deterministically, using $2^{O(n)}$ time and space.

The reduction from ref. 11 can also be used for a special case CVP in any norm called the bounded distance decoding problem. Here one assumes that the distance to the lattice of the query point is bounded by some factor $\gamma$ times the length of the shortest nonzero lattice vector. In this case, $G(\gamma \lambda_1 L,L) = (2+\gamma)^{O(n)}$ and we obtain a deterministic $(2+\gamma)^{O(n)}$ algorithm.

Theorem 1.9. Given a basis for a lattice $L$, any well-centered n-dimensional convex body $K$, and a query point $x$ in $\mathbb{R}^n$, the closest vector in $L$ to $x$ in the norm $||\cdot||_K$ defined by $K$ can be computed deterministically, using $(2+\gamma)^{O(n)}$ time and space, provided that the minimum distance is at most $\gamma$ times the length of the shortest nonzero vector of $L$ under $||\cdot||_K$.

It remains open to solve the CVP deterministically in time $2^{O(n)}$ with no assumptions on the minimum distance. Even the special case of the CVP under any norm other than the Euclidean norm is open.

2. Techniques from Convex Geometry

2.1. The Lewis Ellipsoid. Let $\alpha : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}_+$ be a norm on $n \times n$ real matrices. We define the dual norm $\alpha^*$ for any $S \in \mathbb{R}^{n \times n}$ as

$$\alpha^*(S) = \sup \{\text{tr}(SA) : A \in \mathbb{R}^{n \times n}, \alpha(A) \leq 1\}. \[2.1\]$$

For a matrix $A \in \mathbb{R}^{n \times n}$, we denote its transpose by $A^T$, its inverse (when it exists) by $A^{-1}$ and $A^{-T} = (A^{-1})^T$, and its trace by $\text{tr}(A) = \sum_{i=1}^{n} A_{ii}$.

Theorem 2.1 (21). For any norm $\alpha$ on $\mathbb{R}^{n \times n}$, there is an invertible linear transformation $A \in \mathbb{R}^{n \times n}$ such that

$$\alpha(A) = 1 \text{ and } \alpha^*(A^{-1}) = \alpha(A).$$

The ellipsoid $AB^2_n$, corresponding to the optimal matrix $A$ for a norm $\alpha$ is called the Lewis ellipsoid for $\alpha$. The proof of Theorem 2.1 is based on examining the properties of the optimal solution to the following optimization problem:
max \det(A) \text{ s.t. } \\
A \in \mathbb{R}^{n \times n} \\
\alpha(A) \leq 1. \tag{2.2}

Lewis showed that the optimal A satisfies \(\alpha'(A^{-1}) = n\) by a simple variational argument (which we use later in Lemma 3.2).

We are interested in norms \(\alpha\) of the following form. Let \(K \subseteq \mathbb{R}^n\) denote a symmetric convex body with associated norm \(\|\cdot\|_K\), and let \(\gamma_n\) denote the canonical Gaussian measure on \(\mathbb{R}^n\). We define the \(\ell\)-norm with respect to \(K\) for \(A \in \mathbb{R}^{n \times n}\) as

\[
\ell_k(A) = \left( \int \|Ax\|_K^2 \, d\gamma_n(x) \right)^{\frac{1}{2}}.
\]

The \(\ell\)-norm was first studied and defined by Figiel and Tomczak-Jaegermann (22). Roughly speaking, one can think of the \(\ell\)-ellipsoid as the largest ellipsoid with the property that half of its volume is contained in \(K\) (8). The \(\ell\)-norm with respect to the polar \(K^* = \{x \in \mathbb{R}^n : \langle x, y \rangle \leq 1 \forall y \in K\}\) is

\[
\ell_{K^*}(A) = \left( \int \|Ax\|^2_{K^*} \, d\gamma_n(x) \right)^{\frac{1}{2}}.
\]

The norm and the dual norm with respect to a convex body \(K\) are related by the “roundness” of \(K\), as measured by its Banach–Mazur distance to a Euclidean ball. We recall the latter and then state the connection precisely. For two convex bodies, \(K, L \subseteq \mathbb{R}^n\) the Banach–Mazur distance between \(K\) and \(L\) is

\[
d_{BM}(K, L) = \inf \{ s : s \geq 1, \exists x \in \mathbb{R}^n, T \in \mathbb{R}^{n \times n} \text{ invertible}, TK \subseteq L - x \subseteq sTK \}.
\]

In words, it is the minimum dilation \(s\) such that there is some point \(x\) and transformation \(T\) for which the set \(L - x\) is sandwiched between \(TK\) and \(sTK\). Lemma 2.2 plays an important role.

**Lemma 2.2 (8).** For \(A \in \mathbb{R}^{n \times n}\), we have that

\[
\ell_k(A) \leq \ell_{K^*}(A) \left\{ T \right\} \leq 4(1 + \log d_{BM}(K, B^n_2)) \ell_k(A).
\]

As shown by Pisier (8), one can think of the \(\ell\)-ellipsoid as the largest ellipsoid with the property that half of its volume is contained in \(K\).

### 2.2. Covering Numbers and Volume Estimates

Let \(B^n_2 \subseteq \mathbb{R}^n\) denote the \(n\)-dimensional Euclidean ball. Recall that \(N(K, D)\) is the number of translates of \(D\) required to cover \(K\). The following bounds for convex bodies \(K, D \subseteq \mathbb{R}^n\) are classical. We use \(c, C\) to denote absolute constants throughout this paper.

**Lemma 2.3.** For any two symmetric convex bodies \(K, D\),

\[
\frac{\text{vol}(K)}{\text{vol}(K \cap D)} \leq N(K, D) \leq 3^n \frac{\text{vol}(K)}{\text{vol}(K \cap D)}.
\]

Lemma 2.4 is from ref. 23.

**Lemma 2.4.** Let \(D \subseteq 0\beta K, \beta \geq 1\). Then,

\[
\text{vol}(\text{conv}(K \cup D)) \leq 4\beta n N(D, K) \text{vol}(K).
\]

The following are the Sudakov and dual Sudakov inequalities (e.g., ref. 24, section 6).

**Lemma 2.5 (Sudakov Inequality).** For any \(t > 0\), convex body \(K \subseteq \mathbb{R}^n\), and invertible matrix \(A \in \mathbb{R}^{n \times n}\),

\[
N(K, tAB^n_2) \leq e^{C_k(t^{-\ell})^2}.
\]

**Lemma 2.6 (Dual Sudakov Inequality).** For any \(t > 0\) and \(A \in \mathbb{R}^{n \times n}\)

\[
N(AB^n_2, tK) \leq e^{C_k(t^{-\ell})^2}.
\]

Lemma 2.7 gives a simple containment relationship.

**Lemma 2.7.** For any \(A \in \mathbb{R}^{n \times n}, A\) invertible, we have that

\[
\frac{1}{\ell_k(A^{-1})} K \subseteq AB^n_2 \subseteq \ell_k(A) K.
\]

**Proof:** We first show that \(E = AB^n_2 \subseteq \ell_k(A) K\). Assuming not, then there exists \(x \in E\) such that

\[
\|x\|_K = \sup_{y \in K} \|\langle y, x \rangle\|_K > \ell_k(A).
\]

Let \(y \in K^*\) be such that \(\|\langle y, x \rangle\|_K = \|x\|_K\). Then we have

\[
\ell_k(A) < \|\langle y, x \rangle\|_K = \sup_{z \in B^n_2} \|\langle z, A^T y \rangle\|_2 = \|A^T y\|_2.
\]

However, now note that

\[
\ell_k(A) = E\left[ \|AX\|^2_K \right]^{\frac{1}{2}} \geq E\left[ \|\langle y, AX \rangle\|^2_K \right]^{\frac{1}{2}} = \|A^T y\|_2,
\]

a contradiction. Therefore, \(AB^n_2 \subseteq \ell_k(A) K\) as needed. Now applying the same argument on \(E^* = A^{-1} K^*\) and \(K^*\), we get that \(E^* \subseteq \ell_{K^*}(A^{-1}) K^*\). From here via duality \((K \subseteq L \Rightarrow L^* \subseteq K^*)\), we get that

\[
\frac{1}{\ell_{K^*}(A^{-1})} K^* = (\ell_{K^*}(A^{-1}) K^*)^* \subseteq (A^{-1})^* B^n_2 = AB^n_2
\]

as needed.

### 2.3. Approximating the \(\ell\)-Norm

In our algorithm we need to approximate the integral defining the \(\ell\) norm by a finite sum. Our approximation of the \(\ell\) norm is defined as follows:

\[
\ell_k(A) = \sum_{x \in \{-1, 1\}^n} \frac{1}{2^n} \|Ax\|_K.
\]

**Lemma 2.8.** For a symmetric convex body \(K\) and any \(A \in \mathbb{R}^{n \times n}\), we have

\[
\ell_k(A) \leq 4\sqrt{8n} (1 + \log d_{BM}(K, B^n_2)) \ell_k(A).
\]

**Proof:** Let \(g_1, \ldots, g_n\) denote i.i.d. \(N(0, 1)\) Gaussians, let \(u_1, \ldots, u_n\) denote i.i.d. uniform \([-1, 1]\) random variables, and let \(A_1, \ldots, A_n \in \mathbb{R}^n\) denote the columns of \(A\). Then we have that
\[ \ell_k(A) \leq 4(1 + \log dB_M(K, B^*_2)) \sup \left\{ \sum_i (A_i, y_i) : E \left[ \left\| \sum_i A_i y_i \right\|_{K^*}^2 \right]^2 \leq 1 \right\} \] (using Lemma 2.2)

\[ \leq 4\sqrt{\frac{\pi}{2}}(1 + \log dB_M(K, B^*_2)) \sup \left\{ \sum_i (A_i, y_i) : E \left[ \left\| \sum_i u_i A_i \right\|_{K^*}^2 \right]^2 \leq 1 \right\} \]

\[ \leq 4\sqrt{\frac{\pi}{2}}(1 + \log dB_M(K, B^*_2)) E \left[ \left\| \sum_i u_i A_i \right\|_{K^*}^2 \right] = 4\sqrt{\frac{\pi}{2}}(1 + \log dB_M(K, B^*_2)) \tilde{\ell}_k(A). \]

The second inequality follows from the classical comparison $E[f(u_1, \ldots, u_n)] \leq E [\sqrt{\frac{\pi}{2}}(1 + \log dB_M(K, B^*_2))]$ for any convex function $f : \mathbb{R}^n \to \mathbb{R}$ and setting $f(x_1, \ldots, x_n) = \left\| \sum_i x_i y_i \right\|_C^2$. The last inequality follows from the following weak duality relation:

\[ \sum_i \langle A_i, y_i \rangle = E \left[ \left\| \sum_i u_i A_i \right\|_{K^*}^2 \right] \leq E \left[ \left\| \sum_j u_j y_{\ast} \right\|_{K^*}^2 \right] \leq \ell_k(A). \]

Lemma 2.9 is a strengthening due to Pisier, using proposition 8 from ref. 25. Although it is not critical for our results (the difference is only in absolute constants), we use this stronger bound in our analysis.

Lemma 2.9. For a symmetric convex body $K$ and any $A \in \mathbb{R}^{n \times n}$, we have

\[ \sqrt{\frac{\pi}{2}} \tilde{\ell}_k(A) \leq \ell_k(A) \leq c_1 \sqrt{1 + \log dB_M(K, B^*_2)} \tilde{\ell}_k(A), \]

where $c_0, c_1$ are absolute constants. Furthermore, by duality, we get that

\[ \frac{1}{c_1 \sqrt{1 + \log dB_M(K, B^*_2)}} \tilde{\ell}_k(A) \leq \ell_k(A) \leq \sqrt{\frac{\pi}{2}} \tilde{\ell}_k(A). \]

3. Algorithm for Computing an M-Ellipsoid

In this section, we present the algorithm for computing an M-ellipsoid of an arbitrary convex body given in the oracle model.

We first observe that it suffices to give an algorithm for centrally symmetric $K$. For a general convex body $K$, we may replace $K$ by the difference body $K - K$ (which is symmetric). An M-ellipsoid for $K - K$ remains one for $K$, as the covering estimate changes by at most a $2^{O(n)}$ factor. To see this, note that for any ellipsoid $E$ we have that $N(K, E) \leq N(K - K, E)$ and that

\[ N(E, K) \leq N(E, K - K) N(K - K, K) \leq N(E, K - K) N(K - K, K) \leq N(E, K - K) 2^{O(n)}, \]

where the last inequality follows by using Lemma 2.3 and the Rogers–Shephard inequality (26); i.e., $\text{vol}(K - K) \leq 4^n \text{vol}(K)$.

Our algorithm has two main components: a subroutine to compute an approximate Lewis ellipsoid for a norm given by a convex body and an implementation of the iteration that makes this ellipsoid converge to an M-ellipsoid of the original convex body. To compute the approximate $\ell$-ellipsoid we use the following convex program:

\[
\begin{align*}
\max & \quad \det(A)^{\frac{1}{2}} \\
A & \in \mathbb{R}^{n \times n}, \text{ symmetric} \\
A & \succeq 0 \\
\tilde{\ell}_k(A) & \leq 1.
\end{align*}
\] [3.1]

Here $A \succ 0$ denotes the constraint that the real symmetric matrix $A$ is positive semidefinite, i.e., all its eigenvalues are nonnegative. So, in contrast to Lewis’ program [2.2], we optimize over only symmetric positive semidefinite matrices. Another important difference is that we have replaced the $\ell$-norm with $\tilde{\ell}_k$ to make the objective function computable.

With these changes, we can solve the convex program to arbitrary accuracy in polynomial time, using the ellipsoid algorithm (4). The main theorem from ref. 4 is that a convex function can be minimized over a convex body given by a well-guaranteed membership oracle to within accuracy $\varepsilon$ so that the number of calls to the oracle is polynomial in $n$, the size of the input representation, and $\log(1/\varepsilon)$. In more detail, the set $\mathcal{S}$ over which we optimize is convex and the logarithm of the objective function is concave over this set. In addition, it is not hard to find a feasible starting point in the set and derive bounds on the radii of balls that sandwich the set (e.g., ref. 14). A membership oracle for the feasible region is straightforward: Given any $n \times n$ real matrix $X$, we can verify that it is symmetric positive semidefinite and that its $\tilde{\ell}_k$ norm is at most 1 (in fact we can obtain a separation oracle for $S$, i.e., one that provides a hyperplane that separates an infeasible $X$ from $S$). We will find approximately optimal solutions to this convex program applied to a series of convex bodies and ensure that we have an efficient oracle for each one, given only the oracle for the initial body $K$.

Given a centrally symmetric convex body $K$, as a preprocessing step, we put it in approximate John position using the Ellipsoid algorithm in polynomial time (4), so that $B^2_2 \subseteq K \subseteq nB^2_2$; i.e., $dB_M(K, B^2_2) \leq n$. We then use the M-ellipsoid algorithm described next. By $\log_i(n)$ we mean the $i$th iterated logarithm; i.e., $\log_1(n) = \log n, \log_2(n) = \log \log n$, and so on.

**M-ellipsoid algorithm**

1) Let $K_1 = K$ and $T = \log^* n$

2) For $i = 1 \ldots T - 1$,

a) Compute an approximate $\ell$-ellipsoid of $K_i$ using the convex program [3.1] to get an approximately optimal transformation $A_i$ (the corresponding ellipsoid is $A_iB^2_2$).

b) Set

\[
\ell_{out} = \frac{\sqrt{n} \tilde{\ell}_k(A_i)}{\log(\log(n))} \text{ and } \ell_{out} = \log(\log(n)) \frac{\tilde{\ell}_k(A_i^{-1})}{\sqrt{n}}
\]
c) Define
\[ K_{i+1} = \text{conv} \{ K_i \cap \text{cav}(A^n B_i^n, r_{A^n}B_i^n) \} \].

3) Output \( E = \frac{\sqrt{n}}{2^{\ell_i(T_{r,1})}} A_{r-1} B_i^n \) as the M-ellipsoid.

This is essentially an algorithmic version of Milman’s proof of the existence of M-ellipsoids. We try to construct a good ellipsoid for the original body \( K \). However, its quality depends on \( d_{BM}(K, B_i^n) \), which can be high in the beginning. Each iteration then constructs a more “round” version of \( K \) by taking the convex hull of two bodies, i.e., the first is the restriction of the current \( K \) to a not-too-large ball, and the second is a smaller ball contained in the first. Thus, the new Banach–Mazur distance of \( K \) to the unit ball is bounded by the ratio of the radii of these balls, which we will maintain as at most polylogarithmic in the previous ratio. Finally, given a good ellipsoid for the new body, i.e., one with small covering number, we will see that needs only a relatively small number of copies of it to cover the original body; i.e., we keep the ratio of volumes bounded. Because the roundness is dropping so quickly, the total number of iterations is small and the total blow-up in volume ratios is also small. We formally prove all these properties of the M-ellipsoid algorithm in the next section.

3.1 Analysis. We note that the time complexity of the algorithm is bounded by \( \text{poly}(n)^{2(n^4)} \) and the space complexity is polynomial in \( n \). In fact, the only step that takes exponential time is the evaluation of the \( \ell \)-norm constraint of the semidefinite program. This evaluation happens a polynomial number of times. The rest of computation involves applying the ellipsoid algorithm and computing oracles for successive bodies (i.e., an oracle for \( K_{i+1} \) given an oracle for \( K_i \)). Given membership oracles for two convex bodies \( A, B \), we can build membership oracles for their intersection \( A \cap B \) and for their convex hull \( \text{conv} \{ A, B \} \). These oracles only a polynomial (in \( n \)) number of calls to the oracles for \( A \) and \( B \). The complexity of the oracle grows as \( n^{(n)} \) in the \( i \)th iteration, for a maximum of \( n^{(n^{(n^{(n^4)})})} \).

A well-guaranteed oracle for a convex body consists of a membership oracle and a bound on the ratio between two balls that sandwich the body. Our analysis below includes the sandwiching ratio, which gets smaller with each iteration.

We begin by showing that Lewis’ optimality condition (Theorem 2.1) is robust to approximation and works when restricted to positive semidefinite transformations. This allows us to establish the desired properties for approximate optimizers of the convex program [3.1]. Following this, we show that the algorithm, with the property established for approximately optimal solutions, finds an M-ellipsoid of the original body.

3.1.1. Approximate Lewis ellipsoids. The main statement of this section is the following.

**Theorem 3.1.** Let \( A \) be a \((1-\varepsilon)\)-approximate optimizer to the convex program [3.1] for \( \varepsilon \leq 1/\sqrt{36n^4} \). Then

\[ \ell_k(\alpha) \leq C n (1 + \log d_{BM}(K, B_i^n))^2 \]

for an absolute constant \( C > 0 \).

The proof of Theorem 3.1 is based on Lemma 3.2. For a matrix \( T \), recall that \( \| T \|_F = \sqrt{\sum_{ij} T_{ij}^2} \) is its Frobenius norm, and \( \| T \|_2 = \sup_{\| x \|_2^2 = 1} \| Tx \|_2 \) is the operator norm.

**Lemma 3.2.** Let \( K \) be such that \( B_i^n \subseteq K \subseteq n B_i^n \) and \( A \in \mathbb{R}^{n \times n} \) be an \((1-\varepsilon)\)-approximate optimizer for the convex program [3.1], i.e.,

\[ \det(A) \geq (1-\varepsilon) \text{OPT} \].

Then for \( \varepsilon \leq 1/\sqrt{36n^4} \), we have that

\[ \ell_k(\alpha)^2 \leq n (1 + 6n^2 \varepsilon^2) \leq 2n \].

**Proof:** For simplicity of notation, we write \( \ell_k(T) = \alpha(T) \) for \( T \in \mathbb{R}^{n \times n} \). Take \( T \in \mathbb{R}^{n \times n} \) (not necessarily positive semidefinite) satisfying \( \alpha(T) \leq 1 \).

First note that \( I_n / \alpha(I_n) \) is a feasible solution to [3.1], satisfying

\[ \det \left( \frac{I_n}{\alpha(I_n)} \right)^2 = \frac{1}{\alpha(I_n)^2} \geq \frac{1}{\| I_n \|_F^2} = \frac{1}{\sqrt{n}} \].

Let \( A_{\text{OPT}} \geq 0 \) denote the optimal solution to [3.1]. Because \( \det(A_{\text{OPT}}) \geq \frac{1}{\sqrt{n}} \), we clearly have that \( A_{\text{OPT}} > 0 \). Therefore, for \( \delta > 0 \) small enough we have that \( A_{\text{OPT}} + \delta I \geq 0 \). From this, we see that \( (A_{\text{OPT}} + \delta I) / (\alpha(A_{\text{OPT}} + \delta I)) \) is also feasible for [3.1] as \( (A_{\text{OPT}} + \delta I) / (\alpha(A_{\text{OPT}} + \delta I)) = 1 \). Because \( A_{\text{OPT}} \) is the optimal solution, we have that

\[ \det \left( \frac{A_{\text{OPT}} + \delta I}{\alpha(A_{\text{OPT}} + \delta I)} \right) \leq \det(A_{\text{OPT}})^2 \].

Rewriting this and using the triangle inequality,

\[ \det(A_{\text{OPT}} + \delta I) \leq \det(A_{\text{OPT}})^2 (\alpha(A_{\text{OPT}}) + \delta I) \]

\[ \leq \det(A_{\text{OPT}})^2 (1 + \delta) \].

Dividing by \( \det(A_{\text{OPT}})^2 \) on both sides, we get that

\[ (I_n + \delta A_{\text{OPT}}^{-1} T)^2 \leq 1 + \delta \].

Because both sides are equal at \( \delta = 0 \), we must have the same inequality for the derivatives with respect to \( \delta \) at 0. This yields

\[ \frac{1}{n} \text{tr}(A_{\text{OPT}}^{-1} T) \leq 1 \implies \text{tr}(A_{\text{OPT}}^{-1} T) \leq n \].

Up to this point the **Proof** is essentially the same as Lewis’ proof of Theorem 2.1. We now depart from that **Proof** to account for approximately optimal solutions. We use the following three claims.

**Claim 1.** \( \alpha(T) \leq \| T \|_F \leq n \alpha(T) \).

**Proof (of Claim 1):** Let \( U \) denote a uniform vector in \((-1,1)^n\). Because \( \frac{1}{n} \| x \|_2 \leq \| x \|_2 \) for any \( x \in \mathbb{R}^n \), we have that

\[ \alpha(T) = E \left[ \| UT \|_2^2 \right] \geq \frac{1}{n} \left[ \| UT \|_2^2 \right] = \frac{1}{n} \| T \|_F. \]

Now using the inequality \( \| x \|_K \leq \| x \|_2 \) for \( x \in \mathbb{R}^n \), a similar argument yields \( \alpha(T) \leq \| T \|_K \).

**Claim 2.** \( \| A_{\text{OPT}} \|_K \leq n \).

**Proof (of Claim 2):** Let \( \sigma \) denote the largest eigenvalue of \( A_{\text{OPT}}^{-1} \) and \( v \in \mathbb{R}^n \) be an associated unit eigenvector. Because \( A_{\text{OPT}} \geq 0 \), we have that \( A_{\text{OPT}}^{-1} \geq 0 \), and hence \( \sigma = \| A_{\text{OPT}}^{-1} \|_K \). Now note that \( A_{\text{OPT}} + \delta v v^T \geq 0 \) for any \( \delta \geq 0 \) and that \( \| v v^T \|_F = \| v \|_2^2 = 1 \). Therefore, by Eq. 3.3, we have that

\[ n \geq \text{tr}(A^{-1}(v v^T)) = \text{tr}(\sigma v v^T) = \sigma \]

as needed.

**Claim 3.** \( A^{-1} \leq (1 + 6\sqrt{n} e) A_{\text{OPT}}^{-1} \).

We can now complete the **Proof** of Lemma 3.2 (we will prove the last claim presently). Take \( T \in \mathbb{R}^{n \times n} \) satisfying \( \alpha(T) \leq 1 \). By
Claim 1, we note that \( \|T\|_F \leq n\alpha(T) \leq n \). Now by Eq. 3.3, we have that
\[
\text{tr}(A^{-1}T) = \text{tr}(A^{-1}_{OPT}T) + \text{tr}(A^{-1} - A^{-1}_{OPT})T) \leq n
\]
\[
+ \|A^{-1} - A^{-1}_{OPT}\|_F \|T\|_F \leq n + n\|A^{-1} - A^{-1}_{OPT}\|_F.
\]
We bound the second term using Claim 3. Because \( A^{-1} \leq (1 + 6\sqrt{n}/e)^{-1}A_{OPT} \), we have that \( A^{-1} - A_{OPT} \leq 6\sqrt{n}/e A_{OPT} \), and hence, using Claim 2,
\[
\|A^{-1} - A_{OPT}\|_F \leq \sqrt{n}\|A^{-1} - A_{OPT}\|_2 \leq 6n\sqrt{\epsilon}\|A_{OPT}\|_2 \leq 6n^2\sqrt{\epsilon}.
\]
Using this bound, we get
\[
\text{tr}(A^{-1}T) \leq n + 6n^3\sqrt{\epsilon} = n(1 + 6n^2\sqrt{\epsilon})
\]
for any \( T \in \mathbb{R}^{n \times n} \) satisfying \( \alpha(T) \leq 1 \). Thus, we get that \( \alpha^*(A^{-1}) \leq 1 + 6n^2\sqrt{\epsilon} \). Together with the constraint \( \alpha(A) \leq 1 \), the conclusion of Lemma 3.2 follows. It remains to prove Claim 3.

**Proof of Claim 3:** Since \( A \) is a \((1 - \epsilon)\)-approximate maximizer to (3.1), we have that
\[
\text{det}(A)^1 \geq (1 - \epsilon)\text{det}(A_{OPT}) \rightarrow \text{det}(A) \geq (1 - n\epsilon)\text{det}(A_{OPT}).
\]
We begin by proving by proving \( A \geq (1 - 3\sqrt{n}/e)A_{OPT} \). Now note that
\[
A \geq (1 - 3\sqrt{n}/e)A_{OPT} \Rightarrow A_{OPT}^{-1/2}AA_{OPT}^{-1/2} \geq (1 - 3\sqrt{n}/e)I_n.
\]
Hence letting \( B = A_{OPT}^{-1/2}AA_{OPT}^{-1/2} \), it suffices to show that \( B \geq (1 - 3\sqrt{n}/e)I_n \). From here, we note that \( 1 \geq \text{det}(B) = \text{det}(A) / \text{det}(A_{OPT}) \geq (1 - n\epsilon) \). Now from Eq. 3.3, we have that
\[
\text{tr}(B) = \text{tr}(A_{OPT}^{-1/2}AA_{OPT}^{-1/2}) = \text{tr}(A_{OPT}^{-1/2}A) \leq n.
\]
Let \( \sigma_1, \ldots, \sigma_n \) denote the eigenvalues of \( B \) in nonincreasing order. We first note that \( \sigma_n \geq 1 \) because otherwise
\[
\text{det}(B) = \prod_{i=1}^{n} \sigma_i \geq \sigma_n^n > 1
\]
is a contradiction. Furthermore, because \( B \geq 0 \), we have that \( 0 < \sigma_n \leq 1 \). So we may write \( \sigma_n = 1 - \epsilon_0 \), for \( 1 > \epsilon_0 \geq 0 \). Now because \( \sum_{i=1}^{n} \sigma_i = \text{tr}(B) \leq n \), by the inequality between the arithmetic mean and the geometric mean, we have that
\[
\text{det}(B) = \sigma_n \prod_{i=1}^{n-1} \sigma_i \leq (1 - \epsilon_0) \left( \frac{\sum_{i=1}^{n-1} \sigma_i}{n-1} \right)^{n-1} \leq (1 - \epsilon_0) \left( 1 + \frac{\epsilon_0}{n-1} \right)^{n-1}.
\]
Using the inequality \( 1 + x \leq e^x \leq 1 + x + \frac{e-1}{2} x^2 \) for \( x \in [-1, 1] \), we get that
\[
(1 - \epsilon_0) \left( 1 + \frac{\epsilon_0}{n-1} \right)^{n-1} \leq (1 - \epsilon_0) e^{\epsilon_0} \leq (1 - \epsilon_0) \left( 1 + \frac{e-1}{2} \epsilon_0 \right) = 1 - \frac{3 - e}{2} \epsilon_0 - \frac{e-1}{2} \epsilon_0 \leq 1 \frac{3 - e}{2} \epsilon_0.
\]
From this we have
\[
1 - \frac{3 - e}{2} \epsilon_0 \geq \text{det}(B) \geq (1 - n\epsilon) \Rightarrow \epsilon_0 \leq \frac{\sqrt{2}}{3 - e} n \epsilon \leq 3n \epsilon.
\]
Therefore, \( \alpha_n = 1 - \epsilon_0 \geq 1 - 3\sqrt{n}/e \Rightarrow B \geq (1 - 3\sqrt{n}/e)I_n \Rightarrow A \geq (1 - 3\sqrt{n}/e)A_{OPT} \) as needed. Hence,
\[
A^{-1} \geq \left( \frac{1}{1 - 3\sqrt{n}/e} \right) A_{OPT}^{-1} \geq (1 + 6\sqrt{n}/e)A_{OPT}^{-1}
\]
for \( \epsilon \leq 1/36n \), proving the claim.

This completes the proof of Theorem 3.2.

We can now prove Theorem 3.1.

**Proof of Theorem 3.1:** Using Lemmas 2.2, 2.9, and 3.2 in that order, we have
\[
k_c(A) \leq 4 (1 + \log d_{BM}(K, B_2^c)) k_c(A) \leq C (1 + \log d_{BM}(K, B_2^c)) k_c(A) \leq 2 C n (1 + \log d_{BM}(K, B_2^c))
\]
for \( 1 \leq i \leq T - 1 \) define
\[
K_{i+1}^{in} = \text{conv} \{ K_i^{in}, r_{in}^{i}, A_iB_2^{in} \} K_{i+1}^{out} = K_{i+1}^{in} \cap r_{out}^{i}A_iB_2^{in},
\]
where \( r_{in}^{i}, r_{out}^{i} \) are defined as \( r_{in}^{i}, r_{out}^{i} \) in the \( i \)th iteration of the main loop of the M-ellipsoid algorithm. Recall that
\[
r_{in}^{i} = \frac{\sqrt{n}}{\log^{(i)}(n) k_c(A_i)} \text{ and } r_{out}^{i} = \log^{(i)}(n) \frac{k_c(A_i)}{\sqrt{n}}
\]
so that
\[
r_{out}^{i} = n \frac{k_c(A_i)}{k_c(A_{OPT})} r_{out}^{i} A_{OPT}^{-1}.
\]
Thus, \( K_{i}^{in} \) contains a ball of radius \( r_{in}^{i} \) whereas \( K_{i}^{out} \) is contained in a ball of radius \( r_{out}^{i} \). By construction, we have the relations
\[
K \subseteq K_{i}^{in} \subseteq \cdots \subseteq K_{T}^{in} \subseteq K_{T}^{out} \subseteq K_{i}^{out} \subseteq \cdots \subseteq K_{T}^{out},
\]
for any constant \( C \geq 1 \).

The proof of Theorem 3.1 is based on the following inductive lemmas that quantify the properties of the sequences of bodies defined above.

**Lemma 3.3:** \( \forall i \in [T], \) we have that \( d_{BM}(K_i, B_2^c) \leq C (\log^{(i-1)}(n)) \).

**Proof:** For the base case, we have that \( d_{BM}(K_1, B_2^c) \leq \sqrt{n} \leq C n \) for any constant \( C \geq 1 \). For the general case, by construction of \( K_{i+1} \) we have that
\[
r_{out}^{i} A_iB_2^{in} \subseteq K_{i+1} \subseteq r_{out}^{i} A_iB_2^{in}.
\]
Therefore,
\[ d_{BM}(K_{i+1}, B_i^1) \leq \frac{c_{d_{BM}}}{r_i} \]
\[ = \frac{c_{d_{BM}}}{n} \ell_{K_i}(A_i) \]
\[ \leq C_{d_{BM}} \ell_{K_i}(A_i) \]
\[ \leq C_{d_{BM}} \left( \log \frac{1}{n} \right)^\frac{3}{2} \]
\[ \text{(by Theorem 3.1).} \]

Using the fact that \( \log \frac{1}{n} \geq 1, \forall i \in [T-1], \) a direct computation shows that the above recurrence equation implies the existence of a constant \( C \geq 1 \) depending only on \( C_1 \) such that the stated bound on \( d_{BM}(K_{i+1}, B_i^1) \) holds.

**Lemma 3.4.** For \( i \in [T-1], \) we have that
\[
\max \left\{ \frac{\text{vol}(K_{i+1})}{\text{vol}(K_i)}, \frac{\text{vol}(K_i)}{\text{vol}(K_{i+1})} \right\} \leq e^{C_{1-n} \log \frac{1}{n}}.
\]

**Proof:** By Lemma 2.3, the fact that \( K_{i+1}^n \subseteq K_i, \) Lemma 2.5, Lemma 2.9, and Lemma 3.3, we have that
\[
\frac{\text{vol}(K_{i+1})}{\text{vol}(K_i)} \leq N(K_i, r_{out} A_i B_2) \leq N(K_i, r_{out} A_i B_2^n)
\]
\[
\leq C \left( \frac{\ell_{K_i}(A_i)}{r_i} \right)^2 \leq C \left\{ \frac{\ell_{K_i}(A_i)}{r_i} \right\}^2
\]
\[
\leq C e^{C_{1-n} \log \frac{1}{n}}.
\]

By Lemmas 2.7, 2.9, and 3.3, we see that
\[
r_{out} A_i B_2^n \subseteq r_{out} A_i B_2 \subseteq C_1 \sqrt{n} K_{i+1}^n.
\]

Next, by Lemma 2.4, the fact that \( K_i \subseteq K_{i+1}^n, \) Lemma 2.6, Lemma 2.9, and Lemma 3.3, we have that
\[
\frac{\text{vol}(K_{i+1}^n)}{\text{vol}(K_i)} \leq C_1 \sqrt{n} N(r_{out} A_i B_2, K_i)
\]
\[
\leq C_1 \sqrt{n} e^{C_{1-n} \log \frac{1}{n}}.
\]

We are now ready to complete the proof.

**Proof of Theorem 1.1:** By construction of \( K_T, \) we note that
\[
r_{out}^{-1} A_{T-1} B_2 \subseteq K_T \subseteq r_{out}^{-1} A_{T-1} B_2^n,
\]
where by Lemma 3.3 we have that \( r_{out}^{-1} / r_{in}^{-1} = O(1). \) Therefore, the returned ellipsoid \( E = \frac{\sqrt{n}}{r_{in}^{-1} A_{T-1} B_2^n} \) (last line of the M-ellipsoid algorithm) satisfies that
\[
1 \leq E \subseteq K_T \subseteq CE
\]
for an absolute constant \( C \geq 1. \) Next, by Lemma 2.3, we have that
\[
N(K, E). N(E, K) \leq 3^n \max \{ \text{vol}(K), \text{vol}(E) \}.
\]
Now we see that
\[
K \subseteq K_T \subseteq CK_T \subseteq C K_T
\]
and that
\[
K_T \subseteq K_T^{in} \subseteq CK_T^{in} \subseteq E \subseteq C K_T \subseteq C K_T^{in}.
\]

Therefore,
\[
\frac{\max \{ \text{vol}(K), \text{vol}(E) \}}{\text{vol}(K \cap E)} \leq C e^{C_{1-n} \log \frac{1}{n}}.
\]

Finally, by Lemma 3.4 we have that
\[
\frac{\text{vol}(K_{i+1})}{\text{vol}(K_i)} \leq \prod_{i=1}^{T-1} \frac{\text{vol}(K_i)}{\text{vol}(K_{i+1})} \leq \prod_{i=1}^{T-1} e^{C_{1-n} \log \frac{1}{n}} = 2^{O(n)}.
\]

Combining the above inequalities yields the desired guarantee on the algorithm. The time complexity is \( 2^{O(n)} \), dominated by the time to evaluate the \( \ell_2 \) norm. The space is polynomial because all we need to maintain are efficient oracles for the successive bodies \( K_i \), which can be done space efficiently for the operations of intersection and convex hull used in the algorithm (4).

4. **An Asymptotically Optimal Volume Algorithm**

In this section, we show how to modify our M-ellipsoid algorithm to prove Theorem 1.5.

In the M-ellipsoid algorithm of the previous section, we construct a series of convex bodies \( K_0 = K, K_1, \ldots, K_T \) such that the covering numbers \( N(K_0, K_T) \) and \( N(K_T, K_T) \) are bounded by \( 2^{O(n)} \) and the final body \( K_T \) has \( d_{BM}(K_T, B_2^n) < C \) for some constant \( C \). Our modification constructs a similar sequence of bodies, but rather than bounding covering numbers, we ensure that
\[
e^{-C_{1-n} \text{vol}(K)} \leq \text{vol}(K(i)) \leq e^{C_{1-n} \text{vol}(K)}
\]

and
\[
d_{BM}(K_T, B_2^n) \leq C \frac{\text{ln}(1/e)}{\text{vol}(K_T)}
\]

Then we approximate the volume of \( K_T \) by finding an approximately \( \epsilon \)-ellipsoid \( E \) for it and covering it with translations of a maximal parallelohedron that fits in \( E \). Here is the precise algorithm. The reader can see that it is similar to the iteration from the previous section, but applied at a slower rate.

**Deterministic Volume (\( K, \epsilon \)).**

1. Let \( K_1 = K \) and \( T = \text{log} n \)
2. For \( i = 1 \ldots T-1 \),
   a) Compute an approximate \( \epsilon \)-ellipsoid of \( K_i \) using the convex program [3.1] to get an approximately optimal transformation \( A_i \) (the corresponding ellipsoid is \( A_i B_2^n \),
   b) Set
   \[
r_i = \frac{\epsilon \sqrt{n}}{\text{ln}(1/\epsilon) C \text{vol}(K_i)} \quad \text{and} \quad r_{out} = \frac{\epsilon \sqrt{n}}{\text{vol}(K_i)}.
   \]
   c) Define
   \[
   K_{i+1} = \text{conv} \left\{ K_i \cap r_{out} A_i B_2^n, r_{in} A_i B_2^n \right\}.
   \]
3) Compute the ellipsoid \( E = r_n A_{T-1} B_2^2 \) and a maximum volume parallelepiped \( P \) inscribed in \( E \) (via the principal components of \( A_{T-1} \)).

4) Cover \( K_T \) with disjoint copies of \( eP \). Output \( kvol(P) \), where \( k \) is the number of copies used.

**Proof of Theorem 1.5:** Let \( a_i = \log^{(l)} n \). As in Lemma 3.3, we bound the Banach–Mazur distance via the following recurrence:

\[
d_{BM}(K_{i+1}, B_2^2) \leq \frac{r_{\text{out}}}{r_{\text{in}}} \leq C \frac{\ln(1/e)}{e^2} (\log^{(l)}(n))^2 \left( 1 + \log d_{BM}(K_i, B_2^2) \right)^2.
\]

From the above recurrence a direct computation reveals that for \( \forall i \in [T] \),

\[
d_{BM}(K_i, B_2^2) \leq C \frac{\ln(1/e)}{e^2} (\log^{(l-1)}(n))^2.
\]

We now show that the volumes of the \( K_i \) bodies change very slowly. This enables us to conclude that the volume of \( K_T \) is very close to the volume of \( K \).

By Lemmas 2.7 and 2.9 and the above bound on \( d_{BM}(K_i, B_2^2) \), we have that

\[
r_{\text{out}} A_i B_2^2 \subseteq r_{\text{out}} f_{K_i}(A_i) K_i \subseteq C \frac{\sqrt{n \log d_{BM}(K_i, B_2^2)}}{\sqrt{\ln(1/e)\log^{(l)}(n)}} K_i \subseteq C e^{\sqrt{n} K_i}
\]

and that

\[
r_{\text{out}} A_i B_2^2 =
C \frac{\sqrt{n \log(\ln(1/e)\log^{(l)}(n)) n^{1/2} K_i \cdot (A_i)^{-1}}}{e^{\sqrt{n}} A_i B_2^2 \geq C \frac{1}{e^{\sqrt{n} K_i}}.
\]

Therefore, if \( e \leq C/\sqrt{n} \), then \( K_{i+1} = \text{conv}(r_{\text{out}} A_i B_2^2, K_i \cap r_{\text{out}} A_i B_2^2) = K_i \). Because this holds for all \( i \in [T-1] \), we get that \( K_T = K \) and hence \( \text{vol}(K_T) = \text{vol}(K) \).

Now assume that \( e \geq C/\sqrt{n} \). Then for \( i \in [T-1] \), using Lemmas 2.3 and 2.5, we have

\[
\text{vol}(K_{i+1}) \geq \text{vol}(K_i \cap r_{\text{out}} B_2^2)
\]

\[
\geq \frac{\text{vol}(K_i)}{N(K_i, r_{\text{out}} B_2^2)}
\]

\[
\geq C \left( 1 - C \left( 1 + 1/e \right)^{\sqrt{L_1}} \right)^2 \text{vol}(K_i)
\]

\[
\geq e^{-C (1 + 1/e) \log(\ln(1/e)\log^{(l)}(n)) n^{1/2} \text{vol}(K_i)}
\]

\[
\geq e^{-C \text{ne}^{\log^{(l)}(n)} \text{vol}(K_i)}.
\]

From the above, we get that

\[
\frac{\text{vol}(K_T)}{\text{vol}(K)} = \prod_{i=1}^{T-1} \frac{\text{vol}(K_{i+1})}{\text{vol}(K_i)} \geq \prod_{i=1}^{T-1} e^{-C \text{ne}^{\log^{(l)}(n)} \text{vol}(K_i)} \geq e^{-C \text{ne}}.
\]

Next via Lemma 2.4, the above containment, and Lemma 2.5, we have

\[
\text{vol}(K_{i+1}) \leq \text{vol}(\text{conv}\{K_i, r_n B_2^2\})
\]

\[
\leq C(e^{\sqrt{n}} n N(r_n B_2^2)) \text{vol}(K_i)
\]

\[
\leq C(e^{n})^{2} \text{vol}(K_i)
\]

\[
\leq C(e^{n})^{2} \text{vol}(K_i) \text{vol}(K) / \text{vol}(E)
\]

\[
\leq C(e^{n})^{2} \text{vol}(K_i) / \text{vol}(E)
\]

\[
\leq C(e^{n})^{2} \text{vol}(K_i) / \text{vol}(E)
\]

Finally, we describe the enumeration procedure that will ensure that the time bound is \( (1/e)^{O(n)} \) and the space used is polynomial in \( n \). The number of parallelepipeds enumerated could be as high as \( (1/e)^{O(n)} \). However, we do not need to store all of the copies that intersect \( K \); we need only the number. To do this using polynomial space, we start with a parallelepiped inside \( K \) designated as the root and fix an order on its axes. For every other parallelepiped in the axis-aligned tiling, designate its parent to be an adjacent node closer to the root in Manhattan distance along the axes of the parallelepiped (i.e., the usual \( L_1 \) distance for the centers of the parallelepipeds after transforming parallelepipeds to cuboids), breaking ties using the ordering on coordinates. This ensures that a traversal of the tree defined by this structure takes time linear in the number of nodes in the tree and space linear in the dimension. This is a special case of a more general space-efficient traversal technique studied by Avis and Fukuda (27).

**Acknowledgments.** We thank Assaf Naor and Grigoris Paouris for helpful pointers and discussions, specifically for showing us the proofs of Lemmas 2.8 and 2.9. This work was partially supported by the National Science Foundation.

1. Shor NZ (1977) Cut-off method with space extension in convex programming problems. Kibernetika 13(1):94-96.
2. Yudin DB, Nemirovskii AS (1976) Evaluation of the information complexity of mathematical programming problems (in Russian). Ekonomika i Matematicheskie Metody 13(2):3-46.
3. Khachiyan LG (1980) Polynomial algorithms in linear programming. USSR Comput Math Phys 20:53-72.
4. Grötschel M, Lovász L, Schrijver A (1988) Geometric Algorithms and Combinatorial Optimization (Springer, Berlin).
5. Kannan R, Lovász L, Simonovits M (1997) Random walks and an \( O^{*}(n^4) \) volume algorithm for convex bodies. Random Structures Algorithms 11(1):1-50.
6. Lovász L, Vempala S (2006) Simulated annealing in convex bodies and an \( O^{*}(n^4) \) volume algorithm. J Comput Syst Sci 72(2):392-417.
7. Vempala S (2010) Recent progress and open problems in algorithmic convex geometry. Foundations of Software Technology and Theoretical Computer Science, eds Loday K, Mahajan M (Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, Dagstuhl, Germany), pp 42–64.

8. Pisier G (1989) The Volume of Convex Bodies and Banach Space Geometry (Cambridge Univ Press, Cambridge, UK).

9. Milman V (1986) The reverse Brunn-Minkowski inequality and its applications to the local theory of normed spaces. C R Acad Sci Paris 302(1):25–28.

10. Klartag B (2000) On convex perturbations with a bounded isotropic constant. Geom Funct Anal 16(6):1274–1290.

11. Dadush D, Peikert C, Vempala S (2011) Enumerative lattice algorithms in any norm via m-ellipsoid coverings. IEEE Symposium on the Foundations of Computer Science, ed Ostrovsky R (IEEE Computer Society, Washington, DC), pp 580–589.

12. Furedi Z, Barany I (1986) Computing the volume is difficult. STOC ’86: Proceedings of the Eighteenth annual ACM Symposium on Theory of Computing, ed Hartmanis J (Association for Computing Machinery, New York), pp 442–447.

13. Dyer ME, Frieze AM, Kannan R (1989) A random polynomial time algorithm for approximating the volume of convex bodies. ACM Symposium on the Theory of Computing, ed Simon J (Association for Computing Machinery, New York), pp 375–381.

14. Dadush D, Vempala S (2012) Deterministic construction of an approximate m-ellipsoid and its application to derandomizing lattice algorithms. ACM-SIAM Symposium on Discrete Algorithms, ed Rabani Y (Association for Computing Machinery, New York; Society for Industrial and Applied Mathematics, Philadelphia, PA), pp 1445–1456.

15. Dyer ME, Frieze AM, Kannan R (1991) A random polynomial-time algorithm for approximating the volume of convex bodies. J ACM 38(1):1–17.

16. Elekes G (1986) A geometric inequality and the complexity of computing volume. Discrete Comput Geom 1:289–292.

17. Furedi Z, Barany I (1988) Approximation of the sphere by polytopes having few vertices. Proc AMS 102(3):651–659.

18. Ajtai M, Kumar R, Sivakumar D (2001) A sieve algorithm for the shortest lattice vector problem. ACM Symposium on the Theory of Computing, ed Vitter J, Spirakis P, Yannakakis, M (Association for Computing Machinery, New York), pp 601–610.

19. Arvind V, Joglekar PS (2008) Some sieving algorithms for lattice problems. Foundations of Software Technology and Theoretical Computer Science, eds Hariri, R, Mukund M, Vinay V (Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, Dagstuhl, Germany), pp 25–36.

20. Dadush D, Vempala S (2012) Deterministic construction of an approximate m-ellipsoid and its application to derandomizing lattice algorithms. ACM-SIAM Symposium on Discrete Algorithms, ed Rabani Y (Association for Computing Machinery, New York), pp 351–358.

21. Lewis DR (1979) Ellipsoids defined by Banach ideal norms. Mathematika 26(1):18–29.

22. Figiel T, Tomczak-Jaegermann N (1979) Projections onto Hilbertian subspaces of Banach spaces. J Funct Anal 33(2):155–171.

23. Milman V (1988) Isomorphic symmetrization and geometric inequalities. Geometric Aspects of Functional Analysis, Lecture Notes in Mathematics, eds Lindenstrauss J, Milman V (Springer, Berlin), Vol 1317, pp 107–131.

24. Giannopoulos AA, Milman VD (2001) Euclidean structure in finite dimensional normed spaces. Handbook of the Geometry of Banach Spaces, eds Johnson WB, Lindenstrauss J (Elsevier, Amsterdam), Vol 1, pp 707–779.

25. Pisier G (1981) Remarks on an unpublished result of B. Maurey Ecole Polytechnique, Paris, France. Seminaire d’Analyse Functionnelle 1980-81, Expose 13, V.1–V.12.

26. Rogers CA, Shephard GC (1957) The difference body of a convex body. Arch Math 8: 220–232.

27. Avis D, Fukuda K (1993) Reverse search for enumeration. Discrete Appl Math 65(1-3): 21–46.