APPROXIMATION OF RADII AND NORM-MAXIMA: NO NEED TO RANDOMIZE

ANDREAS BRIEDEN
Zentrum Mathematik
Technische Universität München
80290 München, Germany
brieden@mathematik.tu-muenchen.de

PETER GRITZMANN
Zentrum Mathematik
Technische Universität München
80290 München, Germany
gritzman@mathematik.tu-muenchen.de

RAVI KANNAN
Dept. of Computer Science
Yale University
New Haven, CT 06520
kannan@cs.yale.edu

VICTOR KLEE
Dept. of Mathematics
University of Washington
Seattle, WA 98195
klee@math.washington.edu

LÁSZLÓ LOVÁSZ
Dept. of Computer Science
Yale University
New Haven CT 06520
lovasz@cs.yale.edu

MIKLÓS SIMONOVITS
Math. Inst. Hung. Acad. Sci.
Budapest, Reáltanoda u. 13-15
H-1053 Hungary
miki@math-inst.hu

Abstract: *For a convex body K in euclidean n-space $\mathbb{E}^n$ let $m(K)$ denote the circumradius, the diameter, the inradius or the width of K, or the maximum of the l_2 norm over K. Then for each $c_1 > 1$ there is a deterministic polynomial-time algorithm $\mathcal{A}$ that computes, for each $K \subset \mathbb{R}^n$ given by a well-guaranteed optimization oracle, an approximation $m_{\mathcal{A}}(K)$ of $m(K)$ such that*

$$m_{\mathcal{A}}(K) \leq m(K) \leq c_1\sqrt{\frac{n}{\log n}}m_{\mathcal{A}}(K).$$

This result is essentially best-possible even if randomization is permitted since there exists a positive constant c_2 such that if a randomized polynomial-time algorithm $\mathcal{A}$ produces a value $m_{\mathcal{A}}(K) \leq m(K)$ for each convex body $K \subset \mathbb{R}^n$, then the probability that

$$m_{\mathcal{A}}(K_0) \leq m(K_0) \leq c_2\sqrt{\frac{n}{\log n}}m_{\mathcal{A}}(K_0)$$

is less than $1/2$ for some such body K_0.

In addition to these results for euclidean spaces, we give tight results for the error of deterministic polynomial-time approximations of radii and norm-maxima for convex bodies in finite-dimensional l_p spaces.

Research was supported by the Discrete Mathematics program of Yale University, by NSF grants CCR 9208597, CRC 9402916, and DMS 9300192, by a DAAD-NSF-travel grant, and by a DFG grant.

1. Introduction

Given a convex body K (or simply *body*) in the n-dimensional Minkowski space $(\mathbb{R}^n, \| \quad \|)$ (with $n \geq 2$), we are concerned with computing or approximating its fundamental geometric parameters *diameter* (i.e., the maximal distance between two points of K), *width* (i.e., the minimum of the distances between pairs of parallel supporting hyperplanes), *inradius* (i.e., the radius of a largest ball that is contained in K), and *circumradius* (i.e., the radius of a smallest ball that contains K) – here these are all called *radii* –, and the norm-maximum $\max_{x\in K} \|x\|$. The computational complexity of radii computation and norm-maximization for polytopes was studied in [8] and [10]. Here we assume that K is given by an oracle, as described in detail in Grötschel, Lovász and Schrijver [11] and briefly below, and study the error in deterministic and randomized polynomial-time approximations. Our results are in sharp contrast to those known for another fundamental functional, the volume of K.

To set our results in some broader perspective let us begin with the euclidean case, i.e., with bodies in $\mathbb{E}^n$.

A first rough approximation of the volume and also of the radii of a body K can be obtained by computing an approximate "Löwner–John ellipsoid" of the body [11]. This yields an approximation of its volume with relative error $O(n^{3n/2})$ and of its radii with relative error $O(n^{3/2})$. (Note that we use the 'asymmetric relative error' as a measure of the performance of algorithms here that reflects the fact that we can always guarantee a 'one-sided approximation.' The corresponding 'symmetric relative error' is then just the square root of the error terms given in the following.) While these factors grow with n, nothing substantially better can be achieved in polynomial time, at least not in a deterministic way. Bárány and Füredi [1] showed, extending ideas of Elekes [7], that in order to compute the volume approximately with a relative error less than $(cn/\log(n))^n$, or to compute the diameter or width of K approximately with a relative error less than $(\sqrt{cn/\log n})$, one has to make a superpolynomial number of calls to the oracle. This statement about diameter and width holds also for circumradius, inradius, and norm-maximization (see Theorem 3.2 below). Thus the message of the results of Elekes, Bárány and Füredi is that deterministic algorithms are very bad in estimating these parameters for bodies in high-dimensional euclidean spaces.

These negative results concern the oracle model (see below). However, hardness results are also known when K is given as the solution set of a system of linear inequalities: then the computation of volume is #P-hard [5], [13], and the computation of radii and norm-maximum is NP-hard [8], [10], even for rather simple sorts of bodies.

A breakthrough in the positive direction was achieved by Dyer, Frieze, and Kannan [6], who gave a randomized polynomial-time algorithm that finds an approximation of the volume with arbitrarily small relative error. Thus for volume computation in the oracle model, randomization provably helps. (See [12] for more details and the fastest known volume algorithm).

The success of randomized algorithms in volume approximation, in conjunction with the similar behavior of volume and radii in deterministic approximation, suggests that randomization might also be useful in computing radii. However, a principal result of this paper is that *randomization does not help here.* In fact, an analysis of the complexity (in an oracle model) of both deterministic and non-deterministic algorithms shows that they achieve essentially the same approximation ratio in polynomial time. It turns out that the approximation ratio $O(\sqrt{n/\log n})$ can be achieved by a deterministic polynomial-time algorithm matching the negative result of Bárány and Füredi; on the other hand, we prove that even randomized algorithms cannot achieve, in polynomial time, any better approximation ratio for radii and the norm-maximum than this.

In the positive direction, we show that randomization does give an improvement in the degree of the polynomial.

The proofs depend on results in Section 4 that show the oracle complexity of the norm-maximization and radii problems to be very closely related to the problem of covering a sphere with a prescribed number of caps, or equivalent, approximating a sphere with proper polytopes. More precisely, for norm-maximization, circumradius, and diameter the complexity can be measured in terms of the number of facets of a polytope that contains the unit ball $\mathbb{B}^n$ and that itself is contained in the unit ball scaled by a factor $\lambda \geq 1$ that depends on the approximation error ($\mathcal{H}$-approximation), and for inradius and width in terms of the number of vertices of a polytope contained in $\mathbb{B}^n$ that approximates $\mathbb{B}^n$ with respect to the inradius ($\mathcal{V}$-approximation). This connection enables us to invoke basic results on the measure of caps, along with a construction of Kochol [14].

Another way of viewing the results is that rather than approximating the body K by another body (like an ellipsoid as in the approach of [11] mentioned above) the euclidean space $\mathbb{E}^n$ is approximated by a suitable Minkowski space whose norm is polytopal, i.e., for which the unit ball is a polytope, where the functionals can be computed in polynomial time. This view allows using techniques of Carl and Pajor [3], [4] on the entropy in Banach spaces together with a generalization of Kochol's construction to obtain positive and negative result for deterministic approximation of radii and norm-maxima in an arbitrary finite-dimensional l_p space. This way we get quantitative information on how the "distance" of a Minkowski space from being polytopal influences the error in polynomial-time approximations of radii and norm-maxima.

For details omitted here and various other results see [2], the full journal version of this paper.

2. What is a body?

There is no way to describe a general convex body K by a finite number of data, and hence it is customary to describe bodies by an *oracle* (subroutine), i.e., a "black box" to which we can present questions about K and use the answers in our algorithms. Depending on the kind of questions allowed and on the kind of answers given, we get different descriptions of the body, and these may be used in algorithms in very different ways. However, the main result of Grötschel, Lovász and Schrijver [11] says that all the natural oracles to describe a body are essentially equivalent from the point of view of using them in polynomial-time algorithms. More exactly, if the body is given by any of these oracles, we can compute the answer of any other in polynomial time.

In this field one mostly uses *separation oracles* which, given a point y and a body K, either decide that $y \in K$ or deliver a separating hyperplane. For our present purposes, the most convenient oracle is the closely related *optimization oracle* which, given a vector $u \neq 0$ in $\mathbb{R}^n$ returns the value $\max\{u^T x : x \in K\}$.

To be precise, the equivalence of oracles mentioned above is valid only for their "weak" versions, reflecting the fact that we cannot avoid numerical errors. Furthermore one usually needs a *guarantee* consisting of two numbers $r, R > 0$ such that K is contained in the ball of radius R about the origin and contains some ball of radius r. For the optimization oracle, this means that the input is a rational vector $u \in \mathbb{R}^n \setminus \{0\}$ and an $\varepsilon > 0$, and the oracle returns a value γ such that $|\gamma - \max\{u^T x : x \in K\}| \leq \varepsilon$.

For the simplicity of presentation, we assume throughout this paper that bodies are presented by strong optimization oracles. For the lower bounds on complexity, this gives stronger results than having weak oracles; for the upper bounds, it would be easy to modify the arguments (and the statements of the results) and allow weak oracles. (One may use, e.g., the methods described in [16].) Also, we assume that we have exact real arithmetic; it would again be easy to make modification so as to accommodate the restriction to rational arithmetic with the usual binary encoding.

3. Results

3.1. ℓ_p **spaces.** We begin by stating our results on the error of deterministic polynomial-time approximation of radii and norm-maxima in arbitrary ℓ_p spaces.

Theorem 3.1. *(a) For each p with $1 \leq p < \infty$, the l_p circumradius, diameter, and norm-maximum of bodies in $\mathbb{R}^n$ can be deterministically approximated in polynomial time with relative error*

$$
\begin{aligned}
&O\left(n^{1/2}\right) && \textit{for } p = 1\\
&O\left(\frac{n^{1/2}}{(\log n)^{1-1/p}}\right) && \textit{for } 1 < p \leq 2\\
&O\left(\left(\frac{n}{\log n}\right)^{\frac{1}{p}}\right) && \textit{for } 2 < p < \infty.
\end{aligned}
$$

In l_∞ spaces circumradius, diameter, and norm-maximum can be computed in oracle-polynomial-time.

(b) In l_1 spaces inradius and width can be computed in oracle-polynomial-time. For each p with $1 < p \leq \infty$, the l_p inradius and width of bodies in $\mathbb{R}^n$ can be deterministically approximated in polynomial time with relative error

$$
\begin{aligned}
&O\left(\left(\frac{n}{\log n}\right)^{1-\frac{1}{p}}\right) && \textit{for } 1 < p \leq 2\\
&O\left(\frac{n^{1/2}}{(\log n)^{1/p}}\right) && \textit{for } 2 < p < \infty\\
&O\left(n^{1/2}\right) && \textit{for } p = \infty.
\end{aligned}
$$

These results are obtained by generalization and refinement of a construction of Kochol [14] that uses Hardamard matrices. The following result shows that the above bounds are tight or at least tight up to the exponent in the logarithmic term. The result of Bárány and Füredi [1] mentioned in the introduction is the special case $p = 2$. The general result relies on techniques of Carl and Pajor [3], [4].

Theorem 3.2. *(a) For each p with $1 \leq p < \infty$, the relative error in deterministic polynomial-time approximation of the l_p circumradius, diameter, and norm-maximum of bodies in $\mathbb{R}^n$ is at least*

$$
\begin{aligned}
&\Omega\left(\frac{n^{1/2}}{\log n}\right) && \textit{for } p = 1\\
&\Omega\left(\left(\frac{n}{\log n}\right)^{1/2}\right) && \textit{for } 1 < p \leq 2\\
&\Omega\left(\left(\frac{n}{\log n}\right)^{1/p}\right) && \textit{for } 2 < p < \infty.
\end{aligned}
$$

(b) For each p with $1 < p \leq \infty$, the relative error in deterministic polynomial-time approximation of the l_p inradius and width of bodies in $\mathbb{R}^n$ is at least

$$\Omega\left(\left(\frac{n}{\log n}\right)^{1-\frac{1}{p}}\right) \quad \textit{for } 1 < p \leq 2$$
$$\Omega\left(\left(\frac{n}{\log n}\right)^{1/2}\right) \quad \textit{for } 2 < p < \infty$$
$$\Omega\left(\frac{n^{1/2}}{\log n}\right) \quad \textit{for } p = \infty.$$

3.2. **Euclidean space.** In all that follows, $m(K)$ will denote the euclidean circumradius, the diameter, the inradius or the width of K, or the norm-maximum $\max_{x\in K} \|x\|_2$ over K in $\mathbb{E}^n$.

The following result extends that of Theorem 3.1 for $p = 2$ by describing a tradeoff between the number of oracle calls and the relative error.

Let $0 < r < 1$ and H be a hyperplane in $\mathbb{R}^n$ at distance r from the origin. Then the set of points on the unit sphere separated from the origin by H is called an *r-cap*.

Theorem 3.3. *For each $0 < r < 1$, there is a deterministic algorithm $\mathcal{A}$ that finds, for every body $K \subset \mathbb{R}^n$, a value $m_{\mathcal{A}}(K)$ with $rm(K) \leq m_{\mathcal{A}}(K) \leq m(K)$. $\mathcal{A}$ does this by using an oracle call for each of the $O(\frac{1}{r^2}e^{12r^2n})$ vectors that determine a cover of the sphere with r-caps that can be constructed with $O(\frac{n^2}{r^2}e^{12r^2n})$ operations.*

While randomized approximation of volume is superior, in terms of complexity estimates, to deterministic approximation, the following main result shows that randomization does not decrease the relative error made in polynomial-time approximation of radii and norm-maxima. In fact, the bound is the same as the lower bound of Bárány and Füredi [1] for the deterministic case.

Theorem 3.4. *If $\mathcal{A}$ is a randomized algorithm that uses polynomially many oracle calls to compute an approximation $m_{\mathcal{A}}(K)$ for each body $K \subset \mathbb{E}^n$, then there is a $c > 0$ such that in every dimension n there exists a body $K_0 \subset \mathbb{E}^n$ with*

$$\operatorname{prob}(m_{\mathcal{A}}(K_0) \leq m(K_0) \leq c\sqrt{\frac{n}{\log n}}\, m_{\mathcal{A}}(K_0)) < \frac{1}{4}.$$

The proof of this theorem uses techniques and ideas from Lovász and Simonovits [15], who showed that no randomized polynomial-time algorithm can approximate the euclidean diameter by a factor of $O(n^{1/4})$. In fact, the following more general tradeoff between approximation and the number of oracle calls can be shown:

Theorem 3.5. *Suppose λ is a real number in the interval $(2, \sqrt{n})$. If a randomized algorithm $\mathcal{A}$ computes an approximation $m_{\mathcal{A}}(K)$ of $m(K)$ for each body $K \subset \mathbb{E}^n$, and $\mathcal{A}$ is such that*

$$\operatorname{prob}\left(m_{\mathcal{A}}(K) \leq m(K) \leq \frac{\sqrt{n}}{\lambda} m_{\mathcal{A}}(K)\right) \geq \frac{3}{4}$$

for each K, then $\mathcal{A}$ must make at least $\lambda 2^{\lambda^2/2}$ calls on the oracle.

Let us remark that a similar statement is true if the bound 3/4 for the probability is replaced by any constant greater than 1/2.

Choosing $\lambda = \sqrt{2h\log n}$, Theorem 3.5 yields, the following relation between the quality of approximation and the degree of polynomiality of the algorithm:

Corollary 3.6. *Let $h > 0$ and let $\mathcal{A}$ be a randomized polynomial-time algorithm which for each body $K \subset \mathbb{R}^n$ uses $O(n^{h+1})$ oracle calls to compute two values $\underline{m}_{\mathcal{A}}(K)$ and $\overline{m}_{\mathcal{A}}(K)$ such that*

$$\operatorname{prob}(\underline{m}_{\mathcal{A}}(K) \leq m \leq \overline{m}_{\mathcal{A}}(K)) \geq \frac{3}{4}.$$

Then for some $K_0 \subset \mathbb{E}^n$,

$$\frac{\overline{m}_{\mathcal{A}}(K_0)}{\underline{m}_{\mathcal{A}}(K_0)} \geq \sqrt{\frac{n}{2h\log n}}.$$

On the other side:

Theorem 3.7. *There is a $k_0 \in \mathbb{N}$ and a randomized algorithm $\mathcal{A}$ which, given a body $K \subset \mathbb{E}^n$ and $k \in \mathbb{N}$ with $k_0 \leq k \leq 2^n$, uses a random choice of less than k vectors of $\mathbb{B}^n$ to compute an estimate $m_{\mathcal{A}}(K)$ of $m(K)$ such that $m_{\mathcal{A}}(K) \leq m(K)$ and*

$$\operatorname{prob}\left(m(K) \leq \sqrt{\frac{2n}{\log k}}\, m_{\mathcal{A}}(K)\right) > \frac{6}{7}.$$

Note that standard techiques can be used to boost the lower bound for the probability arbitrarily close to 1.

4. Algorithms and geometric parameters

For simplicity attention in this section is restricted to the euclidean case.

Let $0 < r < 1$ and let $\tau(n,r)$ denote the minimum number of r-caps covering the unit sphere. Equivalently, $\tau(n,r)$ is the minimum number of facets of an $\mathcal{H}$-approximation P of the unit ball $\mathbb{B}^n$ with $\mathbb{B}^n \subset P \subset 1/r\mathbb{B}^n$.

The following theorem shows that the oracle complexity of deterministic algorithms for radii and norm-maximum computation is mainly determined by the function τ.

Theorem 4.1. *(a) For each $0 < r < 1$ there is a deterministic algorithm $\mathcal{A}$ that is based on a covering on the sphere with $\tau(n,r)$ spherical r-caps which, for every body $K \subset \mathbb{E}^n$ given by an optimization oracle, uses $2\tau(n,r)$ oracle calls to compute a value $m_{\mathcal{A}}(K)$ such that $rm(K) \leq m_{\mathcal{A}}(K) \leq m(K)$.*

(b) If $0 < r < 1$ and $\mathcal{A}$ is a deterministic algorithm that computes, for every body $K \subset \mathbb{R}^n$, an estimate $m_{\mathcal{A}}(K)$ of $m(K)$ such that

$$rm(K) < m_{\mathcal{A}}(K) \leq m(K),$$

then $\mathcal{A}$ must make at least $\tau(n,r)/2$ oracle calls in the worst case.

Proof. (a) Let $k = \tau(n,r)$ and let P denote an $\mathcal{H}$-approximation of $\mathbb{B}^n$ with $\mathbb{B}^n \subset P \subset 1/r\mathbb{B}^n$ with outer facet normals $\pm u_1, \ldots, \pm u_k$ such that $P = \{x : \pm u_i^T x \leq 1 \text{ for } i = 1, \ldots, k\}$. To approximate the circumradius of K, use the optimzation oracle for K to compute the $2k$ numbers $\delta_i^{\pm} = \max_{x\in K} \pm u_i^T x$. Then the circumradius of K with respect to the polytopal norm induced by P is given as the solution of the linear program

$$\min \rho \quad \text{s. th. } \rho \pm u_i^T a \geq \delta_i^{\pm} \text{ for } i = 1, \ldots, k,$$

cf. [10]. (Note that a is a center of K's circumradius with respect to the polytopal norm.) Of course, this is the desired approximation for K's euclidean circumradius. (Note that we could actually save a factor 2 by just working with $u_1, \ldots, u_k$. This factor is however needed for the diameter.)

The results for the other radii and the norm-maximum follow readily with the aid of suitable geometric transformations and polarity; see [9].

(b) We will give the argument in detail again for the circumradius. The results for the other radii and the norm-maximum follow similarly.

Suppose that $\mathcal{A}$ makes at most t calls on the optimization oracle, where $t < \tau(n,r)/2$. Apply $\mathcal{A}$ first when $K = \mathbb{B}^n$, thus obtaining t points $u_1, \ldots, u_t$ of the unit sphere. Since $t < \tau(n,r)/2$, there is a point v on the unit sphere such that neither v nor $-v$ is covered by the r-caps centered at $u_1, \ldots, u_t$. Equivalently, the r-caps centered at v and at $-v$ do not contain any of the points $u_1, \ldots, u_t$.

This means that $\mathcal{A}$ cannot distinguish between $\operatorname{conv}\{u_1, \ldots, u_t\}$, $\mathbb{B}^n$ and $\operatorname{conv}(\mathbb{B}^n \cup \{\frac{1}{r}v, -\frac{1}{r}v\}$: the optimization oracle will always return the *same hyperplanes*. Hence the (asymmetric) relative error is at least $1/r$. □

We can prove a similar result for randomized algorithms, showing that the complexity of the algorithm depends on the area of r-caps. Let $\gamma(n,r)$ denote the ($(n-1)$-dimensional) measure of an r-cap, divided by the total measure of the l_2 unit sphere in $\mathbb{R}^n$. It is also convenient to introduce $\tau^*(n,r) = 1/\gamma(n,r)$, which could be viewed as the "fractional covering number" of the sphere by r-caps. Clearly $\tau^*(n,0) = 2$ and $\tau^*(n,r) \leq \tau(n,r)$.

Theorem 4.2. *(a) For each $0 < r < 1$ there is a randomized algorithm that is based on a "randomized covering" on the sphere with $2\lceil\tau^*(n,r)\rceil$ spherical r-caps which, for every body $K \subset \mathbb{R}^n$ given by an optimization oracle, computes an approximation $m_{\mathcal{A}}(K)$ of $m(K)$ such that $m_{\mathcal{A}}(K) \leq m(K)$ and*

$$\operatorname{prob}\Big(rm(K) \leq m_{\mathcal{A}}(K)\Big) > \frac{6}{7}.$$

(b) Let $0 < r < 1$, and let $\mathcal{A}$ be a randomized algorithm that computes, for every body $K \subset \mathbb{R}^n$, an estimate $m_{\mathcal{A}}(K)$ of $m(K)$ such that

$$\operatorname{prob}\Big(rm(K) \leq m_{\mathcal{A}}(K) \leq m(K)\Big) \geq \frac{3}{4}.$$

Then $\mathcal{A}$ must make at least $\tau^*(n,r)/4$ oracle calls in the worst case.

Proof. This time we concentrate on the proof for the diameter $\operatorname{diam}(K)$. Similar ideas work for the other radii and for the norm-maximum.

(a) Let $N = 2\lceil\tau^*(n,r)\rceil$ and let $u_1, \ldots, u_N$ be independently, uniformly distributed random points on the unit sphere $\mathbb{S}^{n-1}$. Compute the maxima

$$\begin{aligned}\omega_i &= \max\{u_i^T x : x \in K\} - \min\{u_i^T x : x \in K\} \\ &= \max\{u_i^T (x - y) : x, y \in K\},\end{aligned}$$

and define $\mathbf{D}(K) = m_{\mathcal{A}}(K) = \max_i \omega_i$.

It is obvious that $\mathbf{D}(K) \le \operatorname{diam}(K)$. To prove that the probabilistic condition in (a) is satisfied, suppose that $\mathbf{D}(K) < r\operatorname{diam}(K)$. Let $p, q \in K$ have $\|p-q\|_2 = \operatorname{diam}(K)$, let v be the unit vector pointing in the direction $q-p$, and let C and $-C$ denote the r-caps centered at v and $-v$, respectively. Then C contains no u_i, because if $u_i \in C$ then

$$\begin{aligned}\omega_i &= \max_{x,y\in K} u_i^T(x-y) \ge u_i^T(q-p)\\ &= \operatorname{diam}(K) u_i^T v \ge r\operatorname{diam}(K)\end{aligned}$$

and hence $\mathbf{D}(K) \ge \omega_i \ge r\operatorname{diam}(K)$, contrary to the supposition. Now, the probability that no u_i belongs to C is

$$\begin{aligned}\left(1 - \frac{\operatorname{vol}_{n-1}(C)}{\operatorname{vol}_{n-1}(\mathbb{S}^{n-1})}\right)^N &= \left(1 - \frac{1}{\tau^*(n,r)}\right)^N\\ &< \exp\left(-\frac{N}{\tau^*(n,r)}\right)\\ &\le e^{-2} < \frac{1}{7}.\end{aligned}$$

(b) Suppose that $\mathcal{A}$ makes at most t oracle calls, where $t < \tau^*(n,r)/2$. Choose $r' < r$ so that $t < \tau^*(n,r')/2$. Run two copies of the algorithm simultaneously. In one, the input is the unit ball $\mathbb{B}^n$. In the other, an input body K is constructed at random as follows: we choose a random unit vector v uniformly, and let K be the convex hull of the set $\mathbb{B}^n \cup \{(1/r')v, -(1/r')v\}$. The algorithm has internal coin flips, and we use the same coin flips in both copies. Let $\mathbf{D}$ and $\mathbf{D}'$ be the outputs of the two algorithms (these are random variables, depending on the internal coin flips of the algorithms as well as on the random choice of v).

Let $u_1, \dots, u_t$ be the unit vectors for which the optimization oracle is called with input $\mathbb{B}^n$, let $C_1, \dots, C_t$ be the r-caps centered at $u_1, \dots, u_t$, and let $Q = C_1 \cup \cdots \cup C_t$. Then

$$\begin{aligned}\operatorname{prob}(v \in Q) &= \frac{\operatorname{vol}_{n-1}(Q)}{\operatorname{vol}_{n-1}(\mathbb{S}^{n-1})}\\ &\le \sum_{i=1}^{t} \frac{\operatorname{vol}_{n-1}(C_i)}{\operatorname{vol}_{n-1}(\mathbb{S}^{n-1})}\\ &= \frac{t}{\tau^*(n,r')} < \frac{1}{2}.\end{aligned}$$

Whenever $v \notin Q$, the two copies of the algorithm run in the same way and produce the same output. Thus $\operatorname{prob}(\mathbf{D} \ne \mathbf{D}') < \frac{1}{2}$.

By the assumptions on the performance of $\mathcal{A}$ we also know that

$$\begin{aligned}\operatorname{prob}(\mathbf{D}' \le 2) &= \operatorname{prob}(\mathbf{D}' \le r'\operatorname{diam}(K))\\ &\le \operatorname{prob}(\mathbf{D}' < r\operatorname{diam}(K)) \le \frac{1}{4}\end{aligned}$$

and

$$\operatorname{prob}(2 < \mathbf{D}) = \operatorname{prob}(\operatorname{diam}(\mathbb{B}^n) < \mathbf{D}) \le \frac{1}{4}.$$

But this means that the three events

$$\mathbf{D} \le 2, \quad 2 < \mathbf{D}', \quad \text{and} \quad \mathbf{D} = \mathbf{D}'$$

occur with positive probablity. Hence we reach the contradictory conclusion that $2 < 2$. □

5. Estimates and proofs

We will again begin by dealing with the euclidean case. At the end of this section we will sketch how the results can be extended to arbitrary ℓ_p spaces.

The previous results reduce the problem of analyzing the error of the algorithms to estimating $\tau(n,r)$ and $\tau^*(n,r)$. The latter (corresponding to the case of randomized algorithms) is easier and a fairly complete answer is well known. Denoting by

$$\omega_n = \frac{\pi^{n/2}}{\Gamma(1+n/2)}$$

the volume of the n-dimensional euclidean unit ball, one has

$$\frac{1}{\tau^*(n,r)} = \gamma(n,r) = \frac{(n-1)\omega_{n-1}}{n\omega_n} \int_r^1 (1-t^2)^{\frac{n-3}{2}}\, dt,$$

whence, using the fact that

$$\sqrt{\frac{n}{2\pi}} < \frac{\omega_{n-1}}{\omega_n} < \sqrt{\frac{n+1}{2\pi}},$$

the following estimates can be derived:

Lemma 5.1. *For* $2/\sqrt{n} < r < 1$,

$$\frac{1}{10r\sqrt{n}}(1-r^2)^{\frac{n-1}{2}} < \gamma(n,r) < \frac{1}{2r\sqrt{n}}(1-r^2)^{\frac{n-1}{2}}.$$

Proof. Define

$$J_m^h(r) = \int_r^1 t^{-h}(1-t^2)^{m/2}\, dt.$$

Then we may apply partial integration with $u(t) = (1-t^2)^{\frac{m+2}{2}}/(m+2)$ and $v(t) = -t^{-h-1}$:

$$\begin{aligned} (m+2)J_m^h(r) &= \left[\frac{-(1-t^2)^{\frac{m+2}{2}}}{t^{h+1}}\right]_r^1 \\ &\quad -(h+1)\int_r^1 t^{-h-2}(1-t^2)^{\frac{m+2}{2}}\,dt \\ &= \frac{1}{r^{h+1}}(1-r^2)^{\frac{m+2}{2}} - (h+1)J_{m+2}^{h+2}(r). \end{aligned}$$

Hence

$$(m+2)J_m^h(r) < \frac{1}{r^{h+1}}(1-r^2)^{\frac{m+2}{2}}$$

and

$$\begin{aligned} (m+2)J_m^h(r) &> \frac{1}{r^{h+1}}(1-r^2)^{\frac{m+2}{2}} \\ &\quad -\frac{(h+1)}{(m+4)}\frac{1}{r^{h+3}}(1-r^2)^{\frac{m+4}{2}}. \end{aligned}$$

We need this for $h=0$:

$$\begin{aligned} &\frac{1}{r}(1-r^2)^{\frac{m+2}{2}} - \frac{1}{(m+4)}\frac{1}{r^3}(1-r^2)^{\frac{m+4}{2}} \\ &< (m+2)J_m^0(r) < \frac{1}{r}(1-r^2)^{\frac{m+2}{2}} \end{aligned}$$

The above is true for all r. Now for $r \geq 2/\sqrt{m+4}$, we obtain

$$\frac{1}{2r}(1-r^2)^{\frac{m+2}{2}} < (m+2)J_m^0(r) < \frac{1}{r}(1-r^2)^{\frac{m+2}{2}},$$

which proves the lemma. □

Theorems 3.5 and 3.7 follow from the above estimates in conjunction with Theorem 4.2 and the fact that $\tau^*(n,r) = 1/\gamma(n,r)$.

In the case of deterministic algorithms, one has to estimate $\tau(n,r)$. In fact, more is needed: it is not enough to know the existence of a "small" covering of the sphere by r-caps, one needs a polynomial-time algorithm to construct one. The following result is essentially due to Kochol [14].

Lemma 5.2. *For the covering number $\tau(n,r)$ of the euclidean sphere by r-caps, the following estimates are valid when $r > 2/\sqrt{n}$:*

$$2r\sqrt{n}\,e^{(1/2)r^2(n-1)} \leq \tau(n,r) \leq \left(\frac{1}{4r^2}+1\right)e^{12r^2n}.$$

The lower bound follows easily from Lemma 5.1, and we invoke a result of Kochol [14] for the upper bound. For every n and $0 < r < 1$, he constructs a covering of the n-sphere by at most $T(n,r) = O(e^{9r^2n}/r^2)$ r-caps. It is important that the construction can be carried out in $O(n^2T(n,r))$ time. This means that counting only oracle calls, the number of other operations that are ignored is only a polynomial factor larger.

Kochol's construction. Let $R = \frac{\sqrt{n}}{1-r}$. Take all integer vectors z with $\|z\|_2 \leq R$, and normalize them so that they have unit length. Let A_r be the resulting set of unit vectors.

Lemma 5.3. *The set A_r has the following properties:*

(a) the r-caps about the points in A_r cover the sphere;

(b) $|A_r| \leq \left(\frac{9(3-r)}{4(1-r)}\right)^n$.

Proof. (a) Since A_r is invariant under changes of signs of coordinates, it suffices to show that each non-negative vector $v = (v_1, \ldots, v_n)^T \in \mathbb{S}^{n-1}$ belongs to the r-cap about some point of A_r. With $z_i = \lfloor Rv_i \rfloor$, $z = (z_1, \ldots, z_n)^T$ and $u = (1/\|z\|_2)z$, it is clear that $u \in A_r$, and since

$$\begin{aligned} u^Tv &= \frac{1}{\|z\|_2}\sum_{i=1}^n \lfloor Rv_i \rfloor v_i \\ &\geq \frac{1}{R}\sum_{i=1}^n (Rv_i - 1)v_i \\ &= 1 - \frac{1}{R}\sum_{i=1}^n v_i \geq 1 - \frac{\sqrt{n}}{R} = r, \end{aligned}$$

v belongs to the r-cap about u.

(b) The ball $\frac{3-r}{2(1-r)}\sqrt{n}\mathbb{B}^n$ contains all cubes $a + (1/2)[-1,1]^n$ with $a \in \mathbb{Z}^n \cap R\mathbb{B}^n$. So it follows from Stirling's formula that

$$\begin{aligned} |A_r| &\leq \frac{(\frac{3-r}{2(1-r)}\sqrt{n})^n \pi^{n/2}}{\Gamma(1+n/2)} \\ &\leq \frac{(2e\pi)^{n/2}}{\sqrt{2\pi}}\left(\frac{3-r}{2(1-r)}\right)^n < \left(\frac{9(3-r)}{4(1-r)}\right)^n. \end{aligned}$$

□

The set A_r is good if r is large (say $r \geq 1/2$), but not if r is small; in particular, it is never of polynomial size. For $r = 1/2$ it yields at most 12^n points, and this fact is needed below. However, we can use A_r to construct a better covering A_r^* when $r < 1/2$.

Let $d = \lceil 4r^2 n \rceil$. Subdivide the interval $\{1, \ldots, n\}$ into segments of length d. More exactly, let $t = \lfloor n/d \rfloor$, and set $I_j := \{m : \lfloor m/d \rfloor = j\}$ for $j = 0, \ldots, t$. (Although the length of I_t may be less than d, we assume for simplicity that it is equal to d.)

For each interval I_j, consider the d–dimensional euclidean unit ball $\mathbb{B}_j^d$ in the coordinate subspace of $\mathbb{E}^n$ of those coordintes belonging to I_j, and fix in it a set A_j so that the (1/2)-caps centered at the points in A_j cover the unit d-sphere. Consider each A_j as a proper subset of $\mathbb{E}^n$, and let A_r^* be their union. By Lemma 5.3(b), we can choose the A_j so that A_r^* is a set of at most $\lceil \frac{n}{d} \rceil 12^d < (\frac{1}{4r^2} + 1)12^{4r^2 n+1}$ unit vectors. Note that for $r = O(\sqrt{(\log n)/n})$, this is polynomial in n.

Lemma 5.4. *The r-caps centered at the points contained in A_r^* cover the unit n-sphere.*

Proof. If $v \in \mathbb{R}^n$ is an arbitrary unit vector, then for some j we have $\sum_{i \in I_j} v_i^2 \geq d/n$. The projection w of v onto the corresponding subspace is of length at least $\sqrt{\frac{d}{n}} \geq 2r$. Hence by Lemma 5.3(a), there is a vector $u \in A_j$ such that $v^T u = w^T u \geq r$. □

Lemmas 5.3 and 5.4 prove Lemma 5.2. Combining this with Theorem 4.1, we get Theorem 3.3.

To prove Theorem 3.1, we need to generalize the deterministic construction in l_2-spaces to l_p spaces. This is facilitated with the aid of the fact that for $1 \leq p \leq q \leq \infty$,

$$\|x\|_q \leq \|x\|_p \leq n^{1/p-1/q} \|x\|_q \quad \text{for each } x \in \mathbb{R}^n.$$

(Here $1/\infty = 0$.) This yields polynomial-size $\mathcal{H}$-approximations P of the unit ball with $\mathbb{B}_p^n \subset P \subset O((n/\log n)^{1/p})\mathbb{B}^n$, and these turn out to be asymptotically optimal for $p \geq 2$. When $1 \leq p < 2$, we need to apply suitable rotations by Hadamard matrices.

For the proof of Theorem 3.2, note that lower bounds for the relative error can be obtained again from lower bounds for suitable polynomial-size $\mathcal{H}$- or $\mathcal{V}$-approximation of the l_p unit ball, and these can be obtained by applying results of [3] and [4].

Acknowledgments. We would like to thank Noga Alon, Imre Bárány, and Bernd Carl for valuable discussions.

References

[1] I. Bárány and Z. Füredi (1986): Computing the volume is difficult, *Proc. of the 18th Annual ACM Symposium on Theory of Computing*, pp. 442–447.

[2] A. Brieden, P. Gritzmann, R. Kannan, V. Klee, L. Lovász and M. Simonovits (1998): Approximation of Radii and Norm-Maximia: Upper and lower bounds for deterministic and randomized oracle-polynomial-time algorithms, in preparation.

[3] B. Carl (1985): Inequalities of Bernstein-Jackson-type and the degree of compactness of operators in Banach spaces, *The Annales de l'Institute Fourier* **35**, pp. 79–118.

[4] B. Carl and A. Pajor (1988): Gelfand numbers of operators with values in a Hilbert space, *Inventiones mathematicae* **94**, pp. 479–504.

[5] M. Dyer and A. Frieze (1988): On the complexity of computing the volume of a polytope. *SIAM J. Comp.* **17**, pp. 967–974.

[6] M. Dyer, A. Frieze and R. Kannan (1989): A random polynomial time algorithm for approximating the volume of convex bodies, *Proc. of the 21st Annual ACM Symposium on Theory of Computing*, pp. 375–381.

[7] G. Elekes (1986): A geometric inequality and the complexity of computing volume, *Discrete and Computational Geometry* **1**, pp. 289–292.

[8] R.M. Freund and J.B. Orlin (1985): On the complexity of four polyhedral set containment problems, Math. Programming, **33** (1985) **2** pp. 139–145.

[9] P. Gritzmann and V. Klee (1992): Inner and outer j-radii of convex bodies in finite-dimensional normed spaces, *Discrete and Computational Geometry*, **7**, pp. 255–280.

[10] P. Gritzmann and V. Klee (1993): Computational complexity of inner and outer j-radii of polytopes in finite dimensional normed spaces, *Mathematical Programming*, **59**, pp. 163–213.

[11] M. Grötschel, L. Lovász and A. Schrijver (1988): *Geometric Algorithms and Combinatorial Optimization*, Springer-Verlag.

[12] R. Kannan, L. Lovász and M. Simonovits, (1998): Random walks and an $O^*(n^5)$ volume algorithm for convex bodies, *Random Structures and Algorithms*, **11**, pp. 1–50.

[13] L. G. Khachiyan (1988): On the complexity of computing the volume of a polytope. *Izvestia Akad. Nauk SSSR, Engineering Cybernetics* **3**, pp. 216–217.

[14] M. Kochol (1994): Constructive approximation of a ball by polytopes, *Math. Slovaca* **44** no 1, pp. 99–105.

[15] L. Lovász and M. Simonovits (1991): On the randomized complexity of the volume and diameter, Proc. 33rd IEEE FOCS, pp. 482–491.

[16] L. Lovász and M. Simonovits (1993): Random walks in a convex body and an improved volume algorithm, *Random Structures and Algorithms* **4**, pp. 359–412.